DISEÑO DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN PARA EL INSTITUTO TOLIMENSE DE FORMACIÓN TÉCNICA PROFESIONAL-ITFIP PARA EL DEPARTAMENTO DE SISTEMAS, BAJO LA NORMA ISO 27001:2013

MARIO ANDRES PADILLA UBAQUE

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
IBAGUE
2019

DISEÑO DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN PARA EL INSTITUTO TOLIMENSE DE FORMACIÓN TÉCNICA PROFESIONAL-ITFIP PARA EL DEPARTAMENTO DE SISTEMAS, BAJO LA NORMA ISO 27001:2013

MARIO ANDRES PADILLA UBAQUE

Trabajo de grado para optar por el título de:
Especialista en Seguridad Informática

Director de proyecto:
EDUARD ANTONIO MANTILLA TORRES

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
IBAGUE
2019

Nota de Aceptación:

_____
_____
_____
_____
_____
_____

_____
Firma del presidente del jurado

_____
Firma del Jurado

_____
Firma del Jurado

AGRADECIMIENTOS

Los autores expresan su agradecimiento a:

Al Dr. Mario Fernando, por su apoyo en la financiación y autorización de esta investigación. También al Ingeniero Wilson Mauricio, a los demás ingenieros que trabajan en la dependencia de sistemas: Ingeniero Jhon Darwin, a la Ingeniera Melissa y al Tecnólogo. Sebastián. Nos brindaron sus conocimientos e información en el funcionamiento de la dependencia que se estaba investigación.

Por último, a cada uno de los tutores que nos formaron en esta etapa educativa

Gracias a todos.

CONTENIDO

LISTA DE TABLAS

LISTA DE ILUSTRACIONES

GLOSARIO

ACTIVO: "componente o funcionalidad de un sistema de información susceptible de ser atacado deliberada o accidentalmente con consecuencias para la organización. Incluye: información, datos, servicios, aplicaciones (software), equipos (hardware), comunicaciones, recursos administrativos, recursos físicos y recursos humanos". [1]

ANÁLISIS DE RIESGOS: "proceso sistemático de la información disponible para identificar peligros y estimar riesgos". [2]

ANÁLISIS DE IMPACTO: estudio de las consecuencias y amenazas que tendría una organización y que tanto la afectaría.

AUTENTICIDAD: "propiedad o característica consistente en que una entidad es quien dice ser o bien que garantiza la fuente de la que proceden los datos".[3]

CONFIDENCIALIDAD: "propiedad o característica consistente en que la información ni se pone a disposición, ni se revela a individuos, entidades o procesos no autorizados".[4]

DIMENSIÓN DE SEGURIDAD: es el aspecto o valor de importancia que se le asigna al activo, según el perjuicio que tendría la organización perderlo.

DISPONIBILIDAD: "propiedad o característica de los activos consistentes en que las entidades o procesos autorizados tienen acceso a los mismos cuando lo requieren".[5]

INTEGRIDAD: "propiedad o característica consistente en que el activo de información no ha sido alterado de manera no autorizada".[6]

POLÍTICAS DE SEGURIDAD: "conjunto de directrices plasmadas en un documento escrito, que rigen la forma en que una organización gestiona y protege la información y servicios que considera críticos".[7]

---

[1] CNIS 2018 VIII Congreso Nacional de Innovación y Servicios Públicos – Glosario Seguridad. [en línea], 2018 [revisado 29 octubre 2018]. Disponible en Internet: http://www.cnis.es/glosario-seguridad/

[2] Ibid.

[3] Ibid.

[4] Ibid.

[5] Ibid.

[6] Ibid.

[7] Ibid.

SALVAGUARDA: conjunto de pasos que con la ayuda de la tecnología reducen el riesgo.

SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN (SGSI): según ISO 27001, "consiste en preservar la confidencialidad, integridad y disponibilidad, además de todos los sistemas implicados en el tratamiento dentro de la organización." [8]

TRAZABILIDAD: "propiedad o característica consistente en que las actuaciones de una entidad pueden ser imputadas exclusivamente a dicha entidad".[9]

[8] ISO27001 – Sistema de Gestión de la Seguridad de la información. [en línea], 2018 [revisado 29 octubre 2018]. Pág.: 3 Disponible en Internet: http://www.iso27000.es/download/doc_sgsi_all.pdf

[9] CNIS 2018 VIII Congreso Nacional de Innovación y Servicios Públicos – Glosario Seguridad. [en línea], 2018 [revisado 29 octubre 2018]. Disponible en Internet: http://www.cnis.es/glosario-seguridad/

1. RESUMEN

El presente proyecto de grado se enfocó en la elaboración del diseño de un sistema de gestión de seguridad de la información (SGSI) en la dependencia de sistemas en la Institución de Educación Superior – ITFIP del Espinal, Tolima. Para llevar a cabo este proyecto se basó en la norma ISO 27001:2013 utilizando como herramienta metodológica para el análisis y gestión de riesgos MAGERIT V3.

La norma ISO 27001:2013 para establecer y gestionar un SGSI, hace uso de las fases de la metodología PHVA (Planificar-Hacer-Verificar-Actuar), ya que es tradicional en los sistemas de gestión de calidad. Para el desarrollo del proyecto se especifican cuatro capítulos, que se detallan de la siguiente manera:

En primer lugar se documenta datos elementales del proyecto, como lo son el título, planteamiento del problema, justificación, objetivos, alcances y limitaciones, también el respectivo marco teórico de la norma ISO 27001:2013 junto con una descripción de cada uno de los libros de la metodología, con su respectivo marco conceptual; detallando los términos elementales de MAGERIT V3, se define su respectivo cronograma de actividades.

Se describe el contexto organizacional, se realiza el reconocimiento y se describe la estructura organizacional. A partir de ahí se empieza con el diagnóstico de la organización con respecto a la norma ISO/IEC 27001:2013, de acuerdo con los diferentes dominios de la misma.

A continuación se realiza un análisis y gestión de riesgos, en donde se utiliza una herramienta propietaria llamada MAGERIT V3; con ella, se especifica paso a paso como encontrar los riesgos sobre cada activo a través de la identificación del inventario de activos, determinar la valorización de los activos, analizar las amenazas, estimar el impacto y riesgo potencial e identificación de las salvaguardas.

Posteriormente, se realiza una declaración aplicabilidad, que consiste en describir los 14 dominios que tiene la ISO 27001:2013 con cada uno de sus controles y por medio de una entrevista al gerente o en este caso al rector del ITFIP. Se explica cada uno de ellos y este decide en si los aplicara, en la organización.

Por último, se proponen una serie de políticas y lineamientos de seguridad de la información de acuerdo con análisis, que servirán para que los activos de información sean mucho más seguros.

Palabras Claves: Metodología, factibilidad, seguridad, valorización, salvaguardas.

2. ABSTRACT

This degree project focused on the development of the design of an information security management system (ISMS) in the dependence of systems in the Institution of Higher Education - ITFIP del Espinal, Tolima. To carry out this project, it was based on the ISO 27001: 2013 standard, using as a methodological tool for the analysis and management of MAGERIT V3 risks.

The ISO 27001: 2013 standard to establish and manage an ISMS makes use of the phases of the PHVA methodology (Plan-Do-Verify-Act), since it is traditional in quality management systems. Four chapters are specified for the development of the project, which are detailed as follows:

In the first place, elementary data of the project is documented, such as the title, problem statement, justification, objectives, scope and limitations, also the respective theoretical framework of ISO 27001: 2013 together with a description of each of the books of the methodology, with its respective conceptual framework; detailing the elementary terms of MAGERIT V3, its respective schedule of activities is defined.

The organizational context is described, recognition is made and the organizational structure is described. From there it begins with the diagnosis of the organization with respect to ISO / IEC 27001: 2013, according to the different domains of it.

A risk analysis and management is then carried out, where a proprietary tool called MAGERIT V3 is used; with it, it is specified step by step how to find the risks on each asset through the identification of the asset inventory, determine the valuation of the assets, analyze the threats, estimate the potential impact and risk and identify the safeguards.

Subsequently, an applicability statement is made, which consists of describing the 14 domains that ISO 27001: 2013 has with each of its controls and through an interview with the manager or in this case the ITFIP rector. Each of them is explained and he decides if he will apply them, in the organization.

Finally, a series of information security policies and guidelines are proposed in accordance with analysis, which will make information assets much safer.

Keywords: Methodology, feasibility, security, recovery, safeguards.

3. INTRODUCCIÓN

Desde hace algunos años la información se ha venido considerando como uno de los activos más valiosos que tiene una organización, la pérdida de esta no solamente afectaría a la misma de manera económica, sino que también afectaría a la imagen de la propia. Por eso, es por lo que cada vez más, la seguridad de la información es objetivo principal dentro de las organizaciones, sin embargo, a pesar de conocer los riesgos que pueden tener con la perdida de la información, muchas compañías no se enfrentan a este aspecto con la profundidad con la que debería tratarse.[10]

La continua evolución y crecimiento diario de la tecnología, ha llevado a que, por medio de ella, los ataques cibernéticos a las organizaciones sean más frecuentes, por lo tanto, nace la necesidad de adoptar medidas y controles de seguridad que permitan proteger a la organización de amenazas que puedan afectar los activos informáticos que manejen información.[11] De esta manera se hace necesario realizar estudio que le permita conocer y controlar los riesgos, vulnerabilidades y amenazas a las que está expuesta la información de la empresa.

Por lo tanto el objetivo de este proyecto de grado es el diseño del sistema de gestión de seguridad de la información que permita salvaguardar los recursos informáticos en la Institución de Educación Superior – ITFIP, específicamente en la dependencia de sistemas, debido a que allí se administra gran parte de la información de la organización, teniendo en cuenta los criterios de la ISO 270001:2013, la cual se encarga de gestionar y verificar la confidencialidad, integridad y disponibilidad de la información. Para ello utiliza una herramienta propia llamada MAGERIT, que ofrece un método sistemático para la gestión de riesgos de la información, también es una de las más utilizadas y está reconocida internacionalmente.

Junto a estas herramientas de desarrollo para la seguridad de la información, se contempló la necesidad de aplicar las políticas (seguridad) que se requiere para este tipo de desarrollo experimental, el uso de análisis de datos cualitativos y cuantitativos expuestos a lo largo de la elaboración del proyecto.

[10] AGUIRRE JUAN Y ARISTIZABAL CATALINA. Diseño del Sistema de Gestión de Seguridad de la Información para el grupo empresarial la Ofrenda, 2013 [revisado 29 octubre 2018, Pág. 7]

[11] Calidad y seguridad de la información y auditoría informática, disponible en internet en: http://earchivo.uc3m.es/bitstream/handle/10016/8510/proyectoEsmeralda.pdf;jsessionid=10850A53006DB846CED4EDCEDEDE1C40?sequence=1 [revisado 29 octubre 2018, Pág. 9]

4. DEFINICIÓN DEL PROBLEMA

4.1. PLANTEAMIENTO DEL PROBLEMA

La información es uno de los activos más importantes que tiene cualquier organización. Esta le da gestión y continuidad al negocio, ayudando a priorizar actividades dando cumplimiento a diferentes objetivos que se puedan tener[12].

Existen unos parámetros y normas que se establecen para darle una certidumbre a lo mencionado, para esto existe el concepto de sistema de gestión de seguridad de la información (SGSI).Un Sistema de gestión de seguridad de la información (SGSI), es la parte de un sistema de gestión global basado directamente en los riesgos para el negocio y los activos de este contemplado en la norma ISO 27001[13], ayuda a las empresas a gestionar de una forma eficaz la seguridad de la información, evitando las amenazas presentes en el entorno y dentro de la misma, la implementación de controles proporcionado coste menos elevado, riesgos rutinarios con la información que allí se maneja.

Cada vez están más en auge las empresas y organizaciones que diseñan un sistema de gestión de seguridad de la información (SGSI). En la actualidad se ha convertido en una técnica utilizada de acuerdo con las circunstancias cambiantes que han generado preocupación y prevención en cada una de las organizaciones[14]. Lo anterior, hace que se establezca como prioridad un sistema de gestión de seguridad de la información como parte relevante de una Organización. En algunos grupos empresariales como ComBanc S.A, Etek International HoldingCorp., Financial Systems Company Ltda., Ricoh Colombia, S.A. están presentes estos sistemas de gestión desde hace muchos años[15], y es la caja fuerte personal (a nivel web), en la que se puede guardar joyas, documentos críticos en papel, o cualquier elemento físico que no debe ser extraviado por el alto valor que tiene.

Asumida en toda la sociedad la importancia de la información concentrada en vídeos, grabaciones de sonido, ficheros, documentos escaneados, fotografías,

---

[12] Lic. Yuniet Rojas Mesa, “De la gestión de información a la gestión del conocimiento”, ACIMED, disponible en: http://scielo.sld.cu/scielo.php?pid=S1024-94352006000100002&script=sci_arttext&tlng=en

[13] ICONTEC, “NORMA TÉCNICA NTC-ISO/IEC COLOMBIANA 27001”, UNAD, disponible en: http://intranet.bogotaturismo.gov.co/sites/intranet.bogotaturismo.gov.co/files/file/NTC-ISO-IEC%2027001.pdf

[14] Jonathan Antonio Hoyos Chaverra, Alejandro Valencia Arias, El papel de las TIC en el entorno organizacional de las Pymes, disponible en: https://revistas.itm.edu.co/index.php/trilogia/article/view/155

[15] Rubén Darío Carvajal herrera, “Seguridad Informática y de Información”. Universidad Tecnológica de Bolívar, disponible en: https://biblioteca.utb.edu.co/notas/tesis/0065029.pdf

planos o todo lo que cada organización considere valioso, se necesita poder guardar cierta información en formato electrónico de modo completamente seguro a salvo de desastres. Por lo tanto en el SGSI a diseñar, una de las medidas más importantes, será el salvaguardar el activo más importante que es la información y establecer los controles necesarios para tal fin.

Se puede pensar si es posible tener diseñado un sistema de gestión de seguridad de la información. No obstante, con el incremento en el uso del entorno digital también se incrementan las amenazas cibernéticas, las vulnerabilidades y los incidentes digitales.[16] Situación que afecta la seguridad de los ciudadanos, de las organizaciones públicas y privadas, e incluso de infraestructuras que hacen parte de los intereses de la nación. Ibíd. Durante los últimos años, Colombia ha sido foco de interés para distintos ataques cibernéticos, los cuales se han sofisticado trayendo consigo el incremento de la efectividad de estos y una mayor dificultad para su oportuna detección. Escenario que preocupa al Gobierno nacional toda vez que las condiciones para desarrollar actividades socioeconómicas en el país cada día se soportan más en el uso de las TIC, y los incidentes digitales en Colombia afectan a varios agentes y sectores, siendo la ciudadanía la mayor afectada.[17]

La seguridad informática entorno a la protección de la información ha tomado una mayor inclinación a aplicarse a cada uno de los procesos que se presentan o llevan a cabo dentro de un ámbito organizacional. Esto, es debido al potencial aumento del uso de las TIC's y las herramientas informáticas creadas a partir del último siglo[18]; en la institución de educación Superior, ITFIP, cuenta con una gran variedad de archivos almacenada de manera física y lógica; entre las que se encuentra información académica, administrativa, financiera, datos concernientes a las últimas adquisiciones y entre otros. Dicha información es totalmente desgastante y extensa como para poder hacer un cálculo aproximado de los datos lógicos almacenados, por lo cual, esta se es almacenada en herramientas en la web, como servicios de Drive en la nube.

Dentro la estructura organizacional de la institución, los directores de cada área son responsables de la información, cada jefe de departamento se hace responsable del custodio de la información que le corresponde, pero no existe un protocolo claro de la manipulación o consulta de esta información, generando riesgos en las

[16] Dinero-ciberseguridad, articulo- 9/5/2019 -"En solo tres meses Colombia sufrió 42 billones de intentos de ataques cibernéticos", disponible en: https://www.dinero.com/actualidad/articulo/cuantos-ataques-ciberneticos-recibe-colombia/276556.

[17] OEA-ASOBANCARIA, "Desafíos del riesgo cibernético en el sector financiero para Colombia y américa latina", disponible en: https://www.oas.org/es/sms/cicte/docs/Desafios-del-riesgo-cibernetico-en-el-sector-financiero-para-Colombia-y-America-Latina.pdf

[18] Juan Voutssas M, Preservación documental digital y seguridad informática, Centro Universitario de Investigaciones Bibliotecológicas de la UNAM, disponible en: http://www.scielo.org.mx/scielo.php?script=sci_arttext&pid=S0187-358X2010000100008

dimensiones de seguridad (Disponibilidad, Integridad, Confidencialidad, Autenticidad y Trazabilidad).

Si se mira más al detalle cada departamento, cada funcionario es responsable de su información, generando una dependencia del funcionario cuando se requiera de dicha información y un riesgo de disponibilidad para el negocio.

El departamento de sistemas no es ajeno a este problema, si bien es cierto que cada funcionario sabe que tiene que hacer, no hay un protocolo claro ni un tratamiento adecuado de seguridad de la información para mitigar la materialización de cualquier riesgo que se presente, porque no lo saben. Este problema se repite en todos los departamentos en toda la institución.

4.2. FORMULACIÓN DEL PROBLEMA.

¿Cuáles son los controles, basados en la ISO27001:2013, que reducirán vulnerabilidades, riesgos y amenazas de la información administrada por la dependencia de sistemas de la Institución de Educación Superior – ITFIP?

5. OBJETIVOS

5.1. OBJETIVO GENERAL

Diseñar el sistema de gestión de seguridad de la información para la institución de educación superior – ITFIP, para el departamento de sistemas, bajo la norma ISO/IEC 27001:2013

5.2. OBJETIVOS ESPECÍFICOS

- Realizar un diagnóstico en el departamento de sistemas de la institución de educación superior – ITFIP sobre procesos o políticas de seguridad de la información, basado en la norma ISO/IEC 27001:2013.

- Efectuar un análisis de riesgo utilizando la metodología MAGERIT, en el departamento de sistemas de la institución de educación superior – ITFIP.

- Construir una declaración de aplicabilidad, para el departamento de sistemas de la institución de educación superior – ITFIP.

- Construir políticas y lineamientos de seguridad de información, de acuerdo con el análisis realizado, basados en la norma ISO 27001:2013, para el departamento de sistemas de la institución de educación superior – ITFIP.

6. JUSTIFICACIÓN

En la Institución de Educación Superior ITFIP; sede principal ubicada en El Espinal – Tolima, específicamente en la dependencia de sistemas, oficina en la cual reposa la información del personal estudiantil, administrativos, funcionarios entre otros; se evidencia la ausencia de un sistema de análisis de gestión de la seguridad de la información, método, que permite salvaguardar, proteger y prever cualquier daño al mismo. Esta se puede almacenar de manera física o digital, dichos datos corresponden a uno de los elementos más importantes para la organización, puesto que en ellos reposan datos cruciales para su subsistencia.

La Institución de Educación Superior – ITFIP no será la excepción, puesto que en ella maneja datos cruciales como la cantidad de personal contratado, en el caso de docentes que equivalencia unitaria informática se puede definir. Recordando que la institución maneja profesores catedráticos y de planta; además de ello, personal administrativo, operario, soporte entre todos.

Aquella información solamente llega a alojar una parte de ella, puesto que la cantidad de estudiante egresado también es almacenada. En promedio 2.350 estudiantes se encuentran matriculados en las diferentes plataformas (RYCA y RYCA V.2.0.0). Como plus adicional, los egresados de la institución redondean un total de 13500, de los diferentes programas académicos ofrecidos por la institución. La información de los jóvenes que actualmente se encuentran cursando en los diferentes periodos lectivos es considerada para la evaluación del rendimiento y crecimiento de cada uno de los ciclos propedéuticos.

La tecnología se encuentra avanzando de manera exponencial, esto se puede evidenciar a gran medida gracias a las nuevas tendencias de secuestro de redes informáticas, las cuales permiten extraer información crucial para una empresa.[19] Además de esto siempre se añade que siempre ha existido una gran falla en toda la operación de un sistema de información, es el ser humano como operario de dichos sistemas de información[20]. Adicionado esto se encuentran nuevas tendencias en el área de la seguridad informática para la fácil protección de los metadatos y paquetes de información que circulan por la red interna de la institución.

[19] Chilán González, I., Bolaños Burgos, F., Angulo Murillo, N., & García Murillo, G. R. (2019). ANÁLISIS DE ATAQUES RANSOMWARE EN SERVIDORES WEB, LINUX Y WINDOWS. UNESUM-Ciencias. Revista Científica Multidisciplinaria. ISSN 2602-8166, 2(3), 89-100. Recuperado a partir de http://186.101.39.22/index.php/unesumciencias/article/view/106

[20] Francisco Nicolás Solarte Solarte, Edgar Rodrigo Enriquez Rosero, Mirian del Carmen Benavides, Metodología de análisis y evaluación de riesgos aplicados a la seguridad informática y de información bajo la norma ISO/IEC 27001, disponible en: http://www.rte.espol.edu.ec/index.php/tecnologica/article/view/456

Con el desarrollo de este sistema de gestión de la seguridad de la información, la Institución, se ve beneficiada con un nuevo estatus entre otras entidades de educación superior, puesto que estas, no cuentan un sistema de seguridad de la información (SGSI), con esto, la institución en pro de sus actuales (normas de Calidad ISO 9001:2008, IQNET y NTCGP 1000: 2009) certificaciones y futuras, le dejan un camino bien estructurado para dar un paso a nuevas certificaciones. Como es tendencia en cada una de las compañías más reconocidas mundialmente, se diseñó y planteo este sistema de seguridad informática, el cual, con la ayuda de los ingenieros de esta área, se analizó cada uno de los componentes de esta para mejorar los niveles de seguridad, asumiendo cada una de las posibilidades que se podría presentar ante una eventual emergencia dependiendo la clasificación de los activos presentes en la institución.

La metodología MAGERIT, en su libro 1 argumenta lo siguiente: "implementa el proceso de gestión de riesgo dentro de un marco de trabajo para que los órganos del gobierno tomen decisiones, teniendo en cuenta los riesgos derivados del uso de tecnologías de información."[21], según lo anterior, cada organización con la implementación de la metodología es capaz de identificar, los posibles causantes de daños y conflictos a su información/activos, a su vez, son capaces de generar las correcciones preventivas y correctivas.

MAGERIT, presenta en la versión tres (3) un numero de libros (MAGERIT V3 – Libro1, MAGERIT V3 – Libro 2 y MAGERIT V3 – Libro 3), unos instructivos de cómo implementar y analizar cada tipo de activo, permitiendo a su vez determinar la óptima solución, tal como se mencionó en el párrafo anterior.

Por otra parte, la norma ISO 27001 en su versión del año 2013, como se aprecia en la siguiente cita:" ISO 27001 es una norma internacional que permite el aseguramiento, la confidencialidad e integridad de los datos y de la información, así como de los sistemas que la procesan." [22].

Se puede aclarar que lo mencionado anteriormente tanto que la metodología MAGERIT se encarga del análisis del riesgo y la norma ISO/IEC 27001:2013 se encarga del soporte de la confidencialidad, integridad y disponibilidad de la información en la organización, complementando de manera idónea para asegurar la información y sus activos que la sostienen.

[21]Ministerio de Administraciones Públicas de España. MAGERIT – Versión 3.0. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Madrid: Ministerio de Hacienda y Administraciones públicas, 2012. Pag 7 de 127. Administración electrónica.

[22] ASTIVIA Tecnologías Avanzadas S.L.L... Sistemas de Gestión de Riesgos y Seguridad. ISO 27001 – Software ISO 27001 de Sistemas de Gestión. [en línea], 2018 [revisado 13 septiembre 2018]. Disponible en Internet: https://www.isotools.org/normas/riesgos-y-seguridad/iso-27001/

7. ALCANCES Y LIMITACIONES

7.1. ALCANCES

El presente proyecto pretende diseñar un sistema de gestión de seguridad de la información en la Institución de Educación Superior – ITFIP, para el departamento de sistemas, bajo la norma ISO/IEC 27001:2013. El propósito de un sistema de gestión de la seguridad de la información es conocer las amenazas, riesgos y salvaguardas para que sean conocidos, asumidos, gestionados y minimizados por la institución de una forma documentada, sistemática, estructurada, repetible, eficiente y adaptada a los cambios que se presentan.

7.2. LIMITACIONES

Es conveniente resaltar que para el desarrollo del presente proyecto no abarcara temas como los que se definen a continuación:

- No se implementará el Sistema de Gestión de Seguridad de la Información propuesto.
- No se realizará la implementación y proceso de gestión de riesgos en la entidad.
- No se analizarán todos los activos de información de la institución.
- No se desarrollarán acciones correctivas, solo se proponen recomendaciones.

8. DISEÑO METODOLÓGICO

8.1. UNIDAD DE ANÁLISIS

Para el desarrollo de este proyecto de investigación, se presenta como enfoque de análisis la dependencia de sistemas del Instituto Tolimense de Educación Superior ITFIP; esto sucede debido a que el instituto como ente público consolidado ante la Republica de Colombia acumula una infinidad de recursos y procesos que son realizados rutinariamente de los cuales solo una pequeña fracción se encuentra documentada, al no encontrarse en su totalidad la documentación que permita encaminar una mejor idea de lo que aquí se genera puede provocar que el objetivo de estudio buscado no sea factible y verídico en cuestión de resultados obtenidos; también se puede observar que a la hora de generar un análisis concreto de investigación en la seguridad y planes de contingencia para los activos de información esta actividad se convierte en una demasiado grande y tediosa para su realización.

Una vez se ha logrado enfocar la unidad de análisis que permitirá llevar a cabo de una manera más centralizada la proyección de la investigación a realizar, se procede a identificar cuáles serán las variables a tener en cuenta y sus respectivas dimensiones; para ello mediante una serie de estudios se obtiene que la variable de referencia seria los activos de información que componen la dependencia de Sistemas de la Institución y la dimensión a la que se encaminara esta variable dentro de este diseño es el análisis de la seguridad que tiene la dependencia de sistemas a la hora de afrontar riesgos que puedan afectar sus activos de información.

Cuando ya se tiene encaminada la variable de análisis y la dimensión de estudio para proyectar de una mejor forma la investigación para el diseño de un Sistema de Gestión para la Seguridad de la Información, se procede a reconocer cual es la medida que estructura el problema que afecta a esta dependencia y hace necesario la realización de este proyecto, esta medida hace referencia a los activos que se encuentran propensos a sufrir daños de alguna índole por los pocos planes de contingencia que se manejan por la dependencia ante la presencia de algunos riesgos que puedan ocasionaren.

8.2. POBLACIÓN Y MUESTRA.

Para la realización del proyecto “Diseño del sistema de gestión de seguridad de la información centrado en la dependencia de sistemas del ITFIP”, se selecciona una población y muestra, las cuales van a ser explicadas a continuación:

8.2.1. Población. La población que se seleccionó para la realización del proyecto fue la empresa y universidad “Institución de Educación Superior – ITFIP”, la cual maneja aproximadamente 28 dependencias cada una de estas administra una gran cantidad de información la cual puede ser afectada, alterada, borrada, etc. Por lo que se hace factible realizar el proyecto en la institución.

8.2.2. Muestra. Debido a la gran cantidad de información que se maneja en el ITFIP, se decide filtrar el proyecto y ejecutarlo en la dependencia en donde tiene almacenada toda la información de la institución; la coordinación de sistemas. Allí se administra, almacena, vigila que todos los datos estén a salvo.

8.3. ESTUDIO METODOLÓGICO

En este capítulo, se hablará acerca de los planteamientos de exploración usados para el proceso de discernimiento del problema y la sugerencia de una posible solución, hasta de la metodología trabajada para el desarrollo de un sistema de gestión de la seguridad de la información basado en la norma ISO 27001 del 2013.

8.3.1. Diseño metodológico del desarrollo Experimental

El tipo de investigación de este proyecto es Desarrollo Experimental, ya que “consiste en trabajos sistemáticos fundamentados en los conocimientos existentes obtenidos por la investigación o la experiencia práctica, que se dirigen a la fabricación de nuevos materiales, productos o dispositivos, a establecer nuevos procedimientos, sistemas o servicios o a mejorar considerablemente los que ya existen”[23]
Se escoge este tipo de investigación debido que se propone mejorar el proceso que está manejando la institución ITFIP en su gestión de la seguridad de la información, construyendo el diseño de un sistema de gestión para la seguridad de la información que pueda ser utilizado como escudo de protección ante posibles amenazas que surjan en un futuro cercano y en donde estas puedan atentar contra la integridad de la información que se maneja en el lugar.

Por medio del avance de una investigación de campo, se busca interpretar la problemática que actualmente se exhibe en los sistemas de información transaccionales y a su vez tratar de presentar una solución apoyada tanto en la tecnología como en la norma ISO 27001 del 2013, diseñando un sistema de gestión de la seguridad de la información.

Como consecuencia a la solución que se pretende plantear, se comenzó una

[23] Colciencias, tipología de proyectos de carácter científico, tecnológico o de innovación, disponible en: https://minciencias.gov.co/sites/default/files/upload/paginas/documento_de_tipologias_-_version_5_vf.pdf

Investigación exploratoria[24], la cual permite inspeccionar a cerca de un tema en particular y así beneficiarse de una mejor interpretación del problema en aplicación.

Así que, de acuerdo con lo anterior, el segundo paso a seguir es realizar una investigación bibliográfica[25], técnica que se efectuó por medio de búsquedas del argumento en investigación, a través de repositorios libres, Google Escolar, Mendeley, manuales de procedimientos, reglamentos y normas basados en la norma ISO 27001. En donde los resultados obtenidos se inspeccionaron, criticaron e interpretaron. Todo este suceso, se forma por medio de las fuentes segundarias y acarrean a poder obtener nuevos conocimientos sobre el tema investigado.

Luego, los investigadores emprenden la experiencia de campo, a través de la cual logran encaminarse en la realidad del problema, lo cual permite evidenciar la rutina diaria de cómo se administra tanto la información como los sistemas en la institución. Con este ejercicio vivencial, se consigue interpretar las evidencias y los procesos desde la misma fuente del problema.

Una vez diagnosticado el problema, el marco teórico y estado del arte, los objetivos alcances y limitaciones, el siguiente avance consiste en formular el diseño de un Sistema de Gestión de la Seguridad de la Información por medio del uso de la metodología MAGERIT que está basada en la norma ISO 27001 del año 2013 y en donde se plantea una investigación a los activos que comprenden a la dependencia de sistemas en la institución.

Como procedimiento para la recolección de datos, se utilizó: las entrevistas y los cuestionarios con los afectados del problema, análisis en un ambiente de trabajo cotidiano, inspecciones del estado del arte, antecedentes del enigma, lecturas de resoluciones, manuales de procesos y revisión bibliográfica. Con esto se logró disponer de las características habituales para el manejo de la información en la dependencia de sistemas de la institución, así como su seguridad en conexiones y comunicaciones.

En la investigación exploratoria, se diagnosticaron dos fuentes de información: la primaria y la segundaria. Donde las fuentes primarias, concuerdan con una serie de preguntas de modelo abierto y cerrado estructuradas en cuestionarios, la cuales fueron adaptadas a una asociación de personas que están comprometidas directa e indirectamente con la dependencia de sistemas de la institución.
En esta investigación, para delimitar la muestra, se procedió de forma no probabilística, que, en el dominio de la estadística, se define como “Muestra por

[24] Gross, M. (2010). Conozca 3 tipos de investigación: Descriptiva, Exploratoria y Explicativa. Pensamiento Imaginativo. Blog. Recuperado el 02 de febrero del 2017. Disponible en: http://manuelgross. bligoo. com/conozca-3-tipos-de-investigaciondescriptivaexploratoria-y-explicativa.
[25] Arias, F. G. (2012). El Proyecto de Investigación. Introducción a la metodología científica. 5ta: Fidias G. Arias Odón. Pág. 60

conveniencia intencional”[26], esto se elaboró teniendo en cuenta a las personas que poseen mayor conocimiento de los problemas que se presentan en la dependencia de sistemas y como trabaja esta con la información que adquiere a través de sus conexiones. La fuente segundaria pertenece a información bibliográfica y verificaciones del estado del arte.

8.3.2. Diseño metodológico del sistema de gestión para la seguridad de la información.

Debido a la aparición del internet y a un sin número de herramientas tecnológicas, la mayor parte de la información que es manejada por las empresas de forma física y digital se encuentra propensa a ser violentada, para usos con fines desconocidos que podrían conllevar a un problema para la organización. Además, cuando esta información es manejada de forma física puede ser demasiado susceptible a una pérdida o modificación de esta; Por este motivo se sugiere tener en cuenta el diseño de un sistema de gestión de seguridad de la información para lograr abatir estas problemáticas que se presentan de forma cotidiana dentro de la misma.

Este proyecto se fundamenta en el diseño de un sistema de gestión de seguridad de la información para la dependencia de sistemas de la Institución de Educación Superior ITFIP.

Fase 1 Recolección de información de la institución y estado actual del ITFIP con respecto al Sistema de Información.

Para comenzar es necesario comprender como funciona la institución, sus estructuras jerárquicas y responsables.
Como se ha propuesto para el desarrollo del sistema de gestión de seguridad de la información (SGSI) basado en la ISO/IEC 27001:2013, es necesario realizar un análisis de la institución que permite evaluar el entorno de la institución, dirección, planificación, soporte, ejecución, seguridad, evaluación del ejercicio y mejoras, Estos elementos son los pilares esenciales para proceder según la norma.

La evaluación, que le permite aclarar el estado de la norma ISO/IEC 27001:2013 por parte del departamento de sistemas de la Institución de Educación Superior - ITFIP.

Fase 2 Análisis de Riesgos

Para el desarrollo del trabajo, se ha optado por trabajar con la metodología

[26] Hernández Sampieri, R., Fernández Collado, C. y Pilar Baptista L. (2010). Metodología de la investigación. México. Ed. Mc Graw Hill.

MAGERIT[27], que es un procedimiento que permite adaptar la implementación de un SGSI en donde se busca alcanzar un alto nivel de éxito y disminuir la incertidumbre de los resultados enfocándose en una perspectiva semántica de unos pasos a seguir en los cuales se pretende implementar un proceso de gestión de riesgos; con esta metodología se busca investigar de manera formal los riesgos que pueden sustentar los sistemas de información para así tratar de recomendar las medidas pertinentes que deberían adoptarse en busca del control de estos riesgos.

Con MAGERIT se proyectan alcanzar los siguientes objetivos.

Directos:

- Concienciar a los responsables de la información dentro de la organización de que existen ciertos riesgos que pueden amenazar su integridad y de la necesidad de gestionarlos para así tener un control oportuno.
- Otorgar un procedimiento semántico que permita examinar los riesgos procedentes del uso de tecnologías de la información y comunicación (TIC).
- Descubrir y planificar el procedimiento adecuado para mantener los riesgos bajo control.

Indirectos:

- Disponer a la institución para procedimientos de evaluación, auditoria, certificación o acreditación

Las labores que se ejecutan bajo la metodología MAGERIT son las siguientes:

1) Identificación de los activos

Se identifican los activos que usufructúa la dependencia de sistemas de la institución categorizados según su función, los cuales derivan en:

- Esenciales
- Arquitectura del Sistema
- Datos
- Claves criptográficas
- Servicios
- Aplicaciones informáticas (Software
- Equipamiento informático (Hardware)
- Redes de Comunicaciones
- Soportes de Información

[27] Dirección general de modernización administrativa, P.e (2012). MAGERIT- versión 3.0 Metodología de análisis y gestión de riesgos de los sistemas de información Madrid.

- Equipamiento Auxiliar
- Instalaciones
- Personal

2) Valoración de los activos

En este apartado no se hace referencia al costo monetario de cada activo sino al valor que este pueda tener según la importancia para la dependencia; pues si el activo es valioso, el nivel de protección que demandaría seria mayor según su dimensión de seguridad, este valor al que se hace referencia puede ser propio o acumulativo.

La manera en la que se pueden valorar los activos puede ser de dos tipos:

- Valoración cualitativa
- Valoración cuantitativa
- Disponibilidad
- Integridad de los Datos
- Confiabilidad de la Información
- Autenticidad
- Trazabilidad

3) Identificación de las Amenazas

Son todos aquellos eventos que pueden repercutir en la reducción del valor de un activo dentro de la empresa; algunas de las amenazas más comunes que podemos encontrar según MAGERIT son las siguientes:

- Desastres naturales
- De origen industrial
- Defectos de las aplicaciones
- Causadas por las personas de forma accidental

Después de que se logra identificar que amenaza puede afectar a un activo como tal, se procede a valorar la consecuencia que esta generaría; esta valoración comprende dos tipos:

Degradación: Que tan delicado podría quedar el activo después de haber afrontado la amenaza presentada; es aquí donde se estima el daño causado por un incidente en caso de que este ocurriera.

Tabla 2.Tabla de Frecuencia de Riesgos

MB		**Muy Baja**	**Muy Raro**	**Extremadamente Difícil**
B		Baja	Poco Probable	Muy Difícil
M		Media	Posible	Difícil
A		Alta	Muy Alto	Medio
MA		Muy Alta	Casi Seguro	Fácil

Fuente (Dirección general de modernización administrativa, P.a. (2012). MAGERIT- versión 3.0 Metodología de análisis y gestión de riesgos de los sistemas de información Madrid).

Probabilidad: En este tipo de valoración se califica que tan probable o improbable es que se materialice la amenaza; esta probabilidad de ocurrencia generalmente es presentada de forma cualitativa por medio de una escala nominal.

Tabla 3. Tabla de Probabilidad de Riesgos

MB	**1/100**	**Muy poco frecuente**	**Siglos**
B	1/10	Poco frecuente	Cada varios años
M	1	Normal	Una vez al año
A	10	Frecuente	Mensualmente
MA	100	Muy frecuente	A Diario

Fuente (Dirección general de modernización administrativa, P.e (2012). MAGERIT- versión 3.0 Metodología de análisis y gestión de riesgos de los sistemas de información Madrid).

4) Diagnóstico del impacto

Se designa como impacto al perjuicio que se ha generado por una amenaza sobre un activo; dentro de los impactos es posible encontrar dos tipos:

- **Impacto acumulado:** Es el que se deduce de manera correspondiente para cada uno de los activos, por cada amenaza y dimensión de valoración, se debe tener en cuenta su valor acumulado y las amenazas a las que ha sido expuesto.

- **Impacto repercutido:** Es aquel que se logra encontrar para cada uno de los activos, por cada amenaza y dimensión de valoración, se debe tener en cuenta su valor propio y las amenazas a las que han expuesto los activos de los cuales depende el mismo.

5) Determinación del riesgo potencial

Después de determinar el impacto que puede ser generado por las amenazas a las que se han evaluado cada uno de los activos, es posible diagnosticar la probabilidad de ocurrencia que estas tendrían dentro de la empresa.

Imagen 1.Grafica de la Determinación del Riesgo Potencial

Fuente: (Dirección general de modernización administrativa, P.e (2012). MAGERIT- versión 3.0 Metodología de análisis y gestión de riesgos de los sistemas de información Madrid).

Cada una de las zonas significa lo siguiente:

- Zona 1: Riesgos muy probables y de muy alto impacto.
- Zona 2: Rango de situaciones improbables y de impacto medio, hasta situaciones muy probables, pero de impacto bajo o muy bajo.
- Zona 3: Riesgos improbables y de bajo impacto.
- Zona 4: Riesgos improbables, pero de muy alto impacto.

Riesgo acumulado

Este tipo de riesgo se determina por cada activo, amenaza y dimensión de valoración; para este proceso es muy importante tener en cuenta el impacto acumulado que ha sido originado sobre un activo por una amenaza y la probabilidad que existe de que esta ocurriera nuevamente. Una vez se obtiene este riesgo acumulado es posible instaurar las salvaguardias necesarias de protección.

Riesgo repercutido

Se determina por cada activo, amenaza y dimensión de valoración; para este

proceso es muy importante tener en cuenta el impacto repercutido sobre un activo ocasionado por una amenaza y la probabilidad que existe de que esta ocurriera nuevamente.

6) Salvaguardas

En un mundo tan contemporáneo como en el que vivimos hoy en día es posible descubrir muchos mecanismos tecnológicos que son utilizados como herramientas para reducir el riesgo de aquellos sistemas que se encuentran desprotegidos. Estas son consideradas como salvaguardas, de las cuales hay un gran mundo de sus posibilidades que se pueden tener en cuenta; a la hora de realizar una selección se debe tener en cuenta lo siguiente:

1. Tipo de activo a proteger.
2. Dimensiones de seguridad que requieren protección.
3. Amenazas de las que se debe proteger.
4. Existencia de salvaguardias alternativas.

También para poseer una mejor visión a la hora de seleccionar una salvaguarda de forma adecuada se debe considerar que al momento de esta selección es obligatorio excluir algunas según las afirmaciones no aplican o no justifica.

Tipos de Salvaguardas

Hoy en día es posible identificar distintos modelos de defensa que son presentados por las salvaguardias, para buscar así una reducción de la degradación y la probabilidad. Estos modelos de defensa se encuentran divididos según el efecto que producen en:

- Preventivas: Estas buscan disminuir la probabilidad de ocurrencia que puede presentarse; en esta división es posible apreciar salvaguardas preventivas, disuasorias y eliminatorias.

- Reducción: Estas buscan disminuir la degeneración que puede producirse; en esta división es posible estimar salvaguardas minimizadoras, correctivas y recuperativas.

- Agrupación: Permiten reunir las causas producidas por las dos anteriores; en esta división es posible estimar salvaguardas de monitorización, de detección, de concienciación y administrativas.

Eficiencia de la salvaguarda

Una de las principales particularidades que adquieren las salvaguardas es la

Eficiencia que estas poseen frente al riesgo que pretenden impedir; la eficiencia ideal sería la del 100%.

Tabla 4. Tabla de la Eficiencia de la Salvaguarda

Factor	Nivel	Significado
0%	L0	Inexistente
	L1	Inicial / ad hoc
	L2	Reproducible, Pero Intuitivo
	L3	Proceso Definido
	L4	Gestionado y Medible
100%	L5	Optimizado

Fuente: (Dirección general de modernización administrativa, P.e (2012). MAGERIT- versión 3.0 Metodología de análisis y gestión de riesgos de los sistemas de información Madrid).

7) Impacto Residual

Una vez se ha implementado cada una de las salvaguardias, el sistema tiende a mantenerse en un estado pasivo de posible impacto; el impacto residual puede deducirse de forma agrupada sobre cada uno de los activos minoritarios o repercutidos sobre los superiores.

8) Riesgo residual

Una vez se ha implementado cada una de las salvaguardas, el sistema tiende a mantenerse en un estado pasivo de posible riesgo; el riesgo residual puede deducirse de forma agrupada sobre cada uno de los activos minoritarios o repercutidos sobre los superiores.

Fase 3 Declaración de aplicabilidad

En esta fase se realizara una declaración de aplicabilidad; un documento que es necesario que requiere la norma ISO/IEC 27001; esta herramienta es generada para que la institución mantengan el registro; de esa forma ejerzan un control de las medidas aplicadas

Esta acta incorpora los controles de seguridad creados en el anexo a de la ISO/IEC 27001, además de esto se establecerán medidas que se ajusten a la necesidad de la institución de acuerdo con el análisis de riesgos previamente documentado.

La Declaración de Aplicabilidad deberá incluir requerimientos legales, obligaciones contractuales, requerimientos del negocio o adopción de buenas prácticas,

Diseñar el SGSI: A la hora de Diseñar el Sistema de Gestión para la Seguridad de la información es necesario tener en cuenta tres de sus componentes que son:

- La documentación del sistema.
- La implementación del plan de tratamiento de riesgos autorizado por la Dirección de la organización en donde se deben comprender los recursos establecidos y el mantenimiento de los controles existentes.
- El monitoreo constante de la seguridad de la información.

9. MARCO DE REFERENCIA

9.1. MARCO TEÓRICO

Los sistemas de gestión de seguridad de la información determinan parámetros a seguir para la protección de los sistemas de información, esto permite que se prevean y se descubran las posibles deficiencias que presentan. La investigación al sistema de información limitado la dependencia de sistemas de la Institución de Educación Superior – ITFIP, tiene como pilares fundamentales la disponibilidad, confiabilidad, trazabilidad y confidencialidad[28] fundamentos esenciales asentados en la metodología MAGERIT.

Las políticas y los procedimientos de seguridad informática nacieron como una herramienta para organizar y dar conciencia a cada uno de los actores de una organización, para se tome la importancia y la sensibilidad de la información que favorecen al progreso y el funcionamiento de la organización. Deben considerarse como un manual de que se debe cumplir para evitar problemas, donde se debe establecer para dar soporte a los sistemas de seguridad implementados en las tecnologías de información y comunicación.

Técnicas de recolección de información: Para la recolección de información en la organización se empleará el método de la metodología cualitativa, etnometodología[29], sabiendo que esta parte de que todo aquello relacionado con lo social tiende a ser rentable, analizable y descriptible, por ende, el grupo de trabajo decidió utilizarla como una de las principales herramientas de recolección de información.

La información cuantificable y aquella cualitativa a la cual no se pueda acceder con las interacciones y posesividad, se implementarán otros métodos de recolección de información según la metodología cualitativa[30], como encuestas y entrevistas al personal pertinente dejando como evidencias grabaciones de las entrevistas hechas. También para el desarrollo de este proyecto se utilizará todas las fuentes bibliográficas que sean necesarias, internet, todos los elementos documentales que sean necesarios para tener una imagen más clara, dar un buen desarrollo a este proyecto.

---

[28] Mirabal Sarria y Maragoto Maragoto.” Propuesta de una guía de seguridad informática integrada a la gestión de la calidad", Observatorio de la Economía Latinoamericana, Nº 164, 2012. Texto disponible en: http://www.eumed.net/cursecon/ecolat/cu/2012/. Citado: 17 de sept. de 18

[29] Juan José Caballero Romero. Etnometodología, Universidad Complutense. Texto disponible en: http://www.reis.cis.es/REIS/PDF/REIS_056_06.pdf. Citado:17 de sept. de 18

[30] Juan Báez y Pérez de Tudela. Investigación cualitativa 2 edición, Libros profesionales de empresa 2009. Disponible en: https://books.google.com.co/books?id=Xmv-PJ9KtzsC&printsec=frontcover&dq=cualitativa&hl=es&sa=X&ved=0ahUKEwi23dCN_8PdAhVR3VMKHdYyDoIQ6AEIJzAA#v=onepage&q=cualitativa&f=false. Citado: 18 de sept. de 18

Normas ISO: La International Organization for Standardization - ISO e International Electrotechnical Commission – IEC, son las que desarrollaron la familia de Normas ISO/IEC 27000, donde se proporcionan las políticas para la gestión de la seguridad en la información en cualquier organización.[31]

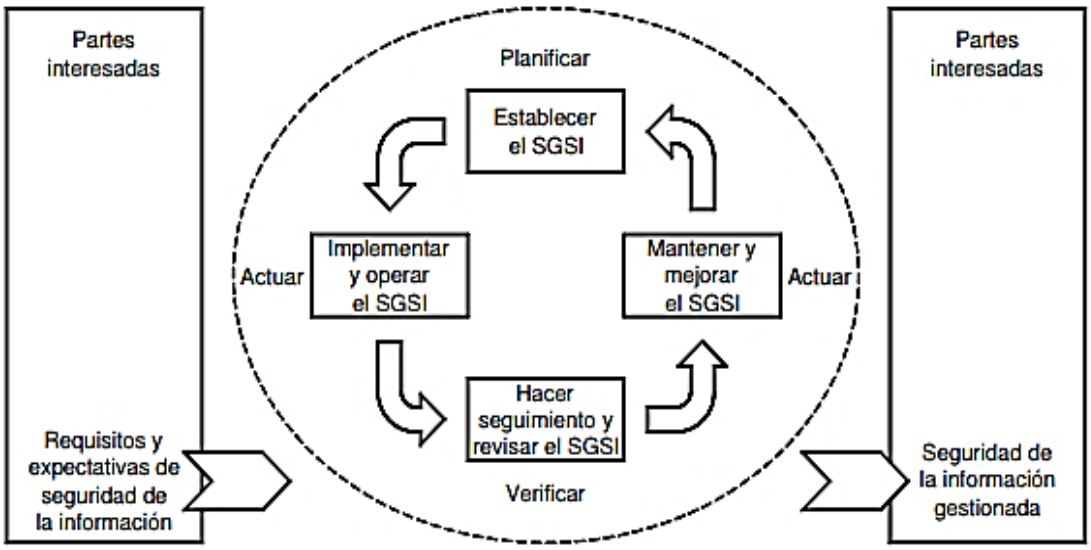
Por otra parte, la norma **ISO 27001**, es fundamental, ya que contiene los requisitos del sistema de gestión de seguridad de la información para cualquier organización y esta es certificada por auditores externos. Esta norma indica cuales son los requerimientos para la implementación de controles de seguridad. El SGSI está diseñado para escoger y brindar las políticas de seguridad que permitan proteger los activos de información.[32]
Esta ISO aplica para todas las disposiciones de un SGSI, un modelo de procesos "Planificar-Hacer-Verificar-Actuar" (PHVA) para estructurar de manera adecuada cada proceso.

"Planificar-Hacer-Verificar-Actuar" (PHVA): "A la hora de implementar un Sistema de Gestión de Seguridad de la Información basado en el estándar internacional ISO 27001, debemos utilizar el ciclo PDCA (siglas en inglés) o PHVA (siglas en español)."[33]

- Planificar: se establece el Sistema de Gestión de Seguridad de la Información.
- Hacer: se implementa el SGSI.
- Verificar: revisión del Sistema de Gestión de Seguridad de la Información.
- Actuar: en este paso del ciclo lo que se hace es mantener y mejorar el SGSI.

[31] Janett Yánez, Raiza Yánez, Auditorías, Mejora Continua y Normas ISO: factores clave para la evolución de las organizaciones, disponible en: https://www.redalyc.org/pdf/2150/215026158006.pdf
[32] ICONTEC, "NORMA TÉCNICA NTC-ISO/IEC COLOMBIANA 27001", UNAD, disponible en: http://intranet.bogotaturismo.gov.co/sites/intranet.bogotaturismo.gov.co/files/file/NTC-ISO-IEC%2027001.pdf
[33] Isotools. ISO 27001: La implementación de un Sistema de Gestión de Seguridad de la Información, Blogs SGSI, 2015. Texto disponible en: https://www.pmg-ssi.com/2015/01/iso-27001-la-implementacion-de-un-sistema-de-gestion-de-seguridad-de-la-informacion/. Citado: 17 de sept. de 18

Imagen 2. Modelo PHVA



Fuente: ICONTEC, "http://intranet.bogotaturismo.gov.co/sites/intranet.bogotaturismo.gov.co/files/file/Norma.%20NTC-ISO-IEC%2027001.pdf"

En la ilustración número 2, se puede evidenciar cada uno de los ítems esenciales en los cuales se realiza cada uno de los procesos necesarios, a continuación, se describirá cada una de ellas:

Planificar*:* Se define cuáles son los alcances del SGSI referente a la norma ISO 14001, la información necesaria se establece y se justifican las exclusiones. En este paso definimos la metodología de trabajo, además de adquirir el conocimiento necesario de la organización.

Hacer*:* Se crea un plan de tratamiento para los riesgos, esto referenciado y encaminados a los objetivos de manejo identificados.
Se implementan métricas que permitan conseguir resultados eficaces y reproducibles a la hora de evaluar los objetivos de manejo encontrados.

Identificar el personal de la organización y dotarle de conocimiento sobre los sistemas de gestión de la seguridad de la información, además se debe gestionar todas las pautas de la norma ISO 27001 y los recursos, esto con el fin de que el SGSI se mantenga.

Verificar*:* La organización debe realizar sus actividades normalmente. Se debe prestar estricta atención al procesamiento de la información y así inferir en los errores, fisuras, amenazas e inseguridades que atenten contra la disponibilidad, confiabilidad, trazabilidad y confidencialidad de la información.

Actuar*:* Cada laxo de tiempo se debe aplicar las mejoras identificadas al sistema de gestión de seguridad de la información de la organización. Instaurar acciones preventivas y correctivas basadas en la estructura de la norma 27001, además de analizar si las mejoras propuestas están a las medidas de la organización y si estando aplicadas al SGSI se sostendrían en la organización.

PDCA: Este significa Plan-Do-Check-Act. Esta es la guía para establecer un sistema de gestión de seguridad de la información teniendo como base a la norma ISO27001, PDCA es un ciclo continuo donde siempre está en evaluación.[34]

MAGERIT: Según Camilo Gutiérrez Amaya, MAGERIT es una metodología de análisis y gestión de los riesgos, la cual fue desarrollada por el Consejo Superior de Administración Electrónica de España, que nos brinda una metodología sistemática del control de riesgos y su correspondiente mitigación, como también nos ofrece las técnicas necesarias para realizar estas mitigaciones con ejemplos puntuales.[35]

COBIT: La metodología COBIT es un ejemplar para la auditoria de la gestión y el control del sistema de información, según la universidad EAFIT este método está enfocado a las organizaciones, administradores TI, usuarios y auditores, teniendo en cuenta su asociación con los procesos.[36]

COBIT tiene como significado “Objetivos de control para la tecnología de información”, este tiene como disposición el evaluar y hacer monitoreo de los sistemas de TI, enfatizando en su seguridad e intervenciones concisas que se centren en el modelo de negocio. Según EAFIT[37], la filosofía principal de esta metodología es el implementar su modelo a toda la organización, no se excluye nada, desde computadoras personales hasta el acceso a la red, se basa en que cada bien o servicio TI deben ser instrumentados mediante procesos agrupados y así obtener información de manera optimizada y confiable que es el medio principal para lograr los objetivos de una organización.

---

[34] Purificación aguilera. Seguridad Informática, Google book. Disponible en: https://books.google.com.co/books?id=Mgvm3AYIT64C&printsec=frontcover&hl=es&source=gbs_ge_summary_r&cad=0#v=onepage&q&f=false. Citado:17 de sept. de 18

[35] GUTIERREZ, Camilo. Welivesecurity. MAGERIT: metodología práctica para gestionar riesgos, [Revisado 12 de Septiembre del 2018]. Disponible en Internet: https://www.welivesecurity.com/la-es/2013/05/14/MAGERIT-metodologia-practica-para-gestionar-riesgos/

[36] Eduardo Martínez Estébanes, Juan Carlos García Cano, Gobierno de ti a través de Cobit 4.1 y cambios esperados en Cobit 5.0, disponible en: https://dialnet.unirioja.es/servlet/articulo?codigo=3823460

[37] AREIZA CORREA JUAN DANIEL, CARVAJAL RAIGOSA JULIAN MAURICIO, GOMEZ OCAMPO SEBASTIAN- universidad EAFIT-Definición de un cuadro de mando para la gestión de servicios de TI, que apoye la toma de decisiones en una empresa de servicios, aplicando los modelos de gobierno TI- disponible en internet: https://repository.eafit.edu.co/bitstream/handle/10784/2471/CarvajalRaigoza%2C%20Julian%20Mauricio_2009.pdf?sequence=1&isAllowed=y

Principios de COBIT: Los lineamientos de la metodología tienen como métodos de inferencia, los requerimientos de calidad: evaluación, calidad, costos y entrega, así mismo los requerimientos fiduciarios: eficacia y competencia operativa, fiabilidad en los reportes financieros y acatamiento de normas y regulaciones.[38]

9.2. MARCO CONCEPTUAL

El Diseñar: El diseño es una palabra proveniente del vocablo italiano (disegno)[39], la cual hace referencia de plantear una solución a un problema, estructurando el cómo, el pilar inicial como el final, que implicar que cada uno de los procesos a realizar, quien es el apropiado para desarrollar dichas fases, entre otras.
El diseño en la línea de investigación aplicada hace mención de la implementación de una metodología, en nuestro caso MAGERIT, teniendo en cuenta una serie de pautas obligatorias.

La Investigación: En todo contexto, la investigación es el pilar fundamental para el desarrollo o contemplación de alguna existencia, puesto que es en él, recae todos los argumentos importantes a los cuales se tendrá en cuenta. Según el DRAE (Diccionario de la Real Academia Española) define investigación como "Investigación que tiene por fin ampliar el conocimiento científico, sin perseguir, en principio, ninguna aplicación práctica."[40], como se menciona en la cita anterior, ampliar el conocimiento científico, antes de ejecutar cualquier acción que proceda el desarrollo, en este caso; la aplicación del sistema de información.

Sistema: Un sistema es el conjunto de indicaciones que trabajan para satisfacer un objetivo en común, un claro ejemplo de ello es la mensajería; en donde el emisor trasmite un mensaje por un medio especifico y llega a manos del receptor. Hablamos de individuos diferentes (emisor, mensaje y receptor), que trabajan para cumplir un objetivo, la comunicación[41].

Información: La información es todo aquello que suma prioridad ante una organización, estos, pueden tener variedad de importancia dependiendo de si mismos. Para una organización, sin importar su razón social es lo más importante para no perder el recorrido de quienes son y a que se dedican.[42]

---

[38] Eduardo Martínez Estébanes, Juan Carlos García Cano, Gobierno de ti a través de Cobit 4.1 y cambios esperados en Cobit 5.0, disponible en: https://dialnet.unirioja.es/servlet/articulo?codigo=3823460
[39] JULIÁN PÉREZ PORTO Y MARÍA MERINO. Publicado: 2014. Actualizado: 2016. Definicion.de: Definición de rediseño (https://definicion.de/rediseno/)
[40] RAE.REAL ACADEMIA ESPAÑOLA. Definición de Investigación, [Revisado 12 de Septiembre del 2018]. Disponible en Internet: http://dle.rae.es/?id=M3YxV5t
[41] JULIÁN PÉREZ PORTO Y ANA GARDEY. Publicado: 2008. Actualizado: 2008. Definicion.de: Definición de sistema de información (https://definicion.de/sistema-de-informacion/)
[42] Ibid.

Análisis: El análisis va encaminado con la investigación, puesto que permite detallar de manera más estructurada cada uno de los componentes de los sistemas que se estudian. Según el diccionario de la real academia española (RAE) define análisis como "Distinción y separación de las partes de algo para conocer su composición."[43], haciendo mención de lo dicho anteriormente.

Gestión: La gestión es el proceso en el cual, se establece una serie de parámetros necesarios y oportunos, que permite enfocar de manera más eficiente cada uno de los recursos en una organización o proyecto. Según la RAE, gestión es la acción de gestionar, lo cual nos define como "Ocuparse de la administración, organización y funcionamiento de una empresa, actividad económica u organismo."[44], dicho planteamiento tiene similitud con la introducción con el comienzo del párrafo.

Seguridad Informática: Según la Universidad Internacional de Valencia, la seguridad informática es el proceso de identificar, procesar y detectar intrusos que hagan uso de un sistema informático sin su autorización. Debido a las altas tasas de incremento del uso de los SI, este esquema de seguridad se ha vuelto indispensable para cualquier ámbito organizacional.[45]

Recolección: Según la RAE, recolección hace mención de la acción de recolectar, el cual se define como "Reunir cosas o personas de procedencia diversa."[46], lo que hace referencia al proceso de acercamiento de personas que poseen información trascendental sobre el correcto funcionamiento de lo que se va a tratar.

Desarrollo experimental: "consiste en trabajos sistemáticos fundamentados en los conocimientos existentes obtenidos por la investigación o la experiencia práctica, que se dirigen a la fabricación de nuevos materiales, productos o dispositivos, a establecer nuevos procedimientos, sistemas o servicios o a mejorar considerablemente los que ya existen"[47].

Disponibilidad: Según el libro MAGERIT en su versión 3, define la disponibilidad como "Propiedad o característica de los activos consistente en que las entidades o

[43] RAE.REAL ACADEMIA ESPAÑOLA. Definición de Análisis, [Revisado 12 de Septiembre del 2018]. Disponible en Internet: http://dle.rae.es/?id=2Vga9Gy
[44] RAE.REAL ACADEMIA ESPAÑOLA. Definición de gestión, [actualizado en 2019]. Disponible en Internet: https://dle.rae.es/gesti%C3%B3n
[45] VIU. UNIVERSIDAD INTERNACIONAL DE VALENCIA. ¿Qué es la seguridad informática y cómo puede ayudarme?, [Revisado 12 de Septiembre del 2018]. Disponible en Internet: https://www.universidadviu.com/la-seguridad-informatica-puede-ayudarme/
[46] RAE.REAL ACADEMIA ESPAÑOLA. Definición de Recolectar, [Revisado 12 de Septiembre del 2018]. Disponible en Internet: http://dle.rae.es/srv/search?m=30&w=recolectar
[47]Tipología de los proyectos – Colciencias - disponible en: https://www.colciencias.gov.co/sites/default/files/upload/paginas/documento_de_tipologias_-_version_5_vf.pdf

procesos autorizados tienen acceso a los mismos cuando lo requieren."[48], lo que da a entender el nivel de complejidad que pueda tener para acceder a dicha información, además, del personal conocedor de la misma.

Integridad de los datos: Para el libro de MAGERIT en su versión 3, la integridad de los datos se define como "Propiedad o característica consistente en que el activo de información no ha sido alterado de manera no autorizada"[49], esto nos da a entender que tan alta es la necesidad de saber ¿Cuándo?, ¿Cómo? y ¿Por qué?, la información que almacenaban ciertos documentos fue modificada, como también cual fue la persona que realizo este cambio para así saber si es o no una persona autorizada para realizar estos cambios.

Confidencialidad de la información: El libro de MAGERIT en su versión 3, considera que la confidencialidad de la información es la "Propiedad o Característica consistente en que la información ni se poner a disposición, ni se revela a individuos, entidades o procesos no autorizados"[50], esto nos da a entender que la información de suprema importancia para las organizaciones no puede ser reveladas u observadas a terceros, no sin que estos estén autorizados para poder acceder a la misma.

Autenticidad: Según el libro de MAGERIT en su versión 3, define a la Autenticidad como la "Propiedad o característica consistente en que una entidad es quien dice ser o bien garantiza la fuente de la que preceden los datos"[51], teniendo en cuenta esto, la autenticidad nos asegura que la persona o entidad la cual accede a la información es quien en verdad tiene acceso a esta para que así no existan fugaz de información en la organización.

Trazabilidad: En el libro de MAGERIT en su versión 3, define a la trazabilidad como el "Aseguramiento de que en todo momento de podrá determinar quién hizo qué y en qué momento"[52], lo cual significa que con la trazabilidad podemos tener un referente de quien creo, modifico y/o elimino la información que tiene la organización.

Riesgos: Según MAGERIT, los riegos son las estimaciones de que tan alta es la posibilidad de que una amenaza se materialice sobre uno o más activos y esto cause daños o perjuicios a la organización.[53]

---

[48] Ministerio de Administraciones Públicas de España. MAGERIT – Versión 3.0. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información libro I. Madrid: Ministerio de Hacienda y Administraciones públicas, 2012. Pag 9. Administración electrónica.
[49] Ibid.
[50] Ibid.
[51] Ibid.
[52] Ibid.
[53] Ibid.

Análisis de riesgos: Para MAGERIT, el análisis de riesgo es el proceso sistemático que nos enseña que tan expuesta esta la organización a estos riegos; sabiendo esto se decide cómo serán tratados estos riesgos, para que así la organización tenga un plan de contingencia para cuando algún riesgo aparezca ente ellos.[54]

Activos: Según el libro de MAGERIT en su versión 3, define los activos como el "Componente o funcionalidad de un sistema de información susceptible de ser atacado deliberada o accidentalmente con consecuencias para la organización. Incluye: Información, datos, servicios, aplicaciones (Software), equipos (Hardware), comunicaciones recursos administrativos, recursos físicos y recursos humanos"[55], esto nos da a entender que los activos es todo aquello que hace parte de la organización ya sea tangible o intangible.

Software: Según la RAE, el Software es el "Conjunto de programas, instrucciones y reglas informáticas para ejecutar ciertas tareas computacionales"[56], lo que nos da a entender que el Software es la parte lógica e intangible de los ordenadores, la cual permite que el ordenador entienda nuestras órdenes.

Hardware: Según la RAE, el Hardware es el "Conjunto de aparatos de una computadora"[57], el Hardware es la parte física y tangible de los ordenadores, la cual no deje realizar las órdenes que deseamos darles a nuestros ordenadores.

9.3. ANTECEDENTES

Actualmente se han desarrollado diferentes diseños e implementaciones de SGSI en Latinoamérica. Un diseño notable es el elaborado por Guerrero A. y Tabagano G.[58] en donde se documenta un SGSI, realizado para un módulo de la universidad de Nariño, el cual se encarga de los servicios de administración de Red de Datos e internet, administración de Bases de Datos y Servidores, Administración del Portal Web, servicios académicos y servicios de mantenimiento de equipos de cómputo, esto género la necesidad de realizar este (SGSI), al módulo ya que como se puede observar todos los datos electrónicos vitales para la Universidad en su ámbito académico está almacenado en dicho lugar. Para esto los autores aplicaron la Norma ISO/IEC 27001 y 27002. Gracias a esta combinación, lograron obtener un

[54] Ibid.
[55] Ministerio de Administraciones Públicas de España. MAGERIT – Versión 3.0. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Madrid: Ministerio de Hacienda y Administraciones públicas, 2012. Pag 12. Administración electrónica.
[56] RAE.REAL ACADEMIA ESPAÑOLA. Definición de Software, [Revisado 12 de Septiembre del 2018]. Disponible en Internet: http://dle.rae.es/?id=YErlG2H
[57] RAE.REAL ACADEMIA ESPAÑOLA. [Definición de Hardware, actualizado en el 2019]. Disponible en Internet: https://dle.rae.es/hardware?m=form
[58] Yezid Camilo Guerrero Angulo, Robert Marcelo Tabagano Goyes, SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN (SGSI) BASADO EN LA NORMA ISO 27001 Y 27002 PARA LA UNIDAD DE INFORMATICA Y TELECOMUNICACIONES DE LA UNIVERSIDAD DE NARIÑO disponible en: http://biblioteca.udenar.edu.co:8085/atenea/biblioteca/90493.pdf

alto nivel de calidad en el proceso de la seguridad de la información, el cual es totalmente independiente del tamaño y/o a la razón social de la organización, pero también aclararan que aunque estas medidas de seguridad se encuentren en funcionamiento, no pueden ofrecer garantía que sean absolutas ya que pueden existir amenazas que vulneren éstas, también afirman que MAGERIT presenta una guía completa y sistemática para el análisis de riesgos. Por ende, el uso de la misma permite acelerar el proceso de realización del mismo mediante las tablas que la metodología MAGERIT ofrece, y por ultimo luego de realizar este (SGSI) y de analizar la norma ISO/IEC 27001:2005 junto a los niveles de madurez la universidad en el módulo al cual se le realizo el (SGSI) podría optar a la certificación de esta norma.

De igual manera, Guamán S.[59]en el año 2015 propone el diseño de un Sistema de Gestión de Seguridad de la Información (SGSI) para las Instituciones Militares, el cual incorporase estándares internacionales que estuviesen ajustados al campo militar y las nuevas tecnologías de información y telecomunicaciones, este se realizado en la Armada del Ecuador a la Dirección de Tecnologías de la Información y Comunicaciones. Para realizar el (SGSI), el autor tomó como referencia la ISO 27001:2005 y combinó éstas con otras metodologías para realizar la evaluación de los riesgos para que con esta pudiese tomar una decisión sobre cuál sería el tratamiento adecuado para estos riesgos. Luego se determinó la factibilidad operativa para establecer el diseño de un Sistema de Gestión de Seguridad de la información para las instituciones Militares, lo que permitió verificar que cumplan con las características acordes de las instituciones Militares y determinar que el proyecto sea puesto en marcha aprovechando todos los beneficios para la institución logrando que los usuarios estén en compromiso de seguridad y el reconocimiento de las responsabilidades de seguridad de la información. Para el diseño de un Sistema de Gestión de Seguridad de la información para las mismas instituciones Militares se identificó el riesgo, las amenazas y vulnerabilidades; tratamiento de riesgos, la revisión de los riesgos y reevaluación de los activos de la información de la dirección de tecnologías de la información y Comunicaciones, lo que permitió aplicar para el Diseño del SGSI la cláusula 4.2.1 de la norma ISO 27001:2005 literales a) a la j).Luego de realizar el (SGSI), el autor concluye que, para el año 2015, las Instituciones Militares de Ecuador, no disponían de dicho sistema lo cual permitía que las amenazas se materializaran, como consecuencia de esto las fuerzas militares tenían una probabilidad muy alta perder este activo muy importante el cual es la información, esta afirmación tiene como fundamento la Norma ISO 27001:2005.

[59] Joseph Alexander Guamán Seis, DISEÑO DE UN SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN PARA INSTITUCIONES MILITARES, disponible en: https://bibdigital.epn.edu.ec/bitstream/15000/10439/3/CD-6187.pdf

Así mismo García H. y Ruiz M.[60], en el año 2017, propusieron un análisis y gestión de riesgos en el marco del SGSI, basado en la metodología MAGERIT y apoyado en una api web para su ejecución. Este proyecto se realizó en TrackSpia S.A.S, una pequeña empresa que se encuentra en el mercado del rastreo satelital, la cual permitió el desarrollo del análisis y gestión de los riesgos mediante el uso de la metodología MAGERIT junto a la norma ISO 27001:2015.La metodología MAGERIT, facilito el trabajo a la hora de que los autores realizaran el análisis de riesgos gracias a la guía que esta ofrece siendo por poco un paso a paso para realizar este. Al final los autores recomiendan que la empresa debe realizar una revisión periódica de las amenazas y de los riesgos que los activos de esta tienen, como también capacitar al personal para que se cumplan las normas de seguridad que fueron aconsejadas/empleadas para la gestión de los riesgos. Para que las organizaciones identifiquen los factores de riesgo internos y externos empezaron por un marco de trabajo basado en la metodología MAGERIT después se establecieron como y quienes facilitaban la información, que información era relevante, simplificando el paso entre la caracterización de los activos de la organización a la identificación de las amenazas a las que se encontraban expuestos los activos, y cómo dichas amenazas podrían impactar los activos. El marco de trabajo les permitió visualizar de forma inmediata las salvaguardas, que de una u otra forma ayudaran anular el riesgo o a mitigar el impacto del mismo. El enfoque cualitativo del marco de trabajo, además de simplificar la comunicación entre consultor y entrevistado, deshabilito la limitante impuesta por el desconocimiento histórico de los incidentes de seguridad ocurridos en la organización.

Cabe resaltar la investigación de Yáñez C., realizado en el año 2017 donde propuso un sistema de gestión de seguridad de la información para la Subsecretaria de Economía y Empresas de Menor Tamaño de Chile[61], utilizando herramientas de open source y modelos de desarrollo de mejora continua con el fin de dar cumplimiento al subconjunto de 44 objetivos de control del anexo normativo de la norma ISO 27001:2013.La elaboración de este proyecto de implementación de un SGSI que detalla la presente tesis, logró un cambio del enfoque de lo que la unidad de sistemas entendía como seguridad de la información, desde una mirada solo de seguridad informática a un concepto más amplio y de carácter estratégico para la organización: la necesidad de proteger la información como el activo valioso. Este nuevo enfoque permitió la implementación de nuevas políticas y procesos de

[60] David Alejando García Hernández, Jeison Herley Ruiz Murillo, ANÁLISIS Y GESTIÓN DE RIESGOS EN EL MARCO DEL SGSI, BASADO EN LA METODOLOGÍA MAGERIT Y APOYADO EN UNA API WEB PARA SU EJECUCIÓN, disponible en: http://repositorios.rumbo.edu.co/handle/123456789/121311

[61] Nelson Alejando Yáñez Cáceres, SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN PARA LA SUBSECRETARIA DE ECONOMÍA Y EMPRESAS DE MENOR TAMAÑO, Universidad de Chile, disponible en: http://repositorio.uchile.cl/bitstream/handle/2250/147976/Sistema-de-gestion-de-seguridad-de-la-informacion-para-la-Subsecretaria-de-Economia-y-Empresas.pdf?sequence=1&isAllowed=y

control, que sientan las bases para la creación de sistemas que monitorean y aseguran la mejora continua de las políticas y procedimientos definidos.

Por último, Bocanegra Q., en el año 2015 desarrolló un análisis y gestión de riesgos de los sistemas de información de la alcaldía municipal de Tuluá aplicando la metodología MAGERIT. Esta metodología les define a los autores dos fases para realizar la gestión de los riesgos; estas fases son, La etapa de análisis y La etapa de tratamiento de los riesgos. En la etapa de análisis, el autor determinó cuales eran los activos de la alcaldía, también identificó las amenazas que tenían respecto a la guía de MAGERIT, y por último realizó los salvaguardas para que estos riesgos tuviesen menor incidencia. La etapa de tratamiento de riesgos se realizó las acciones o medidas necesarias para suplir los riesgos identificados en el análisis y así cambiar esta situación. Y al finalizar las dos etapas se definieron las políticas de seguridad que la alcaldía debía cumplir para que no se presentasen las amenazas que fueron identificadas. Una adecuada gestión de los riesgos identificados durante el presente análisis impactará de forma positiva en la confiabilidad de los usuarios y la mejora de la imagen corporativa.

9.4. MARCO LEGAL

Para el fundamento legal de este proyecto, se examinará el tema referente a la Seguridad de la Información en Colombia, para contribuir al apoyo de la propuesta, estas son las Leyes vigentes hoy:

La siguiente ley protege obras literarias, artístico o científico, puesto que la universidad maneja gran contenido de esta índole.

Derechos de Autor

Decisión 351 de la C.A.N "REGIMEN COMUN SOBRE DERECHO DE AUTOR Y DERECHOS CONEXOS", Esta decisión promueve el reconocimiento adecuado y efectiva protección de los autores y demás titulares de derecho, sobre las obras de ingenio, en el campo literario, artístico o científico.[62]

Decreto 1360 de 1989 "Por el cual se reglamenta la inscripción de soporte lógico (software) en el Registro Nacional del Derecho de Autor" [63]

Artículo 1° Se le considerara al soporte lógico (software) como una invención propia del dominio literario.

---

[62] CARTAGENA, L. C. (17 de 12 de 1993). decisión 351. Obtenido de http://www.sice.oas.org/trade/junac/decisiones/Dec351s.asp

[63] COLOMBIA, E. P. (23 de 6 de 1989). *Decreto 1360 de 1989 Nivel Nacional*. Obtenido de http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=10575

Artículo 2° El soporte lógico (software) estará constituido o poseerá uno o varios de los siguientes elementos los cuales son, el programa de computador, la descripción del programa y el material auxiliar.

Artículo 3° Para la funcionalidad propia de este decreto se definirán los siguientes términos.

a) **Programa de computador:** Son un Conjunto de instrucciones las cuales le permiten al ordenador realizar una serie de tareas específicas.

b) **Descripción de programa:** presentación completa y detallada de las instrucciones que componen un programa de computador.

c) **Material auxiliar:** se le considerara a todo elemento que difiera de ser programa de computador o descripción de programa y el cual tenga como objetivo el brindar comprensión del uso del software, como por ejemplo manuales de usuario entre otros.

Artículo 4° Se le considerada una obra inédita al soporte lógico (software), a no ser que el titular de los derechos de autor manifieste lo contrario.
Artículo 5° Para la filiación en el Registro Nacional de Derechos de Autor del soporte lógico (software) será necesario diligenciar una solicitud con los siguientes datos:

- Nombre, identificación y dominio del solicitante.
- Nombre e identificación del autor.
- Nombre del productor.
- Título de la obra, año de creación, país de origen breve descripción de sus funciones.
- Especificar si es una obra original o es derivada de otra.
- Especificar cuantos autores intervinieron en la obra.

Artículo 6° Al diligenciar la solicitud anterior, esta deberá ser acompañada de al menos uno de los siguientes elementos que deberán componerla que son, el programa de computador, la descripción del programa y el material auxiliar.

Artículo 7° La seguridad que se le brinda al soporte lógico (software) mediante el derecho de autor no lo excluirá de otras formas de defensa por el derecho común.

Artículo 8° La fecha para la cual rige este decreto será el de su revelación.

Ley 44 de 1993 “Por la cual se modifica y adiciona la Ley 23 de 1982 y se modifica la Ley 29 de 1944”. En esta se especifica que los empleados y funcionarios públicos que sean autores de obras protegidas con derechos de autor podrán disponer de

estas en contractualmente ante cualquier entidad de derecho público.[64]

Decreto 460 de 1995 " Por el cual se reglamenta el Registro Nacional del Derecho de Autor y se regula el Depósito Legal"[65]

Decreto 162 de 1996 " Por el cual se reglamenta la Decisión Andina 351de 1993 y la Ley 44 de 1993, en relación con las Sociedades de Gestión Colectiva de Derecho de Autor o de Derechos Conexos"[66]

Ley 545 de 1999 "Por medio de la cual se aprueba el "Tratado de la OMPI - Organización Mundial de la Propiedad Intelectual- sobre Interpretación o Ejecución y Fonogramas (WPPT)", adoptado en Ginebra el veinte (20) de diciembre de mil novecientos noventa y seis (1996)"[67]

Ley 565 de 2000 "por medio de la cual se aprueba el "Tratado de la OMPI – Organización Mundial de la Propiedad Intelectual– sobre Derechos de Autor (WCT)", adoptado en Ginebra, el veinte (20) de diciembre de Mil novecientos noventa y seis (1996)."[68]

Ley 603 de 2000 "Por la cual se modifica el artículo 47 de la Ley 222 de 1995"[69]

Ley 719 de 2001 "Por la cual se modifican las Leyes 23 de 1982 y 44 de 1993 y se dictan otras disposiciones."[70]

Decisión 486 de la C.A.N. "Régimen Común sobre Propiedad Industrial"[71]

Decreto 2591 de 2000 "Por el cual se reglamenta parcialmente la Decisión 486 de la Comisión de la Comunidad Andina."[72]

---

[64] Colombia, E. C. (5 de 2 de 1993). Ley 44 de 1993 Nivel Nacional. Recuperado el 26 de 5 de 2018, de http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=3429

[65] COLOMBIA, E. P. (16 de 3 de 1995). Decreto 460 de 1995 Nivel Nacional. Recuperado el 26 de 5 de 2018, de http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=10576

[66] COLOMBIA, E. P. (22 de 1 de 1996). Decreto 162 de 1996 Nivel Nacional. Obtenido de http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=10574

[67] COLOMBIA, E. C. (31 de 12 de 1999). LEY 545 DE 1999. Recuperado el 26 de 5 de 2018, de http://propiedadintelectual.unal.edu.co/fileadmin/recursos/innovacion/docs/normatividad_pi/ley545_1999.pdf

[68] Colombia, E. C. (8 de 2 de 2000). LEY 565 DE 2000. Recuperado el 26 de 5 de 2018, de https://www.ins.gov.co/Normatividad/Leyes/LEY%200565%20DE%202000.pdf

[69] Colombia, E. C. (27 de 7 de 2000). LEY 603 DE 2000. Recuperado el 26 de 5 de 2018, de http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=13960

[70] COLOMBIA, E. C. (30 de 4 de 2018). LEY 719 DE 2001. Recuperado el 26 de 5 de 2018, de http://www.secretariasenado.gov.co/senado/basedoc/ley_0719_2001.html

[71] Andina, C. d. (1 de 12 de 2000). DECISIÓN 486: Régimen Común sobre Propiedad Industrial *. Recuperado el 26 de 5 de 2018, de http://www.sice.oas.org/Trade/Junac/Decisiones/dec486si.asp

[72] República, P. d. (13 de 12 de 2000). Decreto 2591 de 2000. Recuperado el 26 de 5 de 2018, de http://hdl.handle.net/11520/13737

Ley 463 de 1998 "Por medio de la cual se aprueba el "Tratado de cooperación en materia de patentes (PCT)", elaborado en Washington el 19 de junio de 1970, enmendado el 28 de septiembre de 1979 y modificado el 3 de febrero de 1984, y el reglamento del tratado de cooperación en materia de patentes."[73]

Ley 178 de 1994 "Por medio de la cual se aprueba el "Convenio de París para la Protección de la Propiedad Industrial", hecho en París el 20 de marzo de 1883, revisado en Bruselas el 14 de diciembre de 1900, en Washington el 2 de junio de 1911, en La Haya el 6 de noviembre de 1925, en Londres el 2 de junio de 1934, en Lisboa el 31 de octubre de 1958, en Estocolmo el 14 de julio de 1967 y enmendado el 2 de octubre de 1979. Específica que los países que se le aplica este convenio se constituyen en Unión para la Protección de la Propiedad Industrial, esta tiene como objeto las patentes de invención, los modelos de utilidad, los dibujos o modelos industriales, la marca de fábrica o de comercio, las marcas de servicio, el nombre comercial, las indicaciones de procedencia o denominaciones de origen, así la represión de la competencia desleal"[74].

- **Comercio Electrónico y Firmas Digitales**

Ley 527 de 1999 "Por medio de la cual se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales, y se establecen las entidades de certificación y se dictan otras disposiciones. La ley 527, es una ley de carácter probatorio, que permite aplicar las mismas consecuencias jurídicas que ostentan los medios físicos o tradicionales a la utilización de medio electrónicos."[75]

Para finalizar, **"LEY 1273 DE 2009 DE LA PROTECCIÓN DE LA INFORMACIÓN Y DE LOS DATOS".** Por el cual se modifica el **Código Penal**, se crea un nuevo bien jurídico tutelo- denominado 'de la protección de la información y de los datos' y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones también castiga los delitos informáticos.**"[76]**

LEY ESTATUTARIA 1266 DEL 31 DE DICIEMBRE DE 2008

[73] COLOMBIA, E. C. (2018 de 4 de 30). LEY 463 DE 1998. Recuperado el 26 de 5 de 2018, de http://www.secretariasenado.gov.co/senado/basedoc/ley_0463_1998.html

[74] COLOMBIA, E. C. (30 de 4 de 2018). LEY 178 DE 1994. Recuperado el 26 de 5 de 2018, de http://www.wipo.int/edocs/lexdocs/laws/es/co/co073es.pdf

[75] Colombia, E. C. (18 de 8 de 1999). Ley 527 de 1999 Nivel Nacional. Recuperado el 26 de 5 de 2018, de https://www.ambitojuridico.com/noticias/tic/uso-de-medios-electronicos-i-la-ley-527-de-1999-como-instrumento-normativo-suficiente

[76] EL CONGRESO DE LA REPUBLICA DE COLOMBIA DECRETA. Ley 1273 de 2009 [En línea]. Bogotá. 2009., 1 p. disponible en http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=34492

Esta ley es la encargada de la regulación el manejo de la información a continuación mencionamos una descripción de la norma.

"Por la cual se dictan las disposiciones generales del Hábeas Data y se regula el manejo de la información contenida en bases de datos personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países y se dictan otras disposiciones."[77]

TITULO II

DERECHOS DE LOS TITULARES DE LA INFORMACION

ARTICULO 6. DERECHOS DE LOS TITULARES DE LA INFORMACION. Mencionamos sus respectivos derechos que se dividen en tres, frente a los operadores de los bancos de datos, a las fuentes de información y frente a los usuarios, son explicadas cada una a continuación.

Frente a los operadores de los bancos de datos:

- Ejercer los procedimientos de consulta y reclamos sin afectar los órganos constitucionales y legales.
- Solicitar mediante el procedimiento de reclamos y peticiones, el respeto a las disposiciones de la presente ley.
- Requerir la certificación en la autorización expedida por la fuente o el usuario.
- Exigir la información de los usuarios que estén autorizados para la visualización de los datos.

Frente a las fuentes de la información:

- Ejercer los derechos fundamentales al habeas data, sin perjuicio de los mecanismos legales o constitucionales.
- Solicitar, actualizar, y rectificar la diferente información respecto a la base de datos.
- Pedir la prueba de la autorización en el caso de ser necesaria.

Frente a los usuarios:

- Solicitar información sobre el uso de los datos que le da un usuario a la misma en caso de no haber sido suministrada por el operador.
- Requerir prueba de la autorización cuando sea necesaria de acuerdo con la ley.

[77] EL CONGRESO DE LA REPUBLICA DE COLOMBIA DECRETA. Ley 1266 de 2008 [En línea]. Bogotá. 2008., 1 p. disponible en http://www.redipd.org/legislacion/common/legislacion/Colombia/LEY_1266_31_12_2008_HabeasData_COLOMBIA.pdf

Como se puede ver el primer capítulo, esta Ley está muy ligada a la ISO27000, lo cual coloca al País a la vanguardia en legislación de seguridad de la información, abriendo así la posibilidad de nuevas entradas con este tema.

10. CRONOGRAMA DE ACTIVIDADES

Tabla 5 Cronograma de actividades

ACTIVIDADES	Año 2019	DÍA																														
	MES	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
Fase 1Recolección de información de la institución y estado actual del ITFIP con respecto al Sistema de Información.																																
Rrecolección de información de la organización (presentación de la organización)	Enero															1	2	3	4	5		6	7	8	9							
Estado actual del sistema de información con respecto ISO/IEC 270001:2013 en el departamento de sistemas del ITFIP	Enero																									1	2		3	4	5	
Fase 2Análisis de Riesgos																																
Efectuar un análisis de riesgo empleando la metodología MAGERIT																																
Inventarios de activos	Enero																															1
Inventarios de activos	Febrero	2	3		4	5	6	7	8	9		10	11	12	13	14	15		16	17	18	19	20									
Clasificación de los activos	Febrero																							1		2	3	4	5			
Clasificación de los activos	Marzo	6	7		8																											
Valoración de los activos según su importancia	Marzo					1	2	3	4	5		6	7	8	9	10																
Análisis de la jerarquía de los activos entre sus grupos internos.	Marzo																1		2	3	4	5	6	7								

Tabla 6 Cronograma de actividades (continuación)

ACTIVIDADES	Año 2019	DÍA																															
	MES	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
Estimación de los valores de criterio en sus dimensiones de aplicabilidad	Marzo																									1	2	3	4	5	6	7
Estimación de los valores de criterio en sus dimensiones de aplicabilidad	Abril	8	9	10																												
Estimación de las amenazas que pueden afectar los activos.	Abril				1	2	3		4	5	6	7	8	9																		
Estimación de las amenazas que pueden afectar los activos.																							10	11								
Identificación de vulnerabilidades de los activos de información ante las amenazas potenciales																																
Inspección visual de los activos de información(informe)	Abril																								1	2	3	4		5	6	
Inspección visual de los activos de información(informe)	Mayo		7	8	9		10	11																								

Tabla 7 Cronograma de actividades (continuación)

ACTIVIDADES	Año 2019	DÍA																																
	MES	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
Estimación de las vulnerabilidades que pueden afectar a cada uno de los activos.	Mayo								1	2	3	4		5	6	7	8															
Estimación del impacto que causaría la PÉRDIDA de cada activo	Mayo																	1	2		3	4	5	6	7	8		9	10			
Estimación de la probabilidad de que ocurra perdida del activo	junio	1			2	3	4	5	6		7	8	9	10	11	12																
Estimación del riesgo	Junio																	1	2	3	4	5	6									
Estimación del riesgo	Julio		7	8	9	10	11		12	13	14	15																				
Aplicación de las salvaguardas a cada tipo de activo	Julio												1	2		3	4	5	6	7			8	9	10	11	12	13		14	15	16
Estrategia para el tratamiento de los riesgos de cada uno de los activos de la dependencia	Agosto	1	2	3																												
Técnicas para el tratamiento del riesgo	Agosto					1	2		3	4																						
Informe y evaluación de los tratamientos de riesgo																																
Identificación	Agosto										1		2	3	4	5	6	7			8	9	10	11	12		13	14	15	16	17	18
Identificación	Septiembre		19	20																												

Tabla 8 Cronograma de actividades (continuación)

ACTIVIDADES	Año 2019	DÍA																														
	MES	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
Tratamiento del riesgo	Septiembre				1	2	3																									
Técnicas para el tratamiento del riesgo	Septiembre							1		3	4	5	6	7	8		9	10	11	12	13	14		15								
Fase 3 Declaración de aplicabilidad																																
Declaración de aplicabilidad	Octubre																								1	2	3	4	5		6	7
Declaración de aplicabilidad	Noviembre	8	9	10	11	12		13	14	15																						

Fuente Propia

11. RESULTADOS

CAPITULO 1. RECOLECCIÓN DE INFORMACIÓN DE LA INSTITUCIÓN Y ESTADO ACTUAL DEL ITFIP CON RESPECTO AL SISTEMA DE INFORMACIÓN.

12. PRESENTACIÓN DE LA ORGANIZACIÓN

En esta sección se centrará toda la información recolectada con respecto a la Institución de Educación Superior – ITFIP, a su vez, se mostrará de manera gráfica y textual cada uno de los procesos que en esta se manejan, cada una de las dependencias y sus diferentes microsistemas. Lo contrario de la dependencia de sistemas, la cual se elaborará y de manera minuciosa los diferentes procesos que en ella se realizan

12.1. DESCRIPCIÓN DE LA EMPRESA

12.1.1. Historia. El Instituto Tolimense de Formación Técnica Profesional "ITFIP", fue creada mediante decreto 3462 del 24 de diciembre de 1980, es una institución de educación superior adscrita al Ministerio de Educación Nacional, de naturaleza jurídica pública oficial, con autonomía administrativa del orden nacional, con carácter académico de institución técnica profesional, redefinida para el ofrecimiento de programas por ciclos propedéuticos hasta el nivel profesional universitario, con sede principal en la ciudad de El Espinal, departamento del Tolima.

Actualmente, el ITFIP oferta programas académicos del nivel técnico profesional, tecnológico y profesional universitario por ciclos propedéuticos en las áreas de la Administración, las Ingenierías y las Humanidades, así mismo y en cumplimiento de la política de ampliación de cobertura, hace presencia en siete Centros Regionales de Educación Superior –CERES ubicados en los municipios de Flandes, Icononzo, Ricaurte, Venadillo, Guamo y Tocaima, funcionando como operadores, y en el CERES de Chaparral, Tolima, como oferentes, contando además con una sede por ampliación de cobertura en la ciudad de Ibagué.

12.1.2. Misión. El ITFIP como Institución de Educación Superior, forma integralmente al ser humano por competencias a través de programas académicos y servicios para generar, transformar, aplicar y difundir conocimientos y tecnologías en la solución a necesidades del entorno regional y nacional.

12.1.3. Visión. Al 2019 el ITFIP será una institución universitaria que forme con calidad, responsabilidad social y ambiental, mediante programas académicos acreditados de alta calidad, dándole oportunidad a la sociedad que genere un proyecto de vida que transforme su entorno y contribuya al desarrollo regional y nacional en un contexto internacional.

12.1.4. Ubicación geográfica. La Institución de Educación Superior ITFIP, se encuentra ubicada en la Calle 18 Carrera 1ª Barrio/Arkabal Espinal, Tolima – Colombia. A continuación, se muestra su ubicación satelital desde la herramienta Google Maps. Como se puede apreciar en el Anexo 1 ilustración 1.

12.2. ESTRUCTURA ORGANIZACIONAL

La estructura organizacional del ITFIP está enfocada en procesos, soportando un nuevo enfoque alrededor de una estructura sistemática que agrega valor al que hacer institucional; presentándose una estructura conformada por órganos colegiados y rectores, que le permiten garantizar funcionalidad en los distintos procesos académicos y administrativos de donde se derivan los comités institucionales, dependencias y áreas que bajo, que el sistema de calidad reconoce como procesos de apoyo académico y administrativo.[78]

En el Anexo 1 ilustración 2 se puede apreciar de manera gráfica la estructura organizacional por procesos del ITFIP.

12.2.1. Mapa de Procesos ITFIP. En el ITFIP, se maneja un modelo de operación que por medio del mapa de procesos se describen y está conformado por 13 procesos, los cuales están distribuidos de la siguiente manera: 1 proceso estratégico, 1 proceso de evaluación y control, 4 procesos misionales y 7 procesos de apoyo. [79]

En el Anexo 1 ilustración 3 se aprecia de manera gráfica el mapa de procesos.

12.2.2. Dependencias y sus procesos

Procesos y Procedimientos de "Direccionamiento Estratégico"
Dependencia: Direccionamiento Estratégico

Descripción: El direccionamiento estratégico consiste en planear y direccionar de manera sistemática los diferentes procesos que ejecuta la Institución, trazando

[78] ITFIP, Institución de Educación Superior. Manual de Procesos y Procedimientos "ITFIP" Versión N.º 5.0. Lugar de Publicación: Espinal-Tolima, diciembre de 2016. Pag: 15 [Consultado**:** 19 de septiembre de 2018].
[79] ITFIP, Institución de Educación Superior. Manual de Procesos y Procedimientos "ITFIP" Versión N.º 5.0. Lugar de Publicación: Espinal-Tolima, diciembre de 2016. Pag: 16 [Consultado**:** 19 de septiembre de 2018].

políticas y objetivos que permitan alcanzar la mejora continua de la eficacia, eficiencia y efectividad de la gestión, procurando el cumplimiento de las metas misionales. [80]

Procesos:

- FORMULACIÓN, EJECUCIÓN, ACTUALIZACIÓN Y SEGUIMIENTO DEL PLAN DE DESARROLLO INSTI TUCIONAL Y PLANES DE ACCION.

Este proceso consiste que por medio de un instrumento de planeación (denominado Plan de Desarrollo Institucional y Planes de acción), se desarrollan los objetivos, estrategias y directrices que proyecten el accionar institucional. Por medio de una evaluación y seguimiento en un periodo determino.

- ELABORACIÓN Y PRESENTACIÓN DEL ANTEPROYECTO DE PRESUPUESTO.

Este proceso consiste en analizar y proyectar el presupuesto con base a las necesidades institucionales y las directrices del Ministerio de Hacienda.

- PLANEACIÓN Y DESARROLLO DE LA INFRAESTRUCTURA FÍSICA.

Este proceso consiste en analizar y planear como se va a desarrollar la infraestructura de la planta física acorde a las necesidades de la institución.

- SUSCRIPCIÓN DE CONVENIOS MARCO Y ESPECÍFICO.

Este proceso consiste en fortalecer las alianzas estratégicas que facilita el desarrollo de la función social de la institución a través de convenios que garanticen el crecimiento de los procesos académicos y los demás intereses.

- RENDICIÓN DE CUENTAS A LA CIUDADANÍA.

Este proceso consiste en analizar y determinar todos los lineamientos necesarios que debe llevar a cabo la institución, para dar a conocer a la ciudadanía los resultados de la gestión realizada por la entidad, para que los participantes opinen y aporten ideas para el mejoramiento de la institución.

- IDENTIFICACION, FORMULACION Y SEGUIMIENTO DE INDICADORES.

Este proceso consiste en estableces, diseñar y construir indicadores que por medio de ellos se pueda medir la gestión de la institución y evaluar el desempeño de los procesos.

---

[80] ITFIP, Institución de Educación Superior. Caracterización de Proceso “Direccionamiento estratégico”. Lugar de Publicación: Espinal-Tolima, diciembre de 2016. Pag: 1 [Consultado**:** 26 de septiembre de 2018]. Disponible en Internet: https://www.itfip.edu.co/images/2015/CARACTERIZACION-DIRECCIONAMIENTO-ESTRATEGICO-2015.pdf

- ELABORACIÓN BOLETÍN ESTADÍSTICO.

Este proceso consiste en conocer las principales cifras estadísticas institucionales para ser analizadas para la toma de decisiones, para publicar anualmente un boletín estadístico.

Responsables de estos procesos:

- Asesor de Planeación – Profesional Universitario encargado.
- Rector.
- Profesional Universitario encargado (Planeación) y Líderes de proceso.81

En el Anexo 1 ilustración 4 y 5 se muestra de manera gráfica los procesos que maneja la dependencia de direccionamiento estratégico con sus respectivos responsables.

Procesos y Procedimientos de "Control Interno"

Dependencia: Control Interno

Descripción: Control interno tiene la función de verificar y acompañar el desarrollo de los procesos de la institución, para lograr una eficiencia. También vigilar que se estén cumpliendo los requerimientos establecidos por los entes de control. Todo esto con el fin de procurar que todas las actividades, operaciones y actuaciones, así como la administración de la información y los recursos, se realicen de acuerdo con las normas constitucionales y legales vigentes dentro de las políticas trazadas por la dirección y en atención a las metas u objetivos previstos.[82]

Procesos:

- PLANEACIÓN DE ACTIVIDADES ANUALES DE CONTROL INTERNO.

RESPONSABLE: Asesor Control Interno.

Este proceso consiste en establecer en ordenar todas las labores por realizar durante un año.

- ELABORACIÓN DEL PLAN DE ADMINISTRACIÓN DEL RIESGO.

RESPONSABLE: Alta Dirección y Asesor de Control Interno.

Este proceso consiste en identificar, analizar, valorar los riesgos que puede presentar la institución evaluando y verificando el grado de desarrollo de la

[81]ITFIP, Institución de Educación Superior. Manual de Procesos y Procedimientos "ITFIP" Versión N.º 5.0. Lugar de Publicación: Espinal-Tolima, diciembre de 2016. Pag: 23-44 [Consultado**:** 19 de septiembre de 2018].

[82] ITFIP, Institución de Educación Superior. Control Interno. Lugar de Publicación: Espinal-Tolima, diciembre de 2016. [Consultado: 26 de septiembre de 2018]. Disponible en Internet: http://www.itfip.edu.co/institucional/estructura-administrativa/control-interno.html

administración del riesgo y el cumplimiento de cada uno de los planes de contingencia para garantizar que la misión y visión se están logrando.

- APROBACIÓN Y SEGUIMIENTO DEL PLAN DE MEJORAMIENTO INSTITUCIONAL.

RESPONSABLE: Asesor de Control Interno.
Este proceso consiste en realizar un plan de mejoramiento institucional que corrija los hallazgos detectados por la contraloría general de la república, con esto se logra un mejoramiento continuo de la gestión institucional.

- ELABORACIÓN Y PRESENTACIÓN DE INFORMES A ENTES EXTERNOS.

RESPONSABLE: Asesor Control Interno.

Este proceso consiste en mantener la institución al día de compromisos adquiridos con los entes externos, por medio de solicitudes dentro de los términos de ley, para así obtener credibilidad.

- SEGUIMIENTO, CONTROL Y VERIFICACIÓN DE ACTIVIDADES EJECUTADAS POR LOS PROCESOS INSTITUCIONALES**.**

RESPONSABLE: Asesor de Control Interno y Líderes de Proceso.

Este proceso consiste en desarrollar estrategias e implementar mecanismos de control para evidenciar un mejoramiento continuo de los procesos en la institución.[83]

En el Anexo 1 ilustración 6se muestra de manera gráfica los procesos que maneja la dependencia de control interno con sus respectivos responsables.

Procesos y Procedimientos de "Gestión Jurídica"

Dependencia: Gestión Jurídica

Descripción: Gestión Jurídica se encarga de asesorar a las directivas de la institución en el desarrollo de políticas, planes y programas en el área de su especialidad, junto con las demás actividades que permitan cumplir las normas jurídicas. [84]

Procesos:

[83] ITFIP, Institución de Educación Superior. Manual de Procesos y Procedimientos "ITFIP" Versión N.º 5.0. Lugar de Publicación: Espinal-Tolima, diciembre de 2016. Pag: 45-56 [Consultado**:** 19 de septiembre de 2018].
[84] ITFIP, Institución de Educación Superior. Gestión Jurídica. Lugar de Publicación: Espinal-Tolima, diciembre de 2016. [Consultado: 26 de septiembre de 2018]. Disponible en Internet: http://www.itfip.edu.co/institucional/estructura-administrativa/gestion-juridica.html

- ATENCIÓN DE SUGERENCIAS, QUEJAS, RECLAMOS Y FELICITACIONES.

RESPONSABLE: Asesor Jurídico.

Este proceso consiste en recibir, registrar y analizar cada una de las sugerencias, quejas, reclamos y felicitaciones realizadas por la comunidad. Para tenerlas en cuenta e ir mejorando la institución.

- REVISIÓN JURÍDICA DE CONVENIOS.

RESPONSABLE: Asesor Jurídico.

Este proceso consiste en elaborar y evaluar los convenios que tiene la institución, que estos cumplan con las disposiciones legales establecidas y estén avalados.

- ACTUALIZACIÓN DE NORMAS Y LEYES.

RESPONSABLE: Asesor Jurídico.

Este proceso consiste en actualizar la información jurídica referente a la institución para que al momento de consultar sea rápido y eficaz.

- ASEGURAMIENTO DE BIENES

RESPONSABLE: Asesor Jurídico.

Este proceso consiste en proteger de manera efectiva los bienes de la institución en caso de algún siniestro.

- RECLAMACIÓN ANTE COMPAÑÍA DE SEGUROS POR PÉRDIDA, HURTO O DAÑO DEL BIEN

RESPONSABLE: Asesor Jurídico.

Este proceso consiste en presentar un reclamo ante la compañía de seguros para solicitar reposición o pago de indemnización.

- ATENCIÓN A DEMANDAS.

RESPONSABLE: Asesor Jurídico.

Este proceso consiste en atender las demandas en contra de la institución y defender jurídicamente los derechos e intereses.

- PROCESO DISCIPLINARIO CONTRA FUNCIONARIOS.

RESPONSABLE: Asesor Jurídico.

Este proceso consiste en adelantar el proceso disciplinario en contra de los funcionarios del ITFIP, brindando garantía del debido proceso y el derecho a defensa.

- RECUPERACIÓN DE CARTERA.

RESPONSABLE: Asesor Jurídico.

Este proceso consiste en recuperar la cartera mediante cobro persuasivo y coactivo, evitando que quede en mora.

- REVISIÓN DE ACTOS ADMINISTRATIVOS (RESOLUCIONES Y PROYECTOS DE ACUERDO).

RESPONSABLE: Asesor Jurídico.

Este proceso consiste en revisar que los actos administrativos que emita la institución se ajusten al derecho por medio de resoluciones, actas y proyectos de acuerdos.[85]

En el Anexo 1 ilustración 7 se muestra de manera gráfica los procesos que maneja la dependencia de gestión jurídica con sus respectivos responsables.

Procesos Y Procedimientos De Docencia

Dependencia: Docencia

Descripción: En esta dependencia el objetivo general es avalar cada uno de los componentes de la malla curricular, permitiendo así, la formación integral para los estudiantes de la institución de educación superior ITFIP.[86]

- PROGRAMACIÓN CALENDARIO ACADÉMICO

RESPONSABLE: Concejo académico.

Bajo este proceso, el concejo académico conformado por docentes de la institución busca conformar de manera eficiente la asignación de docentes, materias y grupos a trabajar durante los periodos académicos, con el fin de cada programa se pueda acoger al mismo.

---

[85] ITFIP, Institución de Educación Superior. Manual de Procesos y Procedimientos “ITFIP” Versión N.º 5.0. Lugar de Publicación: Espinal-Tolima, diciembre de 2016. Pag: 57-78 [Consultado**:** 19 de septiembre de 2018].

[86] ITFIP, Institución de Educación Superior. Caracterización de proceso. Lugar de Publicación: Espinal-Tolima, noviembre de 2014. [Consultado: 27 de septiembre de 2018]. Disponible en Internet: http://www.itfip.edu.co/images/2014/CARACTERIZACION%20DOCENCIA%20%202014.pdf

- ASEGURAMIENTO DE RECURSO DOCENTE PARA EL EJERCICIO ACADÉMICO

RESPONSABLE(S): Vicerrector académico, decanos y organizadores.
Bajo este proceso, el área encargada de vicerrectoría académica, en compañía de los ya mencionados anteriormente, se reúnen a establecer los recursos necesarios para cada uno de los programas que la institución ofrece, también se ejecuta la selección adecuada de cada uno de los decentes encargados a orientar los mismos, esto se realiza con el objetivo de dividir de manera acertada los docentes con los cuales cuenta la institución. Esto se realiza a la previa selección del personal institucional para dictar clases.

- PLANEACIÓN Y PROGRAMACIÓN ACADÉMICA

RESPONSABLE(S); Vicerrector académico, decanos, coordinadores grupo interno de trabajo académico y docentes.

En este proceso, los responsables mencionados, tienen como objetivo establecer, diseñar y estructurar la adecuada planeación académica, esto se logra con el propósito de alcanzar unas metas establecidas, entre las que se alcanza a abarcar planes de operación, horarios de clases, la realización de las actividades de grado, entre otras.

- EJECUCIÓN DEL EJERCICIO ACADÉMICO

RESPONSABLE(S): Decanos, coordinadores grupo interno de trabajo académico y docentes.

Para este proceso, el objetivo general de los responsables involucrados es poder implementar en la comunidad educativa, por medio de los docentes las competencias necesarias para la obtención de cualquiera de los títulos en oferta.

- EVALUACIÓN DEL EJERCICIO DOCENTE

RESPONSABLE(S): VICERRECTOR ACADÉMICO Y DECANOS.
Como objetivo principal, la institución en representación de la vicerrectoría académica y decanos, evalúan el nivel del docente, esto se realiza con el fin de hallar las fortalezas y debilidades del personal contratado; obteniendo estadísticas concretas.

- DISEÑO Y REDISEÑO DE PROGRAMAS ACADÉMICOS

RESPONSABLE(S): DECANOS, COORDINADORES GRUPO INTERNO DE TRABAJO Y DOCENTES.

Uno de los procesos más importantes para la institución, puesto que permite estar en la vanguardia de las últimas tendencias a nivel de escolaridad y metodologías de estas; como también permitiendo tener los currículos actualizados ante cualquier auditoria.

- REUNIONES DE ORGANISMOS E INSTANCIAS DE ASESORÍA, DIRECCIÓN Y ACOMPAÑAMIENTO

RESPONSABLE(S): MÁXIMA AUTORIDAD DE CADA ORGANISMO.

Como eje central, en este proceso los interventores directos suelen cumplir un rol de máxima “autoridad”; con el objetivo de indicar el correcto funcionamiento académico ante otras instancias superiores a ellas, esto se realiza con el objetivo de contemplar las debidas constancias a reuniones ejecutadas, como también conceptos básicos sobre sus propias temáticas.

- PRÉSTAMO Y USOS DE LABORATORIOS

RESPONSABLE(S): FUNCIONARIOS RESPONSABLES DE LOS RECURSOS ACADÉMICOS (LABORATORIOS).

En este proceso, se busca poder brindar todas las herramientas con las que cuenta la institución. El préstamo de laboratorios de electrónica, física y demás derivadas a la comunidad educativa. Esto se cataloga y guarda constancia en un documento para poder elaborar las estadísticas pertinentes.

- PROMOCIÓN DE PROGRAMAS ACADÉMICOS

RESPONSABLE(S): VICERRECTOR ACADÉMICO Y DECANOS.

Con este proceso, la institución en cabeza de la vicerrectoría académica y decanos, buscan los medios necesarios para aumentar la publicidad de cada uno de los programas que esta ofrece, con el objetivo de generar más cobertura regional y el reconocimiento necesario ante los demás entes de educación superior.

- SELECCIÓN DE DOCENTES HORA CATEDRA Y OCASIONAL

RESPONSABLE(S): VICERRECTORÍA ACADÉMICA, DECANOS Y COORDINADORES GRUPOS INTERNOS DE TRABAJO ACADÉMICOS.

Este proceso es uno de los más importantes como pilar de la institución, puesto que la estructura principal para la formación de cada uno de los estudiantes que posan su confianza en la institución, puesto que los responsables mencionados anteriormente, analizan cada uno de los perfiles de los orientadores, realizando un

filtro del personal apropiado. La realización de este proceso permite arrojar el resultado de los docentes aprobados para dictar clases en los periodos en cursos.[87]

En el Anexo 1 ilustración 8, se evidenciará de manera gráfica cada uno de los procesos mencionados con anterioridad.

Procesos y procedimientos de Investigación

Dependencia: Investigación

Descripción: Esta dependencia se centra en la fomentación de la investigación de los estudiantes, permitiéndoles alcanzar nuevos logros intelectuales, la adquisición de conocimiento, lo cual conlleva a la solución de problemas del entorno, empleando los conocimientos poseídos.[88]

- INDUCCIÓN Y/O REINDUCCIÓN DEL PROCESO DE INVESTIGACIÓN.

RESPONSABLE(S): VICERRECTORÍA ACADÉMICA, COORDINADOR G.I.T.I. Y PERSONAL DE APOYO.
En este proceso, los encargados directos se encargan de dar capacitación oportuna a la comunidad en general, entre la que se encuentran docentes y estudiantes de la institución. Esto se realiza con el fin de dar a conocer los beneficios de investigar.

- DESARROLLO DE LOS PROYECTOS DE INVESTIGACIÓN E INNOVACIÓN.

RESPONSABLE(S): VICERRECTORÍA ACADÉMICA, DECANOS, COORDINADOR DE INVESTIGACIÓN, LÍDERES DE GRUPOS DE INVESTIGACIÓN Y DOCENTES INVESTIGADORES.
En este apartado, se busca centrar y agrupar las líneas de investigación en beneficio a los programas que ofrece la institución, ya que a su vez permite suplir las necesidades con soluciones surgidas a través de los grupos de investigación.

- VISIBILIDAD DE LA INVESTIGACIÓN.

RESPONSABLE(S): VICERRECTORÍA ACADÉMICA, DECANOS, GRUPO INTERNO DE TRABAJO PARA EL DESARROLLO DE LA INVESTIGACIÓN E INVESTIGADORES.

---

[87] ITFIP, Institución de Educación Superior. Manual de Procesos y Procedimientos “ITFIP” Versión N.º 5.0. Lugar de Publicación: Espinal-Tolima, diciembre de 2016. Pág.: 79-104 [Consultado: 19 de septiembre de 2018].
[88] ITFIP, Institución de Educación Superior. Caracterización de procesos “ITIFP”. Lugar de Publicación: Espinal-Tolima, noviembre de 2015. [Consultado: 26 de septiembre de 2018]. Disponible en Internet:
https://itfip.edu.co/images/2015/CARACTERIZAION-INVESTIGACION-2015.pdf

Teniendo en cuenta el proceso anterior (Desarrollo de los proyectos de investigación e innovación), este proceso busca exponer los resultados obtenidos, permitiéndoles la posibilidad de sustentar dichas investigaciones ante entes nacionales e internacionales.

- PROYECTOS DE GRADO DE INVESTIGACIÓN.

RESPONSABLE(S): DECANOS, COMITÉ CURRICULAR, DOCENTES, COORDINADORES DE GRUPOS INTERNOS DE TRABAJO DE LOS PROGRAMAS Y ESTUDIANTES.

Con la realización de estos proyectos de investigación, la comunidad estudiantil tiene la oportunidad de optar por el título, puesto que la inclusión en semilleros de investigación repercute a una ardua labor en la institución ante los entes investigadores. Como a su vez, la obtención del grado por parte del estudiante.

- DESARROLLO DE SEMILLEROS DE INVESTIGACIÓN

RESPONSABLE(S): ESTUDIANTES, DOCENTES, DECANOS, COORDINADORES DE PROGRAMA, VICERRECTORÍA ACADÉMICA Y COORDINADOR DE INVESTIGACIÓN.

Con la implementación de este proceso, la comunidad educativa podrá encontrar un espacio en el cual podrán adelantar proyectos investigativos, esto además de estar acompañados de los docentes y demás funcionarios capacitados. [89]

En el Anexo 1 ilustración 9, se manifestará de manera gráfica los procesos ya mencionados anteriormente.

Procesos y Procedimientos de "Proyección Social"

Dependencia: Proyección Social

DESCRIPCIÓN: En la dependencia de proyección social es la encargada del desarrollo de los procesos de interacción desde diversos programas académicos, para lograr un impacto en la comunidad y en la región.[90]

[89] ITFIP, Institución de Educación Superior. Manual de Procesos y Procedimientos "ITFIP" Versión N.º 5.0. Lugar de Publicación: Espinal-Tolima, diciembre de 2016. Pág.: 105-118 [Consultado: 19 de septiembre de 2018].

[90] ITFIP, Institución de Educación Superior. Caracterización de procesos "ITIFP". Lugar de Publicación: Espinal-Tolima, noviembre de 2015. [Consultado: 26 de septiembre de 2018]. Disponible en Internet:
https://www.itfip.edu.co/images/2015/CARACTERIZACION-PROYECCION-SOCIAL-2015.pdf

- PLANEACIÓN Y PROGRAMACIÓN DE LA PROYECCIÓN SOCIAL Y EXTENSIÓN

RESPONSABLE(S): Vicerrectoría Académica - Decanos y coordinador de extensión.

Este proceso consiste en la planeación, programación e implementación de los programas académicos de las facultades.

- PRÁCTICAS EMPRESARIALES O SUPERVIDASADA Y PASANTÍAS

RESPONSABLE(S): Decanos – Coordinadores de grupo interno de trabajo académico – Estudiantes - directores de trabajo de grado.

Este proceso consiste En el desarrollo de tecnologías propias de cada programa académico, además de contar con prácticas y pasantías supervisadas en las diferentes facultades.

- OFERTA DE SERVICIOS A LA COMUNIDAD INTERNA Y EXTERNA A TRAVÉS DE EDUCACION NO FORMAL.

RESPONSABLE(S): DECANOS, COORDINADORES DE EXTENCION Y DOCENTES RESPONSABLES.

Este proceso consiste en ofertas de educación no formal de instituciones de diferentes sectores de economía local y regional.

- OFERTA DE SERVICIOS A LA COMUNIDAD INTERNA Y EXTERNA A TRAVÉS DE LOS PROGRAMAS ACADÉMICOS EN ASESORÍAS – CONSULTORÍAS Y OTROS SERVICIOS

RESPONSABLE(S): VICERRECTOR ACADEMICO**,** DECANOS Y COORDINADOR DE EXTENCION.

Este proceso consiste en la prestación de servicios como asesorías y consultorías para la comunidad estudiantil.

- EXTENSIÓN DE LOS PROGRAMAS ACADÉMICOS

RESPONSABLE(S): Rector, Vicerrector Académico, Decanos y coordinadores grupo interno de trabajo.

Este proceso consiste en las ofertas para los programas académicos de la institución a través de convenios con otros entes y municipios.

- PROGRAMA DE SEGUIMIENTO A EGRESADOS

RESPONSABLE(S): RECTORÍA, VICERRECTOR ACADÉMICO, DECANOS.

Este proceso consiste en el desarrollo de vínculos con el egresado, de tal modo que mejore: los servicios, registro de datos y mejore la participación en los organismos en la institución.

- IMPLEMENTACIÓN DEL SISTEMA EVALUATIVO DEL EJERCICIO DE PROYECCIÓN SOCIAL DEL PROGRAMA

RESPONSABLE(S): VICERRECTORÍA ACADÉMICA –COORDINADOR DE EXTENSIÓN – DECANOS – GRUPOS DE TRABAJO.

Este proceso consiste en la evaluación del desarrollo de la Proyección Social en los programas académicos de la institución.[91]

En el Anexo 1 ilustración 10 se muestra de manera gráfica los procesos que maneja la dependencia de proyección social con sus respectivos responsables.

Procesos y Procedimientos de "Registro y Control Académico"

Dependencia: Registro y Control Académico

Descripción: En la dependencia de registro y control académico es la oficina encargada del Registro y control de las calificaciones de los estudiantes; además de la administración de la vida académicas desde su inicio hasta su culminación incluyendo sus registros como egresado. Además, es la encargada de organizar, registrar y controlar toda la información de los estudiantes como: el calendario académico, matrícula académica, registro de notas, certificaciones, administración de documentos e historia académica del estudiante y Actualización de Carnets.[92]

- APERTURA, DESARROLLO Y CIERRE DE PERIODOS ACADEMICOS

RESPONSABLE(S): PROFESIONAL UNIVERSITARIO.

Este proceso consiste en la organización y desarrollo de las actividades programadas desde el inicio hasta la culminación del periodo académico.

---

[91] ITFIP, Institución de Educación Superior. Manual de Procesos y Procedimientos "ITFIP" Versión N.º 5.0. Lugar de Publicación: Espinal-Tolima, diciembre de 2016. Pág.: 119-137 [Consultado: 19 de septiembre de 2018].

[92] ITFIP, Institución de Educación Superior. Caracterización de procesos "ITIFP". Lugar de Publicación: Espinal-Tolima, noviembre de 2015. [Consultado: 26 de septiembre de 2018]. Disponible en Internet: http://www.itfip.edu.co/procesos-academicos/oficina-de-admisiones-registro-y-control-academico.html

- ADMISIÓN DE ESTUDIANTES A LOS DISTINTOS PROGRAMAS ACADÉMICOS.

RESPONSABLE(S): PROFESIONAL UNIVERSITARIO.

Este proceso consiste en el seguimiento oportuno de las inscripciones de los aspirantes a ingresar a los diferentes programas académicos que oferta la institución.

- MATRÍCULA DE ESTUDIANTES

RESPONSABLE(S): PROFESIONAL UNIVERSITARIO.

Este proceso consiste en la actualización de la información de los estudiantes para los programas académicos matriculados.

- ELABORACIÓN DE CONSTANCIAS, CERTIFICADOS, DUPLICADO DE DIPLOMAS, COPIAS ACTAS DE GRADO Y VALIDACIONES DE TITULOS.

RESPONSABLE(S): PROFESIONAL UNIVERSITARIO.

Este proceso consiste en brindar oportunidades a los estudiantes para el desarrollo de actividades dentro del proceso de formación académica

- ORGANIZACIÓN Y MANEJO DEL ARCHIVO DE GESTIÓN.

RESPONSABLE(S): PROFESIONAL UNIVERSITARIO.

Este proceso consiste en contar con una oportuna disposición y fácil acceso a la información documental y magnética de manera organizada con el fin de prestar un óptimo servicio al cliente

- REGISTRÓ DE ESTADÍSTICAS DE POBLACIÓN ESTUDIANTIL EN EL SNIES.

RESPONSABLE(S): PROFESIONAL UNIVERSITARIO.
Este proceso consiste en el registro oportuno del sistema SNIES para la información estadística de la población estudiantil de manera semestral.

- OTORGAMIENTO DE TÍTULOS DE EDUCACIÓN SUPERIOR.

RESPONSABLE(S): PROFESIONAL UNIVERSITARIO.

Este proceso consiste en la organización de los documentos para los graduados; además organizar y archivar las carpetas individuales de los estudiantes graduados.[93]

En el Anexo 1 ilustración 11 se muestra de manera gráfica los procesos que maneja la dependencia de Registro y Control académico con sus respectivos responsables.

Procesos y Procedimientos de "Bienestar Universitario"

Dependencia: Bienestar Universitario

Descripción: En la dependencia de bienestar universitario es la encargada de las actividades, planes, programas y proyectos que se orientan al desarrollo físico, Psicoafectivo, espiritual, social y cultural de los Estudiantes, Docentes, personal Administrativo y en general comunidad institucional.[94]

- PLANEACIÓN Y EJECUCIÓN DE ACTIVIDADES DE SALUD

RESPONSABLE(S): Encargado Bienestar Universitario.
Este proceso consiste en el mejoramiento de las condiciones ambientales y físicas de la comunidad, mediante programas preventivos, prevención a través de consultas y capacitación personal

- PLANEACIÓN Y EJECUCIÓN DE ACTIVIDADES DEPORTIVAS Y RECREATIVAS.

RESPONSABLE(S): Encargado Bienestar Universitario.
Este proceso consiste en el aprovechamiento del tiempo libre de los estudiantes por medio de desarrollos y prácticas en el deporte para la participación de la comunidad académica; estudiantes, docentes y personal administrativo.

- PLANEACIÓN Y EJECUCIÓN DE ACTIVIDADES CULTURALES

RESPONSABLE(S): Encargado Bienestar Universitario.

Este proceso consiste en la conformación y consolidación de grupos artísticos y culturales en la institución

[93] ITFIP, Institución de Educación Superior. Manual de Procesos y Procedimientos "ITFIP" Versión N.º 5.0. Lugar de Publicación: Espinal-Tolima, diciembre de 2016. Pág.: 138-153 [Consultado: 19 de septiembre de 2018].
[94] ITFIP, Institución de Educación Superior. Caracterización de procesos "ITIFP". Lugar de Publicación: Espinal-Tolima, noviembre de 2015. [Consultado: 26 de septiembre de 2018]. Disponible en Internet:
http://www.itfip.edu.co/institucional/estructura-administrativa/vicerrectoria-academica/bienestar-universitario

- PLANEACIÓN Y EJECUCIÓN DE ACTIVIDADES DE DESARROLLOHUMANO

RESPONSABLE(S): Encargado Bienestar Universitario.

Este proceso consiste en el fortalecimiento de las relaciones humanas mediante capacitaciones para los estudiantes nuevos que ingresen al primer semestre a los diferentes programas académicos.

- PLANEACIÓN Y DESARROLLO DEL PROGRAMA ESTÍMULOS EDUCATIVOS.

RESPONSABLE(S): Encargado Bienestar Universitario.

Este proceso consiste en el apoyo y facilidad de ingreso de los estudiantes en los programas de educación superior, mediante la asignación de estímulos otorgados.

- PLANEACIÓN Y EJECUCIÓN PROGRAMA DE ELECTIVAS.

RESPONSABLE(S): Encargado Bienestar Universitario.

Este proceso consiste en la integración de la comunidad estudiantil para que participe activa en diferentes horarios y actividades programas de electivas.

- ATENCIÓN POR CONSULTA DE MEDICINA GENERAL Y ODONTOLOGÍA

RESPONSABLE(S): Encargado Bienestar Universitario.

Este proceso consiste en ofrecer diferentes servicios de consulta externa de medicina general y Odontología, con el fin de proporcionar el bienestar de los estudiantes para tener una mejor calidad de vida.[95]
En el Anexo 1 ilustración 12 se muestra de manera gráfica los procesos que maneja la dependencia de bienestar universitario con sus respectivos responsables.

Procesos y Procedimientos de "Servicios Académicos y Biblioteca"

Dependencia: Servicios Académicos y Biblioteca

Descripción: En la dependencia de servicios académicos y biblioteca es la encargada de proveer a los estudiantes el servicio de apoyo académico como salas

[95] ITFIP, Institución de Educación Superior. Manual de Procesos y Procedimientos "ITFIP" Versión N.º 5.0. Lugar de Publicación: Espinal-Tolima, diciembre de 2016. Pág.: 154-168 [Consultado: 19 de septiembre de 2018].

de proyecciones, equipos audiovisuales, material bibliográfico, ayudas didácticas y laboratorios, para un mejor desarrollo de las actividades académicas.[96]

- ADQUISICIÓN DEL MATERIAL BIBLIOGRÁFICO.

RESPONSABLE(S): PROFESIONAL UNIVERSITARIO.

Este proceso consiste en el préstamo de material bibliográfico actualizado y acorde a las exigencias de los planes de estudio de la institución.

- CLASIFICACIÓN Y REGISTRO DEL MATERIAL BIBLIOGRÁFICO E INCORPORACIÓN EN EL SISTEMA DE INFORMACIÓN EMPLEADO POR LA BIBLIOTECA ITFIP.

RESPONSABLE(S): PROFESIONAL UNIVERSITARIO.

Este proceso consiste en un sistema de colección bibliográfica actualizada en la biblioteca; así por medio de base de datos agilizan el préstamo y circulación del material

- MANTENIMIENTO Y CONSERVACIÓN DEL MATERIAL BIBLIOGRÁFICO

RESPONSABLE(S): PROFESIONAL UNIVERSITARIO.
Este proceso consiste en la protección y conservación de las colecciones de libros que se encuentran en la biblioteca.

- PRÉSTAMO DEL MATERIAL BIBLIOGRÁFICO.

RESPONSABLE(S): ENCARGADO DEL ÁREA DE CIRCULACIÓN Y PRÉSTAMO DE SERVICIOS ACADÉMICOS Y BIBLIOTECA.
Este proceso consiste en ofrecer un buen servicio eficaz y óptimo para todos los estudiantes de la institución.

- PRÉSTAMO DE EQUIPOS Y MATERIAL AUDIOVISUAL.

RESPONSABLE(S): ENCARGADO SERVICIOS ACADÉMICOS Y BIBLIOTECA.

Este proceso consiste en el préstamo oportuno de equipos, salas de proyecciones y material audiovisual acorde con el sistema educativo institucional.

- ELABORACIÓN E IDENTIFICACIÓN INSTITUCIONAL (CARNÉT).

[96] ITFIP, Institución de Educación Superior. Caracterización de procesos “ITIFP”. Lugar de Publicación: Espinal-Tolima, noviembre de 2015. [Consultado: 26 de septiembre de 2018]. Disponible en Internet: https://itfip.edu.co/images/2014/CARACTERIZACION%20SERVICIOS%20ACADEMICOS%202014.pdf

RESPONSABLE(S): ENCARGADO DEL ÁREA PRÉSTAMO EQUIPOS, SALAS Y MATERIAL AUDIOVISUAL DE SERVICIOS ACADÉMICOS Y BIBLIOTECA.

Este proceso consiste en el apoyo de las actividades académicas y administrativas, mediante un carné institucional con el cual facilita el préstamo de equipos salas de proyecciones y material audiovisual para la comunidad estudiantil

- ELABORACIÓN DE ESTADÍSTICAS DEL ÁREA DE BIBLIOTECA Y AUDIOVISUALES.

RESPONSABLE(S): PROFESIONAL UNIVERSITARIO.

Este proceso consiste en la actualización y soporte de datos que permiten el mejoramiento continuo de los procesos del área.[97]

En el Anexo 1 ilustración 13 se muestra de manera gráfica los procesos que maneja la dependencia de servicios académicos y biblioteca con sus respectivos responsables.

Procesos y Procedimientos de "Gestión Administrativa e Infraestructura Física"

Dependencia: Gestión Administrativa e Infraestructura Física.
Descripción: En la dependencia de gestión administrativa e infraestructura física es la encargada de guiar procesos de dirección, organización y supervisión de actividades relacionadas al Recurso Humano, Infraestructura Física y Financiera de la Institución.[98]

- CONTRATACIÓN DE BIENES Y SERVICIOS

RESPONSABLE(S): Vicerrector Administrativo – Profesional de Contratación.
Este proceso consiste en atender las necesidades de bienes y servicios de la institución.

- PRESTAMO DE ELEMENTOS O ESPACIOS FISICOS

RESPONSABLE(S): VICERRECTOR ADMINISTRATIVO.

---

[97] ITFIP, Institución de Educación Superior. Manual de Procesos y Procedimientos "ITFIP" Versión N.º 5.0. Lugar de Publicación: Espinal-Tolima, diciembre de 2016. Pág.: 169-186 [Consultado: 19 de septiembre de 2018].

[98] ITFIP, Institución de Educación Superior. Caracterización de procesos "ITIFP". Lugar de Publicación: Espinal-Tolima, noviembre de 2015. [Consultado: 26 de septiembre de 2018]. Disponible en Internet:
https://www.itfip.edu.co/images/2015/CARACTERIZACION-GESTION-ADMINISTRATIVA-2015.pdf

Este proceso consiste en dirigir y revisar los elementos físicos prestados para un mejor agrado del cliente.

- MANTENIMIENTO DE INFRAESTRUCTURA FISICA, REDES ELECTRICAS, EQUIPOS Y MAQUINARIA

RESPONSABLE(S): Operario Calificado – Contratista.

Este proceso consiste en mantener un buen funcionamiento de las instalaciones, equipos y maquinaria.

- TRAMITE DE VIATICOS

RESPONSABLE(S): VICERRECTORIA ADMINISTRATIVA.

Este proceso consiste en suministrar recursos financieros para viáticos para los funcionarios que tengan que desplazarse fuera del municipio en representación de la institución.

- REPORTE MENSUAL HORAS EXTRAS, RECARGO NOCTURNO, DOMINICALES Y FESTIVO DE ASEO Y VIGILANCIA

RESPONSABLE(S): PROFESIONAL DE APOYO VICERRECTORÍA ADMINISTRATIVA.

Este proceso consiste en contener una relación de horas extras y recargos nocturnos desarrollado y elaborado por el personal de servicios y vigilancia a la oficina de talento humano.

- COORDINACION, EJECUCION Y CONTROL DE LIMPIEZA GENERAL

RESPONSABLE(S): AUXILIAR SERVICIOS GENERALES – VICERRECTORÍA ADMINISTRATIVA.

Este proceso consiste en ordenar y mantener limpia las oficinas, pisos, aulas, baños, laboratorios y áreas comunes de las instalaciones de la Institución.

- COORDINACION, EJECUCIÓN Y CONTROL DE ACTIVIDADES DE VIGILANCIA A INSTALACIONES FÍSICAS Y BIENES MUEBLES DE LA INSTITUCIÓN.

RESPONSABLE(S): VICERRECTORÍA ADMINISTRATIVA - CELADOR DE TURNO**.**

Este proceso consiste en proteger la seguridad del personal estudiantil y bienes de la institución.

- CONSERVACION DE ZONAS VERDES

RESPONSABLE(S): VICERRECTORÍA ADMINISTRATIVA.

Este proceso consiste en proteger y conservar las zonas verdes y jardines de la institución.

- MANEJO DE CAJA MENOR

RESPONSABLE(S): FUNCIONARIO ASIGNADO POR RECTORÍA.

Este proceso consiste en reemplazar las necesidades menores urgentes de la institución.

- ENVÍO DE CORRESPONDENCIA PARA ENTIDADES EXTERNAS

RESPONSABLE(S): FUNCIONARIO ENCARGADO DE OFICINA ATENCIÓN AL CIUDADANO.

Este proceso consiste en supervisar la documentación dirigida a entes externos.

- RECIBO DE CORRESPONDENCIA

RESPONSABLE(S): FUNCIONARIO ENCARGADO DE OFICINA ATENCIÓN AL CIUDADANO**.**

Este proceso consiste en controlar y administrar los documentos recibidos por entes externos.

- MANEJO DEL ARCHIVO CENTRAL DE LA INSTITUCIÓN.

RESPONSABLE(S): TÉCNICO Y AUXILIAR ADMINISTRATIVO.
Este proceso consiste en ordenar correctamente la información de fácil acceso al usuario.

- PRESTAMO DE DOCUMENTOS DEL ARCHIVO CENTRAL

RESPONSABLE(S): AUXILIAR ADMINISTRATIVO.

Este proceso consiste en solucionar cualquier petición del interesado en algún tipo de documento que repose en el archivo de la institución.

- MANTENIMIENTO PREVENTIVO Y CORRECTIVO DE LOS SISTEMAS INFORMATICOS DE LA INSTITUCION

RESPONSABLE(S): FUNCIONARIO ENCARGADO POR LA VICERRECTORÍA ADMINISTRATIVA Y PLANEACIÓN.

Este proceso consiste en proteger y prevenir daños en los sistemas informáticos de la institución.[99]

En el Anexo 1 ilustración 14 se muestra de manera gráfica los procesos que maneja la dependencia de gestión administrativa e infraestructura física con sus respectivos responsables.

Procesos y Procedimientos de "**Gestión Administrativa e Infraestructura Física (Almacén)"**

Dependencia: Gestión Administrativa e Infraestructura Física (Almacén)

Descripción: En la dependencia de gestión administrativa e infraestructura física (Almacén) es la encargada de dar apoyo a vicerrectoría administrativa para dar cumplimiento a políticas y normas establecidas por la institución[100]

- ADQUISICIÓN POR COMPRAS

RESPONSABLE(S): PROFESIONAL UNIVERSITARIO (ALMACÉN).

Este proceso consiste en la compra de elementos necesarios requeridos por la institución para tener un buen funcionamiento de esta.

- ELABORACIÓN PLAN ANUAL DE ADQUISICIONES

RESPONSABLE(S): PROFESIONAL UNIVERSITARIO (ALMACÉN) /LÍDER PROCESO GESTIÓN ADMINISTRATIVO E INFRAESTRUCTURA FÍSICA.

Este proceso consiste en la elaboración de un plan anual para la adquisición de nuevos elementos, insumos y equipos que requiera la institución por cada vigencia.

- INGRESOS DE BIENES A ALMACÉN

RESPONSABLE(S): PROFESIONAL UNIVERSITARIO (ALMACÉN).

---

[99] ITFIP, Institución de Educación Superior. Manual de Procesos y Procedimientos "ITFIP" Versión N.º 5.0. Lugar de Publicación: Espinal-Tolima, diciembre de 2016. Pág.: 187-233 [Consultado: 19 de septiembre de 2018].

[100] ITFIP, Institución de Educación Superior. Caracterización de procesos "ITIFP". Lugar de Publicación: Espinal-Tolima, noviembre de 2015. [Consultado: 26 de septiembre de 2018]. Disponible en Internet: http://www.itfip.edu.co/institucional/estructura-administrativa/vicerrectoria-administrativa/gestion-financiera/almacen

Este proceso consiste en el ingreso al almacén de todos los bines, equipos y muebles que son adquiridos por diferentes modalidades.

- ENTREGA DE ELEMENTOS Y/O BIENES

RESPONSABLE(S): PROFESIONAL UNIVERSITARIO (ALMACÉN) - JEFE ALMACÉN.

Este proceso consiste en el registro de salida de todos los elementos que requieren los funcionarios de la institución.

- BAJA DE BIENES

RESPONSABLE(S): JEFE ALMACÉN **-** PROFESIONAL UNIVERSITARIO (ALMACÉN).

Este proceso consiste en contar con un inventario de los elementos defectuosos o dañados para su respectiva devolución.

- INVENTARIO FÍSICO DE BIENES DEVOLUTIVOS EN SERVICIO (anual)

RESPONSABLE(S): PROFESIONAL UNIVERSITARIO (ALMACÉN)
Este proceso consiste en la realización de un inventario por cada dos años de los elementos funcionales y deteriorados que se encuentran en uso por los funcionarios de cada dependencia.

- ELABORACIÓN DEL BALANCE MENSUAL

RESPONSABLE(S): PROFESIONAL UNIVERSITARIO (ALMACÉN).

Este proceso consiste en la realización de un balanceo en las cuentas de crédito y débito del almacén; además de la realización de un seguimiento de los movimientos registrados mensualmente.

- TRASLADO DE BIENES ENTRE DEPENDENCIAS O TRASPASO

RESPONSABLE(S): PROFESIONAL UNIVERSITARIO (ALMACÉN).

Este proceso consiste en la realización de un inventario para controlar el traslado de equipos o elementos a otras dependencias.

- ADMINISTRACIÓN DE ELEMETOS DE CONSUMO

RESPONSABLE(S): PROFESIONAL UNIVERSITARIO (ALMACÉN).

Este proceso consiste en desarrollar con un control de los bienes materiales para dar un buen uso ellos.

- EVALUACION Y REEVALUACIÓN DE PROVEEDORES Y PRESTADORES DESERVICIOS

RESPONSABLE(S): DE LA CONTRATACIÓN DE BIENES Y SERVICIOS (VICERRECTORA ADMINISTRATIVA- PROFESIONAL UNIVERSITARIO (ALMACÉN) – PROFESIONAL UNIVERSITARIO (CONTRATACIÓN).

Este proceso consiste en desarrollar mecanismos de evaluación para dar control a los bienes y equipos suministrados por proveedores de servicios. .[101]
En el Anexo 1 ilustración 15 se muestra de manera gráfica los procesos que maneja la dependencia de gestión administrativa e infraestructura física (almacén) con sus respectivos responsables.

Procesos y Procedimientos de "Gestión de Talento Humano"

Dependencia: Gestión de Talento Humano

Descripción: En la dependencia de gestión de talento humano es la encargada de desarrollar programas para el fortalecimiento de los jóvenes pertenecientes a la institución por medio de electivas constituyentes a las aptitudes, valores, habilidades y destrezas de los jóvenes para fomentar un mejor desarrollo de las actividades. [102]

- PLANEACION NECESIDAD DE TALENTO HUMANO

RESPONSABLE(S): COORDINADORA GRUPO INTERNO DE TRABAJO DE TALENTO HUMANO.

Este proceso consiste en Organizar las necesidades del área administrativa y académica supliendo las vacantes temporales y definitivas a nivel institucional.

- VINCULACION DE PERSONAL SUPERNUMERARIO.

[101] ITFIP, Institución de Educación Superior. Manual de Procesos y Procedimientos "ITFIP" Versión N.º 5.0. Lugar de Publicación: Espinal-Tolima, diciembre de 2016. Pág.: 234-264 [Consultado: 19 de septiembre de 2018].
[102] ITFIP, Institución de Educación Superior. Caracterización de procesos "ITIFP". Lugar de Publicación: Espinal-Tolima, noviembre de 2015. [Consultado: 26 de septiembre de 2018]. Disponible en Internet:
http://www.itfip.edu.co/institucional/estructura-administrativa/vicerrectoria-administrativa/gestion-talento-humano.htm

RESPONSABLE(S): COORDINADOR GRUPO INTERNO DE TRABAJO DE TALENTO HUMANO.

Este proceso consiste en la vinculación del personal institucional para dar cumplimiento a los parámetros legales y procedimiento internos vigentes.

- VINCULACION DE PERSONAL DOCENTE DE PLANTA

RESPONSABLE(S): PROFESIONAL ESPECIALIZADO.

Este proceso consiste en la vinculación del personal Docente cumpliendo los parámetros legales y procedimientos internos vigentes.

- VINCULACIÓN DE PERSONAL ADMINISTRATIVO

RESPONSABLE(S): COORDINADOR GRUPO INTERNO DE TRABAJO DE TALENTO HUMANO.

Este proceso consiste en la vinculación del personal administrativo cumpliendo los parámetros legales y procedimientos internos vigentes.

- VINCULACIÓN DOCENTES HORA CÁTEDRA

RESPONSABLE(S); COORDINADOR GRUPO INTERNO DE TRABAJO DE TALENTO HUMANO.

Este proceso consiste en la vinculación del personal docente de hora de catedra cumpliendo los parámetros legales y procedimientos internos vigentes.

- PLANILLA ÚNICA DE APORTES SOI.

RESPONSABLE(S): PROFESIONAL ESPECIALIZADO
Este proceso consiste en el Desarrollo del proceso de la planilla del sol, que busca simplificar los procesos de pago de aportes en seguridad social y parafiscal; realizados desde la plataforma web.

- EXPEDICIÓN DE CERTIFICACIONES

RESPONSABLE(S): PROFESIONAL ESPECIALIZADO.

Este proceso consiste en la elaboración de certificados laborales requeridos por docente de planta, docente hora cátedra o prestación de servicios referentes a la vinculación de la entidad.

- ACTUALIZACIÓN DEL MANUAL DE FUNCIONES Y REQUISITOS.

RESPONSABLE(S): COORDINADORA GRUPO INTERNO DE TRABAJO DE TALENTO HUMANO.

Este proceso consiste en la actualización debida del manual de funciones y competencias laborales de acuerdo con las necesidades de la institución.

- REPORTE DE CESANTIAS AL FNA (FONDO NACIONAL DEL AHORRO)

RESPONSABLE(S): COORDINADOR GRUPO INTERNO DE TRABAJO DE TALENTO HUMANO.

Este proceso consiste en la realización del reporte mensual realizado por el área de financiera para efectuar el pago de las cesantías al personal administrativo y docentes de planta.

- ELABORACIÓN DE ACTOS ADMINISTRATIVOS

RESPONSABLE(S): COORDINADORA GRUPO INTERNO DE TRABAJO DE TALENTO HUMANO.

Este proceso consiste en la elaboración de actos administrativo-proyectados y con la firma del asesor jurídico y del rector**.**

- ELABORACION y EJECUCION DEL PLAN INSTITUCIONAL DE CAPACITACION (PIC)

RESPONSABLE(S): COORDINADORA GRUPO INTERNO DE TRABAJO DE TALENTO HUMANO-LIDERES DE PROYECTOS DE APRENDIZAJE.
Este proceso consiste en la elaboración de un plan de capacitación basado en las necesidades para fortalecer las competencias laborales, conocimientos, habilidades e incrementar la capacidad individual y grupal para el desempeño del cargo y al desarrollo personal.

- INDUCCION Y REINDUCCION

RESPONSABLE(S): COORDINADORA GRUPO INTERNO DE TRABAJO DE TALENTO HUMANO Y LÍDERES DE PROCESO.

Este proceso consiste en dar a conocer la normatividad interna a los nuevos funcionarios permitiéndoles conoces la institución y sus respetivas funciones que le exige el cargo para el cual ha sido vinculado.

- PLAN DE ESTIMULOS POR DESEMPEÑO LABORAL ADMINISTRATIVO

RESPONSABLE(S): COORDINADORA GRUPO INTERNO DE TRABAJO DE TALENTO HUMANO.

Este proceso consiste en Dar incentivos y estímulos al personal administrativo de la institución.

- ENCARGO EN PERSONAL DE CARRERA

RESPONSABLE(S): PROFESIONAL ESPECIALIZADO.

Este proceso consiste en Promover empleados que reúnan las condiciones necesarias para el empleo público y carrera administrativa.

- REUBICACION LABORAL

RESPONSABLE(S): PROFESIONAL ESPECIALIZADO.

Este proceso consiste en la ubicación de funcionarios a un nuevo sitio de trabajo ya sea por salud o por disposición legal o directivo.

- EXPEDICIÓN CERTIFICACIÓN BONO PENSIONAL

RESPONSABLE(S): PROFESIONAL ESPECIALIZADO**:** EN TRÁMITE O TRANSICIÓN PARA EL ÁREA DE TESORERÍA.
Este proceso consiste en un proceso de expedición de los certificados de petición del bono pensional a funcionarios vinculados que acreditan los aportes y tiempo de servicio.

- RETIRO DEL SERVICIO Y PAGO DE PRESTACIONES

RESPONSABLE(S): RECTORÍA, COORDINADOR GRUPO INTERNO DE TRABAJO DE TALENTO.

Este proceso consiste en la realización de los trámites para el retiro del funcionario del servicio cualquiera que sea su causal bajo el cumplimiento de las normas establecidas por la institución; además se efectuara el pago de las prestaciones por las que el funcionario tiene derecho.

- LIQUIDACIÓN DE NOMINAS

RESPONSABLE(S): PROFESIONAL UNIVERSITARIO.

Este proceso consiste en la realización de la liquidación correspondiente a los salarios del periodo en curso de acuerdo con las disposiciones legales.

- EVALUACIÓN DE DESEMPEÑO – PERSONAL EN CARRERA ADMINISTRATIVA Y DE LIBRE NOMBRAMIENTO Y REMOCION

RESPONSABLE(S): COORDINADOR GRUPO INTERNO DE TRABAJO DE TALENTO HUMANO.

Este proceso consiste en el desarrollo de la evaluación de desempeño al personal y a funcionarios en carrera administrativa permitiendo la visualización de funciones y logros

- EVALUACIÓN DE DESEMPEÑO PERSONAL EN PROVISIONALIDAD

RESPONSABLE(S): COORDINADOR GRUPO INTERNO DE TRABAJO DE TALENTO HUMANO.

Este proceso consiste en la evaluación del desempeño del personal en provisionalidad con el propósito de medir las funciones y competencias del personal contratado[103]

En el Anexo 1 ilustración 16 se muestra de manera gráfica los procesos que maneja la dependencia de gestión del talento humano con sus respectivos responsables.
Procesos y Procedimientos de "Gestión Del Talento Humano (Salud Ocupacional)".

Dependencia: Salud Ocupacional
Descripción: En la dependencia de salud ocupacional se encuentra dentro del proceso de grupo de talento humano, su objetivo principal es la prevención de accidentes de trabajo y enfermedades profesionales, además de contar con actividades como medicina preventiva, medicina del trabajo, higiene y seguridad industrial.[104]

- DIAGNÓSTICO DE CONDICIONES DE SALUD

RESPONSABLE(S): PROFESIONAL UNIVERSITARIO SEGURIDAD Y SALUD EN EL TRABAJO.
Este proceso consiste en Se realiza un diagnóstico de salud que indique los factores de riesgo que se encuentran expuestos los funcionarios para así tomar las respectivas medidas de prevención y control frente a las enfermedades.

[103] ITFIP, Institución de Educación Superior. Manual de Procesos y Procedimientos "ITFIP" Versión N.º 5.0. Lugar de Publicación: Espinal-Tolima, diciembre de 2016. Pág.: 265-310 [Consultado: 19 de septiembre de 2018].
[104] ITFIP, Institución de Educación Superior. Caracterización de procesos "ITIFP". Lugar de Publicación: Espinal-Tolima, noviembre de 2015. [Consultado: 26 de septiembre de 2018]. Disponible en Internet:
http://www.itfip.edu.co/institucional/estructura-administrativa/vicerrectoria-administrativa/gestion-talento-humano/salud-ocupacional

- IDENTIFICACION Y VALORACION DE FACTORES DE RIESGO

RESPONSABLE(S): PROFESIONAL UNIVERSITARIO EN SALUD OCUPACIONAL.

Este proceso consiste en desarrollar métodos para medir los riesgos que se encuentran expuestos los funcionarios, como causas o consecuencias; además del grado de peligrosidad para así dar recomendaciones para la prevención y control de estos.

- CONFORMACION DEL COPASST O EL COMITÉ PARITARIO EN SEGURIDAD Y SALUD EN EL TRABAJO

RESPONSABLE(S): PROFESIONAL UNIVERSITARIO EN SALUD OCUPACIONAL.
Este proceso consiste en la construcción de un comité de apoyo que vigile y coordine las actividades de medicina preventiva y del trabajo promocionando la salud ocupacional en todos los niveles de la institución.

- ELABORACION Y ACTUALIZACIÓN DEL REGLAMENTO DE HIGIENE Y SEGURIDAD INDUSTRIAL

RESPONSABLE(S): PROFESIONAL UNIVERSITARIO EN SST.

Este proceso consiste en la construcción y la publicación de los reglamentos de higiene y seguridad industrial de la institución**.**

- ELABORACION PROGRAMA DE LA SEGURIDAD Y SALUD EN EL TRABAJO.

RESPONSABLE(S): PROFESIONAL UNIVERSITARIO EN SST.

Este proceso consiste en la elaboración de un documento que integre los aspectos fundamentales de la administración, manejo normativo y de las actividades de Salud Ocupacional.

- PLAN DE EMERGENCIAS

RESPONSABLE(S): PROFESIONAL UNIVERSITARIO EN SST.

Este proceso consiste en Organización un plan de actividades de prevención y control de emergencias para asegurar bienes y salvaguardar vidas en caso de una prevención.[105]

En el Anexo 1 ilustración 17 se muestra de manera gráfica los procesos que maneja la dependencia de gestión del talento humano (Salud Ocupacional) con sus respectivos responsables.

Procesos y Procedimientos de "Gestión Financiera"

Dependencia: Gestión Financiera

Descripción: En la dependencia de gestión financiera es la encargada de administrar de manera eficaz, eficiente y efectiva los recursos financieros de la institución.[106]

- REVISIÓN PAGO DE DECLARACIONES TRIBUTARIAS

RESPONSABLE(S): COORDINADOR ÁREA FINANCIERA
Este proceso consiste en la revisión y verificación de los valores liquidados en la declaración tributaria sean correctos.

- REVISIÓN BOLETINES DE CAJA

RESPONSABLE(S): COORDINADOR ÁREA FINANCIERA.
Este proceso consiste en analizar y revisar los boletines de caja realizados durante el día.

- ARQUEO PERIÓDICO DE CAJA MENOR

RESPONSABLE(S): COORDINADOR ÁREA FINANCIERA – CONTROL INTERNO Y FUNCIONARIO RESPONSABLE DEL MANEJO DEL FONDO FIJO DE CAJA MENOR.

Este proceso consiste en verificar el correcto manejo de la caja menor que contribuya al normal funcionamiento de la institución.

- REVISIÓN ORDENES DE PAGO

[105] ITFIP, Institución de Educación Superior. Manual de Procesos y Procedimientos "ITFIP" Versión N.º 5.0. Lugar de Publicación: Espinal-Tolima, diciembre de 2016. Pág.: 311-323 [Consultado: 19 de septiembre de 2018].
[106] ITFIP, Institución de Educación Superior. Caracterización de procesos "ITIFP". Lugar de Publicación: Espinal-Tolima, noviembre de 2015. [Consultado: 26 de septiembre de 2018]. Disponible en Internet:
https://www.itfip.edu.co/images/2015/CARACTERIZACION-GESTION-FINANCIERA-2015.pdf

RESPONSABLE(S): COORDINADOR ÁREA FINANCIERA.

Este proceso consiste en analizar y verificar los valores cancelados que cumplan con los requisitos; además transacciones financieras deben estar registradas en las órdenes de pago correspondientes a los documentos anexados

- REVISIÓN TRASLADOS PRESUPUESTALES

RESPONSABLE(S): COORDINADOR ÁREA FINANCIERA.

Este proceso consiste en realizar un estudio para las necesidades del presupuesto para así suplir las falencias presupuestales en rubros de vital importancia para el funcionamiento de la institución.

- PROGRAMACIÓN, COORDINACIÓN DEL PAC DE RECURSOS PROPIOS.

RESPONSABLE(S): COORDINADOR ÁREA FINANCIERA.
Este proceso consiste en la distribución de recursos generados acorde con las proyecciones y necesidades mensuales de la institución.[107]
En el Anexo 1 ilustración 18 se muestra de manera gráfica los procesos que maneja la dependencia de gestión Financiera con sus respectivos responsables.

Procesos y Procedimientos de "Presupuesto"

Dependencia: Presupuesto

Descripción: En la dependencia de presupuesto es la encargada de administrar todo el presupuesto de la institución. [108]

- PROGRAMACIÓN Y DESAGREGACION DEL PRESUPUESTO

RESPONSABLE(S): COORDINADOR FINANCIERO, RECTORÍA, PLANEACIÓN Y PROFESIONAL UNIVERSITARIO DE PRESUPUESTO.

Este proceso consiste en desarrollar actividades para la degradación y programación presupuestal, asignando para la vigencia, con forme a los proyectos y necesidades de la institución.

---

[107] ITFIP, Institución de Educación Superior. Manual de Procesos y Procedimientos "ITFIP" Versión N.º 5.0. Lugar de Publicación: Espinal-Tolima, diciembre de 2016. Pág.: 324-336 [Consultado: 19 de septiembre de 2018].
[108] ITFIP, Institución de Educación Superior. Caracterización de procesos "ITIFP". Lugar de Publicación: Espinal-Tolima, noviembre de 2015. [Consultado: 26 de septiembre de 2018]. Disponible en Internet:
https://www.itfip.edu.co/images/2015/CARACTERIZACION-GESTION-ADMINISTRATIVA-2015.pdf

- EJECUCIÓN DEL PRESUPUESTO

RESPONSABLE(S): RECTOR – VICERRECTOR ADMINISTRATIVO - COORDINADOR FINANCIERO Y PROFESIONAL UNIVERSITARIO PRESUPUESTO.

Este proceso consiste en llevar a cabo una adecuada ejecución, registro y control de las apropiaciones presupuestales.

- MODIFICACIÓNES PRESUPUESTAL QUE AFECTAN EL ANEXO DEL DECRETO DE LIQUIDACION

RESPONSABLE(S): RECTOR – VICERRECTOR ADMINISTRATIVO – COORDINADOR FINANCIERO PROFESIONAL UNIVERSITARIO PRESUPUESTO.

Este proceso consiste en garantizar el cumplimiento de los recursos necesarios para el funcionamiento de la institución.

- PRESENTACIÓN DE INFORMES

RESPONSABLE(S): PROFESIONAL UNIVERSITARIO ENCARGADO PRESUPUESTO.

Este proceso consiste en ejecutar un informe de registro los recursos asignados a los entes de control.[109]

En el Anexo 1 ilustración 19 se muestra de manera gráfica los procesos que maneja la dependencia de Presupuesto con sus respectivos responsables.

Procesos y Procedimientos de "Tesorería"

Dependencia: Tesorería

Descripción: En la dependencia de tesorería es la encargada de Brinda un buen servicio y atención a los estudiantes internos y personal externos, con disponibilidad de la información confiable y actualizada.[110]

---

[109] ITFIP, Institución de Educación Superior. Manual de Procesos y Procedimientos "ITFIP" Versión N.º 5.0. Lugar de Publicación: Espinal-Tolima, diciembre de 2016. Pág.: 337-346 [Consultado: 19 de septiembre de 2018].

[110] ITFIP, Institución de Educación Superior. Caracterización de procesos "ITIFP". Lugar de Publicación: Espinal-Tolima, noviembre de 2015. [Consultado: 26 de septiembre de 2018]. Disponible en Internet: http://www.itfip.edu.co/institucional/estructura-administrativa/vicerrectoria-administrativa/gestion-financiera/tesoreria

- PAGO A BENEFICIARIO FINAL SIIF RECURSOS NACIÓN

RESPONSABLE(S): TESORERO.

Este proceso consiste en generar el pago en las fechas establecidas para los diferentes proveedores y acreedores de la institución, se deberán generar y aprobar las órdenes de pago con dos (2) días de anticipación a la fecha límite de pago.

- PAGO CON TRAPASO A PAGADURIA- SCUN SISTEMA DE CUENTA ÚNICA NACIONAL. (RECURSOS PROPIOS)

RESPONSABLE(S): TESORERO.

Como se refiere anteriormente se debe pagar con 2 días de anticipación a la fecha límite de pago de acuerdo con el flujo de efectivo y saldos de la sub-sistema de cuenta única nacional.

- APERTURA DE CUENTAS BANCARIAS Y REGISTRO SIIF

RESPONSABLE(S): TESORERO.

Este proceso consiste en realizar un control de los ingresos depositados en las cuentas que se efectúan por concepto de matrículas, convenios y demás conceptos.

- PAGO DE NÓMINAS CARGA MASIVA SIIF

RESPONSABLE(S): PROFESIONAL UNIVERSITARIO.

Este proceso consiste en efectuar la cancelación de la nómina mensual dentro de los términos fijados, (a los 25 días del mes) de acuerdo con el proceso SIIF

- ELABORACIÓN BOLETÍN DIARIO DE CAJA Y BANCOS

RESPONSABLE(S): TESORERO.

Este proceso consiste en realizar un registro diario de los movimientos contables de las cuentas bancarias y flujo de efectivo de la institución.

- PAGO PARAFISCALES.

RESPONSABLE(S): TESORERO.
Este proceso consiste en cancelar mensualmente los aportes parafiscales dentro de la fecha establecida (el tercer día hábil del mes siguiente) para la institución.

- ELABORACIÓN DE CERTIFICADOS DE INGRESOS Y RETENCIONES

RESPONSABLE(S): TESORERO.

Este proceso consiste en elaborar certificados de ingresos y retenciones de los funcionarios de planta de la institución, contratistas y proveedores.

- ELABORACIÓN DE REPORTES DE PAGO DE CONTRATISTAS, PROVEEDORES Y SERVICIOS PUBLICOS.

RESPONSABLE(S): TESORERO.

Este proceso consiste en elaborar reportes de pagos por conceptos de cancelación de servicios públicos, facturas y contratos para la entrega de información oportuna.

- PROGRAMACIÓN DEL PAC (PROGRAMACIÓN ANUAL DE CAJA).

RESPONSABLE(S): JEFE DE TESORERIA.

Este proceso consiste en verificar que los recursos sean suficientes para cubrir los pagos y obligaciones para garantizar un buen funcionamiento de la institución.

- PROGRAMACIÓN DE GIROS

RESPONSABLE(S): PROFESIONAL UNIVERSITARIO TESORERÍA.

Este proceso consiste en ejecutar los pagos de las obligaciones de forma oportuna y eficaz para los funcionarios de la institución.[111]

En el Anexo 1 ilustración 20 se muestra de manera gráfica los procesos que maneja la dependencia de Tesorería con sus respectivos responsables.

Procesos y Procedimientos de "Contabilidad"

Dependencia: Contabilidad

Descripción: La dependencia de contabilidad es la encargada de producir estados financieros razonables que revelan la situación económica social de la Institución, que sirva a las directivas para el cumplimiento de metas y objetivos propuestos, al

[111] ITFIP, Institución de Educación Superior. Manual de Procesos y Procedimientos "ITFIP" Versión N.º 5.0. Lugar de Publicación: Espinal-Tolima, diciembre de 2016. Pág.: 347-371 [Consultado: 19 de septiembre de 2018].

logro de los planes institucionales y el desarrollo social comunitario.[112]

- IDENTIFICACIÓN, CLASIFICACIÓN, MEDICIÓN, REGISTRO Y AJUSTES DE LA INFORMACIÓN CONTABLE.

RESPONSABLE(S): CONTADOR.

Es el encargado de garantizar y establecer con eficiencia la operatividad del proceso contable en procura de cumplir con funciones, las actividades, tareas, e interacciones del proceso y de esta forma lograr los mejores resultados. Con la realización de este proceso el contador espera proyectar una correcta aplicación de acuerdo con la normatividad. Régimen de Contabilidad Pública y demás normas asociadas al proceso en materia contable pública.

- ELABORACIÓN ESTIMACIONES DE PROVISIONES, DEPRECIACIONES, AMORTIZACIONES DE LA INFORMACIÓN CONTABLE.

RESPONSABLE(S): CONTADOR.

Con la elaboración de estas estimaciones el contador tiene como función calcular el valor del desgaste o pérdida de la capacidad operativa de los bienes; buscando así obtener un total y real cubrimiento de los valores determinados por las posibles contingencias de pérdida en un periodo determinado de tiempo.

- AJUSTE, RECLASIFICACIONES Y CIERRE CONTABLE

RESPONSABLE(S): CONTADOR – PROFESIONALES DE APOYO.

El contador se encarga del cierre del periodo determinado.[113]

En el Anexo 1 ilustración 21 se muestra de manera gráfica los procesos que maneja la dependencia de contabilidad con sus respectivos responsables.

Procesos y Procedimientos de "gestión de calidad y documental"

Dependencia: Gestión de calidad y documental

[112] ITFIP, Institución de Educación Superior. Caracterización de procesos "ITIFP". Lugar de Publicación: Espinal-Tolima, noviembre de 2015. [Consultado: 26 de septiembre de 2018]. Disponible en Internet: http://www.itfip.edu.co/institucional/estructura-administrativa/vicerrectoria-administrativa/gestion-financiera/contabilidad

[113] ITFIP, Institución de Educación Superior. Manual de Procesos y Procedimientos "ITFIP" Versión N.º 5.0. Lugar de Publicación: Espinal-Tolima, diciembre de 2016. Pág.: 372-389 [Consultado: 19 de septiembre de 2018].

Descripción: Dirigir y organizar la instauración sobre el mantenimiento del Sistema Integrado de Gestión en la institución bajo las obligaciones de la NTCGP 1000:2009, ISO 9001:2008 y MECI, para la mejora de la efectividad de los procesos.[114]

- ACTUALIZACIÓN Y CAMBIOS MANUAL DE PROCESOS Y PROCEDIMIENTOS.

RESPONSABLE(S): Profesional Universitario Encargado del proceso de Gestión de Calidad.

Conservar la modernización de los Manuales de Procesos y Procedimientos de la Institución con la intención de respaldar la creación precisa y eficiente de sus procesos. Como consecuente se logra obtener que los procedimientos estén al día con respecto a los mismos.

- DISEÑO DE PLANES DE SENSIBILIZACIÓN Y CAPACITACIÓN DEL SISTEMA DE GESTIÓN DE LA CALIDAD.

RESPONSABLE(S): Profesional Universitario Encargado del proceso Gestión de calidad.
Exponer las instrucciones para la modernización continua de toda la comunidad de la institución en asuntos adecuados al Sistema de Gestión de la Calidad. Por ellos los resultados que se obtienen es que por parte de la asociación establezca y permite que dicha asociación se mantenga al tanto de todo lo que se requiere hacer sobre el **Sistema** de Gestión de Calidad[115]

En el Anexo 1 ilustración 22 se muestra de manera gráfica los procesos que maneja la dependencia de gestión de calidad y documental con sus respectivos responsables.

Procesos y Procedimientos de "procedimientos obligatorios del S.G.C"

Dependencia: Procedimientos obligatorios del S.G.C

- CONTROL DE DOCUMENTOS

RESPONSABLE(S): Profesional Universitario Líder S.I.G.

---

[114] ITFIP, Institución de Educación Superior. Caracterización de procesos "ITIFP". Lugar de Publicación: Espinal-Tolima, noviembre de 2015. [Consultado: 26 de septiembre de 2018]. Disponible en Internet: https://www.itfip.edu.co/images/Institucional/ADMINISTRACIONDERIESGOSGESTIONDECALIDAD2014.pdf

[115] ITFIP, Institución de Educación Superior. Manual de Procesos y Procedimientos "ITFIP" Versión N.º 5.0. Lugar de Publicación: Espinal-Tolima, diciembre de 2016. Pág.: 390-401 [Consultado: 19 de septiembre de 2018].

En el control de documentos el profesional Universitario Líder S.I.G. busca determinar cuáles son los lineamentos que se deben emplear para la elaboración, revisión, aprobación, distribución y modificación de los documentos que conforman el S.I.G de la Institución, así mismo la distribución y revisión de la documentación externa. Una vez realizado este proceso se espera que el profesional pueda contar con documentos actualizados y conservados de acuerdo con el tipo de documento (copia controlada, copia no controlada, copias obsoletas).

- CONTROL DE REGISTROS

RESPONSABLE(S): Profesional Universitario Líder S.I.G.
Instaurar las diferentes funciones de acumulación y comprobación sobre los diferentes métodos de recuperación y la distribución de los registros los cuales son soportados en diferentes procedimientos. Como resultado primario se obtienen las principales anotaciones de como poder evidenciar la eficacia del Sistema Integrado de Gestión en la Institución.

- AUDITORIAS INTERNAS INTEGRALES

RESPONSABLE(S): ASESOR DE CONTROL INTERNO – AUDITOR LÍDER.

Con las auditorías internas integrales se busca generar acciones que permitan estimular el mejoramiento continuo dentro de la gestión institucional. Para lograr alcanzar este mejoramiento el asesor de control interno- auditor líder debe planificar, desarrollar, mantener y realizar un programa de auditorías Integrales para evaluar la efectividad del sistema de Control Interno en el cumplimiento de los objetivos institucionales, por medio del monitoreo, valoración y verificación objetiva e independiente y que estos se desarrollen conforme a los lineamientos legales, constitucionales, institucionales y las normas de calidad aplicables.

- REVISIÓN POR LA DIRECCIÓN AL SISTEMA INTEGRADO DE GESTIÓN.

RESPONSABLE(S): RECTOR.

Se logra constituir diferentes técnicas a través de la eficacia que permite dar como efectividad el sistema de gestión de la calidad la cual se va aplicando dentro de la institución y poder hacer una retroalimentación de sus falencias y poder corregirlas en un futuro.

- CONTROL DE PRODUCTO Y/O SERVICIO NO CONFORME

RESPONSABLE(S): LÍDER PROCESO MISIONAL.

El líder de este proceso es encargado del control del producto o servicio no conforme; como objetivo principal de control su función consiste en realizar el seguimiento al producto o servicio no conforme de la institución, para prevenir su uso o entrega no intencional.

- ACCIONES PREVENTIVAS

RESPONSABLE(S): TODOS LOS FUNCIONARIOS.

El objetivo principal de las acciones preventivas consiste en dictaminar un procedimiento a realizar y estipular una metodología que permita detectar, analizar y eliminar las causas de No Conformidades potenciales, con el fin de promover el Mejoramiento continuo.

- ACCIONES CORRECTIVAS

RESPONSABLE(S): TODOS LOS FUNCIONARIOS.

Se tiene como un principal objetivo el poder decretar una metodología que ayude al alcance de diferentes métodos de no conformidad frente a las acciones de agudeza En la institución tratando de asegurar hacia un futuro un mejor la sistematización de esta.[116]

En el Anexo 1 ilustración 23 se muestra de manera gráfica los procesos que maneja la dependencia de procedimientos obligatorios del S.G.C con sus respectivos responsables.

12.2.3. Procesos del departamento de sistemas

Dependencia: Sistemas.

Descripción: En esta dependencia se lleva a cabalidad todos los procesos informáticos internos con los cuales cuenta la institución, siendo esta una de las más importantes en cuestión de funcionalidad y sostenibilidad de esta.

- SISTEMATIZACIÓN DE PROCESOS

RESPONSABLE: Coordinador de sistemas.

El ingeniero estará dispuesto a participar en la formulación, diseño y administración de planes, programas y proyectos que tengan correlación en la institución; además,

[116] ITFIP, Institución de Educación Superior. Manual de Procesos y Procedimientos “ITFIP” Versión N.º 5.0. Lugar de Publicación: Espinal-Tolima, diciembre de 2016. Pág.: 402-432 [Consultado: 19 de septiembre de 2018].

Implementación, mantenimiento y soporte de sistemas de gestión de contenidos (CMS) multipropósito orientados a los website.

- APOYO DE SISTEMAS A LA INSTITUCIÓN

RESPONSABLE: Coordinador de sistemas.

Apoyar las acciones que deban implementarse en pro a alcanzar cada uno de los objetivos/metas establecidas para el mejoramiento.

- PRESENTACIÓN DE ACTIVIDADES

RESPONSABLE: Coordinador de sistemas.

Presentar informes sobre las actividades desarrolladas dentro del plan establecido por el proceso de proyección social.

- MEJORAMIENTO DEL ESTADO DE LA INSTITUCIÓN

RESPONSABLE: Coordinador de sistemas.
Proponer e implementar los procedimientos e instrumentos requeridos para mejorar la presentación de los servicios a la comunidad.

En el Anexo 1 ilustración 24 se muestra de manera gráfica los procesos que maneja la dependencia de sistemas.

- APOYO A LA SISTEMATIZACIÓN DE LOS PLANES CON ENFOQUE SOCIAL

RESPONSABLE: Coordinador de sistemas

Contribuir en el diseño del modelo y estadísticas en la aplicación del sistema de información de la institución que tengan relación con las funciones inherentes al proceso de proyección social, Participar en la preparación, seguimiento y evaluación de plan de acción institucional y de manera específica.

- DOCUMENTACIÓN DE SISTEMA DE LOS PLANES CON ENFOQUE SOCIAL

RESPONSABLE: Coordinador de sistemas.

Participar en la elaboración y actualización del manual del proceso y procedimientos de proyección social.

- GENERACIÓN DE REPORTES INFORMÁTICOS

RESPONSABLE: Coordinador de sistemas.

Sistematizar los cursos de educación académica y remisión de reporte de listados de personal participante a registro y control académico.

- MANEJO DE CONTRATACIÓN Y NECESIDADES

RESPONSABLE: Coordinador de sistemas.

Coordinar la recepción y trámite de convocatorias de entidades gubernamentales o privadas e ideas conforme a las áreas y requerimientos de acuerdo con las líneas de investigación, experticia en el ramo y oportunidades del mercado.

En el Anexo 1 ilustración 25 se muestra de manera gráfica los procesos que maneja la dependencia de sistemas.

- MANEJO DE ACTIVIDADES ACADÉMICOS

RESPONSABLE: Coordinador de sistemas.

Coordinar todas las actividades pendientes a la extensión de los programas académicos que se le encargue por la alta dirección del área académica o misional.

- INFORMES DEL PORTAFOLIO DE EVIDENCIAS

RESPONSABLE: Coordinador de sistemas.

Cumplir las directrices en materias de portafolio de evidencias dentro del proceso de evaluación del desempeño.

- INFORME DE PERFILES ACADÉMICAS

RESPONSABLE: Coordinador de sistemas.

Rendir todos los informes que demanden el proceso y acordes con su perfil en funciones académicas.

- PROCESOS DE EMERGENCIA

RESPONSABLE: Coordinador de sistemas.

Las demás que se le asignen y correspondan a la naturaleza. Mantenimiento y soporte de hardware, software y redes de datos; asistencia técnica a los sistemas informáticos de la institución y de terceros que use la institución.

En el Anexo 1 ilustración 26 se muestra de manera gráfica los procesos que maneja la dependencia de sistemas.

- MANTENIMIENTO AL SISTEMA

RESPONSABLE: Programador catedrático.

Mantenimiento y soporte a los sistemas informáticos para Registro y Control Académico de la institución.

- MANTENIMIENTO AL SISTEMA ACADÉMICO

RESPONSABLE: Programador catedrático.

Implantación, mantenimiento y soporte de sistemas institucionales para el manejo de contenidos educativos para entornos de aprendizaje virtual.

- MANTENIMIENTO TIC'S

RESPONSABLE: Programador catedrático.

Mantenimiento y soporte a la infraestructura TIC de la institución.

- SOPORTE A LOS CANALES DE COMUNICACIÓN

RESPONSABLE: Programador catedrático.
Operación y soporte de canales de comunicación con los ciudadanos vía chat, redes sociales y correo electrónico.

En el Anexo 1 ilustración 27 se muestra de manera gráfica los procesos que maneja la dependencia de sistemas.

- SOPORTE A SISTEMAS EXTERNOS

RESPONSABLE: Programador catedrático.

Soporte a sistemas de los entes gubernamentales y de terceros que el ITFIP utilice (SNIES, SPADIES, SIIF Nación, SUIT, SIIGO, etc.).

- INSTALACIÓN DE SERVICIOS INFORMÁTICOS

RESPONSABLE: Programador catedrático.

Implantación y soporte de servicios y herramientas en la nube para el trabajo colaborativo (correos, mensajería instantánea, Group office, etc.).

- ANALISTA DE CONTENIDO

RESPONSABLE: Programador catedrático.
Tratamiento de imágenes para publicación de contenidos de información institucional.

- MANEJO DE CONTENIDO VISUALES

RESPONSABLE: Programador catedrático.

Administración y soporte para los sistemas de distribución de contenidos visuales bajo demanda.

En el Anexo 1 ilustración 28 se muestra de manera gráfica los procesos que maneja la dependencia de sistemas.

- MANEJO DE CENTROS DE PARA LA GESTIÓN DE DATOS

RESPONSABLE: Programador catedrático.

Diseño, implementación, implantación y gestión de centros de datos de alta disponibilidad.

- MANEJO DE BASE DE DATOS

RESPONSABLE: Programador catedrático.

Creación, implementación, implantación, administración y soporte a las bases de datos institucionales.

- MANEJO DE PROYECTOS EDUCATIVOS Y TECNOLÓGICOS

RESPONSABLE: Programador catedrático.

Planeación, ejecución, control y evaluación de proyectos y presupuestos en tecnologías de la información y las comunicaciones con miras mejoramiento continuo.

- MANEJO DE SISTEMAS DE MANTENIMIENTO A LA INSTITUCIÓN

RESPONSABLE: Programador catedrático

Planeación, ejecución, control y evaluación de programas de mantenimiento, soporte y asistencia a los sistemas informáticos de la institución.

En el Anexo 1 ilustración 29 se muestra de manera gráfica los procesos que maneja la dependencia de sistemas.

- MANEJO DE REDES CONVERGENTES

RESPONSABLE: Programador catedrático.

Planeación, implementación, administración y soporte de redes convergentes institucionales.

- ADMINISTRACIÓN DE LOS RECURSOS TIC DE LA INSTITUCIÓN

RESPONSABLE: Programador catedrático.

Planeación, gestión, control, verificación y administración de recursos TIC en la institución.

- ELABORACIÓN DE INFORMES SOBRE LOS RECURSOS DE LAS TIC

RESPONSABLE: Programador catedrático.

Rendir informes sobre las actividades realizadas en materia de la administración y ejecución de tareas relacionadas con el uso y beneficios de los recursos TIC de la institución.

- DESARROLLO DE NUEVOS SISTEMAS INFORMÁTICOS

RESPONSABLE: Programador catedrático

Desarrollo y puesta en operación de nuevos sistemas informáticos para la institución.

En el Anexo 1 ilustración 30 se muestra de manera gráfica los procesos que maneja la dependencia de sistemas.

- DESARROLLO DE ESTRATEGIAS PARA PLANES GUBERNAMENTALES

RESPONSABLE: Programador catedrático.

Formulación de políticas, estrategia y planes operativos para la administración y gestión de las buenas prácticas de gobierno en línea, sistemas de gestión de la seguridad de la información y la administración y gestión de tecnologías de la información y las comunicaciones.

- ASISTENCIA EN LA CAPACITACIÓN DE LOS FUNCIONARIOS EN HERRAMIENTAS TIC

RESPONSABLE: Programador catedrático.

Colaborar en la planeación y ejecución de programas de capacitación para los funcionarios de la institución en lo relacionado al uso y aprovechamiento de los recursos TIC con que cuenta la institución.

En el Anexo 1 ilustración 31 se muestra de manera gráfica los procesos que maneja la dependencia de sistemas.

- ASISTENCIA

RESPONSABLE: Programador catedrático.

Cumplir las demás funciones que le sean asignadas, de acuerdo con la naturaleza de su cargo.

- MANEJO DE SERVIDORES, EQUIPOS, REDES Y DEMAS

RESPONSABLE: Soporte técnico.
Mantenimiento de computadores, manejo, asistencia y mantenimiento del sistema operativo Linux Debían 8.0 o superior, Microsoft Windows 8 y 10 o superior, SIIGO Server, Terminal Server, Print and Documents Services, Printer Management, Fortigate, Routing y Switching.

- MANTENIMIENTO Y SOPORTE AUXILIAR

RESPONSABLE: Ingeniero Auxiliar.

El portal web es la página en donde se expone toda la información concerniente de la institución, mantenimiento, gestión y soporte al SUIT; mantenimiento y soporte al diseño implementado RYCA; Mantenimiento de los sistemas de información institucionales en lo referente a la accesibilidad y usabilidad; mantenimiento y gestión de la información manejada en software de ayudas en línea.

En el Anexo 1 ilustración 32 se muestra de manera gráfica los procesos que maneja la dependencia de sistemas.

ANÁLISIS Y RESULTADOS

13. ESTADO ACTUAL DEL SISTEMA DE INFORMACION CON RESPECTO ISO/IEC 270001:2013 EN EL DEPARTAMENTO DE SISTEMAS DEL ITFIP

En esta sección estará ligada a la metodología MAGERIT, la cual fue expuesta en el capítulo anterior, seguido de la utilización de la norma ISO 27001:2013. Adicional a esto, se llevó a cabo el cumplimiento de cuatro (4) objetivos específicos.

Como primera medida para desarrollar el diseño del sistema de gestión de seguridad de la información (SGSI) basado en la ISO/IEC 27001:2013, se realiza un análisis que permite evaluar el contexto de la organización, liderazgo, planificación, soporte, operación, seguridad, evaluación de desempeño y mejoras, los cuales se convierten en elementos esenciales para actuar según la norma.

La evaluación permite establecer el nivel de cumplimiento de la norma por parte del departamento de sistemas de la Institución de Educación Superior - ITFIP. Por lo tanto, las respuestas posibles para este cuestionario aplicado son: No cumple (NC), Cumple Parcialmente (CP), Cumple Satisfactoriamente (CS). De acuerdo con la información que se presenta en la siguiente tabla:

Tabla 9. Parámetros de evaluación

Sigla	Estado de Evaluación	Descripción
NC	NO CUMPLE	No existe y/o no se está haciendo
CP	CUMPLE PARCIALMENTE	Lo que la norma (ISO/IEC 27001 versión 2013) requiere se está haciendo de manera parcial, se está aplicando diferente, no está documentado, se definió y aprobó, pero no se gestiona.
CS	CUMPLE SATISFACTORIAMENTE	Existe, es gestionado y aplicado, se está cumpliendo con lo que la norma ISO/IEC 27001 versión 2013 solicita, está documentado, es conocido y aplicado por todos los involucrados en el SGSI se cumple al 100%.

Fuente: Autoría Propia.

13.1. Cuestionario. A continuación, se presenta el cuestionario aplicado en el departamento de sistemas de la Institución de Educación Superior - ITFIP, dirigida al Ing. Wilson Mauricio Pimiento Cárdenas, Coordinador de Sistemas. Con el cuestionario se evalúan 105 ítems que hacen referencia a los siguientes dominios:

- A5. Políticas de seguridad de la Información.
- A6. Organización de la Seguridad de la Información.
- A7. Seguridad de los Recursos Humanos (RRHH).
- A8. Gestión de activos.
- A9. Control de acceso.
- A10. Criptografía.
- A11. Seguridad física y del entorno.
- A12. Seguridad en las operaciones.
- A13. Seguridad de las comunicaciones.
- A14. Adquisición, desarrollo y mantenimiento de sistemas.
- A15. Relación con proveedores.
- A16. Gestión de los incidentes de seguridad de la información.
- A17. Aspectos de seguridad de la información de la gestión de continuidad de negocio.
- A18. Cumplimiento.

Para visualizar todo el cuestionario, con sus respectivas respuestas puede dirigirse al Anexo 1 desde la tabla 1 a la tabla 16 y también referirse desde el Gráfico 1 al Gráfico 15.

13.1.1. Resultados del cuestionario.

Tabla 10. Resumen resultados de la evaluación

	Dominio	CS	CP	NC	Ítems Evaluados
A5	Políticas de seguridad de la información: En este dominio se busca que la dirección brinde orientación y soporte para la seguridad de la información de acuerdo	2	2	2	6

Tabla 6. Resumen resultados de la evaluación (Continuación)

	con los requisitos del negocio y con las leyes y reglamentos pertinentes.				
A6	Organización de la seguridad de la información: En este dominio se busca establecer un marco de referencia de gestión para iniciar y controlar la implementación y operación de la seguridad de la información dentro de la organización.	4	2	2	8
A7	Seguridad de los recursos humanos (RRHH): En este dominio se busca garantizar de que los empleados y contratistas comprendan sus responsabilidades y que sean idóneos en los roles para los que se consideran.	5	2	2	9
A8	Gestión de activos: En este dominio se busca identificar los activos organizacionales y definir las responsabilidades de protección adecuadas, asegurando que la información se proteja de la manera correcta de acuerdo con su importancia para la organización.	1	3	2	6
A9	Control de accesos: En este dominio se busca que en la organización se limite el acceso a información y a instalaciones de procesamiento de información, vigilando que el acceso sea solamente para los usuarios autorizados y evitando el acceso no autorizado a sistemas y servicios.	12	5	1	18
A10	Criptografía: En este dominio se busca asegurar el uso apropiado y eficaz de técnicas criptográficas para proteger la confidencialidad, autenticidad y/o la integridad de la información.	3	0	0	3
A11	Seguridad física y del entorno: Para este nivel, se evalúa el estado de las diferentes instancias que podrían llegar a afectar la integridad de la información, esto por medio de déficit físico y ambiental.	2	6	2	10
A12	Seguridad de las operaciones: En este recurso, la seguridad de las operaciones	6	3	2	11

Tabla 6. Resumen resultados de la evaluación (Continuación)

	juega un papel demasiado importante, puesto que permite idear de manera correcta cada uno de los componentes que interactúan en él.				
A13	Seguridad de las comunicaciones: La información se maneja a través de unos canales de comunicación, por actores que influyen en la toma de decisiones acerca del destino que debe o tomar la información. Todo ello conlleva a la necesidad de crear una seguridad en cada uno de los componentes de trazabilidad y confiabilidad de esta.	3	1	1	5
A14	Adquisición, desarrollo y mantenimiento de sistemas: La adquisición, elaboración y mantenimiento de cualquiera de los servicios o archivos planos manejados en cualquier ámbito laboral son de suma importancia, por ende, la seguridad de esta debe ser totalmente confidencial; en casos como el uso de operarios externos la firma de contratos de confidencialidad es totalmente necesaria de implementar.	9	0	0	9
A15	Relación con los proveedores: La relación con los proveedores en la seguridad de la información del sistema, en las empresas permite librar cierta responsabilidad, permitiéndoles enfocar su tiempo en otras labores.	3	1	0	4
A16	Gestión de incidentes de seguridad de la información: La gestión de incidentes en la seguridad hace referencia a los probables problemas que puedan ocurrir entorno a la disponibilidad e integridad de los datos y/o sistemas manejados.	1	5	0	6
A17	Aspectos de seguridad de la información de la gestión de continuidad del negocio: En este entorno, se es totalmente requerido la elaboración de cada una de las fases, tales como planeación, diseño, estructuración, implementación, entre otros. Esto se hace con el fin de poder	4	1	0	5

Tabla 6. Resumen resultados de la evaluación (Continuación)

	activar cada una de las funciones vitales dentro de la compañía para su uso.				
A18	Cumplimiento: Dar cumplimiento con los aspectos legales, sus estatutos y cada uno de los factores que influyen en él, es el objetivo del dominio A18, en donde se busca efectuar la operación, el diseño y el uso de las normas.	2	3	0	5
	Suma Total	**57**	**34**	**14**	**105**

Fuente: Autoría Propia.

CAPITULO 2. ANÁLISIS DE RIESGOS

14. EFECTUAR UN ANÁLISIS DE RIESGO EMPLEANDO LA METODOLOGÍA MAGERIT

Para la realización del objetivo numero dos (2), el cual consiste en efectuar un análisis de riesgo empleando la metodología MAGERIT. Con el propósito de determinar y valorar los riesgos, amenazas y vulnerabilidades de cada uno de los activos que allí se encuentran, a su vez, determinar y clasificar cada uno de ellos de acuerdo con su jerarquía, codificación, descripción y demás valores que se apreciaran en el desarrollo de este.

14.1. Inventarios de activos. Para efectuar la gestión de riesgo se debe empezar por conocer el inventario de activos de la entidad, es la base dar inicio al análisis de riesgos, los activos son los recursos que hacen parte del sistema de información y que de esta manera son susceptibles a amenazas de toda índole. En el anexo 1 tabla 17 se evidencia los activos que se encontraron.

14.2. Clasificación de los activos. En este apartado se procederá a realizar el análisis de Riesgo, como primera instancia y de acuerdo a la recolección de la información, se obtuvieron los activos de la dependencia de Sistemas de la Institución de Educación Superior ITFIP para así realizar la clasificación de los mismos en base a la metodología MAGERIT, en donde se describirá cada uno de ellos de acuerdo a su jerarquía, de la forma como la metodología lo tipifica, después de ello se efectuará la valoración de cada activo, la clasificación de los Riesgos de donde se obtendrá la información necesaria para desarrollar la tabla de la estimación del impacto y de la probabilidad.

En el anexo 1, se efectuará lo descrito anteriormente con la tabla 18 junto su respectiva clasificación.

14.3. Valoración de los activos según su importancia. En la organización como tal, los factores que hay que tener en cuenta es la de la valoración con respecto a la importancia de cada activo, para demostrar lo mencionado, en el anexo 1 tabla 19 se creó la tabla con las siguientes especificaciones.

En esta tabla es posible apreciar 7 columnas independientes que corresponden a:

- El código de grupo de activo MAGERIT (código único que se le asigna a cada grupo de activos según su clasificación).
- Nombre del grupo de activo MAGERIT (nombre correspondiente al código que se le asigna a cada grupo de activos según su clasificación).
- Nombre del activo (corresponde al nombre del activo para su clasificación según MAGERIT).
- Descripción (breve explicación sobre que es el activo).

- Código consecutivo ITFIP (código único que es asignado a cada activo dentro de la dependencia).
- Nombre del activo ITFIP (nombre con el que se identifica el activo dentro de la dependencia).
- Función (breve explicación de lo que realiza el activo dentro de la dependencia).
- Valoración (corresponde a un valor numérico dado por los funcionarios de la dependencia a cada activo para así demostrar la importancia que este tiene para ellos).

NOTA: El nivel de importancia para la valoración realizada a cada activo es de 0 a 100; donde 0 es poco importante y 100 es muy importante o indispensable.

14.4. Análisis de la jerarquía de los activos entre sus grupos internos. En el anexo 1 tabla 20, se mostrará de manera cuantificada la jerarquía que representa cada uno de los activos según sus grupos, para dicho acto, se tuvo en cuenta la información recolectada a lo largo de la investigación, como también se hizo uso del conocimiento adquirido de la misma; Esto se puede apreciar en el anexo 1 tabla 20.

15. ESTIMACIÓN DE LOS VALORES DE CRITERIO EN SUS DIMENSIONES DE APLICABILIDAD

La estación de los valores de criterio nos permitirá enfocar de mejor manera la manera en la que cada uno de los activos se comporta, como también es posible realizar un estudio de manera cualitativa/cuantitativa, de la misma.

A continuación, se muestra los criterios con el que se va a valorar las dimensiones afectadas por los activos:

Tabla 11. Criterios de valoración

Valor		Criterio
10	Extremo	Daño extremadamente grave
9	Muy alto	Daño muy grave
6-8	Alto	Daño grave

Tabla 7. Criterios de valoración (Continuación)

3-5	Medio	Daño importante
1-2	Bajo	Daño menor
0	Despreciable	Irrelevantes a efectos prácticos

Fuente: Libro II MAGERIT -versión 3.0.

En el anexo 2 tabla 1, se puede evidenciar los criterios de valoración de acuerdo a MAGERIT[117], según esta metodología hace referencia a dos tipos de criterio cuantitativa se refiere al costo de la materialización de la amenaza y responde a parámetros subjetivos, de acuerdo a la recomendaciones del libro II se realizara la evaluación con el criterio cualitativa, la cual va ser respondida por el área encargado o las personas que se relacionan con el sistema, por lo tanto, va a manejar criterios personales para determinar en una escala el valor del impacto.

En el anexo 2 tabla 1, se muestra las tablas con la valoración según la clasificación de activos:

En esta tabla es posible apreciar 10 columnas independientes que corresponden a:

- El código de grupo de activo MAGERIT (código único que se le asigna a cada grupo de activos según su clasificación).
- Nombre del grupo de activo MAGERIT (nombre correspondiente al código que se le asigna a cada grupo de activos según su clasificación).

[117] MAGERIT V3, Libro 3: Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información.

- Nombre del activo (corresponde al nombre del activo para su clasificación según MAGERIT).
- Código consecutivo ITFIP (código único que es asignado a cada activo dentro de la dependencia).
- Nombre del activo ITFIP (nombre con el que se identifica el activo dentro de la dependencia).

Criterios de valoración (corresponde a 5 columnas identificadas como: confidencialidad, integridad, autenticidad, disponibilidad y trazabilidad en donde será posible visualizar un valor numérico dado por los funcionarios de la dependencia a cada activo para así demostrar la importancia y prioridad que un activo tiene en cada criterio de valoración).

16. ESTIMACIÓN DE LAS AMENAZAS QUE PUEDEN AFECTAR LOS ACTIVOS.

Las amenazas son todos aquellos factores externos de que alguna manera puede causar daños en los activos informáticos o también hace referencia a personas que aprovechan las vulnerabilidades de seguridad existentes para cometer ataques a los sistemas o a los activos informáticos.

En el catálogo 2 de la metodología MAGERIT se detalla los factores externos de amenaza y la clasificación de estos, por eso es importante antes de hacer el ejercicio, leer esta clasificación y revisar las dimensiones de valoración y escalas de valoración de las amenazas.

La evaluación de amenazas se realiza basado en la frecuencia de materialización de la amenaza en cada uno de los activos informáticos existentes, la valoración del impacto en cada una de las dimensiones de seguridad según MAGERIT. Es importante recordar que la valoración dependerá de las dimensiones afectadas que está descrito en el segundo libro de MAGERIT, y la valoración está en relación con la degradación que puede sufrir cada uno de los activos en cada dimensión de seguridad. La escala está dada por un rango porcentual de impactos en los activos.

Tabla 12. Escala de rango de frecuencia de amenazas.

Vulnerabilidad	Rango	Valor
Frecuencia muy alta	1 vez al día	100
Frecuencia alta	1 vez cada semana	70
Frecuencia media	1 vez cada 2 meses	50
Frecuencia baja	1 vez cada 6 meses	10
Frecuencia muy baja	1vez al año	5

Fuente: Autoría Propia.

Tabla 13. Dimensiones de seguridad según MAGERIT, además de la escala de rango porcentual de impactos en los activos para cada dimensión de seguridad.

Dimensiones de Seguridad	Identificación	Impacto	Valor cuantitativo
Autenticidad	A	Muy alto	100%
Confiabilidad	C	Alto	75%
Integridad	I	Medio	50%
Disponibilidad	D	Bajo	20%
Trazabilidad	T	Muy bajo	5%

Fuente: Autoría Propia.

En el anexo 2 tabla 2, se muestra la clasificación de las amenazas que se identifican en MAGERIT, éstas se establecen para cada activo determinando su probabilidad o frecuencia de ocurrencia y el impacto que tiene en cada una de las dimensiones de seguridad.

En esta tabla es posible apreciar 9 columnas independientes que corresponden a:

- ID (código único que se le asigna a cada grupo de amenazas según su clasificación en MAGERIT).
- Amenaza (nombre correspondiente al código que se le asigna a cada grupo de amenazas según su clasificación en MAGERIT).
- Activo (corresponde al nombre del activo para su clasificación según MAGERIT junto con su código de grupo MAGERIT).
- Frecuencia (corresponde al valor numérico otorgado por cada funcionario de la dependencia, este hace referencia a la frecuencia con que la amenaza puede ocurrirle al activo).

Criterios de valoración (corresponde a 5 columnas identificadas como: confidencialidad, integridad, autenticidad, disponibilidad y trazabilidad en donde será posible visualizar un valor numérico dado por los funcionarios de la dependencia a cada activo para así demostrar la importancia y prioridad que un activo tiene en cada criterio de valoración).

17. IDENTIFICACIÓN DE VULNERABILIDADES DE LOS ACTIVOS DE INFORMACIÓN ANTE LAS AMENAZAS POTENCIALES

Esta identificación de vulnerabilidades se halló al momento de visitar las instalaciones en donde se realizó una inspección visual de los activos de información, entrevistas con los administradores, revisión del estado de los equipos y análisis de las vulnerabilidades.

17.1. INSPECCIÓN VISUAL DE LOS ACTIVOS DE INFORMACIÓN

En la inspección visual se tomaron imágenes de 4 puntos de instalaciones en el ITFIP, en donde un punto principal se encuentra en el tercer piso, otros dos puntos en el segundo piso y el último punto en el primer piso.

DataCenter Tercer Piso

En las imágenes se observan el sensor biométrico, la entrada al *DataCenter*, los equipos que manejan y sus respectivas instalaciones.

Ilustración 1. Sensor biométrico con clave de la entrada del *DataCenter* tercer piso

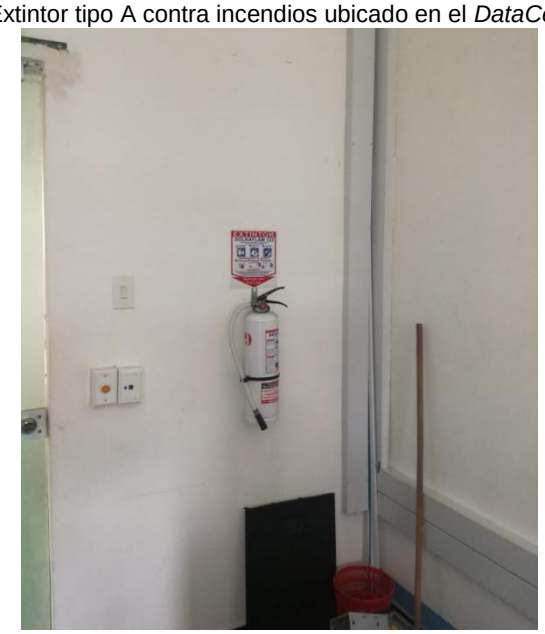
Fuente: Autoría propia

Ilustración 2. Puerta de entrada al *DataCente*r tercer piso

Fuente: Autoría propia

Como se observa el *DataCenter* cuenta con un control de acceso a personas autorizadas por medio de sensor biométrico y clave el cual solo tienen acceso los administradores, la puerta de vidrio de la entrada cuenta con dos cerraduras a llave una en medio y la en la parte inferior izquierda, las cuales en caso tal de que el sensor biométrico no funcione pueden acceder allí por medio de las llaves.

Ilustración 3. Extintor tipo A contra incendios ubicado en el *DataCenter* tercer piso

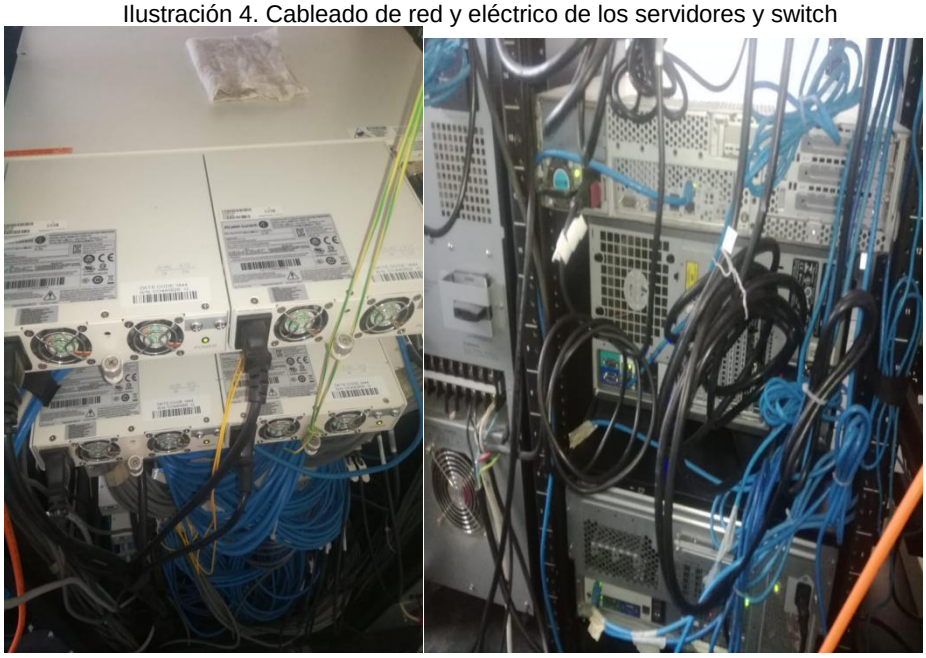


Fuente: Autoría propia.

Se observa que el *DataCenter* cuenta con un extintor tipo A contra incendios, el cual se encuentra ubicado a simple vista en caso de alguna emergencia, también se

visualiza el botón de abrir la cerradura, ya que al momento de cerrar la puerta automáticamente se bloquea para que ningún otro usuario pueda ingresar y el administrador que se encuentre adentro pueda salir.

Ilustración 4. Cableado de red y eléctrico de los servidores y switch



Fuente: Autoría propia.

Como se observa el estado actual del cableado de datos y cableado eléctrico en el *DataCenter* son muy desordenados, debido a que no se utilizan paneles de obturación para el cableado en la sala de servidores.

No se encontró sistema de marquillas en los cables de datos y cables de energía.

Los cables de datos se encuentran enredados con los cables de energía siendo esto uno de los generadores de ruido en el cableado de datos.

Se evidencia claramente que en la sala de servidores no se realiza una limpieza periódica en cuanto a contaminación por polvo y/o suciedad, que podría causar averías de origen físico o lógico en los servidores, switch, UPS y demás.

Ilustración 5. Sistema de refrigeración del *DataCenter* tercer piso

Fuente: Autoría propia

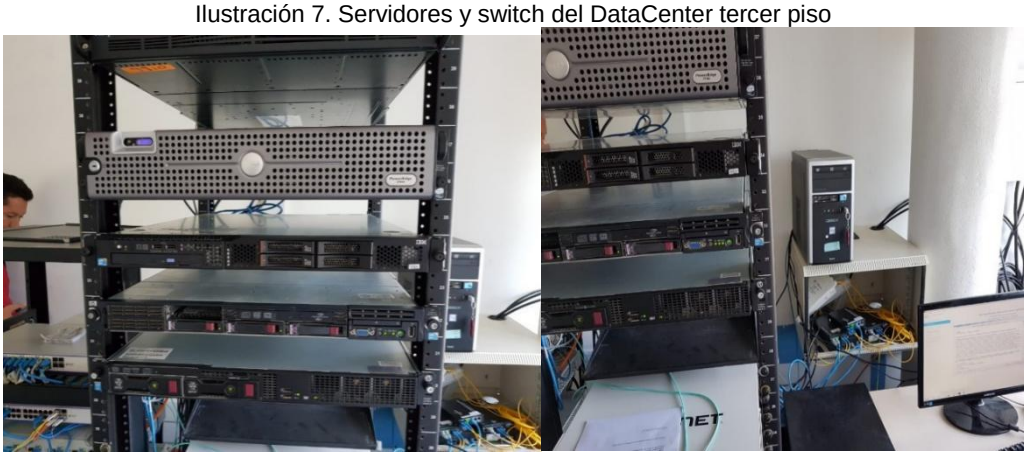
En el *DataCenter* se cuenta con un sistema de refrigeración por aire acondicionado en donde uno está funcionando correctamente y el otro se encuentra fuera de servicio.

Ilustración 6. Canaletas para el cableado de red y eléctrico de las instalaciones del *DataCenter*

Fuente: Autoría propia

El *DataCenter* cuenta con canaletas para las conexiones eléctricas y los puertos de red que se encuentran en buen estado, pero no se manejan canaletas para el cableado entre servidores y switch.

Ilustración 7. Servidores y switch del DataCenter tercer piso



Fuente: Autoría propia.

Se observa que los servidores y switch se encuentra asegurados a los soportes, pero no están protegidos contra el polvo.

DataCenter segundo piso

En las imágenes se observan las instalaciones, el cableado y los equipos que se utilizan en los dos puntos ubicados en el segundo piso.

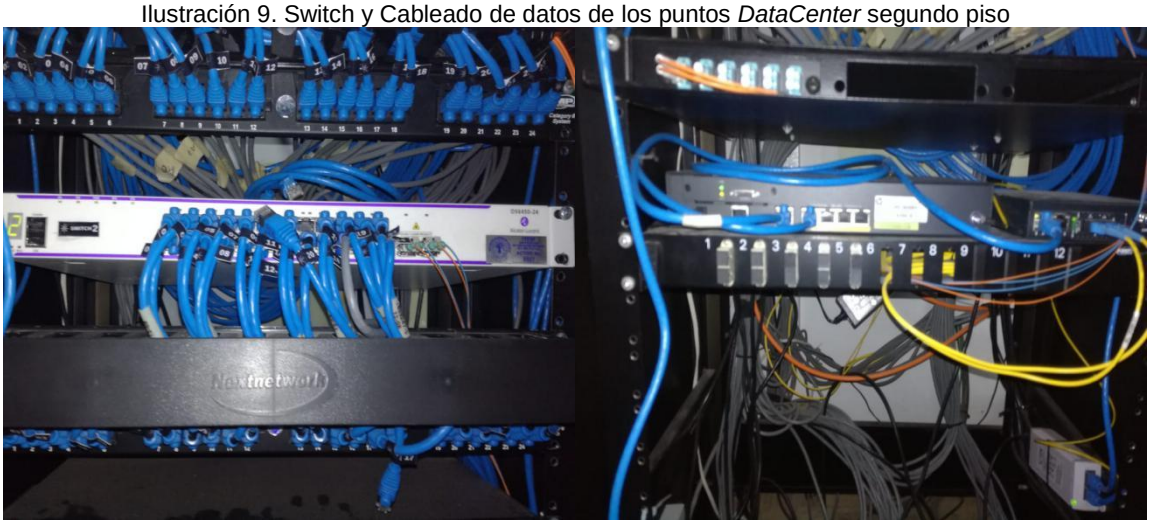
Ilustración 8. Entradas a los puntos DataCenter segundo piso

Fuente: Autoría propia.

Como se observa las entradas a los puntos *DataCenter* no cuenta con una cámara de vigilancia.

El control de acceso al *DataCenter* en las puertas no dispone de un sistema biométrico o de seguridad, sino con una cerradura de llave que no permite identificar al personal autorizado para ingresar al sitio.

Ilustración 9. Switch y Cableado de datos de los puntos *DataCenter* segundo piso



Fuente: Autoría propia.

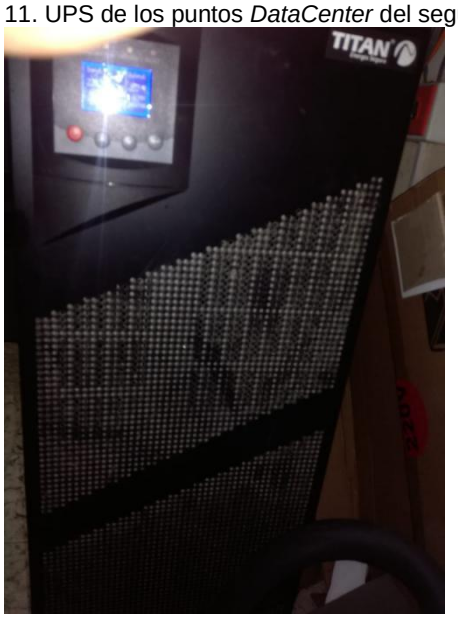
Como se observa se sigue presentado el desorden de cableado de datos y eléctricos, además de que el espacio entre cada equipo es muy limitado para que fluya el aire. También se visualiza mucho polvo en los equipos y UPS.

Ilustración 10. Extintor tipo A contra incendios ubicados en los puntos *DataCenter* del segundo piso

Fuente: Autoría propia

Se observa que los puntos también cuentan con extintores tipo A contra incendios, pero no se visualizan correctamente y además no tienen la señalización debida.

Ilustración 11. UPS de los puntos *DataCenter* del segundo piso



Fuente: Autoría propia

Se observa que los equipos de respaldo eléctrico (UPS), se encuentran con muchísimo polvo y además con cajas a sus alrededores obstaculizando el flujo del aire.

Ilustración 12. Sistema de refrigeración dentro de los puntos *DataCente*r del segundo piso

Fuente: Autoría propia

Se observa que los equipos se encuentran refrigerados por aires acondicionados funcionando en óptimas condiciones.

DataCenter Primer piso

En las imágenes se observan las instalaciones, el cableado y los equipos que se utilizan en el último punto ubicado en el primer piso.

Ilustración 13. Entrada al *DataCenter* primer piso

Fuente: Autoría propia.

Como se observa la entrada al *DataCenter* no cuenta con una cámara de vigilancia.

El control de acceso al *DataCenter* en la puerta no dispone de un sistema biométrico o de seguridad, sino con una cerradura de llave que no permite identificar al personal autorizado para ingresar al sitio.

Ilustración 14. Extintor tipo A contra incendios del *DataCenter* primer piso

Fuente: Autoría propia.

Se observa que los puntos también cuentan con extintores tipo A contra incendios, pero no se visualizan correctamente y además no tienen la señalización debida.

Ilustración 15. Switch y cableado de datos del *DataCenter* primer piso

Fuente: Autoría propia

Como se observa se sigue presentado el desorden de cableado de datos y eléctricos, además de que el espacio entre cada equipo es muy limitado para que fluya el aire. También se visualiza mucho polvo en los equipos y UPS.

No se encontró sistema de marquillas en los cables de datos y cables de energía. Los cables de datos se encuentran enredados con los cables de energía siendo esto uno de los generadores de ruido en el cableado de datos.

Oficina Departamento de sistemas

En las siguientes imágenes se mostrará cómo están distribuidos los equipos en la oficina, que instalaciones manejan y el sistema de refrigeración.

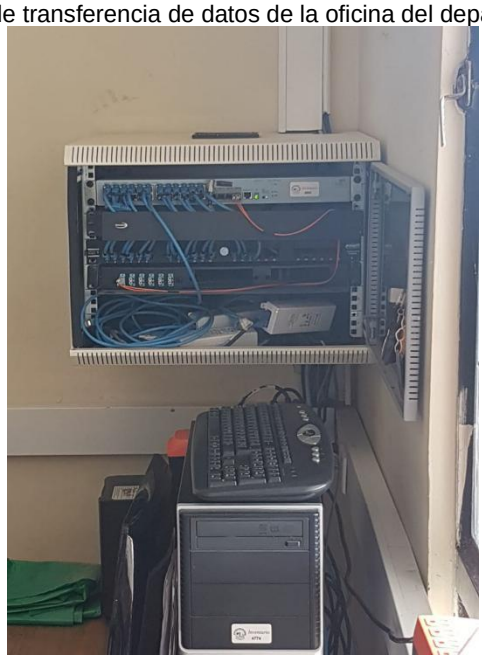
Ilustración 16. Cerradura de la entrada a la oficina del departamento de sistemas

Fuente: Autoría propia

Como se observa la entrada a la oficina del departamento de sistemas no cuenta con una cámara de vigilancia.

El control de acceso a la oficina del departamento de sistemas en la puerta no dispone de un sistema biométrico o de seguridad, sino con una cerradura de llave que no permite identificar al personal autorizado para ingresar al sitio, además de que esta cerradura se encuentra en estado de deterioro y oxidada.

Ilustración 17. Punto de transferencia de datos de la oficina del departamento de sistemas



Fuente: Autoría propia

Como se observa en el punto de transferencia de datos el cableado se encuentra desordenado impidiendo el flujo del aire entre los switch.

Ilustración 18. Panorámica de la oficina del departamento de sistemas

Fuente: Autoría propia

Se puede observar una pésima distribución de los equipos, escritorios y demás instalaciones de la oficina del departamento de sistemas. Este desorden

ocasionaría la perdida de información, equipos y herramientas necesarias para el adecuado desempeño de esta área.

Ilustración 19. Sistema de refrigeración de la oficina del departamento de sistemas

Fuente: Autoría propia

Como se puede observar en la oficina cuentan con dos tipos de sistemas de refrigeración por medio del aire acondicionado y del ventilador de techo convencional, ambos están funcionando en óptimas condiciones.

18. ESTIMACIÓN DE LAS VULNERABILIDADES QUE PUEDEN AFECTAR A CADA UNO DE LOS ACTIVOS.

Teniendo en cuenta lo anterior, existen una serie de exposiciones que se ven envueltas los diferentes activos, para hacer una fácil identificación de estos, se elaboró las siguientes tablas que se pueden apreciar en el anexo 3.

19. ESTIMACIÓN DEL IMPACTO QUE CAUSARÍA LA PÉRDIDA DE CADA ACTIVO.

En la estimación del impacto el objetivo es conocer el daño producido en la Institución derivado a la materialización de las amenazas sobre los activos de la información. Se basa en las siguientes escalas:

1) Según la Degradación donde nos indica que tan perjudicado resulta el valor del activo de información (1%, 50%, 100%), como resultado de la materialización de las amenazas.

- 90% a 100%: Degradación muy considerable del activo
- 25% a 89%: Degradación medianamente considerable del activo
- 1% a 24%: Degradación poco considerable del activo

2) Según el valor del activo.

- Desastroso (8): Impacta fuertemente en la operatividad de los procesos
- Mayor (5): Impacta en la Operatividad de los procesos
- Moderado (3): Impacta en la operatividad del macro proceso
- Menor (2): Impacta en la operatividad del proceso
- Insignificante (1): Impacta levemente en la operatividad del macro proceso

Tabla 14 Explicación de los valores de impacto, degradación y su escala.

IMPACTO		**DEGRADACIÓN**		
		1%	**50%**	**100%**
VALOR DEL ACTIVO	MUY ALTO	3	5	8
	ALTO	2	3	5
	MEDIO	1	2	3
	BAJO	1	1	2
	MUY BAJO	1	1	1

Fuente: Autoría propia

Según lo anterior, se concluyó lo siguiente:

Una tabla en la cual se aprecia 9 columnas independientes que corresponden a:

- ID (código único que es asignado a cada activo dentro de la dependencia) en el anexo 4 esta columna se puede apreciar con el nombre de “Código consecutivo ITFIP”.

- Cantidad (corresponde al número de ejemplares que posee un activo dentro de la dependencia).

  Nota: La “N” en la columna cantidad significa que no se sabe con certeza la cantidad exacta de ejemplares.

- Activo (nombre con el que se identifica el activo dentro de la dependencia) en el anexo 4 esta columna se conoce como “Nombre del activo ITFIP”.

- Criterios de valoración (corresponde a 3 columnas identificadas como: disponibilidad, integridad y confidencialidad en donde será posible visualizar un valor cualitativo dado por los funcionarios de la dependencia a cada activo para así demostrar que tan grande podría ser el impacto si la amenaza se materializa).

Valoración del activo (corresponde a 2 columnas identificadas como: Nivel que hace referencia al promedio cualitativo de las 3 columnas anteriores y valor que corresponde al nivel cuantitativo asignado en la columna Nivel).

20. ESTIMACIÓN DE LA PROBABILIDAD DE QUE OCURRA PERDIDA DEL ACTIVO

En la estimación de la probabilidad consiste en estimar la frecuencia de materialización de una amenaza en función de la cantidad de veces que esta pueda ocurrir, basada en la siguiente escala:

Tabla 15. Explicación de los valores

1	Raro	Puede Ocurrir una vez cada 2 años
2	Muy Baja	Al año
3	Baja	En 6 meses
4	Media	Al mes
5	Alta	A la semana

Fuente: Autoría propia

Según la tabla anterior, se concluyó lo siguiente.

En esta se aprecia con 5 filas en su inicio y 6 columnas independientes que corresponden a:

Filas

- ACTIVO TI (nombre del activo dentro de la dependencia).
- ADMINISTRADOR (responsable del activo en la dependencia).
- DEGRADACION (corresponde al valor dado en la columna nivel de la tabla número 2 del anexo 6 pero en forma porcentual).
- IMPACTO (corresponde al valor dado en la columna nivel de la tabla número 2 del anexo 2).
- TIPO DE ACTIVO (corresponde al nombre del grupo MAGERIT al cual pertenece el activo).

Columnas

- TIPO (corresponde al nombre del grupo de amenazas).
- ID (código único referente a cada tipo de amenaza según MAGERIT).

- AMENAZA (nombre de la amenaza según MAGERIT).
- EXPOSICION/VULNERABILIDAD (breve descripción de la magnitud en la que la amenaza podría afectar el activo).
- FRECUENCIA (corresponde a dos columnas de valoración donde la primera es cualitativa y la segunda cuantitativa).

Esto se puede evidenciar ene le anexo 4 y 5.

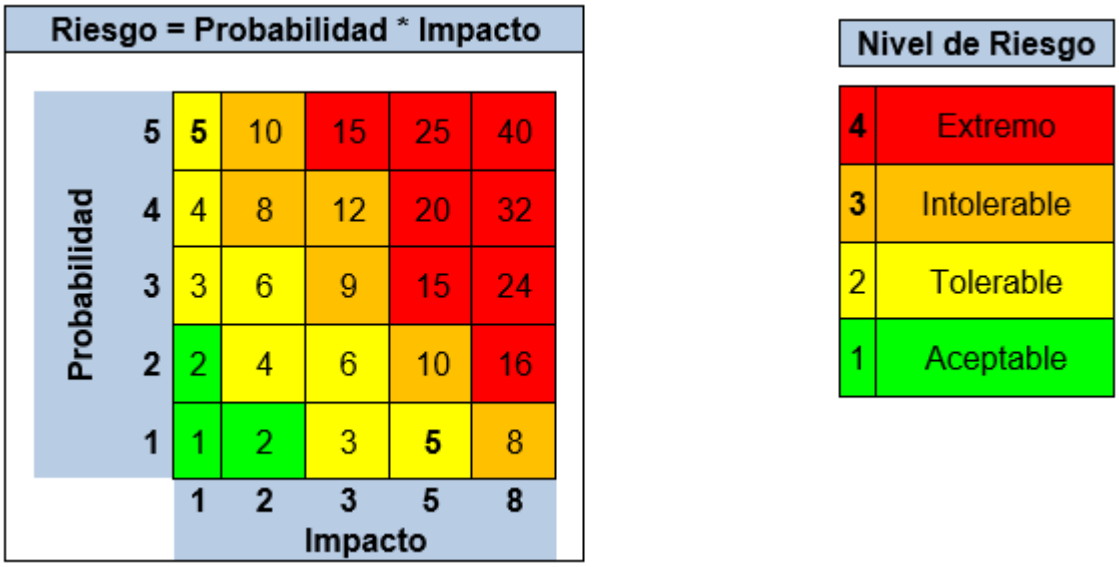
21. ESTIMACIÓN DEL RIESGO

La estimación del riesgo es obtenida por medio de la siguiente ecuación matemática:

Riesgo = probabilidad x impacto

Este proceso de análisis de riesgos normalmente genera un MAPA DE RIESGOS, en el que se ubican los activos de información identificados y los cálculos realizados.

Ilustración 20. Estimación del Riesgo según MAGERIT.



Fuente: MAGERIT V3.0

En la siguiente tabla se encontrarán con 5 filas en su inicio y 9 columnas independientes que corresponden a:

Filas

- ACTIVO TI (nombre del activo dentro de la dependencia).
- ADMINISTRADOR (responsable del activo en la dependencia).
- DEGRADACION (corresponde al valor dado en la columna nivel de la tabla número 17 del anexo 7 pero en forma porcentual).
- IMPACTO (corresponde al valor dado en la columna nivel de la tabla número 17 del anexo 7).
- TIPO DE ACTIVO (corresponde al nombre del grupo MAGERIT al cual pertenece el activo).

Columnas

- TIPO (corresponde al nombre del grupo de amenazas).
- ID (código único referente a cada tipo de amenaza según MAGERIT).
- AMENAZA (nombre de la amenaza según MAGERIT).
- EXPOSICION/VULNERABILIDAD (breve descripción de la magnitud en la que la amenaza podría afectar el activo).
- FRECUENCIA (corresponde a dos columnas de valoración donde la primera es cualitativa y la segunda cuantitativa).
- R (valor correspondiente al riesgo calculado de la probabilidad por el impacto).
- NR (corresponde a la clasificación de nivel de riesgo donde pertenece el riesgo calculado según MAGERIT).

Para una mejor visualización de estas tablas referirse al anexo 7 y 8.

22. APLICACIÓN DE LAS SALVAGUARDAS A CADA TIPO DE ACTIVO

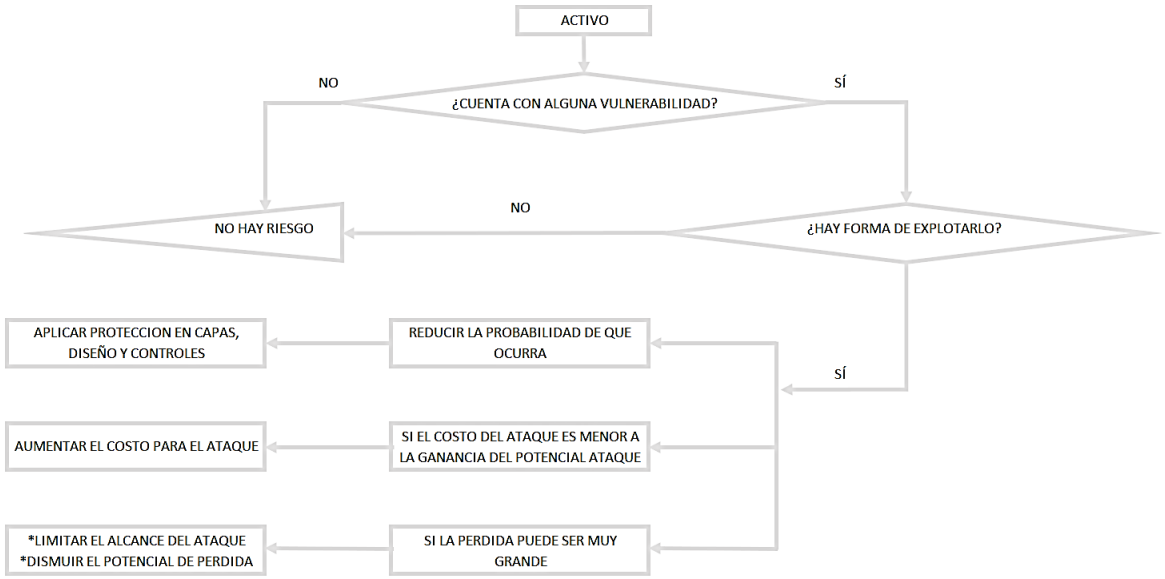
Para la elaboración de las salvaguardas, previamente se desarrolló todo un capítulo de riegos, en los cuales, se busca como medida de protección todo lo relacionado con el inventario de activos, todo esto a raíz de la jerarquía de ellos, su valorización y demás factores que se mostraran más adelante.

Como paso a seguir, se llevará a cabo el establecimiento de la política de seguridad idónea, reglas básicas de la empresa (dependencia). Con el propósito de dar a prevalecer la confidencialidad, disponibilidad e integridad de los datos trabajados. RASCI, será la matriz que se emplearan estas recomendaciones, controles y responsabilidades asignadas.

23. ESTRATEGIA PARA EL TRATAMIENTO DE LOS RIESGOS DE CADA UNO DE LOS ACTIVOS DE LA DEPENDENCIA

Llevar a cabo este ítem, es fundamental conocer como primera medida en que sector se encuentra el riesgo, además, de cómo tratarlo.
A continuación, se expondrá el siguiente diagrama de flujo que nos permitirá evaluar de manera correcta lo ya mencionado anteriormente.

Ilustración 21 Diagrama de flujo para la evaluación de las medidas de salvaguardas.



Fuente: Autoría Propia.

- Al hallarse una vulnerabilidad en cualquier contexto, se debe emplear las técnicas establecidas para permitir la reducción del éxito de ataque.

- De manera que se puede atacar un activo con una vulnerabilidad latente, se requiere de manera urgente aplicar los diferentes controles ubicados en la respectiva capa, analizar los datos y estructura, como también sus controles administrativos, esto se realiza con el fin de suprimir de la manera en la que estos se verían afectados.

- Aumentar el costo, los recursos y demás elementos que sean necesarios para que el atacante pueda efectuar una penetración, esto se realiza con el fin de que es mayor el costo de inversión al de la ganancia bruta llegado al sistema.

- Proteger los activos de mayor importancia para la entidad, esto se puede lograr aplicando las diferentes políticas de seguridad, lineamientos, planes de contingencia y de acceso a la información.

Según los ítems mencionados, se define de manera clara y concisa las estrategias para el tratamiento de los riesgos.

Tabla 16. Estrategias para el tratamiento de los riesgos.

Estrategias para tratamiento de los riesgos		Probabilidad				
				1 – Bajo	2 – Media	3 – Alto
		Impacto	1 – Bajo	1. Zona de riesgo bajo. Tratamiento: Asumir el riesgo	2. Zona de riesgo Bajo Tratamiento: Reducir la probabilidad de ocurrencia	3. Zona de riesgo Moderado Tratamiento: Reducir la probabilidad de ocurrencia Evitar el riesgo
			2 – Medio	2. Zona de riesgo bajo. Tratamiento: Reducir el riesgo, evitar el riesgo	4. Zona de riesgo Moderado Tratamiento: Reducir el riesgo Evitar el riesgo	6. Zona de riesgo extremo Tratamiento: Reducir el riesgo Evitar el riesgo Compartir o transferir
			3 – Alto	3. Zona de riesgo Moderado Tratamiento: Reducir el riesgo Evitar el riesgo	6. Zona de riesgo extremo Tratamiento: Reducir el riesgo Evitar el riesgo Compartir o transferir	9. Zona de riesgo Extremo Tratamiento: Reducir el riesgo Evitar el riesgo Compartir o transferir

Fuente: Autoría Propia.

24. TÉCNICAS PARA EL TRATAMIENTO DEL RIESGO

Según el enfoque del ente, sus prioridades y jerarquías de acciones, se establecen diferentes técnicas que se pueden aplicar para el mejoramiento de los tratamientos de los riesgos. Esta aproximación a veces resulta un poco simplificadora, pues es habitual hablar de diferentes tipos de protección prestados por las salvaguardas:

[PR] Prevención: Se aclara que una salvaguarda de tipo preventivo es aquel que optimiza la posibilidad de que una incidencia ocurra, por otra parte, llegado el caso este llegara ocurrir los contratiempos son mínimos.

[DR] Disuasión: Se aclara que una salvaguarda de tipo disuasorio es aquel que logra llegar a los posibles atacantes alertándolos de los contratiempos que pueden tener, de este modo se logra replantear el modo de ataque o desistir del mismo, exceptuando que si logra atacar los daños son claros y no contaría con disminución alguna.

[EL] Eliminación: Se aclara que una salvaguarda tipo eliminación, es aquel que logra por completo la ocurrencia de este incidente, por lo general son medidas más drásticas a tomar, puesto que no permite que el activo se vea afectado.

[IM] minimización del impacto / limitación del impacto: Se aclara que la imposición de esta técnica solamente minimiza o reduce el daño a consecuencia de la efectuación de una amenaza.

[CR] corrección: Asimilamos que las salvaguardas en su área correctiva permiten actuar una vez la amenaza ya ha tenido lugar, por ende, busca reducir las consecuencias de estas.

[RC] recuperación: Para las salvaguardas de recuperación, como su nombre lo indica, busca a través del daño la restauración al estado previo antes del ataque, permitiendo el restablecimiento de su correcto funcionamiento.

[MN] monitorización: Son aquellas salvaguardas que mantienen en constante verificación del estado actual en el que se encuentra el activo, permitiendo a su vez, detectar en tiempo real las amenazas, aclarando la posibilidad de tomar las medidas correspondientes.

[DC] detección: la detección oportuna de un ataque o amenaza no impida ni retrasa el ataque a diferencia de la monitorización, excluyendo la opción de actuación de alarmas oportunas ya establecidas.

[AW] concienciación son metodologías propias de la integración de cada una de las personas integrantes de la entidad. Los cuales, mediante dichas metodologías

adquieren conocimientos adecuados de cómo afrontar una amenaza, esto por lo general, se añade el rango de experiencia en una plataforma.

[AD] administración: La aclaración de salvaguardas correlacionadas a los diferentes niveles de la seguridad de los sistemas, permite a los diferentes administradores de los sistemas manejar adecuadamente la manipulación de cada uno de los activos, aumentar la posibilidad de prevenir ataques o daños, entre otros. La siguiente tabla relaciona cada uno de estos tipos de protección con el modelo anterior de reducción de la degradación y de la probabilidad:

Tipos de salvaguardas según MAGERIT.

Tabla 17. Efectos y tipo de salvaguardas.

Efecto	Tipo
Preventivas: reducen la probabilidad	[PR] Preventivas
	[DR] Disuasorias
	[EL] Eliminatorias
Acotan la degradación	[IM] Minimiza doras
	[CR] Correctivas
	[RC] Recuperativas
Consolidan el efecto de las demás	[MN] De monitorización
	[DC] De detección
	[AW] De concienciación
	[AD] Administrativas

Fuente: MAGERIT. V 3.0 Libro 1

25. INFORME Y EVALUACIÓN DE LOS TRATAMIENTOS DE RIESGO

25.1. IDENTIFICACIÓN

La aclaración e identificación de los riesgos que pueden llegar a afectar un sistema de gestión de la información, en cada una de las diferentes capas de manejo, es el primer paso para determinar cómo hacer el tratamiento respectivo del riesgo.
Para dicho proceso, se llevó a cabo una serie de pautas, en las cuales consiste en la previa entrevista con el coordinador de la dependencia, él ing. Wilson Mauricio Pimiento, y los demás entes intermediarios en la entidad, como lo son el ingeniero Darwin Muñoz López, la ingeniera Melissa Martínez y el tecnólogo Juan Sebastián Laguna; también, se llevó un análisis detenido del área de trabajo, sus procedimientos, tiempos, y circunstancias con los cuales trabajan.
También se llevó a cabo una serie de apreciación a cada uno de los diferentes medios de información, sean estos almacenados de manera lógica o física, llegando a instancias de talento humano y la oficina de almacén institucional.

A continuación, de la siguiente manera se expondrá cada uno.

- Amenaza hallada
    - Posibles vulnerabilidades

Según lo anterior, se identificaron las siguientes amenazas:

- [Re-]encaminamiento de mensajes
- Abuso de privilegios de acceso
- Acceso no autorizado
- Alteración accidental de la información
- Alteración de secuencia
- Análisis de trafico
- Avería de origen físico o lógico
- Caída del sistema por agotamiento de recursos
- Condiciones inadecuadas de temperatura o humedad
- Contaminación electromagnética
- Contaminación mecánica
- Corte del suministro eléctrico
- Daños por agua

- Daños por agua
- Deficiencias en la organización
- Degradación de los soportes de almacén amiento de la información
- Denegación de servicio
- Desastres industriales
- Desastres naturales
- Destrucción de información
- Destrucción de información
- Difusión de software dañino
- Difusión de software dañino
- Divulgación de información
- Emanaciones electromagnéticas
- Errores de [re-] encaminamiento
- Errores de los usuarios
- Errores de mantenimiento / actualización de equipos(hardware)
- Errores de mantenimiento / actualización de programas (software)
- Errores de secuencia
- Extorsión
- Fallo de servicios de comunicaciones
- Fuego
- Fugas de información
- Indisponibilidad del personal
- Indisponibilidad del personal
- Ingeniería social (picaresca)
- Interceptación de información (escucha)
- Interrupción de otros servicios y suministros esenciales
- Manipulación de los equipos
- Manipulación de programas
- Modificación deliberada de la información
- Perdida de equipos (Robo)

- Robo
- Suplantación de la identidad del usuario
- Uso no previsto
- Vulnerabilidades de los programas (software)

Los ítems que se mencionaron anteriormente (o) hacen referencias a las posibles incidencias, en las cuales, se puede ver afectada la dependencia; a continuación, se hará la explicación de cada una de ellas.
La unión entre los factores de riesgo y cada uno de los activos, nos arrojó como resultado un total de 275 (94 Riesgos Críticos – 179 Riesgos Moderados – 2 Riesgos Bajos); posibilidades que pueden afectar el correcto funcionamiento del sistema. Los cuales; se dividieron de la siguiente manera:

Tabla 18. Calculo para los factores de riesgos de cada uno de los activos

Vector de Amenaza	RC	RM	RB	Total general
Desastres naturales	8	34	2	44
De origen industrial	20	49	0	69
Errores y fallos no intencionados	32	49	0	81
Ataques intencionados	34	47	0	81
Total general	94	179	2	275

Fuente: Autoría propia.

Con el anterior estudio (probabilidad e impacto) añadiéndole el reciente resultado, se puede apreciar el siguiente resumen:

Tabla 19. Resumen promedios de la probabilidad y del impacto en los activos

Vect-id	V-Amenaza	Prom-prob	Prom-imp	Valor P*I	
01-VA	Desastres naturales	2	2	4	RM
02-VA	De origen industrial	2	2	4	RM
03-VA	Errores y fallos no intencionados	2	2	4	RM
04-VA	Ataques intencionados	2	2	4	RM

Fuente: Autoría propia.

Según el resumen de la tabla anterior, realizamos la siguiente matriz, cabe aclarar que la institución se encuentra en un estado moderado, que a su vez, eleva las alarmas en un gran porcentaje.

Tabla 20. Mapa de riesgo por vector de amenaza

Mapa de riesgo por vector de amenaza				
Probabilidad	3 – Alta	01-VA		
	2 – Media		02-VA 03-VA	
	1 – Baja			04-VA
		1 – Baja	2 – Media	3 - Alta
	Impacto			

Fuente: Autoría propia.

25.2. TRATAMIENTO DEL RIESGO

Una vez aclarado cuales son los riesgos que encontramos, a qué tipo de activo puede ver este afectado, lo cual, puede interrumpir su correcto funcionamiento; procedemos a estipular los tratamientos adecuados para cada uno de ellos, factores como que nos aclararan como prevenir, aclarar, interrumpir o eliminar dichas amenazas.

- Al hallarse una vulnerabilidad en cualquier contexto, se debe emplear las técnicas establecidas para permitir la reducción del éxito de ataque.

- De manera que se puede atacar un activo con una vulnerabilidad latente, se requiere de manera urgente aplicar los diferentes controles ubicados en la respectiva capa, analizar los datos y estructura, como también sus controles administrativos, esto se realiza con el fin de suprimir de la manera en la que estos se verían afectados.

- Aumentar el costo, los recursos y demás elementos que sean necesarios para que el atacante pueda efectuar una penetración, esto se realiza con el fin de que es mayor el costo de inversión al de la ganancia bruta llegado al sistema.

- Proteger los activos de mayor importancia para la entidad, esto se puede lograr aplicando las diferentes políticas de seguridad, lineamientos, planes de contingencia y de acceso a la información.

Según los ítems mencionados, se define de manera clara y concisa las estrategias para el tratamiento de los riesgos.

Tabla 21. Estrategias para el tratamiento de los riesgos.

Estrategias para tratamiento de los riesgos					
	Probabilidad				
	Impacto		1 – Bajo	2 – Media	3 – Alto
		1 – Bajo	1. Zona de riesgo bajo. Tratamiento: Asumir el riesgo	2. Zona de riesgo Bajo Tratamiento: Reducir la probabilidad de ocurrencia	3. Zona de riesgo Moderado Tratamiento: Reducir la probabilidad de ocurrencia Evitar el riesgo
		2 – Medio	2. Zona de riesgo bajo. Tratamiento: Reducir el riesgo, evitar el riesgo	4. Zona de riesgo Moderado Tratamiento: Reducir el riesgo Evitar el riesgo	6. Zona de riesgo extremo Tratamiento: Reducir el riesgo Evitar el riesgo Compartir o transferir
		3 – Alto	3. Zona de riesgo Moderado Tratamiento: Reducir el riesgo Evitar el riesgo	6. Zona de riesgo extremo Tratamiento: Reducir el riesgo Evitar el riesgo Compartir o transferir	9. Zona de riesgo Extremo Tratamiento: Reducir el riesgo Evitar el riesgo Compartir o transferir

Fuente: Autoría Propia.

25.3. TÉCNICAS PARA EL TRATAMIENTO DEL RIESGO

Según el enfoque del ente, sus prioridades y jerarquías de acciones, se establecen diferentes técnicas que se pueden aplicar para el mejoramiento de los tratamientos de los riesgos. Esta aproximación a veces resulta un poco simplificadora, pues es habitual hablar de diferentes tipos de protección prestados por las salvaguardas:

- **(T) Transferir:** La acción de esta técnica recure a trasladar los inconvenientes, problemas, y soportes oportunos a otra entidad externa, por lo general, se celebran pólizas de seguro o contratos outsourcing. Los riesgos se pueden medir de dos maneras, una cualitativa y otra cuantitativa. En donde la primera de estas; se adapta por medio de la externalización de los diferentes componentes involucrados, dicha manera reparte las diferentes acciones al cargo. Como segundo riesgo se encuentra el cuantitativo, en donde por medio de la aplicación de contratos referidos al seguro, se transforma la materia prima, se adapta y preserva a las posibles amenazas que puedan correr, esto con el fin de no accionar las consecuencias.

- **(M) Mitigar:** El establecimiento de salvaguardas que toman acción en los diferentes momentos cuando se alza la alarma de ataque o colapso del sistema, dichos recursos permiten al ente minimizar en todos los factores los daños que se puedan presentar, facilitando el acatamiento oportuno de las funciones a elaborar.

- **Investigar:** Esta sección de las diferentes técnicas es importante, puesto que es en la que se realiza la mayor parte del trabajo o se tiene reconocimiento de eventos. Los resultados no se aplican a alguna mitigación, sin embargo, a futuro se identifican soluciones más aptas y a menor respuesta de tiempo.

- **(C) Controlar:** Consistentemente se recurre al monitoreo de la fluctuación que pueda llevar a la probabilidad he impacto altos, no obstante, se mantienen las alertas y a su vez se informa a los supervisores asignados al caso.

- **(E) Evitar:** Evitar la ocurrencia del riesgo se realiza a cuestión de que la probabilidad de que ocurra sea alta o media, evitando daños significativos para la entidad, usualmente se encuentran rápidamente políticas, lineamientos, normas y de más procedimientos en los diferentes controles y capaz de seguridad.

- **Aceptar:** La aceptación es la acción más pasiva de todas, puesto que así mismo permite y acepta el riesgo en cuestión, por lo general, esta técnica es empleada en activos en donde sus riesgos se catalogan como “muy bajos” y “bajos”.

Según las técnicas, criterios y demás factores podemos determinar que cada una de ellas se determina de la siguiente manera:

Tabla 22. Técnicas de tratamiento por riesgo

ID Riesgo	Riesgo	V-AMENAZA	T	M	I	E	C	A
01-RG	[Re-]encaminamiento de mensajes	Ataques intencionados				X		
02-RG	Abuso de privilegios de acceso	Ataques intencionados		X				
03-RG	Acceso no autorizado	Ataques intencionados		X				
04-RG	Alteración accidental de la información	Errores y fallos no intencionados					X	
05-RG	Alteración de secuencia	Ataques intencionados					X	
06-RG	Análisis de trafico	Ataques intencionados					X	
07-RG	Avería de origen físico o lógico	De origen industrial	X					

Tabla 18. Técnicas de tratamiento por riesgo (Continuación)

08-RG	Caída del sistema por agotamiento de recursos	Errores y fallos no intencionados	X					
09-RG	Condiciones inadecuadas de temperatura o humedad	De origen industrial	X					
10-RG	Contaminación electromagnética	De origen industrial	X					
11-RG	Contaminación mecánica	De origen industrial	X					
12-RG	Corte del suministro eléctrico	De origen industrial	X					
13-RG	Daños por agua	Desastres naturales						
14-RG	Deficiencias en la organización	Errores y fallos no intencionados	X					
15-RG	Degradación de los soportes de almacén amiento de la información	De origen industrial	X					
16-RG	Denegación de servicio	Ataques intencionados		X				
17-RG	Desastres industriales	De origen industrial						
18-RG	Desastres naturales	Desastres naturales		X				
19-RG	Destrucción de información	Errores y fallos no intencionados		X				
20-RG	Difusión de software dañino	Errores y fallos no intencionados					X	
21-RG	Divulgación de información	Errores y fallos no intencionados					X	
22-RG	Emanaciones electromagnéticas	Ataques intencionados						X
23-RG	Errores de [re-] encaminamiento	De origen industrial				X		
24-RG	Errores de los usuarios	Errores y fallos no intencionados	X					
25-RG	Errores de mantenimiento / actualización de equipos(hardware)	Errores y fallos no intencionados				X		
26-RG	Errores de mantenimiento / actualización de programas (software)	Errores y fallos no intencionados				X		
27-RG	Errores de secuencia	Errores y fallos no intencionados				X		

Tabla 23. Técnicas de tratamiento por riesgo. (Continuación)

28-RG	Extorsión	Errores y fallos no intencionados						
29-RG	Fallo de servicios de comunicaciones	Ataques intencionados			X			
30-RG	Fuego	De origen industrial	X					
31-RG	Fugas de información	Desastres naturales						X
32-RG	Indisponibilidad del personal	Errores y fallos no intencionados		X				
33-RG	Ingeniería social (picaresca)	Ataques intencionados		X				
34-RG	Interceptación de información (escucha)	Ataques intencionados		X				
35-RG	Interrupción de otros servicios y suministros esenciales	Ataques intencionados			X			
36-RG	Manipulación de los equipos	De origen industrial			X			
37-RG	Manipulación de programas	Ataques intencionados					X	
38-RG	Modificación deliberada de la información	Ataques intencionados					X	
39-RG	Perdida de equipos (Robo)	Ataques intencionados	X					
40-RG	Robo	Errores y fallos no intencionados				X		
41-RG	Suplantación de la identidad del usuario	Errores y fallos no intencionados				X		
42-RG	Uso no previsto	Ataques intencionados				X		
43-RG	Vulnerabilidades de los programas (software)	Ataques intencionados					X	

Fuente: Autoría propia.

La sostenibilidad de un activo se debe a gran medida de las ideas que se toman a tiempo para salvar/proteger dicha información, esto, a su vez reduce en gran nivel las consecuencias, que para toda razón social es realmente necesaria. El estudio de las combinaciones de amenaza/vulnerabilidad servirá como base principal para dictaminar el tratamiento a seguir, para ello le daremos la importancia idónea a cada una de ellas.

La siguiente tabla se expondrá la manera en la cual se le adjudicará los valores y su significado, según la importancia de riesgo.

Tabla 24. Valores prioridad del riesgo.

PRIORIDAD	VALOR
1	Menor
2	
3	Estable
4	
5	Alta

Fuente: Autoría propia

Tabla 250. Priorización del riesgo

ID Riesgo	Riesgo	V-AMENAZA	RB	RC	RM	PRIORIDAD
01-RG	[Re-]encaminamiento de mensajes	Ataques intencionados		X		5
02-RG	Abuso de privilegios de acceso	Ataques intencionados		X		5
03-RG	Acceso no autorizado	Ataques intencionados	X			5
04-RG	Alteración accidental de la información	Errores y fallos no intencionados	X			5
05-RG	Alteración de secuencia	Ataques intencionados	X			5
06-RG	Análisis de trafico	Ataques intencionados		X		4
07-RG	Avería de origen físico o lógico	De origen industrial		X		4
08-RG	Caída del sistema por agotamiento de recursos	Errores y fallos no intencionados		X		5
09-RG	Condiciones inadecuadas de temperatura o humedad	De origen industrial		X		4
10-RG	Contaminación electromagnética	De origen industrial		X		4
11-RG	Contaminación mecánica	De origen industrial		X		4
12-RG	Corte del suministro eléctrico	De origen industrial		X		5
13-RG	Daños por agua	Desastres naturales		X		5
14-RG	Deficiencias en la organización	Errores y fallos no intencionados		X		4
15-RG	Degradación de los soportes de almacén amiento de la información	De origen industrial		X		3
16-RG	Denegación de servicio	Ataques intencionados		X		3
17-RG	Desastres industriales	De origen industrial		X		3
18-RG	Desastres naturales	Desastres naturales		X		3
19-RG	Destrucción de información	Errores y fallos no intencionados		X		5

Tabla 20. Priorización del riesgo. (Continuación)

20-RG	Difusión de software dañino	Errores y fallos no intencionados		X		5
21-RG	Divulgación de información	Errores y fallos no intencionados		X		5
22-RG	Emanaciones electromagnéticas	Ataques intencionados			X	4
23-RG	Errores de [re-] encaminamiento	De origen industrial		X		5
24-RG	Errores de los usuarios	Errores y fallos no intencionados	X			3
25-RG	Errores de mantenimiento / actualización de equipos(hardware)	Errores y fallos no intencionados	X			2
26-RG	Errores de mantenimiento / actualización de programas (software)	Errores y fallos no intencionados	X			2
27-RG	Errores de secuencia	Errores y fallos no intencionados	X			2
28-RG	Extorsión	Errores y fallos no intencionados		X		5
29-RG	Fallo de servicios de comunicaciones	Ataques intencionados		X		4
30-RG	Fuego	De origen industrial		X		4
31-RG	Fugas de información	Desastres naturales		X		3
32-RG	Indisponibilidad del personal	Errores y fallos no intencionados		X		2
33-RG	Ingeniería social (picaresca)	Ataques intencionados	X			2
34-RG	Interceptación de información (escucha)	Ataques intencionados		X		4
35-RG	Interrupción de otros servicios y suministros esenciales	Ataques intencionados		X		4
36-RG	Manipulación de los equipos	De origen industrial		X		3
37-RG	Manipulación de programas	Ataques intencionados	X			3
38-RG	Modificación deliberada de la información	Ataques intencionados	X			2
39-RG	Perdida de equipos (Robo)	Ataques intencionados		X		5
40-RG	Robo	Errores y fallos no intencionados		X		5
41-RG	Suplantación de la identidad del usuario	Errores y fallos no intencionados		X		3
42-RG	Uso no previsto	Ataques intencionados		X		3
43-RG	Vulnerabilidades de los programas (software)	Ataques intencionados		X		5

Fuente: Autoría propia

CAPITULO 3. DECLARACIÓN DE APLICABILIDAD

26. DECLARACIÓN DE APLICABILIDAD

La declaración de aplicabilidad (SoA), se trata de un documento que enlista los controles de seguridad establecidos en el Anexo A del estándar ISO/IEC 27001 (un conjunto de 114 controles agrupados en 35 objetivos de control, en la versión de 2013 de esta norma de seguridad).
Esta matriz está compuesta de la siguiente manera:

- En la columna de objetivo de control va el objetivo del control establecido por el dominio de acuerdo a el Anexo A del estándar ISO/IEC 27001.
- En la columna controles va el nombre de los 114 controles que establece el Anexo A del estándar ISO/IEC 27001.
- En la columna aplicabilidad, se muestra si la organización quiere aplicar o no dichos controles.
- En la columna exclusiones, se colocan todos los controles que no son necesarios para la empresa.
- En la columna razones de la selección se manejan las siguientes abreviaturas.
    - **RL:** requerimientos legales.
    - **CO:** obligaciones contractuales.
    - **BR/BP:** Requerimientos del negocio o adopción de buenas prácticas.
    - **RRA:** Resultados de análisis de riesgos.
- En la columna de justificación el gerente justifica por qué si y no tiene aplicados esos controles.
- En la fila que cruza por toda la matriz contiene el nombre de los 14 dominios establecidos por el Anexo A del estándar ISO/IEC 27001.

A continuación se mostrará la declaración de aplicabilidad:

26.1. POLITICAS Y LINEAMIENTOS DE SEGURIDAD DE INFORMACIÓN

La selección de controles esta seguida de los 14 dominios definidos por la norma ISO/IEC 27001:2013. A continuación se generarán políticas basadas en cada uno de los dominios y se determinara controles de acuerdo al estudio.

Tabla 261 . Dominio y controles definidos por la ISO/IEC 27001:2013

ID	Dominio	Control
A5	Política de seguridad	Orientación de la dirección para la gestión de la seguridad de la información
A6	Organización de la SI	Organización interna Dispositivos móviles y teletrabajo
A7	Seguridad de los RRHH	Antes de asumir el empleo Durante la ejecución del empleo Terminación y cambio de empleo
A8	Gestión de activos	Responsabilidad por los activos Clasificación de la información Manejo de medios
A9	Control de accesos	Requisitos del negocio para el control de acceso Gestión de acceso de usuarios Responsabilidades de los usuarios Control de acceso a sistemas y aplicaciones
A10	Criptografía	Controles criptográficos
A11	Seguridad física y ambiental	Áreas seguras Equipos
A12	Seguridad en las operaciones	Procedimientos operacionales y responsabilidades Protección contra códigos maliciosos Copias de respaldo Registro y seguimiento Control de software operacional Gestión de la vulnerabilidad técnica Consideraciones sobre auditorías de sistemas de información
A13	Seguridad en las comunicaciones	Gestión de la seguridad de las redes Transferencia de información
A14	Adquisición de sistemas, desarrollo y mantenimiento	Requisitos de seguridad de los sistemas de información Seguridad en los procesos de Desarrollo y de Soporte Datos de prueba
A15	Relación con proveedores	Seguridad de la información en las relaciones con los proveedores Gestión de la prestación de servicios de proveedores
A16	Gestión de los incidentes de seguridad	Gestión de incidentes y mejoras en la seguridad de la información
A17	Continuidad del negocio	Continuidad de Seguridad de la información Redundancias
A18	Cumplimiento con requerimientos legales y contractuales	Cumplimiento de requisitos legales y contractuales Revisiones de seguridad de la información

Fuente: Autoría propia.

- **A5-Política de seguridad**

Inicialmente, el mayor inconveniente o vulnerabilidad de la organización hace referencia a la falta de documentos formales que concienticen e informen al personal sobre sus responsabilidades y las reglas básicas que permiten mantener la seguridad de la información. Esta sección ha sido desarrollada pensando en la vulnerabilidad nombrada y que en gran medida es la causante de los riesgos detectados. Por ello, se definen las siguientes políticas de seguridad de la información:

Políticas:

- Se debe establecer la seguridad de la información como uno objetivos vitales en la organización.
- Se debe crear un comité de seguridad de la información que garantice que el personal cumpla con las medidas de seguridad en todas las áreas.
- Garantizar que el personal que tiene acceso a los recursos tecnológicos dispuestos por el ITFIP, estén identificados y sus acciones sean controlados de manera que contribuyan a un ambiente seguro dentro de la organización.
- Definir las reglas de acceso para los diversos sistemas, equipos, instalaciones e información basados en los requerimientos de negocio y seguridad.
- Establecer los requisitos básicos para garantizar que el acceso a las instalaciones de operación de servidores o equipos de cómputo tengan la seguridad correspondiente.
- Definir requisitos básicos para el desarrollo seguro de software siguiendo estándares y directrices utilizadas actualmente en el mercado.

PTR:

El personal encargado del comité de seguridad de la información debe velar que todas las directrices expuestas se estén cumpliendo de manera correcta.

SoA:

Se debe nombrar un comité de seguridad de la información que regule todos los aspectos de seguridad en la organización. Este comité se encargará de:

- Monitorear riesgos y amenazas que puedan afectar el activo de información.
- Plantear modificaciones periódicas en las políticas de seguridad de acuerdo a los nuevos riesgos y amenazas.
- Vigilar que las directrices sean cumplidas por todo el personal de la organización.

- Debe tener un coordinador encargado de brindar los reportes de mejoramiento de la seguridad ya sea semestral o anualmente.

- **A6- Organización de la SI**

La organización de la seguridad de la información incluye la definición de roles y responsabilidades a nivel interno de la organización, mantener actualizada las medidas de seguridad de soporte para proteger la información a la que se tiene acceso, que es procesada o almacenada. Aquí también se incluye la protección de información que se puede ver afectada por el teletrabajo y el uso de dispositivos móviles.

Políticas:

- El comité de seguridad debe implementar las medidas se dé seguridad, además puede diseñar e implementar una base de datos que almacene el personal con sus respectivas responsabilidades de seguridad de información dentro de la organización.
- Es importante tener un registro documental de derechos y deberes del personal y las medidas que se deben tener al momento de implementar la seguridad de la información.
- Se debe tener un registro de que personas son responsables y autorizadas de su área de trabajo, para evitar el acceso de usuarios no autorizados.

PTR:

Definir políticas de control de acceso físico a áreas de almacenamiento de información (servidores y equipos de cómputo).

SoA:

El comité de seguridad de la información debe asignar un personal que se encargue de verificar los protocolos de seguridad, revisar la vigencia, el cumplimiento de las directrices. Además de asegurar que los empleados que manejen teletrabajo cumplan las indicaciones.

- **A7- Seguridad de los RRHH (Recursos Humanos)**

En la seguridad de los recursos humanos se incluye documentos de términos y condiciones del contrato, asignación de roles y responsabilidades de los empleados en la organización, capacitaciones en seguridad de la información para generar conciencia de que ellos hacen parte de la organización y se debe cuidar.

Políticas:

- En el encargado de la contratación de personal debe tener documentos los requerimientos y pasos para el empleo, junto con los términos y condiciones con respecto la confidencialidad de la información.
- Se deben fijar roles y responsabilidades dentro de la organización para así poder tener un seguimiento efectivo al personal.
- Se debe capacitar el personal sobre los estándares en la seguridad de información, concientizándolos a que la información es un activo vital para la organización.
- Una vez terminado el contrato con el empleado se debe verificar la suspensión de los servicios, la devolución de los activos, devolución de documentos, todos los dispositivos que se le han entregado se encuentren en buen estado y la anulación de contraseñas de acceso.

PTR:

En cada contrato de trabajo se tendrá cláusulas de confidencialidad para asegurar información de la empresa.

Todo empleado que utilice los bienes y servicios informáticos se compromete a utilizarlos bajo los principios de confidencialidad de la información.

SoA:

- Se deberá nombrar una persona responsable en el área de seguridad de información**,** que será el encargado de divulgar las políticas de seguridad y el obligatorio cumplimiento de las mismas por todos los empleados de la empresa. Si se generan cambios este se encargará de divulgar dichos cambios.

- Se debe seleccionar un personal profesional para capacitar a los empleados de la organización sobre la importancia de la seguridad de información.

- Establecer términos y condiciones laborales. Mediante cláusulas en los contratos definir acuerdos de confidencialidad y cumplimiento de políticas de seguridad con todo el personal y con terceros.

    - **A8- Gestión de activos**

Este control busca proteger los activos de información, por ello se aconseja el diseño e implementación de una base de datos que contenga el inventario de estos y permita conocer:

- Recursos informáticos disponibles
- Ubicación
- Responsable
- Uso
- Garantías o contratos próximos a vencer

Así mismo se plantea desarrollar e implementar procedimientos adecuados para clasificar y etiquetar la información, de acuerdo a los criterios de confidencialidad, disponibilidad e integridad definidos en la gestión de riesgos.

Políticas:

- Realizar un inventario de activos de información los cuales se encuentren ordenados según su importancia.
- Clasificar la información bajo estos criterios:
  - Información de uso publico
  - Información de uso interno
  - Información confidencial
- Etiquetar la información con códigos propios de la organización para facilitar su búsqueda.
- En el inventario de activos de información manejar las siguientes etiquetas:
  - Recursos informáticos disponibles
  - Ubicación
  - Responsable
  - Uso
  - Garantías o contratos próximos a vencer

PTR:

- A cada empleado se le hace responsable de sus equipos, activos de información y debe cumplir las medidas de seguridad.
- Los empleados no deberán mover o reubicar los equipos, instalar o desinstalar dispositivos. Eso solamente lo hace el personal autorizado para esas tareas.

- **A9- Control de accesos**

Los controles aquí definidos están enfocados a la gestión de acceso de usuarios y el control de acceso a las redes, sistemas y aplicaciones.

Políticas:

- Diseñar e implementar procedimientos para la gestión adecuada de usuarios en los que se considere desde el registro hasta la revocación de los privilegios asignados.

- Establecer puntos de control en la red para validar a los usuarios y tomar decisiones correspondientes cuando se trata de violaciones de seguridad.
- Estar actualizando constantemente el dispositivo seguridad firewall, porque a pesar de que se utiliza un Fortigate1500D de la marca Fortinet el cual es muy bueno, se debe estar actualizando por seguridad.
- Aislar elementos o información sensible del resto de la infraestructura, especialmente los servidores.
- Configurar VPN. Permitir el acceso indiscriminado a la red propia de la organización desde Internet no es adecuado. Aunque el acceso esté protegido con una contraseña, podría ser capturada en un punto de acceso Wifi público o avistada por un observador malintencionado. Por el contrario, el riesgo disminuye si el trabajador y la empresa se conectan mediante una conexión VPN. El acceso está protegido, la conexión está previsiblemente cifrada y el trabajador tiene el mismo acceso que si estuviera presencialmente ahí.[118]
- Se debe utilizar los más recientes tipos de encriptación para las contraseñas de acceso, por seguridad.

PTR:

- Implementar métodos de autenticación y control de acceso.
- Segmentar la red.
- Implementar el control de puertos y ruteo de red.
- Efectuar un control de los registros de auditoria.
- Definir perfiles de acceso.
- Controlar los cambios en los accesos.

SoA:

- Definir un registro formal de usuarios para otorgar y revocar accesos, utilizar identificadores de usuarios únicos.
- Identificar los privilegios, asignarlos de acuerdo a las necesidades del trabajo, mantener un registro actualizado de ellos.
- Los usuarios deben comprometerse a utilizar y mantener en secreto sus contraseñas esto debe estar estipulado en el contrato laboral, cambiarlas periódicamente y deben cumplir con todos los criterios de seguridad.
- Debe haber un encargado de otorgar los permisos para el acceso a la red y sus recursos, realizar normas y procedimientos de autorización, establecer controles y procedimientos de control de acceso, para la autenticación de usuario, para las conexiones externas debe de escogerse un método y

[118] ÁGUEDA A. NOBBOT. VPN: ¿qué es y para qué sirve?. Consultado: 10 de Enero del 2019. Link: https://www.nobbot.com/tecnologia/mi-conexion/vpn-¿que-es-y-para-que-sirve/

protocolo de autenticación, controlar el acceso a sistemas informáticos remotos, protección de puertos para evitar accesos no autorizados. El acceso a internet solo será autorizado por el.

- También tiene aplicar este criterio al acceso a las aplicaciones y al uso de los sistemas en general.

- **A10- Criptografía**

La implementación de controles criptográficos permite proteger la información cuando esta sale de los límites de la organización. Por ello se recomienda que los dispositivos, por ejemplo: USB, discos duros externos, entre otros medios portátiles de almacenamiento. También los archivos planos, correos en donde se maneja información sensible para la organización deben estar cifrados.

Políticas:

- El jefe de cada área debe velar por la información que se maneje por parte de sus empleados y que esta sea clasificada o restringida.
- Al momento de compartir información los empleados deben utilizar algún tipo de cifrado ya sea a los archivos en concreto o al dispositivo de almacenamiento.
- Las contraseñas de los equipos, acceso a plataformas, correos, entre otros. Deben ser totalmente de conocimiento de la persona que trabaja en ese puesto y estar cambiando periódicamente las claves por seguridad.

PTR:

- Los empleados pueden compartir de manera comprimida con clave para así prevenir daños por virus o robo de información.
- Para prevenir robo o alteración de información los empleados deben tratar no ingresar a software malicioso o no proporcionado por la organización.
- Los empleados están obligados a verificar que la información y que los medios de almacenamiento, considerando memorias USB, CDs, estén libres de cualquier tipo de software dañino, para ello deben ejecutar el software antivirus.

SoA:

- Deben desarrollar y establecer un procedimiento para el manejo y la administración de llaves de cifrado.
- Deben desarrollar y establecer estándares para la aplicación de controles criptográficos.

- Deben almacenar y/o transmitir la información digital clasificada bajo técnicas de cifrado con el propósito de proteger su confidencialidad e integridad.

- **A11- Seguridad física y ambiental**

Si el acceso a una instalación de la organización no está correctamente protegido, se incrementa la probabilidad de ataques a los sistemas de información. También si no se encuentra acondicionado con los equipos o parámetros contra desastres naturales o eléctricos, el daño puede ser extremo.

Políticas:

- Implementar seguridad perimetral, es decir controles que eviten el acceso no autorizado a las áreas sensibles de la organización como los servidores, dicha seguridad puede ser video vigilancia, alarmas de seguridad sensoriales, entre otros.
- Manejar un sistema de registro de ingreso y salida de visitantes y/o terceros a las áreas con activos de información vitales para la organización.
- Medidas de protección contra incendios. La selección de extintores debe ser el adecuado que no deje residuos ni sustancias corrosivas que puedan dañar los equipos, las alarmas contra incendios por sensor es otra opción muy viable.
- Controles de refrigeración y ventilación, los equipos deben tener una muy buena refrigeración ya sea por aire acondicionado o ventiladores convencionales de buena potencia debido a que los equipos informáticos con el tiempo tienden a subir de temperatura.
- Ubicar los equipos en lugares que reduzcan los riesgos de amenazas y peligros del entorno y el acceso no autorizado.
- Los equipos deben tener fuente de alimentación de respaldo de energía como las UPS y protección (polo a tierra), para evitar daños eléctricos.

PTR:

- Realizar un estudio previo a la instalación de los lugares a donde se van a colocar, para que se adecuen de acuerdo a las políticas de seguridad física y ambiental.
- Realizar periódicamente revisiones y mantenimientos a los equipos para ver en qué estado se encuentran y así evitar daños.

SoA:

- La adecuación correcta a los lugares donde van a estar los servidores, hace que la seguridad de los mismos sea mucho más confiable y evite daños a la organización.

- **A12- Seguridad en las operaciones**

En este apartado se busca asegurar una correcta gestión de todas las operaciones de procesamiento de información.

Políticas:

- Separar de los ambientes de desarrollo, pruebas y operación, con ello se busca reducir los riesgos de acceso o cambios no autorizados al ambiente de operación. Por lo tanto es indispensable que:
    - Los desarrolladores realicen su trabajo exclusivamente en ambiente de desarrollo, nunca en otros ambientes directamente. Debe ser un ambiente distinto a los de pruebas y producción.
    - Se utilicen nombres de dominio diferentes para los ambientes de producción, pruebas y desarrollo, a efectos de evitar confusión durante la ejecución de las pruebas.
- Verificar periódicamente que los equipos tengan instalado y actualizado el antivirus designado por la organización.
- Verificar que los archivos de origen incierto o recibió a través de redes poco confiables no contengan virus antes de hacer uso de ellos.
- Bloquear los sitios web reportados como falsos o atacantes.
- Es de gran importancia estar realizando copias de seguridad periódicamente a la información, para evitar daños. Dichas copias pueden almacenadas en discos duros externos, servicios de nube, entre otros. Cada una de ellas deben ser encriptados por seguridad.
- Restricciones sobre la instalación de software. Mediante directivas de restricción de software sobre los equipos integrados con los servicios de dominio de firewall y directiva de grupo se puede limitar el software a instalar en los equipos de la organización.

PTR:

- El empleado debe laboral en su sitio asignado, no debe transportar su equipo a ningún otro lado sin autorización.

- Los empleados deben mantener el entorno de su equipo limpio y sin humedad.
- Evitar colocar objeto encima del equipo o cubrir los orificios de ventilación.
- Solo el personal apropiado podrá llevar a cabo los servicios y reparaciones al equipo informático.
- Los empleados no deben extraer o copiar información sin autorización del jefe de área.

SoA:

- Los jefes de cada área vigilaran que los empleados cumplas con las políticas de seguridad establecidas.

- **A13- Seguridad en las comunicaciones**

Se pretende establecer medidas de seguridad técnicas de redes, equipos y sitios web, junto con la gestión segura de los soportes de información y los intercambios de información.

Políticas:

- Analizar periódicamente que información circula por la red evitando daños y ataques.
- Segmentar la red para prevenir la intrusión en la información, además se puede establecer límites de ancho de banda y permisos a los usuarios.
- Establecer controles para asegurar la disponibilidad, la confidencialidad y la integridad de la información.
- Hacer uso de la extensión FTP mediante SSL para el cifrado de datos, esto evita que al momento de realizar transferencias de información la reciba en binario y no en texto evitando el robo de información.

PTR:

- Para el uso del correo electrónico los empleados no deben de usar cuentas de correo electrónico asignadas a otras personas, ni recibir mensajes en cuentas de otros.
- Los empleados deben tratar los mensajes de correo electrónico y archivos adjuntos como información que es de propiedad de la organización.
- El acceso a internet es exclusivamente para actividades relacionadas con las actividades del empleo y funciones que desempeña.
- Debe ser informado y registrado cualquier equipo que pueda acceder a la red de la empresa.

SoA:

- El coordinador del departamento de sistemas debe controlar y administrar toda la red de acuerdo a las políticas de seguridad.

- **A14- Adquisición de sistemas, desarrollo y mantenimiento**

Debido a que para asegurar una correcta implementación de la seguridad es necesario una adecuada administración de la infraestructura base, es decir sistemas operativos, software para desarrollo y mantenimiento.

Políticas:

- Proteger los datos de prueba, es decir al momento de realizar pruebas de nuevos módulos o configuraciones en el desarrollo del software no utilizar datos reales por el contrario se deben anonimizar por seguridad.
- Solicitar una autorización formal para hacer una copia a toda la base de datos para con ella poder hacer pruebas.
- Al terminar las pruebas de desarrollo los datos deben ser eliminados inmediatamente.
- Al ingresar información el software desarrollo debe ser capaz de guiar al usuario y validar el tipo de dato que se esté ingresando. Se debe asegurar que los datos de entrada no contengan código malicioso que pueda alterar el correcto funcionamiento de la aplicación.
- Hacer una revisión técnica de las aplicaciones. Para que al momento de cambiar plataformas o actualizar software de operación no haya impacto adverso en el funcionamiento o la seguridad de la organización.

PTR:

- Realizar copias de la base de datos para realizar pruebas pero se deben anonimizar los datos.
- Hacer que las aplicaciones detecten de que el dato que se le está ingresando no contenga código malicioso y sea el correcto.
- Revisar e ir actualizando periódicamente las aplicaciones a software actual, para prevenir daños en su funcionamiento o la seguridad en la organización.

SoA:

- El personal en la coordinación de sistemas al momento de aplicar nuevas funciones o módulos a las plataformas de desarrollo propio tenga un servidor pequeño para poder realizar pruebas con una copia de la base de datos, para que al momento de implementarlo directamente al software no afecte en nada.

- **A15- Relación con los proveedores**

El principal objetivo de los controles definidos por esta sección es garantizar el nivel apropiado de seguridad de la información en los casos que se le realicen contratos con terceros o proveedores.

Políticas:

- Estipular clausulas en los contratos con los proveedores, en donde se acuerde todos los elementos de seguridad de la información a los cuales el proveedor pueda acceder, procesar, almacenar, comunicar o suministrar componentes o soporte a la infraestructura de tecnologías de la información del ITFIP.

PTR:

- En cada contrato de trabajo se deberá cláusulas de confidencialidad para asegurar información de la empresa.
- Todo contratista tercero que utilice los bienes y servicios informáticos se comprometen a conducirse bajo los principios de confidencialidad de la información.

SoA:

- Se implementará una política por parte del comité para los proveedores sobre la seguridad de la información teniendo en cuenta:
    - Requisitos del tratamiento de la información.
    - Acuerdos sobre el manejo de la información.
    - Seguimientos sobre la información de la empresa.

- **A16- Gestión de los incidentes de seguridad**

Con este dominio se busca asegurar un enfoque coherente y eficaz para la gestión de incidentes de seguridad de la información, incluida la comunicación sobre eventos de seguridad, debilidades y amenazas.

Políticas:

- Todo el personal de la organización, usuarios de los sistemas y terceros pueden fácilmente encontrar error o debilidades en la seguridad de la información que puede generar incidencia. Por lo tanto todos los que utilicen los servicios y sistemas de información están en la obligación de que observen y reporten cualquier debilidad de seguridad de la información.

- El líder del comité de seguridad debe establecer procesos adecuados, para los eventos tales como:
    - Violación de confidencialidad.
    - Uso inadecuado de los sistemas de información.
    - Fallas del sistema.
- Identificar la causa e implementar acciones correctivas y reportar todo el proceso realizado al responsable de la seguridad.
- El responsable, debe llevar un registro de los incidentes presentados, de cómo se han manejado, las posibles causas y cuanto le cuestan a la empresa resolverlos, para en un futuro no cometer los mismos errores.

PTR:

- Los empleados no deben instalar ningún programa tercero no autorizado por la organización en sus equipos de trabajo, para prevenir posibles amenazas a los sistemas de información.
- Se debe llevar un registro de los incidentes encontrados para mejorarlos y no volver a cometerlos.

SoA:

- Se debe establecer un documento con las políticas de seguridad, el cual deben conocer todos los empleados, además ser capacitados ante cualquier situación de amenaza a los sistemas de información.

- **A17- Continuidad del negocio**

Aquí se definen los controles con los cuales se busca contrarrestar los efectos de fallos o desastres que afecten el funcionamiento normal de los sistemas críticos de información.

Políticas:

- Garantizar la disponibilidad de las operaciones sin importar los fallos o desastres.
- Verificar la validez y efectividad de las medidas de continuidad. En el ITFIP se debe revisar los intervalos regulares de controles de continuidad de la seguridad de la información establecidos e implementados, con el fin de asegurar que son válidos y eficaces durante situación adversas.

PTR:

- Implementar modelos redundantes para garantizar alta disponibilidad en el sistema y así mitigar los fallos, reducir los tiempos de respuesta.

- Diseñar políticas de contingencias las cuales deben ser constantemente revisadas y actualizadas para asegurar que las medidas adoptadas son las más adecuadas.

SoA:

- El comité de seguridad de la información será el encargado de identificar los procesos vitales en la organización para así darle a conocer a los empleados la importancia y de los posibles riesgos.
- Elaborar en un documento una estrategia de continuidad del negocio y proponer la adquisición de pólizas y seguros, en caso de algún daño crítico.
- El comité de seguridad establecerá un cronograma de pruebas, el cual se señalará quienes son los responsables, efectuara pruebas, realizara simulaciones y pruebas completas en las instalaciones, involucrando procesos y con todo el personal.

- **A18- Cumplimiento con requerimientos legales y contractuales**

Con los controles seleccionados en el dominio A18 se tiene como principal objetivo evadir todos los incumplimientos de obligaciones legales o contractuales.

Políticas:

- Se deben definir y reconocer los requisitos legales y contractuales, así como el reglamento, en lo que respecta a la privacidad y la protección de los datos.
- Se deben determinar los procedimientos a seguir y de esta forma cumplir con la ley de protección intelectual (LPI), considerando la adquisición de software a través de fuentes confiables, la duplicidad de documentos sin que sea permitido por la ley de derechos de autor.

PTR:

- Determinar respectivos procedimientos para reconocer los requisitos legales y contractuales, con el fin de reconocer los activos que requieren protección de información de datos personales.
- Plantear políticas para el uso legal del software y generando las respectivas medidas en caso de las infracciones.

SoA:

- El comité definirá los procedimientos encaminados a cumplir con todas las normas y restricciones legales, se encargará de realizar revisiones periódicas a la empresa, para verificar el cumplimiento de las políticas de

seguridad, solicitar auditorias periódicas, documentar y dar a conocer los requisitos normativos.

- Todos los empleados y directivos están obligados a conocer y brindar apoyo a los que no conozcan para así hacer cumplir las presentes políticas y la normativa vigente.

27. CONCLUSIONES

- Al realizar la evaluación del estado actual del departamento de sistemas de acuerdo a la ISO/IEC 27001:2013 se encontraron que de los 14 dominios que propone la norma, muchos controles de seguridad no se cumplen. Lo cual genero preocupación debido a que la institución no está del todo capacitada ante cualquier amenaza que pueda afectar la información.
- Con la Metodología MAGERIT se desarrolló el análisis y gestión de riesgos en el departamento sistemas en donde se identificó de una forma más clara el nivel de seguridad que posee cada uno de los activos de información y así fueron identificados los riesgos y amenazas que los afectan. Por lo tanto se diseñó un plan de tratamiento de riesgos.
- De acuerdo a la declaración de aplicabilidad en donde se le exponen al rector del ITFIP de las políticas y mejoras de seguridad, en donde el acepta que la institución esta prematura en ese tema y está de acuerdo en ir aplicando poco a poco las políticas.
- Luego del exhaustivo análisis y gestión de riesgos en el departamento de sistemas, se exponen políticas y recomendaciones de seguridad que ayuden a solventar las amenazas que pueda afectar los activos de información.
- Se establecieron las salvaguardas que concederán en el momento de la implementación del SGSI proteger la seguridad de la dependencia y su información.
- Se identificaron mediante las entrevistas y el trabajo de campo a lo largo de la investigación que dentro de la dependencia existían procesos que no se encontraban documentados lo que provocaba falencias en la creación de planes de contingencias y salvaguardas.
- Se logró observar que dentro del departamento de sistemas de la institución no contaban con planes de contingencia y mitigación de riesgos ante posibles amenazas que se pudiera presentar en el día a día.

28. RECOMENDACIONES

- Es indispensable realizar una auditoría interna para diagnosticar el estado en algunos controles de seguridad que posiblemente no fueron tenidos en cuenta durante el diseño del SGSI o que surgieron posterior a este.
- Se recomienda a la institución realizar un análisis de gestión de seguridad de la información no solo centrado en la dependencia de sistemas; sino que este además abarqué todos los niveles de la institución y su alta dirección.
- Es indispensable que la institución predisponga un presupuesto amplio para así realizar investigaciones más a fondo que permitan mejorar las estrategias de seguridad que estas ya manejan.
- Incrementar las pruebas de seguridad de forma periódica no solo centrándose en la dependencia de sistemas sino abarcando también los demás niveles que componen la institución.
- Se deben vigilar los puntos de acceso a información física donde puedan ingresar personas no autorizadas y aislarlos de las instalaciones conocidas para así evitar la vulneración de la información y el mal uso de ella.
- Se recomienda sincronizar la hora y fecha de todos los servidores y sus sistemas para así no tener incongruencias de información e ingresos.
- Se deben crear canales privados de comunicación en segmentos de red aislados para él envió y tratamiento de información confidencial.
- La información de las aplicaciones usadas a través de la red debe protegerse y cifrarse desde el punto de envió hasta el punto de recepción.

29. BIBLIOGRAFÍA

[10] AGUIRRE JUAN Y ARISTIZABAL CATALINA. Diseño del Sistema de Gestión de Seguridad de la Información para el grupo empresarial la Ofrenda, 2013 [revisado 29 octubre 2018, Pág. 7]

[21] Ministerio de Administraciones Públicas de España. MAGERIT – Versión 3.0. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Madrid: Ministerio de Hacienda y Administraciones públicas, 2012. Pag 7 de 127. Administración electrónica.

[25] Arias, F. G. (2012). El Proyecto de Investigación. Introducción a la metodología científica. 5ta: Fidias G. Arias Odón. Pág. 60

[26] Hernández Sampieri, R., Fernández Collado, C. y Pilar Baptista L. (2010). Metodología de la investigación. México. Ed. Mc Graw Hill.

[27] Dirección general de modernización administrativa, P.e (2012). MAGERIT-versión 3.0 Metodología de análisis y gestión de riesgos de los sistemas de información Madrid.

[48] Ministerio de Administraciones Públicas de España. MAGERIT – Versión 3.0. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información libro I. Madrid: Ministerio de Hacienda y Administraciones públicas, 2012. Pag 9. Administración electrónica.

[55] Ministerio de Administraciones Públicas de España. MAGERIT – Versión 3.0. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Madrid: Ministerio de Hacienda y Administraciones públicas, 2012. Pag 12. Administración electrónica.

[79] ITFIP, Institución de Educación Superior. Manual de Procesos y Procedimientos "ITFIP" Versión N.º 5.0. Lugar de Publicación: Espinal-Tolima, diciembre de 2016. Pag: 15 [Consultado**:** 19 de septiembre de 2018].

[80] ITFIP, Institución de Educación Superior. Manual de Procesos y Procedimientos "ITFIP" Versión N. º 5.0. Lugar de Publicación: Espinal-Tolima, diciembre de 2016. Pag: 16 [Consultado**:** 19 de septiembre de 2018].

[82] ITFIP, Institución de Educación Superior. Manual de Procesos y Procedimientos "ITFIP" Versión N.º 5.0. Lugar de Publicación: Espinal-Tolima, diciembre de 2016. Pag: 23-44 [Consultado**:** 19 de septiembre de 2018].

[84] ITFIP, Institución de Educación Superior. Manual de Procesos y Procedimientos "ITFIP" Versión N.º 5.0. Lugar de Publicación: Espinal-Tolima, diciembre de 2016. Pag: 45-56 [Consultado**:** 19 de septiembre de 2018].

[86], Institución de Educación Superior. Manual de Procesos y Procedimientos "ITFIP" Versión N.º 5.0. Lugar de Publicación: Espinal-Tolima, diciembre de 2016. Pag: 57-78 [Consultado**:** 19 de septiembre de 2018].

[88] ITFIP, Institución de Educación Superior. Manual de Procesos y Procedimientos "ITFIP" Versión N.º 5.0. Lugar de Publicación: Espinal-Tolima, diciembre de 2016. Pág.: 79-104 [Consultado: 19 de septiembre de 2018].

[90] ITFIP, Institución de Educación Superior. Manual de Procesos y Procedimientos “ITFIP” Versión N.º 5.0. Lugar de Publicación: Espinal-Tolima, diciembre de 2016. Pág.: 105-118 [Consultado: 19 de septiembre de 2018].
[92] ITFIP, Institución de Educación Superior. Manual de Procesos y Procedimientos “ITFIP” Versión N.º 5.0. Lugar de Publicación: Espinal-Tolima, diciembre de 2016. Pág.: 119-137 [Consultado: 19 de septiembre de 2018].
[94] ITFIP, Institución de Educación Superior. Manual de Procesos y Procedimientos “ITFIP” Versión N.º 5.0. Lugar de Publicación: Espinal-Tolima, diciembre de 2016. Pág.: 138-153 [Consultado: 19 de septiembre de 2018].
[96] ITFIP, Institución de Educación Superior. Manual de Procesos y Procedimientos “ITFIP” Versión N.º 5.0. Lugar de Publicación: Espinal-Tolima, diciembre de 2016. Pág.: 154-168 [Consultado: 19 de septiembre de 2018].
[98] ITFIP, Institución de Educación Superior. Manual de Procesos y Procedimientos “ITFIP” Versión N.º 5.0. Lugar de Publicación: Espinal-Tolima, diciembre de 2016. Pág.: 169-186 [Consultado: 19 de septiembre de 2018].
[100] ITFIP, Institución de Educación Superior. Manual de Procesos y Procedimientos “ITFIP” Versión N.º 5.0. Lugar de Publicación: Espinal-Tolima, diciembre de 2016. Pág.: 187-233 [Consultado: 19 de septiembre de 2018].
[102] ITFIP, Institución de Educación Superior. Manual de Procesos y Procedimientos “ITFIP” Versión N.º 5.0. Lugar de Publicación: Espinal-Tolima, diciembre de 2016. Pág.: 234-264 [Consultado: 19 de septiembre de 2018].
[104] ITFIP, Institución de Educación Superior. Manual de Procesos y Procedimientos “ITFIP” Versión N.º 5.0. Lugar de Publicación: Espinal-Tolima, diciembre de 2016. Pág.: 265-310 [Consultado: 19 de septiembre de 2018].
[106] ITFIP, Institución de Educación Superior. Manual de Procesos y Procedimientos “ITFIP” Versión N.º 5.0. Lugar de Publicación: Espinal-Tolima, diciembre de 2016. Pág.: 311-323 [Consultado: 19 de septiembre de 2018].
[108] ITFIP, Institución de Educación Superior. Manual de Procesos y Procedimientos “ITFIP” Versión N.º 5.0. Lugar de Publicación: Espinal-Tolima, diciembre de 2016. Pág.: 324-336 [Consultado: 19 de septiembre de 2018].
[110] ITFIP, Institución de Educación Superior. Manual de Procesos y Procedimientos “ITFIP” Versión N.º 5.0. Lugar de Publicación: Espinal-Tolima, diciembre de 2016. Pág.: 337-346 [Consultado: 19 de septiembre de 2018].
[112] ITFIP, Institución de Educación Superior. Manual de Procesos y Procedimientos “ITFIP” Versión N.º 5.0. Lugar de Publicación: Espinal-Tolima, diciembre de 2016. Pág.: 347-371 [Consultado: 19 de septiembre de 2018].
[114] ITFIP, Institución de Educación Superior. Manual de Procesos y Procedimientos “ITFIP” Versión N.º 5.0. Lugar de Publicación: Espinal-Tolima, diciembre de 2016. Pág.: 372-389 [Consultado: 19 de septiembre de 2018].
[116] ITFIP, Institución de Educación Superior. Manual de Procesos y Procedimientos “ITFIP” Versión N.º 5.0. Lugar de Publicación: Espinal-Tolima, diciembre de 2016. Pág.: 390-401 [Consultado: 19 de septiembre de 2018].

30. WEBGRAFIA

CNIS 2018 VIII Congreso Nacional de Innovación y Servicios Públicos – Glosario Seguridad. [en línea], 2018 [revisado 29 octubre 2018]. Disponible en Internet: http://www.cnis.es/glosario-seguridad/

[8] ISO27001 – Sistema de Gestión de la Seguridad de la información. [en línea], 2018 [revisado 29 octubre 2018]. Pág.: 3 Disponible en Internet: http://www.iso27000.es/download/doc_sgsi_all.pdf

[9] CNIS 2018 VIII Congreso Nacional de Innovación y Servicios Públicos – Glosario Seguridad. [en línea], 2018 [revisado 29 octubre 2018]. Disponible en Internet: http://www.cnis.es/glosario-seguridad/

[11] Calidad y seguridad de la información y auditoría informática, disponible en internet en: http://earchivo.uc3m.es/bitstream/handle/10016/8510/proyectoEsmeralda.pdf;jsessionid=10850A53006DB846CED4EDCEDEDE1C40?sequence=1 [revisado 29 octubre 2018, Pág. 9]

[12] Lic. Yuniet Rojas Mesa, "De la gestión de información a la gestión del conocimiento", ACIMED, disponible en: http://scielo.sld.cu/scielo.php?pid=S1024-94352006000100002&script=sci_arttext&tlng=en

[13] ICONTEC, "NORMA TÉCNICA NTC-ISO/IEC COLOMBIANA 27001", UNAD, disponible en: http://intranet.bogotaturismo.gov.co/sites/intranet.bogotaturismo.gov.co/files/file/NTC-ISO-IEC%2027001.pdf

[14] Jonathan Antonio Hoyos Chaverra, Alejandro Valencia Arias, El papel de las TIC en el entorno organizacional de las Pymes, disponible en: https://revistas.itm.edu.co/index.php/trilogia/article/view/155

[15] Rubén Darío Carvajal herrera, "Seguridad Informática y de Información". Universidad Tecnológica de Bolívar, disponible en: https://biblioteca.utb.edu.co/notas/tesis/0065029.pdf

[16] Dinero-ciberseguridad, articulo- 9/5/2019 -"En solo tres meses Colombia sufrió 42 billones de intentos de ataques cibernéticos", disponible en: https://www.dinero.com/actualidad/articulo/cuantos-ataques-ciberneticos-recibe-colombia/276556.

[17] OEA-ASOBANCARIA, "Desafíos del riesgo cibernético en el sector financiero para Colombia y américa latina", disponible en: https://www.oas.org/es/sms/cicte/docs/Desafios-del-riesgo-cibernetico-en-el-sector-financiero-para-Colombia-y-America-Latina.pdf

[18] Juan Voutssas M, Preservación documental digital y seguridad informática, Centro Universitario de Investigaciones Bibliotecológicas de la UNAM, disponible en: http://www.scielo.org.mx/scielo.php?script=sci_arttext&pid=S0187-358X2010000100008

[19] Chilán González, I., Bolaños Burgos, F., Angulo Murillo, N., & García Murillo, G. R. (2019). ANÁLISIS DE ATAQUES RANSOMWARE EN SERVIDORES WEB, LINUX Y WINDOWS. UNESUM-Ciencias. Revista Científica Multidisciplinaria. ISSN

2602-8166, 2(3), 89-100. Recuperado a partir de http://186.101.39.22/index.php/unesumciencias/article/view/106

[20] Francisco Nicolás Solarte Solarte, Edgar Rodrigo Enriquez Rosero, Mirian del Carmen Benavides, Metodología de análisis y evaluación de riesgos aplicados a la seguridad informática y de información bajo la norma ISO/IEC 27001, disponible en: http://www.rte.espol.edu.ec/index.php/tecnologica/article/view/456

[23] Colciencias, tipología de proyectos de carácter científico, tecnológico o de innovación, disponible en: https://minciencias.gov.co/sites/default/files/upload/paginas/documento_de_tipologias_-_version_5_vf.pdf

[24] Gross, M. (2010). Conozca 3 tipos de investigación: Descriptiva, Exploratoria y Explicativa. Pensamiento Imaginativo. Blog. Recuperado el 02 de febrero del 2017. Disponible en: http://manuelgross. bligoo. com/conozca-3-tipos-de-investigaciondescriptivaexploratoria-y-explicativa.

[28] Mirabal Sarria y Maragoto Maragoto." Propuesta de una guía de seguridad informática integrada a la gestión de la calidad", Observatorio de la Economía Latinoamericana, Nº 164, 2012. Texto disponible en: http://www.eumed.net/cursecon/ecolat/cu/2012/. Citado: 17 de sept. de 18

[29] Juan José Caballero Romero. Etnometodología, Universidad Complutense. Texto disponible en:
http://www.reis.cis.es/REIS/PDF/REIS_056_06.pdf. Citado:17 de sept. de 18

[30] Juan Báez y Pérez de Tudela. Investigación cualitativa 2 edición, Libros profesionales de empresa 2009. Disponible en: https://books.google.com.co/books?id=Xmv-PJ9KtzsC&printsec=frontcover&dq=cualitativa&hl=es&sa=X&ved=0ahUKEwi23dCN_8PdAhVR3VMKHdYyDoIQ6AEIJzAA#v=onepage&q=cualitativa&f=false. Citado: 18 de sept. de 18

[31] Janett Yánez, Raiza Yánez, Auditorías, Mejora Continua y Normas ISO: factores clave para la evolución de las organizaciones, disponible en: https://www.redalyc.org/pdf/2150/215026158006.pdf

[32] ICONTEC, "NORMA TÉCNICA NTC-ISO/IEC COLOMBIANA 27001", UNAD, disponible en: http://intranet.bogotaturismo.gov.co/sites/intranet.bogotaturismo.gov.co/files/file/NTC-ISO-IEC%2027001.pdf

[33] Isotools. ISO 27001: La implementación de un Sistema de Gestión de Seguridad de la Información, Blogs SGSI, 2015. Texto disponible en: https://www.pmg-ssi.com/2015/01/iso-27001-la-implementacion-de-un-sistema-de-gestion-de-seguridad-de-la-informacion/. Citado: 17 de sept. de 18

[34] Purificación aguilera. Seguridad Informática, Google book. Disponible en: https://books.google.com.co/books?id=Mgvm3AYIT64C&printsec=frontcover&hl=es&source=gbs_ge_summary_r&cad=0#v=onepage&q&f=false. Citado:17 de sept. de 18

[35] GUTIERREZ, Camilo. Welivesecurity. MAGERIT: metodología práctica para gestionar riesgos, [Revisado 12 de Septiembre del 2018]. Disponible en Internet:

https://www.welivesecurity.com/la-es/2013/05/14/MAGERIT-metodologia-practica-para-gestionar-riesgos/

[36] Eduardo Martínez Estébanes, Juan Carlos García Cano, Gobierno de ti a través de Cobit 4.1 y cambios esperados en Cobit 5.0, disponible en: https://dialnet.unirioja.es/servlet/articulo?codigo=3823460

[37] AREIZA CORREA JUAN DANIEL, CARVAJAL RAIGOSA JULIAN MAURICIO, GOMEZ OCAMPO SEBASTIAN- universidad EAFIT-Definición de un cuadro de mando para la gestión de servicios de TI, que apoye la toma de decisiones en una empresa de servicios, aplicando los modelos de gobierno TI- disponible en internet: https://repository.eafit.edu.co/bitstream/handle/10784/2471/CarvajalRaigoza%2C%20Julian%20Mauricio_2009.pdf?sequence=1&isAllowed=y

[38] Eduardo Martínez Estébanes, Juan Carlos García Cano, Gobierno de ti a través de Cobit 4.1 y cambios esperados en Cobit 5.0, disponible en: https://dialnet.unirioja.es/servlet/articulo?codigo=3823460

[39] JULIÁN PÉREZ PORTO Y MARÍA MERINO. Publicado: 2014. Actualizado: 2016. Definicion.de: Definición de rediseño (https://definicion.de/rediseno/)

[40] RAE.REAL ACADEMIA ESPAÑOLA. Definición de Investigación, [Revisado 12 de Septiembre del 2018]. Disponible en Internet: http://dle.rae.es/?id=M3YxV5t

[41] JULIÁN PÉREZ PORTO Y ANA GARDEY. Publicado: 2008. Actualizado: 2008. Definicion.de: Definición de sistema de información (https://definicion.de/sistema-de-informacion/)

[43] RAE.REAL ACADEMIA ESPAÑOLA. Definición de Análisis, [Revisado 12 de Septiembre del 2018]. Disponible en Internet: http://dle.rae.es/?id=2Vga9Gy

[44] RAE.REAL ACADEMIA ESPAÑOLA. Definición de gestión, [actualizado en 2019]. Disponible en Internet: https://dle.rae.es/gesti%C3%B3n

[45] VIU. UNIVERSIDAD INTERNACIONAL DE VALENCIA. ¿Qué es la seguridad informática y cómo puede ayudarme?, [Revisado 12 de Septiembre del 2018]. Disponible en Internet: https://www.universidadviu.com/la-seguridad-informatica-puede-ayudarme/

[46] RAE.REAL ACADEMIA ESPAÑOLA. Definición de Recolectar, [Revisado 12 de Septiembre del 2018]. Disponible en Internet: http://dle.rae.es/srv/search?m=30&w=recolectar

[47] Tipología de los proyectos – Colciencias - disponible en: https://www.colciencias.gov.co/sites/default/files/upload/paginas/documento_de_tipologias_-_version_5_vf.pdf

[56] RAE.REAL ACADEMIA ESPAÑOLA. Definición de Software, [Revisado 12 de Septiembre del 2018]. Disponible en Internet: http://dle.rae.es/?id=YErlG2H

[57] RAE.REAL ACADEMIA ESPAÑOLA. [Definición de Hardware, actualizado en el 2019]. Disponible en Internet: https://dle.rae.es/hardware?m=form

[58] Yezid Camilo Guerrero Angulo, Robert Marcelo Tabagano Goyes, SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN (SGSI) BASADO EN LA NORMA ISO 27001 Y 27002 PARA LA UNIDAD DE INFORMATICA Y TELECOMUNICACIONES DE LA UNIVERSIDAD DE NARIÑO disponible en: http://biblioteca.udenar.edu.co:8085/atenea/biblioteca/90493.pdf

[59] Joseph Alexander Guamán Seis, DISEÑO DE UN SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN PARA INSTITUCIONES MILITARES, disponible en: https://bibdigital.epn.edu.ec/bitstream/15000/10439/3/CD-6187.pdf
[60] David Alejando García Hernández, Jeison Harley Ruiz Murillo, ANÁLISIS Y GESTIÓN DE RIESGOS EN EL MARCO DEL SGSI, BASADO EN LA METODOLOGÍA MAGERIT Y APOYADO EN UNA API WEB PARA SU EJECUCIÓN, disponible en: http://repositorios.rumbo.edu.co/handle/123456789/121311
[62] Nelson Alejando Yáñez Cáceres, SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN PARA LA SUBSECRETARIA DE ECONOMÍA Y EMPRESAS DE MENOR TAMAÑO, Universidad de Chile, disponible en: http://repositorio.uchile.cl/bitstream/handle/2250/147976/Sistema-de-gestion-de-seguridad-de-la-informacion-para-la-Subsecretaria-de-Economia-y-Empresas.pdf?sequence=1&isAllowed=y
[63] CARTAGENA, L. C. (17 de 12 de 1993). decisión 351. Obtenido de http://www.sice.oas.org/trade/junac/decisiones/Dec351s.asp
[64] COLOMBIA, E. P. (23 de 6 de 1989). *Decreto 1360 de 1989 Nivel Nacional*. Obtenido de http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=10575
[65] Colombia, E. C. (5 de 2 de 1993). Ley 44 de 1993 Nivel Nacional. Recuperado el 26 de 5 de 2018, de http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=3429
[66] COLOMBIA, E. P. (16 de 3 de 1995). Decreto 460 de 1995 Nivel Nacional. Recuperado el 26 de 5 de 2018, de http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=10576
[67] COLOMBIA, E. P. (22 de 1 de 1996). Decreto 162 de 1996 Nivel Nacional. Obtenido de http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=10574
[68] COLOMBIA, E. C. (31 de 12 de 1999). LEY 545 DE 1999. Recuperado el 26 de 5 de 2018, de http://propiedadintelectual.unal.edu.co/fileadmin/recursos/innovacion/docs/normatividad_pi/ley545_1999.pdf
[69] Colombia, E. C. (8 de 2 de 2000). LEY 565 DE 2000. Recuperado el 26 de 5 de 2018, de https://www.ins.gov.co/Normatividad/Leyes/LEY%200565%20DE%202000.pdf
[70] Colombia, E. C. (27 de 7 de 2000). LEY 603 DE 2000. Recuperado el 26 de 5 de 2018, de http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=13960
[71] COLOMBIA, E. C. (30 de 4 de 2018). LEY 719 DE 2001. Recuperado el 26 de 5 de 2018, de http://www.secretariasenado.gov.co/senado/basedoc/ley_0719_2001.html
[72] Andina, C. d. (1 de 12 de 2000). DECISIÓN 486: Régimen Común sobre Propiedad Industrial *. Recuperado el 26 de 5 de 2018, de http://www.sice.oas.org/Trade/Junac/Decisiones/dec486si.asp
[73] República, P. d. (13 de 12 de 2000). Decreto 2591 de 2000. Recuperado el 26 de 5 de 2018, de http://hdl.handle.net/11520/13737

[74] COLOMBIA, E. C. (2018 de 4 de 30). LEY 463 DE 1998. Recuperado el 26 de 5 de 2018, de http://www.secretariasenado.gov.co/senado/basedoc/ley_0463_1998.html

[75] COLOMBIA, E. C. (30 de 4 de 2018). LEY 178 DE 1994. Recuperado el 26 de 5 de 2018, de http://www.wipo.int/edocs/lexdocs/laws/es/co/co073es.pdf

[76] Colombia, E. C. (18 de 8 de 1999). Ley 527 de 1999 Nivel Nacional. Recuperado el 26 de 5 de 2018, de https://www.ambitojuridico.com/noticias/tic/uso-de-medios-electronicos-i-la-ley-527-de-1999-como-instrumento-normativo-suficiente

[77] EL CONGRESO DE LA REPUBLICA DE COLOMBIA DECRETA. Ley 1273 de 2009 [En línea]. Bogotá. 2009., 1 p. disponible en http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=34492

[78] EL CONGRESO DE LA REPUBLICA DE COLOMBIA DECRETA. Ley 1266 de 2008 [En línea]. Bogotá. 2008., 1 p. disponible en http://www.redipd.org/legislacion/common/legislacion/Colombia/LEY_1266_31_12_2008_HabeasData_COLOMBIA.pdf

[81] ITFIP, Institución de Educación Superior. Caracterización de Proceso "Direccionamiento estratégico". Lugar de Publicación: Espinal-Tolima, diciembre de 2016. Pag: 1 [Consultado**:** 26 de septiembre de 2018]. Disponible en Internet: https://www.itfip.edu.co/images/2015/CARACTERIZACION-DIRECCIONAMIENTO-ESTRATEGICO-2015.pdf

[83] ITFIP, Institución de Educación Superior. Control Interno. Lugar de Publicación: Espinal-Tolima, diciembre de 2016. [Consultado: 26 de septiembre de 2018]. Disponible en Internet: http://www.itfip.edu.co/institucional/estructura-administrativa/control-interno.html

[85] ITFIP, Institución de Educación Superior. Gestión Jurídica. Lugar de Publicación: Espinal-Tolima, diciembre de 2016. [Consultado: 26 de septiembre de 2018]. Disponible en Internet: http://www.itfip.edu.co/institucional/estructura-administrativa/gestion-juridica.html

[87] ITFIP, Institución de Educación Superior. Caracterización de proceso. Lugar de Publicación: Espinal-Tolima, noviembre de 2014. [Consultado: 27 de septiembre de 2018]. Disponible en Internet: http://www.itfip.edu.co/images/2014/CARACTERIZACION%20DOCENCIA%20%202014.pdf

[89] ITFIP, Institución de Educación Superior. Caracterización de procesos "ITIFP". Lugar de Publicación: Espinal-Tolima, noviembre de 2015. [Consultado: 26 de septiembre de 2018]. Disponible en Internet: https://itfip.edu.co/images/2015/CARACTERIZAION-INVESTIGACION-2015.pdf

[91] ITFIP, Institución de Educación Superior. Caracterización de procesos "ITIFP". Lugar de Publicación: Espinal-Tolima, noviembre de 2015. [Consultado: 26 de septiembre de 2018]. Disponible en Internet: https://www.itfip.edu.co/images/2015/CARACTERIZACION-PROYECCION-SOCIAL-2015.pdf

[93] ITFIP, Institución de Educación Superior. Caracterización de procesos "ITIFP". Lugar de Publicación: Espinal-Tolima, noviembre de 2015. [Consultado: 26 de septiembre de 2018]. Disponible en Internet:

http://www.itfip.edu.co/procesos-academicos/oficina-de-admisiones-registro-y-control-academico.html

[95] ITFIP, Institución de Educación Superior. Caracterización de procesos “ITIFP”. Lugar de Publicación: Espinal-Tolima, noviembre de 2015. [Consultado: 26 de septiembre de 2018]. Disponible en Internet: http://www.itfip.edu.co/institucional/estructura-administrativa/vicerrectoria-academica/bienestar-universitario

[97] ITFIP, Institución de Educación Superior. Caracterización de procesos “ITIFP”. Lugar de Publicación: Espinal-Tolima, noviembre de 2015. [Consultado: 26 de septiembre de 2018]. Disponible en Internet: https://itfip.edu.co/images/2014/CARACTERIZACION%20SERVICIOS%20ACADEMICOS%202014.pdf

[99] ITFIP, Institución de Educación Superior. Caracterización de procesos “ITIFP”. Lugar de Publicación: Espinal-Tolima, noviembre de 2015. [Consultado: 26 de septiembre de 2018]. Disponible en Internet: https://www.itfip.edu.co/images/2015/CARACTERIZACION-GESTION-ADMINISTRATIVA-2015.pdf

[101] ITFIP, Institución de Educación Superior. Caracterización de procesos “ITIFP”. Lugar de Publicación: Espinal-Tolima, noviembre de 2015. [Consultado: 26 de septiembre de 2018]. Disponible en Internet: http://www.itfip.edu.co/institucional/estructura-administrativa/vicerrectoria-administrativa/gestion-financiera/almacen

[103] ITFIP, Institución de Educación Superior. Caracterización de procesos “ITIFP”. Lugar de Publicación: Espinal-Tolima, noviembre de 2015. [Consultado: 26 de septiembre de 2018]. Disponible en Internet: http://www.itfip.edu.co/institucional/estructura-administrativa/vicerrectoria-administrativa/gestion-talento-humano.htm

[105] ITFIP, Institución de Educación Superior. Caracterización de procesos “ITIFP”. Lugar de Publicación: Espinal-Tolima, noviembre de 2015. [Consultado: 26 de septiembre de 2018]. Disponible en Internet: http://www.itfip.edu.co/institucional/estructura-administrativa/vicerrectoria-administrativa/gestion-talento-humano/salud-ocupacional

[107] ITFIP, Institución de Educación Superior. Caracterización de procesos “ITIFP”. Lugar de Publicación: Espinal-Tolima, noviembre de 2015. [Consultado: 26 de septiembre de 2018]. Disponible en Internet: https://www.itfip.edu.co/images/2015/CARACTERIZACION-GESTION-FINANCIERA-2015.pdf

[109] ITFIP, Institución de Educación Superior. Caracterización de procesos “ITIFP”. Lugar de Publicación: Espinal-Tolima, noviembre de 2015. [Consultado: 26 de septiembre de 2018]. Disponible en Internet: https://www.itfip.edu.co/images/2015/CARACTERIZACION-GESTION-ADMINISTRATIVA-2015.pdf

[111] ITFIP, Institución de Educación Superior. Caracterización de procesos “ITIFP”. Lugar de Publicación: Espinal-Tolima, noviembre de 2015. [Consultado: 26 de septiembre de 2018]. Disponible en Internet:

http://www.itfip.edu.co/institucional/estructura-administrativa/vicerrectoria-administrativa/gestion-financiera/tesoreria

[113] ITFIP, Institución de Educación Superior. Caracterización de procesos “ITIFP”. Lugar de Publicación: Espinal-Tolima, noviembre de 2015. [Consultado: 26 de septiembre de 2018]. Disponible en Internet: http://www.itfip.edu.co/institucional/estructura-administrativa/vicerrectoria-administrativa/gestion-financiera/contabilidad

[115] ITFIP, Institución de Educación Superior. Caracterización de procesos “ITIFP”. Lugar de Publicación: Espinal-Tolima, noviembre de 2015. [Consultado: 26 de septiembre de 2018]. Disponible en Internet: https://www.itfip.edu.co/images/Institucional/ADMINISTRACIONDERIESGOSGESTIONDECALIDAD2014.pdf

[117] ITFIP, Institución de Educación Superior. Manual de Procesos y Procedimientos “ITFIP” Versión N.º 5.0. Lugar de Publicación: Espinal-Tolima, diciembre de 2016. Pág.: 402-432 [Consultado: 19 de septiembre de 2018].

[118] MAGERIT V3, Libro 3: Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información.

ANEXO 1

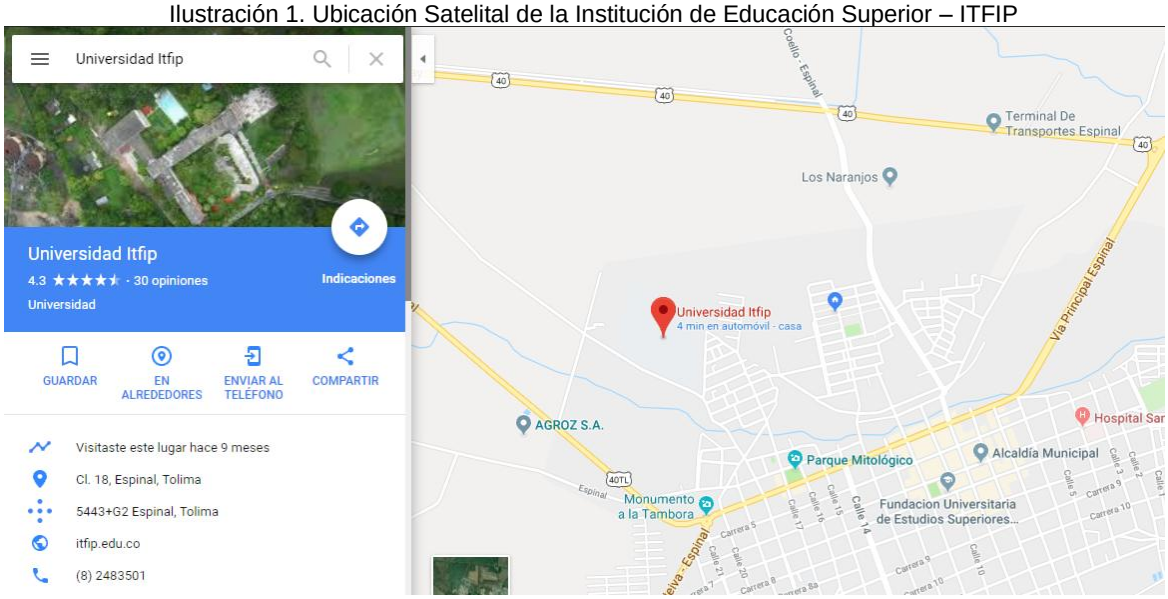
CONTENIDO

INDICE DE TABLAS

TABLA DE ILUSTRACIONES

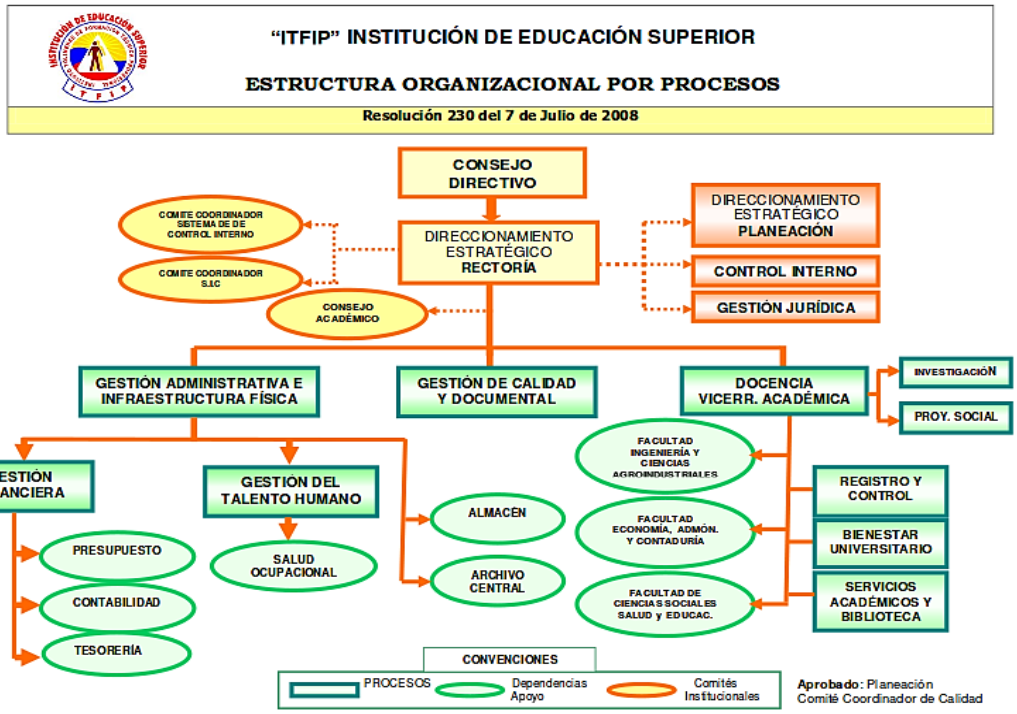
1. ILUSTRACIONES DE LOS PROCSOS DEL ITFIP

Ilustración 1. Ubicación Satelital de la Institución de Educación Superior – ITFIP



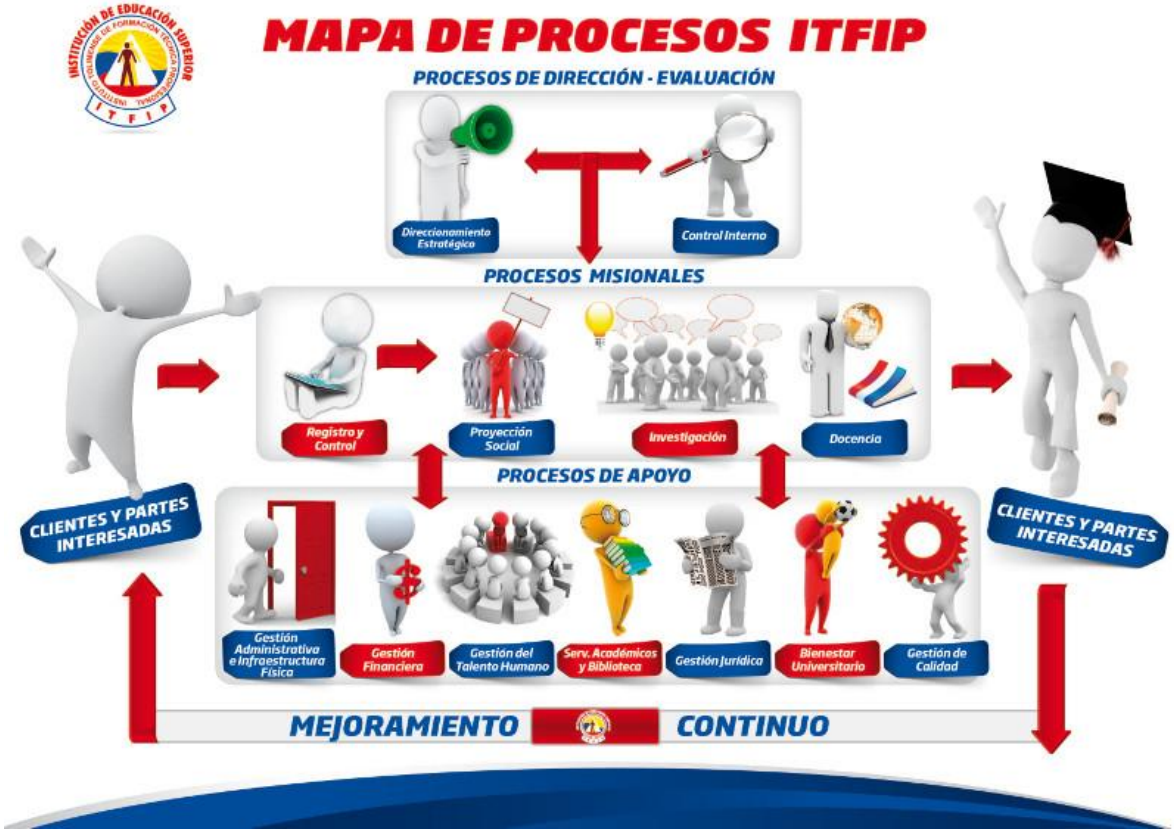
Fuente: Google Maps.

Ilustración 2. Estructura Organizacional por Procesos del ITFIP



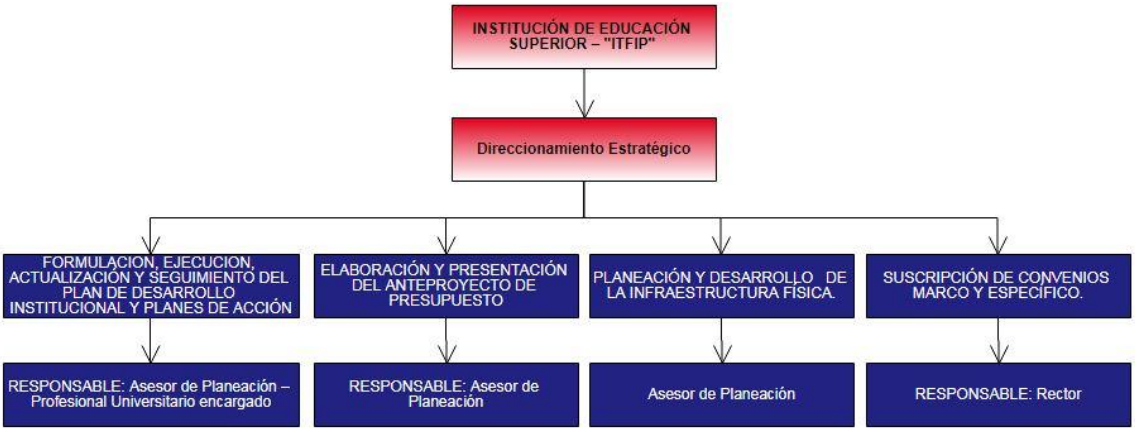
Fuente: http://www.ITFIP.edu.co/images/Institucional/Estructura.png

Ilustración 3. Mapa de Procesos del ITFIP



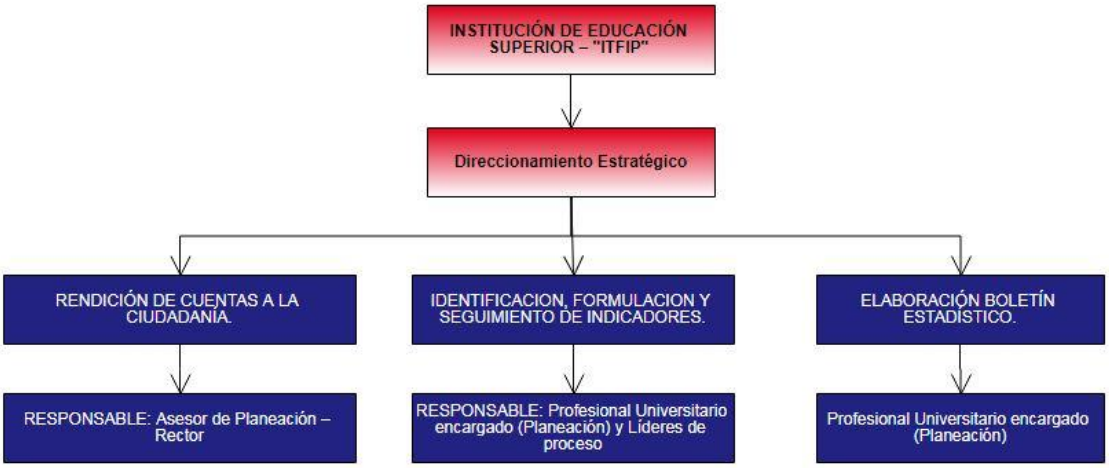
Fuente: http://www.ITFIP.edu.co/images/Institucional/Mapa_de_ProcesosITFIP1.jpg

Ilustración 4. Procesos Dependencia "Direccionamiento Estratégico"



Fuente: Autoría propia.

Ilustración 5. Procesos Dependencia "Direccionamiento Estratégico"

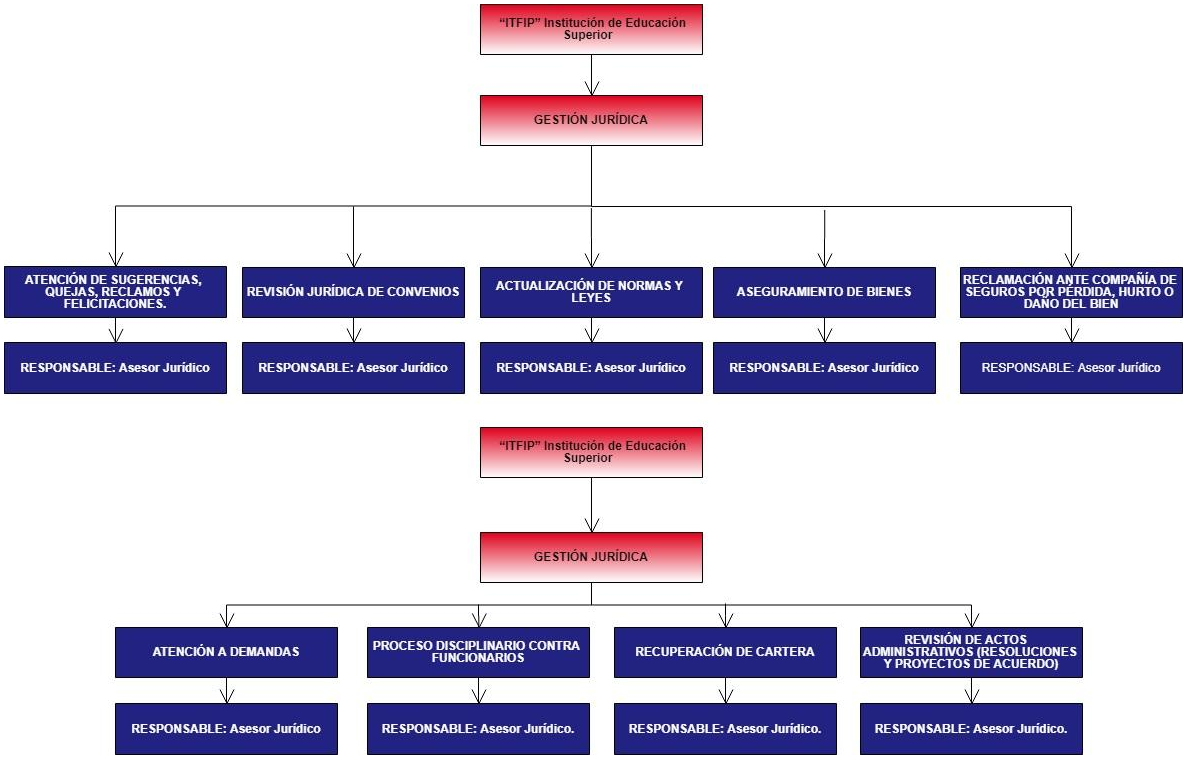


Fuente: Autoría propia.

Ilustración 6. Procesos Dependencia "Control Interno"

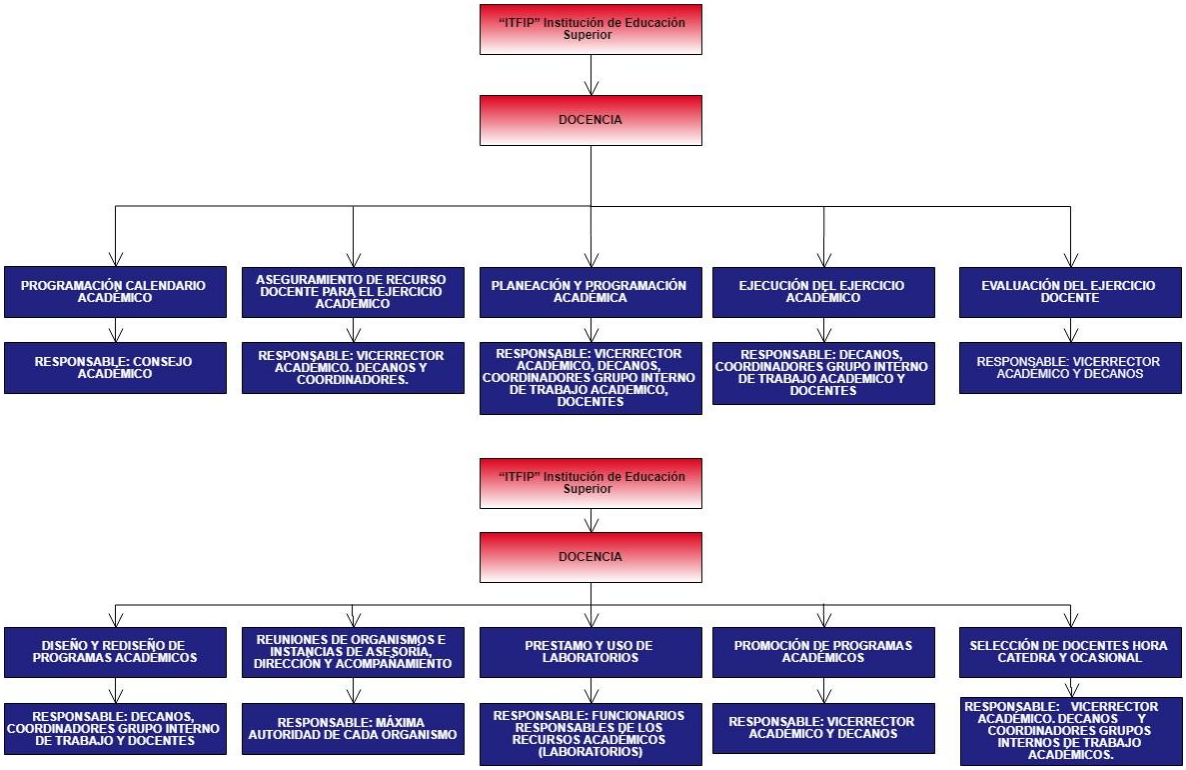
Fuente: Autoría Propia.

Ilustración 7. Procesos Dependencia "Gestión Jurídica"



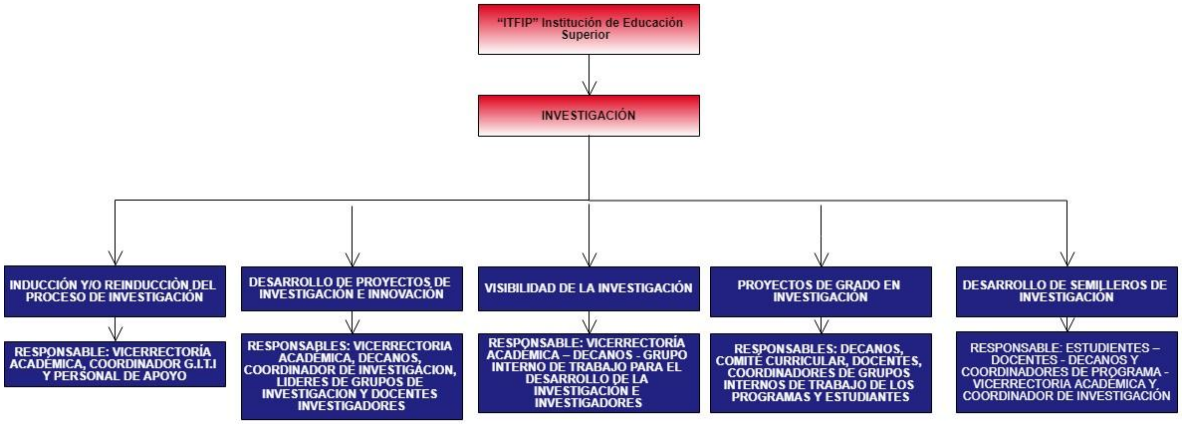
Fuente: Autoría Propia.

Ilustración 8.Procesos Dependencia "Docencia"



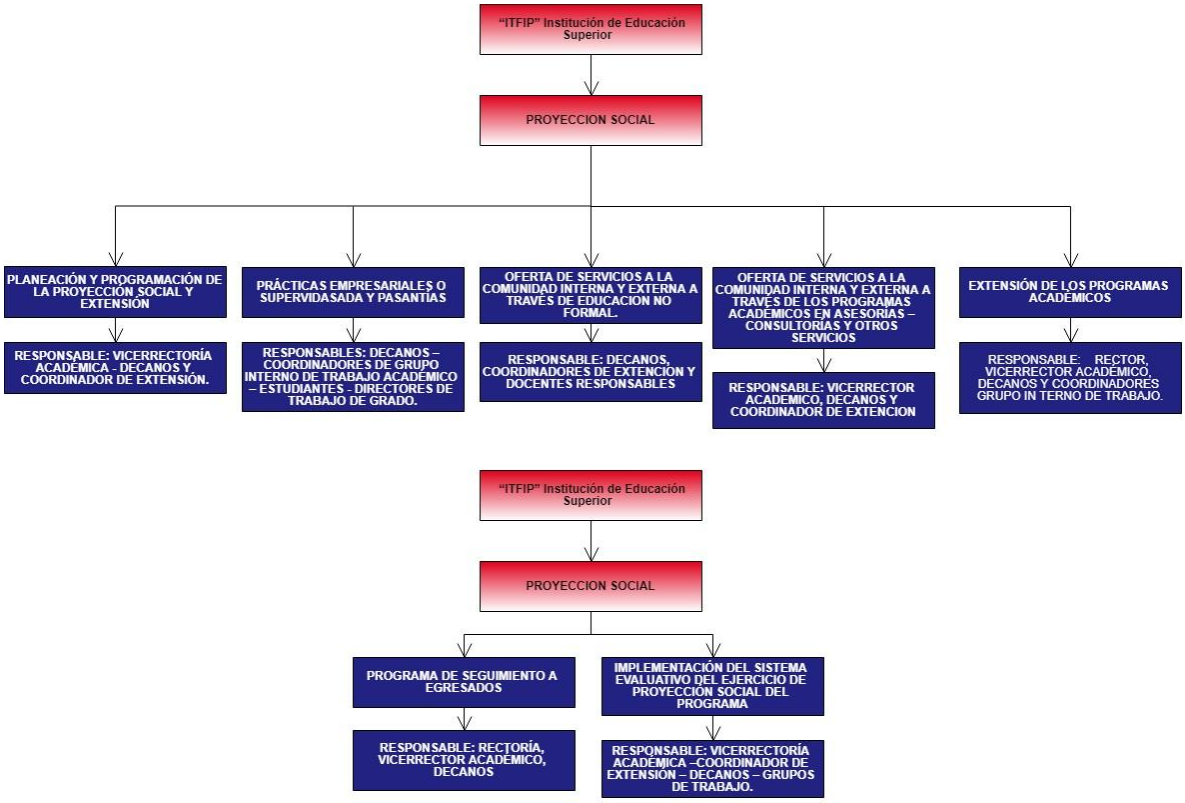
Fuente: Autoría Propia

Ilustración 9. Procesos Dependencia "Investigación"



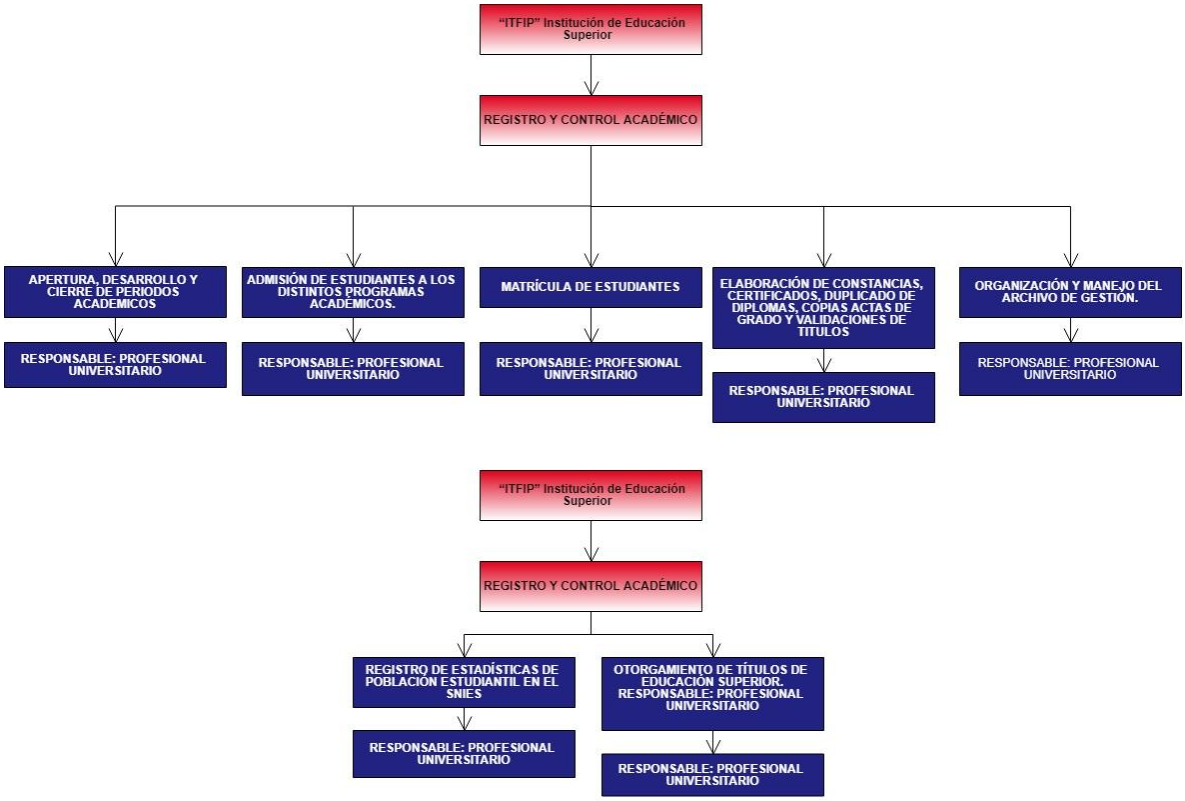
Fuente: Autoría Propia

Ilustración 10.Procesos Dependencia "Proyección Social”



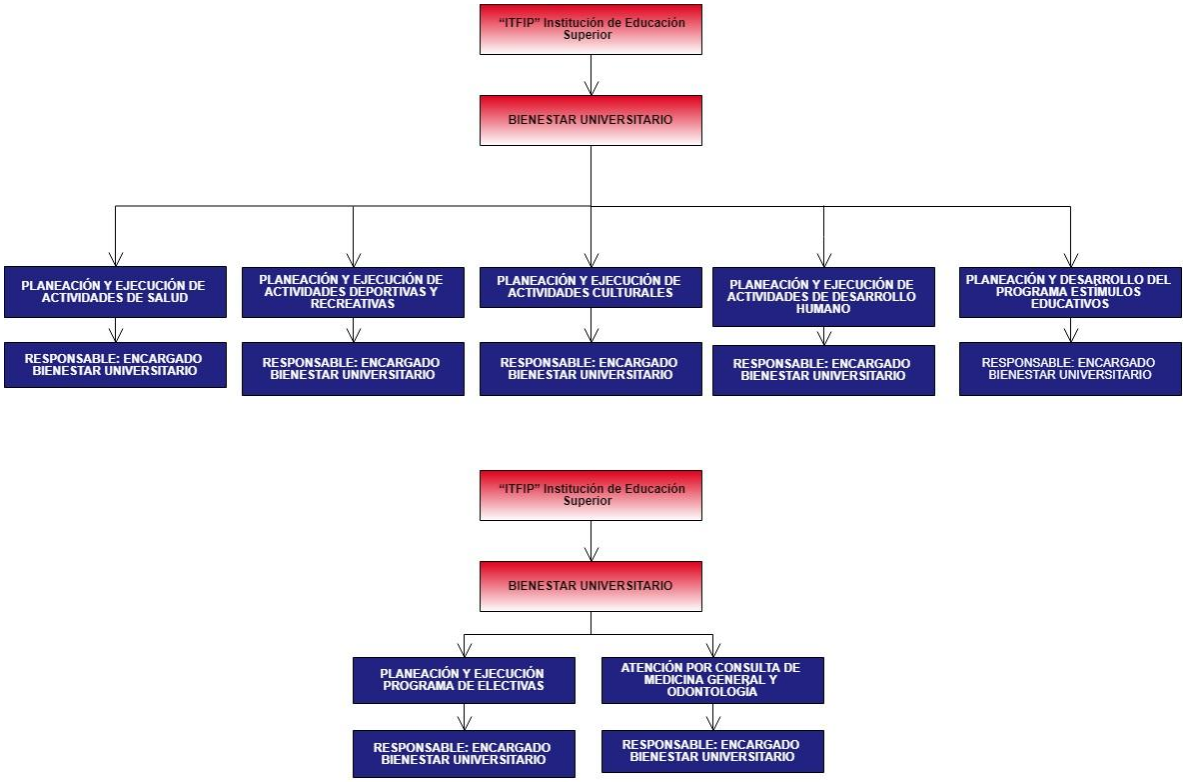
Fuente: Autoría Propia.

Ilustración 11. Procesos Dependencia "Registro y Control Académico”



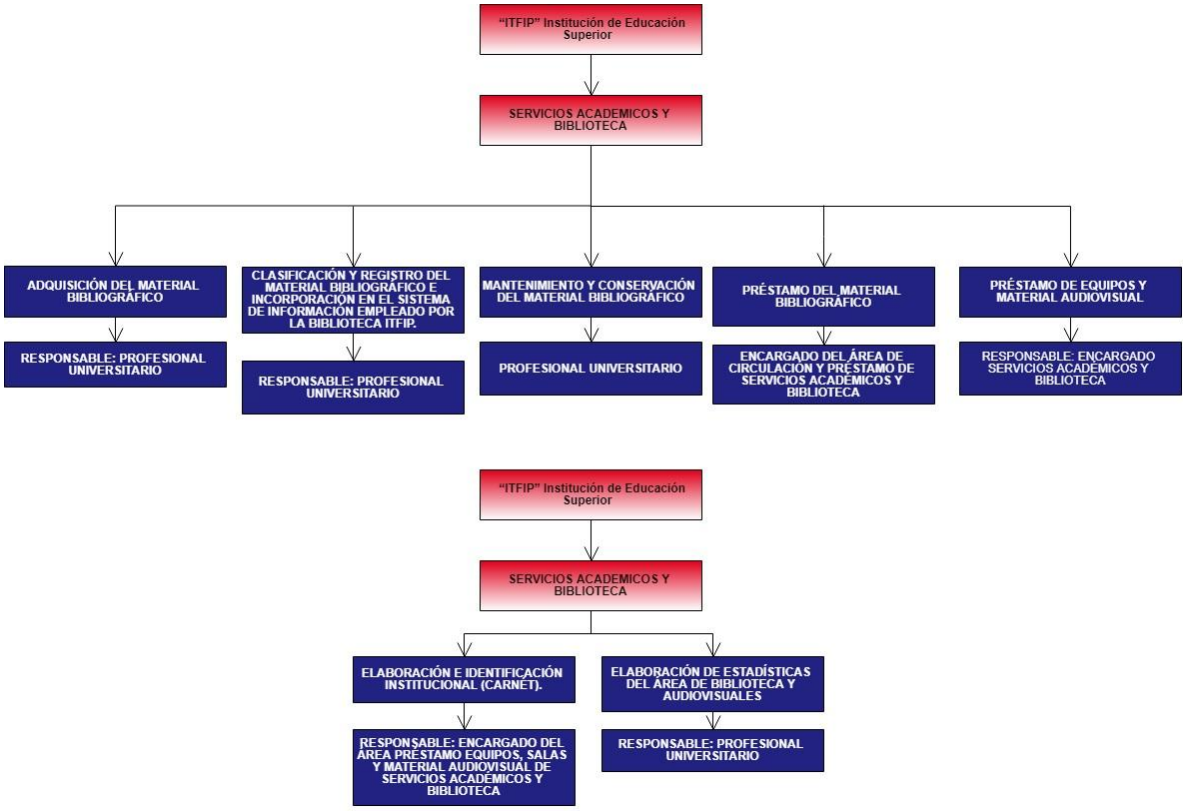
Fuente: Autoría Propia.

Ilustración 12. Procesos Dependencia "Bienestar Universitario”



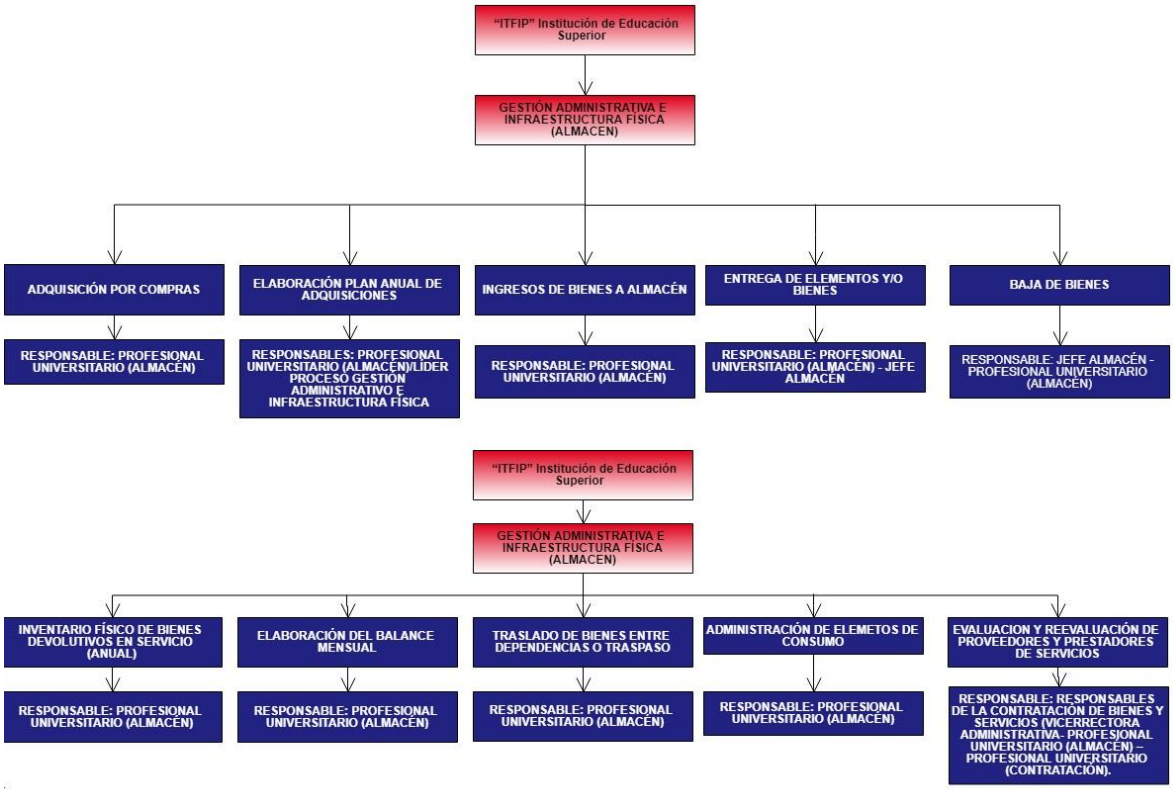
Fuente: Autoría Propia.

Ilustración 13.Procesos Dependencia "Servicios Académicos y Biblioteca”



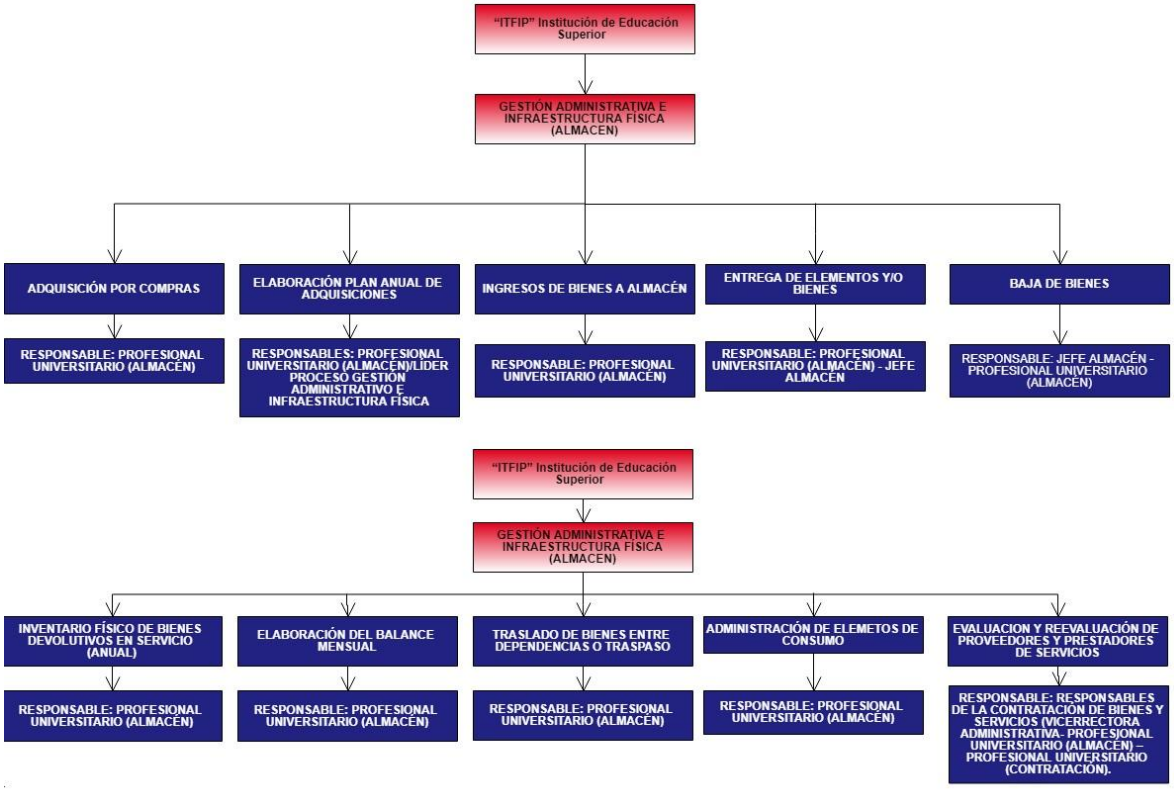
Fuente: Autoría Propia.

Ilustración 14. Procesos Dependencia "Gestión Administrativa e Infraestructura Física"



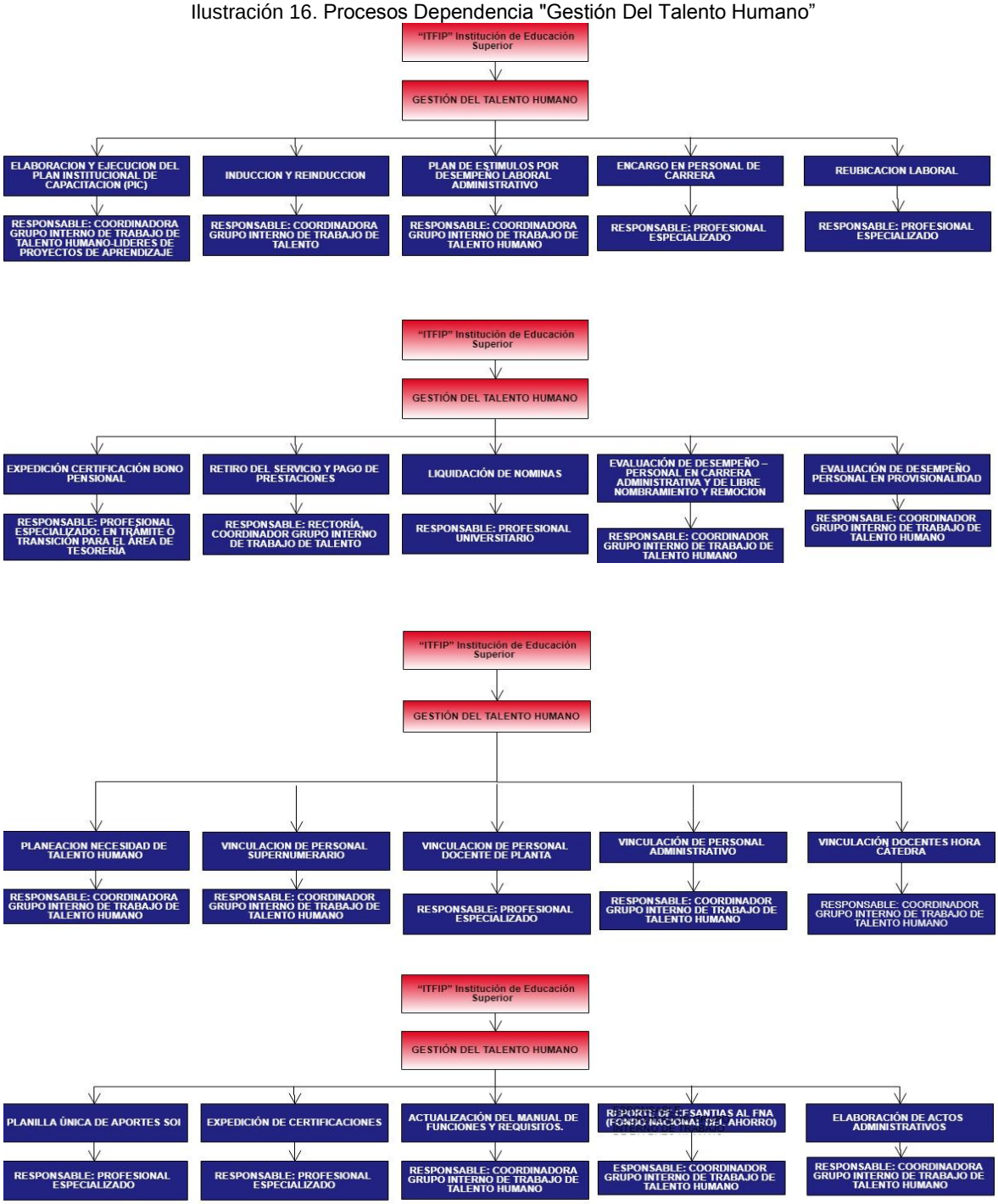
Fuente: Autoría Propia.

Ilustración 15. Procesos Dependencia "Gestión Administrativa e Infraestructura Física (Almacén)"



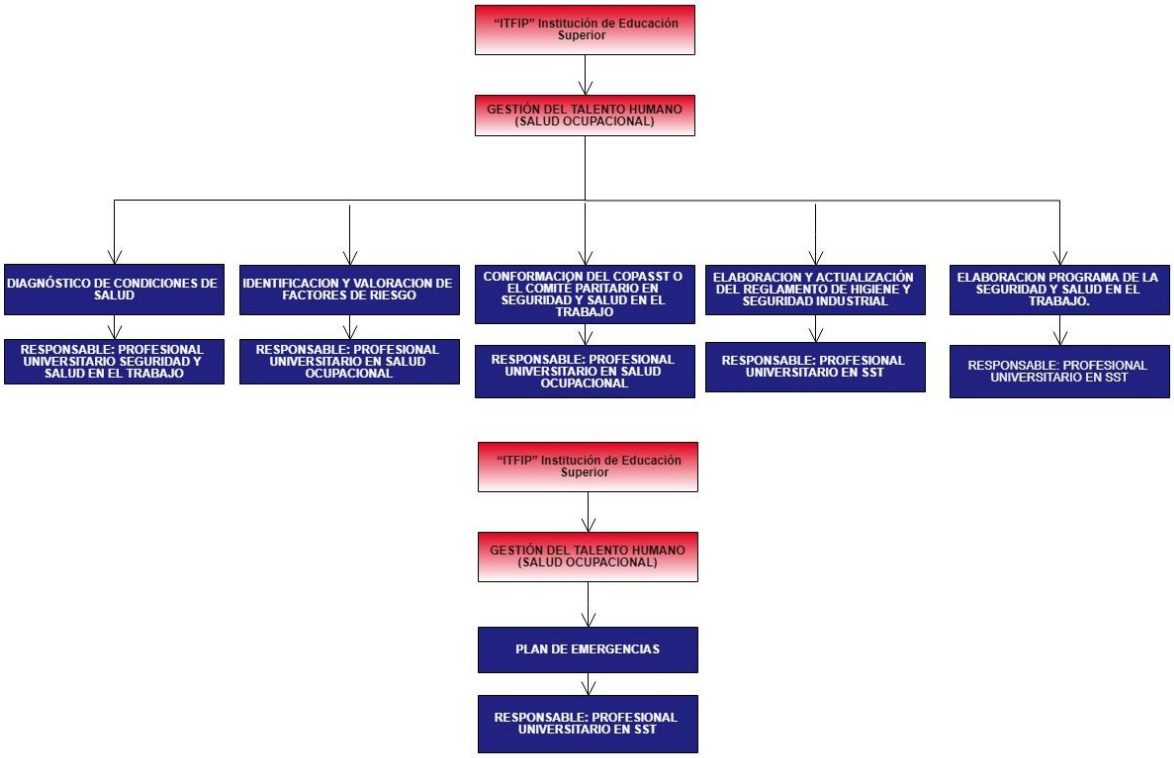
Fuente: Autoría Propia.

Ilustración 16. Procesos Dependencia "Gestión Del Talento Humano"



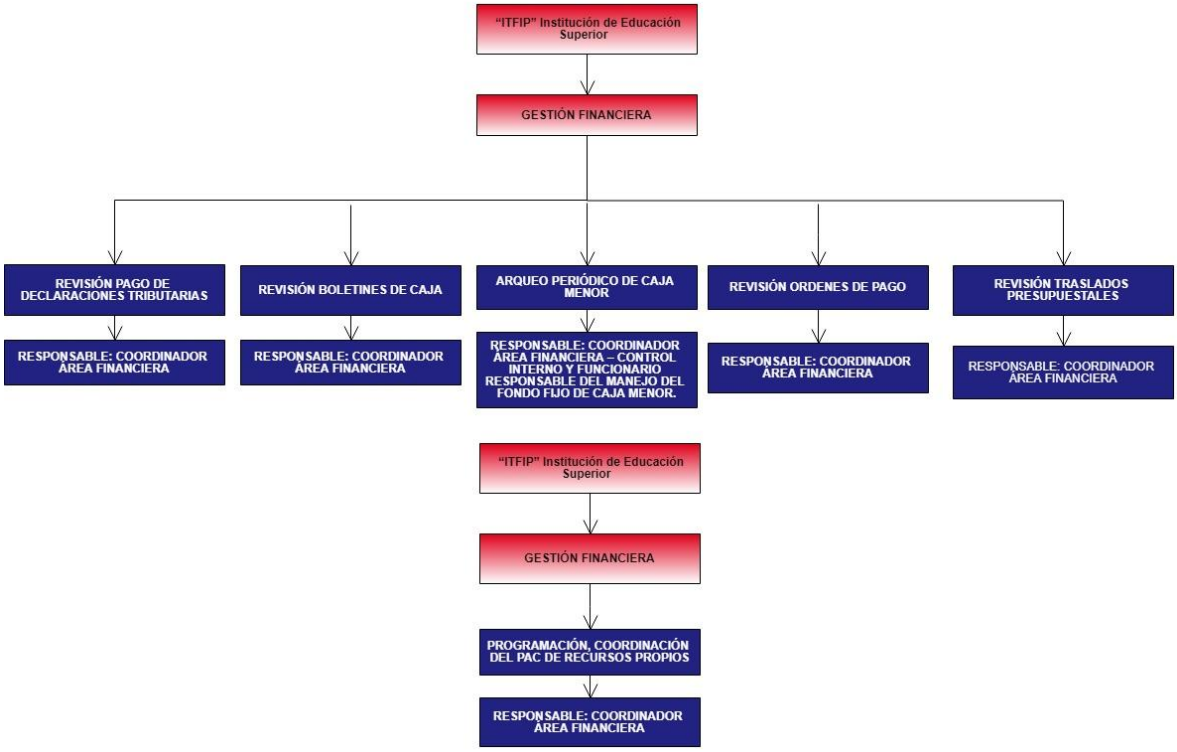
Fuente: Autoría Propia.

Ilustración 17. Procesos Dependencia "Gestión Del Talento Humano (Salud Ocupacional)"



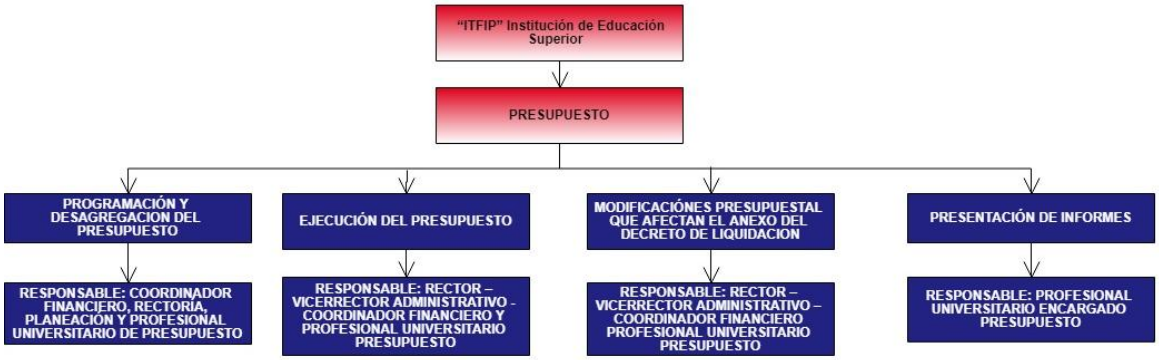
Fuente: Autoría Propia.

Ilustración 18. Procesos Dependencia "Gestión Financiera”



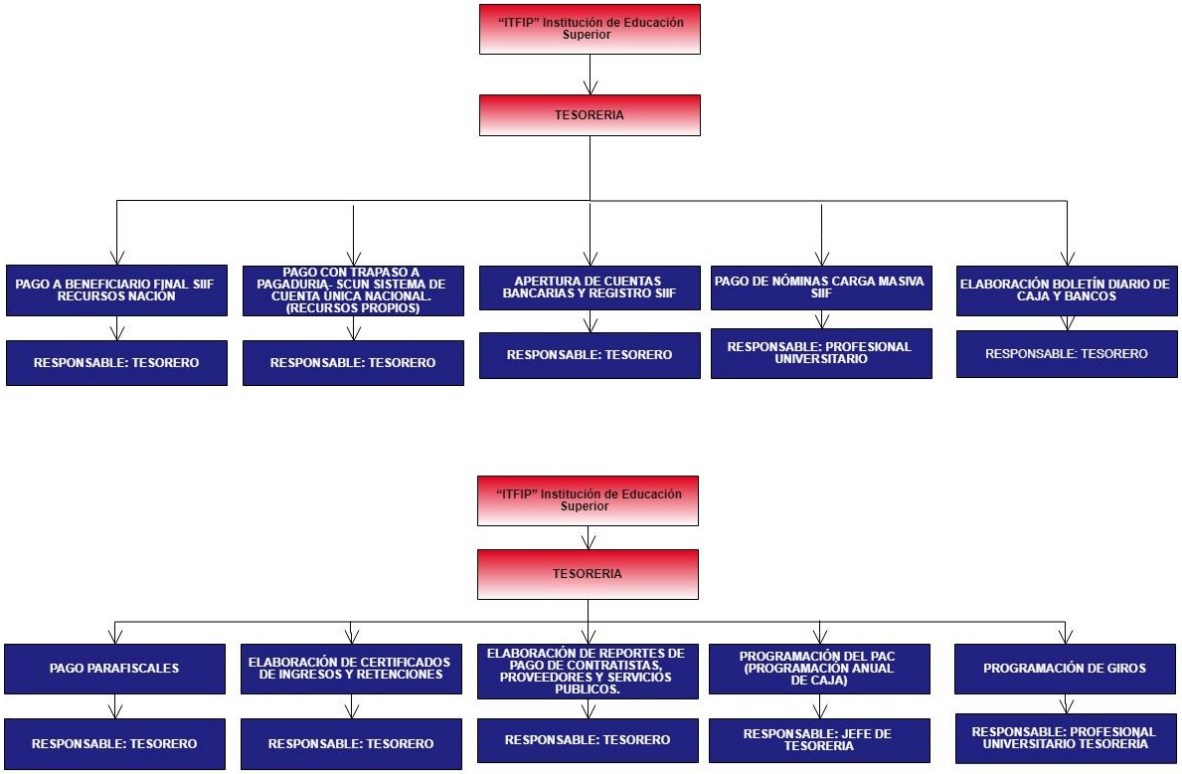
Fuente: Autoría Propia.

Ilustración 19. Procesos Dependencia "Presupuesto”



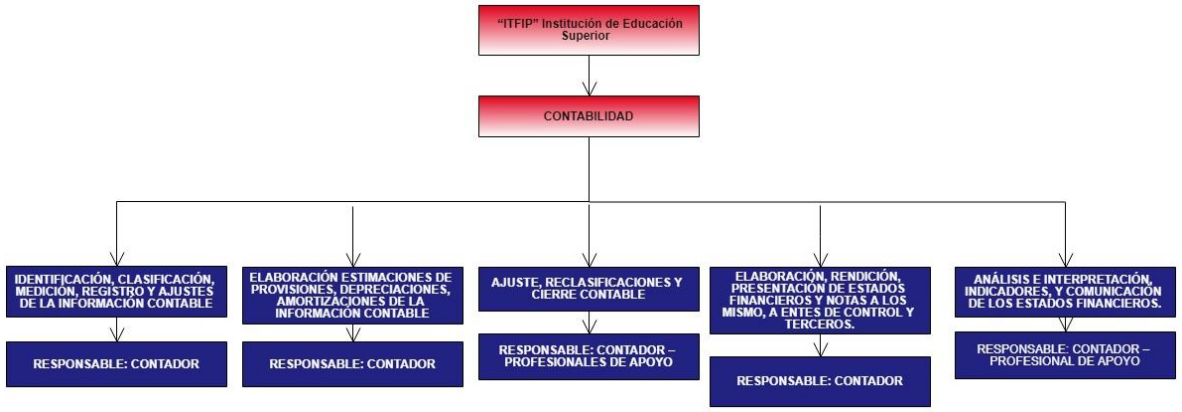
Fuente: Autoría Propia.

Ilustración 20. Procesos Dependencia "Tesorería”



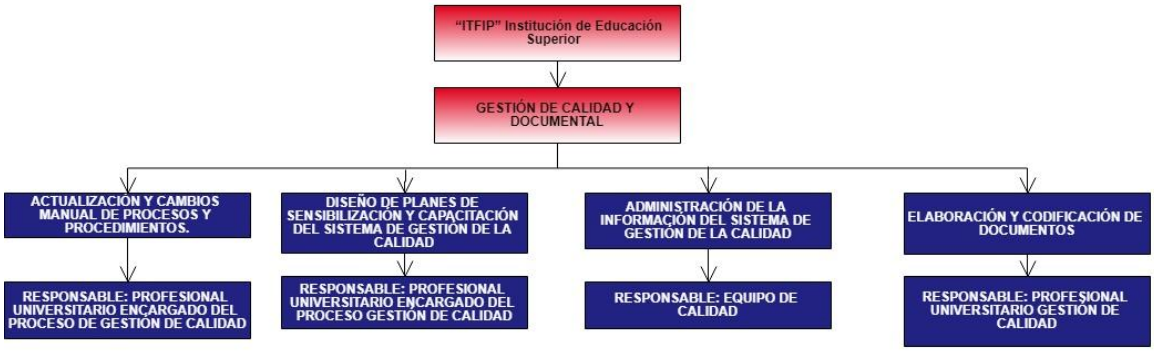
Fuente: Autoría Propia.

Ilustración 21.Procesos Dependencia "Contabilidad”



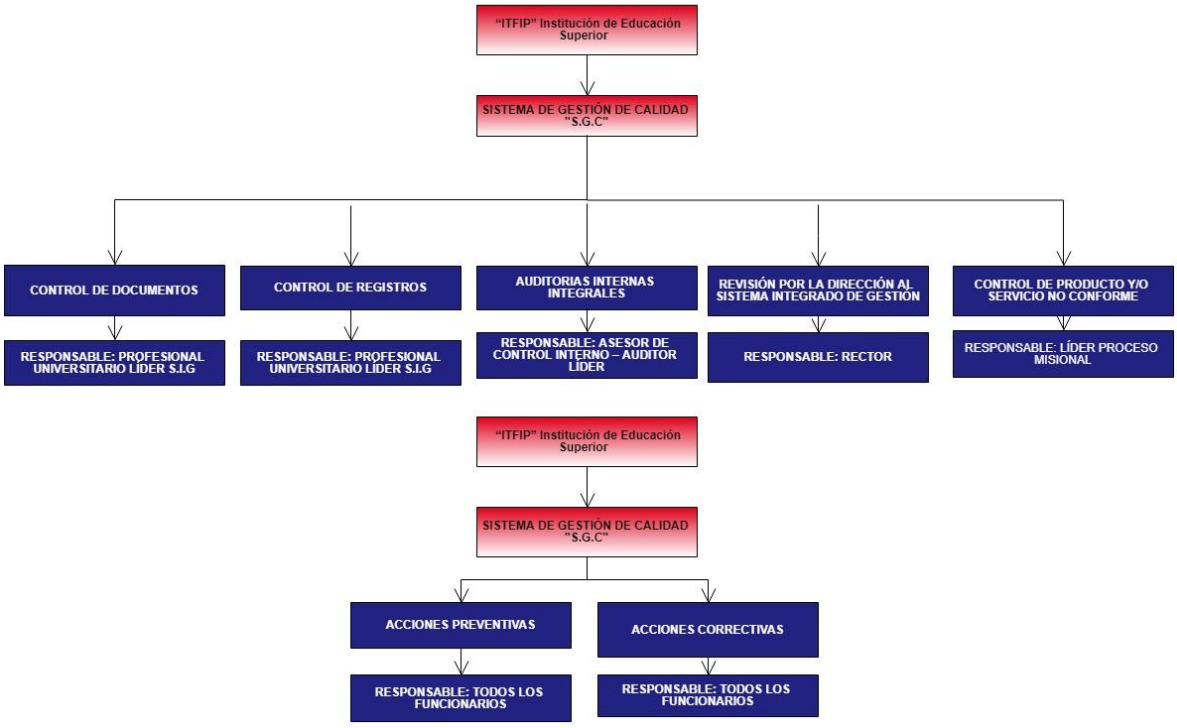
Fuente: Autoría Propia.

Ilustración 22. Procesos Dependencia "Gestión De Calidad Y Documental”



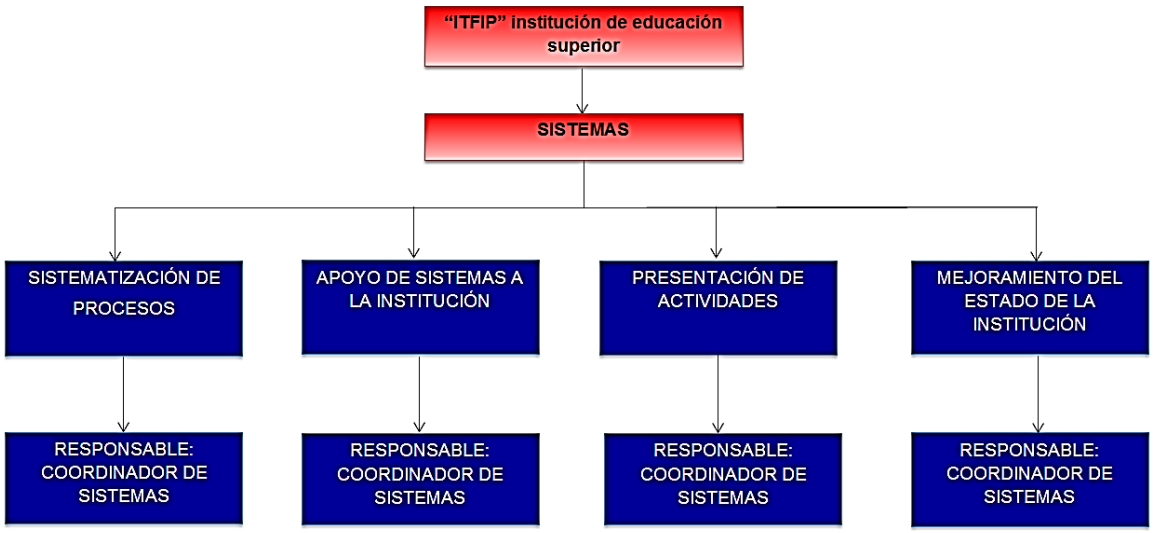
Fuente: Autoría Propia.

Ilustración 23.Procesos Dependencia "Sistema de gestión de calidad del S.G.C”



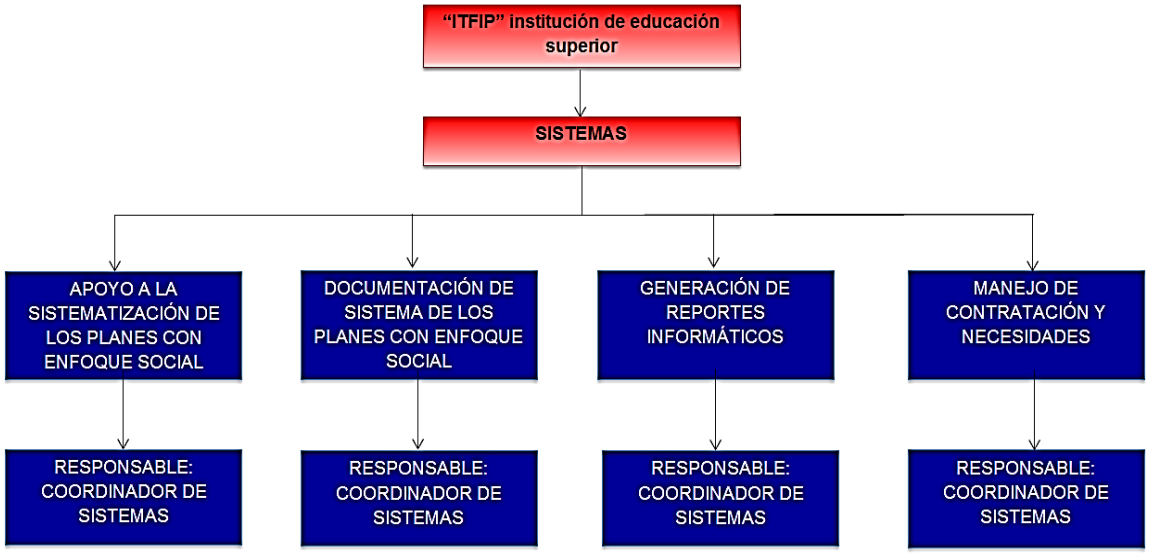
Fuente: Autoría Propia

Ilustración 24. Procesos Dependencia de sistemas



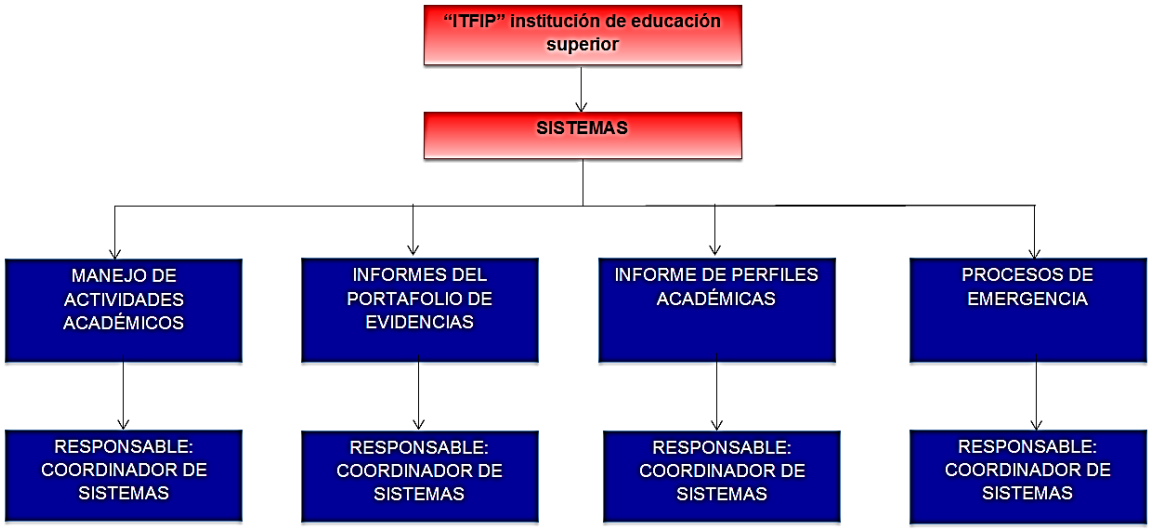
Fuente: Autoría Propia

Ilustración 25. Procesos Dependencia de sistemas (2)



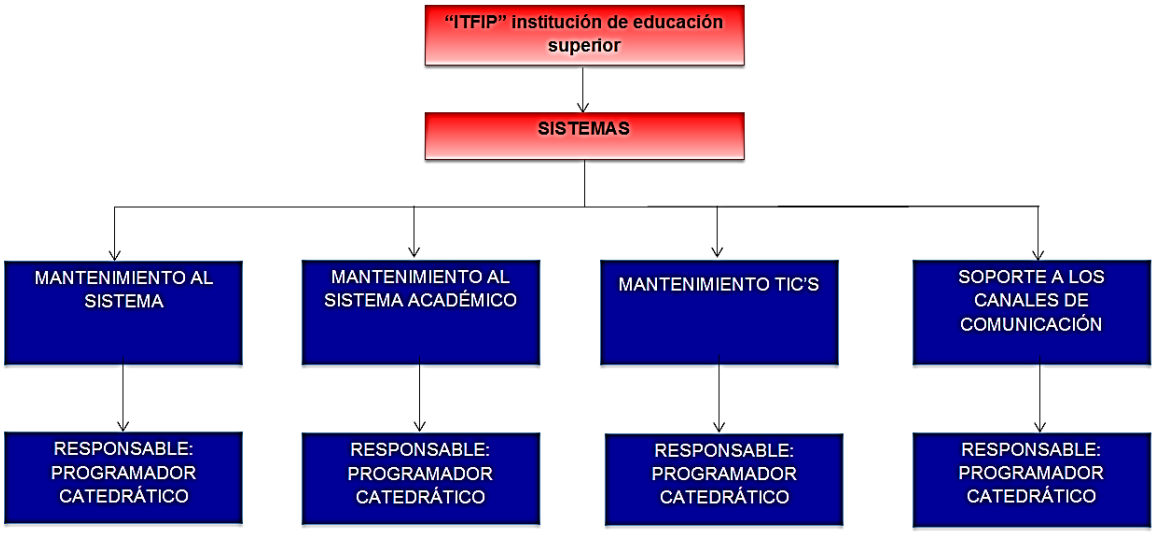
Fuente: Autoría Propia

Ilustración 26. Procesos Dependencia de sistemas (3)



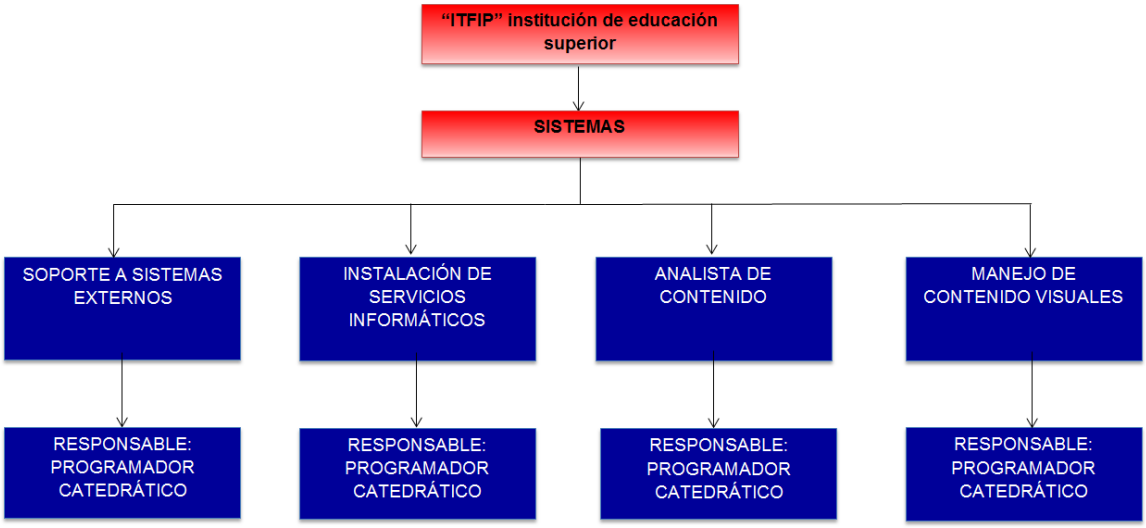
Fuente: Autoría Propia

Ilustración 27. Procesos Dependencia de sistemas (4)



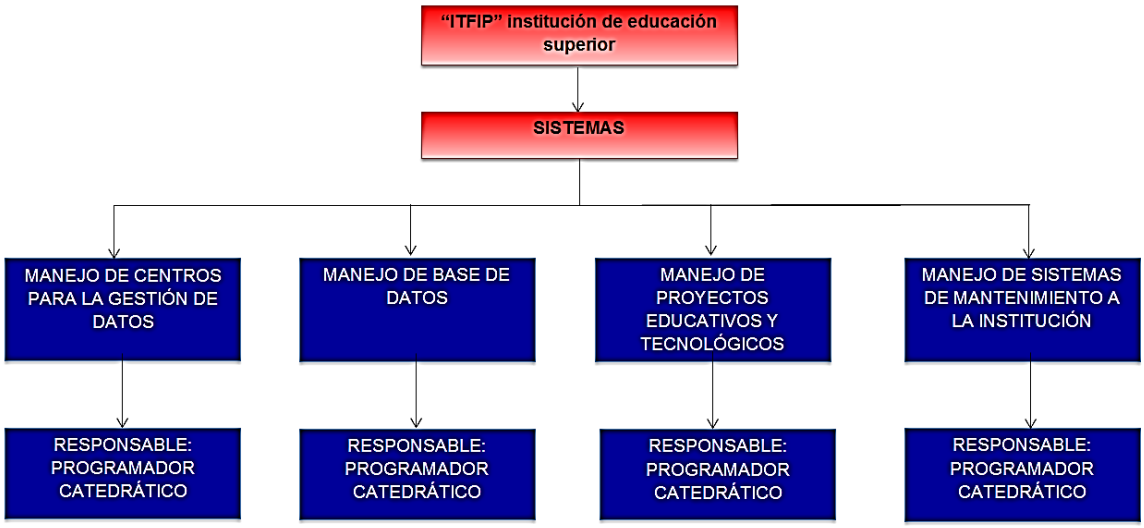
Fuente: Autoría Propia

Ilustración 28. Procesos Dependencia de sistemas (5)



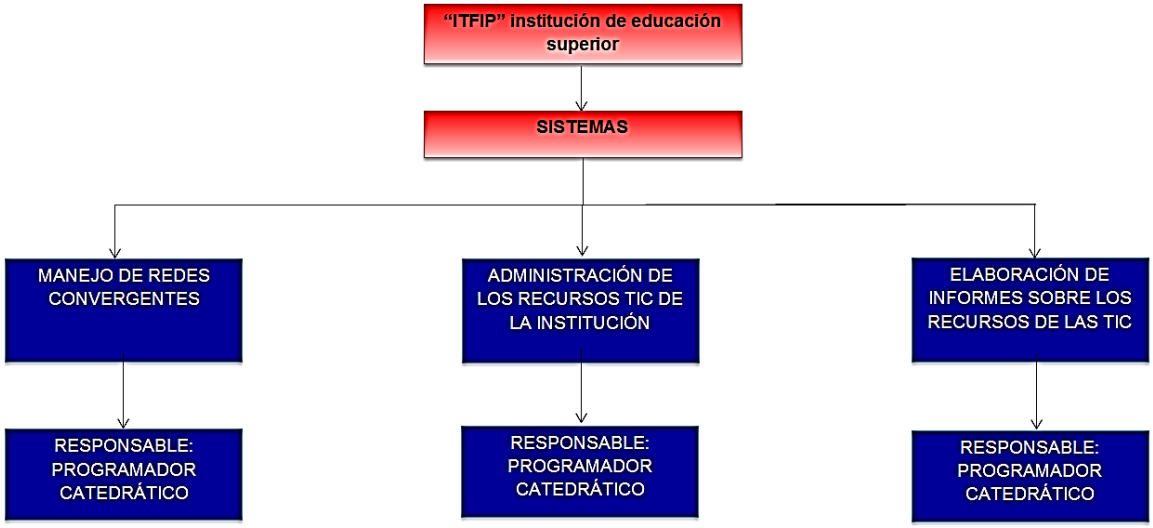
Fuente: Autoría Propia

Ilustración 29. Procesos Dependencia de sistemas (6)



Fuente: Autoría Propia

Ilustración 30. Procesos Dependencia de sistemas (7)

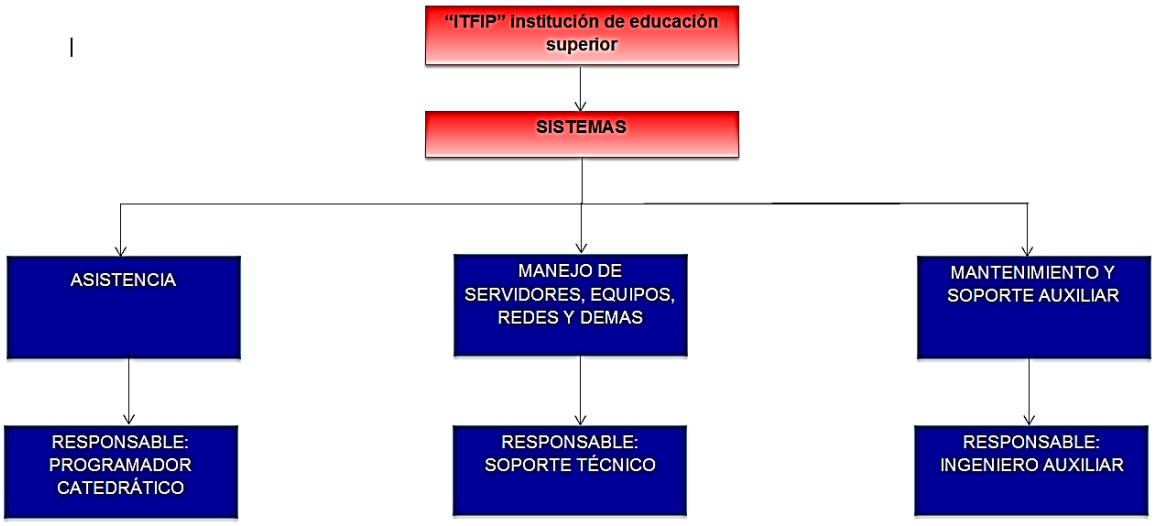


Fuente: Autoría Propia

Ilustración 31. Procesos Dependencia de sistemas (8)

Fuente: Autoría Propia

Ilustración 32. Procesos Dependencia de sistemas (9)



Fuente: Autoría Propia

2. ESTADO ACTUAL DE LA UNIVERSIDAD CON RESPECTO ISO/IEC 270001:2013 EN EL DEPARTAMENTO DE SISTEMAS DEL ITFIP

Como primera medida para desarrollar el diseño del sistema de gestión de seguridad de la información (SGSI) basado en la ISO/IEC 27001:2013, se realiza un análisis que permite evaluar el contexto de la organización, liderazgo, planificación, soporte, operación, seguridad, evaluación de desempeño y mejoras, los cuales se convierten en elementos esenciales para actuar según la norma.

La evaluación permite establecer el nivel de cumplimiento de la norma por parte del departamento de sistemas de la Institución de Educación Superior - ITFIP. Por lo tanto, las respuestas posibles para este cuestionario aplicado son: No cumple (NC), Cumple Parcialmente (CP), Cumple Satisfactoriamente (CS). De acuerdo con la información que se presenta en la siguiente tabla:

Tabla 1. Parámetros de evaluación

Sigla	Estado de Evaluación	Descripción
NC	NO CUMPLE	No existe y/o no se está haciendo
CP	CUMPLE PARCIALMENTE	Lo que la norma (ISO/IEC 27001 versión 2013) requiere se está haciendo de manera parcial, se está aplicando diferente, no está documentado, se definió y aprobó, pero no se gestiona.
CS	CUMPLE SATISFACTORIAMENTE	Existe, es gestionado y aplicado, se está cumpliendo con lo que la norma ISO/IEC 27001 versión 2013 solicita, está documentado, es conocido y aplicado por todos los involucrados en el SGSI se cumple al 100%.

Fuente: Autoría Propia.

2.1 CUESTIONARIO

A continuación, se presenta el cuestionario aplicado en el departamento de sistemas de la Institución de Educación Superior - ITFIP, dirigida al Ing. Wilson Mauricio Pimiento Cárdenas, Coordinador de Sistemas. Con el cuestionario se evalúan 105 ítems que hacen referencia a los siguientes dominios:

- A5. Políticas de seguridad de la Información.
- A6. Organización de la Seguridad de la Información.
- A7. Seguridad de los Recursos Humanos (RRHH).
- A8. Gestión de activos.
- A9. Control de acceso.
- A10. Criptografía.
- A11. Seguridad física y del entorno.
- A12. Seguridad en las operaciones.
- A13. Seguridad de las comunicaciones.
- A14. Adquisición, desarrollo y mantenimiento de sistemas.
- A15. Relación con proveedores.
- A16. Gestión de los incidentes de seguridad de la información.
- A17. Aspectos de seguridad de la información de la gestión de continuidad de negocio.
- A18. Cumplimiento.

2.1.1. A5 Políticas de seguridad de la Información

Tabla 2. Análisis del cumplimiento del Dominio A5

SECCIÓN	DOMINIO	ELEMENTO PARA EVALUAR	HALLAZGO
A5	Política de seguridad	Existen documento(s) de políticas de seguridad de SI	NC
A5	Política de seguridad	Existe normativa relativa a la seguridad de los SI	CP
A5	Política de seguridad	Existen procedimientos relativos a la seguridad de SI	CP
A5	Política de seguridad	Existe un responsable de las políticas, normas y procedimientos	CS
A5	Política de seguridad	Existen mecanismos para la comunicación a los usuarios de las normas	CS
A5	Política de seguridad	Existen controles regulares para verificar la efectividad de las políticas	NC

Fuente: Autoría Propia.

1.1.1. A6 Organización de la Seguridad de la Información

Tabla 3. Análisis del cumplimiento del Dominio A6

SECCIÓN	DOMINIO	ELEMENTO PARA EVALUAR	HALLAZGO
A6	Organización de la SI	Existen roles y responsabilidades definidos para las personas implicadas en la seguridad	CS

Tabla 3. Análisis del cumplimiento del Dominio A6 (Continuación)

A6	Organización de la SI	Existe un responsable encargado de evaluar la adquisición y cambios de SI	CS
A6	Organización de la SI	La Dirección y las áreas de la Organización participa en temas de seguridad	NC
A6	Organización de la SI	Existen condiciones contractuales de seguridad con terceros y outsourcing	CP
A6	Organización de la SI	Existen criterios de seguridad en el manejo de terceras partes	CP
A6	Organización de la SI	Existen programas de formación en seguridad para los empleados, clientes y terceros	CS
A6	Organización de la SI	Existe un acuerdo de confidencialidad de la información a la que se accede	CS
A6	Organización de la SI	Se revisa la seguridad de la organización periódicamente por una empresa externa	NC

Fuente: Autoría Propia.

2.1.2. A7 Seguridad de los Recursos Humanos (RRHH)

Tabla 4. Análisis del cumplimiento del Dominio A7

SECCIÓN	DOMINIO	ELEMENTO PARA EVALUAR	HALLAZGO
A7	Seguridad de los RRHH	Se tienen definidas responsabilidades y roles de seguridad	CS
A7	Seguridad de los RRHH	Se tiene en cuenta la seguridad en la selección y baja del personal	CP
A7	Seguridad de los RRHH	Se plasman las condiciones de confidencialidad y responsabilidades en los contratos	CS
A7	Seguridad de los RRHH	Se imparte la formación adecuada de seguridad y tratamiento de activos	CS

Tabla 4. Análisis del cumplimiento del Dominio A7 (Continuación)

A7	Seguridad de los RRHH	Existe un canal y procedimientos claros a seguir en caso de incidente de seguridad	NC
A7	Seguridad de los RRHH	Se recogen los datos de los incidentes de forma detallada	NC
A7	Seguridad de los RRHH	Informan los usuarios de las vulnerabilidades observadas o sospechadas	CS
A7	Seguridad de los RRHH	Se informa a los usuarios de que no deben, en ninguna circunstancia, probar las vulnerabilidades	CS
A7	Seguridad de los RRHH	Existe un proceso disciplinario de la seguridad de la información	CP

Fuente: Autoría Propia.

2.1.3. A8 Gestión de activos

Tabla 5. Análisis del cumplimiento del Dominio A8

SECCIÓN	DOMINIO	ELEMENTO PARA EVALUAR	HALLAZGO
A8	Gestión de activos	Existe un inventario de activos actualizado	CP
A8	Gestión de activos	El Inventario contiene activos de datos, software, equipos y servicios	CP
A8	Gestión de activos	Se dispone de una clasificación de la información según la criticidad de esta	NC
A8	Gestión de activos	Existe un responsable de los activos	CS
A8	Gestión de activos	Existen procedimientos para clasificar la información	NC
A8	Gestión de activos	Existen procedimientos de etiquetado de la información	CP

Fuente: Autoría Propia.

2.1.4. A9 Control de acceso

Tabla 6. Análisis del cumplimiento del Dominio A9

SECCIÓN	DOMINIO	ELEMENTO PARA EVALUAR	HALLAZGO
A9	Control de accesos	Existe una política de control de accesos	CS

Tabla 6. Análisis del cumplimiento del Dominio A9 (Continuación)

A9	Control de accesos	Existe un procedimiento formal de registro y baja de accesos	CS
A9	Control de accesos	Se controla y restringe la asignación y uso de privilegios en entornos multiusuario	CS
A9	Control de accesos	Existe una gestión de los *password* de usuarios	CS
A9	Control de accesos	Existe una revisión de los derechos de acceso de los usuarios	CS
A9	Control de accesos	Existe el uso del *password*	CS
A9	Control de accesos	Se protege el acceso de los equipos desatendidos	CP
A9	Control de accesos	Existen políticas de limpieza en el escritorio de los equipos	CP
A9	Control de accesos	Existe una política de uso de los servicios de red	CP
A9	Control de accesos	Se asegura la ruta (path) desde el terminal al servicio	CS
A9	Control de accesos	Existe una autenticación de usuarios en conexiones externas	CS
A9	Control de accesos	Existe una autenticación de los nodos	CP
A9	Control de accesos	Existe un control de la conexión de redes	CS
A9	Control de accesos	Existe un control del routing de las redes	CS
A9	Control de accesos	Existe una identificación única de usuario y una automática de terminales	CS
A9	Control de accesos	Existen procedimientos de log-on al terminal	CS
A9	Control de accesos	Se ha incorporado medidas de seguridad a la computación móvil	NC
A9	Control de accesos	Está controlado el teletrabajo por la organización	CP

Fuente: Autoría Propia.

2.1.5. A10 Criptografía

Tabla 7. Análisis del cumplimiento del Dominio A10

SECCIÓN	DOMINIO	ELEMENTO PARA EVALUAR	HALLAZGO
A10	Criptografía	Existen controles criptográficos	CS
A10	Criptografía	Existen procedimientos para uso de llaves criptográficas	CS
A10	Criptografía	Existe una política para la protección y tiempo de vida de las llaves criptográficas	CS

Fuente: Autoría Propia.

2.1.6. A11 Seguridad física y del Entorno

Tabla 8. Análisis del cumplimiento del Dominio A11

SECCIÓN	DOMINIO	ELEMENTO PARA EVALUAR	HALLAZGO
A11	Seguridad física y del Entorno	Existe perímetro de seguridad física (una pared, puerta con llave)	CS
A11	Seguridad física y del Entorno	Existen controles de entrada para protegerse frente al acceso de personal no autorizado	CP
A11	Seguridad física y del Entorno	Un área segura ha de estar cerrada, aislada y protegida de eventos naturales	CP
A11	Seguridad física y del Entorno	En las áreas seguras existen controles adicionales al personal propio y ajeno	NC
A11	Seguridad física y del Entorno	La ubicación de los equipos está de tal manera para minimizar accesos innecesarios	CP
A11	Seguridad física y del Entorno	Existen protecciones frente a fallos en la alimentación eléctrica	CS
A11	Seguridad física y del Entorno	Existe seguridad en el cableado frente a daños e intercepciones	CP
A11	Seguridad física y del Entorno	Se asegura la disponibilidad e integridad de todos los equipos	CP
A11	Seguridad física y del Entorno	Existe algún tipo de seguridad para los equipos retirados o ubicados externamente	CP
A11	Seguridad física y del Entorno	Se incluye la seguridad en equipos móviles	NC

Fuente: Autoría Propia.

2.1.7. A12 Seguridad en las operaciones

Tabla 9. Análisis del cumplimiento del Dominio A12

SECCIÓN	DOMINIO	ELEMENTO PARA EVALUAR	HALLAZGO
A12	Seguridad en las operaciones	Todos los procedimientos operativos identificados en la política de seguridad han de estar documentados	CP
A12	Seguridad en las operaciones	Existe algún método para reducir el mal uso accidental o deliberado de los Sistemas	CS
A12	Seguridad en las operaciones	Existe una separación de los entornos de desarrollo y producción	CS
A12	Seguridad en las operaciones	Existen contratistas externos para la gestión de los Sistemas de Información	CP
A12	Seguridad en las operaciones	Existe un Plan de Capacidad para asegurar la adecuada capacidad de proceso y de almacén amiento	NC
A12	Seguridad en las operaciones	Controles contra software maligno	CS
A12	Seguridad en las operaciones	Realizar copias de backup de la información esencial para el negocio	CS
A12	Seguridad en las operaciones	Existen logs para las actividades realizadas por los operadores y administradores	CS
A12	Seguridad en las operaciones	Existen logs de los fallos detectados	CS
A12	Seguridad en las operaciones	Existen rastros de auditoría	CP
A12	Seguridad en las operaciones	Hay establecidos controles para realizar la gestión de los medios informáticos (cintas, discos, removibles, informes impresos)	NC

Fuente: Autoría Propia.

2.1.8. A13 Seguridad de las comunicaciones

Tabla 10. Análisis del cumplimiento del Dominio A13

SECCIÓN	DOMINIO	ELEMENTO PARA EVALUAR	HALLAZGO
A13	Seguridad en las comunicaciones	Existe algún control en las redes	CS
A13	Seguridad en las comunicaciones	Existe seguridad de la documentación de los Sistemas	CP

Tabla 10.Análisis del cumplimiento del Dominio A13 (Continuación)

A13	Seguridad en las comunicaciones	Existen acuerdos para intercambio de información y software	NC
A13	Seguridad en las comunicaciones	Se han establecido e implantado medidas para proteger la confidencialidad e integridad de información publicada	CS
A13	Seguridad en las comunicaciones	Existen medidas de seguridad en las transacciones en línea	CS

Fuente: Autoría Propia.

2.1.9. A14 Adquisición, desarrollo y mantenimiento de sistemas

Tabla 11. Análisis del cumplimiento del Dominio A14

SECCIÓN	DOMINIO	ELEMENTO PARA EVALUAR	HALLAZGO
A14	Adquisición de sistemas, desarrollo y mantenimiento	Están establecidas las responsabilidades para controlar los cambios en equipos	CS
A14	Adquisición de sistemas, desarrollo y mantenimiento	Existen criterios de aceptación de nuevos SI, incluyendo actualizaciones y nuevas versiones	CS
A14	Adquisición de sistemas, desarrollo y mantenimiento	Se garantiza que la seguridad está implantada en los Sistemas de Información	CS
A14	Adquisición de sistemas, desarrollo y mantenimiento	Existe seguridad en las aplicaciones	CS
A14	Adquisición de sistemas, desarrollo y mantenimiento	Existe seguridad en los ficheros de los sistemas	CS
A14	Adquisición de sistemas, desarrollo y mantenimiento	Existe seguridad en los procesos de desarrollo, testing y soporte	CS
A14	Adquisición de sistemas, desarrollo y mantenimiento	Existen controles de seguridad para los resultados de los sistemas	CS
A14	Adquisición de sistemas, desarrollo y mantenimiento	Existe la gestión de los cambios en los SO	CS

Tabla 11. Análisis del cumplimiento del Dominio A14 (Continuación)

A14	Adquisición de sistemas, desarrollo y mantenimiento	Se controlan las vulnerabilidades de los equipos	CS

Fuente: Autoría Propia.

2.1.10. A15 Relación con los proveedores

Tabla 12. Análisis del cumplimiento del Dominio A15

SECCIÓN	DOMINIO	ELEMENTO PARA EVALUAR	HALLAZGO
A15	Relación con proveedores	Existe una política de seguridad de la información para las relaciones con proveedores	NC
A15	Relación con proveedores	Existe un acuerdo documentado con cada proveedor que tenga acceso a la infraestructura de TI	CS
A15	Relación con proveedores	Se monitorean las actividades relacionadas a la seguridad con los proveedores	CS
A15	Relación con proveedores	Los acuerdos con proveedores incluyen los requisitos para tratar los riesgos de la seguridad de la información	CS

Fuente: Autoría Propia.

2.1.11. A16 Gestión de incidentes de seguridad de la información

Tabla 13. Análisis del cumplimiento del Dominio A16

SECCIÓN	DOMINIO	ELEMENTO PARA EVALUAR	HALLAZGO
A16	Gestión de los incidentes de seguridad	Están establecidas responsabilidades para asegurar una respuesta rápida, ordenada y efectiva frente a incidentes de seguridad	CP
A16	Gestión de los incidentes de seguridad	Se comunican los eventos de seguridad	CS
A16	Gestión de los incidentes de seguridad	Se comunican las debilidades de seguridad	CP
A16	Gestión de los incidentes de seguridad	Existe definidas las responsabilidades ante un incidente	CP

Fuente: Autoría Propia

Tabla 13. Análisis del cumplimiento del Dominio A16 (Continuación)

A16	Gestión de los incidentes de seguridad	Existe un procedimiento formal de respuesta	CP
A16	Gestión de los incidentes de seguridad	Existe la gestión de incidentes	CP

Fuente: Autoría Propia.

2.1.12. A17 Aspectos de seguridad de la información de la gestión de continuidad de negocio

Tabla 14. Análisis del cumplimiento del Dominio A17

SECCIÓN	DOMINIO	ELEMENTO PARA EVALUAR	HALLAZGO
A17	Continuidad del negocio	Existen procesos para la gestión de la continuidad	CP
A17	Continuidad del negocio	Existe un plan de continuidad del negocio y análisis de impacto	CS
A17	Continuidad del negocio	Existe un diseño, redacción e implantación de planes de continuidad	CS
A17	Continuidad del negocio	Existe un marco de planificación para la continuidad del negocio	CS
A17	Continuidad del negocio	Existen prueba, mantenimiento y reevaluación de los planes de continuidad del negocio	CS

Fuente: Autoría Propia.

2.1.13. A18 Cumplimiento

Tabla 15. Análisis del cumplimiento del Domino A18

SECCIÓN	DOMINIO	ELEMENTO PARA EVALUAR	HALLAZGO
A18	Cumplimiento con requerimientos legales y contractuales	Se tiene en cuenta el cumplimiento con la legislación por parte de los sistemas	CP
A18	Cumplimiento con requerimientos legales y contractuales	Existe el resguardo de la propiedad intelectual	CS
A18	Cumplimiento con requerimientos legales y contractuales	Existe el resguardo de los registros de la organización	CS

Tabla 15. Análisis del cumplimiento del Domino A18 (Continuación)

A18	Cumplimiento con requerimientos legales y contractuales	Existe una revisión de la política de seguridad y de la conformidad técnica	CP
A18	Cumplimiento con requerimientos legales y contractuales	Existen consideraciones sobre las auditorías de los sistemas	CP

Fuente: Autoría Propia.

2.2 RESULTADOS

Tras el análisis se obtienen los siguientes resultados:

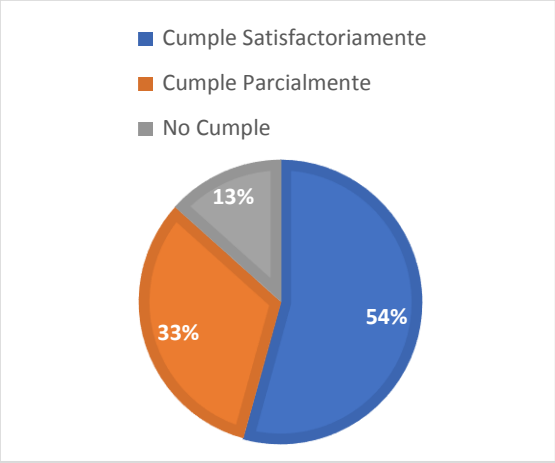
Tabla 16. Resumen resultados de la evaluación

	Dominio	**CS**	**CP**	**NC**	**Ítems Evaluados**
A5	Políticas de seguridad de la información.	2	2	2	6
A6	Organización de la seguridad de la información	4	2	2	8
A7	Seguridad de los recursos humanos (RRHH)	5	2	2	9
A8	Gestión de activos	1	3	2	6
A9	Control de accesos	12	5	1	18
A10	Criptografía	3	0	0	3
A11	Seguridad física y del entorno	2	6	2	10
A12	Seguridad de las operaciones	6	3	2	11
A13	Seguridad de las comunicaciones	3	1	1	5
A14	Adquisición, desarrollo y mantenimiento de sistemas	9	0	0	9
A15	Relación con los proveedores	3	1	0	4
A16	Gestión de incidentes de seguridad de la información	1	5	0	6
A17	Aspectos de seguridad de la información de la gestión de continuidad del negocio	4	1	0	5
A18	Cumplimiento	2	3	0	5
	Suma total	**57**	**34**	**14**	**105**

Fuente: Autoría Propia.

2.3 DESCRIPCION DE LOS RESULTADOS PORCENTUALMENTE

Gráfico 1. Descripción de los resultados obtenidos de la evaluación de los dominios



A nivel general, más del 50% de los dominios cumplen satisfactoriamente con las pautas requeridas, dejando solamente un 33% a labores no culminadas; al contrario del 13% de dominios que no se cumplen.

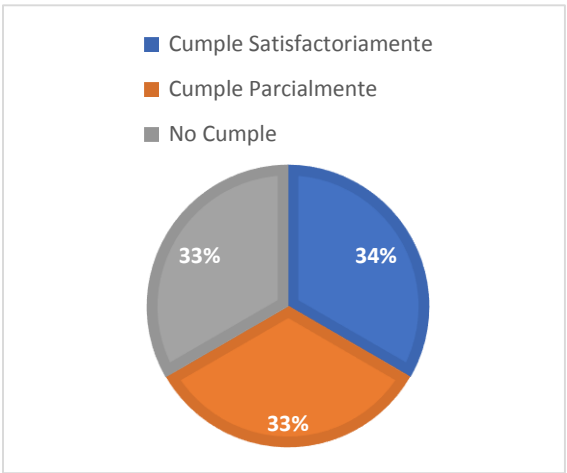
Fuente: Autoría Propia.

2.3.1. Resultados de la evaluación de los 14 dominios.

En los siguientes párrafos se presentará el análisis de cada uno de los dominios evaluados con sus respectivos resultados.

2.3.2. Resultados dominio A5 política de seguridad.

Gráfico 2. Descripción de los resultados obtenidos Dominio A5

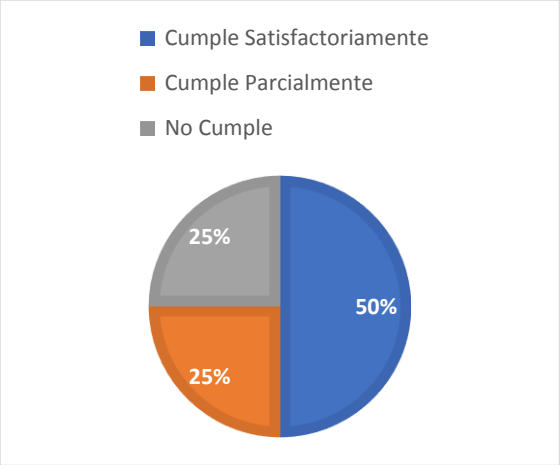


Para este dominio se observa que en la dependencia de sistemas existe un factor imparcial en las tres (3) condiciones dadas a evaluar, permitiendo así concretar las necesidades que más se priorizan dentro de la dependencia de sistemas, en términos de políticas de seguridad.

Fuente: Autoría Propia.

2.3.3. Resultados dominio A6 organización de la seguridad de la información.

Gráfico 3. Descripción de los resultados obtenidos Dominio A6

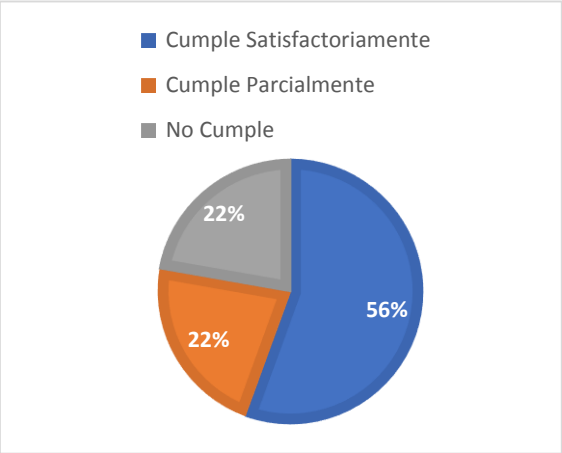


Para este dominio se observa que en la dependencia de sistemas de manera general el 50% de los ítems se cumplen satisfactoriamente, el otro 50% es dividido entre que cumple parcialmente y que no cumplen.

Fuente: Autoría Propia.

2.3.4. Resultados dominio A7 seguridad de los recursos humanos (RRHH).

Gráfico 4. Descripción de los resultados obtenidos Dominio A7

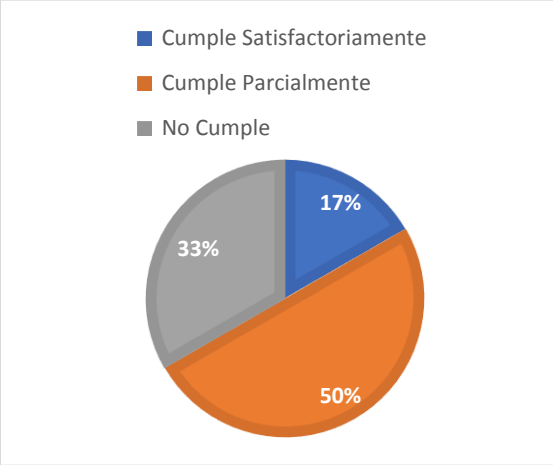


Para este dominio se observa que en la dependencia de sistemas de manera general el 56% de los ítems se cumplen satisfactoriamente, el otro 44% es dividido entre que cumple parcialmente y que no cumplen.

Fuente: Autoría Propia

2.3.5. Resultados dominio A8 gestión de activos.

Gráfico 5. Descripción de los resultados obtenidos Dominio A8

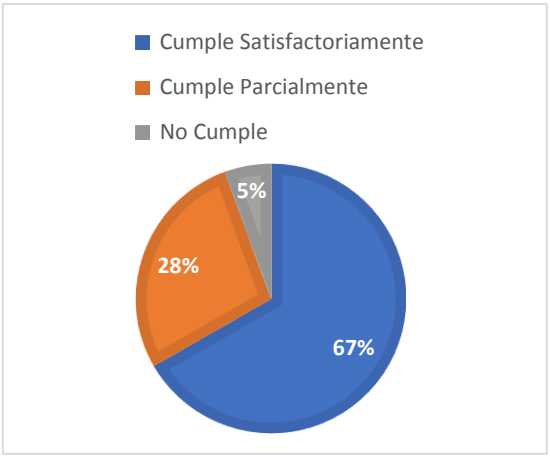


Para este dominio se observa que en la dependencia de sistemas en la gestión de los activos solamente el 17% cumplen satisfactoriamente, el 33% no cumplen y 50% cumplen parcialmente.

Fuente: Autoría Propia.

2.3.6. Resultados dominio A9 control de accesos.

Gráfico 6. Descripción de los resultados obtenidos Dominio A9

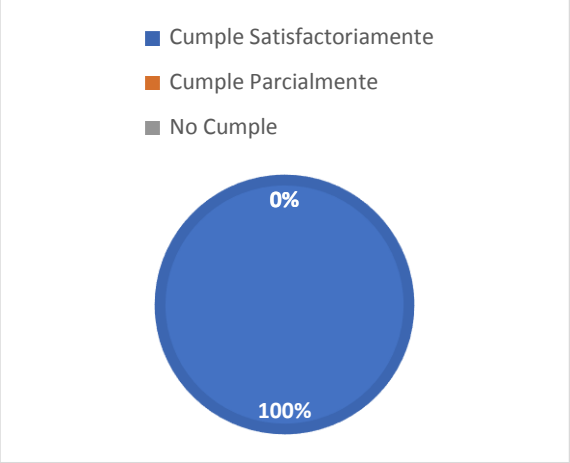


Para este dominio se observa que en la dependencia de sistemas de manera general se cumplen satisfactoriamente el 67% de los ítems, el 28% se cumplen parcial y solamente el 5% no cumplen.

Fuente: Autoría Propia.

2.3.7. Resultados dominio A10 criptografía.

Gráfico 7. Descripción de los resultados obtenidos Dominio A10

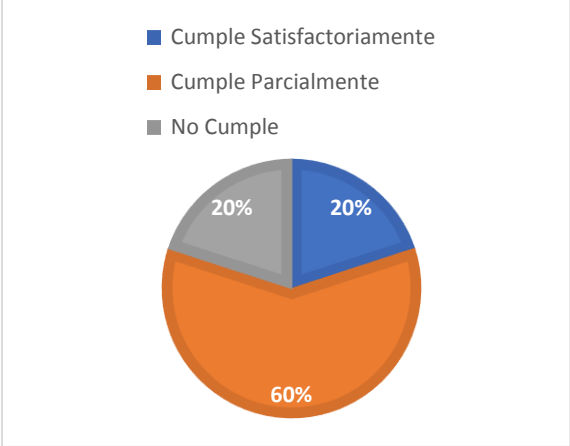


Para este dominio se observa que en la dependencia de sistemas se cumple satisfactoriamente el 100% de los ítems evaluados.

Fuente: Autoría Propia.

2.3.8. Resultados dominio A11 seguridad física y ambiental.

Gráfico 8. Descripción de los resultados obtenidos Dominio A11

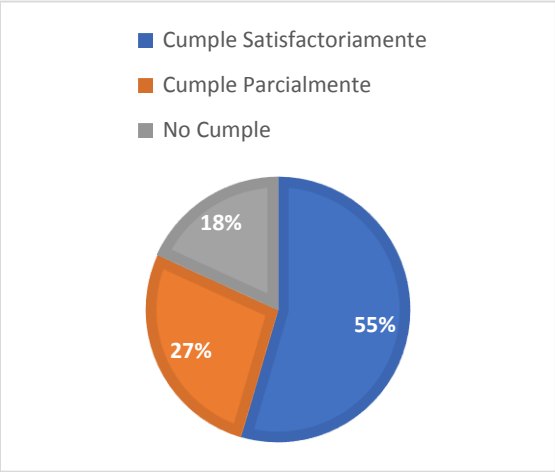


Es claro el alarmante déficit aplicado en esta dependencia, puesto que el 60% de las preguntas efectuadas, se cumplen, pero no en su totalidad, demostrando así el gran problema en este ítem. Un valor igualado (20%) se presentan entre cumplir y no cumplir las especificaciones

Fuente: Autoría Propia.

2.3.9. Resultados dominio A12 seguridad en las operaciones.

Gráfico 9. Descripción de los resultados obtenidos Dominio A12

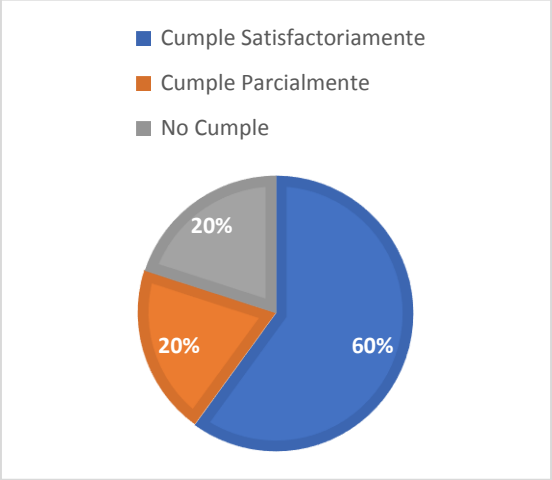


Parte de tranquilidad en el enfoque del dominio 12, puesto que se puede apreciar un 55%, en donde si se cumple con las respectivas recomendaciones de las dependencias, otro 27%, cumple parcialmente con estos recursos, dejando así solo un 18% de ítems no tomados en cuenta.

Fuente: Autoría Propia.

2.3.10. Resultados dominio A13 seguridad en las comunicaciones.

Gráfico 10.Descripción de los resultados obtenidos Dominio A13

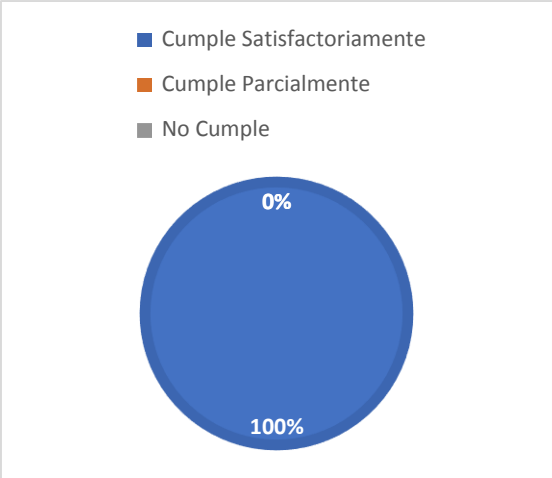


Un 60% de las preguntas efectuadas cumple satisfactoriamente con las indicaciones que la norma lo exige, caso contrario con los ítems que se encuentran igualados (20%), lo que conlleva a un factor preocupante en el dominio.

Fuente: Autoría Propia.

2.3.11. Resultados dominio A14 adquisición de sistemas, desarrollo y mantenimiento.

Gráfico 11. Descripción de los resultados obtenidos Dominio A14

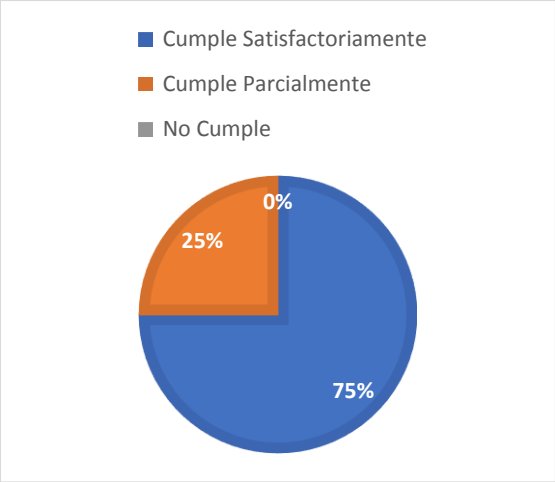


Dominio totalmente cumplido en la dependencia.

Fuente: Autoría Propia.

2.3.12. Resultados dominio A15 relación con proveedores.

Gráfico 12. Descripción de los resultados obtenidos Dominio A15

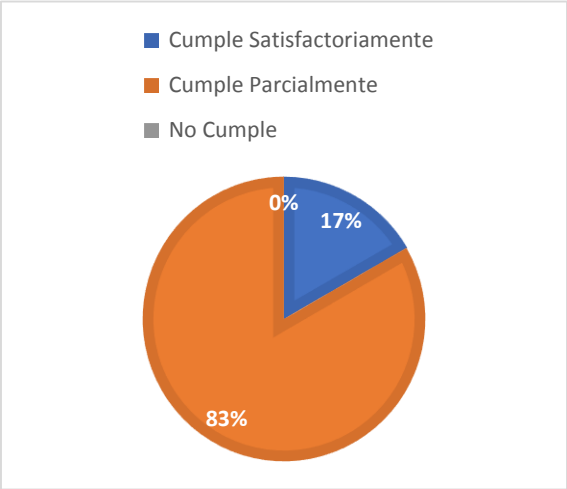


Según la gráfica, dos tercios de partes cumplen los requerimientos necesarios para efectuar este dominio, siendo positivo en donde un tercio solamente cumple parcialmente lo planeado.

Fuente: Autoría Propia.

2.3.13. Resultados dominio A16 gestión de los incidentes de seguridad.

Gráfico 13. Descripción de los resultados obtenidos Dominio A16

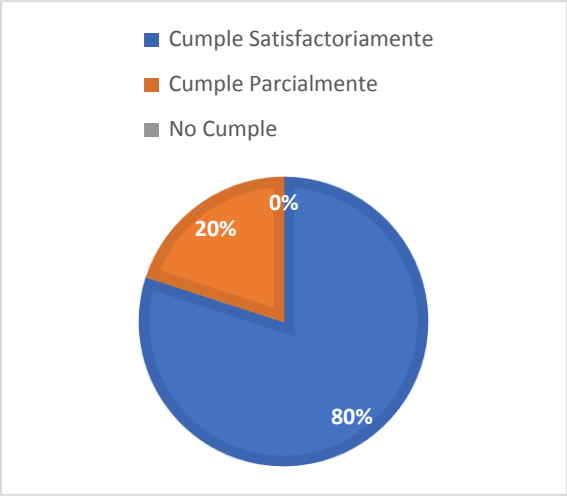


La situación es alarmante en el dominio 16, puesto que más del ochenta por ciento (83%), se realiza de manera inconclusa, dejando cabos sueltos en la realización de cada uno de los ítems mencionados. Ante esta negativa se ve reflejada el porcentaje restante (17%), que si se cumple en su totalidad.

Fuente: Autoría Propia.

2.3.14. Resultados dominio A17 continuidad del negocio.

Gráfico 14. Descripción de los resultados obtenidos Dominio A17

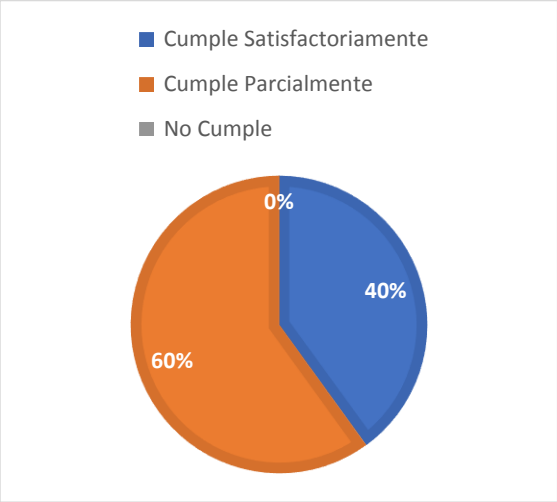


El resultado que arrojan los datos obtenidos se puede plantear de dos maneras paralelas. En la primera podemos apreciar que sola mente una quinta parte de los ítems consultados se llevan a cabo parcialmente, dejándose inconcluso. Caso totalmente contrario con el porcentaje restante que cumple a la perfección lo requerido.

Fuente: Autoría Propia

2.3.15. Resultados dominio A18 cumplimiento con requerimientos legales y contractuales.

Gráfico 15. Descripción de los resultados obtenidos Dominio A18



Uno de los dominios más críticos, puesto que es en este dónde prevalece el trabajo parcial, dejando labores sin concluir que puede llevar concurrir un riesgo a gran escala. No obstante, el porcentaje restante (40%), de nota una aceptabilidad total en cada una de las funciones comprometidas.

Fuente: Autoría Propia.

2.4. INVENTARIO DE ACTIVOS ENTREGADOS POR EL DEPARTAMENTO DE SISTEMAS DEL ITFIP

Tabla 17. Consecutivo y responsable de cada activo.

CODIGO INV.	EQUIPO	RESPONSABLE
22400659	Alcatel lucent 1port802.3af po	Pimiento Cárdenas Wilson Mauricio
22400660	Alcatel lucent 1port802.3af po	Pimiento Cárdenas Wilson Mauricio
22400661	Alcatel lucent 1port802.3af po	Pimiento Cárdenas Wilson Mauricio
22400662	Alcatel lucent 1port802.3af po	Pimiento Cárdenas Wilson Mauricio
22400664	Alcatel lucent 1port802.3af po	Pimiento Cárdenas Wilson Mauricio
22400666	Alcatel lucent 1port802.3af po	Pimiento Cárdenas Wilson Mauricio
22400667	Alcatel lucent 1port802.3af po	Pimiento Cárdenas Wilson Mauricio
22400668	Alcatel lucent 1port802.3af po	Pimiento Cárdenas Wilson Mauricio
22400670	Alcatel lucent 1port802.3af po	Pimiento Cárdenas Wilson Mauricio
22400671	Alcatel lucent 1port802.3af po	Pimiento Cárdenas Wilson Mauricio
22400599	Alcatel lucent antenna dual ba	Pimiento Cárdenas Wilson Mauricio
22400600	Alcatel lucent antenna dual ba	Pimiento Cárdenas Wilson Mauricio
22400601	Alcatel lucent antenna dual ba	Pimiento Cárdenas Wilson Mauricio
22400602	Alcatel lucent antenna dual ba	Pimiento Cárdenas Wilson Mauricio
22400603	Alcatel lucent antenna dual ba	Pimiento Cárdenas Wilson Mauricio
22400604	Alcatel lucent antenna dual ba	Pimiento Cárdenas Wilson Mauricio
22400605	Alcatel lucent antenna dual ba	Pimiento Cárdenas Wilson Mauricio
22400606	Alcatel lucent antenna dual ba	Pimiento Cárdenas Wilson Mauricio

Tabla 17. Consecutivo y responsable de cada activo. (Continuación)

22400630	Alcatel lucent omniacces ap105	Pimiento Cárdenas Wilson Mauricio
22400631	Alcatel lucent omniacces ap105	Pimiento Cárdenas Wilson Mauricio
22400632	Alcatel lucent omniacces ap105	Pimiento Cárdenas Wilson Mauricio
22400633	Alcatel lucent omniacces ap105	Pimiento Cárdenas Wilson Mauricio
22400634	Alcatel lucent omniacces ap105	Pimiento Cárdenas Wilson Mauricio
22400635	Alcatel lucent omniacces ap105	Pimiento Cárdenas Wilson Mauricio
22400636	Alcatel lucent omniacces ap105	Pimiento Cárdenas Wilson Mauricio
22400637	Alcatel lucent omniacces ap105	Pimiento Cárdenas Wilson Mauricio
22400638	Alcatel lucent omniacces ap105	Pimiento Cárdenas Wilson Mauricio
22400639	Alcatel lucent omniacces ap105	Pimiento Cárdenas Wilson Mauricio
22400640	Alcatel lucent omniacces ap105	Pimiento Cárdenas Wilson Mauricio
22400641	Alcatel lucent omniacces ap105	Pimiento Cárdenas Wilson Mauricio
22400642	Alcatel lucent omniacces ap105	Pimiento Cárdenas Wilson Mauricio
22400643	Alcatel lucent omniacces ap105	Pimiento Cárdenas Wilson Mauricio
22400644	Alcatel lucent omniacces ap105	Pimiento Cárdenas Wilson Mauricio
22400645	Alcatel lucent omniacces ap105	Pimiento Cárdenas Wilson Mauricio
22400646	Alcatel lucent omniacces ap105	Pimiento Cárdenas Wilson Mauricio
22400647	Alcatel lucent omniacces ap105	Pimiento Cárdenas Wilson Mauricio
22400648	Alcatel lucent omniacces ap105	Pimiento Cárdenas Wilson Mauricio
22400649	Alcatel lucent omniacces ap105	Pimiento Cárdenas Wilson Mauricio
22400650	Alcatel lucent omniacces ap105	Pimiento Cárdenas Wilson Mauricio
22400595	Alcatel lucent omniacces ap17	Pimiento Cárdenas Wilson Mauricio

Tabla 17. Consecutivo y responsable de cada activo. (Continuación)

22400596	Alcatel lucent omniacces ap17	Pimiento Cárdenas Wilson Mauricio
22400597	Alcatel lucent omniacces ap17	Pimiento Cárdenas Wilson Mauricio
22400598	Alcatel lucent omniacces ap17	Pimiento Cárdenas Wilson Mauricio
22400676	Alcatel lucent os6850e-bp modu	Pimiento Cárdenas Wilson Mauricio
22400677	Alcatel lucent os6850e-bp modu	Pimiento Cárdenas Wilson Mauricio
22400607	Alcatel lucent outdoor antenna	Pimiento Cárdenas Wilson Mauricio
22400608	Alcatel lucent outdoor antenna	Pimiento Cárdenas Wilson Mauricio
22400609	Alcatel lucent outdoor antenna	Pimiento Cárdenas Wilson Mauricio
22400610	Alcatel lucent outdoor antenna	Pimiento Cárdenas Wilson Mauricio
22400611	Alcatel lucent outdoor antenna	Pimiento Cárdenas Wilson Mauricio
22400612	Alcatel lucent outdoor antenna	Pimiento Cárdenas Wilson Mauricio
22400613	Alcatel lucent outdoor antenna	Pimiento Cárdenas Wilson Mauricio
22400614	Alcatel lucent outdoor antenna	Pimiento Cárdenas Wilson Mauricio
22400615	Alcatel lucent outdoor antenna	Pimiento Cárdenas Wilson Mauricio
22400616	Alcatel lucent outdoor antenna	Pimiento Cárdenas Wilson Mauricio
22400617	Alcatel lucent outdoor antenna	Pimiento Cárdenas Wilson Mauricio
22400618	Alcatel lucent outdoor antenna	Pimiento Cárdenas Wilson Mauricio
22400619	Alcatel lucent outdoor antenna	Pimiento Cárdenas Wilson Mauricio
22400620	Alcatel lucent outdoor antenna	Pimiento Cárdenas Wilson Mauricio
22400573	Computador todo en uno Intel c	Pimiento Cárdenas Wilson Mauricio
22400531	Computador iMac Intel Core i5	Pimiento Cárdenas Wilson Mauricio
22400532	Computador iMac Intel Core i5	Pimiento Cárdenas Wilson Mauricio

Tabla 17. Consecutivo y responsable de cada activo. (Continuación)

22400533	Computador iMac Intel Core i5	Pimiento Cárdenas Wilson Mauricio
22400534	Computador iMac Intel Core i5	Pimiento Cárdenas Wilson Mauricio
22400535	Computador iMac Intel Core i5	Pimiento Cárdenas Wilson Mauricio
22400536	Computador iMac Intel Core i5	Pimiento Cárdenas Wilson Mauricio
22400537	Computador iMac Intel Core i5	Pimiento Cárdenas Wilson Mauricio
22400530	Computador p/control de acceso	Pimiento Cárdenas Wilson Mauricio
22400570	Computador todo en uno Core i5	Pimiento Cárdenas Wilson Mauricio
22400571	Computador todo en uno Core i5	Pimiento Cárdenas Wilson Mauricio
22400572	Computador todo en uno Core i5	Pimiento Cárdenas Wilson Mauricio
22400574	Computador todo en uno Core i5	Pimiento Cárdenas Wilson Mauricio
22400575	Computador todo en uno Core i5	Pimiento Cárdenas Wilson Mauricio
22400577	Computador todo en uno Core i5	Pimiento Cárdenas Wilson Mauricio
22400578	Computador todo en uno Core i5	Pimiento Cárdenas Wilson Mauricio
22400579	Computador todo en uno Core i5	Pimiento Cárdenas Wilson Mauricio
22400580	Computador todo en uno Core i5	Pimiento Cárdenas Wilson Mauricio
22400581	Computador todo en uno Core i5	Pimiento Cárdenas Wilson Mauricio
22400583	Computador todo en uno Core i5	Pimiento Cárdenas Wilson Mauricio
22400584	Computador todo en uno Core i5	Pimiento Cárdenas Wilson Mauricio
22400585	Computador todo en uno Core i5	Pimiento Cárdenas Wilson Mauricio
22400586	Computador todo en uno Core i5	Pimiento Cárdenas Wilson Mauricio
22400588	Computador todo en uno Core i5	Pimiento Cárdenas Wilson Mauricio
22400589	Computador todo en uno Core i5	Pimiento Cárdenas Wilson Mauricio

Tabla 17. Consecutivo y responsable de cada activo. (Continuación)

22400148	Computador todo en uno hp pro	Pimiento Cárdenas Wilson Mauricio
22400192	Computador todo en uno hp pro	Pimiento Cárdenas Wilson Mauricio
BACK UP-SISTEMAS	Copias de seguridad de cada pc de la dependencia de sistemas	Pimiento Cárdenas Wilson Mauricio
BACK UP-ITFIP	Copias de seguridad de cada pc de las dependencias de la institución	Pimiento Cárdenas Wilson Mauricio
BACK UP-SERVER'S	Copias de seguridad de las configuraciones de los servidores	Pimiento Cárdenas Wilson Mauricio
E-ORG	Estructura organizacional	Pimiento Cárdenas Wilson Mauricio
22400672	Hp prolina dl320e gen8 sata 9	Pimiento Cárdenas Wilson Mauricio
I-DC	Inventario de contratos	Pimiento Cárdenas Wilson Mauricio
I-DU	Inventario de usuarios	Pimiento Cárdenas Wilson Mauricio
22400529	Lector biométrico 9581	Pimiento Cárdenas Wilson Mauricio
22400899	Lector código de 547 barras	Pimiento Cárdenas Wilson Mauricio
22400900	Lector código de 547 barras	Pimiento Cárdenas Wilson Mauricio
22400540	Portátil tipo estación de trab	Pimiento Cárdenas Wilson Mauricio
22400542	Portátil tipo estación de trab	Pimiento Cárdenas Wilson Mauricio
22400543	Portátil tipo estación de trab	Pimiento Cárdenas Wilson Mauricio
22400544	Portátil tipo estación de trab	Pimiento Cárdenas Wilson Mauricio
22400545	Portátil tipo estación de trab	Pimiento Cárdenas Wilson Mauricio
22400546	Portátil tipo estación de trab	Pimiento Cárdenas Wilson Mauricio
22400547	Portátil tipo estación de trab	Pimiento Cárdenas Wilson Mauricio
22400548	Portátil tipo estación de trab	Pimiento Cárdenas Wilson Mauricio
22400549	Portátil tipo estación de trab	Pimiento Cárdenas Wilson Mauricio
22400554	Portátil tipo estación de trab	Pimiento Cárdenas Wilson Mauricio

Tabla 17. Consecutivo y responsable de cada activo. (Continuación)

22400555	Portátil tipo estación de trab	Pimiento Cárdenas Wilson Mauricio
22400557	Portátil tipo estación de trab	Pimiento Cárdenas Wilson Mauricio
22400562	Portátil tipo estación de trab	Pimiento Cárdenas Wilson Mauricio
22400563	Portátil tipo estación de trab	Pimiento Cárdenas Wilson Mauricio
22400564	Portátil tipo estación de trab	Pimiento Cárdenas Wilson Mauricio
22400565	Portátil tipo estación de trab	Pimiento Cárdenas Wilson Mauricio
R-DA	Registro de actividades	Pimiento Cárdenas Wilson Mauricio
R-AE	Registro de la Arquitectura de los Equipos	Pimiento Cárdenas Wilson Mauricio
R-ME	Registro Mantenimiento Equipos	Pimiento Cárdenas Wilson Mauricio
22400513	Router tp-link archerc 7 9530	Pimiento Cárdenas Wilson Mauricio
22400266	Servidor dell powerd edge ta20	Pimiento Cárdenas Wilson Mauricio
22400264	Servidor hewlett packard ml350	Pimiento Cárdenas Wilson Mauricio
S-PV	Soporte de plataformas virtuales	Pimiento Cárdenas Wilson Mauricio
S-EC	Soporte equipos de computo	Pimiento Cárdenas Wilson Mauricio
22400675	Tabla negra de 9 pulgadas allw	Pimiento Cárdenas Wilson Mauricio
22400526	Ups 10 kva 9578	Pimiento Cárdenas Wilson Mauricio
22400527	Ups 10 kva 9579	Pimiento Cárdenas Wilson Mauricio
22400528	Ups 10 kva 9580	Pimiento Cárdenas Wilson Mauricio
22400673	Ups tecnología de entrada bifá	Pimiento Cárdenas Wilson Mauricio
22400674	Ups tecnología de entrada bifá	Pimiento Cárdenas Wilson Mauricio
VLAN-ADMON	Vlan de administración	Pimiento Cárdenas Wilson Mauricio
VLAN-ALMA	Vlan de almacén	Pimiento Cárdenas Wilson Mauricio

Tabla 17. Consecutivo y responsable de cada activo. (Continuación)

VLAN-CONF	Vlan de configuración	Pimiento Cárdenas Wilson Mauricio
VLAN-EST	Vlan de estudiantes	Pimiento Cárdenas Wilson Mauricio
VLAN-FINAN	Vlan de financiera	Pimiento Cárdenas Wilson Mauricio
VLAN-RYCA	Vlan de registro y control	Pimiento Cárdenas Wilson Mauricio
VLAN-SIS	Vlan de sistemas	Pimiento Cárdenas Wilson Mauricio
VLAN-TALEN	Vlan de talento humano	Pimiento Cárdenas Wilson Mauricio
VLAN-TESO	Vlan de tesorería	Pimiento Cárdenas Wilson Mauricio
V-WIFI	Vlan de wifi	Pimiento Cárdenas Wilson Mauricio
PASS-BIO	Contraseña Biométricas para acceso a la sala de servidor	Pimiento Cárdenas Wilson Mauricio
PASS-SERVER	Contraseña de los usuarios que acceden a los servidores	Pimiento Cárdenas Wilson Mauricio
PASS-SERVER-BACK UP	Contraseña del servidor de copias de seguridad	Pimiento Cárdenas Wilson Mauricio
PASS-PC-ITFIP	Contraseña de los usuarios de los Pc de las demás dependencias	Pimiento Cárdenas Wilson Mauricio
C-CASERVER	Código de confirmación para acceso a la sala de servidor	Pimiento Cárdenas Wilson Mauricio
S-RYCA1	Sistema de Registro y Control Académico (RYCA) V.1	Pimiento Cárdenas Wilson Mauricio
S-RYCA2	Sistema de Registro y Control Académico (RYCA) V.2.0	Pimiento Cárdenas Wilson Mauricio
P-ITFIP	Página Oficial del ITFIP	Pimiento Cárdenas Wilson Mauricio
G-CHROME	Google Chrome	Pimiento Cárdenas Wilson Mauricio
M-F	Mozilla Firefox	Pimiento Cárdenas Wilson Mauricio
SAFI	Safari	Pimiento Cárdenas Wilson Mauricio
M-OFFICE	Microsoft Office 2013	Pimiento Cárdenas Wilson Mauricio
O-OLINUX	Open Office Linux 2017	Pimiento Cárdenas Wilson Mauricio
S-CENTER	System Center	Pimiento Cárdenas Wilson Mauricio

Tabla 17. Consecutivo y responsable de cada activo. (Continuación)

W-DEFEN	Windows Defender	Pimiento Cárdenas Wilson Mauricio
W-8	Windows 8	Pimiento Cárdenas Wilson Mauricio
W-SER09	Windows Server 2009	Pimiento Cárdenas Wilson Mauricio
W-SER12	Windows Server 2012	Pimiento Cárdenas Wilson Mauricio
C-5	CentOS 5	Pimiento Cárdenas Wilson Mauricio
D-7	Debian 7	Pimiento Cárdenas Wilson Mauricio
U-14	Ubuntu 14	Pimiento Cárdenas Wilson Mauricio
M-OSX	Mac OS X	Pimiento Cárdenas Wilson Mauricio
CMD	CoMmanD (CMD)	Pimiento Cárdenas Wilson Mauricio
C-LMAC	CoMmanD line (Mac)	Pimiento Cárdenas Wilson Mauricio
TERM	Terminal	Pimiento Cárdenas Wilson Mauricio
ITFIP	ITFIP	Pimiento Cárdenas Wilson Mauricio
ITFIP 2	ITFIP 2	Pimiento Cárdenas Wilson Mauricio
ITFIP_P1	ITFIP_P1	Pimiento Cárdenas Wilson Mauricio
ITFIP_FUNCIONARIOS_P1	ITFIP_FUNCIONARIOS_P1	Pimiento Cárdenas Wilson Mauricio
ITFIP_FUNCIONARIOS_P1	ITFIP_FUNCIONARIOS_P1	Pimiento Cárdenas Wilson Mauricio
Salas1y2	Salas1y2	Pimiento Cárdenas Wilson Mauricio
Salas_Sis2	Salas_Sis2	Pimiento Cárdenas Wilson Mauricio
Rectoría	Rectoría	Pimiento Cárdenas Wilson Mauricio
DSK1024	DDS 1TB	Pimiento Cárdenas Wilson Mauricio
O-PD	Oficina principal de la dependencia	Pimiento Cárdenas Wilson Mauricio
P-IM	Proveedor de Internet Movistar	Movistar

Tabla 17. Consecutivo y responsable de cada activo. (Continuación)

Prg	Pimiento Cárdenas Wilson Mauricio	Muñoz López Jhon Darwin
C-DDS	Muñoz López Jhon Darwin	Isabel Ortiz Serrano
A-MR	Juan Sebastián Laguna	Muñoz López Jhon Darwin
Ing. Aux	Melisa Rivera Sánchez	Muñoz López Jhon Darwin
22400659	Alcatel lucent 1port802.3af po	Pimiento Cárdenas Wilson Mauricio

Fuente propia

2.5. INVENTARIOS DE ACTIVOS APLICANDO LA METODOLIA MAGERIT

Tabla 18. Clasificación de activos según MAGERIT.

Código grupo de activo MAGERIT	Nombre grupo de activo MAGERIT	Nombre del activo	Descripción	Código Consecutivo ITFIP	Nombre de activo ITFIP	Función
Esenciales						
[vr]	datos vitales	Documentos de la organización	En este activo se almacén a el registro de los usuarios de la parte administrativa.	I-DU	Inventario de usuarios	Poseer el contenido crucial, en el cual, llegado el momento de caída accidental u ocasionada del sistema, se pueda corregir de manera eficiente, permitiéndose así optimizar el tiempo de respuesta.
			Este activo almacén a cada una de las dependencias que tiene la institución.	E-ORG	estructura organizacional	
			Este activo guarda el registro de los contratos.	I-DC	Inventario de contratos	
			Este activo lleva un registro de las actividades que se realizan.	R-DA	Registro de actividades	

Tabla 18. Clasificación de activos según MAGERIT. (Continuación)

			Este activo lleva el registro de los mantenimientos realizados.	R-ME	Registro Mantenimiento equipos	
			Este activo guarda el registro de la arquitectura de los equipos que requieren.	R-AE	Registro de la arquitectura de los equipos	
[service]	Servicios	Servicios ofrecidos de todas las dependencias del ITFIP	Este activo ofrece el servicio de soporte de equipos de cómputo.	S-EC	Soporte equipos de computo	Se encarga del mantenimiento correctivo y preventivo de todos los equipos administrativos de la institución y a las plataformas virtuales.
			Este activo ofrece el servicio de brindarle soporte a las plataformas virtuales.	S-PV	Soporte de plataformas virtuales	
Arquitectura del sistema						
[ip]	punto de interconexión	VLAN	Este activo es la red virtual de administración para poder comunicarse entre ellos.	VLAN-ADMON	Vlan de administración	Su función principal es separar de manera ordenada y optima

Tabla 18. Clasificación de activos según MAGERIT. (Continuación)

			Este activo es la red virtual de financiera para poder comunicarse entre ellos.	VLAN-FINAN	Vlan de financiera	cada una de las dependencias que se someten a los servicios de sistemas, permitiéndoles así, trabajar de manera más cercana entre sus propios núcleos.
			Este activo es la red virtual de tesorería para poder comunicarse entre ellos.	VLAN-TESO	Vlan de tesorería	
			Este activo es la red virtual de estudiantes para poder comunicarse entre ellos.	VLAN-EST	Vlan de estudiantes	
			Este activo es la red virtual de WIFI para poder brindar soporte en caso de algún daño.	V-WIFI	Vlan de wifi	
			Este activo es la red virtual de configuración para poder configurar equipos de manera remota.	VLAN-CONF	Vlan de configuración	

Tabla 18. Clasificación de activos según MAGERIT. (Continuación)

			Este activo es la red virtual de sistemas para poder comunicarse entre ellos.	VLAN-SIS	Vlan de sistemas	
			Este activo es la red virtual de RYCA para poder comunicarse entre ellos.	VLAN-RYCA	Vlan de registro y control	
			Este activo es la red virtual de almacén para poder comunicarse entre ellos.	VLAN-ALMA	Vlan de almacén	
			Este activo es la red virtual de Talento Humano para poder comunicarse entre ellos.	VLAN-TALEN	Vlan de talento humano	
Datos/Información						
[backup]	copias de respaldo	Copias de seguridad	Este activo registra cada una de las copias de seguridad que se les hacen a los	BACK UP-SISTEMAS	De cada pc de la dependencia de sistemas	Salvaguardar la información que se recolecta a

Tabla 18. Clasificación de activos según MAGERIT. (Continuación)

			equipos de sistemas.			diario, previniendo así la perdida de esta, lo cual, puede desencadenar a la perdida de la historia de la institución si no se maneja con cautela,
			Este activo registra cada una de las copias de seguridad que se les hacen a los equipos de la institución.	BACK UP-ITFIP	de cada pc de las dependencias de la institución	
			Este activo registra cada una de las copias de seguridad que se les hacen a los servidores.	BACK UP-SERVER'S	de las configuraciones de los servidores	
[password]	Credenciales	Contraseñas de seguridad	Este activo contiene las contraseñas biométricas que dan acceso a la sala principal de servidores.	PASS-BIO	Biométricas para acceso a la sala de servidor	Su función es dar un filtro a la cantidad de personas que pueden acceder a un sistema o zona en específico, reduciendo el número de personas
			Este activo contiene las contraseñas con las que acceden los administradores a los servidores.	PASS-SERVER	De los usuarios que acceden a los servidores	

Tabla 18. Clasificación de activos según MAGERIT. (Continuación)

			Este activo contiene las contraseñas del servidor de copias de seguridad de la institución.	PASS-SERVER-BACK UP	servidor de copias de seguridad	que puede manipular la información.
[Files]	Ficheros	Archivos	Son todos los archivos planos que se pueden identificar como códigos de programación, archivos en Excel etc.			Se encarga de tener de manera digital la información del departamento de sistemas.
Claves criptográficas						

Tabla 18. Clasificación de activos según MAGERIT. (Continuación)

[info]	protección de la información	Credenciales externas	Para este active, se permite la creación de credenciales para los diferentes accesos a los sistemas, como también de la información que allí se alberga.	PASS-PC-ITFIP	Usuarios de los Pc de las demás dependencias	Permitir o restringir el paso a personas que son o no autorizadas a manipular, visualizar, transportar entre otros la información concerniente a la dependencia de sistemas u otro sitio.
[encrypt]	claves de cifra	Sistema de acceso	Este activo gestiona a través de herramientas las personas que pueden generar paso a otras, por lo general es administrada por el coordinador del área en	S-BIO	Sensor biométrico	Mantener bajo constante monitoreo las personas que tienen acceso a la información, conocer qué tipo de

Tabla 18. Clasificación de activos según MAGERIT. (Continuación)

			donde esta se encuentra.			información manipulan y el uso que se le da a la misma.
[authentication]	claves de autenticación	Contraseña de autenticación	Dicho activo consiste en asignar predeterminadamente una contraseña, que permite identificar que usuario y a donde tiene permitido el acceso.	C-CASERVER	Código de confirmación para acceso a la sala de servidor	Este activo permite controlar que personas tienen control de usuarios por parte de la plataforma.
[prp]	desarrollo propio (in house)	Desarrollo propio (Ryca1 y Ryca2)	Este activo contiene todo el código y software que maneja la plataforma RYCA V.1 para su desarrollo o mantenimiento.	S-RYCA1	Sistema de Registro y Control Académico (RYCA) V.1	Este activo contiene la información concerniente de la carga académica, personal educativo, docentes, administrativos entre otros.
			Este activo contiene todo el código y software que maneja la plataforma	S-RYCA2	Sistema de Registro y Control Académico (RYCA) V.2.0	

Tabla 18. Clasificación de activos según MAGERIT. (Continuación)

			RYCA V.2.0 para su desarrollo o mantenimiento.			
[www]	Servidor de presentación	Página de la institución	En este activo se da conocer a la institución por medio del portal web, que a su vez da acceso a la información al personal externo de la misma	P-ITFIP	Página Oficial del ITFIP	La función plena del portal es mantener al tanto al personal de la institución, tenerla informada acerca de los planes educativos, fechas de ingreso, calendario académico, etc. Además, contiene la información esencial publica de la institución.
[browser]	navegador web	Navegadores	Este activo es el navegador web, utilizado para	G-CHROME	Google Chrome	La función de este activo es la

Tabla 18. Clasificación de activos según MAGERIT. (Continuación)

			múltiples funciones de trabajo.			de permitir el acceso a la información encontrada en las nubes internas y externas de la institución, abrir paginas locales y demás.
			Este activo es el navegador web, utilizado para múltiples funciones de trabajo.	M-F	Mozilla Firefox	
			Este activo es el navegador web, utilizado para múltiples funciones de trabajo.	SAFI	Safari	
[office]	Ofimática	Herramientas ofimáticas	Las herramientas ofimáticas permiten editar archivos planos.	M-OFFICE	Microsoft Office 2013	Este activo es de provecho para la institución, puesto que permite la creación de documentos escritos tales como cartas; presentación de elementos en
			Las herramientas ofimáticas permiten editar archivos planos.	O-OLINUX	Open Office Linux 2017	

Tabla 18. Clasificación de activos según MAGERIT. (Continuación)

						PowerPoint, además, del uso de cálculos básicos y avanzados a través de la herramienta de Excel.
[av]	antivirus	Antivirus	Este activo protege de virus que puedan afectar la información.	S-CENTER	System Center	Este software permite el escaneo de los archivos localizados en cada uno de los componentes del pc, a su vez, este permite alzar una emergencia al detectar archivos infecciosos o malware.
			Este activo protege de virus que puedan afectar la información.	W-DEFEN	Windows Defender	
[os]	sistema operativo	Sistemas operativos	Los sistemas operativos,	W-8	Windows 8	Este activo, permite

Tabla 18. Clasificación de activos según MAGERIT. (Continuación)

			permiten poner en funcionamiento el hardware con el cual se cuenta, a su vez, administrar cada una de sus funciones lógicas.			estructurar de manera lógica cada una de las tareas lógicas otorgadas o en plan de ejecución.
			Este activo es utilizado para administrar y configurar los servidores.	W-SER09	Windows Server 2009	
			Este activo es utilizado para administrar y configurar los servidores.	W-SER12	Windows Server 2012	
			Este activo es utilizado para brindar acompañamiento a la seguridad de la información.	C-5	CentOS 5	
			Este activo es utilizado para brindar acompañamiento	D-7	Debian 7	

Tabla 18. Clasificación de activos según MAGERIT. (Continuación)

			a la seguridad de la información.			
			Los sistemas operativos, permiten poner en funcionamiento el hardware con el cual se cuenta, a su vez, administrar cada una de sus funciones lógicas.	U-14	Ubuntu 14	
			Los sistemas operativos, permiten poner en funcionamiento el hardware con el cual se cuenta, a su vez, administrar cada una de sus funciones lógicas.	M-OSX	Mac OS X	
[ts]	servidor de terminales	Servicio de terminal	Es un componente perteneciente a cada uno de los	CMD	CoMmanD (CMD)	Manejar o dar órdenes de manera

Tabla 18. Clasificación de activos según MAGERIT. (Continuación)

			sistemas operativos			escrita, sin uso de interfaz gráfica, con lo cual, permite agilizar los procesos disminuyendo el consumo de recursos.
				C-LMAC	CoMmanD line (Mac)	
				TERM	Terminal	
Equipamiento Informático (Hardware)						
[host]	equipos grandes	Servidor que contiene el dominio de cada uno de los equipos dentro de la institución, maneja un DNS y un DHCP	Un servidor es un equipo de alta gama que se permite configurar para dar/ofrecer un servicio en específico.	S-DNS	Servidor DNS y DHCP	Distribución y administración de los servicios de DNS y DHCP

Tabla 18. Clasificación de activos según MAGERIT. (Continuación)

[host]	equipos grandes	Servidor de la plataforma RYCA V.2.0.	Un servidor es un equipo de alta gama que se permite configurar para dar/ofrecer un servicio en específico.	S-RYCA2	Servidor Plataforma RYCA V.2.0	En este activo se contiene la información concerniente a la plataforma de RYCA V.2.0.
[host]	equipos grandes	Servidor que contiene las máquinas virtuales de RYCA1 y la plataforma	Un servidor es un equipo de alta gama que se permite configurar para dar/ofrecer un servicio en específico.	S-RYCA1	Servidor Plataforma RYCA V.1	En este activo se contiene la información concerniente a la plataforma de RYCA V.1.
[host]	equipos grandes	Servidor de base de datos	Un servidor es un equipo de alta gama que se permite configurar para dar/ofrecer un servicio en específico.	S-BD	Servidor de Base de Datos ITFIP	Para este servicio, se categoriza toda la información contenida en la institución y se pone a disposición para los demás

Tabla 18. Clasificación de activos según MAGERIT. (Continuación)

						servicios internos.
[host]	equipos grandes	Servidor de cortafuegos	Un servidor es un equipo de alta gama que se permite configurar para dar/ofrecer un servicio en específico.	S-FIREW	Servidor Firewall Fortigate	Dicha función de este activo es la de tener en restricción los accesos de usuarios NO autorizados por el sistema.
[host]	equipos grandes	Servidor que contiene a SIIGO	Un servidor es un equipo de alta gama que se permite configurar para dar/ofrecer un servicio en específico.	S-SIIGO	Servidor Contable SIIGO	En este servicio, se contiene toda la información contable de la institución.
[host]	equipos grandes	Servidor de Pruebas “Desarrollito”	Un servidor es un equipo de alta gama que se permite configurar para dar/ofrecer un servicio en específico.	S-PDESA	Servidor de Pruebas “Desarrollito”	Sirve para hacer pruebas de los nuevos módulos de las plataformas

Tabla 18. Clasificación de activos según MAGERIT. (Continuación)

[host]	equipos grandes	Servidor de Copias de seguridad de la institución	Un servidor es un equipo de alta gama que se permite configurar para dar/ofrecer un servicio en específico.	S-CSECURITY	Servidor de Copias de seguridad de la información del ITFIP	Contiene las copias de seguridad de la información del ITFIP
[mid]	equipos medios (hw)	Computadores Apple	Equipos de cómputo utilizado para emplear la digitación de código u otros	022400532 AL 022400534	Computador IMAC APPLE (3 Equipos)	Debido a su gran calidad de imagen, rapidez y demás componentes que le permiten sobresalir son empleados para el desarrollo y la edición de páginas web como de programas locales.
[mid]	equipos medios (hw)	Computadores HP all-one Pro	Equipo todo en uno	022400570 AL	Computadores HP all-one Pro (18 Equipos)	Uso para las tareas

Tabla 18. Clasificación de activos según MAGERIT. (Continuación)

				022400192		que requieran.
[pc]	informática personal	Portátil Toshiba	Este equipo permite llevar varias tareas a cabo de manera estructurada y eficiente.	022400540 AL 022400565	Portátil Toshiba (16 equipos)	La funcionalidad de cada uno de estos equipos varía dependiendo del enfoque a la que le aplique su uso.
[mobile]	informática móvil	Tablet negra 9”	Este equipo permite llevar varias tareas a cabo de manera estructurada y eficiente	022400675	Tablet negra 9” (1 Equipo)	La funcionalidad de cada uno de estos equipos varía dependiendo del enfoque a la que le aplique su uso.
[backup]	equipamiento de respaldo(hw)	Equipo de respaldo	Son aquellos equipos preparados para	022400534 AL	Computador IMAC APPLE (3 Equipos)	Los utilizan para respaldar

Tabla 18. Clasificación de activos según MAGERIT. (Continuación)

			hacerse cargo inmediato de los equipos en producción.	022400537		cuando los equipos se dañan.
[peripheral]	periféricos	Periférico	Los periféricos son dispositivos de salida/entrada/mixtos, lo que permite la recepción de información al usuario	MUSB234	Memoria USB	Algunos de ellos son empleados como almacén adores de información, backups, entre otros
				DD234	Discos duros	
				DDX334	Discos duros externos	
[switch]	conmutadores(hw)	Conmutadores	Este activo permite la interconexión con las diferentes redes existentes.	020700059	SWITCH ALCATEL LUCENT 9553	Este activo, permite a su vez, conectar varias redes, ampliar el número de computadores que se puedan conectar a una misma red.
				020700130	SWITCH 24 10/100/1000 BASE T C SWITCH 24 10/100/1000 BASE T C	
				020700158	SWITCH 24/10/100/1000 BASE T4S	
				020700136	SWITCH 24/10/100/1000PWR CORD	
				020700067	SWITCH ALCATEL LUCEN 9561	
				020700062	SWITCH ALCATEL LUCENT 9556	

Tabla 18. Clasificación de activos según MAGERIT. (Continuación)

				020700063	SWITCH ALCATEL LUCENT 9557	
				020700064	SWITCH ALCATEL LUCENT 9558	
				020700065	SWITCH ALCATEL LUCENT 9559	
				020700049	SWITCH ALCATEL LUCENT 9543	
				020700050	SWITCH ALCATEL LUCENT 9544	
				020700051	SWITCH ALCATEL LUCENT 9545	
				020700054	SWITCH ALCATEL LUCENT 9548	
				020700056	SWITCH ALCATEL LUCENT 9550	
				020700057	SWITCH ALCATEL LUCENT 9551	
				020700058	SWITCH ALCATEL LUCENT 9552	
				020700060	SWITCH ALCATEL LUCENT 9554	
				020700061	SWITCH ALCATEL LUCENT 9555	
				020700066	SWITCH ALCATEL LUCENT 9560	
				020700080	SWITCH LAYER 3 9574	
				020700082	SWITCH LAYER 3 9576	

Tabla 18. Clasificación de activos según MAGERIT. (Continuación)

				020700083	SWITCH LAYER 3 9577	
				020700081	SWITCH LAYER 3 9575	
[router]	encaminadores (hw)	Router	Este activo permite la direccionar a los diferentes canales de información.		ROUTER CISCO MODELO 1800 4781	Para este activo, es indispensable tener definidas cada uno de los diferentes canales de distribución.
[pabx]	centralita telefónica(hw)	Central telefónica	Esta sección de los activos permite conectar dependencias o instancias de diferentes entidades internas.			Como función especial, la central telefónica busca tener comunicación instantánea con cada una de las dependencias que se encuentran entrelazadas.

Tabla 18. Clasificación de activos según MAGERIT. (Continuación)

Redes de comunicación						
[PSTN]	Red de telefonía	Red teleónica	Una red telefónica, es aquella que entrelaza entre si varias líneas telefónicas internas.			Como función especial, la red telefónica busca tener comunicación instantánea con cada una de las dependencias que se encuentran entrelazadas.
[INTERNET]	Internet	Internet Movistar	Este activo, es un servicio de internet externo, que como su nombre lo indica concede el acceso a la navegación por medio de sus fibras.			Su función principal, es conceder navegación a internet a cada una de las redes instanciadas de manera interna.

Tabla 18. Clasificación de activos según MAGERIT. (Continuación)

[LAN]	Red Local	Red LAN	Es una red que trasmite paquetes de datos por medio de cableado estructurado.			La red de navegación LAN, permite la transmisión de archivos de manera más ágil y privada, siendo esta segmentada.
[WIFI]	Red Wifi	Red WIFI	Las redes Wifi, permiten de igual manera, la conexión y transmisión de archivos, pero de manera inalámbrica.		ITFIP ITFIP 2 ITFIP_P1 ITFIP_FUNCIONARIOS_P1 Salas1y2 Salas_Sis2 Rectoría	La función principal de este activo en la institución es permitir que la comunidad académica y administrativa, tenga acceso a la red de navegación.
[X25]	Red de datos	Red de datos	Es la comunicación de máquinas por			Suple la misma función que

Tabla 18. Clasificación de activos según MAGERIT. (Continuación)

			medios cableados y no cableados.			la red Wifi y la red LAN.
[disk]	discos	Discos duros	Un disco duro es un dispositivo de almacén amiento físico.	DSK1024	DDS1TB	Este activo permite salvaguardar cada una de las copias de seguridad generadas, principalmente en cada uno de sus procesos más importantes
[printed]	Materiales impresos	Materiales físicos	Todo aquel dispositivo de consistencia física, que permita almacenar información (DD, Memorias, CD, CD/DVD, etc.)			Este activo en especial permite el respaldo de la información en cualquier momento, puesto que es aquel que se encuentra aislado de

Tabla 18. Clasificación de activos según MAGERIT. (Continuación)

						demás funciones a excepción, de almacenar.
Equipamiento Auxiliar						
[ups]	sistemas de alimentación ininterrumpida	UPS	Un UPS, es un sistema de alimentación de energía interrumpida,	02240052 6	UPS 10 KVA 9578	La función de esta herramienta es priorizar cada uno de los servicios que el alimenta de manera indirecta cada vez haya un fallo de energía
				02240052 7	UPS 10 KVA 9579	
				02240052 8	UPS 10 KVA 9580	
[supply]	Suministros esenciales	suministros esenciales	Estos suministros esenciales son necesarios para funcionar la institución con su totalidad de comodidades.			Suplir las necesidades básicas en cuanto infraestructura corresponde.

Tabla 18. Clasificación de activos según MAGERIT. (Continuación)

[furniture]	Mobiliario	mobiliario	Lugar en el cual se encuentra el establecimiento.			Albergar todo lo relacionado de la empresa para su cómodo funcionamiento y servicio
[site]	recinto Cuarto o recinto (Oficina)		El recinto es la sección u/o edificio en donde se encuentra albergado para operar.			
Personal						
[adm]	Administradores de sistemas	Coordinador de sistemas				
[des]	Desarrollador	Programador				
[Sub]	subcontratas	Ingeniero Auxiliar/ Soporte técnico				

Fuente: Autoría Propia

2.6. VALORACIÓN DE LOS ACTIVOS SEGÚN SU IMPORTANCIA

Tabla 19. Valoración para cada uno de los activos de la dependencia de sistemas.

Código grupo de activo MAGERIT	Nombre grupo de activo MAGERIT	Nombre del activo	Descripción	Código Consecutivo ITFIP	Nombre de activo ITFIP	Función	Valoración
Esenciales							
[vr]	datos vitales	Documentos de la organización	En este activo se almacéna el registro de los usuarios de la parte administrativa.	I-DU	Inventario de usuarios	Poseer el contenido crucial, en el cual, llegado el momento de caída accidental u ocasionada del sistema, se pueda corregir de manera eficiente, permitiéndose así	100
							100
			Este activo almacéna cada una de las dependencias que tiene la institución.	E-ORG	estructura organizacional		100
			Este activo guarda el registro de los contratos.	I-DC	Inventario de contratos		100

Tabla 19. Valoración para cada uno de los activos de la dependencia de sistemas (Continuación)

			Este activo lleva un registro de las actividades que se realizan.	R-DA	Registro de actividades	optimizar el tiempo de respuesta.	100
			Este activo lleva el registro de los mantenimientos realizados.	R-ME	Registro Mantenimiento equipos		100
			Este activo guarda el registro de la arquitectura de los equipos que requieren.	R-AE	Registro de la arquitectura de los equipos		100
[service]	Servicios	Servicios ofrecidos de todas las dependenci	Este activo ofrece el servicio de soporte de equipos de cómputo.	S-EC	Soporte equipos de computo	Se encarga del mantenimiento correctivo y preventivo de	100

Tabla 19. Valoración para cada uno de los activos de la dependencia de sistemas (Continuación)

		as del ITFIP	Este activo ofrece el servicio de brindarle soporte a las plataformas virtuales.	S-PV	Soporte de plataformas virtuales	todos los equipos administrativos de la institución y a las plataformas virtuales.	100
Arquitectura del sistema							
[ip]	punto de interconexión	VLAN	Este activo es la red virtual de administración para poder comunicarse entre ellos.	VLAN - ADMON	Vlan de administración	Su función principal es separar de manera ordenada y optimacada una de las dependencias que se someten a los servicios de sistemas, permitiéndole	100
			Este activo es la red virtual de financiera para poder comunicarse entre ellos.	VLAN - FINAN	Vlan de financiera		100
			Este activo es la red virtual de tesorería para poder	VLAN - TESO	Vlan de tesorería		100

Tabla 19. Valoración para cada uno de los activos de la dependencia de sistemas (Continuación)

			comunicarse entre ellos.			s así, trabajar de manera más cercana entre sus propios núcleos.	
			Este activo es la red virtual de estudiantes para poder comunicarse entre ellos.	VLAN-EST	Vlan de estudiantes		100
			Este activo es la red virtual de WIFI para poder brindar soporte en caso de algún daño.	V-WIFI	Vlan de wifi		100
			Este activo es la red virtual de configuración para poder configurar equipos de manera remota.	VLAN-CONF	Vlan de configuración		100
			Este activo es la red virtual de sistemas para poder	VLAN-SIS	Vlan de sistemas		100

Tabla 19. Valoración para cada uno de los activos de la dependencia de sistemas (Continuación)

			comunicarse entre ellos.				
			Este activo es la red virtual de RYCA para poder comunicarse entre ellos.	VLAN-RYCA	Vlan de registro y control		100
			Este activo es la red virtual de almacén para poder comunicarse entre ellos.	VLAN-ALMA	Vlan de almacén		100
			Este activo es la red virtual de Talento Humano para poder comunicarse entre ellos.	VLAN-TALEN	Vlan de talento humano		100
Datos/Información							
[backup]	copias de respaldo	Copias de seguridad	Este activo registra cada una de las copias de seguridad que se	BACKUP-SISTEMAS	De cada pc de la dependencia de sistemas	Salvaguardar la información que se recolecta a	90

Tabla 19. Valoración para cada uno de los activos de la dependencia de sistemas (Continuación)

			les hacen a los equipos de sistemas.			diario, previniendo así la perdida de esta, lo cual, puede desencadenar a la perdida de la historia de la institución si no se maneja con cautela.	
			Este activo registra cada una de las copias de seguridad que se les hacen a los equipos de la institución.	BACK UP-ITFIP	de cada pc de las dependencias de la institución		95
			Este activo registra cada una de las copias de seguridad que se les hacen a los servidores.	BACK UP-SERVER'S	de las configuraciones de los servidores		100
[password]	Credenciales	Contraseñas de seguridad	Este activo contiene las contraseñas biométricas que dan acceso a la sala principal de	PASS-BIO	Biométricas para acceso a la sala de servidor	Su función es dar un filtro a la cantidad de personas que pueden acced	100

Tabla 19. Valoración para cada uno de los activos de la dependencia de sistemas (Continuación)

			servidores.			er a un sistema o zona en específico, reduciendo el número de personas que puede manipular la información.	
			Este activo contiene las contraseñas con las que acceden los administradores a los servidores.	PASS-SERVER	De los usuarios que acceden a los servidores		100
			Este activo contiene las contraseñas del servidor de copias de seguridad de la institución.	PASS-SERVER-BACK UP	servidor de copias de seguridad		100
[Files]	Ficheros	Archivos	Son todos los archivos planos que se pueden identificar como códigos de programación, archivos			Se encarga de tener de manera digital la información del department	80

Tabla 19. Valoración para cada uno de los activos de la dependencia de sistemas (Continuación)

			en Excel etc.			o de sistemas.	
Claves criptográficas							
[info]	protección de la información	Credenciales externas	Para este active, se permite la creación de credenciales para los diferentes accesos a los sistemas, como también de la información que allí se alberga.	PASS-PC-ITFIP	Usuarios de los Pc de las demás dependencias	Permitir o restringir el paso a personas que son o no autorizadas a manipular, visualizar, transportar entre otros la información concerniente a la dependencia de sistemas u otro sitio.	80
[encrypt]	claves de cifra	Sistema de acceso	Este activo gestiona a través de herramientas las personas	S-BIO	Sensor biométrico	Mantener bajo constante monitoreo las person	80

Tabla 19. Valoración para cada uno de los activos de la dependencia de sistemas (Continuación)

			que pueden generar paso a otras, por lo general es administrada por el coordinador del área en donde esta se encuentra.			as que tienen acceso a la información, conocer qué tipo de información manipulan y el uso que se le da a la misma.	
[authentication]	claves de autenticación	Contraseña de autenticación	Dicho activo consiste en asignar predeterminadamente una contraseña, que permite identificar que usuario y ha donde tiene permitido el acceso.	C-CASERVER	Código de confirmación para acceso a la sala de servidor	Este activo permite controlar que personas tienen control de usuarios por parte de la plataforma.	100
Aplicaciones (Software)							
[prp]	desarrollo propio (in house)	Desarrollo propio (Ryca 1 y	Este activo contiene todo el código y	S-RYCA1	Sistema de Registro y Control Académico (RYCA) V.1	Este activo contiene la inform	100

Tabla 19. Valoración para cada uno de los activos de la dependencia de sistemas (Continuación)

		Ryca2)	software que maneja la plataforma RYCA V.1 para su desarrollo o mantenimiento.			ación concerniente de la carga académica, personal educativo, docentes, administrativos entre otros.	
			Este activo contiene todo el código y software que maneja la plataforma RYCA V.2.0 para su desarrollo o mantenimiento.	S-RYCA2	Sistema de Registro y Control Académico (RYCA) V.2.0		100
[www]	Servidor de presentación	Página de la institución	En este activo se da conocer a la institución por medio del portal web, que a su vez da acceso a la informaci	P-ITFIP	Página Oficial del ITFIP	La función plena del portales mantener al tanto al personal de la institu	90

Tabla 19. Valoración para cada uno de los activos de la dependencia de sistemas (Continuación)

			ón al personal externo de la misma			ción, tenerla informada acerca de los planes educativos, fechas de ingreso, calendario académico, etc. Además, contiene la información esencial pública de la institución.	
[browser]	navegador web	Navegadores	Los navegadores permiten abrir los motores de búsqueda, como también las aplicaciones locales	G-CHROME	Google Chrome	La función de este activo es la de permitir el acceso a la información encont	50
				M-F	Mozilla Firefox		45
				SAFI	Safari		40

Tabla 19. Valoración para cada uno de los activos de la dependencia de sistemas (Continuación)

			desarrolladas para ambiente web.			rada en las nubes internas y externas de la institución, abrir paginas locales y demás.	
[office]	Ofimática	Herramientas ofimáticas	Las herramientas ofimáticas permiten editar archivos planos.	M-OFFICE	Microsoft Office 2013	Este activo es de provecho para la institución, puesto que permite la creación de documentos escritos tales como cartas; presentación de elementos en Power	50
				O-OLINUX	Open Office Linux 2017		45

Tabla 19. Valoración para cada uno de los activos de la dependencia de sistemas (Continuación)

						Point, además, del uso de cálculos básicos y avanzados a través de la herramienta de Excel.	
[av]	antivirus	Antivirus	Este activo protege de virus que puedan afectar la información.	S-CENTER	System Center	Este software permite el escaneo de los archivos localizados en cada uno de los componentes del pc, a su vez, este permite alzar una emergencia al	80
			Este activo protege de virus que puedan afectar la información.	W-DEFEN	Windows Defender		80

Tabla 19. Valoración para cada uno de los activos de la dependencia de sistemas (Continuación)

						detectar archivos infecciosos o malware.	
[os]	sistema operativo	Sistemas operativos	Los sistemas operativos, permiten poner en funcionamiento el hardware con el cual se cuenta, a su vez, administrar cada una de sus funciones lógicas.	W-8	Windows 8	Este activo, permite estructurar de manera lógica cada una de las tareas lógicas otorgadas o en plan de ejecución.	90
				W-SER09	Windows Server 2009		90
				W-SER12	Windows Server 2012		100
				C-5	CentOS 5		100
				D-7	Debian 7		90
				U-14	Ubuntu 14		80
				M-OSX	Mac OS X		100
[ts]	servidor de terminales	Servicio de terminal	Es un componente perteneciente a cada uno de los sistemas operativos, utilizado para administr	CMD	CoMmanD (CMD)	Manejar o dar órdenes de manera escrita, sin uso de interfaz gráfica	75
				C-LMAC	CoMmanD line (Mac)		100
				TERM	Terminal		90

Tabla 19. Valoración para cada uno de los activos de la dependencia de sistemas (Continuación)

			ador por medio de comandos los servicios que ofrecen.			, con lo cual, permite agilizar los procesos disminuyendo el consumo de recursos.	
Equipamiento Informático (Hardware)							
[host]	equipos grandes	Servidor que contiene el dominio de cada uno de los equipos dentro de la institución, maneja un DNS y un DHCP	Este activo es el encargado distribuir dinámicamente una IP a cada equipo conectado.	S-DNS	Servidor DNS y DHCP	Distribución y administración de los servicios de DNS y DHCP	100
[host]	equipos grandes	Servidor de la plataforma RYCA V.2.0.	Este activo contiene todo el código y configuraciones	S-RYCA2	Servidor Plataforma RYCA V.2.0	En este activo se contiene la inform	100

Tabla 19. Valoración para cada uno de los activos de la dependencia de sistemas (Continuación)

			del software de RYCA V.2.0.			ación concerniente a la plataforma de RYCA V.2.0.	
[host]	equipos grandes	Servdor que contiene las máquinas virtuales de RYCA 1 y la plataforma	Este activo contiene todo el código y configuraciones del software de RYCA V.1.	S-RYCA1	Servidor Plataforma RYCA V.1	En este activo se contiene la información concerniente a la plataforma de RYCA V.1.	100
[host]	equipos grandes	Servidor de base de datos	Este activo contiene toda la información de la institución en una base de datos.	S-BD	Servidor de Base de Datos ITFIP	Para este servicio, se categoriza toda la información contenida en la institución y se pone a disposición para	100

Tabla 19. Valoración para cada uno de los activos de la dependencia de sistemas (Continuación)

						los demás servicios internos.	
[host]	equipos grandes	Servidor de cortafuegos	Este activo es el encargado de toda la seguridad de la red, servidores e información que tiene la información.	S-FIREW	Servidor Firewall Fortigate	Dicha función de este activo es la de tener en restricción los accesos de usuarios NO autorizados por el sistema.	100
[host]	equipos grandes	Servidor que contiene a SIIGO	Este activo maneja toda la información contable de la institución.	S-SIIGO	Servidor Contable SIIGO	En este servicio, se contiene toda la información contable de la institución.	100
[host]	equipos grandes	Servidor de Prueb	Este activo es utilizado	S-PDESA	Servidor de Pruebas “Desarrollito”	Sirve para hacer	80

Tabla 19. Valoración para cada uno de los activos de la dependencia de sistemas (Continuación)

		as “Desarrollito”	para pruebas de nuevas actualizaciones a las plataformas.			pruebas de los nuevos módulos de las plataformas	
[host]	equipos grandes	Servidor de Copias de seguridad de la institución	Este activo almacéna toda la información de las dependencias de la institución.	S-CSECURITY	Servidor de Copias de seguridad de la información del ITFIP	Contiene las copias de seguridad de la información del ITFIP	100
[mid]	equipos medios (hw)	Computadores Apple	Equipos de cómputo utilizado para emplear la digitación de código u otros.	022400532AL 022400534	Computador IMAC APPLE (3 Equipos)	Debido a su gran calidad de imagen, rapidez y demás componentes que le permiten sobresalir son empleados para el desarrollo y	80

Tabla 19. Valoración para cada uno de los activos de la dependencia de sistemas (Continuación)

						la edición de páginas web como de programas locales.	
[mid]	equipos medios (hw)	Computadores HP all-one Pro	Equipo todo en uno	02240057 0 AL 02240019 2	Computadores HP all-one Pro (18 Equipos)	Uso para las tareas que requieran.	80
[pc]	informática personal	Portátil Toshiba	Este equipo permite llevar varias tareas a cabo de manera estructurada y eficiente	02240054 0 AL 02240056 5	Portátil Toshiba (16 equipos)	La funcionalidad de cada uno de estos equipos varía dependiendo del enfoque a la que le aplique su uso.	80
[mobile]	informática móvil	Tablet negra 9”	Este equipo permite llevar varias tareas a cabo de manera	02240067 5	Tablet negra 9” (1 Equipo)	La funcionalidad de cada uno de estos equipo	70

Tabla 19. Valoración para cada uno de los activos de la dependencia de sistemas (Continuación)

			estructurada y eficiente.			s varía dependiendo del enfoque a la que le apliqu e su uso.	
[backup]	equipamiento de respaldo (hw)	Equipo de respaldo	Son aquellos equipos preparados para hacerse cargo inmediato de los equipos en producción.	02240053 4 AL 02240053 7	Computador IMAC APPLE (3 Equipos)	Los utilizan para respaldar cuando los equipos se dañan.	60
[peripheral]	periféricos	Periférico	Los periféricos son dispositivos de salida/entrada/mixtos, lo que permite la recepción de información al usuario.	MUSB234	Memoria USB	Algunos de ellos son empleados como almacénadores de información, backups, entre otros	50
				DD234	Discos duros		
				DDX334	Discos duros externos		
[switch]	conmutadores(hw)	Conmutadores	Este activo permite	02070005 9	SWITCH ALCATEL LUCENT 9553	Este activo, permit	100

Tabla 19. Valoración para cada uno de los activos de la dependencia de sistemas (Continuación)

			la interconexión con las diferentes redes existentes.	02070013 0	SWITCH 24 10/100/1000 BASE T C SWITCH 24 10/100/1000 BASE T C	e a su vez, conectar varias redes, ampliar el número de computadores que se puedan conectar a una misma red.	
				02070015 8	SWITCH 24/10/100/1000 BASE T4S		
				02070013 6	SWITCH 24/10/100/1000PWR CORD		
				02070006 7	SWITCH ALCATEL LUCEN 9561		
				02070006 2	SWITCH ALCATEL LUCENT 9556		
				02070006 3	SWITCH ALCATEL LUCENT 9557		
				02070006 4	SWITCH ALCATEL LUCENT 9558		
				02070006 5	SWITCH ALCATEL LUCENT 9559		
				02070004 9	SWITCH ALCATEL LUCENT 9543		
				02070005 0	SWITCH ALCATEL LUCENT 9544		
				02070005 1	SWITCH ALCATEL LUCENT 9545		
				02070005 4	SWITCH ALCATEL LUCENT 9548		
				02070005 6	SWITCH ALCATEL LUCENT 9550		

Tabla 19. Valoración para cada uno de los activos de la dependencia de sistemas (Continuación)

				02070005 7	SWITCH ALCATEL LUCENT 9551		
				02070005 8	SWITCH ALCATEL LUCENT 9552		
				02070006 0	SWITCH ALCATEL LUCENT 9554		
				02070006 1	SWITCH ALCATEL LUCENT 9555		
				02070006 6	SWITCH ALCATEL LUCENT 9560		
				02070008 0	SWITCH LAYER 3 9574		
				02070008 2	SWITCH LAYER 3 9576		
				02070008 3	SWITCH LAYER 3 9577		
				02070008 1	SWITCH LAYER 3 9575		
[router]	encaminadores(hw)	Router	Este activo permite la direccionar a los diferentes canales de información.		ROUTER CISCO MODELO 1800 4781	Para este activo, es indispensable tener definidas cada uno de los diferentes canales de	100

Tabla 19. Valoración para cada uno de los activos de la dependencia de sistemas (Continuación)

						distribución.	
[pabx]	centralita telefónica(hw)	Central telefónica	Esta sección de los activos permite conectar dependencias o instancias de diferentes entidades internas.			Como función especial, la central telefónica busca tener comunicación instantánea con cada una de las dependencias que se encuentran entrelazadas.	80
Redes de comunicación							
[PSTN]	Red de telefonía	Red telefónica	Una red telefónica, es aquella que entrelaza entre si varias líneas telefónicas internas.			Como función especial, la red telefónica busca tener comunicación instant	80

Tabla 19. Valoración para cada uno de los activos de la dependencia de sistemas (Continuación)

						ánea con cada una de las dependencias que se encuentran entrelazadas.	
[INTERNET]	Internet	Internet Movistar	Este activo, es un servicio de internet externo, que como su nombre lo indica concede el acceso a la navegación por medio de sus fibras.			Su función principal, es conceder navegación a internet a cada una de las redes instanciadas de manera interna.	100
[LAN]	Red Local	Red LAN	Es una red que trasmite paquetes de datos por medio de cableado			La red de navegación LAN, permite la transm	100

Tabla 19. Valoración para cada uno de los activos de la dependencia de sistemas (Continuación)

			estructurado.			isión de archivos de manera más ágil y privada, siendo esta segmentada.	
[WIFI]	Red Wifi	Red WIFI	Las redes Wifi, permiten de igual manera, la conexión y transmisión de archivos, pero de manera inalámbrica.		ITFIP ITFIP 2 ITFIP_P1 ITFIP_FUNCIONARIOS_P1 Salas1y2 Salas_Sis2 Rectoría	La función principal de este activo en la institución es permitir que la comunidad académica y administrativa, tenga acceso a la red de navegación.	100
[X25]	Red de datos	Red de datos	Es la comunicación de máquina			Suple la misma funció	100

Tabla 19. Valoración para cada uno de los activos de la dependencia de sistemas (Continuación)

			s por medios cableados y no cableados.			n que la red Wifi y la red LAN.	
Soportes de información							
[disk]	discos	Discos duros	Este activo es utilizado para realizar copias de seguridad.	DSK1024	DDS 1TB	Este activo permite salvaguardar cada una de las copias de seguridad generadas, principalmente en cada uno de sus procesos más importantes.	80
				DSK1024	DDS 1TB		
				DSK1024	DDS 1TB		
				DSK1024	DDS 1TB		
				DSK1024	DDS 1TB		
[printed]	Materiales impresos	Materiales físicos	Todo aquel dispositivo de consistencia física, que permita almacenar informaci			Este activo en especial permite el respaldo de la inform	80

Tabla 19. Valoración para cada uno de los activos de la dependencia de sistemas (Continuación)

			ón (DD, Memorias, CD, CD/DVD, etc.)			ación en cualquier momento, puesto que es aquel que se encuentra aislado de demás funciones a excepción, de almacenar.	
Equipamiento Auxiliar							
[ups]	sistemas de alimentación ininterrumpida	UPS	Un UPS, es un sistema de alimentación de energía interrumpida,			La función de esta herramientas es priorizar cada uno de los servicios que el alimenta de manera indirecta	80

Tabla 19. Valoración para cada uno de los activos de la dependencia de sistemas (Continuación)

						cada vez haya un fallo de energía	
[gen]	Generadores eléctricos	planta eléctrica	Una planta eléctrica, es aquella que funciona con base de gasolina y otras herramientas, para poder dar energía ante eventuales emergencias			Dar energía eléctrica en caso de falla.	80
[ac]	Equipos de climatización	equipos de climatización	Un equipo de climatización es aquel que regula la energía del entorno.			Regular la energía del entorno teniendo en cuenta los componentes que allí se	100

Tabla 19. Valoración para cada uno de los activos de la dependencia de sistemas (Continuación)

						alberg an.	
[suppl y]	Suminist ros esencial es	sumin istros esenc iales	Estos suministr os esenciale s son necesari os para funcionar la institució n con su totalidad de comodid ades.			Suplir las necesi dades básica s en cuanto infraes structur a corres ponde.	70
[furnit ure]	Mobiliari o	mobili ario	Lugar en el cual se encuentr a el estableci miento.			Alberg ar todo lo relacio nado de la empre sa para su cómod o funcio namie nto y servici o	100
Instalaciones							
[site]	recinto Cuarto o recinto (Oficina)		El recinto es la sección u/o edificio en donde se encuentra albergado y amoblado para operar.				0
Personal							

Tabla 19. Valoración para cada uno de los activos de la dependencia de sistemas (Continuación)

[adm]	Administradores de sistemas	Coordinador de sistemas					100
[des]	Desarrollador	Programador					100
[Sub]	subcontratas	Ingeniero Auxiliar/ Soporte técnico					100

Fuente: Autoría propia.

2.7. ANÁLISIS DE LA JERARQUÍA DE LOS ACTIVOS ENTRE SUS GRUPOS INTERNOS

Tabla 20. Jerarquía de cada uno de los activos.

Código grupo de activo MAGERIT	Nombre grupo de activo MAGERIT	Nombre del activo	Descripción	Código Consecutivo ITFIP	Nombre de activo ITFIP	Función	Jerarquía
Esenciales							
[vr]	datos vitales	Documentos de la organización	En este activo se almacén a el registro de los usuarios de la parte administrativa.	I-DU	Inventario de usuarios	Poseer el contenido crucial, en el cual, llegado el momento de caída accidental u ocasionada del sistema, se pueda corregir de manera eficiente, permitiéndose así optimizar el tiempo de respuesta.	10
			Este activo almacén a cada una de las dependencias que tiene la institución.	E-ORG	estructura organizacional		10
			Este activo guarda el registro de los contratos.	I-DC	Inventario de contratos		10
			Este activo lleva un registro de las actividades que se realizan.	R-DA	Registro de actividades		10

Tabla 20. Jerarquía de cada uno de los activos (Continuación)

			Este activo lleva el registro de los mantenimientos realizados.	R-ME	Registro Mantenimiento equipos		10
			Este activo guarda el registro de la arquitectura de los equipos que requieren.	R-AE	Registro de la arquitectura de los equipos		10
[service]	Servicios	Servicios ofrecidos de todas las dependencias del ITFIP	Este activo ofrece el servicio de soporte de equipos de cómputo.	S-EC	Soporte equipos de computo	Se encarga del mantenimiento correctivo y preventivo de todos los equipos administrativos de la institución y a las plataformas virtuales.	10
			Este activo ofrece el servicio de brindarle soporte a las plataformas virtuales.	S-PV	Soporte de plataformas virtuales		10
Arquitectura del sistema							
[ip]	punto de interconexión	VLAN	Este activo es la red virtual de administración para poder comunicarse entre ellos.	VLAN-ADMON	Vlan de administración	Su función principal es separar de manera ordenada y	10

Tabla 20. Jerarquía de cada uno de los activos (Continuación)

			Este activo es la red virtual de financiera para poder comunicarse entre ellos.	VLAN-FINAN	Vlan de financiera	optima cada una de las dependencias que se someten a los servicios de sistemas, permitiéndoles así, trabajar de manera más cercana entre sus propios núcleos.	10
			Este activo es la red virtual de tesorería para poder comunicarse entre ellos.	VLAN-TESO	Vlan de tesorería		10
			Este activo es la red virtual de estudiantes para poder comunicarse entre ellos.	VLAN-EST	Vlan de estudiantes		10
			Este activo es la red virtual de WIFI para poder brindar soporte en caso de algún daño.	V-WIFI	Vlan de wifi		10
			Este activo es la red virtual de configuración para poder configurar equipos de manera remota.	VLAN-CONF	Vlan de configuración		10
			Este activo es la red virtual de sistemas para poder comunicarse entre ellos.	VLAN-SIS	Vlan de sistemas		10

Tabla 20. Jerarquía de cada uno de los activos (Continuación)

			Este activo es la red virtual de RYCA para poder comunicarse entre ellos.	VLAN-RYCA	Vlan de registro y control		10
			Este activo es la red virtual de almacén para poder comunicarse entre ellos.	VLAN-ALMA	Vlan de almacén		10
			Este activo es la red virtual de Talento Humano para poder comunicarse entre ellos.	VLAN-TALEN	Vlan de talento humano		10
Datos/Información							
[backup]	copias de respaldo	Copias de seguridad	Este activo registra cada una de las copias de seguridad que se les hacen a los equipos de sistemas.	BACK UP-SISTEMAS	De cada pc de la dependencia de sistemas	Salvaguardar la información que se recolecta a diario, previniendo así la perdida de esta, lo cual, puede desencadenar a la perdida de la historia	5
			Este activo registra cada una de las copias de seguridad que se les hacen a los equipos de la institución.	BACK UP-ITFIP	de cada pc de las dependencias de la institución		8
			Este activo registra cada una de las copias de seguridad	BACK UP-SERVER'S	de las configuracion		10

Tabla 20. Jerarquía de cada uno de los activos (Continuación)

			que se les hacen a los servidores.		es de los servidores	de la institución si no se maneja con cautela,	
[password]	Credenciales	Contraseñas de seguridad	Este activo contiene las contraseñas biométricas que dan acceso a la sala principal de servidores.	PASS-BIO	Biométricas para acceso a la sala de servidor	Su función es dar un filtro a la cantidad de personas que pueden acceder a un sistema o zona en específico, reduciendo el número de personas que puede manipular la información.	10
			Este activo contiene las contraseñas con las que acceden los administradores a los servidores.	PASS-SERVER	De los usuarios que acceden a los servidores		10
			Este activo contiene las contraseñas del servidor de copias de seguridad de la institución.	PASS-SERVER-BACK UP	servidor de copias de seguridad		10
[Files]	Ficheros	Archivos	Son todos los archivos planos que se pueden identificar como códigos de programación, archivos en Excel etc.			Se encarga de tener de manera digital la información del departamento de sistemas.	5
Claves criptográficas							

Tabla 20. Jerarquía de cada uno de los activos (Continuación)

[info]	protección de la información	Credenciales externas	Para este active, se permite la creación de credenciales para los diferentes accesos a los sistemas, como también de la información que allí se alberga.	PASS-PC-ITFIP	Usuarios de los Pc de las demás dependencias	Permitir o restringir el paso a personas que son o no autorizadas a manipular, visualizar, transportar entre otros la información concerniente a la dependencia de sistemas u otro sitio.	5
[encrypt]	claves de cifra	Sistema de acceso	Este activo gestiona a través de herramientas las personas que pueden generar paso a otras, por lo general es administrada por el coordinador del área en donde esta se encuentra.	S-BIO	Sensor biométrico	Mantener bajo constante monitoreo las personas que tienen acceso a la información, conocer qué tipo de información	5

Tabla 20. Jerarquía de cada uno de los activos (Continuación)

						manipulan y el uso que se le da a la misma.	
[authentication]	claves de autenticación	Contraseña de autenticación	Dicho activo consiste en asignar predeterminadamente una contraseña, que permite identificar que usuario y a donde tiene permitido el acceso.	C-CASERVER	Código de confirmación para acceso a la sala de servidor	Este activo permite controlar que personas tienen control de usuarios por parte de la plataforma.	10
Aplicaciones (Software)							
[prp]	desarrollo propio (in house)	Desarrollo propio (Ryca1 y Ryca2)	Este activo contiene todo el código y software que maneja la plataforma RYCA V.1 para su desarrollo o mantenimiento.	S-RYCA1	Sistema de Registro y Control Académico (RYCA) V.1	Este activo contiene la información concerniente de la carga académica, personal educativo, docentes, administrativos entre otros.	10
			Este activo contiene todo el código y software que maneja la plataforma RYCA V.2.0 para su desarrollo o mantenimiento.	S-RYCA2	Sistema de Registro y Control Académico (RYCA) V.2.0		10

Tabla 20. Jerarquía de cada uno de los activos (Continuación)

[www]	Servidor de presentación	Página de la institución	En este activo se da conocer a la institución por medio del portal web, que a su vez da acceso a la información al personal externo de la misma.	P-ITFIP	Página Oficial del ITFIP	La función plena del portal es mantener al tanto al personal de la institución, tenerla informada acerca de los planes educativos, fechas de ingreso, calendario académico, etc. Además, contiene la información esencial pública de la institución.	8
[browser]	navegador web	Navegadores	Los navegadores permiten abrir los motores de búsqueda, como también las aplicaciones locales	G-CHROME	Google Chrome	La función de este activo es la de permitir el acceso a la	3
				M-F	Mozilla Firefox		2

Tabla 20. Jerarquía de cada uno de los activos (Continuación)

			desarrolladas para ambiente web.	SAFI	Safari	información encontrada en las nubes internas y externas de la institución, abrir paginas locales y demás.	3
[office]	Ofimática	Herramientas ofimáticas	Las herramientas ofimáticas permiten editar archivos planos.	M-OFFICE	Microsoft Office 2013	Este activo es de provecho para la institución, puesto que permite la creación de documentos escritos tales como cartas; presentación de elementos en PowerPoint, además, del uso de	5
				O-OLINUX	Open Office Linux 2017		3

Tabla 20. Jerarquía de cada uno de los activos (Continuación)

						cálculos básicos y avanzados a través de la herramienta de Excel.	
[av]	antivirus	Antivirus	Este activo protege de virus que puedan afectar la información.	S-CENTER	System Center	Este software permite el escaneo de los archivos localizados en cada uno de los componentes del pc, a su vez, este permite alzar una emergencia al detectar archivos infecciosos o malware.	5
			Este activo protege de virus que puedan afectar la información.	W-DEFEN	Windows Defender		5
[os]	sistema operativo	Sistemas operativos	Los sistemas operativos, permiten poner en funcionamiento el hardware con el cual	W-8	Windows 8	Este activo, permite estructurar de manera lógica cada	8
				W-SER09	Windows Server 2009		8
				W-SER12	Windows Server 2012		10

Tabla 20. Jerarquía de cada uno de los activos (Continuación)

			se cuenta, a su vez, administrar cada una de sus funciones lógicas.	C-5	CentOS 5	una de las tareas lógicas otorgadas o en plan de ejecución.	10
				D-7	Debian 7		8
				U-14	Ubuntu 14		5
				M-OSX	Mac OS X		10
[ts]	servidor de terminales	Servicio de terminal	Es un componente perteneciente a cada uno de los sistemas operativos, utilizado para administrador por medio de comandos los servicios que ofrecen.	CMD	CoMmanD (CMD)	Manejar o dar órdenes de manera escrita, sin uso de interfaz gráfica, con lo cual, permite agilizar los procesos disminuyendo el consumo de recursos.	5
				C-LMAC	CoMmanD line (Mac)		10
				TERM	Terminal		8
Equipamiento Informático (Hardware)							
[host]	equipos grandes	Servidor que contiene el dominio de cada uno de los equipos dentro de	Este activo es el encargado distribuir dinámicamente una IP a cada equipo conectado.	S-DNS	Servidor DNS y DHCP	Distribución y administración de los servicios de DNS y DHCP	10

Tabla 20. Jerarquía de cada uno de los activos (Continuación)

		la institución, maneja un DNS y un DHCP					
[host]	equipos grandes	Servidor de la plataforma RYCA V.2.0.	Este activo contiene todo el código y configuraciones del software de RYCA V.2.0.	S-RYCA2	Servidor Plataforma RYCA V.2.0	En este activo se contiene la información concernient e a la plataforma de RYCA V.2.0.	10
[host]	equipos grandes	Servidor que contiene las máquinas virtuales de RYCA1 y la plataforma	Este activo contiene todo el código y configuraciones del software de RYCA V.1.	S-RYCA1	Servidor Plataforma RYCA V.1	En este activo se contiene la información concernient e a la plataforma de RYCA V.1.	10
[host]	equipos grandes	Servidor de base de datos	Este activo contiene toda la información de la institución en una base de datos.	S-BD	Servidor de Base de Datos ITFIP	Para este servicio, se categoriza toda la información contenida en la institución y	10

Tabla 20. Jerarquía de cada uno de los activos (Continuación)

						se pone a disposición para los demás servicios internos.	
[host]	equipos grandes	Servidor de cortafuegos	Este activo es el encargado de toda la seguridad de la red, servidores e información que tiene la información.	S-FIREW	Servidor Firewall Fortigate	Dicha función de este activo es la de tener en restricción los accesos de usuarios NO autorizados por el sistema.	10
[host]	equipos grandes	Servidor que contiene a SIIGO	Este activo maneja toda la información contable de la institución.	S-SIIGO	Servidor Contable SIIGO	En este servicio, se contiene toda la información contable de la institución.	10
[host]	equipos grandes	Servidor de Pruebas “Desarrollito”	Este activo es utilizado para pruebas de nuevas actualizaciones a las plataformas.	S-PDESA	Servidor de Pruebas “Desarrollito”	Sirve para hacer pruebas de los nuevos módulos de	5

Tabla 20. Jerarquía de cada uno de los activos (Continuación)

						las plataformas	
[host]	equipos grandes	Servidor de Copias de seguridad de la institución	Este activo almacén a toda la información de las dependencias de la institución.	S-CSECURITY	Servidor de Copias de seguridad de la información del ITFIP	Contiene las copias de seguridad de la información del ITFIP	10
[mid]	equipos medios (hw)	Computad ores Apple	Equipos de cómputo utilizado para emplear la digitación de código u otros	022400532 AL 022400534	Computador IMAC APPLE (3 Equipos)	Debido a su gran calidad de imagen, rapidez y demás componente s que le permiten sobresalir son empleados para el desarrollo y la edición de páginas web como de programas locales.	5
[mid]	equipos medios (hw)	Computad ores HP all-one Pro	Equipo todo en uno	022400570 AL 022400192	Computadore s HP all-one	Uso para las tareas	5

Tabla 20. Jerarquía de cada uno de los activos (Continuación)

					Pro (18 Equipos)	que requieran.	
[pc]	informática personal	Portátil Toshiba	Este equipo permite llevar varias tareas a cabo de manera estructurada y eficiente.	022400540 AL 022400565	Portátil Toshiba (16 equipos)	La funcionalidad de cada uno de estos equipos varía dependiendo del enfoque a la que le aplique su uso.	5
[mobile]	informática móvil	Tablet negra 9”	Este equipo permite llevar varias tareas a cabo de manera estructurada y eficiente.	022400675	Tablet negra 9” (1 Equipo)	La funcionalidad de cada uno de estos equipos varía dependiendo del enfoque a la que le aplique su uso.	3
[backup]	equipamiento de	Equipo de respaldo	Son aquellos equipos preparados para hacerse cargo	022400534 AL 022400537	Computador IMAC APPLE (3 Equipos)	Los utilizan para respaldar	3

Tabla 20. Jerarquía de cada uno de los activos (Continuación)

	respaldo(hw)		inmediato de los equipos en producción.			cuando los equipos se dañan.	
[peripheral]	periféricos	Periférico	Los periféricos son dispositivos de salida/entrada/mixtos, lo que permite la recepción de información al usuario	MUSB234	Memoria USB	Algunos de ellos son empleados como almacén adores de información, backups, entre otros	2
				DD234	Discos duros		
				DDX334	Discos duros externos		
[switch]	conmutadores(hw)	Conmutadores	Este activo permite la interconexión con las diferentes redes existentes.	020700059	SWITCH ALCATEL LUCENT 9553	Este activo, permite a su vez, conectar varias redes, ampliar el número de computadores que se puedan conectar a una misma red.	10
				020700130	SWITCH 24 10/100/1000 BASE T C SWITCH 24 10/100/1000 BASE T C		
				020700158	SWITCH 24/10/100/1000 BASE T4S		
				020700136	SWITCH 24/10/100/1000PWR CORD		

Tabla 20. Jerarquía de cada uno de los activos (Continuación)

				020700067	SWITCH ALCATEL LUCEN 9561		
				020700062	SWITCH ALCATEL LUCENT 9556		
				020700063	SWITCH ALCATEL LUCENT 9557		
				020700064	SWITCH ALCATEL LUCENT 9558		
				020700065	SWITCH ALCATEL LUCENT 9559		
				020700049	SWITCH ALCATEL LUCENT 9543		
				020700050	SWITCH ALCATEL LUCENT 9544		
				020700051	SWITCH ALCATEL LUCENT 9545		

Tabla 20. Jerarquía de cada uno de los activos (Continuación)

				020700054	SWITCH ALCATEL LUCENT 9548		
				020700056	SWITCH ALCATEL LUCENT 9550		
				020700057	SWITCH ALCATEL LUCENT 9551		
				020700058	SWITCH ALCATEL LUCENT 9552		
				020700060	SWITCH ALCATEL LUCENT 9554		
				020700061	SWITCH ALCATEL LUCENT 9555		
				020700066	SWITCH ALCATEL LUCENT 9560		
				020700080	SWITCH LAYER 3 9574		

Tabla 20. Jerarquía de cada uno de los activos (Continuación)

				020700082	SWITCH LAYER 3 9576		
				020700083	SWITCH LAYER 3 9577		
				020700081	SWITCH LAYER 3 9575		
[router]	encaminadores(hw)	Router	Este activo permite la direccionar a los diferentes canales de información.		ROUTER CISCO MODELO 1800 4781	Para este activo, es indispensable tener definidas cada uno de los diferentes canales de distribución.	10
[pabx]	centralita telefónica(hw)	Central telefónica	Esta sección de los activos permite conectar dependencias o instancias de diferentes entidades internas.			Como función especial, la central telefónica busca tener comunicación instantánea con cada una de las dependenci	5

Tabla 20. Jerarquía de cada uno de los activos (Continuación)

						as que se encuentran entrelazadas.	
Redes de comunicación							
[PSTN]	Red de telefonía	Red telefónica	Una red telefónica, es aquella que entrelaza entre si varias líneas telefónicas internas.			Como función especial, la red telefónica busca tener comunicación instantánea con cada una de las dependencias que se encuentran entrelazadas.	5
[INTERNET]	Internet	Internet Movistar	Este activo, es un servicio de internet externo, que como su nombre lo indica concede el acceso a la navegación por medio de sus fibras.			Su función principal, es conceder navegación a internet a cada una de las redes instanciadas de	10

Tabla 20. Jerarquía de cada uno de los activos (Continuación)

						manera interna.	
[LAN]	Red Local	Red LAN	Es una red que trasmite paquetes de datos por medio de cableado estructurado.			La red de navegación LAN, permite la transmisión de archivos de manera más ágil y privada, siendo esta segmentada.	10
[WIFI]	Red Wifi	Red WIFI	Las redes Wifi, permiten de igual manera, la conexión y transmisión de archivos, pero de manera inalámbrica.		ITFIP	La función principal de este activo en la institución es permitir que la comunidad académica y administrativa, tenga acceso a la red de navegación.	10
					ITFIP 2		
					ITFIP_P1		
					ITFIP_FUNCIONARIOS_P1		
					Salas1y2		
					Salas_Sis2		
					Rectoría		

Tabla 20. Jerarquía de cada uno de los activos (Continuación)

[X25]	Red de datos	Red de datos	Es la comunicación de máquinas por medios cableados y no cableados.			Suple la misma función que la red Wifi y la red LAN.	10
Soportes de información							
[disk]	discos	Discos duros	Un disco duro es un dispositivo de almacén amiento físico.	DSK1024	DDS1TB	Este activo permite salvaguardar cada una de las copias de seguridad generadas, principalmente en cada uno de sus procesos más importantes.	5
[printed]	Materiales impresos	Materiales físicos	Todo aquel dispositivo de consistencia física, que permita almacén ar información (DD, Memorias, CD, CD/DVD, etc.)			Este activo en especial permite el respaldo de la información en cualquier momento, puesto que es aquel que se	5

Tabla 20. Jerarquía de cada uno de los activos (Continuación)

						encuentra aislado de demás funciones a excepción, de almacén ar.	
Equipamiento Auxiliar							
[ups]	sistemas de alimentación ininterrumpida	UPS	Un UPS, es un sistema de alimentación de energía interrumpida			La función de esta herramienta es priorizar cada uno de los servicios que el alimenta de manera indirecta cada vez haya un fallo de energía	5
[gen]	Generadores eléctricos	planta eléctrica	Una planta eléctrica, es aquella que funciona con base de gasolina y otras herramientas, para poder dar energía ante eventuales emergencias			Dar energía eléctrica en caso de falla.	5

Tabla 20. Jerarquía de cada uno de los activos (Continuación)

[ac]	Equipos de climatización	equipos de climatización	Un equipo de climatización es aquel que regula la energía del entorno.			Regular la energía del entorno teniendo en cuenta los componentes que allí se albergan.	10
[supply]	Suministros esenciales	suministros esenciales	Estos suministros esenciales son necesarios para funcionar la institución con su totalidad de comodidades.			Suplir las necesidades básicas en cuanto infraestructura corresponde.	5
[furniture]	Mobiliario	mobiliario	Lugar en el cual se encuentra el establecimiento.			Albergar todo lo relacionado de la empresa para su cómodo funcionamiento y servicio	10
Instalaciones							
[site]	recinto Cuarto o recinto (Oficina)		El recinto es la sección u/o edificio en donde se encuentra albergado				1

Tabla 20. Jerarquía de cada uno de los activos (Continuación)

			y amoblado para operar.				
Personal							
[adm]	Administradores de sistemas	Coordinador de sistemas					10
[des]	Desarrollador	Programador					10
[Sub]	subcontratas	Ingeniero Auxiliar/ Soporte técnico					10

Fuente: Autoría propia.

ANEXO 2

CONTENIDO

LISTA DE TABLAS

1. ESTIMACIÓN DE LOS VALORES DE CRITERIO EN SUS DIMENSIONES DE APLICABILIDAD

.

Tabla 1. Clasificación de activos con sus criterios de evaluación.

Código grupo de activo MAGERIT	Nombre grupo de activo MAGERIT	Nombre del activo	Código Consecutivo ITFIP	Nombre de activo ITFIP	Criterios de valoración				
					Confidencialidad	Integridad	Autenticidad	Disponibilidad	Trazabilidad
[vr]	datos vitales	Documentos de la organización	I-DU	Inventario de usuarios	6	8	8	0	5
			E-ORG	estructura organizacional	6	8	8	0	5
			I-DC	Inventario de contratos	6	8	8	0	5
			R-DA	Registro de actividades	6	8	8	0	5
			R-ME	Registro Mantenimiento equipos	6	8	8	0	5

Tabla 1. Clasificación de activos con sus criterios de evaluación. (Continuación)

			R-AE	Registro de la arquitectura de los equipos	6	8	8	0	5
[service]	Servicios	Servicios ofrecidos de todas las dependencias del ITFIP	S-EC	Soporte equipos de computo	1	10	8	10	10
			S-PV	Soporte de plataformas virtuales	1	10	8	10	10
[ip]	punto de interconexión	VLAN	VLAN-ADMON	Vlan de administración	4	10	10	5	2
			VLAN-FINAN	Vlan de financiera	4	10	10	5	2
			VLAN-TESO	Vlan de tesorería	4	10	10	5	2
			VLAN-EST	Vlan de estudiantes	4	10	10	5	2
			V-WIFI	Vlan de wifi	4	10	10	5	2
			VLAN-CONF	Vlan de configuración	4	10	10	5	2
			VLAN-SIS	Vlan de sistemas	4	10	10	5	2

Tabla 1. Clasificación de activos con sus criterios de evaluación. (Continuación)

			VLAN-RYCA	Vlan de registro y control	4	10	10	5	2
			VLAN-ALMA	Vlan de almacén	4	10	10	5	2
			VLAN-TALEN	Vlan de talento humano	4	10	10	5	2
[backup]	copias de respaldo	Copias de seguridad	BACK UP-SISTEMAS	De cada pc de la dependencia de sistemas	8	10	10	10	4
			BACK UP-ITFIP	de cada pc de las dependencias de la institución	8	10	10	10	4
			BACK UP-SERVER'S	de las configuraciones de los servidores	8	10	10	10	4
[password]	Credenciales	Contraseñas de seguridad	PASS-BIO	Biométricas para acceso a la sala de servidor	10	8	8	0	0

Tabla 1. Clasificación de activos con sus criterios de evaluación. (Continuación)

			PASS-SERVER	De los usuarios que acceden a los servidores	10	8	8	0	0
			PASS-SERVER-BACKUP	servidor de copias de seguridad	10	8	8	0	0
[Files]	Ficheros	Archivos			8	8	10	10	2
[info]	protección de la información	Credenciales externas	PASS-PC-ITFIP	Usuarios de los Pc de las demás dependencias	10	10	10	2	2
[encrypt]	claves de cifrado	Sistema de acceso	S-BIO	Sensor biométrico	8	8	8	2	2
[authentication]	claves de autenticación	Contraseña de autenticación	C-CASERVER	Código de confirmación para acceso a la sala de servidor	10	10	8	2	2

Tabla 1. Clasificación de activos con sus criterios de evaluación. (Continuación)

[prp]	desarrollo propio (in house)	Desarrollo propio (Ryca1 y Ryca2)	S-RYCA1	Sistema de Registro y Control Académico (RYCA) V.1	8	8	10	5	4
			S-RYCA2	Sistema de Registro y Control Académico (RYCA) V.2.0	8	8	10	5	4
[www]	Servidor de presentación	Página de la institución	P-ITFIP	Página Oficial del ITFIP	2	8	8	10	10
[browser]	navegador web	Navegadores	G-CHROME	Google Chrome	10	10	2	10	10
			M-F	Mozilla Firefox	10	10	2	10	10
			SAFI	Safari	10	10	2	10	10
[office]	Ofimática	Herramientas ofimáticas	M-OFFICE	Microsoft Office 2013	10	8	8	8	0
			O-OLINUX	Open Office Linux 2017	10	8	8	8	0
[av]	antivirus	Antivirus	S-CENTER	System Center	10	10	0	10	2

Tabla 1. Clasificación de activos con sus criterios de evaluación. (Continuación)

			W-DEFEN	Windows Defender	10	10	0	10	2
[os]	sistema operativo	Sistemas operativos	W-8	Windows 8	10	10	2	10	0
			W-SER09	Windows Server 2009	10	10	2	10	0
			W-SER12	Windows Server 2012	10	10	2	10	0
			C-5	CentOS 5	10	10	2	10	0
			D-7	Debian 7	10	10	2	10	0
			U-14	Ubuntu 14	10	10	2	10	0
			M-OSX	Mac OS X	10	10	2	10	0
[ts]	servidor de terminales	Servicio de terminal	CMD	CoMmanD (CMD)	10	10	0	10	0
			C-LMAC	CoMmanD line (Mac)	10	10	0	10	0
			TERM	Terminal	10	10	0	10	0

Tabla 1. Clasificación de activos con sus criterios de evaluación. (Continuación)

[host]	equipos grandes	Servidor que contiene el dominio de cada uno de los equipos dentro de la institución, maneja un DNS y un DHCP	S-DNS	Servidor DNS y DHCP	10	10	10	8	8
[host]	equipos grandes	Servidor de la plataforma RYCA V.2.0.	S-RYCA2	Servidor Plataforma RYCA V.2.0	10	10	10	8	8
[host]	equipos grandes	Servidor que contiene las máquinas virtuales de RYCA1 y la plataforma	S-RYCA1	Servidor Plataforma RYCA V.1	10	10	10	10	7
[host]	equipos grandes	Servidor de base de datos	S-BD	Servidor de Base de Datos ITFIP	10	10	10	8	8
[host]	equipos grandes	Servidor de cortafuegos	S-FIREW	Servidor Firewall Fortigate	10	10	10	8	8
[host]	equipos grandes	Servidor que contiene a SIIGO	S-SIIGO	Servidor Contable SIIGO	10	10	10	10	7

Tabla 1. Clasificación de activos con sus criterios de evaluación. (Continuación)

[host]	equipos grandes	Servidor de Pruebas “Desarrollito”	S-PDESA	Servidor de Pruebas “Desarrollito”	10	10	10	8	8
[host]	equipos grandes	Servidor de Copias de seguridad de la institución	S-CSECURITY	Servidor de Copias de seguridad de la información del ITFIP	10	10	8	10	8
[mid]	equipos medios (hw)	Computadores Apple	022400532 AL 022400534	Computador IMAC APPLE (3 Equipos)	7	8	8	5	0
[mid]	equipos medios (hw)	Computadores HP all-one Pro	022400570 AL 022400192	Computadores HP all-one Pro (18 Equipos)	7	8	8	5	0
[pc]	informática personal	Portátil Toshiba	022400540 AL 022400565	Portátil Toshiba (16 equipos)	0	8	6	8	0
[mobile]	informática móvil	Tablet negra 9”	022400675	Tablet negra 9” (1 Equipo)	0	7	7	9	0
[backup]	equipamiento de respaldo(hw)	Equipo de respaldo	022400534 AL 022400537	Computador IMAC APPLE (3 Equipos)	0	8	7	10	0

Tabla 1. Clasificación de activos con sus criterios de evaluación. (Continuación)

[peripheral]	periféricos	Periférico	MUSB234	Memoria USB	2	5	5	5	5
			DD234	Discos duros	2	5	5	5	5
			DDX334	Discos duros externos	2	5	5	5	5
[switch]	conmutadores(hw)	Conmutadores	020700059	SWITCH ALCATEL LUCENT 9553	8	8	5	10	0
			020700130	SWITCH 24 10/100/1000 BASE TC SWITCH 24 10/100/1000 BASE TC	8	8	5	10	0
			020700158	SWITCH 24/10/100/1000 BASE T4S	8	8	5	10	0
			020700136	SWITCH 24/10/100/1000 PWR CORD	8	8	5	10	0

Tabla 1. Clasificación de activos con sus criterios de evaluación. (Continuación)

			02070006 7	SWITCH ALCATEL LUCEN 9561	8	8	5	10	0
			02070006 2	SWITCH ALCATEL LUCENT 9556	8	8	5	10	0
			02070006 3	SWITCH ALCATEL LUCENT 9557	8	8	5	10	0
			02070006 4	SWITCH ALCATEL LUCENT 9558	8	8	5	10	0
			02070006 5	SWITCH ALCATEL LUCENT 9559	8	8	5	10	0
			02070004 9	SWITCH ALCATEL LUCENT 9543	8	8	5	10	0
			02070005 0	SWITCH ALCATEL LUCENT 9544	8	8	5	10	0

Tabla 1. Clasificación de activos con sus criterios de evaluación. (Continuación)

			02070005 1	SWITCH ALCATEL LUCENT 9545	8	8	5	10	0
			02070005 4	SWITCH ALCATEL LUCENT 9548	8	8	5	10	0
			02070005 6	SWITCH ALCATEL LUCENT 9550	8	8	5	10	0
			02070005 7	SWITCH ALCATEL LUCENT 9551	8	8	5	10	0
			02070005 8	SWITCH ALCATEL LUCENT 9552	8	8	5	10	0
			02070006 0	SWITCH ALCATEL LUCENT 9554	8	8	5	10	0
			02070006 1	SWITCH ALCATEL LUCENT 9555	8	8	5	10	0

Tabla 1. Clasificación de activos con sus criterios de evaluación. (Continuación)

			020700066	SWITCH ALCATEL LUCENT 9560	8	8	5	10	0
			020700080	SWITCH LAYER 3 9574	8	8	5	10	0
			020700082	SWITCH LAYER 3 9576	8	8	5	10	0
			020700083	SWITCH LAYER 3 9577	8	8	5	10	0
			020700081	SWITCH LAYER 3 9575	8	8	5	10	0
[router]	encaminadores(hw)	Router		ROUTER CISCO MODELO 1800 4781	5	5	5	8	0
[pabx]	centralita telefónica(hw)	Central telefónica			5	5	2	10	0
[PSTN]	Red de telefonía	Red telefónica			5	5	2	10	0
[INTERNET]	Internet	Internet Movistar			8	8	8	5	0

Tabla 1. Clasificación de activos con sus criterios de evaluación. (Continuación)

[LAN]	Red Local	Red LAN			5	8	8	10	6
[WIFI]	Red Wifi	Red WIFI		ITFIP	5	5	8	10	8
				ITFIP 2	5	5	8	10	8
				ITFIP_P1	5	5	8	10	8
				ITFIP_FUNCIONARIOS_P1	5	5	8	2	8
				Salas1y2	5	5	8	10	8
				Salas_Sis2	5	5	8	10	8
				Rectoría	5	5	8	2	8
[X25]	Red de datos	Red de datos			10	5	8	10	8
[disk]	discos	Discos duros	DSK1024	DDS 1TB	10	10	10	0	0
[printed]	Materiales impresos	Materiales físicos			10	10	2	10	0
[ups]	sistemas de alimentación ininterrumpida	UPS	022400526	UPS 10 KVA 9578	5	5	5	10	0
			022400527	UPS 10 KVA 9579	5	5	5	10	0
			022400528	UPS 10 KVA 9580	5	5	5	10	0

Tabla 1. Clasificación de activos con sus criterios de evaluación. (Continuación)

[supply]	Suministros esenciales	suministros esenciales			0	5	5	10	10
[furniture]	Mobiliario	mobiliario			0	10	5	10	0
[site]	recinto Cuarto o recinto (Oficina)				0	8	5	10	0
[adm]	Administradores de sistemas	Coordinador de sistemas			10	8	8	10	0
[des]	Desarrollador	Programador			10	8	8	10	0
[Sub]	subcontratas	Ingeniero Auxiliar/ Soporte técnico			10	8	8	10	0

Fuente: Autoría propia.

2. ESTIMACIÓN DE LAS AMENAZAS QUE PUEDEN AFECTAR LOS ACTIVOS.

Tabla 2. Impacto para cada dimensión.

RELACIÓN DE AMENAZAS POR ACTIVO IDENTIFICANDO SU FRECUENCIA E IMPACTO								
ID	**AMENAZA**	**ACTIVO**	**FRECUENCIA**	**IMPACTO PARA CADA DIMENSIÓN %**				
				[A]	**[C]**	**[I]**	**[D]**	**[T]**
N.1	Fuego	[HW] Servidor DNS y DHCP	5				**100%**	
		[HW] Servidor Plataforma RYCA V.2.0	5				**100%**	
		[HW] Servidor Plataforma RYCA V.1	5				**100%**	
		[HW] Servidor de Base de Datos ITFIP	50				**100%**	
		[HW] Servidor Firewall Fortigate	5				**100%**	
		[HW] Servidor Contable SIIGO	10				**100%**	

Tabla 2. Impacto para cada dimensión. (Continuación)

		[HW] Servidor de Pruebas “Desarrollito”	5				**100%**	
		[HW] Servidor de Copias de seguridad de la información del ITFIP	10				**100%**	
		[HW] Computador IMAC APPLE (3 Equipos)	10				**50%**	
		[HW] Computadores HP all-one Pro (18 Equipos)	10				**20%**	
		[HW] Portátil Toshiba (16 equipos)	10				**20%**	
		[HW] Tablet negra 9” (1 Equipo)	10				**100%**	
		[HW] Computador IMAC APPLE (3 Equipos)	10				**50%**	
		[HW] Memoria USB	10				**100%**	
		[HW] Discos duros	10				**100%**	
		[HW] Discos duros externos	10				**100%**	

Tabla 2.Impacto para cada dimensión. (Continuación)

		[HW] SWITCH ALCATEL LUCENT 9553	10				**100%**	
		[HW] SWITCH 24 10/100/1000 BASE T C	10				**100%**	
		[HW] SWITCH 24/10/100/1000 BASE T4S	10				**100%**	
		[HW] SWITCH 24/10/100/1000PWR CORD	10				**100%**	
		[HW] SWITCH ALCATEL LUCEN 9561	10				**100%**	
		[HW] SWITCH ALCATEL LUCENT 9556	10				**100%**	
		[HW] SWITCH ALCATEL LUCENT 9557	10				**100%**	
		[HW] SWITCH ALCATEL LUCENT 9558	10				**100%**	

Tabla 2.Impacto para cada dimensión. (Continuación)

		[HW] SWITCH ALCATEL LUCENT 9559	10				**100%**	
		[HW] SWITCH ALCATEL LUCENT 9543	10				**100%**	
		[HW] SWITCH ALCATEL LUCENT 9544	10				**100%**	
		[HW] SWITCH ALCATEL LUCENT 9545	10				**100%**	
		[HW] SWITCH ALCATEL LUCENT 9548	10				**100%**	
		[HW] SWITCH ALCATEL LUCENT 9550	10				**100%**	
		[HW] SWITCH ALCATEL LUCENT 9551	10				**100%**	
		[HW] SWITCH ALCATEL LUCENT 9552	10				**100%**	

Tabla.2 Impacto para cada dimensión. (Continuación)

		[HW] SWITCH ALCATEL LUCENT 9554	10				**100%**	
		[HW] SWITCH ALCATEL LUCENT 9555	10				**100%**	
		[HW] SWITCH ALCATEL LUCENT 9560	10				**100%**	
		[HW] SWITCH LAYER 3 9574	10				**100%**	
		[HW] SWITCH LAYER 3 9576	10				**100%**	
		[HW] SWITCH LAYER 3 9577	10				**100%**	
		[HW] SWITCH LAYER 3 9575	10				**100%**	
		[HW] ROUTER CISCO MODELO 1800 4781	10				**100%**	
		[MEDIA] DDS 1TB	10				**100%**	
		[MEDIA] Materiales físicos	50				**100%**	

Tabla 2. Impacto para cada dimensión. (Continuación)

		[AUX] UPS 10 KVA 9578	10				**50%**	
		[AUX] UPS 10 KVA 9579	10				**50%**	
		[AUX] UPS 10 KVA 9580	10				**50%**	
		[L] Cuarto o recinto (Oficina)	10				**100%**	
N.2	Daños por agua	[HW] Servidor DNS y DHCP	5				**100%**	
		[HW] Servidor Plataforma RYCA V.2.0	5				**100%**	
		[HW] Servidor Plataforma RYCA V.1	5				**100%**	
		[HW] Servidor de Base de Datos ITFIP	5				**100%**	
		[HW] Servidor Firewall Fortigate	5				**100%**	
		[HW] Servidor Contable SIIGO	5				**100%**	

Tabla. 2 Impacto para cada dimensión. (Continuación)

		[HW] Servidor de Pruebas “Desarrollito”	5				**100%**	
		[HW] Servidor de Copias de seguridad de la información del ITFIP	5				**100%**	
		[HW] Computador IMAC APPLE (3 Equipos)	10				**50%**	
		[HW] Computadores HP all-one Pro (18 Equipos)	10				**20%**	
		[HW] Portátil Toshiba (16 equipos)	10				**20%**	
		[HW] Tablet negra 9” (1 Equipo)	10				**100%**	
		[HW] Computador IMAC APPLE (3 Equipos)	10				**50%**	
		[HW] Memoria USB	50				**100%**	

Tabla. 2 Impacto para cada dimensión. (Continuación)

		[HW] Discos duros	10				**100%**	
		[HW] Discos duros externos	50				**100%**	
		[HW] SWITCH ALCATEL LUCENT 9553	10				**100%**	
		[HW] SWITCH 24 10/100/1000 BASE T C	10				**100%**	
		[HW] SWITCH 24/10/100/1000 BASE T4S	10				**100%**	
		[HW] SWITCH 24/10/100/1000PWR CORD	10				**100%**	
		[HW] SWITCH ALCATEL LUCEN 9561	10				**100%**	
		[HW] SWITCH ALCATEL LUCENT 9556	10				**100%**	
		[HW] SWITCH ALCATEL LUCENT 9557	10				**100%**	

Tabla. 2 Impacto para cada dimensión. (Continuación)

		[HW] SWITCH ALCATEL LUCENT 9558	10				**100%**	
		[HW] SWITCH ALCATEL LUCENT 9559	10				**100%**	
		[HW] SWITCH ALCATEL LUCENT 9543	10				**100%**	
		[HW] SWITCH ALCATEL LUCENT 9544	10				**100%**	
		[HW] SWITCH ALCATEL LUCENT 9545	10				**100%**	
		[HW] SWITCH ALCATEL LUCENT 9548	10				**100%**	
		[HW] SWITCH ALCATEL LUCENT 9550	10				**100%**	
		[HW] SWITCH ALCATEL LUCENT 9551	10				**100%**	

Tabla. 2 Impacto para cada dimensión. (Continuación)

		[HW] SWITCH ALCATEL LUCENT 9552	10				**100%**	
		[HW] SWITCH ALCATEL LUCENT 9554	10				**100%**	
		[HW] SWITCH ALCATEL LUCENT 9555	10				**100%**	
		[HW] SWITCH ALCATEL LUCENT 9560	10				**100%**	
		[HW] SWITCH LAYER 3 9574	10				**100%**	
		[HW] SWITCH LAYER 3 9576	10				**100%**	
		[HW] SWITCH LAYER 3 9577	10				**100%**	
		[HW] SWITCH LAYER 3 9575	10				**100%**	
		[HW] ROUTER CISCO MODELO 1800 4781	10				**100%**	
		[MEDIA] DDS 1TB	10				**100%**	

Tabla 2 Impacto para cada dimensión. (Continuación)

		[MEDIA] Materiales físicos	50				**100%**	
		[AUX] UPS 10 KVA 9578	10				**50%**	
		[AUX] UPS 10 KVA 9579	10				**50%**	
		[AUX] UPS 10 KVA 9580	10				**50%**	
		[L] Cuarto o recinto (Oficina)	5				**100%**	
N.*	Desastres naturales	[HW] Servidor DNS y DHCP	10				**100%**	
		[HW] Servidor Plataforma RYCA V.2.0	10				**100%**	
		[HW] Servidor Plataforma RYCA V.1	10				**100%**	
		[HW] Servidor de Base de Datos ITFIP	10				**100%**	
		[HW] Servidor Firewall Fortigate	10				**100%**	

Tabla 2. Impacto para cada dimensión. (Continuación)

		[HW] Servidor Contable SIIGO	10				**100%**	
		[HW] Servidor de Pruebas “Desarrollito”	10				**100%**	
		[HW] Servidor de Copias de seguridad de la información del ITFIP	10				**100%**	
		[HW] Computador IMAC APPLE (3 Equipos)	10				**50%**	
		[HW] Computadores HP all-one Pro (18 Equipos)	10				**20%**	
		[HW] Portátil Toshiba (16 equipos)	10				**20%**	
		[HW] Tablet negra 9” (1 Equipo)	10				**100%**	
		[HW] Computador IMAC APPLE (3 Equipos)	10				**50%**	

Tabla. 2 Impacto para cada dimensión. (Continuación)

		[HW] Memoria USB	10				**100%**	
		[HW] Discos duros	10				**100%**	
		[HW] Discos duros externos	10				**100%**	
		[HW] SWITCH ALCATEL LUCENT 9553	10				**100%**	
		[HW] SWITCH 24 10/100/1000 BASE T C	10				**100%**	
		[HW] SWITCH 24/10/100/1000 BASE T4S	10				**100%**	
		[HW] SWITCH 24/10/100/1000PWR CORD	10				**100%**	
		[HW] SWITCH ALCATEL LUCEN 9561	10				**100%**	
		[HW] SWITCH ALCATEL LUCENT 9556	10				**100%**	

Tabla 2. Impacto para cada dimensión. (Continuación)

		[HW] SWITCH ALCATEL LUCEN 9557	10				**100%**	
		[HW] SWITCH ALCATEL LUCEN 9558	10				**100%**	
		[HW] SWITCH ALCATEL LUCEN 9559	10				**100%**	
		[HW] SWITCH ALCATEL LUCEN 9543	10				**100%**	
		[HW] SWITCH ALCATEL LUCEN 9544	10				**100%**	
		[HW] SWITCH ALCATEL LUCEN 9545	10				**100%**	
		[HW] SWITCH ALCATEL LUCEN 9548	10				**100%**	
		[HW] SWITCH ALCATEL LUCEN 9550	10				**100%**	

Tabla 2 Impacto para cada dimensión. (Continuación)

		[HW] SWITCH ALCATEL LUCEN 9551	10				**100%**	
		[HW] SWITCH ALCATEL LUCEN 9552	10				**100%**	
		[HW] SWITCH ALCATEL LUCEN 9554	10				**100%**	
		[HW] SWITCH ALCATEL LUCEN 9555	10				**100%**	
		[HW] SWITCH ALCATEL LUCEN 9560	10				**100%**	
		[HW] SWITCH LAYER 3 9574	10				**100%**	
		[HW] SWITCH LAYER 3 9576	10				**100%**	
		[HW] SWITCH LAYER 3 9577	10				**100%**	
		[HW] SWITCH LAYER 3 9575	10				**100%**	

Tabla 2. Impacto para cada dimensión. (Continuación)

		[HW] ROUTER CISCO MODELO 1800 4781	10				**100%**	
		[MEDIA] DDS 1TB	10				**100%**	
		[MEDIA] Materiales físicos	10				**100%**	
		[AUX] UPS 10 KVA 9578	10				**50%**	
		[AUX] UPS 10 KVA 9579	10				**50%**	
		[AUX] UPS 10 KVA 9580	10				**50%**	
		[L] Cuarto o recinto (Oficina)	10				**100%**	
		De origen industriales						
I.1	Fuego	[HW] Servidor DNS y DHCP	10				**100%**	
		[HW] Servidor Plataforma RYCA V.2.0	10				**100%**	
		[HW] Servidor Plataforma RYCA V.1	10				**100%**	

Tabla 2. Impacto para cada dimensión. (Continuación)

		[HW] Servidor de Base de Datos ITFIP	10				**100%**	
		[HW] Servidor Firewall Fortigate	10				**100%**	
		[HW] Servidor Contable SIIGO	10				**100%**	
		[HW] Servidor de Pruebas “Desarrollito”	10				**100%**	
		[HW] Servidor de Copias de seguridad de la información del ITFIP	10				**100%**	
		[HW] Computador IMAC APPLE (3 Equipos)	10				**50%**	
		[HW] Computadores HP all-one Pro (18 Equipos)	10				**20%**	
		[HW] Portátil Toshiba (16 equipos)	10				**20%**	

Tabla 2. Impacto para cada dimensión. (Continuación)

		[HW] Tablet negra 9” (1 Equipo)	10				**100%**	
		[HW] Computador IMAC APPLE (3 Equipos)	10				**50%**	
		[HW] Memoria USB	10				**100%**	
		[HW] Discos duros	10				**100%**	
		[HW] Discos duros externos	10				**100%**	
		[HW] SWITCH ALCATEL LUCEN 9553	10				**100%**	
		[HW] SWITCH 24 10/100/1000 BASE T C	10				**100%**	
		[HW] SWITCH 24/10/100/1000 BASE T4S	10				**100%**	
		[HW] SWITCH 24/10/100/1000PWR CORD	10				**100%**	
		[HW] SWITCH ALCATEL LUCEN 9561	10				**100%**	

Tabla 2. Impacto para cada dimensión. (Continuación)

		[HW] SWITCH ALCATEL LUCEN 9556	10				**100%**	
		[HW] SWITCH ALCATEL LUCEN 9557	10				**100%**	
		[HW] SWITCH ALCATEL LUCEN 9558	10				**100%**	
		[HW] SWITCH ALCATEL LUCEN 9559	10				**100%**	
		[HW] SWITCH ALCATEL LUCEN 9543	10				**100%**	
		[HW] SWITCH ALCATEL LUCEN 9544	10				**100%**	
		[HW] SWITCH ALCATEL LUCEN 9545	10				**100%**	
		[HW] SWITCH ALCATEL LUCEN 9548	10				**100%**	

Tabla 2. Impacto para cada dimensión. (Continuación)

		[HW] SWITCH ALCATEL LUCEN 9550	10				**100%**	
		[HW] SWITCH ALCATEL LUCEN 9551	10				**100%**	
		[HW] SWITCH ALCATEL LUCEN 9552	10				**100%**	
		[HW] SWITCH ALCATEL LUCEN 9554	10				**100%**	
		[HW] SWITCH ALCATEL LUCEN 9555	10				**100%**	
		[HW] SWITCH ALCATEL LUCEN 9560	10				**100%**	
		[HW] SWITCH LAYER 3 9574	10				**100%**	
		[HW] SWITCH LAYER 3 9576	10				**100%**	
		[HW] SWITCH LAYER 3 9577	10				**100%**	
		[HW] SWITCH LAYER 3 9575	10				**100%**	

Tabla 2. Impacto para cada dimensión. (Continuación)

		[HW] ROUTER CISCO MODELO 1800 4781	10				**100%**	
		[MEDIA] DDS 1TB	10				**100%**	
		[MEDIA] Materiales físicos	10				**100%**	
		[AUX] UPS 10 KVA 9578	10				**50%**	
		[AUX] UPS 10 KVA 9579	10				**50%**	
		[AUX] UPS 10 KVA 9580	10				**50%**	
		[L] Cuarto o recinto (Oficina)	10				**100%**	
I.2	Daños por agua	[HW] Servidor DNS y DHCP	10				**100%**	
		[HW] Servidor Plataforma RYCA V.2.0	10				**100%**	
		[HW] Servidor Plataforma RYCA V.1	10				**100%**	

Tabla 2. Impacto para cada dimensión. (Continuación)

		[HW] Servidor de Base de Datos ITFIP	10				**100%**	
		[HW] Servidor Firewall Fortigate	10				**100%**	
		[HW] Servidor Contable SIIGO	10				**100%**	
		[HW] Servidor de Pruebas “Desarrollito”	10				**100%**	
		[HW] Servidor de Copias de seguridad de la información del ITFIP	10				**100%**	
		[HW] Computador IMAC APPLE (3 Equipos)	10				**50%**	
		[HW] Computadores HP all-one Pro (18 Equipos)	10				**20%**	
		[HW] Portátil Toshiba (16 equipos)	10				**20%**	
		[HW] Tablet negra 9” (1 Equipo)	10				**100%**	

Tabla 2. Impacto para cada dimensión. (Continuación)

		[HW] Computador IMAC APPLE (3 Equipos)	10				**50%**	
		[HW] Memoria USB	10				**100%**	
		[HW] Discos duros	10				**100%**	
		[HW] Discos duros externos	10				**100%**	
		[HW] SWITCH ALCATEL LUCEN 9553	10				**100%**	
		[HW] SWITCH 24 10/100/1000 BASE T C	10				**100%**	
		[HW] SWITCH 24/10/100/1000 BASE T4S	10				**100%**	
		[HW] SWITCH 24/10/100/1000PWR CORD	10				**100%**	
		[HW] SWITCH ALCATEL LUCEN 9561	10				**100%**	

Tabla 2. Impacto para cada dimensión. (Continuación)

		[HW] SWITCH ALCATEL LUCEN 9556	10				**100%**	
		[HW] SWITCH ALCATEL LUCEN 9557	10				**100%**	
		[HW] SWITCH ALCATEL LUCEN 9558	10				**100%**	
		[HW] SWITCH ALCATEL LUCEN 9559	10				**100%**	
		[HW] SWITCH ALCATEL LUCEN 9543	10				**100%**	
		[HW] SWITCH ALCATEL LUCEN 9544	10				**100%**	
		[HW] SWITCH ALCATEL LUCEN 9545	10				**100%**	
		[HW] SWITCH ALCATEL LUCEN 9548	10				**100%**	

Tabla 2. Impacto para cada dimensión. (Continuación)

		[HW] SWITCH ALCATEL LUCEN 9550	10				**100%**	
		[HW] SWITCH ALCATEL LUCEN 9551	10				**100%**	
		[HW] SWITCH ALCATEL LUCEN 9552	10				**100%**	
		[HW] SWITCH ALCATEL LUCEN 9554	10				**100%**	
		[HW] SWITCH ALCATEL LUCEN 9555	10				**100%**	
		[HW] SWITCH ALCATEL LUCEN 9560	10				**100%**	
		[HW] SWITCH LAYER 3 9574	10				**100%**	
		[HW] SWITCH LAYER 3 9576	10				**100%**	
		[HW] SWITCH LAYER 3 9577	10				**100%**	
		[HW] SWITCH LAYER 3 9575	10				**100%**	

Tabla 2. Impacto para cada dimensión. (Continuación)

		[HW] ROUTER CISCO MODELO 1800 4781	10				**100%**	
		[MEDIA] DDS 1TB	10				**100%**	
		[MEDIA] Materiales físicos	10				**100%**	
		[AUX] UPS 10 KVA 9578	10				**50%**	
		[AUX] UPS 10 KVA 9579	10				**50%**	
		[AUX] UPS 10 KVA 9580	10				**50%**	
		[L] Cuarto o recinto (Oficina)	10				**100%**	
I.*	Desastres industriales	[HW] Servidor DNS y DHCP	50				**100%**	
		[HW] Servidor Plataforma RYCA V.2.0	50				**100%**	
		[HW] Servidor Plataforma RYCA V.1	50				**100%**	

Tabla 2. Impacto para cada dimensión. (Continuación)

		[HW] Servidor de Base de Datos ITFIP	50				**100%**	
		[HW] Servidor Firewall Fortigate	50				**100%**	
		[HW] Servidor Contable SIIGO	50				**100%**	
		[HW] Servidor de Pruebas “Desarrollito”	50				**100%**	
		[HW] Servidor de Copias de seguridad de la información del ITFIP	50				**100%**	
		[HW] Computador IMAC APPLE (3 Equipos)	50				**50%**	
		[HW] Computadores HP all-one Pro (18 Equipos)	50				**20%**	
		[HW] Portátil Toshiba (16 equipos)	50				**20%**	

Tabla 2. Impacto para cada dimensión. (Continuación)

		[HW] Tablet negra 9” (1 Equipo)	50				**100%**	
		[HW] Computador IMAC APPLE (3 Equipos)	50				**50%**	
		[HW] Memoria USB	50				**100%**	
		[HW] Discos duros	50				**100%**	
		[HW] Discos duros externos	50				**100%**	
		[HW] SWITCH ALCATEL LUCEN 9553	50				**100%**	
		[HW] SWITCH 24 10/100/1000 BASE T C	50				**100%**	
		[HW] SWITCH 24/10/100/1000 BASE T4S	50				**100%**	
		[HW] SWITCH 24/10/100/1000PWR CORD	50				**100%**	
		[HW] SWITCH ALCATEL LUCEN 9561	50				**100%**	

Tabla 2. Impacto para cada dimensión. (Continuación)

		[HW] SWITCH ALCATEL LUCEN 9556	50				**100%**	
		[HW] SWITCH ALCATEL LUCEN 9557	50				**100%**	
		[HW] SWITCH ALCATEL LUCEN 9558	50				**100%**	
		[HW] SWITCH ALCATEL LUCEN 9559	50				**100%**	
		[HW] SWITCH ALCATEL LUCEN 9543	50				**100%**	
		[HW] SWITCH ALCATEL LUCEN 9544	50				**100%**	
		[HW] SWITCH ALCATEL LUCEN 9545	50				**100%**	
		[HW] SWITCH ALCATEL LUCEN 9548	50				**100%**	

Tabla 2. Impacto para cada dimensión. (Continuación)

		[HW] SWITCH ALCATEL LUCEN 9550	50				**100%**	
		[HW] SWITCH ALCATEL LUCEN 9551	50				**100%**	
		[HW] SWITCH ALCATEL LUCEN 9552	50				**100%**	
		[HW] SWITCH ALCATEL LUCEN 9554	50				**100%**	
		[HW] SWITCH ALCATEL LUCEN 9555	50				**100%**	
		[HW] SWITCH ALCATEL LUCEN 9560	50				**100%**	
		[HW] SWITCH LAYER 3 9574	50				**100%**	
		[HW] SWITCH LAYER 3 9576	50				**100%**	
		[HW] SWITCH LAYER 3 9577	50				**100%**	
		[HW] SWITCH LAYER 3 9575	50				**100%**	

Tabla 2. Impacto para cada dimensión. (Continuación)

		[HW] ROUTER CISCO MODELO 1800 4781	50				**100%**	
		[MEDIA] DDS 1TB	50				**100%**	
		[MEDIA] Materiales físicos	50				**100%**	
		[AUX] UPS 10 KVA 9578	50				**50%**	
		[AUX] UPS 10 KVA 9579	50				**50%**	
		[AUX] UPS 10 KVA 9580	50				**50%**	
		[L] Cuarto o recinto (Oficina)	50				**100%**	
I.3	Contaminación mecánica	[HW] Servidor DNS y DHCP	50				**50%**	
		[HW] Servidor Plataforma RYCA V.2.0	50				**50%**	
		[HW] Servidor Plataforma RYCA V.1	50				**50%**	

Tabla 2. Impacto para cada dimensión. (Continuación)

		[HW] Servidor de Base de Datos ITFIP	50				**50%**	
		[HW] Servidor Firewall Fortigate	50				**50%**	
		[HW] Servidor Contable SIIGO	50				**50%**	
		[HW] Servidor de Pruebas “Desarrollito”	50				**50%**	
		[HW] Servidor de Copias de seguridad de la información del ITFIP	50				**50%**	
		[HW] Computador IMAC APPLE (3 Equipos)	50				**50%**	
		[HW] Computadores HP all-one Pro (18 Equipos)	50				**50%**	
		[HW] Portátil Toshiba (16 equipos)	50				**50%**	

Tabla 2. Impacto para cada dimensión. (Continuación)

		[HW] Tablet negra 9” (1 Equipo)	50				**50%**	
		[HW] Computador IMAC APPLE (3 Equipos)	50				**50%**	
		[HW] Memoria USB	50				**20%**	
		[HW] Discos duros	50				**50%**	
		[HW] Discos duros externos	50				**50%**	
		[HW] SWITCH ALCATEL LUCEN 9553	50				**20%**	
		[HW] SWITCH 24 10/100/1000 BASE T C	50				**20%**	
		[HW] SWITCH 24/10/100/1000 BASE T4S	50				**20%**	
		[HW] SWITCH 24/10/100/1000PWR CORD	50				**20%**	
		[HW] SWITCH ALCATEL LUCEN 9561	50				**20%**	

Tabla 2. Impacto para cada dimensión. (Continuación)

		[HW] SWITCH ALCATEL LUCEN 9556	50				**20%**	
		[HW] SWITCH ALCATEL LUCEN 9557	50				**20%**	
		[HW] SWITCH ALCATEL LUCEN 9558	50				**20%**	
		[HW] SWITCH ALCATEL LUCEN 9559	50				**20%**	
		[HW] SWITCH ALCATEL LUCEN 9543	50				**20%**	
		[HW] SWITCH ALCATEL LUCEN 9544	50				**20%**	
		[HW] SWITCH ALCATEL LUCEN 9545	50				**20%**	
		[HW] SWITCH ALCATEL LUCEN 9548	50				**20%**	

Tabla 2. Impacto para cada dimensión. (Continuación)

		[HW] SWITCH ALCATEL LUCEN 9550	50				**20%**	
		[HW] SWITCH ALCATEL LUCEN 9551	50				**20%**	
		[HW] SWITCH ALCATEL LUCEN 9552	50				**20%**	
		[HW] SWITCH ALCATEL LUCEN 9554	50				**20%**	
		[HW] SWITCH ALCATEL LUCEN 9555	50				**20%**	
		[HW] SWITCH ALCATEL LUCEN 9560	50				**20%**	
		[HW] SWITCH LAYER 3 9574	50				**20%**	
		[HW] SWITCH LAYER 3 9576	50				**20%**	
		[HW] SWITCH LAYER 3 9577	50				**20%**	
		[HW] SWITCH LAYER 3 9575	50				**20%**	

Tabla 2. Impacto para cada dimensión. (Continuación)

		[HW] ROUTER CISCO MODELO 1800 4781	50				**20%**	
		[MEDIA] DDS 1TB	50				**5%**	
		[MEDIA] Materiales físicos	50				**5%**	
		[AUX] UPS 10 KVA 9578	50				**20%**	
		[AUX] UPS 10 KVA 9579	50				**20%**	
		[AUX] UPS 10 KVA 9580	50				**20%**	
I.4	Contaminación electromagnética	[HW] Servidor DNS y DHCP	10				**100%**	
		[HW] Servidor Plataforma RYCA V.2.0	10				**100%**	
		[HW] Servidor Plataforma RYCA V.1	10				**100%**	
		[HW] Servidor de Base de Datos ITFIP	10				**100%**	

Tabla 2. Impacto para cada dimensión. (Continuación)

		[HW] Servidor Firewall Fortigate	10				**100%**	
		[HW] Servidor Contable SIIGO	10				**100%**	
		[HW] Servidor de Pruebas “Desarrollito”	10				**100%**	
		[HW] Servidor de Copias de seguridad de la información del ITFIP	10				**100%**	
		[HW] Computador IMAC APPLE (3 Equipos)	10				**100%**	
		[HW] Computadores HP all-one Pro (18 Equipos)	10				**100%**	
		[HW] Portátil Toshiba (16 equipos)	10				**100%**	
		[HW] Tablet negra 9” (1 Equipo)	10				**100%**	

Tabla 2. Impacto para cada dimensión. (Continuación)

		[HW] Computador IMAC APPLE (3 Equipos)	10				**100%**	
		[HW] Memoria USB	10				**100%**	
		[HW] Discos duros	10				**100%**	
		[HW] Discos duros externos	10				**100%**	
		[HW] SWITCH ALCATEL LUCEN 9553	10				**100%**	
		[HW] SWITCH 24 10/100/1000 BASE T C	10				**100%**	
		[HW] SWITCH 24/10/100/1000 BASE T4S	10				**100%**	
		[HW] SWITCH 24/10/100/1000PWR CORD	10				**100%**	
		[HW] SWITCH ALCATEL LUCEN 9561	10				**100%**	

Tabla 2. Impacto para cada dimensión. (Continuación)

		[HW] SWITCH ALCATEL LUCEN 9556	10				**100%**	
		[HW] SWITCH ALCATEL LUCEN 9557	10				**100%**	
		[HW] SWITCH ALCATEL LUCEN 9558	10				**100%**	
		[HW] SWITCH ALCATEL LUCEN 9559	10				**100%**	
		[HW] SWITCH ALCATEL LUCEN 9543	10				**100%**	
		[HW] SWITCH ALCATEL LUCEN 9544	10				**100%**	
		[HW] SWITCH ALCATEL LUCEN 9545	10				**100%**	
		[HW] SWITCH ALCATEL LUCEN 9548	10				**100%**	

Tabla 2. Impacto para cada dimensión. (Continuación)

		[HW] SWITCH ALCATEL LUCEN 9550	10				**100%**	
		[HW] SWITCH ALCATEL LUCEN 9551	10				**100%**	
		[HW] SWITCH ALCATEL LUCEN 9552	10				**100%**	
		[HW] SWITCH ALCATEL LUCEN 9554	10				**100%**	
		[HW] SWITCH ALCATEL LUCEN 9555	10				**100%**	
		[HW] SWITCH ALCATEL LUCEN 9560	10				**100%**	
		[HW] SWITCH LAYER 3 9574	10				**100%**	
		[HW] SWITCH LAYER 3 9576	10				**100%**	
		[HW] SWITCH LAYER 3 9577	10				**100%**	

Tabla 2. Impacto para cada dimensión. (Continuación)

		[HW] SWITCH LAYER 3 9575	10				**100%**	
		[HW] ROUTER CISCO MODELO 1800 4781	10				**100%**	
		[MEDIA] DDS 1TB	10				**20%**	
		[MEDIA] Materiales físicos	10				**5%**	
		[AUX] UPS 10 KVA 9578	10				**50%**	
		[AUX] UPS 10 KVA 9579	10				**50%**	
		[AUX] UPS 10 KVA 9580	10				**50%**	
I.5	Avería de origen físico o lógico	[SW] Sistema de Registro y Control Académico (RYCA) V.1	10				**75%**	
		[SW] Sistema de Registro y Control Académico (RYCA) V.2.0	10				**75%**	
		[SW] Página Oficial del ITFIP	10				**75%**	

Tabla 2. Impacto para cada dimensión. (Continuación)

		[SW] Google Chrome	10				**50%**	
		[SW] Mozilla Firefox	10				**50%**	
		[SW] Safari	10				**50%**	
		[SW] Microsoft Office 2013	10				**75%**	
		[SW] Open Office Linux 2017	10				**50%**	
		[SW] System Center	10				**50%**	
		[SW] Windows Defender	10				**100%**	
		[SW] Windows 8	10				**100%**	
		[SW] Windows Server 2009	10				**100%**	
		[SW] Windows Server 2012	10				**100%**	
		[SW] CentOS 5	10				**100%**	
		[SW] Debian 7	10				**100%**	
		[SW] Ubuntu 14	10				**100%**	
		[SW] Mac OS X	10				**100%**	

Tabla 2. Impacto para cada dimensión. (Continuación)

		[SW] CoMmanD (CMD)	10				**50%**	
		[SW] CoMmanD line (Mac)	10				**50%**	
		[SW] Terminal	10				**50%**	
		[HW] Servidor DNS y DHCP	10				**100%**	
		[HW] Servidor Plataforma RYCA V.2.0	10				**100%**	
		[HW] Servidor Plataforma RYCA V.1	10				**100%**	
		[HW] Servidor de Base de Datos ITFIP	10				**100%**	
		[HW] Servidor Firewall Fortigate	10				**100%**	
		[HW] Servidor Contable SIIGO	10				**100%**	
		[HW] Servidor de Pruebas “Desarrollito”	10				**100%**	

Tabla 2. Impacto para cada dimensión. (Continuación)

		[HW] Servidor de Copias de seguridad de la información del ITFIP	10				**100%**	
		[HW] Computador IMAC APPLE (3 Equipos)	10				**100%**	
		[HW] Computadores HP all-one Pro (18 Equipos)	10				**100%**	
		[HW] Portátil Toshiba (16 equipos)	10				**100%**	
		[HW] Tablet negra 9” (1 Equipo)	10				**100%**	
		[HW] Computador IMAC APPLE (3 Equipos)	10				**100%**	
		[HW] Memoria USB	10				**100%**	
		[HW] Discos duros	10				**100%**	
		[HW] Discos duros externos	10				**100%**	

Tabla 2. Impacto para cada dimensión. (Continuación)

		[HW] SWITCH ALCATEL LUCEN 9553	10				**100%**	
		[HW] SWITCH 24 10/100/1000 BASE T C	10				**100%**	
		[HW] SWITCH 24/10/100/1000 BASE T4S	10				**100%**	
		[HW] SWITCH 24/10/100/1000PWR CORD	10				**100%**	
		[HW] SWITCH ALCATEL LUCEN 9561	10				**100%**	
		[HW] SWITCH ALCATEL LUCEN 9556	10				**100%**	
		[HW] SWITCH ALCATEL LUCEN 9557	10				**100%**	
		[HW] SWITCH ALCATEL LUCEN 9558	10				**100%**	

Tabla 2. Impacto para cada dimensión. (Continuación)

		[HW] SWITCH ALCATEL LUCEN 9559	10				**100%**	
		[HW] SWITCH ALCATEL LUCEN 9543	10				**100%**	
		[HW] SWITCH ALCATEL LUCEN 9544	10				**100%**	
		[HW] SWITCH ALCATEL LUCEN 9545	10				**100%**	
		[HW] SWITCH ALCATEL LUCEN 9548	10				**100%**	
		[HW] SWITCH ALCATEL LUCEN 9550	10				**100%**	
		[HW] SWITCH ALCATEL LUCEN 9551	10				**100%**	
		[HW] SWITCH ALCATEL LUCEN 9552	10				**100%**	

Tabla 2. Impacto para cada dimensión. (Continuación)

		[HW] SWITCH ALCATEL LUCEN 9554	10				**100%**	
		[HW] SWITCH ALCATEL LUCEN 9555	10				**100%**	
		[HW] SWITCH ALCATEL LUCEN 9560	10				**100%**	
		[HW] SWITCH LAYER 3 9574	10				**100%**	
		[HW] SWITCH LAYER 3 9576	10				**100%**	
		[HW] SWITCH LAYER 3 9577	10				**100%**	
		[HW] SWITCH LAYER 3 9575	10				**100%**	
		[HW] ROUTER CISCO MODELO 1800 4781	10				**100%**	
		[MEDIA] DDS 1TB	10				**100%**	
		[MEDIA] Materiales físicos	10				**5%**	

Tabla 2. Impacto para cada dimensión. (Continuación)

		[AUX] UPS 10 KVA 9578	10				**50%**	
		[AUX] UPS 10 KVA 9579	10				**50%**	
		[AUX] UPS 10 KVA 9580	10				**50%**	
I.6	Corte del suministro eléctrico	[HW] Servidor DNS y DHCP	50				**100%**	
		[HW] Servidor Plataforma RYCA V.2.0	50				**100%**	
		[HW] Servidor Plataforma RYCA V.1	50				**100%**	
		[HW] Servidor de Base de Datos ITFIP	50				**100%**	
		[HW] Servidor Firewall Fortigate	50				**100%**	
		[HW] Servidor Contable SIIGO	50				**100%**	
		[HW] Servidor de Pruebas “Desarrollito”	50				**100%**	

Tabla 2. Impacto para cada dimensión. (Continuación)

		[HW] Servidor de Copias de seguridad de la información del ITFIP	50				**100%**	
		[HW] Computador IMAC APPLE (3 Equipos)	50				**100%**	
		[HW] Computadores HP all-one Pro (18 Equipos)	50				**100%**	
		[HW] Portátil Toshiba (16 equipos)	50				**100%**	
		[HW] Tablet negra 9” (1 Equipo)	50				**100%**	
		[HW] Computador IMAC APPLE (3 Equipos)	50				**100%**	
		[HW] Memoria USB	50				**5%**	
		[HW] Discos duros	50				**5%**	
		[HW] Discos duros externos	50				**5%**	

Tabla 2. Impacto para cada dimensión. (Continuación)

		[HW] SWITCH ALCATEL LUCEN 9553	50				**100%**	
		[HW] SWITCH 24 10/100/1000 BASE T C	50				**100%**	
		[HW] SWITCH 24/10/100/1000 BASE T4S	50				**100%**	
		[HW] SWITCH 24/10/100/1000PWR CORD	50				**100%**	
		[HW] SWITCH ALCATEL LUCEN 9561	50				**100%**	
		[HW] SWITCH ALCATEL LUCEN 9556	50				**100%**	
		[HW] SWITCH ALCATEL LUCEN 9557	50				**100%**	
		[HW] SWITCH ALCATEL LUCEN 9558	50				**100%**	

Tabla 2. Impacto para cada dimensión. (Continuación)

		[HW] SWITCH ALCATEL LUCEN 9559	50				**100%**	
		[HW] SWITCH ALCATEL LUCEN 9543	50				**100%**	
		[HW] SWITCH ALCATEL LUCEN 9544	50				**100%**	
		[HW] SWITCH ALCATEL LUCEN 9545	50				**100%**	
		[HW] SWITCH ALCATEL LUCEN 9548	50				**100%**	
		[HW] SWITCH ALCATEL LUCEN 9550	50				**100%**	
		[HW] SWITCH ALCATEL LUCEN 9551	50				**100%**	
		[HW] SWITCH ALCATEL LUCEN 9552	50				**100%**	

Tabla 2. Impacto para cada dimensión. (Continuación)

		[HW] SWITCH ALCATEL LUCEN 9554	50				**100%**	
		[HW] SWITCH ALCATEL LUCEN 9555	50				**100%**	
		[HW] SWITCH ALCATEL LUCEN 9560	50				**100%**	
		[HW] SWITCH LAYER 3 9574	50				**100%**	
		[HW] SWITCH LAYER 3 9576	50				**100%**	
		[HW] SWITCH LAYER 3 9577	50				**100%**	
		[HW] SWITCH LAYER 3 9575	50				**100%**	
		[HW] ROUTER CISCO MODELO 1800 4781	50				**100%**	
		[MEDIA] DDS 1TB	50				**5%**	
		[MEDIA] Materiales físicos	50				**5%**	
		[AUX] UPS 10 KVA 9578	50				**50%**	

Tabla 2. Impacto para cada dimensión. (Continuación)

		[AUX] UPS 10 KVA 9579	50				**50%**	
		[AUX] UPS 10 KVA 9580	50				**50%**	
I.7	Condiciones inadecuadas de temperatura o humedad	[HW] Servidor DNS y DHCP	50				**100%**	
		[HW] Servidor Plataforma RYCA V.2.0	50				**100%**	
		[HW] Servidor Plataforma RYCA V.1	50				**100%**	
		[HW] Servidor de Base de Datos ITFIP	50				**100%**	
		[HW] Servidor Firewall Fortigate	50				**100%**	
		[HW] Servidor Contable SIIGO	50				**100%**	
		[HW] Servidor de Pruebas “Desarrollito”	50				**100%**	

Tabla 2. Impacto para cada dimensión. (Continuación)

		[HW] Servidor de Copias de seguridad de la información del ITFIP	50				**100%**	
		[HW] Computador IMAC APPLE (3 Equipos)	50				**50%**	
		[HW] Computadores HP all-one Pro (18 Equipos)	50				**50%**	
		[HW] Portátil Toshiba (16 equipos)	50				**50%**	
		[HW] Tablet negra 9” (1 Equipo)	50				**50%**	
		[HW] Computador IMAC APPLE (3 Equipos)	50				**50%**	
		[HW] Memoria USB	50				**20%**	
		[HW] Discos duros	50				**20%**	
		[HW] Discos duros externos	50				**20%**	

Tabla 2. Impacto para cada dimensión. (Continuación)

		[HW] SWITCH ALCATEL LUCEN 9553	50				**50%**	
		[HW] SWITCH 24 10/100/1000 BASE T C	50				**50%**	
		[HW] SWITCH 24/10/100/1000 BASE T4S	50				**50%**	
		[HW] SWITCH 24/10/100/1000PWR CORD	50				**50%**	
		[HW] SWITCH ALCATEL LUCEN 9561	50				**50%**	
		[HW] SWITCH ALCATEL LUCEN 9556	50				**50%**	
		[HW] SWITCH ALCATEL LUCEN 9557	50				**50%**	
		[HW] SWITCH ALCATEL LUCEN 9558	50				**50%**	

Tabla 2. Impacto para cada dimensión. (Continuación)

		[HW] SWITCH ALCATEL LUCEN 9559	50				**50%**	
		[HW] SWITCH ALCATEL LUCEN 9543	50				**50%**	
		[HW] SWITCH ALCATEL LUCEN 9544	50				**50%**	
		[HW] SWITCH ALCATEL LUCEN 9545	50				**50%**	
		[HW] SWITCH ALCATEL LUCEN 9548	50				**50%**	
		[HW] SWITCH ALCATEL LUCEN 9550	50				**50%**	
		[HW] SWITCH ALCATEL LUCEN 9551	50				**50%**	
		[HW] SWITCH ALCATEL LUCEN 9552	50				**50%**	

Tabla 2. Impacto para cada dimensión. (Continuación)

		[HW] SWITCH ALCATEL LUCEN 9554	50				**50%**	
		[HW] SWITCH ALCATEL LUCEN 9555	50				**50%**	
		[HW] SWITCH ALCATEL LUCEN 9560	50				**50%**	
		[HW] SWITCH LAYER 3 9574	50				**50%**	
		[HW] SWITCH LAYER 3 9576	50				**50%**	
		[HW] SWITCH LAYER 3 9577	50				**50%**	
		[HW] SWITCH LAYER 3 9575	50				**50%**	
		[HW] ROUTER CISCO MODELO 1800 4781	50				**50%**	
		[MEDIA] DDS 1TB	50				**20%**	
		[MEDIA] Materiales físicos	50				**50%**	
		[AUX] UPS 10 KVA 9578	50				**20%**	

Tabla 2. Impacto para cada dimensión. (Continuación)

		[AUX] UPS 10 KVA 9579	50				**20%**	
		[AUX] UPS 10 KVA 9580	50				**20%**	
I.8	Fallo de servicios de comunicaciones	[COM] Red telefónica	50				**100%**	
		[COM] Internet Movistar	50				**100%**	
		[COM] Red LAN	50				**75%**	
		[COM] Red WIFI	50				**75%**	
		[COM] Red de datos	50				**100%**	
I.9	Interrupción de otros servicios y suministros esenciales	[AUX] UPS 10 KVA 9578	50				**5%**	
		[AUX] UPS 10 KVA 9579	50				**5%**	
		[AUX] UPS 10 KVA 9580	50				**5%**	
I.10	Degradación de los soportes de almacén amiento de la información	[MEDIA] DDS 1TB	10				**75%**	
		[MEDIA] Materiales físicos	10				**75%**	

Tabla 2. Impacto para cada dimensión. (Continuación)

I.11	Emanaciones electromagnéticas	[HW] Servidor DNS y DHCP	10				**20%**	
		[HW] Servidor Plataforma RYCA V.2.0	10				**20%**	
		[HW] Servidor Plataforma RYCA V.1	10				**20%**	
		[HW] Servidor de Base de Datos ITFIP	10				**20%**	
		[HW] Servidor Firewall Fortigate	10				**20%**	
		[HW] Servidor Contable SIIGO	10				**20%**	
		[HW] Servidor de Pruebas “Desarrollito”	10				**20%**	
		[HW] Servidor de Copias de seguridad de la información del ITFIP	10				**20%**	
		[HW] Computador IMAC APPLE (3 Equipos)	10				**20%**	

Tabla 2. Impacto para cada dimensión. (Continuación)

		[HW] Computadores HP all-one Pro (18 Equipos)	10				**20%**	
		[HW] Portátil Toshiba (16 equipos)	10				**20%**	
		[HW] Tablet negra 9” (1 Equipo)	10				**20%**	
		[HW] Computador IMAC APPLE (3 Equipos)	10				**20%**	
		[HW] Memoria USB	10				**20%**	
		[HW] Discos duros	10				**20%**	
		[HW] Discos duros externos	10				**20%**	
		[HW] SWITCH ALCATEL LUCEN 9553	10				**20%**	
		[HW] SWITCH 24 10/100/1000 BASE T C	10				**20%**	

Tabla 2. Impacto para cada dimensión. (Continuación)

		[HW] SWITCH 24/10/100/1000 BASE T4S	10				**20%**	
		[HW] SWITCH 24/10/100/1000PWR CORD	10				**20%**	
		[HW] SWITCH ALCATEL LUCEN 9561	10				**20%**	
		[HW] SWITCH ALCATEL LUCEN 9556	10				**20%**	
		[HW] SWITCH ALCATEL LUCEN 9557	10				**20%**	
		[HW] SWITCH ALCATEL LUCEN 9558	10				**20%**	
		[HW] SWITCH ALCATEL LUCEN 9559	10				**20%**	
		[HW] SWITCH ALCATEL LUCEN 9543	10				**20%**	

Tabla 2. Impacto para cada dimensión. (Continuación)

		[HW] SWITCH ALCATEL LUCEN 9544	10				**20%**	
		[HW] SWITCH ALCATEL LUCEN 9545	10				**20%**	
		[HW] SWITCH ALCATEL LUCEN 9548	10				**20%**	
		[HW] SWITCH ALCATEL LUCEN 9550	10				**20%**	
		[HW] SWITCH ALCATEL LUCEN 9551	10				**20%**	
		[HW] SWITCH ALCATEL LUCEN 9552	10				**20%**	
		[HW] SWITCH ALCATEL LUCEN 9554	10				**20%**	
		[HW] SWITCH ALCATEL LUCEN 9555	10				**20%**	

Tabla 2. Impacto para cada dimensión. (Continuación)

		[HW] SWITCH ALCATEL LUCEN 9560	10				**20%**	
		[HW] SWITCH LAYER 3 9574	10				**20%**	
		[HW] SWITCH LAYER 3 9576	10				**20%**	
		[HW] SWITCH LAYER 3 9577	10				**20%**	
		[HW] SWITCH LAYER 3 9575	10				**20%**	
		[HW] ROUTER CISCO MODELO 1800 4781	10				**20%**	
		[MEDIA] DDS 1TB	10				**5%**	
		[MEDIA] Materiales físicos	10				**5%**	
		[AUX] UPS 10 KVA 9578	10				**5%**	
		[AUX] UPS 10 KVA 9579	10				**5%**	
		[AUX] UPS 10 KVA 9580	10				**5%**	
		[L] Cuarto o recinto (Oficina)	10				**5%**	

Tabla 2. Impacto para cada dimensión. (Continuación)

E.1	Errores de los usuarios	[D] De cada pc de la dependencia de sistemas	70		**50%**	**75%**	**50%**	
		[D] de cada pc de las dependencias de la institución	70		**50%**	**75%**	**50%**	
		[D] de las configuraciones de los servidores	70		**50%**	**100%**	**75%**	
		[D] Biométricas para acceso a la sala de servidor	70		**100%**	**100%**	**50%**	
		[D] De los usuarios que acceden a los servidores	70		**75%**	**50%**	**75%**	
		[D] servidor de copias de seguridad	70		**75%**	**100%**	**50%**	
		[keys] Usuarios de los Pc de las demás dependencias	70		**75%**	**75%**	**50%**	
		[keys] Sensor biométrico	70		**50%**	**100%**	**50%**	

Tabla 2. Impacto para cada dimensión. (Continuación)

		[keys] Código de confirmación para acceso a la sala de servidor	70		**100%**	**100%**	**75%**	
		[SW] Sistema de Registro y Control Académico (RYCA) V.1	70		**20%**	**75%**	**50%**	
		[SW] Sistema de Registro y Control Académico (RYCA) V.2.0	70		**20%**	**75%**	**50%**	
		[SW] Página Oficial del ITFIP	70		**20%**	**75%**	**50%**	
		[SW] Google Chrome	70		**5%**	**50%**	**20%**	
		[SW] Mozilla Firefox	70		**5%**	**50%**	**20%**	
		[SW] Safari	70		**5%**	**50%**	**20%**	
		[SW] Microsoft Office 2013	70		**5%**	**50%**	**20%**	
		[SW] Open Office Linux 2017	70		**5%**	**50%**	**20%**	
		[SW] System Center	70		**5%**	**50%**	**20%**	

Tabla 2. Impacto para cada dimensión. (Continuación)

		[SW] Windows Defender	70		**5%**	**50%**	**20%**	
		[SW] Windows 8	70		**5%**	**50%**	**20%**	
		[SW] Windows Server 2009	70		**5%**	**50%**	**20%**	
		[SW] Windows Server 2012	70		**5%**	**50%**	**20%**	
		[SW] CentOS 5	70		**5%**	**50%**	**20%**	
		[SW] Debian 7	70		**5%**	**50%**	**20%**	
		[SW] Ubuntu 14	70		**5%**	**50%**	**20%**	
		[SW] Mac OS X	70		**5%**	**50%**	**20%**	
		[SW] CoMmanD (CMD)	70		**5%**	**50%**	**20%**	
		[SW] CoMmanD line (Mac)	70		**5%**	**50%**	**20%**	
		[SW] Terminal	70		**5%**	**50%**	**20%**	
		[MEDIA] DDS 1TB	70		**50%**	**50%**	**20%**	
		[MEDIA] Materiales físicos	70		**100%**	**100%**	**75%**	
E.2	Errores del administrador	[D] De cada pc de la dependencia de sistemas	50		**50%**	**75%**	**50%**	

Tabla 2. Impacto para cada dimensión. (Continuación)

		[D] de cada pc de las dependencias de la institución	50		**50%**	**50%**	**20%**	
		[D] de las configuraciones de los servidores	50		**100%**	**100%**	**100%**	
		[D] Biométricas para acceso a la sala de servidor	50		**75%**	**75%**	**50%**	
		[D] De los usuarios que acceden a los servidores	50		**50%**	**50%**	**50%**	
		[D] servidor de copias de seguridad	50		**100%**	**100%**	**100%**	
		[keys] Usuarios de los Pc de las demás dependencias	50		**20%**	**20%**	**20%**	
		[keys] Sensor biométrico	50		**20%**	**20%**	**20%**	
		[keys] Código de confirmación para acceso a la sala de servidor	50		**100%**	**100%**	**75%**	

Tabla 2. Impacto para cada dimensión. (Continuación)

		[SW] Sistema de Registro y Control Académico (RYCA) V.1	50		**100%**	**75%**	**100%**	
		[SW] Sistema de Registro y Control Académico (RYCA) V.2.0	50		**100%**	**75%**	**100%**	
		[SW] Página Oficial del ITFIP	50		**100%**	**75%**	**100%**	
		[SW] Google Chrome	50		**20%**	**20%**	**20%**	
		[SW] Mozilla Firefox	50		**20%**	**20%**	**20%**	
		[SW] Safari	50		**20%**	**20%**	**20%**	
		[SW] Microsoft Office 2013	50		**20%**	**20%**	**20%**	
		[SW] Open Office Linux 2017	50		**20%**	**20%**	**20%**	
		[SW] System Center	50		**20%**	**20%**	**20%**	
		[SW] Windows Defender	50		**20%**	**20%**	**20%**	
		[SW] Windows 8	50		**20%**	**20%**	**20%**	

Tabla 2. Impacto para cada dimensión. (Continuación)

		[SW] Windows Server 2009	50		**20%**	**20%**	**20%**	
		[SW] Windows Server 2012	50		**20%**	**20%**	**20%**	
		[SW] CentOS 5	50		**20%**	**20%**	**20%**	
		[SW] Debian 7	50		**20%**	**20%**	**20%**	
		[SW] Ubuntu 14	50		**20%**	**20%**	**20%**	
		[SW] Mac OS X	50		**20%**	**20%**	**20%**	
		[SW] CoMmanD (CMD)	50		**20%**	**20%**	**20%**	
		[SW] CoMmanD line (Mac)	50		**20%**	**20%**	**20%**	
		[SW] Terminal	50		**20%**	**20%**	**20%**	
		[HW] Servidor DNS y DHCP	50		**75%**	**100%**	**75%**	
		[HW] Servidor Plataforma RYCA V.2.0	50		**75%**	**100%**	**75%**	
		[HW] Servidor Plataforma RYCA V.1	50		**75%**	**100%**	**75%**	

Tabla 2. Impacto para cada dimensión. (Continuación)

		[HW] Servidor de Base de Datos ITFIP	50		**75%**	**100%**	**75%**	
		[HW] Servidor Firewall Fortigate	50		**75%**	**100%**	**75%**	
		[HW] Servidor Contable SIIGO	50		**75%**	**100%**	**75%**	
		[HW] Servidor de Pruebas “Desarrollito”	50		**75%**	**100%**	**75%**	
		[HW] Servidor de Copias de seguridad de la información del ITFIP	50		**75%**	**100%**	**75%**	
		[HW] Computador IMAC APPLE (3 Equipos)	50		**20%**	**20%**	**20%**	
		[HW] Computadores HP all-one Pro (18 Equipos)	50		**20%**	**20%**	**20%**	
		[HW] Portátil Toshiba (16 equipos)	50		**20%**	**20%**	**20%**	

Tabla 2. Impacto para cada dimensión. (Continuación)

		[HW] Tablet negra 9” (1 Equipo)	50		**20%**	**20%**	**20%**	
		[HW] Computador IMAC APPLE (3 Equipos)	50		**20%**	**20%**	**20%**	
		[HW] Memoria USB	50		**20%**	**20%**	**20%**	
		[HW] Discos duros	50		**20%**	**20%**	**20%**	
		[HW] Discos duros externos	50		**20%**	**20%**	**20%**	
		[HW] SWITCH ALCATEL LUCEN 9553	50		**20%**	**20%**	**20%**	
		[HW] SWITCH 24 10/100/1000 BASE T C	50		**20%**	**20%**	**20%**	
		[HW] SWITCH 24/10/100/1000 BASE T4S	50		**20%**	**20%**	**20%**	
		[HW] SWITCH 24/10/100/1000PWR CORD	50		**20%**	**20%**	**20%**	
		[HW] SWITCH ALCATEL LUCEN 9561	50		**20%**	**20%**	**20%**	

Tabla 2. Impacto para cada dimensión. (Continuación)

		[HW] SWITCH ALCATEL LUCEN 9556	50		**20%**	**20%**	**20%**	
		[HW] SWITCH ALCATEL LUCEN 9557	50		**20%**	**20%**	**20%**	
		[HW] SWITCH ALCATEL LUCEN 9558	50		**20%**	**20%**	**20%**	
		[HW] SWITCH ALCATEL LUCEN 9559	50		**20%**	**20%**	**20%**	
		[HW] SWITCH ALCATEL LUCEN 9543	50		**20%**	**20%**	**20%**	
		[HW] SWITCH ALCATEL LUCEN 9544	50		**20%**	**20%**	**20%**	
		[HW] SWITCH ALCATEL LUCEN 9545	50		**20%**	**20%**	**20%**	
		[HW] SWITCH ALCATEL LUCEN 9548	50		**20%**	**20%**	**20%**	

Tabla 2. Impacto para cada dimensión. (Continuación)

		[HW] SWITCH ALCATEL LUCEN 9550	50		**20%**	**20%**	**20%**	
		[HW] SWITCH ALCATEL LUCEN 9551	50		**20%**	**20%**	**20%**	
		[HW] SWITCH ALCATEL LUCEN 9552	50		**20%**	**20%**	**20%**	
		[HW] SWITCH ALCATEL LUCEN 9554	50		**20%**	**20%**	**20%**	
		[HW] SWITCH ALCATEL LUCEN 9555	50		**20%**	**20%**	**20%**	
		[HW] SWITCH ALCATEL LUCEN 9560	50		**20%**	**20%**	**20%**	
		[HW] SWITCH LAYER 3 9574	50		**20%**	**20%**	**20%**	
		[HW] SWITCH LAYER 3 9576	50		**20%**	**20%**	**20%**	
		[HW] SWITCH LAYER 3 9577	50		**20%**	**20%**	**20%**	
		[HW] SWITCH LAYER 3 9575	50		**20%**	**20%**	**20%**	

Tabla 2. Impacto para cada dimensión. (Continuación)

		[HW] ROUTER CISCO MODELO 1800 4781	50		**20%**	**20%**	**20%**	
		[COM] Red telefónica	50		**20%**	**20%**	**20%**	
		[COM] Internet Movistar	50		**20%**	**20%**	**20%**	
		[COM] Red LAN	50		**20%**	**20%**	**20%**	
		[COM] Red WIFI	50		**20%**	**20%**	**20%**	
		[COM] Red de datos	50		**20%**	**20%**	**20%**	
		[MEDIA] DDS 1TB	50		**50%**	**50%**	**50%**	
		[MEDIA] Materiales físicos	50		**50%**	**50%**	**50%**	
E.7	Deficiencias en la organización	[P] Coordinador de sistemas	10			**50%**		
		[P] Programador	10			**75%**		
		[P] Ingeniero Auxiliar/ Soporte técnico	10			**75%**		

Tabla 2. Impacto para cada dimensión. (Continuación)

E.8	Difusión de software dañino	[SW] Sistema de Registro y Control Académico (RYCA) V.1	10		**100%**	**100%**	**100%**	
		[SW] Sistema de Registro y Control Académico (RYCA) V.2.0	10		**100%**	**100%**	**100%**	
		[SW] Página Oficial del ITFIP	10		**100%**	**100%**	**100%**	
		[SW] Google Chrome	10		**50%**	**75%**	**100%**	
		[SW] Mozilla Firefox	10		**50%**	**75%**	**100%**	
		[SW] Safari	10		**50%**	**75%**	**100%**	
		[SW] Microsoft Office 2013	10		**100%**	**75%**	**100%**	
		[SW] Open Office Linux 2017	10		**100%**	**75%**	**100%**	
		[SW] System Center	10		**100%**	**75%**	**100%**	
		[SW] Windows Defender	10		**100%**	**75%**	**100%**	
		[SW] Windows 8	10		**100%**	**75%**	**100%**	

Tabla 2. Impacto para cada dimensión. (Continuación)

		[SW] Windows Server 2009	10		**100%**	**75%**	**100%**	
		[SW] Windows Server 2012	10		**100%**	**75%**	**100%**	
		[SW] CentOS 5	10		**100%**	**75%**	**100%**	
		[SW] Debian 7	10		**5%**	**75%**	**50%**	
		[SW] Ubuntu 14	10		**5%**	**75%**	**50%**	
		[SW] Mac OS X	10		**100%**	**75%**	**50%**	
		[SW] CoMmanD (CMD)	10		**5%**	**100%**	**75%**	
		[SW] CoMmanD line (Mac)	10		**5%**	**100%**	**75%**	
		[SW] Terminal	10		**5%**	**100%**	**75%**	
E.9	Errores de [re-] encaminamiento	[SW] Sistema de Registro y Control Académico (RYCA) V.1	10		**50%**			
		[SW] Sistema de Registro y Control Académico (RYCA) V.2.0	10		**50%**			

Tabla 2. Impacto para cada dimensión. (Continuación)

		[SW] Página Oficial del ITFIP	10		**5%**			
		[SW] Google Chrome	10		**5%**			
		[SW] Mozilla Firefox	10		**5%**			
		[SW] Safari	10		**5%**			
		[SW] Microsoft Office 2013	10		**50%**			
		[SW] Open Office Linux 2017	10		**50%**			
		[SW] System Center	10		**5%**			
		[SW] Windows Defender	10		**5%**			
		[SW] Windows 8	10		**5%**			
		[SW] Windows Server 2009	10		**75%**			
		[SW] Windows Server 2012	10		**75%**			
		[SW] CentOS 5	10		**75%**			
		[SW] Debian 7	10		**20%**			
		[SW] Ubuntu 14	10		**20%**			

Tabla 2. Impacto para cada dimensión. (Continuación)

		[SW] Mac OS X	10		**75%**			
		[SW] CoMmanD (CMD)	10		**5%**			
		[SW] CoMmanD line (Mac)	10		**5%**			
		[SW] Terminal	10		**5%**			
		[COM] Red telefónica	10		**50%**			
		[COM] Internet Movistar	10		**50%**			
		[COM] Red LAN	10		**50%**			
		[COM] Red WIFI	10		**50%**			
		[COM] Red de datos	10		**75%**			
E.10	Errores de secuencia	[SW] Sistema de Registro y Control Académico (RYCA) V.1	50			**50%**		
		[SW] Sistema de Registro y Control Académico (RYCA) V.2.0	50			**50%**		

Tabla 2. Impacto para cada dimensión. (Continuación)

		[SW] Página Oficial del ITFIP	50			**50%**		
		[SW] Google Chrome	50			**20%**		
		[SW] Mozilla Firefox	50			**20%**		
		[SW] Safari	50			**20%**		
		[SW] Microsoft Office 2013	50			**50%**		
		[SW] Open Office Linux 2017	50			**50%**		
		[SW] System Center	50			**20%**		
		[SW] Windows Defender	50			**20%**		
		[SW] Windows 8	50			**50%**		
		[SW] Windows Server 2009	50			**75%**		
		[SW] Windows Server 2012	50			**75%**		
		[SW] CentOS 5	50			**75%**		

Tabla 2. Impacto para cada dimensión. (Continuación)

		[SW] Debian 7	50			**50%**		
		[SW] Ubuntu 14	50			**50%**		
		[SW] Mac OS X	50			**50%**		
		[SW] CoMmanD (CMD)	50			**20%**		
		[SW] CoMmanD line (Mac)	50			**20%**		
		[SW] Terminal	50			**20%**		
		[COM] Red telefónica	50			**20%**		
		[COM] Internet Movistar	50			**50%**		
		[COM] Red LAN	50			**50%**		
		[COM] Red WIFI	50			**50%**		
		[COM] Red de datos	50			**50%**		
E.15	Alteración accidental de la información	[D] De cada pc de la dependencia de sistemas	10			**50%**		

Tabla 2. Impacto para cada dimensión. (Continuación)

		[D] de cada pc de las dependencias de la institución	10			**50%**		
		[D] de las configuraciones de los servidores	10			**75%**		
		[D] Biométricas para acceso a la sala de servidor	10			**75%**		
		[D] De los usuarios que acceden a los servidores	10			**75%**		
		[D] servidor de copias de seguridad	10			**100%**		
		[keys] Usuarios de los Pc de las demás dependencias	10			**75%**		
		[keys] Sensor biométrico	10			**100%**		
		[keys] Código de confirmación para acceso a la sala de servidor	10			**100%**		

Tabla 2. Impacto para cada dimensión. (Continuación)

		[SW] Sistema de Registro y Control Académico (RYCA) V.1	10			**75%**		
		[SW] Sistema de Registro y Control Académico (RYCA) V.2.0	10			**75%**		
		[SW] Página Oficial del ITFIP	10			**75%**		
		[SW] Google Chrome	10			**20%**		
		[SW] Mozilla Firefox	10			**20%**		
		[SW] Safari	10			**20%**		
		[SW] Microsoft Office 2013	10			**75%**		
		[SW] Open Office Linux 2017	10			**75%**		
		[SW] System Center	10			**50%**		
		[SW] Windows Defender	10			**50%**		

Tabla 2. Impacto para cada dimensión. (Continuación)

		[SW] Windows 8	10			**100%**		
		[SW] Windows Server 2009	10			**75%**		
		[SW] Windows Server 2012	10			**100%**		
		[SW] CentOS 5	10			**100%**		
		[SW] Debian 7	10			**50%**		
		[SW] Ubuntu 14	10			**50%**		
		[SW] Mac OS X	10			**50%**		
		[SW] CoMmanD (CMD)	10			**20%**		
		[SW] CoMmanD line (Mac)	10			**20%**		
		[SW] Terminal	10			**20%**		
		[COM] Red telefónica	10			**100%**		
		[COM] Internet Movistar	10			**100%**		

Tabla 2. Impacto para cada dimensión. (Continuación)

		[COM] Red LAN	10			**20%**		
		[COM] Red WIFI	10			**20%**		
		[COM] Red de datos	10			**20%**		
		[MEDIA] DDS 1TB	10			**50%**		
		[MEDIA] Materiales físicos	10			**100%**		
		[L] Cuarto o recinto (Oficina)	10			**5%**		
E.18	Destrucción de información	[D] De cada pc de la dependencia de sistemas	10				**100%**	
		[D] de cada pc de las dependencias de la institución	10				**100%**	
		[D] de las configuraciones de los servidores	10				**100%**	
		[D] Biométricas para acceso a la sala de servidor	10				**100%**	

Tabla 2. Impacto para cada dimensión. (Continuación)

		[D] De los usuarios que acceden a los servidores	10				**5%**	
		[D] servidor de copias de seguridad	10				**100%**	
		[keys] Usuarios de los Pc de las demás dependencias	10				**5%**	
		[keys] Sensor biométrico	10				**100%**	
		[keys] Código de confirmación para acceso a la sala de servidor	10				**100%**	
		[SW] Sistema de Registro y Control Académico (RYCA) V.1	10				**100%**	
		[SW] Sistema de Registro y Control Académico (RYCA) V.2.0	10				**100%**	
		[SW] Página Oficial del ITFIP	10				**100%**	

Tabla 2. Impacto para cada dimensión. (Continuación)

		[SW] Google Chrome	10				**20%**	
		[SW] Mozilla Firefox	10				**20%**	
		[SW] Safari	10				**20%**	
		[SW] Microsoft Office 2013	10				**100%**	
		[SW] Open Office Linux 2017	10				**100%**	
		[SW] System Center	10				**100%**	
		[SW] Windows Defender	10				**100%**	
		[SW] Windows 8	10				**100%**	
		[SW] Windows Server 2009	10				**100%**	
		[SW] Windows Server 2012	10				**100%**	
		[SW] CentOS 5	10				**100%**	
		[SW] Debian 7	10				**100%**	
		[SW] Ubuntu 14	10				**100%**	

Tabla 2. Impacto para cada dimensión. (Continuación)

		[SW] Mac OS X	10				**100%**	
		[SW] CoMmanD (CMD)	10				**5%**	
		[SW] CoMmanD line (Mac)	10				**5%**	
		[SW] Terminal	10				**5%**	
		[COM] Red telefónica	10				**20%**	
		[COM] Internet Movistar	10				**20%**	
		[COM] Red LAN	10				**20%**	
		[COM] Red WIFI	10				**20%**	
		[COM] Red de datos	10				**20%**	
		[MEDIA] DDS 1TB	10				**100%**	
		[MEDIA] Materiales físicos	10				**50%**	
		[L] Cuarto o recinto (Oficina)	10				**100%**	

Tabla 2. Impacto para cada dimensión. (Continuación)

E.19	Fugas de información	[D] De cada pc de la dependencia de sistemas	10		**100%**			
		[D] de cada pc de las dependencias de la institución	10		**100%**			
		[D] de las configuraciones de los servidores	10		**100%**			
		[D] Biométricas para acceso a la sala de servidor	10		**100%**			
		[D] De los usuarios que acceden a los servidores	10		**100%**			
		[D] servidor de copias de seguridad	10		**100%**			
		[keys] Usuarios de los Pc de las demás dependencias	10		**75%**			
		[keys] Sensor biométrico	10		**100%**			

Tabla 2. Impacto para cada dimensión. (Continuación)

		[keys] Código de confirmación para acceso a la sala de servidor	10		**100%**			
		[SW] Sistema de Registro y Control Académico (RYCA) V.1	10		**100%**			
		[SW] Sistema de Registro y Control Académico (RYCA) V.2.0	10		**100%**			
		[SW] Página Oficial del ITFIP	10		**50%**			
		[SW] Google Chrome	10		**75%**			
		[SW] Mozilla Firefox	10		**75%**			
		[SW] Safari	10		**75%**			
		[SW] Microsoft Office 2013	10		**50%**			
		[SW] Open Office Linux 2017	10		**50%**			
		[SW] System Center	10		**100%**			

Tabla 2. Impacto para cada dimensión. (Continuación)

		[SW] Windows Defender	10		**75%**			
		[SW] Windows 8	10		**75%**			
		[SW] Windows Server 2009	10		**100%**			
		[SW] Windows Server 2012	10		**100%**			
		[SW] CentOS 5	10		**100%**			
		[SW] Debian 7	10		**75%**			
		[SW] Ubuntu 14	10		**75%**			
		[SW] Mac OS X	10		**75%**			
		[SW] CoMmanD (CMD)	10		**5%**			
		[SW] CoMmanD line (Mac)	10		**5%**			
		[SW] Terminal	10		**5%**			
		[COM] Red telefónica	10		**75%**			

Tabla 2. Impacto para cada dimensión. (Continuación)

		[COM] Internet Movistar	10		**75%**			
		[COM] Red LAN	10		**100%**			
		[COM] Red WIFI	10		**100%**			
		[COM] Red de datos	10		**100%**			
		[MEDIA] DDS 1TB	10		**100%**			
		[MEDIA] Materiales físicos	10		**75%**			
		[L] Cuarto o recinto (Oficina)	10		**5%**			
		[P] Coordinador de sistemas	10		**75%**			
		[P] Programador	10		**50%**			
		[P] Ingeniero Auxiliar/ Soporte técnico	10		**5%**			
E.20	Vulnerabilidades de los programas (software)	[SW] Sistema de Registro y Control Académico (RYCA) V.1	10		**50%**	**75%**	**100%**	

Tabla 2. Impacto para cada dimensión. (Continuación)

		[SW] Sistema de Registro y Control Académico (RYCA) V.2.0	10		**50%**	**75%**	**100%**	
		[SW] Página Oficial del ITFIP	10		**50%**	**75%**	**100%**	
		[SW] Google Chrome	10		**50%**	**75%**	**100%**	
		[SW] Mozilla Firefox	10		**50%**	**75%**	**100%**	
		[SW] Safari	10		**50%**	**75%**	**100%**	
		[SW] Microsoft Office 2013	10		**50%**	**75%**	**100%**	
		[SW] Open Office Linux 2017	10		**50%**	**75%**	**100%**	
		[SW] System Center	10		**20%**	**50%**	**50%**	
		[SW] Windows Defender	10		**20%**	**50%**	**50%**	
		[SW] Windows 8	10		**50%**	**50%**	**75%**	
		[SW] Windows Server 2009	10		**50%**	**50%**	**75%**	

Tabla 2. Impacto para cada dimensión. (Continuación)

		[SW] Windows Server 2012	10		**50%**	**50%**	**75%**	
		[SW] CentOS 5	10		**50%**	**50%**	**75%**	
		[SW] Debian 7	10		**50%**	**50%**	**75%**	
		[SW] Ubuntu 14	10		**50%**	**50%**	**75%**	
		[SW] Mac OS X	10		**50%**	**50%**	**75%**	
		[SW] CoMmanD (CMD)	10		**75%**	**50%**	**100%**	
		[SW] CoMmanD line (Mac)	10		**75%**	**50%**	**100%**	
		[SW] Terminal	10		**75%**	**50%**	**100%**	
E.21	Errores de mantenimiento / actualización de programas (software)	[SW] Sistema de Registro y Control Académico (RYCA) V.1	10			**75%**	**50%**	
		[SW] Sistema de Registro y Control Académico (RYCA) V.2.0	10			**75%**	**50%**	

Tabla 2. Impacto para cada dimensión. (Continuación)

		[SW] Página Oficial del ITFIP	10			**75%**	**50%**	
		[SW] Google Chrome	10			**50%**	**20%**	
		[SW] Mozilla Firefox	10			**50%**	**20%**	
		[SW] Safari	10			**50%**	**20%**	
		[SW] Microsoft Office 2013	10			**75%**	**50%**	
		[SW] Open Office Linux 2017	10			**75%**	**50%**	
		[SW] System Center	10			**75%**	**50%**	
		[SW] Windows Defender	10			**75%**	**75%**	
		[SW] Windows 8	10			**75%**	**75%**	
		[SW] Windows Server 2009	10			**75%**	**75%**	
		[SW] Windows Server 2012	10			**75%**	**75%**	
		[SW] CentOS 5	10			**75%**	**75%**	

Tabla 2. Impacto para cada dimensión. (Continuación)

		[SW] Debian 7	10			**75%**	**75%**	
		[SW] Ubuntu 14	10			**75%**	**75%**	
		[SW] Mac OS X	10			**75%**	**75%**	
		[SW] CoMmanD (CMD)	10			**75%**	**100%**	
		[SW] CoMmanD line (Mac)	10			**50%**	**75%**	
		[SW] Terminal	10			**100%**	**75%**	
E.23	Errores de mantenimiento / actualización de equipos(hardware)	[HW] Servidor DNS y DHCP	10				**100%**	
		[HW] Servidor Plataforma RYCA V.2.0	10				**100%**	
		[HW] Servidor Plataforma RYCA V.1	10				**100%**	
		[HW] Servidor de Base de Datos ITFIP	10				**100%**	
		[HW] Servidor Firewall Fortigate	10				**100%**	

Tabla 2. Impacto para cada dimensión. (Continuación)

		[HW] Servidor Contable SIIGO	10				**100%**	
		[HW] Servidor de Pruebas “Desarrollito”	10				**100%**	
		[HW] Servidor de Copias de seguridad de la información del ITFIP	10				**100%**	
		[HW] Computador IMAC APPLE (3 Equipos)	10				**100%**	
		[HW] Computadores HP all-one Pro (18 Equipos)	10				**100%**	
		[HW] Portátil Toshiba (16 equipos)	10				**100%**	
		[HW] Tablet negra 9” (1 Equipo)	10				**100%**	
		[HW] Computador IMAC APPLE (3 Equipos)	10				**100%**	

Tabla 2. Impacto para cada dimensión. (Continuación)

		[HW] Memoria USB	10				**75%**	
		[HW] Discos duros	10				**50%**	
		[HW] Discos duros externos	10				**50%**	
		[HW] SWITCH ALCATEL LUCEN 9553	10				**50%**	
		[HW] SWITCH 24 10/100/1000 BASE T C	10				**50%**	
		[HW] SWITCH 24/10/100/1000 BASE T4S	10				**50%**	
		[HW] SWITCH 24/10/100/1000PWR CORD	10				**50%**	
		[HW] SWITCH ALCATEL LUCEN 9561	10				**50%**	
		[HW] SWITCH ALCATEL LUCEN 9556	10				**50%**	

Tabla 2. Impacto para cada dimensión. (Continuación)

		[HW] SWITCH ALCATEL LUCEN 9557	10				**50%**	
		[HW] SWITCH ALCATEL LUCEN 9558	10				**50%**	
		[HW] SWITCH ALCATEL LUCEN 9559	10				**50%**	
		[HW] SWITCH ALCATEL LUCEN 9543	10				**50%**	
		[HW] SWITCH ALCATEL LUCEN 9544	10				**50%**	
		[HW] SWITCH ALCATEL LUCEN 9545	10				**50%**	
		[HW] SWITCH ALCATEL LUCEN 9548	10				**50%**	
		[HW] SWITCH ALCATEL LUCEN 9550	10				**50%**	

Tabla 2. Impacto para cada dimensión. (Continuación)

		[HW] SWITCH ALCATEL LUCEN 9551	10				**50%**	
		[HW] SWITCH ALCATEL LUCEN 9552	10				**50%**	
		[HW] SWITCH ALCATEL LUCEN 9554	10				**50%**	
		[HW] SWITCH ALCATEL LUCEN 9555	10				**50%**	
		[HW] SWITCH ALCATEL LUCEN 9560	10				**50%**	
		[HW] SWITCH LAYER 3 9574	10				**50%**	
		[HW] SWITCH LAYER 3 9576	10				**50%**	
		[HW] SWITCH LAYER 3 9577	10				**50%**	
		[HW] SWITCH LAYER 3 9575	10				**50%**	
		[HW] ROUTER CISCO MODELO 1800 4781	10				**50%**	

Tabla 2. Impacto para cada dimensión. (Continuación)

		[MEDIA] DDS 1TB	10				**50%**	
		[MEDIA] Materiales físicos	10				**50%**	
		[AUX] UPS 10 KVA 9578	10				**50%**	
		[AUX] UPS 10 KVA 9579	10				**50%**	
		[AUX] UPS 10 KVA 9580	10				**50%**	
E.24	Caída del sistema por agotamiento de recursos	[HW] Servidor DNS y DHCP	10				**100%**	
		[HW] Servidor Plataforma RYCA V.2.0	10				**100%**	
		[HW] Servidor Plataforma RYCA V.1	10				**100%**	
		[HW] Servidor de Base de Datos ITFIP	10				**100%**	
		[HW] Servidor Firewall Fortigate	10				**100%**	
		[HW] Servidor Contable SIIGO	10				**100%**	

Tabla 2. Impacto para cada dimensión.

		[HW] Servidor de Pruebas “Desarrollito”	10				**100%**	
		[HW] Servidor de Copias de seguridad de la información del ITFIP	10				**100%**	
		[HW] Computador IMAC APPLE (3 Equipos)	10				**100%**	
		[HW] Computadores HP all-one Pro (18 Equipos)	10				**100%**	
		[HW] Portátil Toshiba (16 equipos)	10				**100%**	
		[HW] Tablet negra 9” (1 Equipo)	10				**100%**	
		[HW] Computador IMAC APPLE (3 Equipos)	10				**100%**	
		[HW] Memoria USB	10				**75%**	

Tabla 2. Impacto para cada dimensión. (Continuación)

		[HW] Discos duros	10				**100%**	
		[HW] Discos duros externos	10				**75%**	
		[HW] SWITCH ALCATEL LUCEN 9553	10				**100%**	
		[HW] SWITCH 24 10/100/1000 BASE T C	10				**100%**	
		[HW] SWITCH 24/10/100/1000 BASE T4S	10				**100%**	
		[HW] SWITCH 24/10/100/1000PWR CORD	10				**100%**	
		[HW] SWITCH ALCATEL LUCEN 9561	10				**100%**	
		[HW] SWITCH ALCATEL LUCEN 9556	10				**100%**	
		[HW] SWITCH ALCATEL LUCEN 9557	10				**100%**	

Tabla 2. Impacto para cada dimensión. (Continuación)

		[HW] SWITCH ALCATEL LUCEN 9558	10				**100%**	
		[HW] SWITCH ALCATEL LUCEN 9559	10				**100%**	
		[HW] SWITCH ALCATEL LUCEN 9543	10				**100%**	
		[HW] SWITCH ALCATEL LUCEN 9544	10				**100%**	
		[HW] SWITCH ALCATEL LUCEN 9545	10				**100%**	
		[HW] SWITCH ALCATEL LUCEN 9548	10				**100%**	
		[HW] SWITCH ALCATEL LUCEN 9550	10				**100%**	
		[HW] SWITCH ALCATEL LUCEN 9551	10				**100%**	

Tabla 2. Impacto para cada dimensión. (Continuación)

		[HW] SWITCH ALCATEL LUCEN 9552	10				**100%**	
		[HW] SWITCH ALCATEL LUCEN 9554	10				**100%**	
		[HW] SWITCH ALCATEL LUCEN 9555	10				**100%**	
		[HW] SWITCH ALCATEL LUCEN 9560	10				**100%**	
		[HW] SWITCH LAYER 3 9574	10				**100%**	
		[HW] SWITCH LAYER 3 9576	10				**100%**	
		[HW] SWITCH LAYER 3 9577	10				**100%**	
		[HW] SWITCH LAYER 3 9575	10				**100%**	
		[HW] ROUTER CISCO MODELO 1800 4781	10				**100%**	
		[COM] Red telefónica	10				**100%**	

Tabla 2. Impacto para cada dimensión. (Continuación)

		[COM] Internet Movistar	10				**50%**	
		[COM] Red LAN	10				**50%**	
		[COM] Red WIFI	10				**75%**	
		[COM] Red de datos	10				**100%**	
E.25	Perdida de equipos (Robo)	[HW] Servidor DNS y DHCP	10		**100%**		**100%**	
		[HW] Servidor Plataforma RYCA V.2.0	10		**100%**		**100%**	
		[HW] Servidor Plataforma RYCA V.1	10		**100%**		**100%**	
		[HW] Servidor de Base de Datos ITFIP	10		**100%**		**100%**	
		[HW] Servidor Firewall Fortigate	10		**100%**		**100%**	
		[HW] Servidor Contable SIIGO	10		**100%**		**100%**	
		[HW] Servidor de Pruebas “Desarrollito”	10		**100%**		**100%**	

Tabla 2. Impacto para cada dimensión. (Continuación)

		[HW] Servidor de Copias de seguridad de la información del ITFIP	10		**100%**		**100%**	
		[HW] Computador IMAC APPLE (3 Equipos)	10		**75%**		**100%**	
		[HW] Computadores HP all-one Pro (18 Equipos)	10		**75%**		**100%**	
		[HW] Portátil Toshiba (16 equipos)	10		**75%**		**100%**	
		[HW] Tablet negra 9” (1 Equipo)	10		**50%**		**100%**	
		[HW] Computador IMAC APPLE (3 Equipos)	10		**75%**		**100%**	
		[HW] Memoria USB	10		**20%**		**100%**	
		[HW] Discos duros	10		**20%**		**100%**	
		[HW] Discos duros externos	10		**20%**		**100%**	

Tabla 2. Impacto para cada dimensión. (Continuación)

		[HW] SWITCH ALCATEL LUCEN 9553	10		**20%**		**100%**	
		[HW] SWITCH 24 10/100/1000 BASE T C	10		**20%**		**100%**	
		[HW] SWITCH 24/10/100/1000 BASE T4S	10		**20%**		**100%**	
		[HW] SWITCH 24/10/100/1000PWR CORD	10		**20%**		**100%**	
		[HW] SWITCH ALCATEL LUCEN 9561	10		**20%**		**100%**	
		[HW] SWITCH ALCATEL LUCEN 9556	10		**20%**		**100%**	
		[HW] SWITCH ALCATEL LUCEN 9557	10		**20%**		**100%**	
		[HW] SWITCH ALCATEL LUCEN 9558	10		**20%**		**100%**	

Tabla 2. Impacto para cada dimensión. (Continuación)

		[HW] SWITCH ALCATEL LUCEN 9559	10		**20%**		**100%**	
		[HW] SWITCH ALCATEL LUCEN 9543	10		**20%**		**100%**	
		[HW] SWITCH ALCATEL LUCEN 9544	10		**20%**		**100%**	
		[HW] SWITCH ALCATEL LUCEN 9545	10		**20%**		**100%**	
		[HW] SWITCH ALCATEL LUCEN 9548	10		**20%**		**100%**	
		[HW] SWITCH ALCATEL LUCEN 9550	10		**20%**		**100%**	
		[HW] SWITCH ALCATEL LUCEN 9551	10		**20%**		**100%**	
		[HW] SWITCH ALCATEL LUCEN 9552	10		**20%**		**100%**	

Tabla 2. Impacto para cada dimensión. (Continuación)

		[HW] SWITCH ALCATEL LUCEN 9554	10		**20%**		**100%**	
		[HW] SWITCH ALCATEL LUCEN 9555	10		**20%**		**100%**	
		[HW] SWITCH ALCATEL LUCEN 9560	10		**20%**		**100%**	
		[HW] SWITCH LAYER 3 9574	10		**20%**		**100%**	
		[HW] SWITCH LAYER 3 9576	10		**20%**		**100%**	
		[HW] SWITCH LAYER 3 9577	10		**20%**		**100%**	
		[HW] SWITCH LAYER 3 9575	10		**20%**		**100%**	
		[HW] ROUTER CISCO MODELO 1800 4781	10		**20%**		**100%**	
		[MEDIA] DDS 1TB	10		**20%**		**100%**	
		[MEDIA] Materiales físicos	10		**20%**		**100%**	

Tabla 2. Impacto para cada dimensión. (Continuación)

		[AUX] UPS 10 KVA 9578	10		**20%**		**100%**	
		[AUX] UPS 10 KVA 9579	10		**20%**		**100%**	
		[AUX] UPS 10 KVA 9580	10		**20%**		**100%**	
E.28	Indisponibilidad del personal	[P] Coordinador de sistemas	10				**100%**	
		[P] Programador	10				**100%**	
		[P] Ingeniero Auxiliar/ Soporte técnico	10				**100%**	
A.5	Suplantación de la identidad del usuario	[D] De cada pc de la dependencia de sistemas	10	**100%**	**75%**	**50%**		
		[D] de cada pc de las dependencias de la institución	10	**100%**	**100%**	**75%**		
		[D] de las configuraciones de los servidores	10	**100%**	**100%**	**100%**		
		[D] Biométricas para acceso a la sala de servidor	10	**100%**	**100%**	**100%**		

Tabla 2. Impacto para cada dimensión. (Continuación)

		[D] De los usuarios que acceden a los servidores	10	**100%**	**100%**	**100%**		
		[D] servidor de copias de seguridad	10	**100%**	**100%**	**100%**		
		[keys] Usuarios de los Pc de las demás dependencias	10	**100%**	**100%**	**100%**		
		[keys] Sensor biométrico	10	**100%**	**100%**	**100%**		
		[keys] Código de confirmación para acceso a la sala de servidor	10	**100%**	**100%**	**100%**		
		[SW] Sistema de Registro y Control Académico (RYCA) V.1	10	**100%**	**100%**	**100%**		
		[SW] Sistema de Registro y Control Académico (RYCA) V.2.0	10	**100%**	**100%**	**100%**		
		[SW] Página Oficial del ITFIP	10	**5%**	**5%**	**5%**		

Tabla 2. Impacto para cada dimensión. (Continuación)

		[SW] Google Chrome	10	**5%**	**5%**	**5%**		
		[SW] Mozilla Firefox	10	**5%**	**5%**	**5%**		
		[SW] Safari	10	**5%**	**5%**	**5%**		
		[SW] Microsoft Office 2013	10	**5%**	**5%**	**5%**		
		[SW] Open Office Linux 2017	10	**5%**	**5%**	**5%**		
		[SW] System Center	10	**5%**	**5%**	**5%**		
		[SW] Windows Defender	10	**5%**	**5%**	**5%**		
		[SW] Windows 8	10	**20%**	**20%**	**20%**		
		[SW] Windows Server 2009	10	**100%**	**100%**	**100%**		
		[SW] Windows Server 2012	10	**100%**	**100%**	**100%**		
		[SW] CentOS 5	10	**100%**	**100%**	**100%**		
		[SW] Debian 7	10	**20%**	**20%**	**20%**		

Tabla 2. Impacto para cada dimensión. (Continuación)

		[SW] Ubuntu 14	10	**20%**	**20%**	**20%**		
		[SW] Mac OS X	10	**100%**	**100%**	**100%**		
		[SW] CoMmanD (CMD)	10	**5%**	**5%**	**5%**		
		[SW] CoMmanD line (Mac)	10	**5%**	**5%**	**5%**		
		[SW] Terminal	10	**5%**	**5%**	**5%**		
		[COM] Red telefónica	10	**50%**	**50%**	**50%**		
		[{ñ-COM] Internet Movistar	10	**5%**	**5%**	**5%**		
		[COM] Red LAN	10	**50%**	**50%**	**50%**		
		[COM] Red WIFI	10	**50%**	**50%**	**50%**		
		[COM] Red de datos	10	**75%**	**75%**	**75%**		
A.6	Abuso de privilegios de acceso	[D] De cada pc de la dependencia de sistemas	10		**100%**	**50%**	**20%**	
		[D] de cada pc de las dependencias de la institución	10		**75%**	**50%**	**20%**	

Tabla 2. Impacto para cada dimensión. (Continuación)

		[D] de las configuraciones de los servidores	10		**100%**	**50%**	**20%**	
		[D] Biométricas para acceso a la sala de servidor	10		**75%**	**50%**	**20%**	
		[D] De los usuarios que acceden a los servidores	10		**75%**	**50%**	**75%**	
		[D] servidor de copias de seguridad	10		**20%**	**75%**	**100%**	
		[keys] Usuarios de los Pc de las demás dependencias	10		**100%**	**50%**	**20%**	
		[keys] Sensor biométrico	10		**75%**	**50%**	**20%**	
		[keys] Código de confirmación para acceso a la sala de servidor	10		**75%**	**50%**	**75%**	
		[SW] Sistema de Registro y Control Académico (RYCA) V.1	10		**50%**	**75%**	**100%**	

Tabla 2. Impacto para cada dimensión. (Continuación)

		[SW] Sistema de Registro y Control Académico (RYCA) V.2.0	10		**50%**	**75%**	**100%**	
		[SW] Página Oficial del ITFIP	10		**50%**	**75%**	**100%**	
		[SW] Google Chrome	10		**20%**	**50%**	**20%**	
		[SW] Mozilla Firefox	10		**20%**	**50%**	**20%**	
		[SW] Safari	10		**20%**	**50%**	**20%**	
		[SW] Microsoft Office 2013	10		**100%**	**50%**	**20%**	
		[SW] Open Office Linux 2017	10		**75%**	**50%**	**20%**	
		[SW] System Center	10		**100%**	**50%**	**20%**	
		[SW] Windows Defender	10		**75%**	**50%**	**20%**	
		[SW] Windows 8	10		**100%**	**50%**	**20%**	

Tabla 2. Impacto para cada dimensión. (Continuación)

		[SW] Windows Server 2009	10		**75%**	**50%**	**20%**	
		[SW] Windows Server 2012	10		**75%**	**50%**	**75%**	
		[SW] CentOS 5	10		**50%**	**75%**	**100%**	
		[SW] Debian 7	10		**100%**	**50%**	**20%**	
		[SW] Ubuntu 14	10		**75%**	**50%**	**20%**	
		[SW] Mac OS X	10		**100%**	**50%**	**20%**	
		[SW] CoMmanD (CMD)	10		**75%**	**50%**	**20%**	
		[SW] CoMmanD line (Mac)	10		**75%**	**50%**	**75%**	
		[SW] Terminal	10		**50%**	**75%**	**100%**	
		[HW] Servidor DNS y DHCP	10		**75%**	**50%**	**75%**	
		[HW] Servidor Plataforma RYCA V.2.0	10		**50%**	**75%**	**100%**	

Tabla 2. Impacto para cada dimensión. (Continuación)

		[HW] Servidor Plataforma RYCA V.1	10		**100%**	**75%**	**100%**	
		[HW] Servidor de Base de Datos ITFIP	10		**100%**	**75%**	**100%**	
		[HW] Servidor Firewall Fortigate	10		**100%**	**75%**	**100%**	
		[HW] Servidor Contable SIIGO	10		**100%**	**75%**	**100%**	
		[HW] Servidor de Pruebas “Desarrollito”	10		**100%**	**75%**	**100%**	
		[HW] Servidor de Copias de seguridad de la información del ITFIP	10		**100%**	**75%**	**100%**	
		[HW] Computador IMAC APPLE (3 Equipos)	10		**20%**	**50%**	**20%**	
		[HW] Computadores HP all-one Pro (18 Equipos)	10		**20%**	**50%**	**20%**	

Tabla 2. Impacto para cada dimensión. (Continuación)

		[HW] Portátil Toshiba (16 equipos)	10		**20%**	**50%**	**20%**	
		[HW] Tablet negra 9” (1 Equipo)	10		**100%**	**50%**	**20%**	
		[HW] Computador IMAC APPLE (3 Equipos)	10		**75%**	**50%**	**20%**	
		[HW] Memoria USB	10		**100%**	**50%**	**20%**	
		[HW] Discos duros	10		**75%**	**50%**	**20%**	
		[HW] Discos duros externos	10		**100%**	**50%**	**20%**	
		[HW] SWITCH ALCATEL LUCEN 9553	10		**75%**	**50%**	**20%**	
		[HW] SWITCH 24 10/100/1000 BASE T C	10		**20%**	**50%**	**20%**	
		[HW] SWITCH 24/10/100/1000 BASE T4S	10		**20%**	**50%**	**20%**	

Tabla 2. Impacto para cada dimensión. (Continuación)

		[HW] SWITCH 24/10/100/1000PWR CORD	10		**20%**	**50%**	**20%**	
		[HW] SWITCH ALCATEL LUCEN 9561	10		**100%**	**50%**	**20%**	
		[HW] SWITCH ALCATEL LUCEN 9556	10		**75%**	**50%**	**20%**	
		[HW] SWITCH ALCATEL LUCEN 9557	10		**100%**	**50%**	**20%**	
		[HW] SWITCH ALCATEL LUCEN 9558	10		**75%**	**50%**	**20%**	
		[HW] SWITCH ALCATEL LUCEN 9559	10		**100%**	**50%**	**20%**	
		[HW] SWITCH ALCATEL LUCEN 9543	10		**75%**	**50%**	**20%**	
		[HW] SWITCH ALCATEL LUCEN 9544	10		**20%**	**50%**	**20%**	

Tabla 2. Impacto para cada dimensión. (Continuación)

		[HW] SWITCH ALCATEL LUCEN 9545	10		**20%**	**50%**	**20%**	
		[HW] SWITCH ALCATEL LUCEN 9548	10		**20%**	**50%**	**20%**	
		[HW] SWITCH ALCATEL LUCEN 9550	10		**100%**	**50%**	**20%**	
		[HW] SWITCH ALCATEL LUCEN 9551	10		**75%**	**50%**	**20%**	
		[HW] SWITCH ALCATEL LUCEN 9552	10		**100%**	**50%**	**20%**	
		[HW] SWITCH ALCATEL LUCEN 9554	10		**75%**	**50%**	**20%**	
		[HW] SWITCH ALCATEL LUCEN 9555	10		**100%**	**50%**	**20%**	
		[HW] SWITCH ALCATEL LUCEN 9560	10		**75%**	**50%**	**20%**	
		[HW] SWITCH LAYER 3 9574	10		**20%**	**50%**	**20%**	

Tabla 2. Impacto para cada dimensión. (Continuación)

		[HW] SWITCH LAYER 3 9576	10		**20%**	**50%**	**20%**	
		[HW] SWITCH LAYER 3 9577	10		**20%**	**50%**	**20%**	
		[HW] SWITCH LAYER 3 9575	10		**100%**	**50%**	**20%**	
		[HW] ROUTER CISCO MODELO 1800 4781	10		**75%**	**50%**	**20%**	
		[COM] Red telefónica	10		**100%**	**50%**	**20%**	
		[COM] Internet Movistar	10		**75%**	**50%**	**20%**	
		[COM] Red LAN	10		**100%**	**50%**	**20%**	
		[COM] Red WIFI	10		**75%**	**50%**	**20%**	
		[COM] Red de datos	10		**20%**	**20%**	**20%**	
A.7	Uso no previsto	[SW] Sistema de Registro y Control Académico (RYCA) V.1	10		**20%**	**20%**	**20%**	

Tabla 2. Impacto para cada dimensión. (Continuación)

		[SW] Sistema de Registro y Control Académico (RYCA) V.2.0	10		**20%**	**50%**	**20%**	
		[SW] Página Oficial del ITFIP	10		**20%**	**50%**	**20%**	
		[SW] Google Chrome	10		**100%**	**50%**	**20%**	
		[SW] Mozilla Firefox	10		**75%**	**50%**	**20%**	
		[SW] Safari	10		**100%**	**50%**	**20%**	
		[SW] Microsoft Office 2013	10		**75%**	**50%**	**20%**	
		[SW] Open Office Linux 2017	10		**100%**	**50%**	**20%**	
		[SW] System Center	10		**75%**	**50%**	**20%**	
		[SW] Windows Defender	10		**20%**	**50%**	**20%**	
		[SW] Windows 8	10		**20%**	**50%**	**20%**	
		[SW] Windows Server 2009	10		**20%**	**50%**	**20%**	

Tabla 2. Impacto para cada dimensión. (Continuación)

		[SW] Windows Server 2012	10		**100%**	**50%**	**20%**	
		[SW] CentOS 5	10		**75%**	**50%**	**20%**	
		[SW] Debian 7	10		**100%**	**50%**	**20%**	
		[SW] Ubuntu 14	10		**75%**	**50%**	**20%**	
		[SW] Mac OS X	10		**100%**	**50%**	**20%**	
		[SW] CoMmanD (CMD)	10		**75%**	**50%**	**20%**	
		[SW] CoMmanD line (Mac)	10		**20%**	**50%**	**20%**	
		[SW] Terminal	10		**20%**	**50%**	**20%**	
		[HW] Servidor DNS y DHCP	10		**20%**	**50%**	**20%**	
		[HW] Servidor Plataforma RYCA V.2.0	10		**100%**	**50%**	**20%**	
		[HW] Servidor Plataforma RYCA V.1	10		**75%**	**50%**	**20%**	

Tabla 2. Impacto para cada dimensión. (Continuación)

		[HW] Servidor de Base de Datos ITFIP	10		**100%**	**50%**	**20%**	
		[HW] Servidor Firewall Fortigate	10		**75%**	**50%**	**20%**	
		[HW] Servidor Contable SIIGO	10		**100%**	**50%**	**20%**	
		[HW] Servidor de Pruebas “Desarrollito”	10		**75%**	**50%**	**20%**	
		[HW] Servidor de Copias de seguridad de la información del ITFIP	10		**20%**	**50%**	**20%**	
		[HW] Computador IMAC APPLE (3 Equipos)	10		**20%**	**50%**	**20%**	
		[HW] Computadores HP all-one Pro (18 Equipos)	10		**20%**	**50%**	**20%**	
		[HW] Portátil Toshiba (16 equipos)	10		**100%**	**50%**	**20%**	

Tabla 2. Impacto para cada dimensión. (Continuación)

		[HW] Tablet negra 9” (1 Equipo)	10		**75%**	**50%**	**20%**	
		[HW] Computador IMAC APPLE (3 Equipos)	10		**100%**	**50%**	**20%**	
		[HW] Memoria USB	10		**75%**	**50%**	**20%**	
		[HW] Discos duros	10		**100%**	**50%**	**20%**	
		[HW] Discos duros externos	10		**75%**	**50%**	**20%**	
		[HW] SWITCH ALCATEL LUCEN 9553	10		**20%**	**50%**	**20%**	
		[HW] SWITCH 24 10/100/1000 BASE T C	10		**20%**	**50%**	**20%**	
		[HW] SWITCH 24/10/100/1000 BASE T4S	10		**20%**	**50%**	**20%**	
		[HW] SWITCH 24/10/100/1000PWR CORD	10		**100%**	**50%**	**20%**	
		[HW] SWITCH ALCATEL LUCEN 9561	10		**75%**	**50%**	**20%**	

Tabla 2. Impacto para cada dimensión. (Continuación)

		[HW] SWITCH ALCATEL LUCEN 9556	10		**100%**	**50%**	**20%**	
		[HW] SWITCH ALCATEL LUCEN 9557	10		**75%**	**50%**	**20%**	
		[HW] SWITCH ALCATEL LUCEN 9558	10		**100%**	**50%**	**20%**	
		[HW] SWITCH ALCATEL LUCEN 9559	10		**75%**	**50%**	**20%**	
		[HW] SWITCH ALCATEL LUCEN 9543	10		**20%**	**50%**	**20%**	
		[HW] SWITCH ALCATEL LUCEN 9544	10		**20%**	**50%**	**20%**	
		[HW] SWITCH ALCATEL LUCEN 9545	10		**20%**	**50%**	**20%**	
		[HW] SWITCH ALCATEL LUCEN 9548	10		**100%**	**50%**	**20%**	

Tabla 2. Impacto para cada dimensión. (Continuación)

		[HW] SWITCH ALCATEL LUCEN 9550	10		**75%**	**50%**	**20%**	
		[HW] SWITCH ALCATEL LUCEN 9551	10		**100%**	**50%**	**20%**	
		[HW] SWITCH ALCATEL LUCEN 9552	10		**75%**	**50%**	**20%**	
		[HW] SWITCH ALCATEL LUCEN 9554	10		**100%**	**50%**	**20%**	
		[HW] SWITCH ALCATEL LUCEN 9555	10		**75%**	**50%**	**20%**	
		[HW] SWITCH ALCATEL LUCEN 9560	10		**20%**	**50%**	**20%**	
		[HW] SWITCH LAYER 3 9574	10		**20%**	**50%**	**20%**	
		[HW] SWITCH LAYER 3 9576	10		**20%**	**50%**	**20%**	
		[HW] SWITCH LAYER 3 9577	10		**100%**	**50%**	**20%**	

Tabla 2. Impacto para cada dimensión. (Continuación)

		[HW] SWITCH LAYER 3 9575	10		**75%**	**50%**	**20%**	
		[HW] ROUTER CISCO MODELO 1800 4781	10		**100%**	**50%**	**20%**	
		[COM] Red telefónica	10		**75%**	**50%**	**20%**	
		[COM] Internet Movistar	10		**100%**	**50%**	**20%**	
		[COM] Red LAN	10		**75%**	**50%**	**20%**	
		[COM] Red WIFI	10		**100%**	**50%**	**20%**	
		[COM] Red de datos	10		**75%**	**50%**	**20%**	
		[MEDIA] DDS 1TB	10		**100%**	**50%**	**20%**	
		[MEDIA] Materiales físicos	10		**75%**	**50%**	**20%**	
		[AUX] UPS 10 KVA 9578	10		**100%**	**50%**	**20%**	
		[AUX] UPS 10 KVA 9579	10		**75%**	**50%**	**20%**	
		[AUX] UPS 10 KVA 9580	10		**100%**	**50%**	**20%**	

Tabla 2. Impacto para cada dimensión. (Continuación)

		[L] Cuarto o recinto (Oficina)	10		**75%**	**50%**	**20%**	
A.8	Difusión de software dañino	[SW] Sistema de Registro y Control Académico (RYCA) V.1	10		**100%**	**75%**	**100%**	
		[SW] Sistema de Registro y Control Académico (RYCA) V.2.0	10		**100%**	**75%**	**100%**	
		[SW] Página Oficial del ITFIP	10		**100%**	**75%**	**100%**	
		[SW] Google Chrome	10		**20%**	**50%**	**75%**	
		[SW] Mozilla Firefox	10		**20%**	**50%**	**75%**	
		[SW] Safari	10		**20%**	**50%**	**75%**	
		[SW] Microsoft Office 2013	10		**100%**	**75%**	**100%**	
		[SW] Open Office Linux 2017	10		**100%**	**75%**	**100%**	
		[SW] System Center	10		**100%**	**75%**	**100%**	

Tabla 2. Impacto para cada dimensión. (Continuación)

		[SW] Windows Defender	10		**100%**	**75%**	**100%**	
		[SW] Windows 8	10		**100%**	**75%**	**100%**	
		[SW] Windows Server 2009	10		**100%**	**75%**	**100%**	
		[SW] Windows Server 2012	10		**100%**	**75%**	**100%**	
		[SW] CentOS 5	10		**100%**	**75%**	**100%**	
		[SW] Debian 7	10		**100%**	**75%**	**100%**	
		[SW] Ubuntu 14	10		**100%**	**75%**	**100%**	
		[SW] Mac OS X	10		**100%**	**75%**	**100%**	
		[SW] CoMmanD (CMD)	10		**100%**	**75%**	**100%**	
		[SW] CoMmanD line (Mac)	10		**100%**	**75%**	**100%**	
		[SW] Terminal	10		**100%**	**75%**	**100%**	

Tabla 2. Impacto para cada dimensión. (Continuación)

A.9	[Re-]encaminamiento de mensajes	[SW] Sistema de Registro y Control Académico (RYCA) V.1	50		**75%**			
		[SW] Sistema de Registro y Control Académico (RYCA) V.2.0	50		**75%**			
		[SW] Página Oficial del ITFIP	50		**75%**			
		[SW] Google Chrome	50		**50%**			
		[SW] Mozilla Firefox	50		**50%**			
		[SW] Safari	50		**50%**			
		[SW] Microsoft Office 2013	50		**50%**			
		[SW] Open Office Linux 2017	50		**50%**			
		[SW] System Center	50		**50%**			
		[SW] Windows Defender	50		**50%**			

Tabla 2. Impacto para cada dimensión. (Continuación)

		[SW] Windows 8	50		**50%**			
		[SW] Windows Server 2009	50		**50%**			
		[SW] Windows Server 2012	50		**50%**			
		[SW] CentOS 5	50		**50%**			
		[SW] Debian 7	50		**75%**			
		[SW] Ubuntu 14	50		**50%**			
		[SW] Mac OS X	50		**50%**			
		[SW] CoMmanD (CMD)	50		**50%**			
		[SW] CoMmanD line (Mac)	50		**50%**			
		[SW] Terminal	50		**75%**			
		[COM] Red telefónica	50		**50%**			
		[COM] Internet Movistar	50		**20%**			

Tabla 2. Impacto para cada dimensión. (Continuación)

		[COM] Red LAN	50		**20%**			
		[COM] Red WIFI	50		**20%**			
		[COM] Red de datos	50		**20%**			
A.10	Alteración de secuencia	[SW] Sistema de Registro y Control Académico (RYCA) V.1	10			**75%**		
		[SW] Sistema de Registro y Control Académico (RYCA) V.2.0	10			**50%**		
		[SW] Página Oficial del ITFIP	10			**75%**		
		[SW] Google Chrome	10			**20%**		
		[SW] Mozilla Firefox	10			**20%**		
		[SW] Safari	10			**20%**		
		[SW] Microsoft Office 2013	10			**20%**		
		[SW] Open Office Linux 2017	10			**50%**		

Tabla 2. Impacto para cada dimensión. (Continuación)

		[SW] System Center	10			**50%**		
		[SW] Windows Defender	10			**20%**		
		[SW] Windows 8	10			**20%**		
		[SW] Windows Server 2009	10			**75%**		
		[SW] Windows Server 2012	10			**75%**		
		[SW] CentOS 5	10			**75%**		
		[SW] Debian 7	10			**75%**		
		[SW] Ubuntu 14	10			**75%**		
		[SW] Mac OS X	10			**75%**		
		[SW] CoMmanD (CMD)	10			**75%**		
		[SW] CoMmanD line (Mac)	10			**75%**		
		[SW] Terminal	10			**75%**		
		[COM] Red telefónica	10			**50%**		

Tabla 2. Impacto para cada dimensión. (Continuación)

		[COM] Internet Movistar	10			**50%**		
		[COM] Red LAN	10			**50%**		
		[COM] Red WIFI	10			**50%**		
		[COM] Red de datos	10			**20%**		
A.11	Acceso no autorizado	[D] De cada pc de la dependencia de sistemas	10		**100%**	**75%**		
		[D] de cada pc de las dependencias de la institución	10		**100%**	**75%**		
		[D] de las configuraciones de los servidores	10		**100%**	**75%**		
		[D] Biométricas para acceso a la sala de servidor	10		**100%**	**100%**		
		[D] De los usuarios que acceden a los servidores	10		**100%**	**100%**		

Tabla 2. Impacto para cada dimensión. (Continuación)

		[D] servidor de copias de seguridad	10		**100%**	**100%**		
		[keys] Usuarios de los Pc de las demás dependencias	10		**100%**	**100%**		
		[keys] Sensor biométrico	10		**100%**	**100%**		
		[keys] Código de confirmación para acceso a la sala de servidor	10		**100%**	**75%**		
		[SW] Sistema de Registro y Control Académico (RYCA) V.1	10		**100%**	**100%**		
		[SW] Sistema de Registro y Control Académico (RYCA) V.2.0	10		**100%**	**100%**		
		[SW] Página Oficial del ITFIP	10		**100%**	**100%**		
		[SW] Google Chrome	10		**20%**	**20%**		

Tabla 2. Impacto para cada dimensión. (Continuación)

		[SW] Mozilla Firefox	10		**20%**	**20%**		
		[SW] Safari	10		**20%**	**20%**		
		[SW] Microsoft Office 2013	10		**20%**	**20%**		
		[SW] Open Office Linux 2017	10		**20%**	**20%**		
		[SW] System Center	10		**100%**	**100%**		
		[SW] Windows Defender	10		**100%**	**100%**		
		[SW] Windows 8	10		**100%**	**100%**		
		[SW] Windows Server 2009	10		**100%**	**100%**		
		[SW] Windows Server 2012	10		**100%**	**75%**		
		[SW] CentOS 5	10		**100%**	**100%**		
		[SW] Debian 7	10		**20%**	**20%**		
		[SW] Ubuntu 14	10		**20%**	**20%**		

Tabla 2. Impacto para cada dimensión. (Continuación)

		[SW] Mac OS X	10		**20%**	**20%**		
		[SW] CoMmanD (CMD)	10		**20%**	**20%**		
		[SW] CoMmanD line (Mac)	10		**20%**	**20%**		
		[SW] Terminal	10		**20%**	**20%**		
		[HW] Servidor DNS y DHCP	10		**100%**	**100%**		
		[HW] Servidor Plataforma RYCA V.2.0	10		**100%**	**100%**		
		[HW] Servidor Plataforma RYCA V.1	10		**100%**	**100%**		
		[HW] Servidor de Base de Datos ITFIP	10		**100%**	**100%**		
		[HW] Servidor Firewall Fortigate	10		**100%**	**75%**		
		[HW] Servidor Contable SIIGO	10		**100%**	**100%**		

Tabla 2. Impacto para cada dimensión. (Continuación)

		[HW] Servidor de Pruebas “Desarrollito”	10		**100%**	**100%**		
		[HW] Servidor de Copias de seguridad de la información del ITFIP	10		**100%**	**100%**		
		[HW] Computador IMAC APPLE (3 Equipos)	10		**100%**	**100%**		
		[HW] Computadores HP all-one Pro (18 Equipos)	10		**100%**	**100%**		
		[HW] Portátil Toshiba (16 equipos)	10		**100%**	**75%**		
		[HW] Tablet negra 9” (1 Equipo)	10		**100%**	**100%**		
		[HW] Computador IMAC APPLE (3 Equipos)	10		**100%**	**100%**		
		[HW] Memoria USB	10		**100%**	**100%**		

Tabla 2. Impacto para cada dimensión. (Continuación)

		[HW] Discos duros	10		**100%**	**100%**		
		[HW] Discos duros externos	10		**100%**	**100%**		
		[HW] SWITCH ALCATEL LUCEN 9553	10		**100%**	**75%**		
		[HW] SWITCH 24 10/100/1000 BASE T C	10		**100%**	**100%**		
		[HW] SWITCH 24/10/100/1000 BASE T4S	10		**100%**	**100%**		
		[HW] SWITCH 24/10/100/1000PWR CORD	10		**100%**	**100%**		
		[HW] SWITCH ALCATEL LUCEN 9561	10		**100%**	**100%**		
		[HW] SWITCH ALCATEL LUCEN 9556	10		**100%**	**100%**		
		[HW] SWITCH ALCATEL LUCEN 9557	10		**100%**	**75%**		

Tabla 2. Impacto para cada dimensión. (Continuación)

		[HW] SWITCH ALCATEL LUCEN 9558	10		**100%**	**100%**		
		[HW] SWITCH ALCATEL LUCEN 9559	10		**100%**	**100%**		
		[HW] SWITCH ALCATEL LUCEN 9543	10		**100%**	**100%**		
		[HW] SWITCH ALCATEL LUCEN 9544	10		**100%**	**100%**		
		[HW] SWITCH ALCATEL LUCEN 9545	10		**100%**	**100%**		
		[HW] SWITCH ALCATEL LUCEN 9548	10		**100%**	**75%**		
		[HW] SWITCH ALCATEL LUCEN 9550	10		**100%**	**100%**		
		[HW] SWITCH ALCATEL LUCEN 9551	10		**100%**	**100%**		

Tabla 2. Impacto para cada dimensión. (Continuación)

		[HW] SWITCH ALCATEL LUCEN 9552	10		**100%**	**100%**		
		[HW] SWITCH ALCATEL LUCEN 9554	10		**100%**	**100%**		
		[HW] SWITCH ALCATEL LUCEN 9555	10		**100%**	**100%**		
		[HW] SWITCH ALCATEL LUCEN 9560	10		**100%**	**75%**		
		[HW] SWITCH LAYER 3 9574	10		**100%**	**100%**		
		[HW] SWITCH LAYER 3 9576	10		**100%**	**100%**		
		[HW] SWITCH LAYER 3 9577	10		**100%**	**100%**		
		[HW] SWITCH LAYER 3 9575	10		**100%**	**100%**		
		[HW] ROUTER CISCO MODELO 1800 4781	10		**100%**	**100%**		
		[COM] Red telefónica	10		**100%**	**75%**		

Tabla 2. Impacto para cada dimensión. (Continuación)

		[COM] Internet Movistar	10		**100%**	**100%**		
		[COM] Red LAN	10		**100%**	**100%**		
		[COM] Red WIFI	10		**100%**	**100%**		
		[COM] Red de datos	10		**100%**	**100%**		
		[MEDIA] DDS 1TB	10		**100%**	**100%**		
		[MEDIA] Materiales físicos	10		**100%**	**75%**		
		[AUX] UPS 10 KVA 9578	10		**100%**	**100%**		
		[AUX] UPS 10 KVA 9579	10		**100%**	**100%**		
		[AUX] UPS 10 KVA 9580	10		**100%**	**75%**		
		[L] Cuarto o recinto (Oficina)	10		**100%**	**100%**		
A.12	Análisis de trafico	[COM] Red telefónica	10		**75%**			
		[COM] Internet Movistar	10		**50%**			
		[COM] Red LAN	10		**50%**			

Tabla 2. Impacto para cada dimensión. (Continuación)

		[COM] Red WIFI	10		**100%**			
		[COM] Red de datos	10		**100%**			
A.14	Interceptación de información (escucha)	[COM] Red telefónica	10		**50%**			
		[COM] Internet Movistar	10		**75%**			
		[COM] Red LAN	10		**75%**			
		[COM] Red WIFI	10		**75%**			
		[COM] Red de datos	10		**75%**			
A.15	Modificación deliberada de la información	[D] De cada pc de la dependencia de sistemas	10			**75%**		
		[D] de cada pc de las dependencias de la institución	10			**75%**		
		[D] de las configuraciones de los servidores	10			**75%**		
		[D] Biométricas para acceso a la sala de servidor	10			**50%**		

Tabla 2. Impacto para cada dimensión. (Continuación)

		[D] De los usuarios que acceden a los servidores	10			**75%**		
		[D] servidor de copias de seguridad	10			**50%**		
		[keys] Usuarios de los Pc de las demás dependencias	10			**75%**		
		[keys] Sensor biométrico	10			**75%**		
		[keys] Código de confirmación para acceso a la sala de servidor	10			**75%**		
		[SW] Sistema de Registro y Control Académico (RYCA) V.1	10			**75%**		
		[SW] Sistema de Registro y Control Académico (RYCA) V.2.0	10			**75%**		

Tabla 2. Impacto para cada dimensión. (Continuación)

		[SW] Página Oficial del ITFIP	10			**50%**		
		[SW] Google Chrome	10			**75%**		
		[SW] Mozilla Firefox	10			**50%**		
		[SW] Safari	10			**75%**		
		[SW] Microsoft Office 2013	10			**75%**		
		[SW] Open Office Linux 2017	10			**75%**		
		[SW] System Center	10			**75%**		
		[SW] Windows Defender	10			**75%**		
		[SW] Windows 8	10			**50%**		
		[SW] Windows Server 2009	10			**75%**		
		[SW] Windows Server 2012	10			**50%**		
		[SW] CentOS 5	10			**75%**		

Tabla 2. Impacto para cada dimensión. (Continuación)

		[SW] Debian 7	10			**75%**		
		[SW] Ubuntu 14	10			**75%**		
		[SW] Mac OS X	10			**75%**		
		[SW] CoMmanD (CMD)	10			**75%**		
		[SW] CoMmanD line (Mac)	10			**50%**		
		[SW] Terminal	10			**75%**		
		[COM] Red telefónica	10			**50%**		
		[COM] Internet Movistar	10			**75%**		
		[COM] Red LAN	10			**75%**		
		[COM] Red WIFI	10			**75%**		
		[COM] Red de datos	10			**75%**		
		[MEDIA] DDS 1TB	10			**75%**		
		[MEDIA] Materiales físicos	10			**50%**		

Tabla 2. Impacto para cada dimensión. (Continuación)

		[L] Cuarto o recinto (Oficina)	10			**75%**		
A.18	Destrucción de información	[D] De cada pc de la dependencia de sistemas	10				**100%**	
		[D] de cada pc de las dependencias de la institución	10				**100%**	
		[D] de las configuraciones de los servidores	10				**100%**	
		[D] Biométricas para acceso a la sala de servidor	10				**100%**	
		[D] De los usuarios que acceden a los servidores	10				**100%**	
		[D] servidor de copias de seguridad	10				**100%**	
		[keys] Usuarios de los Pc de las demás dependencias	10				**100%**	

Tabla 2. Impacto para cada dimensión. (Continuación)

		[keys] Sensor biométrico	10				**100%**	
		[keys] Código de confirmación para acceso a la sala de servidor	10				**100%**	
		[SW] Sistema de Registro y Control Académico (RYCA) V.1	10				**100%**	
		[SW] Sistema de Registro y Control Académico (RYCA) V.2.0	10				**100%**	
		[SW] Página Oficial del ITFIP	10				**100%**	
		[SW] Google Chrome	10				**5%**	
		[SW] Mozilla Firefox	10				**5%**	
		[SW] Safari	10				**5%**	
		[SW] Microsoft Office 2013	10				**100%**	
		[SW] Open Office Linux 2017	10				**100%**	

Tabla 2. Impacto para cada dimensión. (Continuación)

		[SW] System Center	10				**100%**	
		[SW] Windows Defender	10				**100%**	
		[SW] Windows 8	10				**100%**	
		[SW] Windows Server 2009	10				**100%**	
		[SW] Windows Server 2012	10				**100%**	
		[SW] CentOS 5	10				**100%**	
		[SW] Debian 7	10				**100%**	
		[SW] Ubuntu 14	10				**100%**	
		[SW] Mac OS X	10				**100%**	
		[SW] CoMmanD (CMD)	10				**5%**	
		[SW] CoMmanD line (Mac)	10				**5%**	
		[SW] Terminal	10				**5%**	
		[MEDIA] DDS 1TB	10				**100%**	

Tabla 2. Impacto para cada dimensión. (Continuación)

		[MEDIA] Materiales físicos	10				**100%**	
		[L] Cuarto o recinto (Oficina)	10				**100%**	
A.19	Divulgación de información	[D] De cada pc de la dependencia de sistemas	10		**100%**			
		[D] de cada pc de las dependencias de la institución	10		**100%**			
		[D] de las configuraciones de los servidores	10		**100%**			
		[D] Biométricas para acceso a la sala de servidor	10		**100%**			
		[D] De los usuarios que acceden a los servidores	10		**100%**			
		[D] servidor de copias de seguridad	10		**100%**			

Tabla 2. Impacto para cada dimensión. (Continuación)

		[keys] Usuarios de los Pc de las demás dependencias	10		**100%**			
		[keys] Sensor biométrico	10		**100%**			
		[keys] Código de confirmación para acceso a la sala de servidor	10		**100%**			
		[SW] Sistema de Registro y Control Académico (RYCA) V.1	10		**100%**			
		[SW] Sistema de Registro y Control Académico (RYCA) V.2.0	10		**100%**			
		[SW] Página Oficial del ITFIP	10		**100%**			
		[SW] Google Chrome	10		**50%**			
		[SW] Mozilla Firefox	10		**50%**			
		[SW] Safari	10		**50%**			

Tabla 2. Impacto para cada dimensión. (Continuación)

		[SW] Microsoft Office 2013	10		**100%**			
		[SW] Open Office Linux 2017	10		**100%**			
		[SW] System Center	10		**100%**			
		[SW] Windows Defender	10		**100%**			
		[SW] Windows 8	10		**100%**			
		[SW] Windows Server 2009	10		**100%**			
		[SW] Windows Server 2012	10		**100%**			
		[SW] CentOS 5	10		**100%**			
		[SW] Debian 7	10		**100%**			
		[SW] Ubuntu 14	10		**100%**			
		[SW] Mac OS X	10		**100%**			
		[SW] CoMmanD (CMD)	10		**5%**			
		[SW] CoMmanD line (Mac)	10		**5%**			

Tabla 2. Impacto para cada dimensión. (Continuación)

		[SW] Terminal	10		**5%**			
		[COM] Red telefónica	10		**100%**			
		[COM] Internet Movistar	10		**5%**			
		[COM] Red LAN	10		**100%**			
		[COM] Red WIFI	10		**100%**			
		[COM] Red de datos	10		**100%**			
		[MEDIA] DDS 1TB	10		**100%**			
		[MEDIA] Materiales físicos	10		**100%**			
		[L] Cuarto o recinto (Oficina)	10		**50%**			
A.22	Manipulación de programas	[SW] Sistema de Registro y Control Académico (RYCA) V.1	10		**100%**	**100%**	**100%**	
		[SW] Sistema de Registro y Control Académico (RYCA) V.2.0	10		**100%**	**100%**	**100%**	

Tabla 2. Impacto para cada dimensión. (Continuación)

		[SW] Página Oficial del ITFIP	10		**100%**	**100%**	**100%**	
		[SW] Google Chrome	10		**5%**	**5%**	**20%**	
		[SW] Mozilla Firefox	10		**5%**	**5%**	**20%**	
		[SW] Safari	10		**5%**	**5%**	**20%**	
		[SW] Microsoft Office 2013	10		**100%**	**5%**	**75%**	
		[SW] Open Office Linux 2017	10		**100%**	**5%**	**75%**	
		[SW] System Center	10		**5%**	**5%**	**20%**	
		[SW] Windows Defender	10		**5%**	**5%**	**20%**	
		[SW] Windows 8	10		**20%**	**5%**	**20%**	
		[SW] Windows Server 2009	10		**100%**	**100%**	**100%**	
		[SW] Windows Server 2012	10		**100%**	**100%**	**100%**	
		[SW] CentOS 5	10		**100%**	**100%**	**100%**	
		[SW] Debian 7	10		**20%**	**5%**	**20%**	

Tabla 2. Impacto para cada dimensión. (Continuación)

		[SW] Ubuntu 14	10		**20%**	**5%**	**20%**	
		[SW] Mac OS X	10		**100%**	**100%**	**100%**	
		[SW] CoMmanD (CMD)	10		**5%**	**5%**	**5%**	
		[SW] CoMmanD line (Mac)	10		**5%**	**5%**	**5%**	
		[SW] Terminal	10		**5%**	**5%**	**5%**	
A.23	Manipulación de los equipos	[HW] Servidor DNS y DHCP	10		**100%**		**100%**	
		[HW] Servidor Plataforma RYCA V.2.0	10		**100%**		**100%**	
		[HW] Servidor Plataforma RYCA V.1	10		**100%**		**100%**	
		[HW] Servidor de Base de Datos ITFIP	10		**100%**		**100%**	
		[HW] Servidor Firewall Fortigate	10		**100%**		**100%**	
		[HW] Servidor Contable SIIGO	10		**100%**		**100%**	

Tabla 2. Impacto para cada dimensión. (Continuación)

		[HW] Servidor de Pruebas “Desarrollito”	10		**100%**		**100%**	
		[HW] Servidor de Copias de seguridad de la información del ITFIP	10		**100%**		**100%**	
		[HW] Computador IMAC APPLE (3 Equipos)	10		**100%**		**100%**	
		[HW] Computadores HP all-one Pro (18 Equipos)	10		**20%**		**100%**	
		[HW] Portátil Toshiba (16 equipos)	10		**20%**		**100%**	
		[HW] Tablet negra 9” (1 Equipo)	10		**20%**		**100%**	
		[HW] Computador IMAC APPLE (3 Equipos)	10		**100%**		**100%**	
		[HW] Memoria USB	10		**20%**		**20%**	

Tabla 2. Impacto para cada dimensión. (Continuación)

		[HW] Discos duros	10		**100%**		**20%**	
		[HW] Discos duros externos	10		**100%**		**20%**	
		[HW] SWITCH ALCATEL LUCEN 9553	10		**20%**		**100%**	
		[HW] SWITCH 24 10/100/1000 BASE T C	10		**20%**		**100%**	
		[HW] SWITCH 24/10/100/1000 BASE T4S	10		**20%**		**100%**	
		[HW] SWITCH 24/10/100/1000PWR CORD	10		**20%**		**100%**	
		[HW] SWITCH ALCATEL LUCEN 9561	10		**20%**		**100%**	
		[HW] SWITCH ALCATEL LUCEN 9556	10		**20%**		**100%**	
		[HW] SWITCH ALCATEL LUCEN 9557	10		**20%**		**100%**	

Tabla 2. Impacto para cada dimensión. (Continuación)

		[HW] SWITCH ALCATEL LUCEN 9558	10		**20%**		**100%**	
		[HW] SWITCH ALCATEL LUCEN 9559	10		**20%**		**100%**	
		[HW] SWITCH ALCATEL LUCEN 9543	10		**20%**		**100%**	
		[HW] SWITCH ALCATEL LUCEN 9544	10		**20%**		**100%**	
		[HW] SWITCH ALCATEL LUCEN 9545	10		**20%**		**100%**	
		[HW] SWITCH ALCATEL LUCEN 9548	10		**20%**		**100%**	
		[HW] SWITCH ALCATEL LUCEN 9550	10		**20%**		**100%**	
		[HW] SWITCH ALCATEL LUCEN 9551	10		**20%**		**100%**	

Tabla 2. Impacto para cada dimensión. (Continuación)

		[HW] SWITCH ALCATEL LUCEN 9552	10		**20%**		**100%**	
		[HW] SWITCH ALCATEL LUCEN 9554	10		**20%**		**100%**	
		[HW] SWITCH ALCATEL LUCEN 9555	10		**20%**		**100%**	
		[HW] SWITCH ALCATEL LUCEN 9560	10		**20%**		**100%**	
		[HW] SWITCH LAYER 3 9574	10		**20%**		**100%**	
		[HW] SWITCH LAYER 3 9576	10		**20%**		**100%**	
		[HW] SWITCH LAYER 3 9577	10		**20%**		**100%**	
		[HW] SWITCH LAYER 3 9575	10		**20%**		**100%**	
		[HW] ROUTER CISCO MODELO 1800 4781	10		**20%**		**100%**	
		[MEDIA] DDS 1TB	10		**50%**		**50%**	

Tabla 2. Impacto para cada dimensión. (Continuación)

		[MEDIA] Materiales físicos	10		**50%**		**50%**	
		[AUX] UPS 10 KVA 9578	10		**20%**		**20%**	
		[AUX] UPS 10 KVA 9579	10		**20%**		**20%**	
		[AUX] UPS 10 KVA 9580	10		**20%**		**20%**	
A.24	Denegación de servicio	[HW] Servidor DNS y DHCP	50				**100%**	
		[HW] Servidor Plataforma RYCA V.2.0	50				**100%**	
		[HW] Servidor Plataforma RYCA V.1	50				**100%**	
		[HW] Servidor de Base de Datos ITFIP	50				**100%**	
		[HW] Servidor Firewall Fortigate	50				**100%**	
		[HW] Servidor Contable SIIGO	50				**100%**	

Tabla 2. Impacto para cada dimensión. (Continuación)

		[HW] Servidor de Pruebas “Desarrollito”	50				**100%**	
		[HW] Servidor de Copias de seguridad de la información del ITFIP	50				**100%**	
		[HW] Computador IMAC APPLE (3 Equipos)	50				**100%**	
		[HW] Computadores HP all-one Pro (18 Equipos)	50				**50%**	
		[HW] Portátil Toshiba (16 equipos)	50				**50%**	
		[HW] Tablet negra 9” (1 Equipo)	50				**20%**	
		[HW] Computador IMAC APPLE (3 Equipos)	50				**100%**	
		[HW] Memoria USB	50				**50%**	

Tabla 2. Impacto para cada dimensión. (Continuación)

		[HW] Discos duros	50				**50%**	
		[HW] Discos duros externos	50				**50%**	
		[HW] SWITCH ALCATEL LUCEN 9553	50				**50%**	
		[HW] SWITCH 24 10/100/1000 BASE T C	50				**50%**	
		[HW] SWITCH 24/10/100/1000 BASE T4S	50				**50%**	
		[HW] SWITCH 24/10/100/1000PWR CORD	50				**50%**	
		[HW] SWITCH ALCATEL LUCEN 9561	50				**50%**	
		[HW] SWITCH ALCATEL LUCEN 9556	50				**50%**	
		[HW] SWITCH ALCATEL LUCEN 9557	50				**50%**	

Tabla 2. Impacto para cada dimensión. (Continuación)

		[HW] SWITCH ALCATEL LUCEN 9558	50				**50%**	
		[HW] SWITCH ALCATEL LUCEN 9559	50				**50%**	
		[HW] SWITCH ALCATEL LUCEN 9543	50				**50%**	
		[HW] SWITCH ALCATEL LUCEN 9544	50				**50%**	
		[HW] SWITCH ALCATEL LUCEN 9545	50				**50%**	
		[HW] SWITCH ALCATEL LUCEN 9548	50				**50%**	
		[HW] SWITCH ALCATEL LUCEN 9550	50				**50%**	
		[HW] SWITCH ALCATEL LUCEN 9551	50				**50%**	

Tabla 2. Impacto para cada dimensión. (Continuación)

		[HW] SWITCH ALCATEL LUCEN 9552	50				**50%**	
		[HW] SWITCH ALCATEL LUCEN 9554	50				**50%**	
		[HW] SWITCH ALCATEL LUCEN 9555	50				**50%**	
		[HW] SWITCH ALCATEL LUCEN 9560	50				**50%**	
		[HW] SWITCH LAYER 3 9574	50				**50%**	
		[HW] SWITCH LAYER 3 9576	50				**50%**	
		[HW] SWITCH LAYER 3 9577	50				**50%**	
		[HW] SWITCH LAYER 3 9575	50				**50%**	
		[HW] ROUTER CISCO MODELO 1800 4781	50				**50%**	
		[COM] Red telefónica	50				**50%**	

Tabla 2. Impacto para cada dimensión. (Continuación)

		[COM] Internet Movistar	50				**100%**	
		[COM] Red LAN	50				**100%**	
		[COM] Red WIFI	50				**100%**	
		[COM] Red de datos	50				**100%**	
A.25	Robo	[HW] Servidor DNS y DHCP	10		**100%**		**100%**	
		[HW] Servidor Plataforma RYCA V.2.0	10		**100%**		**100%**	
		[HW] Servidor Plataforma RYCA V.1	10		**100%**		**100%**	
		[HW] Servidor de Base de Datos ITFIP	10		**100%**		**100%**	
		[HW] Servidor Firewall Fortigate	10		**100%**		**100%**	
		[HW] Servidor Contable SIIGO	10		**100%**		**100%**	

Tabla 2. Impacto para cada dimensión. (Continuación)

		[HW] Servidor de Pruebas “Desarrollito”	10		**100%**		**100%**	
		[HW] Servidor de Copias de seguridad de la información del ITFIP	10		**100%**		**100%**	
		[HW] Computador IMAC APPLE (3 Equipos)	10		**100%**		**100%**	
		[HW] Computadores HP all-one Pro (18 Equipos)	10		**100%**		**100%**	
		[HW] Portátil Toshiba (16 equipos)	10		**100%**		**100%**	
		[HW] Tablet negra 9” (1 Equipo)	10		**100%**		**100%**	
		[HW] Computador IMAC APPLE (3 Equipos)	10		**100%**		**100%**	
		[HW] Memoria USB	10		**50%**		**100%**	

Tabla 2. Impacto para cada dimensión. (Continuación)

		[HW] Discos duros	10		**50%**		**100%**	
		[HW] Discos duros externos	10		**50%**		**100%**	
		[HW] SWITCH ALCATEL LUCEN 9553	10		**20%**		**100%**	
		[HW] SWITCH 24 10/100/1000 BASE T C	10		**20%**		**100%**	
		[HW] SWITCH 24/10/100/1000 BASE T4S	10		**20%**		**100%**	
		[HW] SWITCH 24/10/100/1000PWR CORD	10		**20%**		**100%**	
		[HW] SWITCH ALCATEL LUCEN 9561	10		**20%**		**100%**	
		[HW] SWITCH ALCATEL LUCEN 9556	10		**20%**		**100%**	
		[HW] SWITCH ALCATEL LUCEN 9557	10		**20%**		**100%**	

Tabla 2. Impacto para cada dimensión. (Continuación)

		[HW] SWITCH ALCATEL LUCEN 9558	10		**20%**		**100%**	
		[HW] SWITCH ALCATEL LUCEN 9559	10		**20%**		**100%**	
		[HW] SWITCH ALCATEL LUCEN 9543	10		**20%**		**100%**	
		[HW] SWITCH ALCATEL LUCEN 9544	10		**20%**		**100%**	
		[HW] SWITCH ALCATEL LUCEN 9545	10		**20%**		**100%**	
		[HW] SWITCH ALCATEL LUCEN 9548	10		**20%**		**100%**	
		[HW] SWITCH ALCATEL LUCEN 9550	10		**20%**		**100%**	
		[HW] SWITCH ALCATEL LUCEN 9551	10		**20%**		**100%**	

Tabla 2. Impacto para cada dimensión. (Continuación)

		[HW] SWITCH ALCATEL LUCEN 9552	10		**20%**		**100%**	
		[HW] SWITCH ALCATEL LUCEN 9554	10		**20%**		**100%**	
		[HW] SWITCH ALCATEL LUCEN 9555	10		**20%**		**100%**	
		[HW] SWITCH ALCATEL LUCEN 9560	10		**20%**		**100%**	
		[HW] SWITCH LAYER 3 9574	10		**20%**		**100%**	
		[HW] SWITCH LAYER 3 9576	10		**20%**		**100%**	
		[HW] SWITCH LAYER 3 9577	10		**20%**		**100%**	
		[HW] SWITCH LAYER 3 9575	10		**20%**		**100%**	
		[HW] ROUTER CISCO MODELO 1800 4781	10		**20%**		**100%**	
		[MEDIA] DDS 1TB	10		**50%**		**100%**	

Tabla 2. Impacto para cada dimensión. (Continuación)

		[MEDIA] Materiales físicos	10		**50%**		**100%**	
		[AUX] UPS 10 KVA 9578	10		**20%**		**100%**	
		[AUX] UPS 10 KVA 9579	10		**20%**		**100%**	
		[AUX] UPS 10 KVA 9580	10		**20%**		**100%**	
A.26	Ataque destructivo	[HW] Servidor DNS y DHCP	10				**100%**	
		[HW] Servidor Plataforma RYCA V.2.0	10				**100%**	
		[HW] Servidor Plataforma RYCA V.1	10				**100%**	
		[HW] Servidor de Base de Datos ITFIP	10				**100%**	
		[HW] Servidor Firewall Fortigate	10				**100%**	
		[HW] Servidor Contable SIIGO	10				**100%**	

Tabla 2. Impacto para cada dimensión. (Continuación)

		[HW] Servidor de Pruebas “Desarrollito”	10				**100%**	
		[HW] Servidor de Copias de seguridad de la información del ITFIP	10				**100%**	
		[HW] Computador IMAC APPLE (3 Equipos)	10				**100%**	
		[HW] Computadores HP all-one Pro (18 Equipos)	10				**100%**	
		[HW] Portátil Toshiba (16 equipos)	10				**100%**	
		[HW] Tablet negra 9” (1 Equipo)	10				**100%**	
		[HW] Computador IMAC APPLE (3 Equipos)	10				**100%**	
		[HW] Memoria USB	10				**20%**	

Tabla 2. Impacto para cada dimensión. (Continuación)

		[HW] Discos duros	10				**50%**	
		[HW] Discos duros externos	10				**50%**	
		[HW] SWITCH ALCATEL LUCEN 9553	10				**20%**	
		[HW] SWITCH 24 10/100/1000 BASE T C	10				**20%**	
		[HW] SWITCH 24/10/100/1000 BASE T4S	10				**20%**	
		[HW] SWITCH 24/10/100/1000PWR CORD	10				**20%**	
		[HW] SWITCH ALCATEL LUCEN 9561	10				**20%**	
		[HW] SWITCH ALCATEL LUCEN 9556	10				**20%**	
		[HW] SWITCH ALCATEL LUCEN 9557	10				**20%**	

Tabla 2. Impacto para cada dimensión. (Continuación)

		[HW] SWITCH ALCATEL LUCEN 9558	10				**20%**	
		[HW] SWITCH ALCATEL LUCEN 9559	10				**20%**	
		[HW] SWITCH ALCATEL LUCEN 9543	10				**20%**	
		[HW] SWITCH ALCATEL LUCEN 9544	10				**20%**	
		[HW] SWITCH ALCATEL LUCEN 9545	10				**20%**	
		[HW] SWITCH ALCATEL LUCEN 9548	10				**20%**	
		[HW] SWITCH ALCATEL LUCEN 9550	10				**20%**	
		[HW] SWITCH ALCATEL LUCEN 9551	10				**20%**	

Tabla 2. Impacto para cada dimensión. (Continuación)

		[HW] SWITCH ALCATEL LUCEN 9552	10				**20%**	
		[HW] SWITCH ALCATEL LUCEN 9554	10				**20%**	
		[HW] SWITCH ALCATEL LUCEN 9555	10				**20%**	
		[HW] SWITCH ALCATEL LUCEN 9560	10				**20%**	
		[HW] SWITCH LAYER 3 9574	10				**20%**	
		[HW] SWITCH LAYER 3 9576	10				**20%**	
		[HW] SWITCH LAYER 3 9577	10				**20%**	
		[HW] SWITCH LAYER 3 9575	10				**20%**	
		[HW] ROUTER CISCO MODELO 1800 4781	10				**20%**	
		[MEDIA] DDS 1TB	10				**50%**	

Tabla 2. Impacto para cada dimensión. (Continuación)

		[MEDIA] Materiales físicos	10				**50%**	
		[AUX] UPS 10 KVA 9578	10				**20%**	
		[AUX] UPS 10 KVA 9579	10				**20%**	
		[AUX] UPS 10 KVA 9580	10				**20%**	
		[L] Cuarto o recinto (Oficina)	10				**100%**	
A.27	Ocupación enemiga	[L] Cuarto o recinto (Oficina)	10		**5%**		**100%**	
A.28	Indisponibilidad del personal	[P] Coordinador de sistemas	10				**100%**	
		[P] Programador	10				**100%**	
		[P] Ingeniero Auxiliar/ Soporte técnico	10				**50%**	
A.29	Extorsión	[P] Coordinador de sistemas	10		**20%**	**100%**	**20%**	
		[P] Programador	10		**20%**	**100%**	**20%**	

Tabla 2. Impacto para cada dimensión. (Continuación)

		[P] Ingeniero Auxiliar/ Soporte técnico	10		**20%**	**100%**	**20%**	
A.30	Ingeniería social (picaresca)	[P] Coordinador de sistemas	10		**20%**	**100%**	**20%**	
		[P] Programador	10		**20%**	**100%**	**20%**	
		[P] Ingeniero Auxiliar/ Soporte técnico	10		**20%**	**100%**	**20%**	

Fuente: Autoría propia.

ANEXO 3

CONTENIDO

LISTA DE TABLAS

1. ESTIMACIÓN DE LAS VULNERABILIDADES QUE PUEDEN AFECTAR A CADA UNO DE LOS ACTIVOS.

Tabla 1. Estimación de la vulnerabilidad activo de cada pc de la dependencia de sistemas

ACTIVO TI	DE CADA PC DE LA DEPENDENCIA DE SISTEMAS
ADMINISTRADOR	PIMIENTO CARDENAS WILSON MAURICIO
TIPO DE ACTIVO	DATOS/INFORMACIÓN

Tipo	ID	Amenaza	Exposición/Vulnerabilidad
ERRORES Y FALLOS NO INTENCIONADOS	**E.1**	Errores de los usuarios	Pérdida total o parcial del tiempo de ejecución de sus actividades, dependiendo de la gravedad del asunto.
	E.2	Errores del administrador	Pérdida total o parcial del tiempo de ejecución de sus actividades, dependiendo de la gravedad del asunto.
	E.15	Alteración accidental de la información	La dependencia cuenta con sistemas de cifrado y verificación (puerto – puerto) para el manejo de la movilidad de la información.
	E.18	Destrucción de información	El departamento de sistemas cuenta con copias de seguridad periódicas
	E.19	Fugas de información	Las personas contratadas están atadas a cláusulas de confidencialidad.
ATAQUES INTENCIONAD	**A.5**	Suplantación de la identidad del usuario	Acceso a personas que no cuenten con los permisos necesarios o con las credenciales necesarias.
	A.6	Abuso de privilegios de acceso	Abuso de cada uno de los derechos otorgados.
	A.11	Acceso no autorizado	Uso ilícito del hardware

Tabla 1. Estimación de la vulnerabilidad activo de cada pc de la dependencia de sistemas. (Continuación)

	A.15	Modificación deliberada de la información	Datos erróneos en el momento de la movilización de la información.
	A.18	Destrucción de información	Perdida de la información.
	A.19	Divulgación de información	Información filtrada abiertamente a personas no correspondientes.

Fuente: Autoría propia

Tabla 2. Estimación de la vulnerabilidad activo de cada pc de las dependencias de la institución

ACTIVO TI		DE CADA PC DE LAS DEPENDENCIAS DE LA INSTITUCIÓN	
ADMINISTRADOR		PIMIENTO CARDENAS WILSON MAURICIO	
TIPO DE ACTIVO		DATOS/INFORMACIÓN	
Tipo	**ID**	**Amenaza**	**Exposición/Vulnerabilidad**
ERRORES Y FALLOS NO INTENCIONADOS	**E.1**	Errores de los usuarios	Pérdida total o parcial del tiempo de ejecución de sus actividades, dependiendo de la gravedad del asunto.
	E.2	Errores del administrador	Pérdida total o parcial del tiempo de ejecución de sus actividades, dependiendo de la gravedad del asunto.
	E.15	Alteración accidental de la información	La dependencia cuenta con sistemas de cifrado y verificación (puerto – puerto) para el manejo de la movilidad de la información.
	E.18	Destrucción de información	El departamento de sistemas cuenta con copias de seguridad periódicas
	E.19	Fugas de información	Las personas contratadas están atadas a cláusulas de confidencialidad.
ATAQUES	**A.5**	Suplantación de la identidad del usuario	Acceso a personas que no cuenten con los permisos necesarios o con las credenciales necesarias.

Tabla 2. Estimación de la vulnerabilidad activo de cada pc de las dependencias de la institución. (Continuación)

	A.6	Abuso de privilegios de acceso	Abuso de cada uno de los derechos otorgados.
	A.11	Acceso no autorizado	Uso ilícito del hardware
	A.15	Modificación deliberada de la información	Datos erróneos en el momento de la movilización de la información.
	A.18	Destrucción de información	Perdida de la información.
	A.19	Divulgación de información	Información filtrada abiertamente a personas no correspondientes.

Fuente: Autoría propia

Tabla 3. Estimación de la vulnerabilidad activo de las configuraciones de los servidores

ACTIVO TI		DE LAS CONFIGURACIONES DE LOS SERVIDORES	
ADMINISTRADOR		PIMIENTO CARDENAS WILSON MAURICIO	
TIPO DE ACTIVO		DATOS/INFORMACIÓN	
Tipo	**ID**	**Amenaza**	**Exposición/Vulnerabilidad**
NO FALLOS Y ERRORES INTENCIONADOS	**E.1**	Errores de los usuarios	Pérdida total o parcial del tiempo de ejecución de sus actividades, dependiendo de la gravedad del asunto.
	E.2	Errores del administrador	Pérdida total o parcial del tiempo de ejecución de sus actividades, dependiendo de la gravedad del asunto.
	E.15	Alteración accidental de la información	La dependencia cuenta con copias de seguridad para los servidores; para así tener respaldo de la información almacén a en ello.
	E.18	Destrucción de información	El departamento de sistemas cuenta con copias de seguridad periódicas

Tabla 3. Estimación de la vulnerabilidad activo de las configuraciones de los servidores. (Continuación)

	E.19	Fugas de información	Las personas contratadas están atadas a cláusulas de confidencialidad.
ATAQUES INTENCIONAD	**A.5**	Suplantación de la identidad del usuario	Acceso a personas que no cuenten con los permisos necesarios o con las credenciales necesarias.
	A.6	Abuso de privilegios de acceso	Abuso de cada uno de los derechos otorgados.
	A.11	Acceso no autorizado	Uso ilícito de los servidores
	A.15	Modificación deliberada de la información	Datos erróneos en el momento de la movilización de la información.
	A.18	Destrucción de información	Perdida de la información en los servidores.
	A.19	Divulgación de información	Información filtrada abiertamente a personas no correspondientes.

Fuente: Autoría propia

Tabla 4. Estimación de la vulnerabilidad activo biométricas para acceso a la sala de servidor

ACTIVO TI		BIOMÉTRICAS PARA ACCESO A LA SALA DE SERVIDOR	
ADMINISTRADOR		PIMIENTO CARDENAS WILSON MAURICIO	
TIPO DE ACTIVO		DATOS/INFORMACIÓN	
Tipo	**ID**	**Amenaza**	**Exposición/Vulnerabilidad**
ERRORES Y FALLOS NO	**E.1**	Errores de los usuarios	Pérdida total o parcial del tiempo de ejecución de sus actividades, dependiendo de la gravedad del asunto.
	E.2	Errores del administrador	Pérdida total o parcial del tiempo de ejecución de sus actividades, dependiendo de la gravedad del asunto.

Tabla 4. Estimación de la vulnerabilidad activo biométricas para acceso a la sala de servidor. (Continuación)

	E.15	Alteración accidental de la información	La dependencia cuenta con sistemas biométricos para el acceso a la sala de servidores.
	E.18	Destrucción de información	El departamento de sistemas cuenta con copias de seguridad periódicas
	E.19	Fugas de información	Las personas contratadas están atadas a cláusulas de confidencialidad.
ATAQUES INTENCIONAD	**A.5**	Suplantación de la identidad del usuario	Acceso a personas que no cuenten con los permisos necesarios o con las credenciales necesarias.
	A.6	Abuso de privilegios de acceso	Abuso de cada uno de los derechos otorgados.
	A.11	Acceso no autorizado	Uso ilícito del sistema biométrico para el acceso a la sala de servidores.
	A.15	Modificación deliberada de la información	Datos erróneos en el momento de la movilización de la información.
	A.18	Destrucción de información	Perdida de la información.
	A.19	Divulgación de información	Información filtrada abiertamente a personas no correspondientes.

Fuente: Autoría propia

Tabla 5. Estimación de la vulnerabilidad activo de los usuarios que acceden a los servidores

ACTIVO TI		DE LOS USUARIOS QUE ACCEDEN A LOS SERVIDORES	
ADMINISTRADOR		PIMIENTO CARDENAS WILSON MAURICIO	
TIPO DE ACTIVO		DATOS/INFORMACIÓN	
Tipo	**ID**	**Amenaza**	**Exposición/Vulnerabilidad**

Tabla 5. Estimación de la vulnerabilidad activo de los usuarios que acceden a los servidores. (Continuación)

ERRORES Y FALLOS NO INTENCIONADOS	**E.1**	Errores de los usuarios	Pérdida total o parcial del tiempo de ejecución de sus actividades, dependiendo de la gravedad del asunto.
	E.2	Errores del administrador	Pérdida total o parcial del tiempo de ejecución de sus actividades, dependiendo de la gravedad del asunto.
	E.15	Alteración accidental de la información	La dependencia cuenta con sistemas de cifrado y verificación (puerto – puerto) para el manejo de la movilidad de la información.
	E.18	Destrucción de información	El departamento de sistemas cuenta con copias de seguridad periódicas
	E.19	Fugas de información	Las personas contratadas están atadas a cláusulas de confidencialidad.
ATAQUES INTENCIONAD	**A.5**	Suplantación de la identidad del usuario	Acceso a personas que no cuenten con los permisos necesarios o con las credenciales necesarias.
	A.6	Abuso de privilegios de acceso	Abuso de cada uno de los derechos otorgados.
	A.11	Acceso no autorizado	Uso ilícito del sistema biométrico para el acceso a la sala de servidores.
	A.15	Modificación deliberada de la información	Datos erróneos en el momento de la movilización de la información.
	A.18	Destrucción de información	Perdida de la información.
	A.19	Divulgación de información	Información filtrada abiertamente a personas no correspondientes.

Fuente: Autoría propia

Tabla 6. Estimación de la vulnerabilidad activo servidor de copias de seguridad

ACTIVO TI		SERVIDOR DE COPIAS DE SEGURIDAD	
ADMINISTRADOR		PIMIENTO CARDENAS WILSON MAURICIO	
TIPO DE ACTIVO		DATOS/INFORMACIÓN	
Tipo	**ID**	**Amenaza**	**Exposición/Vulnerabilidad**
ERRORES Y FALLOS NO INTENCIONADOS	**E.1**	Errores de los usuarios	Pérdida total o parcial del tiempo de ejecución de sus actividades, dependiendo de la gravedad del asunto.
	E.2	Errores del administrador	Pérdida total o parcial del tiempo de ejecución de sus actividades, dependiendo de la gravedad del asunto.
	E.15	Alteración accidental de la información	La dependencia cuenta con sistemas de cifrado y verificación (puerto – puerto) para el manejo de la movilidad de la información.
	E.18	Destrucción de información	El departamento de sistemas cuenta con copias de seguridad periódicas
	E.19	Fugas de información	Las personas contratadas están atadas a cláusulas de confidencialidad.
ATAQUES INTENCIONAD	**A.5**	Suplantación de la identidad del usuario	Acceso a personas que no cuenten con los permisos necesarios o con las credenciales necesarias.
	A.6	Abuso de privilegios de acceso	Abuso de cada uno de los derechos otorgados.
	A.11	Acceso no autorizado	Uso ilícito del sistema biométrico para el acceso a la sala de servidores.
	A.15	Modificación deliberada de la información	Datos erróneos en el momento de la movilización de la información.
	A.18	Destrucción de información	Perdida de la información.

Tabla 6. Estimación de la vulnerabilidad activo servidor de copias de seguridad (Continuación)

	A.19	Divulgación de información	Información filtrada abiertamente a personas no correspondientes.

Fuente: Autoría propia

Tabla 7. Estimación de la vulnerabilidad activo usuarios de los pc de las demás dependencias

ACTIVO TI		USUARIOS DE LOS PC DE LAS DEMÁS DEPENDENCIAS	
ADMINISTRADOR		PIMIENTO CARDENAS WILSON MAURICIO	
TIPO DE ACTIVO		CLAVES CRIPTOGRÁFICAS	
Tipo	**ID**	**Amenaza**	**Exposición/Vulnerabilidad**
ERRORES Y FALLOS NO INTENCIONADOS	**E.1**	Errores de los usuarios	Pérdida total o parcial del tiempo de ejecución de sus actividades, dependiendo de la gravedad del asunto.
	E.2	Errores del administrador	Pérdida total o parcial del tiempo de ejecución de sus actividades, dependiendo de la gravedad del asunto.
	E.15	Alteración accidental de la información	La dependencia cuenta con sistemas de cifrado y verificación (puerto – puerto) para el manejo de la movilidad de la información.
	E.18	Destrucción de información	El departamento de sistemas cuenta con copias de seguridad periódicas
	E.19	Fugas de información	Las personas contratadas están atadas a cláusulas de confidencialidad.
ATAQUES INTENCIONAD	**A.5**	Suplantación de la identidad del usuario	Acceso a personas que no cuenten con los permisos necesarios o con las credenciales necesarias.
	A.6	Abuso de privilegios de acceso	Abuso de cada uno de los derechos otorgados.
	A.11	Acceso no autorizado	Uso ilícito de pc a usuarios externos de las demás dependencias

Tabla 7. Estimación de la vulnerabilidad activo usuarios de los pc de las demás dependencias. (Continuación)

	A.15	Modificación deliberada de la información	Datos erróneos en el momento de la movilización de la información.
	A.18	Destrucción de información	Perdida de la información.
	A.19	Divulgación de información	Información filtrada abiertamente a personas no correspondientes.

Fuente: Autoría propia

Tabla 8. Estimación de la vulnerabilidad activo sensor biométrico

ACTIVO TI		SENSOR BIOMÉTRICO	
ADMINISTRADOR		PIMIENTO CARDENAS WILSON MAURICIO	
TIPO DE ACTIVO		CLAVES CRIPTOGRÁFICAS	
Tipo	**ID**	**Amenaza**	**Exposición/Vulnerabilidad**
ERRORES Y FALLOS NO INTENCIONADOS	**E.1**	Errores de los usuarios	Pérdida total o parcial del tiempo de ejecución de sus actividades, dependiendo de la gravedad del asunto.
	E.2	Errores del administrador	Pérdida total o parcial del tiempo de ejecución de sus actividades, dependiendo de la gravedad del asunto.
	E.15	Alteración accidental de la información	La dependencia cuenta con sistemas de cifrado y verificación (puerto – puerto) para el manejo de la movilidad de la información.
	E.18	Destrucción de información	El departamento de sistemas cuenta con copias de seguridad periódicas
	E.19	Fugas de información	Las personas contratadas están atadas a cláusulas de confidencialidad.
ATAQUES	**A.5**	Suplantación de la identidad del usuario	Acceso a personas que no cuenten con los permisos necesarios o con las credenciales necesarias.

Tabla 8. Estimación de la vulnerabilidad activo sensor biométrico. (Continuación)

	A.6	Abuso de privilegios de acceso	Abuso de cada uno de los derechos otorgados.
	A.11	Acceso no autorizado	Uso ilícito del sistema biométrico para el acceso a la sala de servidores.
	A.15	Modificación deliberada de la información	Datos erróneos en el momento de la movilización de la información.
	A.18	Destrucción de información	Perdida de la información.
	A.19	Divulgación de información	Información filtrada abiertamente a personas no correspondientes.

Fuente: Autoría propia

Tabla 9. Estimación de la vulnerabilidad activo código de confirmación para acceso a la sala de servidor

ACTIVO TI		CÓDIGO DE CONFIRMACIÓN PARA ACCESO A LA SALA DE SERVIDOR	
ADMINISTRADOR		PIMIENTO CARDENAS WILSON MAURICIO	
TIPO DE ACTIVO		CLAVES CRIPTOGRÁFICAS	
Tipo	**ID**	**Amenaza**	**Exposición/Vulnerabilidad**
NO FALLOS Y ERRORES INTENCIONADOS	**E.1**	Errores de los usuarios	Pérdida total o parcial del tiempo de ejecución de sus actividades, dependiendo de la gravedad del asunto.
	E.2	Errores del administrador	Pérdida total o parcial del tiempo de ejecución de sus actividades, dependiendo de la gravedad del asunto.
	E.15	Alteración accidental de la información	La dependencia cuenta con sistemas de cifrado y verificación (puerto – puerto) para el manejo de la movilidad de la información.
	E.18	Destrucción de información	El departamento de sistemas cuenta con copias de seguridad periódicas

Tabla 9. Estimación de la vulnerabilidad activo código confirmación para acceso sala de servidor. (Continuación)

	E.19	Fugas de información	Las personas contratadas están atadas a cláusulas de confidencialidad.
ATAQUES INTENCIONAD	**A.5**	Suplantación de la identidad del usuario	Acceso a personas que no cuenten con los permisos necesarios o con las credenciales necesarias.
	A.6	Abuso de privilegios de acceso	Abuso de cada uno de los derechos otorgados.
	A.11	Acceso no autorizado	Uso ilícito del código de confirmación para acceso a la sala de servidor
	A.15	Modificación deliberada de la información	Datos erróneos en el momento de la movilización de la información.
	A.18	Destrucción de información	Perdida de la información.
	A.19	Divulgación de información	Información filtrada abiertamente a personas no correspondientes.

Fuente: Autoría propia

Tabla 10. Estimación de la vulnerabilidad activo sistema de registro y control académico (RYCA) V.1

ACTIVO TI	SISTEMA DE REGISTRO Y CONTROL ACADÉMICO (RYCA) V.1		
ADMINISTRADOR	PIMIENTO CARDENAS WILSON MAURICIO		
TIPO DE ACTIVO	SOFTWARE		
Tipo	**ID**	**Amenaza**	**Exposición/Vulnerabilidad**
DE ORIGEN	**I.5**	Avería de origen físico o lógico	La manipulación por parte de cada uno de los componentes encontrados en la dependencia, como también por defectos de los componentes desde fabrica
ERRORES Y	**E.1**	Errores de los usuarios	Pérdida total o parcial del tiempo de ejecución de sus actividades, dependiendo de la gravedad del asunto.

Tabla 10. Estimación de la vulnerabilidad activo sistema de reg y control académico (RYCA) V.1. (Continuación)

	E.2	Errores del administrador	Pérdida total o parcial del tiempo de ejecución de sus actividades, dependiendo de la gravedad del asunto.
	E.8	Difusión de software dañino	La dependencia cuenta con antivirus capaces de controlar software malicioso
	E.9	Errores de [re-] encaminamiento	La dependencia cuenta con sistemas de cifrado y verificación (puerto – puerto) para el manejo de la movilidad de la información.
	E.10	Errores de secuencia	La dependencia cuenta con sistemas de cifrado y verificación (puerto – puerto) para el manejo de la movilidad de la información.
	E.15	Alteración accidental de la información	La dependencia cuenta con sistemas de cifrado y verificación (puerto – puerto) para el manejo de la movilidad de la información.
	E.18	Destrucción de información	El departamento de sistemas cuenta con copias de seguridad periódicas
	E.19	Fugas de información	Las personas contratadas están atadas a cláusulas de confidencialidad.
	E.20	Vulnerabilidades de los programas (software)	La dependencia cuenta con programas licenciados para mejorar la seguridad de las aplicaciones instaladas en los computadores de esta.
	E.21	Errores de mantenimiento / actualización de programas (software)	Falla de funcionamiento del software.

Tabla 10. Estimación de la vulnerabilidad activo sistema de reg y control académico (RYCA) V.1. (Continuación)

ATAQUES INTENCIONAD	**A.5**	Suplantación de la identidad del usuario	Acceso a personas que no cuenten con los permisos necesarios o con las credenciales necesarias.
	A.6	Abuso de privilegios de acceso	Abuso de cada uno de los derechos otorgados.
	A.7	Uso no previsto	Implementación de recursos (económicos y de tiempo) en actividades no relacionadas.
	A.8	Difusión de software dañino	Afectación en los sistemas de información y los procesos que ello conlleva.
	A.9	[Re-]encaminamiento de mensajes	La dependencia cuenta con sistemas de cifrado y verificación (puerto – puerto) para el manejo de la movilidad de la información.
	A.10	Alteración de secuencia	Alteración de datos.
	A.11	Acceso no autorizado	Uso ilícito del sistema de registro y control académico (RYCA) V.1
	A.15	Modificación deliberada de la información	Datos erróneos en el momento de la movilización de la información.
	A.18	Destrucción de información	Perdida de la información.
	A.19	Divulgación de información	Información filtrada abiertamente a personas no correspondientes.
	A.22	Manipulación de programas	Alteración del funcionamiento de cada uno de los programas de la dependencia.

Fuente: Autoría propia

Tabla 11. Estimación de la vulnerabilidad activo sistema de registro y control académico (RYCA) V.2.0

ACTIVO TI		SISTEMA DE REGISTRO Y CONTROL ACADÉMICO (RYCA) V.2.0	
ADMINISTRADOR		PIMIENTO CARDENAS WILSON MAURICIO	
TIPO DE ACTIVO		SOFTWARE	
Tipo	**ID**	**Amenaza**	**Exposición/Vulnerabilidad**
DE ORIGEN	**I.5**	Avería de origen físico o lógico	La manipulación por parte de cada uno de los componentes encontrados en la dependencia, como también por defectos de los componentes desde fabrica
ERRORES Y FALLOS NO INTENCIONADOS	**E.1**	Errores de los usuarios	Pérdida total o parcial del tiempo de ejecución de sus actividades, dependiendo de la gravedad del asunto.
	E.2	Errores del administrador	Pérdida total o parcial del tiempo de ejecución de sus actividades, dependiendo de la gravedad del asunto.
	E.8	Difusión de software dañino	La dependencia cuenta con antivirus capaces de controlar software malicioso
	E.9	Errores de [re-] encaminamiento	La dependencia cuenta con sistemas de cifrado y verificación (puerto – puerto) para el manejo de la movilidad de la información.
	E.10	Errores de secuencia	La dependencia cuenta con sistemas de cifrado y verificación (puerto – puerto) para el manejo de la movilidad de la información.
	E.15	Alteración accidental de la información	La dependencia cuenta con sistemas de cifrado y verificación (puerto – puerto) para el manejo de la movilidad de la información.
	E.18	Destrucción de información	El departamento de sistemas cuenta con copias de seguridad periódicas

Tabla 11. Estimación de la vulnerabilidad activo sistema de reg. Y ctrl. Académico (RYCA) V.2.0 (Continuación)

	E.19	Fugas de información	Las personas contratadas están atadas a cláusulas de confidencialidad.
	E.20	Vulnerabilidades de los programas (software)	La dependencia cuenta con programas licenciados para mejorar la seguridad de las aplicaciones instaladas en los computadores de esta.
	E.21	Errores de mantenimiento / actualización de programas (software)	Falla de funcionamiento del software.
ATAQUES INTENCIONAD	**A.5**	Suplantación de la identidad del usuario	Acceso a personas que no cuenten con los permisos necesarios o con las credenciales necesarias.
	A.6	Abuso de privilegios de acceso	Abuso de cada uno de los derechos otorgados.
	A.7	Uso no previsto	Implementación de recursos (económicos y de tiempo) en actividades no relacionadas.
	A.8	Difusión de software dañino	Afectación en los sistemas de información y los procesos que ello conlleva.
	A.9	[Re-]encaminamiento de mensajes	La dependencia cuenta con sistemas de cifrado y verificación (puerto – puerto) para el manejo de la movilidad de la información.
	A.10	Alteración de secuencia	Alteración de datos.
	A.11	Acceso no autorizado	Uso ilícito del sistema de registro y control académico (RYCA) V.2.0.

Tabla 11. Estimación de la vulnerabilidad activo sistema de reg. Y ctrl. Académico (RYCA) V.2.0 (Continuación)

	A.15	Modificación deliberada de la información	Datos erróneos en el momento de la movilización de la información.
	A.18	Destrucción de información	Perdida de la información.
	A.19	Divulgación de información	Información filtrada abiertamente a personas no correspondientes.
	A.22	Manipulación de programas	Alteración del funcionamiento de cada uno de los programas de la dependencia.

Fuente: Autoría propia

Tabla 12. Estimación de la vulnerabilidad activo página oficial del ITFIP

ACTIVO TI	PÁGINA OFICIAL DEL ITFIP		
ADMINISTRADOR	PIMIENTO CARDENAS WILSON MAURICIO		
TIPO DE ACTIVO	SOFTWARE		
Tipo	**ID**	**Amenaza**	**Exposición/Vulnerabilidad**
DE ORIGEN	**I.5**	Avería de origen físico o lógico	La manipulación por parte de cada uno de los componentes encontrados en la dependencia, como también por defectos de los componentes desde fabrica
NO FALLOS Y INTENCIONADOS ERRORES	**E.1**	Errores de los usuarios	Pérdida total o parcial del tiempo de ejecución de sus actividades, dependiendo de la gravedad del asunto.
	E.2	Errores del administrador	Pérdida total o parcial del tiempo de ejecución de sus actividades, dependiendo de la gravedad del asunto.
	E.8	Difusión de software dañino	La dependencia cuenta con antivirus capaces de controlar software malicioso
	E.9	Errores de [re-] encaminamiento	La dependencia cuenta con sistemas de cifrado y verificación (puerto – puerto) para el manejo de la movilidad de la información.

Tabla 12. Estimación de la vulnerabilidad activo página oficial del ITFIP. (Continuación)

	E.10	Errores de secuencia	La dependencia cuenta con sistemas de cifrado y verificación (puerto – puerto) para el manejo de la movilidad de la información.
	E.15	Alteración accidental de la información	La dependencia cuenta con sistemas de cifrado y verificación (puerto – puerto) para el manejo de la movilidad de la información.
	E.18	Destrucción de información	El departamento de sistemas cuenta con copias de seguridad periódicas
	E.19	Fugas de información	Las personas contratadas están atadas a cláusulas de confidencialidad.
	E.20	Vulnerabilidades de los programas (software)	La dependencia cuenta con programas licenciados para mejorar la seguridad de las aplicaciones instaladas en los computadores de esta.
	E.21	Errores de mantenimiento / actualización de programas (software)	Falla de funcionamiento del software.
ATAQUES INTENCIONAD	**A.5**	Suplantación de la identidad del usuario	Acceso a personas que no cuenten con los permisos necesarios o con las credenciales necesarias.
	A.6	Abuso de privilegios de acceso	Abuso de cada uno de los derechos otorgados.
	A.7	Uso no previsto	Implementación de recursos (económicos y de tiempo) en actividades no relacionadas.
	A.8	Difusión de software dañino	Afectación en los sistemas de información y los procesos que ello conlleva.

Tabla 12. Estimación de la vulnerabilidad activo página oficial del ITFIP. (Continuación)

	A.9	[Re-]encaminamiento de mensajes	La dependencia cuenta con sistemas de cifrado y verificación (puerto – puerto) para el manejo de la movilidad de la información.
	A.10	Alteración de secuencia	Alteración de datos.
	A.11	Acceso no autorizado	Uso ilícito de la página oficial del ITFIP.
	A.15	Modificación deliberada de la información	Datos erróneos en el momento de la movilización de la información.
	A.18	Destrucción de información	Perdida de la información.
	A.19	Divulgación de información	Información filtrada abiertamente a personas no correspondientes.
	A.22	Manipulación de programas	Alteración del funcionamiento de cada uno de los programas de la dependencia.

Fuente: Autoría propia

Tabla 13. Estimación de la vulnerabilidad activo Google Chrome

ACTIVO TI	GOOGLE CHROME		
ADMINISTRADOR	PIMIENTO CARDENAS WILSON MAURICIO		
TIPO DE ACTIVO	SOFTWARE		
Tipo	**ID**	**Amenaza**	**Exposición/Vulnerabilidad**
DE ORIGEN INDUSTRIAL	**I.5**	Avería de origen físico o lógico	La manipulación por parte de cada uno de los componentes encontrados en la dependencia, como también por defectos de los componentes desde fabrica
ERRORES Y FALLO	**E.1**	Errores de los usuarios	Pérdida total o parcial del tiempo de ejecución de sus actividades, dependiendo de la gravedad del asunto.

Tabla 13. Estimación de la vulnerabilidad activo Google Chrome. (Continuación)

	E.2	Errores del administrador	Pérdida total o parcial del tiempo de ejecución de sus actividades, dependiendo de la gravedad del asunto.
	E.8	Difusión de software dañino	La dependencia cuenta con antivirus capaces de controlar software malicioso
	E.9	Errores de [re-] encaminamiento	La dependencia cuenta con sistemas de cifrado y verificación (puerto – puerto) para el manejo de la movilidad de la información.
	E.10	Errores de secuencia	La dependencia cuenta con sistemas de cifrado y verificación (puerto – puerto) para el manejo de la movilidad de la información.
	E.15	Alteración accidental de la información	La dependencia cuenta con sistemas de cifrado y verificación (puerto – puerto) para el manejo de la movilidad de la información.
	E.18	Destrucción de información	El departamento de sistemas cuenta con copias de seguridad periódicas
	E.19	Fugas de información	Las personas contratadas están atadas a cláusulas de confidencialidad.
	E.20	Vulnerabilidades de los programas (software)	La dependencia cuenta con programas licenciados para mejorar la seguridad de las aplicaciones instaladas en los computadores de esta.
	E.21	Errores de mantenimiento / actualización de programas (software)	Falla de funcionamiento del software.

Tabla 13. Estimación de la vulnerabilidad activo Google Chrome. (Continuación)

ATAQUES INTENCIONAD	**A.5**	Suplantación de la identidad del usuario	Acceso a personas que no cuenten con los permisos necesarios o con las credenciales necesarias.
	A.6	Abuso de privilegios de acceso	Abuso de cada uno de los derechos otorgados.
	A.7	Uso no previsto	Implementación de recursos (económicos y de tiempo) en actividades no relacionadas.
	A.8	Difusión de software dañino	Afectación en los sistemas de información y los procesos que ello conlleva.
	A.9	[Re-]encaminamiento de mensajes	La dependencia cuenta con sistemas de cifrado y verificación (puerto – puerto) para el manejo de la movilidad de la información.
	A.10	Alteración de secuencia	Alteración de datos.
	A.11	Acceso no autorizado	Uso ilícito del software Google Chrome
	A.15	Modificación deliberada de la información	Datos erróneos en el momento de la movilización de la información.
	A.18	Destrucción de información	Perdida de la información.
	A.19	Divulgación de información	Información filtrada abiertamente a personas no correspondientes.
	A.22	Manipulación de programas	Alteración del funcionamiento de cada uno de los programas de la dependencia.

Fuente: Autoría propia

Tabla 14. Estimación de la vulnerabilidad activo Mozilla Firefox

ACTIVO TI		MOZILLA FIREFOX	
ADMINISTRADOR		PIMIENTO CARDENAS WILSON MAURICIO	
TIPO DE ACTIVO		SOFTWARE	
Tipo	**ID**	**Amenaza**	**Exposición/Vulnerabilidad**
DE ORIGEN INDUSTRI	**I.5**	Avería de origen físico o lógico	La manipulación por parte de cada uno de los componentes encontrados en la dependencia, como también por defectos de los componentes desde fabrica
ERRORES Y FALLOS NO INTENCIONADOS	**E.1**	Errores de los usuarios	Pérdida total o parcial del tiempo de ejecución de sus actividades, dependiendo de la gravedad del asunto.
	E.2	Errores del administrador	Pérdida total o parcial del tiempo de ejecución de sus actividades, dependiendo de la gravedad del asunto.
	E.8	Difusión de software dañino	La dependencia cuenta con antivirus capaces de controlar software malicioso
	E.9	Errores de [re-] encaminamiento	La dependencia cuenta con sistemas de cifrado y verificación (puerto – puerto) para el manejo de la movilidad de la información.
	E.10	Errores de secuencia	La dependencia cuenta con sistemas de cifrado y verificación (puerto – puerto) para el manejo de la movilidad de la información.
	E.15	Alteración accidental de la información	La dependencia cuenta con sistemas de cifrado y verificación (puerto – puerto) para el manejo de la movilidad de la información.
	E.18	Destrucción de información	El departamento de sistemas cuenta con copias de seguridad periódicas
	E.19	Fugas de información	Las personas contratadas están atadas a cláusulas de confidencialidad.

Tabla 14. Estimación de la vulnerabilidad activo Mozilla Firefox. (Continuación)

	E.20	Vulnerabilidades de los programas (software)	La dependencia cuenta con programas licenciados para mejorar la seguridad de las aplicaciones instaladas en los computadores de esta.
	E.21	Errores de mantenimiento / actualización de programas (software)	Falla de funcionamiento del software.
ATAQUES INTENCIONAD	**A.5**	Suplantación de la identidad del usuario	Acceso a personas que no cuenten con los permisos necesarios o con las credenciales necesarias.
	A.6	Abuso de privilegios de acceso	Abuso de cada uno de los derechos otorgados.
	A.7	Uso no previsto	Implementación de recursos (económicos y de tiempo) en actividades no relacionadas.
	A.8	Difusión de software dañino	Afectación en los sistemas de información y los procesos que ello conlleva.
	A.9	[Re-]encaminamiento de mensajes	La dependencia cuenta con sistemas de cifrado y verificación (puerto – puerto) para el manejo de la movilidad de la información.
	A.10	Alteración de secuencia	Alteración de datos.
	A.11	Acceso no autorizado	Uso ilícito del software Mozilla Firefox
	A.15	Modificación deliberada de la información	Datos erróneos en el momento de la movilización de la información.

Tabla 14. Estimación de la vulnerabilidad activo Mozilla Firefox. (Continuación)

	A.18	Destrucción de información	Perdida de la información.
	A.19	Divulgación de información	Información filtrada abiertamente a personas no correspondientes.
	A.22	Manipulación de programas	Alteración del funcionamiento de cada uno de los programas de la dependencia.

Fuente: Autoría propia

Tabla 15. Estimación de la vulnerabilidad activo safari

ACTIVO TI		SAFARI	
ADMINISTRADOR		PIMIENTO CARDENAS WILSON MAURICIO	
TIPO DE ACTIVO		SOFTWARE	
Tipo	**ID**	**Amenaza**	**Exposición/Vulnerabilidad**
DE ORIGEN INDUSTRI	**I.5**	Avería de origen físico o lógico	La manipulación por parte de cada uno de los componentes encontrados en la dependencia, como también por defectos de los componentes desde fabrica
ERRORES Y FALLOS NO INTENCIONADOS	**E.1**	Errores de los usuarios	Pérdida total o parcial del tiempo de ejecución de sus actividades, dependiendo de la gravedad del asunto.
	E.2	Errores del administrador	Pérdida total o parcial del tiempo de ejecución de sus actividades, dependiendo de la gravedad del asunto.
	E.8	Difusión de software dañino	La dependencia cuenta con antivirus capaces de controlar software malicioso
	E.9	Errores de [re-] encaminamiento	La dependencia cuenta con sistemas de cifrado y verificación (puerto – puerto) para el manejo de la movilidad de la información.
	E.10	Errores de secuencia	La dependencia cuenta con sistemas de cifrado y verificación (puerto – puerto) para el manejo de la movilidad de la información.

Tabla 15. Estimación de la vulnerabilidad activo safari. (Continuación)

	E.15	Alteración accidental de la información	La dependencia cuenta con sistemas de cifrado y verificación (puerto – puerto) para el manejo de la movilidad de la información.
	E.18	Destrucción de información	El departamento de sistemas cuenta con copias de seguridad periódicas
	E.19	Fugas de información	Las personas contratadas están atadas a cláusulas de confidencialidad.
	E.20	Vulnerabilidades de los programas (software)	La dependencia cuenta con programas licenciados para mejorar la seguridad de las aplicaciones instaladas en los computadores de esta.
	E.21	Errores de mantenimiento / actualización de programas (software)	Falla de funcionamiento del software.
ATAQUES INTENCIONAD	**A.5**	Suplantación de la identidad del usuario	Acceso a personas que no cuenten con los permisos necesarios o con las credenciales necesarias.
	A.6	Abuso de privilegios de acceso	Abuso de cada uno de los derechos otorgados.
	A.7	Uso no previsto	Implementación de recursos (económicos y de tiempo) en actividades no relacionadas.
	A.8	Difusión de software dañino	Afectación en los sistemas de información y los procesos que ello conlleva.
	A.9	[Re-]encaminamiento de mensajes	La dependencia cuenta con sistemas de cifrado y verificación (puerto – puerto) para el manejo de la movilidad de la información.

Tabla 15. Estimación de la vulnerabilidad activo safari. (Continuación)

	A.10	Alteración de secuencia	Alteración de datos.
	A.11	Acceso no autorizado	Uso ilícito del software safari
	A.15	Modificación deliberada de la información	Datos erróneos en el momento de la movilización de la información.
	A.18	Destrucción de información	Perdida de la información.
	A.19	Divulgación de información	Información filtrada abiertamente a personas no correspondientes.
	A.22	Manipulación de programas	Alteración del funcionamiento de cada uno de los programas de la dependencia.

Fuente: Autoría propia

Tabla 16. Estimación de la vulnerabilidad activo Microsoft office 2013

ACTIVO TI		MICROSOFT OFFICE 2013	
ADMINISTRADOR		PIMIENTO CARDENAS WILSON MAURICIO	
TIPO DE ACTIVO		SOFTWARE	
Tipo	**ID**	**Amenaza**	**Exposición/Vulnerabilidad**
DE ORIGEN INDUSTRI	**I.5**	Avería de origen físico o lógico	La manipulación por parte de cada uno de los componentes encontrados en la dependencia, como también por defectos de los componentes desde fabrica
ERRORES Y FALLOS NO INTENCIONADOS	**E.1**	Errores de los usuarios	Pérdida total o parcial del tiempo de ejecución de sus actividades, dependiendo de la gravedad del asunto.
	E.2	Errores del administrador	Pérdida total o parcial del tiempo de ejecución de sus actividades, dependiendo de la gravedad del asunto.
	E.8	Difusión de software dañino	La dependencia cuenta con antivirus capaces de controlar software malicioso

Tabla 16. Estimación de la vulnerabilidad activo Microsoft office 2013. (Continuación)

	E.9	Errores de [re-] encaminamiento	La dependencia cuenta con sistemas de cifrado y verificación (puerto – puerto) para el manejo de la movilidad de la información.
	E.10	Errores de secuencia	La dependencia cuenta con sistemas de cifrado y verificación (puerto – puerto) para el manejo de la movilidad de la información.
	E.15	Alteración accidental de la información	La dependencia cuenta con sistemas de cifrado y verificación (puerto – puerto) para el manejo de la movilidad de la información.
	E.18	Destrucción de información	El departamento de sistemas cuenta con copias de seguridad periódicas
	E.19	Fugas de información	Las personas contratadas están atadas a cláusulas de confidencialidad.
	E.20	Vulnerabilidades de los programas (software)	La dependencia cuenta con programas licenciados para mejorar la seguridad de las aplicaciones instaladas en los computadores de esta.
	E.21	Errores de mantenimiento / actualización de programas (software)	Falla de funcionamiento del software.
ATAQUES INTENCIONAD	**A.5**	Suplantación de la identidad del usuario	Acceso a personas que no cuenten con los permisos necesarios o con las credenciales necesarias.
	A.6	Abuso de privilegios de acceso	Abuso de cada uno de los derechos otorgados.

Tabla 16. Estimación de la vulnerabilidad activo Microsoft office 2013. (Continuación)

	A.7	Uso no previsto	Implementación de recursos (económicos y de tiempo) en actividades no relacionadas.
	A.8	Difusión de software dañino	Afectación en los sistemas de información y los procesos que ello conlleva.
	A.9	[Re-]encaminamiento de mensajes	La dependencia cuenta con sistemas de cifrado y verificación (puerto – puerto) para el manejo de la movilidad de la información.
	A.10	Alteración de secuencia	Alteración de datos.
	A.11	Acceso no autorizado	Uso ilícito del software Microsoft office 2013
	A.15	Modificación deliberada de la información	Datos erróneos en el momento de la movilización de la información.
	A.18	Destrucción de información	Perdida de la información.
	A.19	Divulgación de información	Información filtrada abiertamente a personas no correspondientes.
	A.22	Manipulación de programas	Alteración del funcionamiento de cada uno de los programas de la dependencia.

Fuente: Autoría propia

Tabla 17. Estimación de la vulnerabilidad activo open office Linux 2017

ACTIVO TI		OPEN OFFICE LINUX 2017	
ADMINISTRADOR		PIMIENTO CARDENAS WILSON MAURICIO	
TIPO DE ACTIVO		SOFTWARE	
Tipo	**ID**	**Amenaza**	**Exposición/Vulnerabilidad**
DE ORIGEN INDUSTRI	**I.5**	Avería de origen físico o lógico	La manipulación por parte de cada uno de los componentes encontrados en la dependencia, como también por defectos de los componentes desde fabrica

Tabla 17. Estimación de la vulnerabilidad activo open office Linux 2017. (Continuación)

ERRORES Y FALLOS NO INTENCIONADOS	**E.1**	Errores de los usuarios	Pérdida total o parcial del tiempo de ejecución de sus actividades, dependiendo de la gravedad del asunto.
	E.2	Errores del administrador	Pérdida total o parcial del tiempo de ejecución de sus actividades, dependiendo de la gravedad del asunto.
	E.8	Difusión de software dañino	La dependencia cuenta con antivirus capaces de controlar software malicioso
	E.9	Errores de [re-] encaminamiento	La dependencia cuenta con sistemas de cifrado y verificación (puerto – puerto) para el manejo de la movilidad de la información.
	E.10	Errores de secuencia	La dependencia cuenta con sistemas de cifrado y verificación (puerto – puerto) para el manejo de la movilidad de la información.
	E.15	Alteración accidental de la información	La dependencia cuenta con sistemas de cifrado y verificación (puerto – puerto) para el manejo de la movilidad de la información.
	E.18	Destrucción de información	El departamento de sistemas cuenta con copias de seguridad periódicas
	E.19	Fugas de información	Las personas contratadas están atadas a cláusulas de confidencialidad.
	E.20	Vulnerabilidades de los programas (software)	La dependencia cuenta con programas licenciados para mejorar la seguridad de las aplicaciones instaladas en los computadores de esta.
	E.21	Errores de mantenimiento / actualización de	Falla de funcionamiento del software.

Tabla 17. Estimación de la vulnerabilidad activo open office Linux 2017. (Continuación)

		programas (software)	
ATAQUES INTENCIONAD	**A.5**	Suplantación de la identidad del usuario	Acceso a personas que no cuenten con los permisos necesarios o con las credenciales necesarias.
	A.6	Abuso de privilegios de acceso	Abuso de cada uno de los derechos otorgados.
	A.7	Uso no previsto	Implementación de recursos (económicos y de tiempo) en actividades no relacionadas.
	A.8	Difusión de software dañino	Afectación en los sistemas de información y los procesos que ello conlleva.
	A.9	[Re-]encaminamiento de mensajes	La dependencia cuenta con sistemas de cifrado y verificación (puerto – puerto) para el manejo de la movilidad de la información.
	A.10	Alteración de secuencia	Alteración de datos.
	A.11	Acceso no autorizado	Uso ilícito del software open office Linux 2017
	A.15	Modificación deliberada de la información	Datos erróneos en el momento de la movilización de la información.
	A.18	Destrucción de información	Perdida de la información.
	A.19	Divulgación de información	Información filtrada abiertamente a personas no correspondientes.
	A.22	Manipulación de programas	Alteración del funcionamiento de cada uno de los programas de la dependencia.

Fuente: Autoría propia

Tabla 18. Estimación de la vulnerabilidad activo *System center*

ACTIVO TI	SYSTEM CENTER		
ADMINISTRADOR	PIMIENTO CARDENAS WILSON MAURICIO		
TIPO DE ACTIVO	SOFTWARE		
Tipo	**ID**	**Amenaza**	**Exposición/Vulnerabilidad**
DE ORIGEN INDUSTRI	**I.5**	Avería de origen físico o lógico	La manipulación por parte de cada uno de los componentes encontrados en la dependencia, como también por defectos de los componentes desde fabrica
ERRORES Y FALLOS NO INTENCIONADOS	**E.1**	Errores de los usuarios	Pérdida total o parcial del tiempo de ejecución de sus actividades, dependiendo de la gravedad del asunto.
	E.2	Errores del administrador	Pérdida total o parcial del tiempo de ejecución de sus actividades, dependiendo de la gravedad del asunto.
	E.8	Difusión de software dañino	La dependencia cuenta con antivirus capaces de controlar software malicioso
	E.9	Errores de [re-] encaminamiento	La dependencia cuenta con sistemas de cifrado y verificación (puerto – puerto) para el manejo de la movilidad de la información.
	E.10	Errores de secuencia	La dependencia cuenta con sistemas de cifrado y verificación (puerto – puerto) para el manejo de la movilidad de la información.
	E.15	Alteración accidental de la información	La dependencia cuenta con sistemas de cifrado y verificación (puerto – puerto) para el manejo de la movilidad de la información.
	E.18	Destrucción de información	El departamento de sistemas cuenta con copias de seguridad periódicas
	E.19	Fugas de información	Las personas contratadas están atadas a cláusulas de confidencialidad.

Tabla 18. Estimación de la vulnerabilidad activo *System center*. (Continuación)

	E.20	Vulnerabilidades de los programas (software)	La dependencia cuenta con programas licenciados para mejorar la seguridad de las aplicaciones instaladas en los computadores de esta.
	E.21	Errores de mantenimiento / actualización de programas (software)	Falla de funcionamiento del software.
ATAQUES INTENCIONAD	**A.5**	Suplantación de la identidad del usuario	Acceso a personas que no cuenten con los permisos necesarios o con las credenciales necesarias.
	A.6	Abuso de privilegios de acceso	Abuso de cada uno de los derechos otorgados.
	A.7	Uso no previsto	Implementación de recursos (económicos y de tiempo) en actividades no relacionadas.
	A.8	Difusión de software dañino	Afectación en los sistemas de información y los procesos que ello conlleva.
	A.9	[Re-]encaminamiento de mensajes	La dependencia cuenta con sistemas de cifrado y verificación (puerto – puerto) para el manejo de la movilidad de la información.
	A.10	Alteración de secuencia	Alteración de datos.
	A.11	Acceso no autorizado	Uso ilícito del software System center
	A.15	Modificación deliberada de la información	Datos erróneos en el momento de la movilización de la información.

Tabla 18. Estimación de la vulnerabilidad activo *System center*. (Continuación)

	A.18	Destrucción de información	Perdida de la información.
	A.19	Divulgación de información	Información filtrada abiertamente a personas no correspondientes.
	A.22	Manipulación de programas	Alteración del funcionamiento de cada uno de los programas de la dependencia.

Fuente: Autoría propia

Tabla 19. Estimación de la vulnerabilidad activo Windows defender

ACTIVO TI		WINDOWS DEFENDER	
ADMINISTRADOR		PIMIENTO CARDENAS WILSON MAURICIO	
TIPO DE ACTIVO		SOFTWARE	
Tipo	**ID**	**Amenaza**	**Exposición/Vulnerabilidad**
DE ORIGEN INDUSTRI	**I.5**	Avería de origen físico o lógico	La manipulación por parte de cada uno de los componentes encontrados en la dependencia, como también por defectos de los componentes desde fabrica
ERRORES Y FALLOS NO INTENCIONADOS	**E.1**	Errores de los usuarios	Pérdida total o parcial del tiempo de ejecución de sus actividades, dependiendo de la gravedad del asunto.
	E.2	Errores del administrador	Pérdida total o parcial del tiempo de ejecución de sus actividades, dependiendo de la gravedad del asunto.
	E.8	Difusión de software dañino	La dependencia cuenta con antivirus capaces de controlar software malicioso
	E.9	Errores de [re-] encaminamiento	La dependencia cuenta con sistemas de cifrado y verificación (puerto – puerto) para el manejo de la movilidad de la información.
	E.10	Errores de secuencia	La dependencia cuenta con sistemas de cifrado y verificación (puerto – puerto) para el manejo de la movilidad de la información.

Tabla 19. Estimación de la vulnerabilidad activo Windows defender. (Continuación)

	E.15	Alteración accidental de la información	La dependencia cuenta con sistemas de cifrado y verificación (puerto – puerto) para el manejo de la movilidad de la información.
	E.18	Destrucción de información	El departamento de sistemas cuenta con copias de seguridad periódicas
	E.19	Fugas de información	Las personas contratadas están atadas a cláusulas de confidencialidad.
	E.20	Vulnerabilidades de los programas (software)	La dependencia cuenta con programas licenciados para mejorar la seguridad de las aplicaciones instaladas en los computadores de esta.
	E.21	Errores de mantenimiento / actualización de programas (software)	Falla de funcionamiento del software.
ATAQUES INTENCIONAD	**A.5**	Suplantación de la identidad del usuario	Acceso a personas que no cuenten con los permisos necesarios o con las credenciales necesarias.
	A.6	Abuso de privilegios de acceso	Abuso de cada uno de los derechos otorgados.
	A.7	Uso no previsto	Implementación de recursos (económicos y de tiempo) en actividades no relacionadas.
	A.8	Difusión de software dañino	Afectación en los sistemas de información y los procesos que ello conlleva.
	A.9	[Re-]encaminamiento de mensajes	La dependencia cuenta con sistemas de cifrado y verificación (puerto – puerto) para el manejo de la movilidad de la información.

Tabla 19. Estimación de la vulnerabilidad activo Windows defender. (Continuación)

	A.10	Alteración de secuencia	Alteración de datos.
	A.11	Acceso no autorizado	Uso ilícito del software Windows defender
	A.15	Modificación deliberada de la información	Datos erróneos en el momento de la movilización de la información.
	A.18	Destrucción de información	Perdida de la información.
	A.19	Divulgación de información	Información filtrada abiertamente a personas no correspondientes.
	A.22	Manipulación de programas	Alteración del funcionamiento de cada uno de los programas de la dependencia.

Fuente: Autoría propia

Tabla 20. Estimación de la vulnerabilidad activo Windows 8

ACTIVO TI		WINDOWS 8	
ADMINISTRADOR		PIMIENTO CARDENAS WILSON MAURICIO	
TIPO DE ACTIVO		SOFTWARE	
Tipo	**ID**	**Amenaza**	**Exposición/Vulnerabilidad**
DE ORIGEN INDUSTRI	**I.5**	Avería de origen físico o lógico	La manipulación por parte de cada uno de los componentes encontrados en la dependencia, como también por defectos de los componentes desde fabrica
ERRORES Y FALLOS NO INTENCIONADOS	**E.1**	Errores de los usuarios	Pérdida total o parcial del tiempo de ejecución de sus actividades, dependiendo de la gravedad del asunto.
	E.2	Errores del administrador	Pérdida total o parcial del tiempo de ejecución de sus actividades, dependiendo de la gravedad del asunto.
	E.8	Difusión de software dañino	La dependencia cuenta con antivirus capaces de controlar software malicioso

Tabla 20. Estimación de la vulnerabilidad activo Windows 8. (Continuación)

	E.9	Errores de [re-] encaminamiento	La dependencia cuenta con sistemas de cifrado y verificación (puerto – puerto) para el manejo de la movilidad de la información.
	E.10	Errores de secuencia	La dependencia cuenta con sistemas de cifrado y verificación (puerto – puerto) para el manejo de la movilidad de la información.
	E.15	Alteración accidental de la información	La dependencia cuenta con sistemas de cifrado y verificación (puerto – puerto) para el manejo de la movilidad de la información.
	E.18	Destrucción de información	El departamento de sistemas cuenta con copias de seguridad periódicas
	E.19	Fugas de información	Las personas contratadas están atadas a cláusulas de confidencialidad.
	E.20	Vulnerabilidades de los programas (software)	La dependencia cuenta con programas licenciados para mejorar la seguridad de las aplicaciones instaladas en los computadores de esta.
	E.21	Errores de mantenimiento / actualización de programas (software)	Falla de funcionamiento del software.
ATAQUES INTENCIONAD	**A.5**	Suplantación de la identidad del usuario	Acceso a personas que no cuenten con los permisos necesarios o con las credenciales necesarias.
	A.6	Abuso de privilegios de acceso	Abuso de cada uno de los derechos otorgados.

Tabla 20. Estimación de la vulnerabilidad activo Windows 8. (Continuación)

	A.7	Uso no previsto	Implementación de recursos (económicos y de tiempo) en actividades no relacionadas.
	A.8	Difusión de software dañino	Afectación en los sistemas de información y los procesos que ello conlleva.
	A.9	[Re-]encaminamiento de mensajes	La dependencia cuenta con sistemas de cifrado y verificación (puerto – puerto) para el manejo de la movilidad de la información.
	A.10	Alteración de secuencia	Alteración de datos.
	A.11	Acceso no autorizado	Uso ilícito del software Windows 8
	A.15	Modificación deliberada de la información	Datos erróneos en el momento de la movilización de la información.
	A.18	Destrucción de información	Perdida de la información.
	A.19	Divulgación de información	Información filtrada abiertamente a personas no correspondientes.
	A.22	Manipulación de programas	Alteración del funcionamiento de cada uno de los programas de la dependencia.

Fuente: Autoría propia

Tabla 21. Estimación de la vulnerabilidad activo Windows server 2009

ACTIVO TI		WINDOWS SERVER 2009	
ADMINISTRADOR		PIMIENTO CARDENAS WILSON MAURICIO	
TIPO DE ACTIVO		SOFTWARE	
Tipo	**ID**	**Amenaza**	**Exposición/Vulnerabilidad**
DE ORIGEN INDUSTRI	**I.5**	Avería de origen físico o lógico	La manipulación por parte de cada uno de los componentes encontrados en la dependencia, como también por defectos de los componentes desde fabrica

Tabla 21. Estimación de la vulnerabilidad activo Windows server 2009. (Continuación)

ERRORES Y FALLOS NO INTENCIONADOS	**E.1**	Errores de los usuarios	Pérdida total o parcial del tiempo de ejecución de sus actividades, dependiendo de la gravedad del asunto.
	E.2	Errores del administrador	Pérdida total o parcial del tiempo de ejecución de sus actividades, dependiendo de la gravedad del asunto.
	E.8	Difusión de software dañino	La dependencia cuenta con antivirus capaces de controlar software malicioso
	E.9	Errores de [re-] encaminamiento	La dependencia cuenta con sistemas de cifrado y verificación (puerto – puerto) para el manejo de la movilidad de la información.
	E.10	Errores de secuencia	La dependencia cuenta con sistemas de cifrado y verificación (puerto – puerto) para el manejo de la movilidad de la información.
	E.15	Alteración accidental de la información	La dependencia cuenta con sistemas de cifrado y verificación (puerto – puerto) para el manejo de la movilidad de la información.
	E.18	Destrucción de información	El departamento de sistemas cuenta con copias de seguridad periódicas
	E.19	Fugas de información	Las personas contratadas están atadas a cláusulas de confidencialidad.
	E.20	Vulnerabilidades de los programas (software)	La dependencia cuenta con programas licenciados para mejorar la seguridad de las aplicaciones instaladas en los computadores de esta.
	E.21	Errores de mantenimiento / actualización de	Falla de funcionamiento del software.

Tabla 21. Estimación de la vulnerabilidad activo Windows server 2009. (Continuación)

		programas (software)	
ATAQUES INTENCIONAD	**A.5**	Suplantación de la identidad del usuario	Acceso a personas que no cuenten con los permisos necesarios o con las credenciales necesarias.
	A.6	Abuso de privilegios de acceso	Abuso de cada uno de los derechos otorgados.
	A.7	Uso no previsto	Implementación de recursos (económicos y de tiempo) en actividades no relacionadas.
	A.8	Difusión de software dañino	Afectación en los sistemas de información y los procesos que ello conlleva.
	A.9	[Re-]encaminamiento de mensajes	La dependencia cuenta con sistemas de cifrado y verificación (puerto – puerto) para el manejo de la movilidad de la información.
	A.10	Alteración de secuencia	Alteración de datos.
	A.11	Acceso no autorizado	Uso ilícito del software Windows server 2009
	A.15	Modificación deliberada de la información	Datos erróneos en el momento de la movilización de la información.
	A.18	Destrucción de información	Perdida de la información.
	A.19	Divulgación de información	Información filtrada abiertamente a personas no correspondientes.
	A.22	Manipulación de programas	Alteración del funcionamiento de cada uno de los programas de la dependencia.

Fuente: Autoría propia

Tabla 22. Estimación de la vulnerabilidad activo Windows server 2012

ACTIVO TI		WINDOWS SERVER 2012	
ADMINISTRADOR		PIMIENTO CARDENAS WILSON MAURICIO	
TIPO DE ACTIVO		SOFTWARE	
Tipo	**ID**	**Amenaza**	**Exposición/Vulnerabilidad**
DE ORIGEN INDUSTRI	**I.5**	Avería de origen físico o lógico	La manipulación por parte de cada uno de los componentes encontrados en la dependencia, como también por defectos de los componentes desde fabrica
ERRORES Y FALLOS NO INTENCIONADOS	**E.1**	Errores de los usuarios	Pérdida total o parcial del tiempo de ejecución de sus actividades, dependiendo de la gravedad del asunto.
	E.2	Errores del administrador	Pérdida total o parcial del tiempo de ejecución de sus actividades, dependiendo de la gravedad del asunto.
	E.8	Difusión de software dañino	La dependencia cuenta con antivirus capaces de controlar software malicioso
	E.9	Errores de [re-] encaminamiento	La dependencia cuenta con sistemas de cifrado y verificación (puerto – puerto) para el manejo de la movilidad de la información.
	E.10	Errores de secuencia	La dependencia cuenta con sistemas de cifrado y verificación (puerto – puerto) para el manejo de la movilidad de la información.
	E.15	Alteración accidental de la información	La dependencia cuenta con sistemas de cifrado y verificación (puerto – puerto) para el manejo de la movilidad de la información.
	E.18	Destrucción de información	El departamento de sistemas cuenta con copias de seguridad periódicas
	E.19	Fugas de información	Las personas contratadas están atadas a cláusulas de confidencialidad.

Tabla 22. Estimación de la vulnerabilidad activo Windows server 2012. (Continuación)

	E.20	Vulnerabilidades de los programas (software)	La dependencia cuenta con programas licenciados para mejorar la seguridad de las aplicaciones instaladas en los computadores de esta.
	E.21	Errores de mantenimiento / actualización de programas (software)	Falla de funcionamiento del software.
ATAQUES INTENCIONAD	**A.5**	Suplantación de la identidad del usuario	Acceso a personas que no cuenten con los permisos necesarios o con las credenciales necesarias.
	A.6	Abuso de privilegios de acceso	Abuso de cada uno de los derechos otorgados.
	A.7	Uso no previsto	Implementación de recursos (económicos y de tiempo) en actividades no relacionadas.
	A.8	Difusión de software dañino	Afectación en los sistemas de información y los procesos que ello conlleva.
	A.9	[Re-]encaminamiento de mensajes	La dependencia cuenta con sistemas de cifrado y verificación (puerto – puerto) para el manejo de la movilidad de la información.
	A.10	Alteración de secuencia	Alteración de datos.
	A.11	Acceso no autorizado	Uso ilícito del software Windows server 2012
	A.15	Modificación deliberada de la información	Datos erróneos en el momento de la movilización de la información.

Tabla 22. Estimación de la vulnerabilidad activo Windows server 2012. (Continuación)

	A.18	Destrucción de información	Perdida de la información.
	A.19	Divulgación de información	Información filtrada abiertamente a personas no correspondientes.
	A.22	Manipulación de programas	Alteración del funcionamiento de cada uno de los programas de la dependencia.

Fuente: Autoría propia

Tabla 23. Estimación de la vulnerabilidad activo CentOS 5

ACTIVO TI		CENTOS 5	
ADMINISTRADOR		PIMIENTO CARDENAS WILSON MAURICIO	
TIPO DE ACTIVO		SOFTWARE	
Tipo	**ID**	**Amenaza**	**Exposición/Vulnerabilidad**
DE ORIGEN INDUSTRI	**I.5**	Avería de origen físico o lógico	La manipulación por parte de cada uno de los componentes encontrados en la dependencia, como también por defectos de los componentes desde fabrica
ERRORES Y FALLOS NO INTENCIONADOS	**E.1**	Errores de los usuarios	Pérdida total o parcial del tiempo de ejecución de sus actividades, dependiendo de la gravedad del asunto.
	E.2	Errores del administrador	Pérdida total o parcial del tiempo de ejecución de sus actividades, dependiendo de la gravedad del asunto.
	E.8	Difusión de software dañino	La dependencia cuenta con antivirus capaces de controlar software malicioso
	E.9	Errores de [re-] encaminamiento	La dependencia cuenta con sistemas de cifrado y verificación (puerto – puerto) para el manejo de la movilidad de la información.
	E.10	Errores de secuencia	La dependencia cuenta con sistemas de cifrado y verificación (puerto – puerto) para el manejo de la movilidad de la información.

Tabla 23. Estimación de la vulnerabilidad activo CentOS 5. (Continuación)

	E.15	Alteración accidental de la información	La dependencia cuenta con sistemas de cifrado y verificación (puerto – puerto) para el manejo de la movilidad de la información.
	E.18	Destrucción de información	El departamento de sistemas cuenta con copias de seguridad periódicas
	E.19	Fugas de información	Las personas contratadas están atadas a cláusulas de confidencialidad.
	E.20	Vulnerabilidades de los programas (software)	La dependencia cuenta con programas licenciados para mejorar la seguridad de las aplicaciones instaladas en los computadores de esta.
	E.21	Errores de mantenimiento / actualización de programas (software)	Falla de funcionamiento del software.
ATAQUES INTENCIONAD	**A.5**	Suplantación de la identidad del usuario	Acceso a personas que no cuenten con los permisos necesarios o con las credenciales necesarias.
	A.6	Abuso de privilegios de acceso	Abuso de cada uno de los derechos otorgados.
	A.7	Uso no previsto	Implementación de recursos (económicos y de tiempo) en actividades no relacionadas.
	A.8	Difusión de software dañino	Afectación en los sistemas de información y los procesos que ello conlleva.
	A.9	[Re-]encaminamiento de mensajes	La dependencia cuenta con sistemas de cifrado y verificación (puerto – puerto) para el manejo de la movilidad de la información.

Tabla 23. Estimación de la vulnerabilidad activo CentOS 5. (Continuación)

	A.10	Alteración de secuencia	Alteración de datos.
	A.11	Acceso no autorizado	Uso ilícito del software CentOS 5
	A.15	Modificación deliberada de la información	Datos erróneos en el momento de la movilización de la información.
	A.18	Destrucción de información	Perdida de la información.
	A.19	Divulgación de información	Información filtrada abiertamente a personas no correspondientes.
	A.22	Manipulación de programas	Alteración del funcionamiento de cada uno de los programas de la dependencia.

Fuente: Autoría propia

Tabla 24. Estimación de la vulnerabilidad activo Debian 7

ACTIVO TI		DEBIAN 7	
ADMINISTRADOR		PIMIENTO CARDENAS WILSON MAURICIO	
TIPO DE ACTIVO		SOFTWARE	
Tipo	**ID**	**Amenaza**	**Exposición/Vulnerabilidad**
DE ORIGEN INDUSTRI	**I.5**	Avería de origen físico o lógico	La manipulación por parte de cada uno de los componentes encontrados en la dependencia, como también por defectos de los componentes desde fabrica
ERRORES Y FALLOS NO INTENCIONADOS	**E.1**	Errores de los usuarios	Pérdida total o parcial del tiempo de ejecución de sus actividades, dependiendo de la gravedad del asunto.
	E.2	Errores del administrador	Pérdida total o parcial del tiempo de ejecución de sus actividades, dependiendo de la gravedad del asunto.
	E.8	Difusión de software dañino	La dependencia cuenta con antivirus capaces de controlar software malicioso

Tabla 24. Estimación de la vulnerabilidad activo Debian 7. (Continuación)

	E.9	Errores de [re-] encaminamiento	La dependencia cuenta con sistemas de cifrado y verificación (puerto – puerto) para el manejo de la movilidad de la información.
	E.10	Errores de secuencia	La dependencia cuenta con sistemas de cifrado y verificación (puerto – puerto) para el manejo de la movilidad de la información.
	E.15	Alteración accidental de la información	La dependencia cuenta con sistemas de cifrado y verificación (puerto – puerto) para el manejo de la movilidad de la información.
	E.18	Destrucción de información	El departamento de sistemas cuenta con copias de seguridad periódicas
	E.19	Fugas de información	Las personas contratadas están atadas a cláusulas de confidencialidad.
	E.20	Vulnerabilidades de los programas (software)	La dependencia cuenta con programas licenciados para mejorar la seguridad de las aplicaciones instaladas en los computadores de esta.
	E.21	Errores de mantenimiento / actualización de programas (software)	Falla de funcionamiento del software.
ATAQUES INTENCIONAD	**A.5**	Suplantación de la identidad del usuario	Acceso a personas que no cuenten con los permisos necesarios o con las credenciales necesarias.
	A.6	Abuso de privilegios de acceso	Abuso de cada uno de los derechos otorgados.

Tabla 24. Estimación de la vulnerabilidad activo Debian 7. (Continuación)

	A.7	Uso no previsto	Implementación de recursos (económicos y de tiempo) en actividades no relacionadas.
	A.8	Difusión de software dañino	Afectación en los sistemas de información y los procesos que ello conlleva.
	A.9	[Re-]encaminamiento de mensajes	La dependencia cuenta con sistemas de cifrado y verificación (puerto – puerto) para el manejo de la movilidad de la información.
	A.10	Alteración de secuencia	Alteración de datos.
	A.11	Acceso no autorizado	Uso ilícito del software Debian 7
	A.15	Modificación deliberada de la información	Datos erróneos en el momento de la movilización de la información.
	A.18	Destrucción de información	Perdida de la información.
	A.19	Divulgación de información	Información filtrada abiertamente a personas no correspondientes.
	A.22	Manipulación de programas	Alteración del funcionamiento de cada uno de los programas de la dependencia.

Fuente: Autoría propia

Tabla 25. Estimación de la vulnerabilidad activo Ubuntu 14

ACTIVO TI		UBUNTU 14	
ADMINISTRADOR		PIMIENTO CARDENAS WILSON MAURICIO	
TIPO DE ACTIVO		SOFTWARE	
Tipo	ID	Amenaza	Exposición/Vulnerabilidad
DE ORIGEN INDUSTRI	**I.5**	Avería de origen físico o lógico	La manipulación por parte de cada uno de los componentes encontrados en la dependencia, como también por defectos de los componentes desde fabrica

Tabla 25. Estimación de la vulnerabilidad activo Ubuntu 14. (Continuación)

ERRORES Y FALLOS NO INTENCIONADOS	**E.1**	Errores de los usuarios	Pérdida total o parcial del tiempo de ejecución de sus actividades, dependiendo de la gravedad del asunto.
	E.2	Errores del administrador	Pérdida total o parcial del tiempo de ejecución de sus actividades, dependiendo de la gravedad del asunto.
	E.8	Difusión de software dañino	La dependencia cuenta con antivirus capaces de controlar software malicioso
	E.9	Errores de [re-] encaminamiento	La dependencia cuenta con sistemas de cifrado y verificación (puerto – puerto) para el manejo de la movilidad de la información.
	E.10	Errores de secuencia	La dependencia cuenta con sistemas de cifrado y verificación (puerto – puerto) para el manejo de la movilidad de la información.
	E.15	Alteración accidental de la información	La dependencia cuenta con sistemas de cifrado y verificación (puerto – puerto) para el manejo de la movilidad de la información.
	E.18	Destrucción de información	El departamento de sistemas cuenta con copias de seguridad periódicas
	E.19	Fugas de información	Las personas contratadas están atadas a cláusulas de confidencialidad.
	E.20	Vulnerabilidades de los programas (software)	La dependencia cuenta con programas licenciados para mejorar la seguridad de las aplicaciones instaladas en los computadores de esta.
	E.21	Errores de mantenimiento / actualización de	Falla de funcionamiento del software.

Tabla 25. Estimación de la vulnerabilidad activo Ubuntu 14. (Continuación)

		programas (software)	
ATAQUES INTENCIONAD	**A.5**	Suplantación de la identidad del usuario	Acceso a personas que no cuenten con los permisos necesarios o con las credenciales necesarias.
	A.6	Abuso de privilegios de acceso	Abuso de cada uno de los derechos otorgados.
	A.7	Uso no previsto	Implementación de recursos (económicos y de tiempo) en actividades no relacionadas.
	A.8	Difusión de software dañino	Afectación en los sistemas de información y los procesos que ello conlleva.
	A.9	[Re-]encaminamiento de mensajes	La dependencia cuenta con sistemas de cifrado y verificación (puerto – puerto) para el manejo de la movilidad de la información.
	A.10	Alteración de secuencia	Alteración de datos.
	A.11	Acceso no autorizado	Uso ilícito del software Ubuntu 14
	A.15	Modificación deliberada de la información	Datos erróneos en el momento de la movilización de la información.
	A.18	Destrucción de información	Perdida de la información.
	A.19	Divulgación de información	Información filtrada abiertamente a personas no correspondientes.
	A.22	Manipulación de programas	Alteración del funcionamiento de cada uno de los programas de la dependencia.

Fuente: Autoría propia

Tabla 26. Estimación de la vulnerabilidad activo Mac os x

ACTIVO TI		MAC OS X	
ADMINISTRADOR		PIMIENTO CARDENAS WILSON MAURICIO	
TIPO DE ACTIVO		SOFTWARE	
Tipo	**ID**	**Amenaza**	**Exposición/Vulnerabilidad**
DE ORIGEN INDUSTRI	**I.5**	Avería de origen físico o lógico	La manipulación por parte de cada uno de los componentes encontrados en la dependencia, como también por defectos de los componentes desde fabrica
ERRORES Y FALLOS NO INTENCIONADOS	**E.1**	Errores de los usuarios	Pérdida total o parcial del tiempo de ejecución de sus actividades, dependiendo de la gravedad del asunto.
	E.2	Errores del administrador	Pérdida total o parcial del tiempo de ejecución de sus actividades, dependiendo de la gravedad del asunto.
	E.8	Difusión de software dañino	La dependencia cuenta con antivirus capaces de controlar software malicioso
	E.9	Errores de [re-] encaminamiento	La dependencia cuenta con sistemas de cifrado y verificación (puerto – puerto) para el manejo de la movilidad de la información.
	E.10	Errores de secuencia	La dependencia cuenta con sistemas de cifrado y verificación (puerto – puerto) para el manejo de la movilidad de la información.
	E.15	Alteración accidental de la información	La dependencia cuenta con sistemas de cifrado y verificación (puerto – puerto) para el manejo de la movilidad de la información.
	E.18	Destrucción de información	El departamento de sistemas cuenta con copias de seguridad periódicas
	E.19	Fugas de información	Las personas contratadas están atadas a cláusulas de confidencialidad.

Tabla 26. Estimación de la vulnerabilidad activo Mac os x. (Continuación)

	E.20	Vulnerabilidades de los programas (software)	La dependencia cuenta con programas licenciados para mejorar la seguridad de las aplicaciones instaladas en los computadores de esta.
	E.21	Errores de mantenimiento / actualización de programas (software)	Falla de funcionamiento del software.
ATAQUES INTENCIONAD	**A.5**	Suplantación de la identidad del usuario	Acceso a personas que no cuenten con los permisos necesarios o con las credenciales necesarias.
	A.6	Abuso de privilegios de acceso	Abuso de cada uno de los derechos otorgados.
	A.7	Uso no previsto	Implementación de recursos (económicos y de tiempo) en actividades no relacionadas.
	A.8	Difusión de software dañino	Afectación en los sistemas de información y los procesos que ello conlleva.
	A.9	[Re-]encaminamiento de mensajes	La dependencia cuenta con sistemas de cifrado y verificación (puerto – puerto) para el manejo de la movilidad de la información.
	A.10	Alteración de secuencia	Alteración de datos.
	A.11	Acceso no autorizado	Uso ilícito del software Mac os x
	A.15	Modificación deliberada de la información	Datos erróneos en el momento de la movilización de la información.

Tabla 26. Estimación de la vulnerabilidad activo Mac os x. (Continuación)

	A.18	Destrucción de información	Perdida de la información.
	A.19	Divulgación de información	Información filtrada abiertamente a personas no correspondientes.
	A.22	Manipulación de programas	Alteración del funcionamiento de cada uno de los programas de la dependencia.

Fuente: Autoría propia

Tabla 27. Estimación de la vulnerabilidad activo CoMmanD (CMD)

ACTIVO TI		COMMAND (CMD)	
ADMINISTRADOR		PIMIENTO CARDENAS WILSON MAURICIO	
TIPO DE ACTIVO		SOFTWARE	
Tipo	**ID**	**Amenaza**	**Exposición/Vulnerabilidad**
DE ORIGEN INDUSTRI	**I.5**	Avería de origen físico o lógico	La manipulación por parte de cada uno de los componentes encontrados en la dependencia, como también por defectos de los componentes desde fabrica
ERRORES Y FALLOS NO INTENCIONADOS	**E.1**	Errores de los usuarios	Pérdida total o parcial del tiempo de ejecución de sus actividades, dependiendo de la gravedad del asunto.
	E.2	Errores del administrador	Pérdida total o parcial del tiempo de ejecución de sus actividades, dependiendo de la gravedad del asunto.
	E.8	Difusión de software dañino	La dependencia cuenta con antivirus capaces de controlar software malicioso
	E.9	Errores de [re-] encaminamiento	La dependencia cuenta con sistemas de cifrado y verificación (puerto – puerto) para el manejo de la movilidad de la información.
	E.10	Errores de secuencia	La dependencia cuenta con sistemas de cifrado y verificación (puerto – puerto) para el manejo de la movilidad de la información.

Tabla 27. Estimación de la vulnerabilidad activo CoMmanD (CMD). (Continuación)

	E.15	Alteración accidental de la información	La dependencia cuenta con sistemas de cifrado y verificación (puerto – puerto) para el manejo de la movilidad de la información.
	E.18	Destrucción de información	El departamento de sistemas cuenta con copias de seguridad periódicas
	E.19	Fugas de información	Las personas contratadas están atadas a cláusulas de confidencialidad.
	E.20	Vulnerabilidades de los programas (software)	La dependencia cuenta con programas licenciados para mejorar la seguridad de las aplicaciones instaladas en los computadores de esta.
	E.21	Errores de mantenimiento / actualización de programas (software)	Falla de funcionamiento del software.
ATAQUES INTENCIONAD	**A.5**	Suplantación de la identidad del usuario	Acceso a personas que no cuenten con los permisos necesarios o con las credenciales necesarias.
	A.6	Abuso de privilegios de acceso	Abuso de cada uno de los derechos otorgados.
	A.7	Uso no previsto	Implementación de recursos (económicos y de tiempo) en actividades no relacionadas.
	A.8	Difusión de software dañino	Afectación en los sistemas de información y los procesos que ello conlleva.
	A.9	[Re-]encaminamiento de mensajes	La dependencia cuenta con sistemas de cifrado y verificación (puerto – puerto) para el manejo de la movilidad de la información.

Tabla 27. Estimación de la vulnerabilidad activo CoMmanD (CMD). (Continuación)

	A.10	Alteración de secuencia	Alteración de datos.
	A.11	Acceso no autorizado	Uso ilícito del software CoMmanD (CMD)
	A.15	Modificación deliberada de la información	Datos erróneos en el momento de la movilización de la información.
	A.18	Destrucción de información	Perdida de la información.
	A.19	Divulgación de información	Información filtrada abiertamente a personas no correspondientes.
	A.22	Manipulación de programas	Alteración del funcionamiento de cada uno de los programas de la dependencia.

Fuente: Autoría propia

Tabla 28. Estimación de la vulnerabilidad activo CoMmanD line (Mac)

ACTIVO TI		COMMAND LINE (MAC)	
ADMINISTRADOR		PIMIENTO CARDENAS WILSON MAURICIO	
TIPO DE ACTIVO		SOFTWARE	
Tipo	**ID**	**Amenaza**	**Exposición/Vulnerabilidad**
DE ORIGEN INDUSTRI	**I.5**	Avería de origen físico o lógico	La manipulación por parte de cada uno de los componentes encontrados en la dependencia, como también por defectos de los componentes desde fabrica
ERRORES Y FALLOS NO INTENCIONADOS	**E.1**	Errores de los usuarios	Pérdida total o parcial del tiempo de ejecución de sus actividades, dependiendo de la gravedad del asunto.
	E.2	Errores del administrador	Pérdida total o parcial del tiempo de ejecución de sus actividades, dependiendo de la gravedad del asunto.
	E.8	Difusión de software dañino	La dependencia cuenta con antivirus capaces de controlar software malicioso

Tabla 28. Estimación de la vulnerabilidad activo CoMmanD line (Mac). (Continuación)

	E.9	Errores de [re-] encaminamiento	La dependencia cuenta con sistemas de cifrado y verificación (puerto – puerto) para el manejo de la movilidad de la información.
	E.10	Errores de secuencia	La dependencia cuenta con sistemas de cifrado y verificación (puerto – puerto) para el manejo de la movilidad de la información.
	E.15	Alteración accidental de la información	La dependencia cuenta con sistemas de cifrado y verificación (puerto – puerto) para el manejo de la movilidad de la información.
	E.18	Destrucción de información	El departamento de sistemas cuenta con copias de seguridad periódicas
	E.19	Fugas de información	Las personas contratadas están atadas a cláusulas de confidencialidad.
	E.20	Vulnerabilidades de los programas (software)	La dependencia cuenta con programas licenciados para mejorar la seguridad de las aplicaciones instaladas en los computadores de esta.
	E.21	Errores de mantenimiento / actualización de programas (software)	Falla de funcionamiento del software.
ATAQUES INTENCIONAD	**A.5**	Suplantación de la identidad del usuario	Acceso a personas que no cuenten con los permisos necesarios o con las credenciales necesarias.
	A.6	Abuso de privilegios de acceso	Abuso de cada uno de los derechos otorgados.

Tabla 28. Estimación de la vulnerabilidad activo CoMmanD line (Mac). (Continuación)

	A.7	Uso no previsto	Implementación de recursos (económicos y de tiempo) en actividades no relacionadas.
	A.8	Difusión de software dañino	Afectación en los sistemas de información y los procesos que ello conlleva.
	A.9	[Re-]encaminamiento de mensajes	La dependencia cuenta con sistemas de cifrado y verificación (puerto – puerto) para el manejo de la movilidad de la información.
	A.10	Alteración de secuencia	Alteración de datos.
	A.11	Acceso no autorizado	Uso ilícito del software CoMmanD line (Mac)
	A.15	Modificación deliberada de la información	Datos erróneos en el momento de la movilización de la información.
	A.18	Destrucción de información	Perdida de la información.
	A.19	Divulgación de información	Información filtrada abiertamente a personas no correspondientes.
	A.22	Manipulación de programas	Alteración del funcionamiento de cada uno de los programas de la dependencia.

Fuente: Autoría propia

Tabla 29. Estimación de la vulnerabilidad activo terminal

ACTIVO TI		TERMINAL	
ADMINISTRADOR		PIMIENTO CARDENAS WILSON MAURICIO	
TIPO DE ACTIVO		SOFTWARE	
Tipo	**ID**	**Amenaza**	**Exposición/Vulnerabilidad**
DE ORIGEN INDUSTRI	**I.5**	Avería de origen físico o lógico	La manipulación por parte de cada uno de los componentes encontrados en la dependencia, como también por defectos de los componentes desde fabrica

Tabla 29. Estimación de la vulnerabilidad activo terminal. (Continuación)

ERRORES Y FALLOS NO INTENCIONADOS	**E.1**	Errores de los usuarios	Pérdida total o parcial del tiempo de ejecución de sus actividades, dependiendo de la gravedad del asunto.
	E.2	Errores del administrador	Pérdida total o parcial del tiempo de ejecución de sus actividades, dependiendo de la gravedad del asunto.
	E.8	Difusión de software dañino	La dependencia cuenta con antivirus capaces de controlar software malicioso
	E.9	Errores de [re-] encaminamiento	La dependencia cuenta con sistemas de cifrado y verificación (puerto – puerto) para el manejo de la movilidad de la información.
	E.10	Errores de secuencia	La dependencia cuenta con sistemas de cifrado y verificación (puerto – puerto) para el manejo de la movilidad de la información.
	E.15	Alteración accidental de la información	La dependencia cuenta con sistemas de cifrado y verificación (puerto – puerto) para el manejo de la movilidad de la información.
	E.18	Destrucción de información	El departamento de sistemas cuenta con copias de seguridad periódicas
	E.19	Fugas de información	Las personas contratadas están atadas a cláusulas de confidencialidad.
	E.20	Vulnerabilidades de los programas (software)	La dependencia cuenta con programas licenciados para mejorar la seguridad de las aplicaciones instaladas en los computadores de esta.
	E.21	Errores de mantenimiento / actualización de	Falla de funcionamiento del software.

Tabla 29. Estimación de la vulnerabilidad activo terminal. (Continuación)

		programas (software)	
ATAQUES INTENCIONAD	**A.5**	Suplantación de la identidad del usuario	Acceso a personas que no cuenten con los permisos necesarios o con las credenciales necesarias.
	A.6	Abuso de privilegios de acceso	Abuso de cada uno de los derechos otorgados.
	A.7	Uso no previsto	Implementación de recursos (económicos y de tiempo) en actividades no relacionadas.
	A.8	Difusión de software dañino	Afectación en los sistemas de información y los procesos que ello conlleva.
	A.9	[Re-]encaminamiento de mensajes	La dependencia cuenta con sistemas de cifrado y verificación (puerto – puerto) para el manejo de la movilidad de la información.
	A.10	Alteración de secuencia	Alteración de datos.
	A.11	Acceso no autorizado	Uso ilícito del software terminal
	A.15	Modificación deliberada de la información	Datos erróneos en el momento de la movilización de la información.
	A.18	Destrucción de información	Perdida de la información.
	A.19	Divulgación de información	Información filtrada abiertamente a personas no correspondientes.
	A.22	Manipulación de programas	Alteración del funcionamiento de cada uno de los programas de la dependencia.

Fuente: Autoría propia

Tabla 30. Estimación de la vulnerabilidad activo servidor DNS Y DHCP

ACTIVO TI	SERVIDOR DNS Y DHCP
ADMINISTRADOR	PIMIENTO CARDENAS WILSON MAURICIO
TIPO DE ACTIVO	HARDWARE

Tipo	ID	Amenaza	Exposición/Vulnerabilidad
DESASTRES NATURALES	**N.1**	Fuego	No existe sistema de alarma contra incendios. Se posee un solo extintor de solkaflam (clase c) recomendados para incendios en lugares donde se encuentren equipos eléctricos.
	N.2	Daños por agua	La infraestructura está expuesta a goteras, cuenta con averías en el techo en donde el agua de las lluvias
	N.*	Desastres naturales	La oficina de la dependencia de sistemas se encuentra en zona baja de riesgo de desastre natural de origen volcánico debido a su cercanía con el volcán nevado del Tolima.
DE ORIGEN INDUSTRIAL	**I.1**	Fuego	No existe sistema de alarma contra incendios. Se posee un solo extintor de solkaflam (clase c) recomendados para incendios en lugares donde se encuentren equipos eléctricos.
	I.2	Daños por agua	La concentración del líquido sobrante por parte del aire acondicionado causaría daños en los equipos.
	I.*	Desastres industriales	No hay exposición o vulnerabilidad, por parte de esta amenaza.
	I.3	Contaminación mecánica	No hay exposición o vulnerabilidad, por parte de esta amenaza.
	I.4	Contaminación electromagnética	No hay exposición o vulnerabilidad, por parte de esta amenaza.

Tabla 30. Estimación de la vulnerabilidad activo servidor DNS Y DHCP. (Continuación)

	I.5	Avería de origen físico o lógico	La manipulación por parte de cada uno de los componentes encontrados en la dependencia, como también por defectos de los componentes desde fabrica
	I.6	Corte del suministro eléctrico	Amenaza debida a factores externos, a clemencias de tipo naturales como lluvias u otros.
	I.7	Condiciones inadecuadas de temperatura o humedad	No se cuenta con una infraestructura adecuada para soportar los defectos del sistema de refrigeración.
	I.11	Emanaciones electromagnéticas	No hay exposición o vulnerabilidad, por parte de esta amenaza.
ERRORES Y FALLOS NO INTENCIONADOS	**E.2**	Errores del administrador	Pérdida total o parcial del tiempo de ejecución de sus actividades, dependiendo de la gravedad del asunto.
	E.23	Errores de mantenimiento / actualización de equipos(hardware)	Perjuicio a la mantenibilidad del sistema de información.
	E.24	Caída del sistema por agotamiento de recursos	Saturación del sistema informático.
	E.25	Perdida de equipos (Robo)	Recuperación de soportes reciclados o desechados.
ATAQUES INTENCIONADOS	**A.6**	Abuso de privilegios de acceso	Abuso de cada uno de los derechos otorgados.
	A.7	Uso no previsto	Implementación de recursos (económicos y de tiempo) en actividades no relacionadas.

Tabla 30. Estimación de la vulnerabilidad activo servidor DNS Y DHCP. (Continuación)

	A.11	Acceso no autorizado	Uso ilícito del hardware
	A.23	Manipulación de los equipos	Sabotaje del hardware.
	A.24	Denegación de servicio	Saturación del sistema de información.
	A.25	Robo	Robo de porte de la información, puede esta ser física o digital.
	A.26	Ataque destructivo	Destrucción de los contenedores de la información, en recipientes físicos y lógicos.

Fuente: Autoría propia

Tabla 31. Estimación de la vulnerabilidad activo servidor plataforma RYCA V.2.0

ACTIVO TI		SERVIDOR PLATAFORMA RYCA V.2.0	
ADMINISTRADOR		PIMIENTO CARDENAS WILSON MAURICIO	
TIPO DE ACTIVO		HARDWARE	
Tipo	**ID**	**Amenaza**	**Exposición/Vulnerabilidad**
DESASTRES NATURALES	**N.1**	Fuego	No existe sistema de alarma contra incendios. Se posee un solo extintor de solkaflam (clase c) recomendados para incendios en lugares donde se encuentren equipos eléctricos.
	N.2	Daños por agua	La infraestructura está expuesta a goteras, cuenta con averías en el techo en donde el agua de las lluvias
	N.*	Desastres naturales	La oficina de la dependencia de sistemas se encuentra en zona baja de riesgo de desastre natural de origen volcánico debido a su cercanía con el volcán nevado del Tolima.

Tabla 31. Estimación de la vulnerabilidad activo servidor plataforma RYCA V.2.0. (Continuación)

DE ORIGEN INDUSTRIAL	**I.1**	Fuego	No existe sistema de alarma contra incendios. Se posee un solo extintor de solkaflam (clase c) recomendados para incendios en lugares donde se encuentren equipos eléctricos.
	I.2	Daños por agua	La concentración del líquido sobrante por parte del aire acondicionado causaría daños en los equipos.
	I.*	Desastres industriales	No hay exposición o vulnerabilidad, por parte de esta amenaza.
	I.3	Contaminación mecánica	No hay exposición o vulnerabilidad, por parte de esta amenaza.
	I.4	Contaminación electromagnética	No hay exposición o vulnerabilidad, por parte de esta amenaza.
	I.5	Avería de origen físico o lógico	La manipulación por parte de cada uno de los componentes encontrados en la dependencia, como también por defectos de los componentes desde fabrica
	I.6	Corte del suministro eléctrico	Amenaza debida a factores externos, a clemencias de tipo naturales como lluvias u otros.
	I.7	Condiciones inadecuadas de temperatura o humedad	No se cuenta con una infraestructura adecuada para soportar los defectos del sistema de refrigeración.
	I.11	Emanaciones electromagnéticas	No hay exposición o vulnerabilidad, por parte de esta amenaza.
ERRORES Y FALLOS	**E.2**	Errores del administrador	Pérdida total o parcial del tiempo de ejecución de sus actividades, dependiendo de la gravedad del asunto.

Tabla 31. Estimación de la vulnerabilidad activo servidor plataforma RYCA V.2.0. (Continuación)

	E.23	Errores de mantenimiento / actualización de equipos(hardware)	Perjuicio a la mantenibilidad del sistema de información.
	E.24	Caída del sistema por agotamiento de recursos	Saturación del sistema informático.
	E.25	Perdida de equipos (Robo)	Recuperación de soportes reciclados o desechados.
ATAQUES INTENCIONADOS	**A.6**	Abuso de privilegios de acceso	Abuso de cada uno de los derechos otorgados.
	A.7	Uso no previsto	Implementación de recursos (económicos y de tiempo) en actividades no relacionadas.
	A.11	Acceso no autorizado	Uso ilícito del hardware
	A.23	Manipulación de los equipos	Sabotaje del hardware.
	A.24	Denegación de servicio	Saturación del sistema de información.
	A.25	Robo	Robo de porte de la información, puede esta ser física o digital.
	A.26	Ataque destructivo	Destrucción de los contenedores de la información, en recipientes físicos y lógicos.

Fuente: Autoría propia

Tabla 32. Estimación de la vulnerabilidad activo servidor plataforma RYCA V.1

ACTIVO TI		SERVIDOR PLATAFORMA RYCA V.1	
ADMINISTRADOR		PIMIENTO CARDENAS WILSON MAURICIO	
TIPO DE ACTIVO		HARDWARE	
Tipo	**ID**	**Amenaza**	**Exposición/Vulnerabilidad**

Tabla 32. Estimación de la vulnerabilidad activo servidor plataforma RYCA V.1. (Continuación)

DESASTRES NATURALES	**N.1**	Fuego	No existe sistema de alarma contra incendios. Se posee un solo extintor de solkaflam (clase c) recomendados para incendios en lugares donde se encuentren equipos eléctricos.
	N.2	Daños por agua	La infraestructura está expuesta a goteras, cuenta con averías en el techo en donde el agua de las lluvias
	N.*	Desastres naturales	La oficina de la dependencia de sistemas se encuentra en zona baja de riesgo de desastre natural de origen volcánico debido a su cercanía con el volcán nevado del Tolima.
DE ORIGEN INDUSTRIAL	**I.1**	Fuego	No existe sistema de alarma contra incendios. Se posee un solo extintor de solkaflam (clase c) recomendados para incendios en lugares donde se encuentren equipos eléctricos.
	I.2	Daños por agua	La concentración del líquido sobrante por parte del aire acondicionado causaría daños en los equipos.
	I.*	Desastres industriales	No hay exposición o vulnerabilidad, por parte de esta amenaza.
	I.3	Contaminación mecánica	No hay exposición o vulnerabilidad, por parte de esta amenaza.
	I.4	Contaminación electromagnética	No hay exposición o vulnerabilidad, por parte de esta amenaza.
	I.5	Avería de origen físico o lógico	La manipulación por parte de cada uno de los componentes encontrados en la dependencia, como también por defectos de los componentes desde fabrica

Tabla 32. Estimación de la vulnerabilidad activo servidor plataforma RYCA V.1. (Continuación)

	I.6	Corte del suministro eléctrico	Amenaza debida a factores externos, a clemencias de tipo naturales como lluvias u otros.
	I.7	Condiciones inadecuadas de temperatura o humedad	No se cuenta con una infraestructura adecuada para soportar los defectos del sistema de refrigeración.
	I.11	Emanaciones electromagnéticas	No hay exposición o vulnerabilidad, por parte de esta amenaza.
ERRORES Y FALLOS NO INTENCIONADOS	**E.2**	Errores del administrador	Pérdida total o parcial del tiempo de ejecución de sus actividades, dependiendo de la gravedad del asunto.
	E.23	Errores de mantenimiento / actualización de equipos(hardware)	Perjuicio a la mantenibilidad del sistema de información.
	E.24	Caída del sistema por agotamiento de recursos	Saturación del sistema informático.
	E.25	Perdida de equipos (Robo)	Recuperación de soportes reciclados o desechados.
ATAQUES INTENCIONADOS	**A.6**	Abuso de privilegios de acceso	Abuso de cada uno de los derechos otorgados.
	A.7	Uso no previsto	Implementación de recursos (económicos y de tiempo) en actividades no relacionadas.
	A.11	Acceso no autorizado	Uso ilícito del hardware
	A.23	Manipulación de los equipos	Sabotaje del hardware.

Tabla 32. Estimación de la vulnerabilidad activo servidor plataforma RYCA V.1. (Continuación)

	A.24	Denegación de servicio	Saturación del sistema de información.
	A.25	Robo	Robo de porte de la información, puede esta ser física o digital.
	A.26	Ataque destructivo	Destrucción de los contenedores de la información, en recipientes físicos y lógicos.

Fuente: Autoría propia

Tabla 33. Estimación de la vulnerabilidad activo servidor de base de datos ITFIP

ACTIVO TI		SERVIDOR DE BASE DE DATOS ITFIP	
ADMINISTRADOR		PIMIENTO CARDENAS WILSON MAURICIO	
TIPO DE ACTIVO		HARDWARE	
Tipo	**ID**	**Amenaza**	**Exposición/Vulnerabilidad**
DESASTRES NATURALES	**N.1**	Fuego	No existe sistema de alarma contra incendios. Se posee un solo extintor de solkaflam (clase c) recomendados para incendios en lugares donde se encuentren equipos eléctricos.
	N.2	Daños por agua	La infraestructura está expuesta a goteras, cuenta con averías en el techo en donde el agua de las lluvias
	N.*	Desastres naturales	La oficina de la dependencia de sistemas se encuentra en zona baja de riesgo de desastre natural de origen volcánico debido a su cercanía con el volcán nevado del Tolima.
DE ORIGEN INDUSTRIAL	**I.1**	Fuego	No existe sistema de alarma contra incendios. Se posee un solo extintor de solkaflam (clase c) recomendados para incendios en lugares donde se encuentren equipos eléctricos.

Tabla 33. Estimación de la vulnerabilidad activo servidor de base de datos ITFIP. (Continuación)

	I.2	Daños por agua	La concentración del líquido sobrante por parte del aire acondicionado causaría daños en los equipos.
	I.*	Desastres industriales	No hay exposición o vulnerabilidad, por parte de esta amenaza.
	I.3	Contaminación mecánica	No hay exposición o vulnerabilidad, por parte de esta amenaza.
	I.4	Contaminación electromagnética	No hay exposición o vulnerabilidad, por parte de esta amenaza.
	I.5	Avería de origen físico o lógico	La manipulación por parte de cada uno de los componentes encontrados en la dependencia, como también por defectos de los componentes desde fabrica
	I.6	Corte del suministro eléctrico	Amenaza debida a factores externos, a clemencias de tipo naturales como lluvias u otros.
	I.7	Condiciones inadecuadas de temperatura o humedad	No se cuenta con una infraestructura adecuada para soportar los defectos del sistema de refrigeración.
	I.11	Emanaciones electromagnéticas	No hay exposición o vulnerabilidad, por parte de esta amenaza.
ERRORES Y FALLOS NO INTENCIONADOS	**E.2**	Errores del administrador	Pérdida total o parcial del tiempo de ejecución de sus actividades, dependiendo de la gravedad del asunto.
	E.23	Errores de mantenimiento / actualización de equipos(hardware)	Perjuicio a la mantenibilidad del sistema de información.

Tabla 33. Estimación de la vulnerabilidad activo servidor de base de datos ITFIP. (Continuación)

	E.24	Caída del sistema por agotamiento de recursos	Saturación del sistema informático.
	E.25	Perdida de equipos (Robo)	Recuperación de soportes reciclados o desechados.
ATAQUES INTENCIONADOS	**A.6**	Abuso de privilegios de acceso	Abuso de cada uno de los derechos otorgados.
	A.7	Uso no previsto	Implementación de recursos (económicos y de tiempo) en actividades no relacionadas.
	A.11	Acceso no autorizado	Uso ilícito del hardware
	A.23	Manipulación de los equipos	Sabotaje del hardware.
	A.24	Denegación de servicio	Saturación del sistema de información.
	A.25	Robo	Robo de porte de la información, puede esta ser física o digital.
	A.26	Ataque destructivo	Destrucción de los contenedores de la información, en recipientes físicos y lógicos.

Fuente: Autoría propia

Tabla 34. Estimación de la vulnerabilidad activo servidor firewall Fortigate

ACTIVO TI		SERVIDOR FIREWALL FORTIGATE	
ADMINISTRADOR		PIMIENTO CARDENAS WILSON MAURICIO	
TIPO DE ACTIVO		HARDWARE	
Tipo	**ID**	**Amenaza**	**Exposición/Vulnerabilidad**
DESASTRES NATURA	**N.1**	Fuego	No existe sistema de alarma contra incendios. Se posee un solo extintor de solkaflam (clase c) recomendados para

Tabla 34. Estimación de la vulnerabilidad activo servidor firewall Fortigate. (Continuación)

			incendios en lugares donde se encuentren equipos eléctricos.
	N.2	Daños por agua	La infraestructura está expuesta a goteras, cuenta con averías en el techo en donde el agua de las lluvias
	N.*	Desastres naturales	La oficina de la dependencia de sistemas se encuentra en zona baja de riesgo de desastre natural de origen volcánico debido a su cercanía con el volcán nevado del Tolima.
DE ORIGEN INDUSTRIAL	**I.1**	Fuego	No existe sistema de alarma contra incendios. Se posee un solo extintor de solkaflam (clase c) recomendados para incendios en lugares donde se encuentren equipos eléctricos.
	I.2	Daños por agua	La concentración del líquido sobrante por parte del aire acondicionado causaría daños en los equipos.
	I.*	Desastres industriales	No hay exposición o vulnerabilidad, por parte de esta amenaza.
	I.3	Contaminación mecánica	No hay exposición o vulnerabilidad, por parte de esta amenaza.
	I.4	Contaminación electromagnética	No hay exposición o vulnerabilidad, por parte de esta amenaza.
	I.5	Avería de origen físico o lógico	La manipulación por parte de cada uno de los componentes encontrados en la dependencia, como también por defectos de los componentes desde fabrica
	I.6	Corte del suministro eléctrico	Amenaza debida a factores externos, a clemencias de tipo naturales como lluvias u otros.

Tabla 34. Estimación de la vulnerabilidad activo servidor firewall Fortigate. (Continuación)

	I.7	Condiciones inadecuadas de temperatura o humedad	No se cuenta con una infraestructura adecuada para soportar los defectos del sistema de refrigeración.
	I.11	Emanaciones electromagnéticas	No hay exposición o vulnerabilidad, por parte de esta amenaza.
ERRORES Y FALLOS NO INTENCIONADOS	**E.2**	Errores del administrador	Pérdida total o parcial del tiempo de ejecución de sus actividades, dependiendo de la gravedad del asunto.
	E.23	Errores de mantenimiento / actualización de equipos(hardware)	Perjuicio a la mantenibilidad del sistema de información.
	E.24	Caída del sistema por agotamiento de recursos	Saturación del sistema informático.
	E.25	Perdida de equipos (Robo)	Recuperación de soportes reciclados o desechados.
ATAQUES INTENCIONADOS	**A.6**	Abuso de privilegios de acceso	Abuso de cada uno de los derechos otorgados.
	A.7	Uso no previsto	Implementación de recursos (económicos y de tiempo) en actividades no relacionadas.
	A.11	Acceso no autorizado	Uso ilícito del hardware
	A.23	Manipulación de los equipos	Sabotaje del hardware.
	A.24	Denegación de servicio	Saturación del sistema de información.

Tabla 34. Estimación de la vulnerabilidad activo servidor firewall Fortigate. (Continuación)

	A.25	Robo	Robo de porte de la información, puede esta ser física o digital.
	A.26	Ataque destructivo	Destrucción de los contenedores de la información, en recipientes físicos y lógicos.

Fuente: Autoría propia

Tabla 35. Estimación de la vulnerabilidad activo servidor contable SIIGO

ACTIVO TI	SERVIDOR CONTABLE SIIGO		
ADMINISTRADOR	PIMIENTO CARDENAS WILSON MAURICIO		
TIPO DE ACTIVO	HARDWARE		
Tipo	**ID**	**Amenaza**	**Exposición/Vulnerabilidad**
DESASTRES NATURALES	**N.1**	Fuego	No existe sistema de alarma contra incendios. Se posee un solo extintor de solkaflam (clase c) recomendados para incendios en lugares donde se encuentren equipos eléctricos.
	N.2	Daños por agua	La infraestructura está expuesta a goteras, cuenta con averías en el techo en donde el agua de las lluvias
	N.*	Desastres naturales	La oficina de la dependencia de sistemas se encuentra en zona baja de riesgo de desastre natural de origen volcánico debido a su cercanía con el volcán nevado del Tolima.
ORIGEN INDUSTRIAL DE	**I.1**	Fuego	No existe sistema de alarma contra incendios. Se posee un solo extintor de solkaflam (clase c) recomendados para incendios en lugares donde se encuentren equipos eléctricos.
	I.2	Daños por agua	La concentración del líquido sobrante por parte del aire acondicionado causaría daños en los equipos.

Tabla 35. Estimación de la vulnerabilidad activo servidor contable SIIGO. (Continuación)

	I.*	Desastres industriales	No hay exposición o vulnerabilidad, por parte de esta amenaza.
	I.3	Contaminación mecánica	No hay exposición o vulnerabilidad, por parte de esta amenaza.
	I.4	Contaminación electromagnética	No hay exposición o vulnerabilidad, por parte de esta amenaza.
	I.5	Avería de origen físico o lógico	La manipulación por parte de cada uno de los componentes encontrados en la dependencia, como también por defectos de los componentes desde fabrica
	I.6	Corte del suministro eléctrico	Amenaza debida a factores externos, a clemencias de tipo naturales como lluvias u otros.
	I.7	Condiciones inadecuadas de temperatura o humedad	No se cuenta con una infraestructura adecuada para soportar los defectos del sistema de refrigeración.
	I.11	Emanaciones electromagnéticas	No hay exposición o vulnerabilidad, por parte de esta amenaza.
ERRORES Y FALLOS NO INTENCIONADOS	**E.2**	Errores del administrador	Pérdida total o parcial del tiempo de ejecución de sus actividades, dependiendo de la gravedad del asunto.
	E.23	Errores de mantenimiento / actualización de equipos(hardware)	Perjuicio a la mantenibilidad del sistema de información.
	E.24	Caída del sistema por agotamiento de recursos	Saturación del sistema informático.
	E.25	Perdida de equipos (Robo)	Recuperación de soportes reciclados o desechados.

Tabla 35. Estimación de la vulnerabilidad activo servidor contable SIIGO. (Continuación)

ATAQUES INTENCIONADOS	**A.6**	Abuso de privilegios de acceso	Abuso de cada uno de los derechos otorgados.
	A.7	Uso no previsto	Implementación de recursos (económicos y de tiempo) en actividades no relacionadas.
	A.11	Acceso no autorizado	Uso ilícito del hardware
	A.23	Manipulación de los equipos	Sabotaje del hardware.
	A.24	Denegación de servicio	Saturación del sistema de información.
	A.25	Robo	Robo de porte de la información, puede esta ser física o digital.
	A.26	Ataque destructivo	Destrucción de los contenedores de la información, en recipientes físicos y lógicos.

Fuente: Autoría propia

Tabla 36. Estimación de la vulnerabilidad activo servidor de pruebas “desarrollito”

ACTIVO TI		SERVIDOR DE PRUEBAS “DESARROLLITO”	
ADMINISTRADOR		PIMIENTO CARDENAS WILSON MAURICIO	
TIPO DE ACTIVO		HARDWARE	
Tipo	**ID**	**Amenaza**	**Exposición/Vulnerabilidad**
DESASTRES NATURALES	**N.1**	Fuego	No existe sistema de alarma contra incendios. Se posee un solo extintor de solkaflam (clase c) recomendados para incendios en lugares donde se encuentren equipos eléctricos.
	N.2	Daños por agua	La infraestructura está expuesta a goteras, cuenta con averías en el techo en donde el agua de las lluvias

Tabla 36. Estimación de la vulnerabilidad activo servidor de pruebas “desarrollito”. (Continuación)

	N.*	Desastres naturales	La oficina de la dependencia de sistemas se encuentra en zona baja de riesgo de desastre natural de origen volcánico debido a su cercanía con el volcán nevado del Tolima.
DE ORIGEN INDUSTRIAL	**I.1**	Fuego	No existe sistema de alarma contra incendios. Se posee un solo extintor de solkaflam (clase c) recomendados para incendios en lugares donde se encuentren equipos eléctricos.
	I.2	Daños por agua	La concentración del líquido sobrante por parte del aire acondicionado causaría daños en los equipos.
	I.*	Desastres industriales	No hay exposición o vulnerabilidad, por parte de esta amenaza.
	I.3	Contaminación mecánica	No hay exposición o vulnerabilidad, por parte de esta amenaza.
	I.4	Contaminación electromagnética	No hay exposición o vulnerabilidad, por parte de esta amenaza.
	I.5	Avería de origen físico o lógico	La manipulación por parte de cada uno de los componentes encontrados en la dependencia, como también por defectos de los componentes desde fabrica
	I.6	Corte del suministro eléctrico	Amenaza debida a factores externos, a clemencias de tipo naturales como lluvias u otros.
	I.7	Condiciones inadecuadas de temperatura o humedad	No se cuenta con una infraestructura adecuada para soportar los defectos del sistema de refrigeración.
	I.11	Emanaciones electromagnéticas	No hay exposición o vulnerabilidad, por parte de esta amenaza.

Tabla 36. Estimación de la vulnerabilidad activo servidor de pruebas “desarrollito”. (Continuación)

ERRORES Y FALLOS NO INTENCIONADOS	**E.2**	Errores del administrador	Pérdida total o parcial del tiempo de ejecución de sus actividades, dependiendo de la gravedad del asunto.
	E.23	Errores de mantenimiento / actualización de equipos(hardware)	Perjuicio a la mantenibilidad del sistema de información.
	E.24	Caída del sistema por agotamiento de recursos	Saturación del sistema informático.
	E.25	Perdida de equipos (Robo)	Recuperación de soportes reciclados o desechados.
ATAQUES INTENCIONADOS	**A.6**	Abuso de privilegios de acceso	Abuso de cada uno de los derechos otorgados.
	A.7	Uso no previsto	Implementación de recursos (económicos y de tiempo) en actividades no relacionadas.
	A.11	Acceso no autorizado	Uso ilícito del hardware
	A.23	Manipulación de los equipos	Sabotaje del hardware.
	A.24	Denegación de servicio	Saturación del sistema de información.
	A.25	Robo	Robo de porte de la información, puede esta ser física o digital.
	A.26	Ataque destructivo	Destrucción de los contenedores de la información, en recipientes físicos y lógicos.

Fuente: Autoría propia

Tabla 37. Estimación de la vulnerabilidad activo servidor de copias de seguridad de la información del ITFIP

ACTIVO TI		SERVIDOR DE COPIAS DE SEGURIDAD DE LA INFORMACIÓN DEL ITFIP	
ADMINISTRADOR		PIMIENTO CARDENAS WILSON MAURICIO	
TIPO DE ACTIVO		HARDWARE	
Tipo	**ID**	**Amenaza**	**Exposición/Vulnerabilidad**
DESASTRES NATURALES	**N.1**	Fuego	No existe sistema de alarma contra incendios. Se posee un solo extintor de solkaflam (clase c) recomendados para incendios en lugares donde se encuentren equipos eléctricos.
	N.2	Daños por agua	La infraestructura está expuesta a goteras, cuenta con averías en el techo en donde el agua de las lluvias
	N.*	Desastres naturales	La oficina de la dependencia de sistemas se encuentra en zona baja de riesgo de desastre natural de origen volcánico debido a su cercanía con el volcán nevado del Tolima.
DE ORIGEN INDUSTRIAL	**I.1**	Fuego	No existe sistema de alarma contra incendios. Se posee un solo extintor de solkaflam (clase c) recomendados para incendios en lugares donde se encuentren equipos eléctricos.
	I.2	Daños por agua	La concentración del líquido sobrante por parte del aire acondicionado causaría daños en los equipos.
	I.*	Desastres industriales	No hay exposición o vulnerabilidad, por parte de esta amenaza.
	I.3	Contaminación mecánica	No hay exposición o vulnerabilidad, por parte de esta amenaza.
	I.4	Contaminación electromagnética	No hay exposición o vulnerabilidad, por parte de esta amenaza.

Tabla 37. Estimación de la vulnerabilidad activo serv. de copias seguridad de infor del ITFIP. (Continuación)

	I.5	Avería de origen físico o lógico	La manipulación por parte de cada uno de los componentes encontrados en la dependencia, como también por defectos de los componentes desde fabrica
	I.6	Corte del suministro eléctrico	Amenaza debida a factores externos, a clemencias de tipo naturales como lluvias u otros.
	I.7	Condiciones inadecuadas de temperatura o humedad	No se cuenta con una infraestructura adecuada para soportar los defectos del sistema de refrigeración.
	I.11	Emanaciones electromagnéticas	No hay exposición o vulnerabilidad, por parte de esta amenaza.
ERRORES Y FALLOS NO INTENCIONADOS	**E.2**	Errores del administrador	Pérdida total o parcial del tiempo de ejecución de sus actividades, dependiendo de la gravedad del asunto.
	E.23	Errores de mantenimiento / actualización de equipos(hardware)	Perjuicio a la mantenibilidad del sistema de información.
	E.24	Caída del sistema por agotamiento de recursos	Saturación del sistema informático.
	E.25	Perdida de equipos (Robo)	Recuperación de soportes reciclados o desechados.
ATAQUES INTENCIONADOS	**A.6**	Abuso de privilegios de acceso	Abuso de cada uno de los derechos otorgados.
	A.7	Uso no previsto	Implementación de recursos (económicos y de tiempo) en actividades no relacionadas.

Tabla 37. Estimación de la vulnerabilidad activo serv. de copias seguridad de infor del ITFIP. (Continuación)

	A.11	Acceso no autorizado	Uso ilícito del hardware
	A.23	Manipulación de los equipos	Sabotaje del hardware.
	A.24	Denegación de servicio	Saturación del sistema de información.
	A.25	Robo	Robo de porte de la información, puede esta ser física o digital.
	A.26	Ataque destructivo	Destrucción de los contenedores de la información, en recipientes físicos y lógicos.

Fuente: Autoría propia Fuente: Autoría propia

Tabla 38. Estimación de la vulnerabilidad activo computador iMac Apple (3 equipos)

ACTIVO TI		COMPUTADOR IMAC APPLE (3 EQUIPOS)	
ADMINISTRADOR		PIMIENTO CARDENAS WILSON MAURICIO	
TIPO DE ACTIVO		HARDWARE	
Tipo	**ID**	**Amenaza**	**Exposición/Vulnerabilidad**
DESASTRES NATURALES	**N.1**	Fuego	No existe sistema de alarma contra incendios. Se posee un solo extintor de solkaflam (clase c) recomendados para incendios en lugares donde se encuentren equipos eléctricos.
	N.2	Daños por agua	La infraestructura está expuesta a goteras, cuenta con averías en el techo en donde el agua de las lluvias
	N.*	Desastres naturales	La oficina de la dependencia de sistemas se encuentra en zona baja de riesgo de desastre natural de origen volcánico debido a su cercanía con el volcán nevado del Tolima.

Tabla 38. Estimación de la vulnerabilidad activo computador iMac Apple (3 equipos). (Continuación)

DE ORIGEN INDUSTRIAL	**I.1**	Fuego	No existe sistema de alarma contra incendios. Se posee un solo extintor de solkaflam (clase c) recomendados para incendios en lugares donde se encuentren equipos eléctricos.
	I.2	Daños por agua	La concentración del líquido sobrante por parte del aire acondicionado causaría daños en los equipos.
	I.*	Desastres industriales	No hay exposición o vulnerabilidad, por parte de esta amenaza.
	I.3	Contaminación mecánica	No hay exposición o vulnerabilidad, por parte de esta amenaza.
	I.4	Contaminación electromagnética	No hay exposición o vulnerabilidad, por parte de esta amenaza.
	I.5	Avería de origen físico o lógico	La manipulación por parte de cada uno de los componentes encontrados en la dependencia, como también por defectos de los componentes desde fabrica
	I.6	Corte del suministro eléctrico	Amenaza debida a factores externos, a clemencias de tipo naturales como lluvias u otros.
	I.7	Condiciones inadecuadas de temperatura o humedad	No se cuenta con una infraestructura adecuada para soportar los defectos del sistema de refrigeración.
	I.11	Emanaciones electromagnéticas	No hay exposición o vulnerabilidad, por parte de esta amenaza.
ERRORES Y FALLOS	**E.2**	Errores del administrador	Pérdida total o parcial del tiempo de ejecución de sus actividades, dependiendo de la gravedad del asunto.

Tabla 38. Estimación de la vulnerabilidad activo computador iMac Apple (3 equipos). (Continuación)

	E.23	Errores de mantenimiento / actualización de equipos(hardware)	Perjuicio a la mantenibilidad del sistema de información.
	E.24	Caída del sistema por agotamiento de recursos	Saturación del sistema informático.
	E.25	Perdida de equipos (Robo)	Recuperación de soportes reciclados o desechados.
ATAQUES INTENCIONADOS	**A.6**	Abuso de privilegios de acceso	Abuso de cada uno de los derechos otorgados.
	A.7	Uso no previsto	Implementación de recursos (económicos y de tiempo) en actividades no relacionadas.
	A.11	Acceso no autorizado	Uso ilícito del hardware
	A.23	Manipulación de los equipos	Sabotaje del hardware.
	A.24	Denegación de servicio	Saturación del sistema de información.
	A.25	Robo	Robo de porte de la información, puede esta ser física o digital.
	A.26	Ataque destructivo	Destrucción de los contenedores de la información, en recipientes físicos y lógicos.

Fuente: Autoría propia

Tabla 39. Estimación de la vulnerabilidad activo computadores hp all-one pro (18 equipos)

ACTIVO TI		COMPUTADORES HP ALL-ONE PRO (18 EQUIPOS)	
ADMINISTRADOR		PIMIENTO CARDENAS WILSON MAURICIO	
TIPO DE ACTIVO		HARDWARE	
Tipo	**ID**	**Amenaza**	**Exposición/Vulnerabilidad**

Tabla 39. Estimación de la vulnerabilidad activo computadores hp all-one pro (18 equipos). (Continuación)

DESASTRES NATURALES	**N.1**	Fuego	No existe sistema de alarma contra incendios. Se posee un solo extintor de solkaflam (clase c) recomendados para incendios en lugares donde se encuentren equipos eléctricos.
	N.2	Daños por agua	La infraestructura está expuesta a goteras, cuenta con averías en el techo en donde el agua de las lluvias
	N.*	Desastres naturales	La oficina de la dependencia de sistemas se encuentra en zona baja de riesgo de desastre natural de origen volcánico debido a su cercanía con el volcán nevado del Tolima.
DE ORIGEN INDUSTRIAL	**I.1**	Fuego	No existe sistema de alarma contra incendios. Se posee un solo extintor de solkaflam (clase c) recomendados para incendios en lugares donde se encuentren equipos eléctricos.
	I.2	Daños por agua	La concentración del líquido sobrante por parte del aire acondicionado causaría daños en los equipos.
	I.*	Desastres industriales	No hay exposición o vulnerabilidad, por parte de esta amenaza.
	I.3	Contaminación mecánica	No hay exposición o vulnerabilidad, por parte de esta amenaza.
	I.4	Contaminación electromagnética	No hay exposición o vulnerabilidad, por parte de esta amenaza.
	I.5	Avería de origen físico o lógico	La manipulación por parte de cada uno de los componentes encontrados en la dependencia, como también por defectos de los componentes desde fabrica

Tabla 39. Estimación de la vulnerabilidad activo computadores hp all-one pro (18 equipos). (Continuación)

	I.6	Corte del suministro eléctrico	Amenaza debida a factores externos, a clemencias de tipo naturales como lluvias u otros.
	I.7	Condiciones inadecuadas de temperatura o humedad	No se cuenta con una infraestructura adecuada para soportar los defectos del sistema de refrigeración.
	I.11	Emanaciones electromagnéticas	No hay exposición o vulnerabilidad, por parte de esta amenaza.
ERRORES Y FALLOS NO INTENCIONADOS	**E.2**	Errores del administrador	Pérdida total o parcial del tiempo de ejecución de sus actividades, dependiendo de la gravedad del asunto.
	E.23	Errores de mantenimiento / actualización de equipos(hardware)	Perjuicio a la mantenibilidad del sistema de información.
	E.24	Caída del sistema por agotamiento de recursos	Saturación del sistema informático.
	E.25	Perdida de equipos (Robo)	Recuperación de soportes reciclados o desechados.
ATAQUES INTENCIONADOS	**A.6**	Abuso de privilegios de acceso	Abuso de cada uno de los derechos otorgados.
	A.7	Uso no previsto	Implementación de recursos (económicos y de tiempo) en actividades no relacionadas.
	A.11	Acceso no autorizado	Uso ilícito del hardware
	A.23	Manipulación de los equipos	Sabotaje del hardware.

Tabla 39. Estimación de la vulnerabilidad activo computadores hp all-one pro (18 equipos). (Continuación)

	A.24	Denegación de servicio	Saturación del sistema de información.
	A.25	Robo	Robo de porte de la información, puede esta ser física o digital.
	A.26	Ataque destructivo	Destrucción de los contenedores de la información, en recipientes físicos y lógicos.

Fuente: Autoría propia

Tabla 40. Estimación de la vulnerabilidad activo portátil Toshiba (16 equipos)

ACTIVO TI		PORTÁTIL TOSHIBA (16 EQUIPOS)	
ADMINISTRADOR		PIMIENTO CARDENAS WILSON MAURICIO	
TIPO DE ACTIVO		HARDWARE	
Tipo	**ID**	**Amenaza**	**Exposición/Vulnerabilidad**
DESASTRES NATURALES	**N.1**	Fuego	No existe sistema de alarma contra incendios. Se posee un solo extintor de solkaflam (clase c) recomendados para incendios en lugares donde se encuentren equipos eléctricos.
	N.2	Daños por agua	La infraestructura está expuesta a goteras, cuenta con averías en el techo en donde el agua de las lluvias
	N.*	Desastres naturales	La oficina de la dependencia de sistemas se encuentra en zona baja de riesgo de desastre natural de origen volcánico debido a su cercanía con el volcán nevado del Tolima.
DE ORIGEN INDUSTRIAL	**I.1**	Fuego	No existe sistema de alarma contra incendios. Se posee un solo extintor de solkaflam (clase c) recomendados para incendios en lugares donde se encuentren equipos eléctricos.

Tabla 40. Estimación de la vulnerabilidad activo portátil Toshiba (16 equipos). (Continuación)

	I.2	Daños por agua	La concentración del líquido sobrante por parte del aire acondicionado causaría daños en los equipos.
	I.*	Desastres industriales	No hay exposición o vulnerabilidad, por parte de esta amenaza.
	I.3	Contaminación mecánica	No hay exposición o vulnerabilidad, por parte de esta amenaza.
	I.4	Contaminación electromagnética	No hay exposición o vulnerabilidad, por parte de esta amenaza.
	I.5	Avería de origen físico o lógico	La manipulación por parte de cada uno de los componentes encontrados en la dependencia, como también por defectos de los componentes desde fabrica
	I.6	Corte del suministro eléctrico	Amenaza debida a factores externos, a clemencias de tipo naturales como lluvias u otros.
	I.7	Condiciones inadecuadas de temperatura o humedad	No se cuenta con una infraestructura adecuada para soportar los defectos del sistema de refrigeración.
	I.11	Emanaciones electromagnéticas	No hay exposición o vulnerabilidad, por parte de esta amenaza.
ERRORES Y FALLOS NO INTENCIONADOS	**E.2**	Errores del administrador	Pérdida total o parcial del tiempo de ejecución de sus actividades, dependiendo de la gravedad del asunto.
	E.23	Errores de mantenimiento / actualización de equipos(hardware)	Perjuicio a la mantenibilidad del sistema de información.

Tabla 40. Estimación de la vulnerabilidad activo portátil Toshiba (16 equipos). (Continuación)

	E.24	Caída del sistema por agotamiento de recursos	Saturación del sistema informático.
	E.25	Perdida de equipos (Robo)	Recuperación de soportes reciclados o desechados.
ATAQUES INTENCIONADOS	**A.6**	Abuso de privilegios de acceso	Abuso de cada uno de los derechos otorgados.
	A.7	Uso no previsto	Implementación de recursos (económicos y de tiempo) en actividades no relacionadas.
	A.11	Acceso no autorizado	Uso ilícito del hardware
	A.23	Manipulación de los equipos	Sabotaje del hardware.
	A.24	Denegación de servicio	Saturación del sistema de información.
	A.25	Robo	Robo de porte de la información, puede esta ser física o digital.
	A.26	Ataque destructivo	Destrucción de los contenedores de la información, en recipientes físicos y lógicos.

Fuente: Autoría propia

Tabla 41. Estimación de la vulnerabilidad activo Tablet negra 9" (1 equipo)

ACTIVO TI		TABLET NEGRA 9" (1 EQUIPO)	
ADMINISTRADOR		PIMIENTO CARDENAS WILSON MAURICIO	
TIPO DE ACTIVO		HARDWARE	
Tipo	**ID**	**Amenaza**	**Exposición/Vulnerabilidad**
DESASTRES NATURA	**N.1**	Fuego	No existe sistema de alarma contra incendios. Se posee un solo extintor de solkaflam (clase c) recomendados para

Tabla 41. Estimación de la vulnerabilidad activo Tablet negra 9" (1 equipo). (Continuación)

			incendios en lugares donde se encuentren equipos eléctricos.
	N.2	Daños por agua	La infraestructura está expuesta a goteras, cuenta con averías en el techo en donde el agua de las lluvias
	N.*	Desastres naturales	La oficina de la dependencia de sistemas se encuentra en zona baja de riesgo de desastre natural de origen volcánico debido a su cercanía con el volcán nevado del Tolima.
DE ORIGEN INDUSTRIAL	**I.1**	Fuego	No existe sistema de alarma contra incendios. Se posee un solo extintor de solkaflam (clase c) recomendados para incendios en lugares donde se encuentren equipos eléctricos.
	I.2	Daños por agua	La concentración del líquido sobrante por parte del aire acondicionado causaría daños en los equipos.
	I.*	Desastres industriales	No hay exposición o vulnerabilidad, por parte de esta amenaza.
	I.3	Contaminación mecánica	No hay exposición o vulnerabilidad, por parte de esta amenaza.
	I.4	Contaminación electromagnética	No hay exposición o vulnerabilidad, por parte de esta amenaza.
	I.5	Avería de origen físico o lógico	La manipulación por parte de cada uno de los componentes encontrados en la dependencia, como también por defectos de los componentes desde fabrica
	I.6	Corte del suministro eléctrico	Amenaza debida a factores externos, a clemencias de tipo naturales como lluvias u otros.

Tabla 41. Estimación de la vulnerabilidad activo Tablet negra 9" (1 equipo). (Continuación)

	I.7	Condiciones inadecuadas de temperatura o humedad	No se cuenta con una infraestructura adecuada para soportar los defectos del sistema de refrigeración.
	I.11	Emanaciones electromagnéticas	No hay exposición o vulnerabilidad, por parte de esta amenaza.
ERRORES Y FALLOS NO INTENCIONADOS	**E.2**	Errores del administrador	Pérdida total o parcial del tiempo de ejecución de sus actividades, dependiendo de la gravedad del asunto.
	E.23	Errores de mantenimiento / actualización de equipos(hardware)	Perjuicio a la mantenibilidad del sistema de información.
	E.24	Caída del sistema por agotamiento de recursos	Saturación del sistema informático.
	E.25	Perdida de equipos (Robo)	Recuperación de soportes reciclados o desechados.
ATAQUES INTENCIONADOS	**A.6**	Abuso de privilegios de acceso	Abuso de cada uno de los derechos otorgados.
	A.7	Uso no previsto	Implementación de recursos (económicos y de tiempo) en actividades no relacionadas.
	A.11	Acceso no autorizado	Uso ilícito del hardware
	A.23	Manipulación de los equipos	Sabotaje del hardware.
	A.24	Denegación de servicio	Saturación del sistema de información.

Tabla 41. Estimación de la vulnerabilidad activo Tablet negra 9" (1 equipo). (Continuación)

	A.25	Robo	Robo de porte de la información, puede esta ser física o digital.
	A.26	Ataque destructivo	Destrucción de los contenedores de la información, en recipientes físicos y lógicos.

Fuente: Autoría propia

Tabla 42. Estimación de la vulnerabilidad activo computador iMac Apple (3 equipos)

ACTIVO TI		COMPUTADOR IMAC APPLE (3 EQUIPOS)	
ADMINISTRADOR		PIMIENTO CARDENAS WILSON MAURICIO	
TIPO DE ACTIVO		HARDWARE	
Tipo	**ID**	**Amenaza**	**Exposición/Vulnerabilidad**
DESASTRES NATURALES	**N.1**	Fuego	No existe sistema de alarma contra incendios. Se posee un solo extintor de solkaflam (clase c) recomendados para incendios en lugares donde se encuentren equipos eléctricos.
	N.2	Daños por agua	La infraestructura está expuesta a goteras, cuenta con averías en el techo en donde el agua de las lluvias
	N.*	Desastres naturales	La oficina de la dependencia de sistemas se encuentra en zona baja de riesgo de desastre natural de origen volcánico debido a su cercanía con el volcán nevado del Tolima.
ORIGEN INDUSTRIAL DE	**I.1**	Fuego	No existe sistema de alarma contra incendios. Se posee un solo extintor de solkaflam (clase c) recomendados para incendios en lugares donde se encuentren equipos eléctricos.
	I.2	Daños por agua	La concentración del líquido sobrante por parte del aire acondicionado causaría daños en los equipos.

Tabla 42. Estimación de la vulnerabilidad activo computador iMac Apple (3 equipos). (Continuación)

	I.*	Desastres industriales	No hay exposición o vulnerabilidad, por parte de esta amenaza.
	I.3	Contaminación mecánica	No hay exposición o vulnerabilidad, por parte de esta amenaza.
	I.4	Contaminación electromagnética	No hay exposición o vulnerabilidad, por parte de esta amenaza.
	I.5	Avería de origen físico o lógico	La manipulación por parte de cada uno de los componentes encontrados en la dependencia, como también por defectos de los componentes desde fabrica
	I.6	Corte del suministro eléctrico	Amenaza debida a factores externos, a clemencias de tipo naturales como lluvias u otros.
	I.7	Condiciones inadecuadas de temperatura o humedad	No se cuenta con una infraestructura adecuada para soportar los defectos del sistema de refrigeración.
	I.11	Emanaciones electromagnéticas	No hay exposición o vulnerabilidad, por parte de esta amenaza.
ERRORES Y FALLOS NO INTENCIONADOS	**E.2**	Errores del administrador	Pérdida total o parcial del tiempo de ejecución de sus actividades, dependiendo de la gravedad del asunto.
	E.23	Errores de mantenimiento / actualización de equipos(hardware)	Perjuicio a la mantenibilidad del sistema de información.
	E.24	Caída del sistema por agotamiento de recursos	Saturación del sistema informático.
	E.25	Perdida de equipos (Robo)	Recuperación de soportes reciclados o desechados.

Tabla 42. Estimación de la vulnerabilidad activo computador iMac Apple (3 equipos). (Continuación)

ATAQUES INTENCIONADOS	**A.6**	Abuso de privilegios de acceso	Abuso de cada uno de los derechos otorgados.
	A.7	Uso no previsto	Implementación de recursos (económicos y de tiempo) en actividades no relacionadas.
	A.11	Acceso no autorizado	Uso ilícito del hardware
	A.23	Manipulación de los equipos	Sabotaje del hardware.
	A.24	Denegación de servicio	Saturación del sistema de información.
	A.25	Robo	Robo de porte de la información, puede esta ser física o digital.
	A.26	Ataque destructivo	Destrucción de los contenedores de la información, en recipientes físicos y lógicos.

Fuente: Autoría propia

Tabla 43. Estimación de la vulnerabilidad activo memoria USB

ACTIVO TI		MEMORIA USB	
ADMINISTRADOR		PIMIENTO CARDENAS WILSON MAURICIO	
TIPO DE ACTIVO		HARDWARE	
Tipo	**ID**	**Amenaza**	**Exposición/Vulnerabilidad**
DESASTRES NATURALES	**N.1**	Fuego	No existe sistema de alarma contra incendios. Se posee un solo extintor de solkaflam (clase c) recomendados para incendios en lugares donde se encuentren equipos eléctricos.
	N.2	Daños por agua	La infraestructura está expuesta a goteras, cuenta con averías en el techo en donde el agua de las lluvias

Tabla 43. Estimación de la vulnerabilidad activo memoria USB. (Continuación)

	N.*	Desastres naturales	La oficina de la dependencia de sistemas se encuentra en zona baja de riesgo de desastre natural de origen volcánico debido a su cercanía con el volcán nevado del Tolima.
DE ORIGEN INDUSTRIAL	**I.1**	Fuego	No existe sistema de alarma contra incendios. Se posee un solo extintor de solkaflam (clase c) recomendados para incendios en lugares donde se encuentren equipos eléctricos.
	I.2	Daños por agua	La concentración del líquido sobrante por parte del aire acondicionado causaría daños en los equipos.
	I.*	Desastres industriales	No hay exposición o vulnerabilidad, por parte de esta amenaza.
	I.3	Contaminación mecánica	No hay exposición o vulnerabilidad, por parte de esta amenaza.
	I.4	Contaminación electromagnética	No hay exposición o vulnerabilidad, por parte de esta amenaza.
	I.5	Avería de origen físico o lógico	La manipulación por parte de cada uno de los componentes encontrados en la dependencia, como también por defectos de los componentes desde fabrica
	I.6	Corte del suministro eléctrico	Amenaza debida a factores externos, a clemencias de tipo naturales como lluvias u otros.
	I.7	Condiciones inadecuadas de temperatura o humedad	No se cuenta con una infraestructura adecuada para soportar los defectos del sistema de refrigeración.
	I.11	Emanaciones electromagnéticas	No hay exposición o vulnerabilidad, por parte de esta amenaza.

Tabla 43. Estimación de la vulnerabilidad activo memoria USB. (Continuación)

ERRORES Y FALLOS NO INTENCIONADOS	**E.2**	Errores del administrador	Pérdida total o parcial del tiempo de ejecución de sus actividades, dependiendo de la gravedad del asunto.
	E.23	Errores de mantenimiento / actualización de equipos(hardware)	Perjuicio a la mantenibilidad del sistema de información.
	E.24	Caída del sistema por agotamiento de recursos	Saturación del sistema informático.
	E.25	Perdida de equipos (Robo)	Recuperación de soportes reciclados o desechados.
ATAQUES INTENCIONADOS	**A.6**	Abuso de privilegios de acceso	Abuso de cada uno de los derechos otorgados.
	A.7	Uso no previsto	Implementación de recursos (económicos y de tiempo) en actividades no relacionadas.
	A.11	Acceso no autorizado	Uso ilícito del hardware
	A.23	Manipulación de los equipos	Sabotaje del hardware.
	A.24	Denegación de servicio	Saturación del sistema de información.
	A.25	Robo	Robo de porte de la información, puede esta ser física o digital.
	A.26	Ataque destructivo	Destrucción de los contenedores de la información, en recipientes físicos y lógicos.

Fuente: Autoría propia

Tabla 44. Estimación de la vulnerabilidad activo discos duros

ACTIVO TI		DISCOS DUROS	
ADMINISTRADOR		PIMIENTO CARDENAS WILSON MAURICIO	
TIPO DE ACTIVO		HARDWARE	
Tipo	**ID**	**Amenaza**	**Exposición/Vulnerabilidad**
DESASTRES NATURALES	**N.1**	Fuego	No existe sistema de alarma contra incendios. Se posee un solo extintor de solkaflam (clase c) recomendados para incendios en lugares donde se encuentren equipos eléctricos.
	N.2	Daños por agua	La infraestructura está expuesta a goteras, cuenta con averías en el techo en donde el agua de las lluvias
	N.*	Desastres naturales	La oficina de la dependencia de sistemas se encuentra en zona baja de riesgo de desastre natural de origen volcánico debido a su cercanía con el volcán nevado del Tolima.
DE ORIGEN INDUSTRIAL	**I.1**	Fuego	No existe sistema de alarma contra incendios. Se posee un solo extintor de solkaflam (clase c) recomendados para incendios en lugares donde se encuentren equipos eléctricos.
	I.2	Daños por agua	La concentración del líquido sobrante por parte del aire acondicionado causaría daños en los equipos.
	I.*	Desastres industriales	No hay exposición o vulnerabilidad, por parte de esta amenaza.
	I.3	Contaminación mecánica	No hay exposición o vulnerabilidad, por parte de esta amenaza.
	I.4	Contaminación electromagnética	No hay exposición o vulnerabilidad, por parte de esta amenaza.

Tabla 44. Estimación de la vulnerabilidad activo discos duros.. (Continuación)

	I.5	Avería de origen físico o lógico	La manipulación por parte de cada uno de los componentes encontrados en la dependencia, como también por defectos de los componentes desde fabrica
	I.6	Corte del suministro eléctrico	Amenaza debida a factores externos, a clemencias de tipo naturales como lluvias u otros.
	I.7	Condiciones inadecuadas de temperatura o humedad	No se cuenta con una infraestructura adecuada para soportar los defectos del sistema de refrigeración.
	I.11	Emanaciones electromagnéticas	No hay exposición o vulnerabilidad, por parte de esta amenaza.
ERRORES Y FALLOS NO INTENCIONADOS	**E.2**	Errores del administrador	Pérdida total o parcial del tiempo de ejecución de sus actividades, dependiendo de la gravedad del asunto.
	E.23	Errores de mantenimiento / actualización de equipos(hardware)	Perjuicio a la mantenibilidad del sistema de información.
	E.24	Caída del sistema por agotamiento de recursos	Saturación del sistema informático.
	E.25	Perdida de equipos (Robo)	Recuperación de soportes reciclados o desechados.
ATAQUES INTENCIONADOS	**A.6**	Abuso de privilegios de acceso	Abuso de cada uno de los derechos otorgados.
	A.7	Uso no previsto	Implementación de recursos (económicos y de tiempo) en actividades no relacionadas.

Tabla 44. Estimación de la vulnerabilidad activo discos duros.. (Continuación)

	A.11	Acceso no autorizado	Uso ilícito del hardware
	A.23	Manipulación de los equipos	Sabotaje del hardware.
	A.24	Denegación de servicio	Saturación del sistema de información.
	A.25	Robo	Robo de porte de la información, puede esta ser física o digital.
	A.26	Ataque destructivo	Destrucción de los contenedores de la información, en recipientes físicos y lógicos.

Fuente: Autoría propia

Tabla 45. Estimación de la vulnerabilidad activo discos duros externos

ACTIVO TI	DISCOS DUROS EXTERNOS		
ADMINISTRADOR	PIMIENTO CARDENAS WILSON MAURICIO		
TIPO DE ACTIVO	HARDWARE		
Tipo	**ID**	**Amenaza**	**Exposición/Vulnerabilidad**
DESASTRES NATURALES	**N.1**	Fuego	No existe sistema de alarma contra incendios. Se posee un solo extintor de solkaflam (clase c) recomendados para incendios en lugares donde se encuentren equipos eléctricos.
	N.2	Daños por agua	La infraestructura está expuesta a goteras, cuenta con averías en el techo en donde el agua de las lluvias
	N.*	Desastres naturales	La oficina de la dependencia de sistemas se encuentra en zona baja de riesgo de desastre natural de origen volcánico debido a su cercanía con el volcán nevado del Tolima.

Tabla 45. Estimación de la vulnerabilidad activo discos duros externos. (Continuación)

DE ORIGEN INDUSTRIAL	**I.1**	Fuego	No existe sistema de alarma contra incendios. Se posee un solo extintor de solkaflam (clase c) recomendados para incendios en lugares donde se encuentren equipos eléctricos.
	I.2	Daños por agua	La concentración del líquido sobrante por parte del aire acondicionado causaría daños en los equipos.
	I.*	Desastres industriales	No hay exposición o vulnerabilidad, por parte de esta amenaza.
	I.3	Contaminación mecánica	No hay exposición o vulnerabilidad, por parte de esta amenaza.
	I.4	Contaminación electromagnética	No hay exposición o vulnerabilidad, por parte de esta amenaza.
	I.5	Avería de origen físico o lógico	La manipulación por parte de cada uno de los componentes encontrados en la dependencia, como también por defectos de los componentes desde fabrica
	I.6	Corte del suministro eléctrico	Amenaza debida a factores externos, a clemencias de tipo naturales como lluvias u otros.
	I.7	Condiciones inadecuadas de temperatura o humedad	No se cuenta con una infraestructura adecuada para soportar los defectos del sistema de refrigeración.
	I.11	Emanaciones electromagnéticas	No hay exposición o vulnerabilidad, por parte de esta amenaza.
ERRORES Y FALLOS	**E.2**	Errores del administrador	Pérdida total o parcial del tiempo de ejecución de sus actividades, dependiendo de la gravedad del asunto.

Tabla 45. Estimación de la vulnerabilidad activo discos duros externos. (Continuación)

	E.23	Errores de mantenimiento / actualización de equipos(hardware)	Perjuicio a la mantenibilidad del sistema de información.
	E.24	Caída del sistema por agotamiento de recursos	Saturación del sistema informático.
	E.25	Perdida de equipos (Robo)	Recuperación de soportes reciclados o desechados.
ATAQUES INTENCIONADOS	**A.6**	Abuso de privilegios de acceso	Abuso de cada uno de los derechos otorgados.
	A.7	Uso no previsto	Implementación de recursos (económicos y de tiempo) en actividades no relacionadas.
	A.11	Acceso no autorizado	Uso ilícito del hardware
	A.23	Manipulación de los equipos	Sabotaje del hardware.
	A.24	Denegación de servicio	Saturación del sistema de información.
	A.25	Robo	Robo de porte de la información, puede esta ser física o digital.
	A.26	Ataque destructivo	Destrucción de los contenedores de la información, en recipientes físicos y lógicos.

Fuente: Autoría propia

Tabla 46. Estimación de la vulnerabilidad activo switch ALCATEL LUCEN 9553

ACTIVO TI		SWITCH ALCATEL LUCEN 9553	
ADMINISTRADOR		PIMIENTO CARDENAS WILSON MAURICIO	
TIPO DE ACTIVO		HARDWARE	
Tipo	**ID**	**Amenaza**	**Exposición/Vulnerabilidad**

Tabla 46. Estimación de la vulnerabilidad activo switch ALCATEL LUCEN 9553. (Continuación)

DESASTRES NATURALES	**N.1**	Fuego	No existe sistema de alarma contra incendios. Se posee un solo extintor de solkaflam (clase c) recomendados para incendios en lugares donde se encuentren equipos eléctricos.
	N.2	Daños por agua	La infraestructura está expuesta a goteras, cuenta con averías en el techo en donde el agua de las lluvias
	N.*	Desastres naturales	La oficina de la dependencia de sistemas se encuentra en zona baja de riesgo de desastre natural de origen volcánico debido a su cercanía con el volcán nevado del Tolima.
DE ORIGEN INDUSTRIAL	**I.1**	Fuego	No existe sistema de alarma contra incendios. Se posee un solo extintor de solkaflam (clase c) recomendados para incendios en lugares donde se encuentren equipos eléctricos.
	I.2	Daños por agua	La concentración del líquido sobrante por parte del aire acondicionado causaría daños en los equipos.
	I.*	Desastres industriales	No hay exposición o vulnerabilidad, por parte de esta amenaza.
	I.3	Contaminación mecánica	No hay exposición o vulnerabilidad, por parte de esta amenaza.
	I.4	Contaminación electromagnética	No hay exposición o vulnerabilidad, por parte de esta amenaza.
	I.5	Avería de origen físico o lógico	La manipulación por parte de cada uno de los componentes encontrados en la dependencia, como también por defectos de los componentes desde fabrica

Tabla 46. Estimación de la vulnerabilidad activo switch ALCATEL LUCEN 9553. (Continuación)

	I.6	Corte del suministro eléctrico	Amenaza debida a factores externos, a clemencias de tipo naturales como lluvias u otros.
	I.7	Condiciones inadecuadas de temperatura o humedad	No se cuenta con una infraestructura adecuada para soportar los defectos del sistema de refrigeración.
	I.11	Emanaciones electromagnéticas	No hay exposición o vulnerabilidad, por parte de esta amenaza.
ERRORES Y FALLOS NO INTENCIONADOS	**E.2**	Errores del administrador	Pérdida total o parcial del tiempo de ejecución de sus actividades, dependiendo de la gravedad del asunto.
	E.23	Errores de mantenimiento / actualización de equipos(hardware)	Perjuicio a la mantenibilidad del sistema de información.
	E.24	Caída del sistema por agotamiento de recursos	Saturación del sistema informático.
	E.25	Perdida de equipos (Robo)	Recuperación de soportes reciclados o desechados.
ATAQUES INTENCIONADOS	**A.6**	Abuso de privilegios de acceso	Abuso de cada uno de los derechos otorgados.
	A.7	Uso no previsto	Implementación de recursos (económicos y de tiempo) en actividades no relacionadas.
	A.11	Acceso no autorizado	Uso ilícito del hardware
	A.23	Manipulación de los equipos	Sabotaje del hardware.

Tabla 46. Estimación de la vulnerabilidad activo switch ALCATEL LUCEN 9553. (Continuación)

	A.24	Denegación de servicio	Saturación del sistema de información.
	A.25	Robo	Robo de porte de la información, puede esta ser física o digital.
	A.26	Ataque destructivo	Destrucción de los contenedores de la información, en recipientes físicos y lógicos.

Fuente: Autoría propia

Tabla 47. Estimación de la vulnerabilidad activo switch 24 10/100/1000 base t c

ACTIVO TI		SWITCH 24 10/100/1000 BASE T C	
ADMINISTRADOR		PIMIENTO CARDENAS WILSON MAURICIO	
TIPO DE ACTIVO		HARDWARE	
Tipo	**ID**	**Amenaza**	**Exposición/Vulnerabilidad**
DESASTRES NATURALES	**N.1**	Fuego	No existe sistema de alarma contra incendios. Se posee un solo extintor de solkaflam (clase c) recomendados para incendios en lugares donde se encuentren equipos eléctricos.
	N.2	Daños por agua	La infraestructura está expuesta a goteras, cuenta con averías en el techo en donde el agua de las lluvias
	N.*	Desastres naturales	La oficina de la dependencia de sistemas se encuentra en zona baja de riesgo de desastre natural de origen volcánico debido a su cercanía con el volcán nevado del Tolima.
DE ORIGEN INDUSTRIAL	**I.1**	Fuego	No existe sistema de alarma contra incendios. Se posee un solo extintor de solkaflam (clase c) recomendados para incendios en lugares donde se encuentren equipos eléctricos.

Tabla 47. Estimación de la vulnerabilidad activo switch 24 10/100/1000 base t c. (Continuación)

	I.2	Daños por agua	La concentración del líquido sobrante por parte del aire acondicionado causaría daños en los equipos.
	I.*	Desastres industriales	No hay exposición o vulnerabilidad, por parte de esta amenaza.
	I.3	Contaminación mecánica	No hay exposición o vulnerabilidad, por parte de esta amenaza.
	I.4	Contaminación electromagnética	No hay exposición o vulnerabilidad, por parte de esta amenaza.
	I.5	Avería de origen físico o lógico	La manipulación por parte de cada uno de los componentes encontrados en la dependencia, como también por defectos de los componentes desde fabrica
	I.6	Corte del suministro eléctrico	Amenaza debida a factores externos, a clemencias de tipo naturales como lluvias u otros.
	I.7	Condiciones inadecuadas de temperatura o humedad	No se cuenta con una infraestructura adecuada para soportar los defectos del sistema de refrigeración.
	I.11	Emanaciones electromagnéticas	No hay exposición o vulnerabilidad, por parte de esta amenaza.
ERRORES Y FALLOS NO INTENCIONADOS	**E.2**	Errores del administrador	Pérdida total o parcial del tiempo de ejecución de sus actividades, dependiendo de la gravedad del asunto.
	E.23	Errores de mantenimiento / actualización de equipos(hardware)	Perjuicio a la mantenibilidad del sistema de información.

Tabla 47. Estimación de la vulnerabilidad activo switch 24 10/100/1000 base t c. (Continuación)

	E.24	Caída del sistema por agotamiento de recursos	Saturación del sistema informático.
	E.25	Perdida de equipos (Robo)	Recuperación de soportes reciclados o desechados.
ATAQUES INTENCIONADOS	**A.6**	Abuso de privilegios de acceso	Abuso de cada uno de los derechos otorgados.
	A.7	Uso no previsto	Implementación de recursos (económicos y de tiempo) en actividades no relacionadas.
	A.11	Acceso no autorizado	Uso ilícito del hardware
	A.23	Manipulación de los equipos	Sabotaje del hardware.
	A.24	Denegación de servicio	Saturación del sistema de información.
	A.25	Robo	Robo de porte de la información, puede esta ser física o digital.
	A.26	Ataque destructivo	Destrucción de los contenedores de la información, en recipientes físicos y lógicos.

Fuente: Autoría propia

Tabla 48. Estimación de la vulnerabilidad activo switch 24/10/100/1000 base t4s

ACTIVO TI		SWITCH 24/10/100/1000 BASE T4S	
ADMINISTRADOR		PIMIENTO CARDENAS WILSON MAURICIO	
TIPO DE ACTIVO		HARDWARE	
Tipo	**ID**	**Amenaza**	**Exposición/Vulnerabilidad**
DESASTRES NATURA	**N.1**	Fuego	No existe sistema de alarma contra incendios. Se posee un solo extintor de solkaflam (clase c) recomendados para

Tabla 48. Estimación de la vulnerabilidad activo switch 24/10/100/1000 base t4s. (Continuación)

			incendios en lugares donde se encuentren equipos eléctricos.
	N.2	Daños por agua	La infraestructura está expuesta a goteras, cuenta con averías en el techo en donde el agua de las lluvias
	N.*	Desastres naturales	La oficina de la dependencia de sistemas se encuentra en zona baja de riesgo de desastre natural de origen volcánico debido a su cercanía con el volcán nevado del Tolima.
DE ORIGEN INDUSTRIAL	**I.1**	Fuego	No existe sistema de alarma contra incendios. Se posee un solo extintor de solkaflam (clase c) recomendados para incendios en lugares donde se encuentren equipos eléctricos.
	I.2	Daños por agua	La concentración del líquido sobrante por parte del aire acondicionado causaría daños en los equipos.
	I.*	Desastres industriales	No hay exposición o vulnerabilidad, por parte de esta amenaza.
	I.3	Contaminación mecánica	No hay exposición o vulnerabilidad, por parte de esta amenaza.
	I.4	Contaminación electromagnética	No hay exposición o vulnerabilidad, por parte de esta amenaza.
	I.5	Avería de origen físico o lógico	La manipulación por parte de cada uno de los componentes encontrados en la dependencia, como también por defectos de los componentes desde fabrica
	I.6	Corte del suministro eléctrico	Amenaza debida a factores externos, a clemencias de tipo naturales como lluvias u otros.

Tabla 48. Estimación de la vulnerabilidad activo switch 24/10/100/1000 base t4s. (Continuación)

	I.7	Condiciones inadecuadas de temperatura o humedad	No se cuenta con una infraestructura adecuada para soportar los defectos del sistema de refrigeración.
	I.11	Emanaciones electromagnéticas	No hay exposición o vulnerabilidad, por parte de esta amenaza.
ERRORES Y FALLOS NO INTENCIONADOS	**E.2**	Errores del administrador	Pérdida total o parcial del tiempo de ejecución de sus actividades, dependiendo de la gravedad del asunto.
	E.23	Errores de mantenimiento / actualización de equipos(hardware)	Perjuicio a la mantenibilidad del sistema de información.
	E.24	Caída del sistema por agotamiento de recursos	Saturación del sistema informático.
	E.25	Perdida de equipos (Robo)	Recuperación de soportes reciclados o desechados.
ATAQUES INTENCIONADOS	**A.6**	Abuso de privilegios de acceso	Abuso de cada uno de los derechos otorgados.
	A.7	Uso no previsto	Implementación de recursos (económicos y de tiempo) en actividades no relacionadas.
	A.11	Acceso no autorizado	Uso ilícito del hardware
	A.23	Manipulación de los equipos	Sabotaje del hardware.
	A.24	Denegación de servicio	Saturación del sistema de información.

Tabla 48. Estimación de la vulnerabilidad activo switch 24/10/100/1000 base t4s. (Continuación)

	A.25	Robo	Robo de porte de la información, puede esta ser física o digital.
	A.26	Ataque destructivo	Destrucción de los contenedores de la información, en recipientes físicos y lógicos.

Fuente: Autoría propia

Tabla 49. Estimación de la vulnerabilidad activo switch 24/10/100/1000pwr cord

ACTIVO TI	SWITCH 24/10/100/1000PWR CORD		
ADMINISTRADOR	PIMIENTO CARDENAS WILSON MAURICIO		
TIPO DE ACTIVO	HARDWARE		
Tipo	**ID**	**Amenaza**	**Exposición/Vulnerabilidad**
DESASTRES NATURALES	**N.1**	Fuego	No existe sistema de alarma contra incendios. Se posee un solo extintor de solkaflam (clase c) recomendados para incendios en lugares donde se encuentren equipos eléctricos.
	N.2	Daños por agua	La infraestructura está expuesta a goteras, cuenta con averías en el techo en donde el agua de las lluvias
	N.*	Desastres naturales	La oficina de la dependencia de sistemas se encuentra en zona baja de riesgo de desastre natural de origen volcánico debido a su cercanía con el volcán nevado del Tolima.
ORIGEN INDUSTRIAL DE	**I.1**	Fuego	No existe sistema de alarma contra incendios. Se posee un solo extintor de solkaflam (clase c) recomendados para incendios en lugares donde se encuentren equipos eléctricos.
	I.2	Daños por agua	La concentración del líquido sobrante por parte del aire acondicionado causaría daños en los equipos.

Tabla 49. Estimación de la vulnerabilidad activo switch 24/10/100/1000pwr cord. (Continuación)

	I.*	Desastres industriales	No hay exposición o vulnerabilidad, por parte de esta amenaza.
	I.3	Contaminación mecánica	No hay exposición o vulnerabilidad, por parte de esta amenaza.
	I.4	Contaminación electromagnética	No hay exposición o vulnerabilidad, por parte de esta amenaza.
	I.5	Avería de origen físico o lógico	La manipulación por parte de cada uno de los componentes encontrados en la dependencia, como también por defectos de los componentes desde fabrica
	I.6	Corte del suministro eléctrico	Amenaza debida a factores externos, a clemencias de tipo naturales como lluvias u otros.
	I.7	Condiciones inadecuadas de temperatura o humedad	No se cuenta con una infraestructura adecuada para soportar los defectos del sistema de refrigeración.
	I.11	Emanaciones electromagnéticas	No hay exposición o vulnerabilidad, por parte de esta amenaza.
ERRORES Y FALLOS NO INTENCIONADOS	**E.2**	Errores del administrador	Pérdida total o parcial del tiempo de ejecución de sus actividades, dependiendo de la gravedad del asunto.
	E.23	Errores de mantenimiento / actualización de equipos(hardware)	Perjuicio a la mantenibilidad del sistema de información.
	E.24	Caída del sistema por agotamiento de recursos	Saturación del sistema informático.
	E.25	Perdida de equipos (Robo)	Recuperación de soportes reciclados o desechados.

Tabla 49. Estimación de la vulnerabilidad activo switch 24/10/100/1000pwr cord. (Continuación)

ATAQUES INTENCIONADOS	**A.6**	Abuso de privilegios de acceso	Abuso de cada uno de los derechos otorgados.
	A.7	Uso no previsto	Implementación de recursos (económicos y de tiempo) en actividades no relacionadas.
	A.11	Acceso no autorizado	Uso ilícito del hardware
	A.23	Manipulación de los equipos	Sabotaje del hardware.
	A.24	Denegación de servicio	Saturación del sistema de información.
	A.25	Robo	Robo de porte de la información, puede esta ser física o digital.
	A.26	Ataque destructivo	Destrucción de los contenedores de la información, en recipientes físicos y lógicos.

Fuente: Autoría propia

Tabla 50. Estimación de la vulnerabilidad activo switch Alcatel lucen 9561

ACTIVO TI	SWITCH ALCATEL LUCEN 9561		
ADMINISTRADOR	PIMIENTO CARDENAS WILSON MAURICIO		
TIPO DE ACTIVO	HARDWARE		
Tipo	**ID**	**Amenaza**	**Exposición/Vulnerabilidad**
DESASTRES NATURALES	**N.1**	Fuego	No existe sistema de alarma contra incendios. Se posee un solo extintor de solkaflam (clase c) recomendados para incendios en lugares donde se encuentren equipos eléctricos.
	N.2	Daños por agua	La infraestructura está expuesta a goteras, cuenta con averías en el techo en donde el agua de las lluvias

Tabla 50. Estimación de la vulnerabilidad activo switch Alcatel lucen 9561. (Continuación)

	N.*	Desastres naturales	La oficina de la dependencia de sistemas se encuentra en zona baja de riesgo de desastre natural de origen volcánico debido a su cercanía con el volcán nevado del Tolima.
DE ORIGEN INDUSTRIAL	**I.1**	Fuego	No existe sistema de alarma contra incendios. Se posee un solo extintor de solkaflam (clase c) recomendados para incendios en lugares donde se encuentren equipos eléctricos.
	I.2	Daños por agua	La concentración del líquido sobrante por parte del aire acondicionado causaría daños en los equipos.
	I.*	Desastres industriales	No hay exposición o vulnerabilidad, por parte de esta amenaza.
	I.3	Contaminación mecánica	No hay exposición o vulnerabilidad, por parte de esta amenaza.
	I.4	Contaminación electromagnética	No hay exposición o vulnerabilidad, por parte de esta amenaza.
	I.5	Avería de origen físico o lógico	La manipulación por parte de cada uno de los componentes encontrados en la dependencia, como también por defectos de los componentes desde fabrica
	I.6	Corte del suministro eléctrico	Amenaza debida a factores externos, a clemencias de tipo naturales como lluvias u otros.
	I.7	Condiciones inadecuadas de temperatura o humedad	No se cuenta con una infraestructura adecuada para soportar los defectos del sistema de refrigeración.
	I.11	Emanaciones electromagnéticas	No hay exposición o vulnerabilidad, por parte de esta amenaza.

Tabla 50. Estimación de la vulnerabilidad activo switch Alcatel lucen 9561. (Continuación)

ERRORES Y FALLOS NO INTENCIONADOS	**E.2**	Errores del administrador	Pérdida total o parcial del tiempo de ejecución de sus actividades, dependiendo de la gravedad del asunto.
	E.23	Errores de mantenimiento / actualización de equipos(hardware)	Perjuicio a la mantenibilidad del sistema de información.
	E.24	Caída del sistema por agotamiento de recursos	Saturación del sistema informático.
	E.25	Perdida de equipos (Robo)	Recuperación de soportes reciclados o desechados.
ATAQUES INTENCIONADOS	**A.6**	Abuso de privilegios de acceso	Abuso de cada uno de los derechos otorgados.
	A.7	Uso no previsto	Implementación de recursos (económicos y de tiempo) en actividades no relacionadas.
	A.11	Acceso no autorizado	Uso ilícito del hardware
	A.23	Manipulación de los equipos	Sabotaje del hardware.
	A.24	Denegación de servicio	Saturación del sistema de información.
	A.25	Robo	Robo de porte de la información, puede esta ser física o digital.
	A.26	Ataque destructivo	Destrucción de los contenedores de la información, en recipientes físicos y lógicos.

Fuente: Autoría propia

Tabla 51. Estimación de la vulnerabilidad activo switch ALCATEL LUCEN 9556

ACTIVO TI		SWITCH ALCATEL LUCEN 9556	
ADMINISTRADOR		PIMIENTO CARDENAS WILSON MAURICIO	
TIPO DE ACTIVO		HARDWARE	
Tipo	**ID**	**Amenaza**	**Exposición/Vulnerabilidad**
DESASTRES NATURALES	**N.1**	Fuego	No existe sistema de alarma contra incendios. Se posee un solo extintor de solkaflam (clase c) recomendados para incendios en lugares donde se encuentren equipos eléctricos.
	N.2	Daños por agua	La infraestructura está expuesta a goteras, cuenta con averías en el techo en donde el agua de las lluvias
	N.*	Desastres naturales	La oficina de la dependencia de sistemas se encuentra en zona baja de riesgo de desastre natural de origen volcánico debido a su cercanía con el volcán nevado del Tolima.
DE ORIGEN INDUSTRIAL	**I.1**	Fuego	No existe sistema de alarma contra incendios. Se posee un solo extintor de solkaflam (clase c) recomendados para incendios en lugares donde se encuentren equipos eléctricos.
	I.2	Daños por agua	La concentración del líquido sobrante por parte del aire acondicionado causaría daños en los equipos.
	I.*	Desastres industriales	No hay exposición o vulnerabilidad, por parte de esta amenaza.
	I.3	Contaminación mecánica	No hay exposición o vulnerabilidad, por parte de esta amenaza.
	I.4	Contaminación electromagnética	No hay exposición o vulnerabilidad, por parte de esta amenaza.

Tabla 51. Estimación de la vulnerabilidad activo switch ALCATEL LUCEN 9556. (Continuación)

	I.5	Avería de origen físico o lógico	La manipulación por parte de cada uno de los componentes encontrados en la dependencia, como también por defectos de los componentes desde fabrica
	I.6	Corte del suministro eléctrico	Amenaza debida a factores externos, a clemencias de tipo naturales como lluvias u otros.
	I.7	Condiciones inadecuadas de temperatura o humedad	No se cuenta con una infraestructura adecuada para soportar los defectos del sistema de refrigeración.
	I.11	Emanaciones electromagnéticas	No hay exposición o vulnerabilidad, por parte de esta amenaza.
ERRORES Y FALLOS NO INTENCIONADOS	**E.2**	Errores del administrador	Pérdida total o parcial del tiempo de ejecución de sus actividades, dependiendo de la gravedad del asunto.
	E.23	Errores de mantenimiento / actualización de equipos(hardware)	Perjuicio a la mantenibilidad del sistema de información.
	E.24	Caída del sistema por agotamiento de recursos	Saturación del sistema informático.
	E.25	Perdida de equipos (Robo)	Recuperación de soportes reciclados o desechados.
ATAQUES INTENCIONADOS	**A.6**	Abuso de privilegios de acceso	Abuso de cada uno de los derechos otorgados.
	A.7	Uso no previsto	Implementación de recursos (económicos y de tiempo) en actividades no relacionadas.

Tabla 51. Estimación de la vulnerabilidad activo switch ALCATEL LUCEN 9556. (Continuación)

	A.11	Acceso no autorizado	Uso ilícito del hardware
	A.23	Manipulación de los equipos	Sabotaje del hardware.
	A.24	Denegación de servicio	Saturación del sistema de información.
	A.25	Robo	Robo de porte de la información, puede esta ser física o digital.
	A.26	Ataque destructivo	Destrucción de los contenedores de la información, en recipientes físicos y lógicos.

Fuente: Autoría propia

Tabla 52. Estimación de la vulnerabilidad activo switch ALCATEL LUCEN 9557

ACTIVO TI	SWITCH ALCATEL LUCEN 9557	
ADMINISTRADOR	PIMIENTO CARDENAS WILSON MAURICIO	
TIPO DE ACTIVO	HARDWARE	
Tipo	**ID**	**Amenaza**	**Exposición/Vulnerabilidad**
DESASTRES NATURALES	**N.1**	Fuego	No existe sistema de alarma contra incendios. Se posee un solo extintor de solkaflam (clase c) recomendados para incendios en lugares donde se encuentren equipos eléctricos.
	N.2	Daños por agua	La infraestructura está expuesta a goteras, cuenta con averías en el techo en donde el agua de las lluvias
	N.*	Desastres naturales	La oficina de la dependencia de sistemas se encuentra en zona baja de riesgo de desastre natural de origen volcánico debido a su cercanía con el volcán nevado del Tolima.

Tabla 52. Estimación de la vulnerabilidad activo switch ALCATEL LUCEN 9557. (Continuación)

DE ORIGEN INDUSTRIAL	**I.1**	Fuego	No existe sistema de alarma contra incendios. Se posee un solo extintor de solkaflam (clase c) recomendados para incendios en lugares donde se encuentren equipos eléctricos.
	I.2	Daños por agua	La concentración del líquido sobrante por parte del aire acondicionado causaría daños en los equipos.
	I.*	Desastres industriales	No hay exposición o vulnerabilidad, por parte de esta amenaza.
	I.3	Contaminación mecánica	No hay exposición o vulnerabilidad, por parte de esta amenaza.
	I.4	Contaminación electromagnética	No hay exposición o vulnerabilidad, por parte de esta amenaza.
	I.5	Avería de origen físico o lógico	La manipulación por parte de cada uno de los componentes encontrados en la dependencia, como también por defectos de los componentes desde fabrica
	I.6	Corte del suministro eléctrico	Amenaza debida a factores externos, a clemencias de tipo naturales como lluvias u otros.
	I.7	Condiciones inadecuadas de temperatura o humedad	No se cuenta con una infraestructura adecuada para soportar los defectos del sistema de refrigeración.
	I.11	Emanaciones electromagnéticas	No hay exposición o vulnerabilidad, por parte de esta amenaza.
ERRORES Y FALLOS	**E.2**	Errores del administrador	Pérdida total o parcial del tiempo de ejecución de sus actividades, dependiendo de la gravedad del asunto.

Tabla 52. Estimación de la vulnerabilidad activo switch ALCATEL LUCEN 9557. (Continuación)

	E.23	Errores de mantenimiento / actualización de equipos(hardware)	Perjuicio a la mantenibilidad del sistema de información.
	E.24	Caída del sistema por agotamiento de recursos	Saturación del sistema informático.
	E.25	Perdida de equipos (Robo)	Recuperación de soportes reciclados o desechados.
ATAQUES INTENCIONADOS	**A.6**	Abuso de privilegios de acceso	Abuso de cada uno de los derechos otorgados.
	A.7	Uso no previsto	Implementación de recursos (económicos y de tiempo) en actividades no relacionadas.
	A.11	Acceso no autorizado	Uso ilícito del hardware
	A.23	Manipulación de los equipos	Sabotaje del hardware.
	A.24	Denegación de servicio	Saturación del sistema de información.
	A.25	Robo	Robo de porte de la información, puede esta ser física o digital.
	A.26	Ataque destructivo	Destrucción de los contenedores de la información, en recipientes físicos y lógicos.

Fuente: Autoría propia

Tabla 53. Estimación de la vulnerabilidad activo switch ALCATEL LUCEN 9558

ACTIVO TI		SWITCH ALCATEL LUCEN 9558	
ADMINISTRADOR		PIMIENTO CARDENAS WILSON MAURICIO	
TIPO DE ACTIVO		HARDWARE	
Tipo	**ID**	**Amenaza**	**Exposición/Vulnerabilidad**

Tabla 53. Estimación de la vulnerabilidad activo switch ALCATEL LUCEN 9558. (Continuación)

DESASTRES NATURALES	**N.1**	Fuego	No existe sistema de alarma contra incendios. Se posee un solo extintor de solkaflam (clase c) recomendados para incendios en lugares donde se encuentren equipos eléctricos.
	N.2	Daños por agua	La infraestructura está expuesta a goteras, cuenta con averías en el techo en donde el agua de las lluvias
	N.*	Desastres naturales	La oficina de la dependencia de sistemas se encuentra en zona baja de riesgo de desastre natural de origen volcánico debido a su cercanía con el volcán nevado del Tolima.
DE ORIGEN INDUSTRIAL	**I.1**	Fuego	No existe sistema de alarma contra incendios. Se posee un solo extintor de solkaflam (clase c) recomendados para incendios en lugares donde se encuentren equipos eléctricos.
	I.2	Daños por agua	La concentración del líquido sobrante por parte del aire acondicionado causaría daños en los equipos.
	I.*	Desastres industriales	No hay exposición o vulnerabilidad, por parte de esta amenaza.
	I.3	Contaminación mecánica	No hay exposición o vulnerabilidad, por parte de esta amenaza.
	I.4	Contaminación electromagnética	No hay exposición o vulnerabilidad, por parte de esta amenaza.
	I.5	Avería de origen físico o lógico	La manipulación por parte de cada uno de los componentes encontrados en la dependencia, como también por defectos de los componentes desde fabrica

Tabla 53. Estimación de la vulnerabilidad activo switch ALCATEL LUCEN 9558. (Continuación)

	I.6	Corte del suministro eléctrico	Amenaza debida a factores externos, a clemencias de tipo naturales como lluvias u otros.
	I.7	Condiciones inadecuadas de temperatura o humedad	No se cuenta con una infraestructura adecuada para soportar los defectos del sistema de refrigeración.
	I.11	Emanaciones electromagnéticas	No hay exposición o vulnerabilidad, por parte de esta amenaza.
ERRORES Y FALLOS NO INTENCIONADOS	**E.2**	Errores del administrador	Pérdida total o parcial del tiempo de ejecución de sus actividades, dependiendo de la gravedad del asunto.
	E.23	Errores de mantenimiento / actualización de equipos(hardware)	Perjuicio a la mantenibilidad del sistema de información.
	E.24	Caída del sistema por agotamiento de recursos	Saturación del sistema informático.
	E.25	Perdida de equipos (Robo)	Recuperación de soportes reciclados o desechados.
ATAQUES INTENCIONADOS	**A.6**	Abuso de privilegios de acceso	Abuso de cada uno de los derechos otorgados.
	A.7	Uso no previsto	Implementación de recursos (económicos y de tiempo) en actividades no relacionadas.
	A.11	Acceso no autorizado	Uso ilícito del hardware
	A.23	Manipulación de los equipos	Sabotaje del hardware.

Tabla 53. Estimación de la vulnerabilidad activo switch ALCATEL LUCEN 9558. (Continuación)

	A.24	Denegación de servicio	Saturación del sistema de información.
	A.25	Robo	Robo de porte de la información, puede esta ser física o digital.
	A.26	Ataque destructivo	Destrucción de los contenedores de la información, en recipientes físicos y lógicos.

Fuente: Autoría propia

Tabla 54. Estimación de la vulnerabilidad activo switch ALCATEL LUCEN 9559

ACTIVO TI		SWITCH ALCATEL LUCEN 9559	
ADMINISTRADOR		PIMIENTO CARDENAS WILSON MAURICIO	
TIPO DE ACTIVO		HARDWARE	
Tipo	**ID**	**Amenaza**	**Exposición/Vulnerabilidad**
DESASTRES NATURALES	**N.1**	Fuego	No existe sistema de alarma contra incendios. Se posee un solo extintor de solkaflam (clase c) recomendados para incendios en lugares donde se encuentren equipos eléctricos.
	N.2	Daños por agua	La infraestructura está expuesta a goteras, cuenta con averías en el techo en donde el agua de las lluvias
	N.*	Desastres naturales	La oficina de la dependencia de sistemas se encuentra en zona baja de riesgo de desastre natural de origen volcánico debido a su cercanía con el volcán nevado del Tolima.
DE ORIGEN INDUSTRIAL	**I.1**	Fuego	No existe sistema de alarma contra incendios. Se posee un solo extintor de solkaflam (clase c) recomendados para incendios en lugares donde se encuentren equipos eléctricos.

Tabla 54. Estimación de la vulnerabilidad activo switch ALCATEL LUCEN 9559. (Continuación)

	I.2	Daños por agua	La concentración del líquido sobrante por parte del aire acondicionado causaría daños en los equipos.
	I.*	Desastres industriales	No hay exposición o vulnerabilidad, por parte de esta amenaza.
	I.3	Contaminación mecánica	No hay exposición o vulnerabilidad, por parte de esta amenaza.
	I.4	Contaminación electromagnética	No hay exposición o vulnerabilidad, por parte de esta amenaza.
	I.5	Avería de origen físico o lógico	La manipulación por parte de cada uno de los componentes encontrados en la dependencia, como también por defectos de los componentes desde fabrica
	I.6	Corte del suministro eléctrico	Amenaza debida a factores externos, a clemencias de tipo naturales como lluvias u otros.
	I.7	Condiciones inadecuadas de temperatura o humedad	No se cuenta con una infraestructura adecuada para soportar los defectos del sistema de refrigeración.
	I.11	Emanaciones electromagnéticas	No hay exposición o vulnerabilidad, por parte de esta amenaza.
ERRORES Y FALLOS NO INTENCIONADOS	**E.2**	Errores del administrador	Pérdida total o parcial del tiempo de ejecución de sus actividades, dependiendo de la gravedad del asunto.
	E.23	Errores de mantenimiento / actualización de equipos(hardware)	Perjuicio a la mantenibilidad del sistema de información.

Tabla 54. Estimación de la vulnerabilidad activo switch ALCATEL LUCEN 9559. (Continuación)

	E.24	Caída del sistema por agotamiento de recursos	Saturación del sistema informático.
	E.25	Perdida de equipos (Robo)	Recuperación de soportes reciclados o desechados.
ATAQUES INTENCIONADOS	**A.6**	Abuso de privilegios de acceso	Abuso de cada uno de los derechos otorgados.
	A.7	Uso no previsto	Implementación de recursos (económicos y de tiempo) en actividades no relacionadas.
	A.11	Acceso no autorizado	Uso ilícito del hardware
	A.23	Manipulación de los equipos	Sabotaje del hardware.
	A.24	Denegación de servicio	Saturación del sistema de información.
	A.25	Robo	Robo de porte de la información, puede esta ser física o digital.
	A.26	Ataque destructivo	Destrucción de los contenedores de la información, en recipientes físicos y lógicos.

Fuente: Autoría propia

Tabla 55. Estimación de la vulnerabilidad activo switch ALCATEL LUCEN 9543

ACTIVO TI		SWITCH ALCATEL LUCEN 9543	
ADMINISTRADOR		PIMIENTO CARDENAS WILSON MAURICIO	
TIPO DE ACTIVO		HARDWARE	
Tipo	**ID**	**Amenaza**	**Exposición/Vulnerabilidad**
DESASTRES NATURA	**N.1**	Fuego	No existe sistema de alarma contra incendios. Se posee un solo extintor de solkaflam (clase c) recomendados para

Tabla 55. Estimación de la vulnerabilidad activo switch ALCATEL LUCEN 9543. (Continuación)

			incendios en lugares donde se encuentren equipos eléctricos.
	N.2	Daños por agua	La infraestructura está expuesta a goteras, cuenta con averías en el techo en donde el agua de las lluvias
	N.*	Desastres naturales	La oficina de la dependencia de sistemas se encuentra en zona baja de riesgo de desastre natural de origen volcánico debido a su cercanía con el volcán nevado del Tolima.
DE ORIGEN INDUSTRIAL	**I.1**	Fuego	No existe sistema de alarma contra incendios. Se posee un solo extintor de solkaflam (clase c) recomendados para incendios en lugares donde se encuentren equipos eléctricos.
	I.2	Daños por agua	La concentración del líquido sobrante por parte del aire acondicionado causaría daños en los equipos.
	I.*	Desastres industriales	No hay exposición o vulnerabilidad, por parte de esta amenaza.
	I.3	Contaminación mecánica	No hay exposición o vulnerabilidad, por parte de esta amenaza.
	I.4	Contaminación electromagnética	No hay exposición o vulnerabilidad, por parte de esta amenaza.
	I.5	Avería de origen físico o lógico	La manipulación por parte de cada uno de los componentes encontrados en la dependencia, como también por defectos de los componentes desde fabrica
	I.6	Corte del suministro eléctrico	Amenaza debida a factores externos, a clemencias de tipo naturales como lluvias u otros.

Tabla 55. Estimación de la vulnerabilidad activo switch ALCATEL LUCEN 9543. (Continuación)

	I.7	Condiciones inadecuadas de temperatura o humedad	No se cuenta con una infraestructura adecuada para soportar los defectos del sistema de refrigeración.
	I.11	Emanaciones electromagnéticas	No hay exposición o vulnerabilidad, por parte de esta amenaza.
ERRORES Y FALLOS NO INTENCIONADOS	**E.2**	Errores del administrador	Pérdida total o parcial del tiempo de ejecución de sus actividades, dependiendo de la gravedad del asunto.
	E.23	Errores de mantenimiento / actualización de equipos(hardware)	Perjuicio a la mantenibilidad del sistema de información.
	E.24	Caída del sistema por agotamiento de recursos	Saturación del sistema informático.
	E.25	Perdida de equipos (Robo)	Recuperación de soportes reciclados o desechados.
ATAQUES INTENCIONADOS	**A.6**	Abuso de privilegios de acceso	Abuso de cada uno de los derechos otorgados.
	A.7	Uso no previsto	Implementación de recursos (económicos y de tiempo) en actividades no relacionadas.
	A.11	Acceso no autorizado	Uso ilícito del hardware
	A.23	Manipulación de los equipos	Sabotaje del hardware.
	A.24	Denegación de servicio	Saturación del sistema de información.

Tabla 55. Estimación de la vulnerabilidad activo switch ALCATEL LUCEN 9543. (Continuación)

	A.25	Robo	Robo de porte de la información, puede esta ser física o digital.
	A.26	Ataque destructivo	Destrucción de los contenedores de la información, en recipientes físicos y lógicos.

Fuente: Autoría propia

Tabla 56. Estimación de la vulnerabilidad activo switch ALCATEL LUCEN 9544

ACTIVO TI		SWITCH ALCATEL LUCEN 9544	
ADMINISTRADOR		PIMIENTO CARDENAS WILSON MAURICIO	
TIPO DE ACTIVO		HARDWARE	
Tipo	**ID**	**Amenaza**	**Exposición/Vulnerabilidad**
DESASTRES NATURALES	**N.1**	Fuego	No existe sistema de alarma contra incendios. Se posee un solo extintor de solkaflam (clase c) recomendados para incendios en lugares donde se encuentren equipos eléctricos.
	N.2	Daños por agua	La infraestructura está expuesta a goteras, cuenta con averías en el techo en donde el agua de las lluvias
	N.*	Desastres naturales	La oficina de la dependencia de sistemas se encuentra en zona baja de riesgo de desastre natural de origen volcánico debido a su cercanía con el volcán nevado del Tolima.
ORIGEN INDUSTRIAL DE	**I.1**	Fuego	No existe sistema de alarma contra incendios. Se posee un solo extintor de solkaflam (clase c) recomendados para incendios en lugares donde se encuentren equipos eléctricos.
	I.2	Daños por agua	La concentración del líquido sobrante por parte del aire acondicionado causaría daños en los equipos.

Tabla 56. Estimación de la vulnerabilidad activo switch ALCATEL LUCEN 9544. (Continuación)

	I.*	Desastres industriales	No hay exposición o vulnerabilidad, por parte de esta amenaza.
	I.3	Contaminación mecánica	No hay exposición o vulnerabilidad, por parte de esta amenaza.
	I.4	Contaminación electromagnética	No hay exposición o vulnerabilidad, por parte de esta amenaza.
	I.5	Avería de origen físico o lógico	La manipulación por parte de cada uno de los componentes encontrados en la dependencia, como también por defectos de los componentes desde fabrica
	I.6	Corte del suministro eléctrico	Amenaza debida a factores externos, a clemencias de tipo naturales como lluvias u otros.
	I.7	Condiciones inadecuadas de temperatura o humedad	No se cuenta con una infraestructura adecuada para soportar los defectos del sistema de refrigeración.
	I.11	Emanaciones electromagnéticas	No hay exposición o vulnerabilidad, por parte de esta amenaza.
ERRORES Y FALLOS NO INTENCIONADOS	**E.2**	Errores del administrador	Pérdida total o parcial del tiempo de ejecución de sus actividades, dependiendo de la gravedad del asunto.
	E.23	Errores de mantenimiento / actualización de equipos(hardware)	Perjuicio a la mantenibilidad del sistema de información.
	E.24	Caída del sistema por agotamiento de recursos	Saturación del sistema informático.
	E.25	Perdida de equipos (Robo)	Recuperación de soportes reciclados o desechados.

Tabla 56. Estimación de la vulnerabilidad activo switch ALCATEL LUCEN 9544. (Continuación)

ATAQUES INTENCIONADOS	**A.6**	Abuso de privilegios de acceso	Abuso de cada uno de los derechos otorgados.
	A.7	Uso no previsto	Implementación de recursos (económicos y de tiempo) en actividades no relacionadas.
	A.11	Acceso no autorizado	Uso ilícito del hardware
	A.23	Manipulación de los equipos	Sabotaje del hardware.
	A.24	Denegación de servicio	Saturación del sistema de información.
	A.25	Robo	Robo de porte de la información, puede esta ser física o digital.
	A.26	Ataque destructivo	Destrucción de los contenedores de la información, en recipientes físicos y lógicos.

Fuente: Autoría propia

Tabla 57. Estimación de la vulnerabilidad activo switch ALCATEL LUCEN 9545

ACTIVO TI		SWITCH ALCATEL LUCEN 9545	
ADMINISTRADOR		PIMIENTO CARDENAS WILSON MAURICIO	
TIPO DE ACTIVO		HARDWARE	
Tipo	**ID**	**Amenaza**	**Exposición/Vulnerabilidad**
DESASTRES NATURALES	**N.1**	Fuego	No existe sistema de alarma contra incendios. Se posee un solo extintor de solkaflam (clase c) recomendados para incendios en lugares donde se encuentren equipos eléctricos.
	N.2	Daños por agua	La infraestructura está expuesta a goteras, cuenta con averías en el techo en donde el agua de las lluvias

Tabla 57. Estimación de la vulnerabilidad activo switch ALCATEL LUCEN 9545. (Continuación)

	N.*	Desastres naturales	La oficina de la dependencia de sistemas se encuentra en zona baja de riesgo de desastre natural de origen volcánico debido a su cercanía con el volcán nevado del Tolima.
DE ORIGEN INDUSTRIAL	**I.1**	Fuego	No existe sistema de alarma contra incendios. Se posee un solo extintor de solkaflam (clase c) recomendados para incendios en lugares donde se encuentren equipos eléctricos.
	I.2	Daños por agua	La concentración del líquido sobrante por parte del aire acondicionado causaría daños en los equipos.
	I.*	Desastres industriales	No hay exposición o vulnerabilidad, por parte de esta amenaza.
	I.3	Contaminación mecánica	No hay exposición o vulnerabilidad, por parte de esta amenaza.
	I.4	Contaminación electromagnética	No hay exposición o vulnerabilidad, por parte de esta amenaza.
	I.5	Avería de origen físico o lógico	La manipulación por parte de cada uno de los componentes encontrados en la dependencia, como también por defectos de los componentes desde fabrica
	I.6	Corte del suministro eléctrico	Amenaza debida a factores externos, a clemencias de tipo naturales como lluvias u otros.
	I.7	Condiciones inadecuadas de temperatura o humedad	No se cuenta con una infraestructura adecuada para soportar los defectos del sistema de refrigeración.
	I.11	Emanaciones electromagnéticas	No hay exposición o vulnerabilidad, por parte de esta amenaza.

Tabla 57. Estimación de la vulnerabilidad activo switch ALCATEL LUCEN 9545. (Continuación)

ERRORES Y FALLOS NO INTENCIONADOS	**E.2**	Errores del administrador	Pérdida total o parcial del tiempo de ejecución de sus actividades, dependiendo de la gravedad del asunto.
	E.23	Errores de mantenimiento / actualización de equipos(hardware)	Perjuicio a la mantenibilidad del sistema de información.
	E.24	Caída del sistema por agotamiento de recursos	Saturación del sistema informático.
	E.25	Perdida de equipos (Robo)	Recuperación de soportes reciclados o desechados.
ATAQUES INTENCIONADOS	**A.6**	Abuso de privilegios de acceso	Abuso de cada uno de los derechos otorgados.
	A.7	Uso no previsto	Implementación de recursos (económicos y de tiempo) en actividades no relacionadas.
	A.11	Acceso no autorizado	Uso ilícito del hardware
	A.23	Manipulación de los equipos	Sabotaje del hardware.
	A.24	Denegación de servicio	Saturación del sistema de información.
	A.25	Robo	Robo de porte de la información, puede esta ser física o digital.
	A.26	Ataque destructivo	Destrucción de los contenedores de la información, en recipientes físicos y lógicos.

Fuente: Autoría propia

Tabla 58. Estimación de la vulnerabilidad activo switch ALCATEL LUCEN 9548

ACTIVO TI		SWITCH ALCATEL LUCEN 9548	
ADMINISTRADOR		PIMIENTO CARDENAS WILSON MAURICIO	
TIPO DE ACTIVO		HARDWARE	
Tipo	**ID**	**Amenaza**	**Exposición/Vulnerabilidad**
DESASTRES NATURALES	**N.1**	Fuego	No existe sistema de alarma contra incendios. Se posee un solo extintor de solkaflam (clase c) recomendados para incendios en lugares donde se encuentren equipos eléctricos.
	N.2	Daños por agua	La infraestructura está expuesta a goteras, cuenta con averías en el techo en donde el agua de las lluvias
	N.*	Desastres naturales	La oficina de la dependencia de sistemas se encuentra en zona baja de riesgo de desastre natural de origen volcánico debido a su cercanía con el volcán nevado del Tolima.
DE ORIGEN INDUSTRIAL	**I.1**	Fuego	No existe sistema de alarma contra incendios. Se posee un solo extintor de solkaflam (clase c) recomendados para incendios en lugares donde se encuentren equipos eléctricos.
	I.2	Daños por agua	La concentración del líquido sobrante por parte del aire acondicionado causaría daños en los equipos.
	I.*	Desastres industriales	No hay exposición o vulnerabilidad, por parte de esta amenaza.
	I.3	Contaminación mecánica	No hay exposición o vulnerabilidad, por parte de esta amenaza.
	I.4	Contaminación electromagnética	No hay exposición o vulnerabilidad, por parte de esta amenaza.

Tabla 58. Estimación de la vulnerabilidad activo switch ALCATEL LUCEN 9548. (Continuación)

	I.5	Avería de origen físico o lógico	La manipulación por parte de cada uno de los componentes encontrados en la dependencia, como también por defectos de los componentes desde fabrica
	I.6	Corte del suministro eléctrico	Amenaza debida a factores externos, a clemencias de tipo naturales como lluvias u otros.
	I.7	Condiciones inadecuadas de temperatura o humedad	No se cuenta con una infraestructura adecuada para soportar los defectos del sistema de refrigeración.
	I.11	Emanaciones electromagnéticas	No hay exposición o vulnerabilidad, por parte de esta amenaza.
ERRORES Y FALLOS NO INTENCIONADOS	**E.2**	Errores del administrador	Pérdida total o parcial del tiempo de ejecución de sus actividades, dependiendo de la gravedad del asunto.
	E.23	Errores de mantenimiento / actualización de equipos(hardware)	Perjuicio a la mantenibilidad del sistema de información.
	E.24	Caída del sistema por agotamiento de recursos	Saturación del sistema informático.
	E.25	Perdida de equipos (Robo)	Recuperación de soportes reciclados o desechados.
ATAQUES INTENCIONADOS	**A.6**	Abuso de privilegios de acceso	Abuso de cada uno de los derechos otorgados.
	A.7	Uso no previsto	Implementación de recursos (económicos y de tiempo) en actividades no relacionadas.

Tabla 58. Estimación de la vulnerabilidad activo switch ALCATEL LUCEN 9548. (Continuación)

	A.11	Acceso no autorizado	Uso ilícito del hardware
	A.23	Manipulación de los equipos	Sabotaje del hardware.
	A.24	Denegación de servicio	Saturación del sistema de información.
	A.25	Robo	Robo de porte de la información, puede esta ser física o digital.
	A.26	Ataque destructivo	Destrucción de los contenedores de la información, en recipientes físicos y lógicos.

Fuente: Autoría propia

Tabla 59. Estimación de la vulnerabilidad activo switch ALCATEL LUCEN 9550

ACTIVO TI		SWITCH ALCATEL LUCEN 9550	
ADMINISTRADOR		PIMIENTO CARDENAS WILSON MAURICIO	
TIPO DE ACTIVO		HARDWARE	
Tipo	**ID**	**Amenaza**	**Exposición/Vulnerabilidad**
DESASTRES NATURALES	**N.1**	Fuego	No existe sistema de alarma contra incendios. Se posee un solo extintor de solkaflam (clase c) recomendados para incendios en lugares donde se encuentren equipos eléctricos.
	N.2	Daños por agua	La infraestructura está expuesta a goteras, cuenta con averías en el techo en donde el agua de las lluvias
	N.*	Desastres naturales	La oficina de la dependencia de sistemas se encuentra en zona baja de riesgo de desastre natural de origen volcánico debido a su cercanía con el volcán nevado del Tolima.

Tabla 59. Estimación de la vulnerabilidad activo switch ALCATEL LUCEN 9550. (Continuación)

DE ORIGEN INDUSTRIAL	**I.1**	Fuego	No existe sistema de alarma contra incendios. Se posee un solo extintor de solkaflam (clase c) recomendados para incendios en lugares donde se encuentren equipos eléctricos.
	I.2	Daños por agua	La concentración del líquido sobrante por parte del aire acondicionado causaría daños en los equipos.
	I.*	Desastres industriales	No hay exposición o vulnerabilidad, por parte de esta amenaza.
	I.3	Contaminación mecánica	No hay exposición o vulnerabilidad, por parte de esta amenaza.
	I.4	Contaminación electromagnética	No hay exposición o vulnerabilidad, por parte de esta amenaza.
	I.5	Avería de origen físico o lógico	La manipulación por parte de cada uno de los componentes encontrados en la dependencia, como también por defectos de los componentes desde fabrica
	I.6	Corte del suministro eléctrico	Amenaza debida a factores externos, a clemencias de tipo naturales como lluvias u otros.
	I.7	Condiciones inadecuadas de temperatura o humedad	No se cuenta con una infraestructura adecuada para soportar los defectos del sistema de refrigeración.
	I.11	Emanaciones electromagnéticas	No hay exposición o vulnerabilidad, por parte de esta amenaza.
ERRORES Y FALLOS	**E.2**	Errores del administrador	Pérdida total o parcial del tiempo de ejecución de sus actividades, dependiendo de la gravedad del asunto.

Tabla 59. Estimación de la vulnerabilidad activo switch ALCATEL LUCEN 9550. (Continuación)

	E.23	Errores de mantenimiento / actualización de equipos(hardware)	Perjuicio a la mantenibilidad del sistema de información.
	E.24	Caída del sistema por agotamiento de recursos	Saturación del sistema informático.
	E.25	Perdida de equipos (Robo)	Recuperación de soportes reciclados o desechados.
ATAQUES INTENCIONADOS	**A.6**	Abuso de privilegios de acceso	Abuso de cada uno de los derechos otorgados.
	A.7	Uso no previsto	Implementación de recursos (económicos y de tiempo) en actividades no relacionadas.
	A.11	Acceso no autorizado	Uso ilícito del hardware
	A.23	Manipulación de los equipos	Sabotaje del hardware.
	A.24	Denegación de servicio	Saturación del sistema de información.
	A.25	Robo	Robo de porte de la información, puede esta ser física o digital.
	A.26	Ataque destructivo	Destrucción de los contenedores de la información, en recipientes físicos y lógicos.

Fuente: Autoría propia

Tabla 60. Estimación de la vulnerabilidad activo switch ALCATEL LUCEN 9551

ACTIVO TI		SWITCH ALCATEL LUCEN 9551	
ADMINISTRADOR		PIMIENTO CARDENAS WILSON MAURICIO	
TIPO DE ACTIVO		HARDWARE	
Tipo	**ID**	**Amenaza**	**Exposición/Vulnerabilidad**

Tabla 60. Estimación de la vulnerabilidad activo switch ALCATEL LUCEN 9551. (Continuación)

DESASTRES NATURALES	**N.1**	Fuego	No existe sistema de alarma contra incendios. Se posee un solo extintor de solkaflam (clase c) recomendados para incendios en lugares donde se encuentren equipos eléctricos.
	N.2	Daños por agua	La infraestructura está expuesta a goteras, cuenta con averías en el techo en donde el agua de las lluvias
	N.*	Desastres naturales	La oficina de la dependencia de sistemas se encuentra en zona baja de riesgo de desastre natural de origen volcánico debido a su cercanía con el volcán nevado del Tolima.
DE ORIGEN INDUSTRIAL	**I.1**	Fuego	No existe sistema de alarma contra incendios. Se posee un solo extintor de solkaflam (clase c) recomendados para incendios en lugares donde se encuentren equipos eléctricos.
	I.2	Daños por agua	La concentración del líquido sobrante por parte del aire acondicionado causaría daños en los equipos.
	I.*	Desastres industriales	No hay exposición o vulnerabilidad, por parte de esta amenaza.
	I.3	Contaminación mecánica	No hay exposición o vulnerabilidad, por parte de esta amenaza.
	I.4	Contaminación electromagnética	No hay exposición o vulnerabilidad, por parte de esta amenaza.
	I.5	Avería de origen físico o lógico	La manipulación por parte de cada uno de los componentes encontrados en la dependencia, como también por defectos de los componentes desde fabrica

Tabla 60. Estimación de la vulnerabilidad activo switch ALCATEL LUCEN 9551. (Continuación)

	I.6	Corte del suministro eléctrico	Amenaza debida a factores externos, a clemencias de tipo naturales como lluvias u otros.
	I.7	Condiciones inadecuadas de temperatura o humedad	No se cuenta con una infraestructura adecuada para soportar los defectos del sistema de refrigeración.
	I.11	Emanaciones electromagnéticas	No hay exposición o vulnerabilidad, por parte de esta amenaza.
ERRORES Y FALLOS NO INTENCIONADOS	**E.2**	Errores del administrador	Pérdida total o parcial del tiempo de ejecución de sus actividades, dependiendo de la gravedad del asunto.
	E.23	Errores de mantenimiento / actualización de equipos(hardware)	Perjuicio a la mantenibilidad del sistema de información.
	E.24	Caída del sistema por agotamiento de recursos	Saturación del sistema informático.
	E.25	Perdida de equipos (Robo)	Recuperación de soportes reciclados o desechados.
ATAQUES INTENCIONADOS	**A.6**	Abuso de privilegios de acceso	Abuso de cada uno de los derechos otorgados.
	A.7	Uso no previsto	Implementación de recursos (económicos y de tiempo) en actividades no relacionadas.
	A.11	Acceso no autorizado	Uso ilícito del hardware
	A.23	Manipulación de los equipos	Sabotaje del hardware.

Tabla 60. Estimación de la vulnerabilidad activo switch ALCATEL LUCEN 9551. (Continuación)

	A.24	Denegación de servicio	Saturación del sistema de información.
	A.25	Robo	Robo de porte de la información, puede esta ser física o digital.
	A.26	Ataque destructivo	Destrucción de los contenedores de la información, en recipientes físicos y lógicos.

Fuente: Autoría propia

Tabla 61. Estimación de la vulnerabilidad activo switch ALCATEL LUCEN 9552

ACTIVO TI		SWITCH ALCATEL LUCEN 9552	
ADMINISTRADOR		PIMIENTO CARDENAS WILSON MAURICIO	
TIPO DE ACTIVO		HARDWARE	
Tipo	**ID**	**Amenaza**	**Exposición/Vulnerabilidad**
DESASTRES NATURALES	**N.1**	Fuego	No existe sistema de alarma contra incendios. Se posee un solo extintor de solkaflam (clase c) recomendados para incendios en lugares donde se encuentren equipos eléctricos.
	N.2	Daños por agua	La infraestructura está expuesta a goteras, cuenta con averías en el techo en donde el agua de las lluvias
	N.*	Desastres naturales	La oficina de la dependencia de sistemas se encuentra en zona baja de riesgo de desastre natural de origen volcánico debido a su cercanía con el volcán nevado del Tolima.
DE ORIGEN INDUSTRIAL	**I.1**	Fuego	No existe sistema de alarma contra incendios. Se posee un solo extintor de solkaflam (clase c) recomendados para incendios en lugares donde se encuentren equipos eléctricos.

Tabla 61. Estimación de la vulnerabilidad activo switch ALCATEL LUCEN 9552. (Continuación)

	I.2	Daños por agua	La concentración del líquido sobrante por parte del aire acondicionado causaría daños en los equipos.
	I.*	Desastres industriales	No hay exposición o vulnerabilidad, por parte de esta amenaza.
	I.3	Contaminación mecánica	No hay exposición o vulnerabilidad, por parte de esta amenaza.
	I.4	Contaminación electromagnética	No hay exposición o vulnerabilidad, por parte de esta amenaza.
	I.5	Avería de origen físico o lógico	La manipulación por parte de cada uno de los componentes encontrados en la dependencia, como también por defectos de los componentes desde fabrica
	I.6	Corte del suministro eléctrico	Amenaza debida a factores externos, a clemencias de tipo naturales como lluvias u otros.
	I.7	Condiciones inadecuadas de temperatura o humedad	No se cuenta con una infraestructura adecuada para soportar los defectos del sistema de refrigeración.
	I.11	Emanaciones electromagnéticas	No hay exposición o vulnerabilidad, por parte de esta amenaza.
ERRORES Y FALLOS NO INTENCIONADOS	**E.2**	Errores del administrador	Pérdida total o parcial del tiempo de ejecución de sus actividades, dependiendo de la gravedad del asunto.
	E.23	Errores de mantenimiento / actualización de equipos(hardware)	Perjuicio a la mantenibilidad del sistema de información.

Tabla 61. Estimación de la vulnerabilidad activo switch ALCATEL LUCEN 9552. (Continuación)

	E.24	Caída del sistema por agotamiento de recursos	Saturación del sistema informático.
	E.25	Perdida de equipos (Robo)	Recuperación de soportes reciclados o desechados.
ATAQUES INTENCIONADOS	**A.6**	Abuso de privilegios de acceso	Abuso de cada uno de los derechos otorgados.
	A.7	Uso no previsto	Implementación de recursos (económicos y de tiempo) en actividades no relacionadas.
	A.11	Acceso no autorizado	Uso ilícito del hardware
	A.23	Manipulación de los equipos	Sabotaje del hardware.
	A.24	Denegación de servicio	Saturación del sistema de información.
	A.25	Robo	Robo de porte de la información, puede esta ser física o digital.
	A.26	Ataque destructivo	Destrucción de los contenedores de la información, en recipientes físicos y lógicos.

Fuente: Autoría propia

Tabla 62. Estimación de la vulnerabilidad activo switch ALCATEL LUCEN 9554

ACTIVO TI		SWITCH ALCATEL LUCEN 9554	
ADMINISTRADOR		PIMIENTO CARDENAS WILSON MAURICIO	
TIPO DE ACTIVO		HARDWARE	
Tipo	**ID**	**Amenaza**	**Exposición/Vulnerabilidad**
DESASTRES NATURA	**N.1**	Fuego	No existe sistema de alarma contra incendios. Se posee un solo extintor de solkaflam (clase c) recomendados para

Tabla 62. Estimación de la vulnerabilidad activo switch ALCATEL LUCEN 9554. (Continuación)

			incendios en lugares donde se encuentren equipos eléctricos.
	N.2	Daños por agua	La infraestructura está expuesta a goteras, cuenta con averías en el techo en donde el agua de las lluvias
	N.*	Desastres naturales	La oficina de la dependencia de sistemas se encuentra en zona baja de riesgo de desastre natural de origen volcánico debido a su cercanía con el volcán nevado del Tolima.
DE ORIGEN INDUSTRIAL	**I.1**	Fuego	No existe sistema de alarma contra incendios. Se posee un solo extintor de solkaflam (clase c) recomendados para incendios en lugares donde se encuentren equipos eléctricos.
	I.2	Daños por agua	La concentración del líquido sobrante por parte del aire acondicionado causaría daños en los equipos.
	I.*	Desastres industriales	No hay exposición o vulnerabilidad, por parte de esta amenaza.
	I.3	Contaminación mecánica	No hay exposición o vulnerabilidad, por parte de esta amenaza.
	I.4	Contaminación electromagnética	No hay exposición o vulnerabilidad, por parte de esta amenaza.
	I.5	Avería de origen físico o lógico	La manipulación por parte de cada uno de los componentes encontrados en la dependencia, como también por defectos de los componentes desde fabrica
	I.6	Corte del suministro eléctrico	Amenaza debida a factores externos, a clemencias de tipo naturales como lluvias u otros.

Tabla 62. Estimación de la vulnerabilidad activo switch ALCATEL LUCEN 9554. (Continuación)

	I.7	Condiciones inadecuadas de temperatura o humedad	No se cuenta con una infraestructura adecuada para soportar los defectos del sistema de refrigeración.
	I.11	Emanaciones electromagnéticas	No hay exposición o vulnerabilidad, por parte de esta amenaza.
ERRORES Y FALLOS NO INTENCIONADOS	**E.2**	Errores del administrador	Pérdida total o parcial del tiempo de ejecución de sus actividades, dependiendo de la gravedad del asunto.
	E.23	Errores de mantenimiento / actualización de equipos(hardware)	Perjuicio a la mantenibilidad del sistema de información.
	E.24	Caída del sistema por agotamiento de recursos	Saturación del sistema informático.
	E.25	Perdida de equipos (Robo)	Recuperación de soportes reciclados o desechados.
ATAQUES INTENCIONADOS	**A.6**	Abuso de privilegios de acceso	Abuso de cada uno de los derechos otorgados.
	A.7	Uso no previsto	Implementación de recursos (económicos y de tiempo) en actividades no relacionadas.
	A.11	Acceso no autorizado	Uso ilícito del hardware
	A.23	Manipulación de los equipos	Sabotaje del hardware.
	A.24	Denegación de servicio	Saturación del sistema de información.

Tabla 62. Estimación de la vulnerabilidad activo switch ALCATEL LUCEN 9554. (Continuación)

	A.25	Robo	Robo de porte de la información, puede esta ser física o digital.
	A.26	Ataque destructivo	Destrucción de los contenedores de la información, en recipientes físicos y lógicos.

Fuente: Autoría propia

Tabla 63. Estimación de la vulnerabilidad activo switch ALCATEL LUCEN 9555

ACTIVO TI	SWITCH ALCATEL LUCEN 9555	
ADMINISTRADOR	PIMIENTO CARDENAS WILSON MAURICIO	
TIPO DE ACTIVO	HARDWARE	
Tipo	**ID**	**Amenaza**	**Exposición/Vulnerabilidad**
DESASTRES NATURALES	**N.1**	Fuego	No existe sistema de alarma contra incendios. Se posee un solo extintor de solkaflam (clase c) recomendados para incendios en lugares donde se encuentren equipos eléctricos.
	N.2	Daños por agua	La infraestructura está expuesta a goteras, cuenta con averías en el techo en donde el agua de las lluvias
	N.*	Desastres naturales	La oficina de la dependencia de sistemas se encuentra en zona baja de riesgo de desastre natural de origen volcánico debido a su cercanía con el volcán nevado del Tolima.
ORIGEN INDUSTRIAL DE	**I.1**	Fuego	No existe sistema de alarma contra incendios. Se posee un solo extintor de solkaflam (clase c) recomendados para incendios en lugares donde se encuentren equipos eléctricos.
	I.2	Daños por agua	La concentración del líquido sobrante por parte del aire acondicionado causaría daños en los equipos.

Tabla 63. Estimación de la vulnerabilidad activo switch ALCATEL LUCEN 9555. (Continuación)

	I.*	Desastres industriales	No hay exposición o vulnerabilidad, por parte de esta amenaza.
	I.3	Contaminación mecánica	No hay exposición o vulnerabilidad, por parte de esta amenaza.
	I.4	Contaminación electromagnética	No hay exposición o vulnerabilidad, por parte de esta amenaza.
	I.5	Avería de origen físico o lógico	La manipulación por parte de cada uno de los componentes encontrados en la dependencia, como también por defectos de los componentes desde fabrica
	I.6	Corte del suministro eléctrico	Amenaza debida a factores externos, a clemencias de tipo naturales como lluvias u otros.
	I.7	Condiciones inadecuadas de temperatura o humedad	No se cuenta con una infraestructura adecuada para soportar los defectos del sistema de refrigeración.
	I.11	Emanaciones electromagnéticas	No hay exposición o vulnerabilidad, por parte de esta amenaza.
ERRORES Y FALLOS NO INTENCIONADOS	**E.2**	Errores del administrador	Pérdida total o parcial del tiempo de ejecución de sus actividades, dependiendo de la gravedad del asunto.
	E.23	Errores de mantenimiento / actualización de equipos(hardware)	Perjuicio a la mantenibilidad del sistema de información.
	E.24	Caída del sistema por agotamiento de recursos	Saturación del sistema informático.
	E.25	Perdida de equipos (Robo)	Recuperación de soportes reciclados o desechados.

Tabla 63. Estimación de la vulnerabilidad activo switch ALCATEL LUCEN 9555. (Continuación)

ATAQUES INTENCIONADOS	**A.6**	Abuso de privilegios de acceso	Abuso de cada uno de los derechos otorgados.
	A.7	Uso no previsto	Implementación de recursos (económicos y de tiempo) en actividades no relacionadas.
	A.11	Acceso no autorizado	Uso ilícito del hardware
	A.23	Manipulación de los equipos	Sabotaje del hardware.
	A.24	Denegación de servicio	Saturación del sistema de información.
	A.25	Robo	Robo de porte de la información, puede esta ser física o digital.
	A.26	Ataque destructivo	Destrucción de los contenedores de la información, en recipientes físicos y lógicos.

Fuente: Autoría propia

Tabla 64. Estimación de la vulnerabilidad activo switch ALCATEL LUCEN 9560

ACTIVO TI		SWITCH ALCATEL LUCEN 9560	
ADMINISTRADOR		PIMIENTO CARDENAS WILSON MAURICIO	
TIPO DE ACTIVO		HARDWARE	
Tipo	**ID**	**Amenaza**	**Exposición/Vulnerabilidad**
DESASTRES NATURALES	**N.1**	Fuego	No existe sistema de alarma contra incendios. Se posee un solo extintor de solkaflam (clase c) recomendados para incendios en lugares donde se encuentren equipos eléctricos.
	N.2	Daños por agua	La infraestructura está expuesta a goteras, cuenta con averías en el techo en donde el agua de las lluvias

Tabla 64. Estimación de la vulnerabilidad activo switch ALCATEL LUCEN 9560. (Continuación)

	N.*	Desastres naturales	La oficina de la dependencia de sistemas se encuentra en zona baja de riesgo de desastre natural de origen volcánico debido a su cercanía con el volcán nevado del Tolima.
DE ORIGEN INDUSTRIAL	**I.1**	Fuego	No existe sistema de alarma contra incendios. Se posee un solo extintor de solkaflam (clase c) recomendados para incendios en lugares donde se encuentren equipos eléctricos.
	I.2	Daños por agua	La concentración del líquido sobrante por parte del aire acondicionado causaría daños en los equipos.
	I.*	Desastres industriales	No hay exposición o vulnerabilidad, por parte de esta amenaza.
	I.3	Contaminación mecánica	No hay exposición o vulnerabilidad, por parte de esta amenaza.
	I.4	Contaminación electromagnética	No hay exposición o vulnerabilidad, por parte de esta amenaza.
	I.5	Avería de origen físico o lógico	La manipulación por parte de cada uno de los componentes encontrados en la dependencia, como también por defectos de los componentes desde fabrica
	I.6	Corte del suministro eléctrico	Amenaza debida a factores externos, a clemencias de tipo naturales como lluvias u otros.
	I.7	Condiciones inadecuadas de temperatura o humedad	No se cuenta con una infraestructura adecuada para soportar los defectos del sistema de refrigeración.
	I.11	Emanaciones electromagnéticas	No hay exposición o vulnerabilidad, por parte de esta amenaza.

Tabla 64. Estimación de la vulnerabilidad activo switch ALCATEL LUCEN 9560. (Continuación)

ERRORES Y FALLOS NO INTENCIONADOS	**E.2**	Errores del administrador	Pérdida total o parcial del tiempo de ejecución de sus actividades, dependiendo de la gravedad del asunto.
	E.23	Errores de mantenimiento / actualización de equipos(hardware)	Perjuicio a la mantenibilidad del sistema de información.
	E.24	Caída del sistema por agotamiento de recursos	Saturación del sistema informático.
	E.25	Perdida de equipos (Robo)	Recuperación de soportes reciclados o desechados.
ATAQUES INTENCIONADOS	**A.6**	Abuso de privilegios de acceso	Abuso de cada uno de los derechos otorgados.
	A.7	Uso no previsto	Implementación de recursos (económicos y de tiempo) en actividades no relacionadas.
	A.11	Acceso no autorizado	Uso ilícito del hardware
	A.23	Manipulación de los equipos	Sabotaje del hardware.
	A.24	Denegación de servicio	Saturación del sistema de información.
	A.25	Robo	Robo de porte de la información, puede esta ser física o digital.
	A.26	Ataque destructivo	Destrucción de los contenedores de la información, en recipientes físicos y lógicos.

Fuente: Autoría propia

Tabla 65. Estimación de la vulnerabilidad activo switch ayer 3 9574

ACTIVO TI		SWITCH LAYER3 95744	
ADMINISTRADOR		PIMIENTO CARDENAS WILSON MAURICIO	
TIPO DE ACTIVO		HARDWARE	
Tipo	**ID**	**Amenaza**	**Exposición/Vulnerabilidad**
DESASTRES NATURALES	**N.1**	Fuego	No existe sistema de alarma contra incendios. Se posee un solo extintor de solkaflam (clase c) recomendados para incendios en lugares donde se encuentren equipos eléctricos.
	N.2	Daños por agua	La infraestructura está expuesta a goteras, cuenta con averías en el techo en donde el agua de las lluvias
	N.*	Desastres naturales	La oficina de la dependencia de sistemas se encuentra en zona baja de riesgo de desastre natural de origen volcánico debido a su cercanía con el volcán nevado del Tolima.
DE ORIGEN INDUSTRIAL	**I.1**	Fuego	No existe sistema de alarma contra incendios. Se posee un solo extintor de solkaflam (clase c) recomendados para incendios en lugares donde se encuentren equipos eléctricos.
	I.2	Daños por agua	La concentración del líquido sobrante por parte del aire acondicionado causaría daños en los equipos.
	I.*	Desastres industriales	No hay exposición o vulnerabilidad, por parte de esta amenaza.
	I.3	Contaminación mecánica	No hay exposición o vulnerabilidad, por parte de esta amenaza.
	I.4	Contaminación electromagnética	No hay exposición o vulnerabilidad, por parte de esta amenaza.

Tabla 65. Estimación de la vulnerabilidad activo switch aver 3 9574. (Continuación)

	I.5	Avería de origen físico o lógico	La manipulación por parte de cada uno de los componentes encontrados en la dependencia, como también por defectos de los componentes desde fabrica
	I.6	Corte del suministro eléctrico	Amenaza debida a factores externos, a clemencias de tipo naturales como lluvias u otros.
	I.7	Condiciones inadecuadas de temperatura o humedad	No se cuenta con una infraestructura adecuada para soportar los defectos del sistema de refrigeración.
	I.11	Emanaciones electromagnéticas	No hay exposición o vulnerabilidad, por parte de esta amenaza.
ERRORES Y FALLOS NO INTENCIONADOS	**E.2**	Errores del administrador	Pérdida total o parcial del tiempo de ejecución de sus actividades, dependiendo de la gravedad del asunto.
	E.23	Errores de mantenimiento / actualización de equipos(hardware)	Perjuicio a la mantenibilidad del sistema de información.
	E.24	Caída del sistema por agotamiento de recursos	Saturación del sistema informático.
	E.25	Perdida de equipos (Robo)	Recuperación de soportes reciclados o desechados.
ATAQUES INTENCIONADOS	**A.6**	Abuso de privilegios de acceso	Abuso de cada uno de los derechos otorgados.
	A.7	Uso no previsto	Implementación de recursos (económicos y de tiempo) en actividades no relacionadas.

Tabla 65. Estimación de la vulnerabilidad activo switch aver 3 9574. (Continuación)

	A.11	Acceso no autorizado	Uso ilícito del hardware
	A.23	Manipulación de los equipos	Sabotaje del hardware.
	A.24	Denegación de servicio	Saturación del sistema de información.
	A.25	Robo	Robo de porte de la información, puede esta ser física o digital.
	A.26	Ataque destructivo	Destrucción de los contenedores de la información, en recipientes físicos y lógicos.

Fuente: Autoría propia

Tabla 66. Estimación de la vulnerabilidad activo switch layer 3 9576

ACTIVO TI		SWITCH LAYER 3 9576	
ADMINISTRADOR		PIMIENTO CARDENAS WILSON MAURICIO	
TIPO DE ACTIVO		HARDWARE	
Tipo	**ID**	**Amenaza**	**Exposición/Vulnerabilidad**
DESASTRES NATURALES	**N.1**	Fuego	No existe sistema de alarma contra incendios. Se posee un solo extintor de solkaflam (clase c) recomendados para incendios en lugares donde se encuentren equipos eléctricos.
	N.2	Daños por agua	La infraestructura está expuesta a goteras, cuenta con averías en el techo en donde el agua de las lluvias
	N.*	Desastres naturales	La oficina de la dependencia de sistemas se encuentra en zona baja de riesgo de desastre natural de origen volcánico debido a su cercanía con el volcán nevado del Tolima.

Tabla 66. Estimación de la vulnerabilidad activo switch layer 3 9576. (Continuación)

DE ORIGEN INDUSTRIAL	**I.1**	Fuego	No existe sistema de alarma contra incendios. Se posee un solo extintor de solkaflam (clase c) recomendados para incendios en lugares donde se encuentren equipos eléctricos.
	I.2	Daños por agua	La concentración del líquido sobrante por parte del aire acondicionado causaría daños en los equipos.
	I.*	Desastres industriales	No hay exposición o vulnerabilidad, por parte de esta amenaza.
	I.3	Contaminación mecánica	No hay exposición o vulnerabilidad, por parte de esta amenaza.
	I.4	Contaminación electromagnética	No hay exposición o vulnerabilidad, por parte de esta amenaza.
	I.5	Avería de origen físico o lógico	La manipulación por parte de cada uno de los componentes encontrados en la dependencia, como también por defectos de los componentes desde fabrica
	I.6	Corte del suministro eléctrico	Amenaza debida a factores externos, a clemencias de tipo naturales como lluvias u otros.
	I.7	Condiciones inadecuadas de temperatura o humedad	No se cuenta con una infraestructura adecuada para soportar los defectos del sistema de refrigeración.
	I.11	Emanaciones electromagnéticas	No hay exposición o vulnerabilidad, por parte de esta amenaza.
ERRORES Y FALLOS	**E.2**	Errores del administrador	Pérdida total o parcial del tiempo de ejecución de sus actividades, dependiendo de la gravedad del asunto.

Tabla 66. Estimación de la vulnerabilidad activo switch layer 3 9576. (Continuación)

	E.23	Errores de mantenimiento / actualización de equipos(hardware)	Perjuicio a la mantenibilidad del sistema de información.
	E.24	Caída del sistema por agotamiento de recursos	Saturación del sistema informático.
	E.25	Perdida de equipos (Robo)	Recuperación de soportes reciclados o desechados.
ATAQUES INTENCIONADOS	**A.6**	Abuso de privilegios de acceso	Abuso de cada uno de los derechos otorgados.
	A.7	Uso no previsto	Implementación de recursos (económicos y de tiempo) en actividades no relacionadas.
	A.11	Acceso no autorizado	Uso ilícito del hardware
	A.23	Manipulación de los equipos	Sabotaje del hardware.
	A.24	Denegación de servicio	Saturación del sistema de información.
	A.25	Robo	Robo de porte de la información, puede esta ser física o digital.
	A.26	Ataque destructivo	Destrucción de los contenedores de la información, en recipientes físicos y lógicos.

Fuente: Autoría propia

Tabla 67. Estimación de la vulnerabilidad activo switch layer 3 9577

ACTIVO TI		SWITCH LAYER 3 9577	
ADMINISTRADOR		PIMIENTO CARDENAS WILSON MAURICIO	
TIPO DE ACTIVO		HARDWARE	
Tipo	**ID**	**Amenaza**	**Exposición/Vulnerabilidad**

Tabla 67. Estimación de la vulnerabilidad activo switch laver 3 9577. (Continuación)

DESASTRES NATURALES	**N.1**	Fuego	No existe sistema de alarma contra incendios. Se posee un solo extintor de solkaflam (clase c) recomendados para incendios en lugares donde se encuentren equipos eléctricos.
	N.2	Daños por agua	La infraestructura está expuesta a goteras, cuenta con averías en el techo en donde el agua de las lluvias
	N.*	Desastres naturales	La oficina de la dependencia de sistemas se encuentra en zona baja de riesgo de desastre natural de origen volcánico debido a su cercanía con el volcán nevado del Tolima.
DE ORIGEN INDUSTRIAL	**I.1**	Fuego	No existe sistema de alarma contra incendios. Se posee un solo extintor de solkaflam (clase c) recomendados para incendios en lugares donde se encuentren equipos eléctricos.
	I.2	Daños por agua	La concentración del líquido sobrante por parte del aire acondicionado causaría daños en los equipos.
	I.*	Desastres industriales	No hay exposición o vulnerabilidad, por parte de esta amenaza.
	I.3	Contaminación mecánica	No hay exposición o vulnerabilidad, por parte de esta amenaza.
	I.4	Contaminación electromagnética	No hay exposición o vulnerabilidad, por parte de esta amenaza.
	I.5	Avería de origen físico o lógico	La manipulación por parte de cada uno de los componentes encontrados en la dependencia, como también por defectos de los componentes desde fabrica

Tabla 67. Estimación de la vulnerabilidad activo switch laver 3 9577. (Continuación)

	I.6	Corte del suministro eléctrico	Amenaza debida a factores externos, a clemencias de tipo naturales como lluvias u otros.
	I.7	Condiciones inadecuadas de temperatura o humedad	No se cuenta con una infraestructura adecuada para soportar los defectos del sistema de refrigeración.
	I.11	Emanaciones electromagnéticas	No hay exposición o vulnerabilidad, por parte de esta amenaza.
ERRORES Y FALLOS NO INTENCIONADOS	**E.2**	Errores del administrador	Pérdida total o parcial del tiempo de ejecución de sus actividades, dependiendo de la gravedad del asunto.
	E.23	Errores de mantenimiento / actualización de equipos(hardware)	Perjuicio a la mantenibilidad del sistema de información.
	E.24	Caída del sistema por agotamiento de recursos	Saturación del sistema informático.
	E.25	Perdida de equipos (Robo)	Recuperación de soportes reciclados o desechados.
ATAQUES INTENCIONADOS	**A.6**	Abuso de privilegios de acceso	Abuso de cada uno de los derechos otorgados.
	A.7	Uso no previsto	Implementación de recursos (económicos y de tiempo) en actividades no relacionadas.
	A.11	Acceso no autorizado	Uso ilícito del hardware
	A.23	Manipulación de los equipos	Sabotaje del hardware.

Tabla 67. Estimación de la vulnerabilidad activo switch layer 3 9577. (Continuación)

	A.24	Denegación de servicio	Saturación del sistema de información.
	A.25	Robo	Robo de porte de la información, puede esta ser física o digital.
	A.26	Ataque destructivo	Destrucción de los contenedores de la información, en recipientes físicos y lógicos.

Fuente: Autoría propia

Tabla 68. Estimación de la vulnerabilidad activo switch layer 3 9575

ACTIVO TI	SWITCH LAYER 3 9575		
ADMINISTRADOR	PIMIENTO CARDENAS WILSON MAURICIO		
TIPO DE ACTIVO	HARDWARE		
Tipo	**ID**	**Amenaza**	**Exposición/Vulnerabilidad**
DESASTRES NATURALES	**N.1**	Fuego	No existe sistema de alarma contra incendios. Se posee un solo extintor de solkaflam (clase c) recomendados para incendios en lugares donde se encuentren equipos eléctricos.
	N.2	Daños por agua	La infraestructura está expuesta a goteras, cuenta con averías en el techo en donde el agua de las lluvias
	N.*	Desastres naturales	La oficina de la dependencia de sistemas se encuentra en zona baja de riesgo de desastre natural de origen volcánico debido a su cercanía con el volcán nevado del Tolima.
DE ORIGEN INDUSTRIAL	**I.1**	Fuego	No existe sistema de alarma contra incendios. Se posee un solo extintor de solkaflam (clase c) recomendados para incendios en lugares donde se encuentren equipos eléctricos.

Tabla 68. Estimación de la vulnerabilidad activo switch layer 3 9575. (Continuación)

	I.2	Daños por agua	La concentración del líquido sobrante por parte del aire acondicionado causaría daños en los equipos.
	I.*	Desastres industriales	No hay exposición o vulnerabilidad, por parte de esta amenaza.
	I.3	Contaminación mecánica	No hay exposición o vulnerabilidad, por parte de esta amenaza.
	I.4	Contaminación electromagnética	No hay exposición o vulnerabilidad, por parte de esta amenaza.
	I.5	Avería de origen físico o lógico	La manipulación por parte de cada uno de los componentes encontrados en la dependencia, como también por defectos de los componentes desde fabrica
	I.6	Corte del suministro eléctrico	Amenaza debida a factores externos, a clemencias de tipo naturales como lluvias u otros.
	I.7	Condiciones inadecuadas de temperatura o humedad	No se cuenta con una infraestructura adecuada para soportar los defectos del sistema de refrigeración.
	I.11	Emanaciones electromagnéticas	No hay exposición o vulnerabilidad, por parte de esta amenaza.
ERRORES Y FALLOS NO INTENCIONADOS	**E.2**	Errores del administrador	Pérdida total o parcial del tiempo de ejecución de sus actividades, dependiendo de la gravedad del asunto.
	E.23	Errores de mantenimiento / actualización de equipos(hardware)	Perjuicio a la mantenibilidad del sistema de información.

Tabla 68. Estimación de la vulnerabilidad activo switch laver 3 9575. (Continuación)

	E.24	Caída del sistema por agotamiento de recursos	Saturación del sistema informático.
	E.25	Perdida de equipos (Robo)	Recuperación de soportes reciclados o desechados.
ATAQUES INTENCIONADOS	**A.6**	Abuso de privilegios de acceso	Abuso de cada uno de los derechos otorgados.
	A.7	Uso no previsto	Implementación de recursos (económicos y de tiempo) en actividades no relacionadas.
	A.11	Acceso no autorizado	Uso ilícito del hardware
	A.23	Manipulación de los equipos	Sabotaje del hardware.
	A.24	Denegación de servicio	Saturación del sistema de información.
	A.25	Robo	Robo de porte de la información, puede esta ser física o digital.
	A.26	Ataque destructivo	Destrucción de los contenedores de la información, en recipientes físicos y lógicos.

Fuente: Autoría propia

Tabla 69. Estimación de la vulnerabilidad activo router cisco modelo 1800 4781

ACTIVO TI		ROUTER CISCO MODELO 1800 4781	
ADMINISTRADOR		PIMIENTO CARDENAS WILSON MAURICIO	
TIPO DE ACTIVO		HARDWARE	
Tipo	**ID**	**Amenaza**	**Exposición/Vulnerabilidad**
DESASTRES NATURA	**N.1**	Fuego	No existe sistema de alarma contra incendios. Se posee un solo extintor de solkaflam (clase c) recomendados para

Tabla 69. Estimación de la vulnerabilidad activo router cisco modelo 1800 4781. (Continuación)

			incendios en lugares donde se encuentren equipos eléctricos.
	N.2	Daños por agua	La infraestructura está expuesta a goteras, cuenta con averías en el techo en donde el agua de las lluvias
	N.*	Desastres naturales	La oficina de la dependencia de sistemas se encuentra en zona baja de riesgo de desastre natural de origen volcánico debido a su cercanía con el volcán nevado del Tolima.
DE ORIGEN INDUSTRIAL	**I.1**	Fuego	No existe sistema de alarma contra incendios. Se posee un solo extintor de solkaflam (clase c) recomendados para incendios en lugares donde se encuentren equipos eléctricos.
	I.2	Daños por agua	La concentración del líquido sobrante por parte del aire acondicionado causaría daños en los equipos.
	I.*	Desastres industriales	No hay exposición o vulnerabilidad, por parte de esta amenaza.
	I.3	Contaminación mecánica	No hay exposición o vulnerabilidad, por parte de esta amenaza.
	I.4	Contaminación electromagnética	No hay exposición o vulnerabilidad, por parte de esta amenaza.
	I.5	Avería de origen físico o lógico	La manipulación por parte de cada uno de los componentes encontrados en la dependencia, como también por defectos de los componentes desde fabrica
	I.6	Corte del suministro eléctrico	Amenaza debida a factores externos, a clemencias de tipo naturales como lluvias u otros.

Tabla 69. Estimación de la vulnerabilidad activo router cisco modelo 1800 4781. (Continuación)

	I.7	Condiciones inadecuadas de temperatura o humedad	No se cuenta con una infraestructura adecuada para soportar los defectos del sistema de refrigeración.
	I.11	Emanaciones electromagnéticas	No hay exposición o vulnerabilidad, por parte de esta amenaza.
ERRORES Y FALLOS NO INTENCIONADOS	**E.2**	Errores del administrador	Pérdida total o parcial del tiempo de ejecución de sus actividades, dependiendo de la gravedad del asunto.
	E.23	Errores de mantenimiento / actualización de equipos(hardware)	Perjuicio a la mantenibilidad del sistema de información.
	E.24	Caída del sistema por agotamiento de recursos	Saturación del sistema informático.
	E.25	Perdida de equipos (Robo)	Recuperación de soportes reciclados o desechados.
ATAQUES INTENCIONADOS	**A.6**	Abuso de privilegios de acceso	Abuso de cada uno de los derechos otorgados.
	A.7	Uso no previsto	Implementación de recursos (económicos y de tiempo) en actividades no relacionadas.
	A.11	Acceso no autorizado	Uso ilícito del hardware
	A.23	Manipulación de los equipos	Sabotaje del hardware.
	A.24	Denegación de servicio	Saturación del sistema de información.

Tabla 69. Estimación de la vulnerabilidad activo router cisco modelo 1800 4781. (Continuación)

	A.25	Robo	Robo de porte de la información, puede esta ser física o digital.
	A.26	Ataque destructivo	Destrucción de los contenedores de la información, en recipientes físicos y lógicos.

Fuente: Autoría propia

Tabla 70. Estimación de la vulnerabilidad activo red telefónica

ACTIVO TI	RED TELEFÓNICA		
ADMINISTRADOR	PIMIENTO CARDENAS WILSON MAURICIO		
TIPO DE ACTIVO	REDES DE COMUNICACIÓN		
Tipo	**ID**	**Amenaza**	**Exposición/Vulnerabilidad**
DE ORIGEN INDUSTRIAL	**I.8**	Fallo de servicios de comunicaciones	Atentados externos por parte de grupos ha margen de la ley que puedan atentar contra la infraestructura que trasmite cada uno de los servicios.
ERRORES Y FALLOS NO INTENCIONADOS	**E.2**	Errores del administrador	Pérdida total o parcial del tiempo de ejecución de sus actividades, dependiendo de la gravedad del asunto.
	E.9	Errores de [re-] encaminamiento	La dependencia cuenta con sistemas de cifrado y verificación (puerto – puerto) para el manejo de la movilidad de la información.
	E.10	Errores de secuencia	La dependencia cuenta con sistemas de cifrado y verificación (puerto – puerto) para el manejo de la movilidad de la información.
	E.15	Alteración accidental de la información	La dependencia cuenta con sistemas de cifrado y verificación (puerto – puerto) para el manejo de la movilidad de la información.
	E.18	Destrucción de información	El departamento de sistemas cuenta con copias de seguridad periódicas

Tabla 70. Estimación de la vulnerabilidad activo red telefónica. (Continuación)

	E.19	Fugas de información	Las personas contratadas están atadas a cláusulas de confidencialidad.
	E.24	Caída del sistema por agotamiento de recursos	Saturación del sistema informático.
ATAQUES INTENCIONADOS	**A.5**	Suplantación de la identidad del usuario	Acceso a personas que no cuenten con los permisos necesarios o con las credenciales necesarias.
	A.6	Abuso de privilegios de acceso	Abuso de cada uno de los derechos otorgados.
	A.7	Uso no previsto	Implementación de recursos (económicos y de tiempo) en actividades no relacionadas.
	A.9	[Re-]encaminamiento de mensajes	La dependencia cuenta con sistemas de cifrado y verificación (puerto – puerto) para el manejo de la movilidad de la información.
	A.10	Alteración de secuencia	Alteración de datos.
	A.11	Acceso no autorizado	Uso ilícito de la red telefónica
	A.12	Análisis de trafico	Análisis de cada uno de los datos transitados por la red interna de la institución.
	A.14	Interceptación de información (escucha)	Escucha pasiva.
	A.15	Modificación deliberada de la información	Datos erróneos en el momento de la movilización de la información.

Tabla 70. Estimación de la vulnerabilidad activo red telefónica. (Continuación)

	A.19	Divulgación de información	Información filtrada abiertamente a personas no correspondientes.
	A.24	Denegación de servicio	Saturación del sistema de información.

Fuente: Autoría propia

Tabla 71. Estimación de la vulnerabilidad activo internet movistar

ACTIVO TI	INTERNET MOVISTAR
ADMINISTRADOR	PIMIENTO CARDENAS WILSON MAURICIO
TIPO DE ACTIVO	REDES DE COMUNICACIÓN

Tipo	ID	Amenaza	Exposición/Vulnerabilidad
DE ORIGEN INDUSTRIAL	**I.8**	Fallo de servicios de comunicaciones	Atentados externos por parte de grupos ha margen de la ley que puedan atentar contra la infraestructura que trasmite cada uno de los servicios.
ERRORES Y FALLOS NO INTENCIONADOS	**E.2**	Errores del administrador	Pérdida total o parcial del tiempo de ejecución de sus actividades, dependiendo de la gravedad del asunto.
	E.9	Errores de [re-] encaminamiento	La dependencia cuenta con sistemas de cifrado y verificación (puerto – puerto) para el manejo de la movilidad de la información.
	E.10	Errores de secuencia	La dependencia cuenta con sistemas de cifrado y verificación (puerto – puerto) para el manejo de la movilidad de la información.
	E.15	Alteración accidental de la información	La dependencia cuenta con sistemas de cifrado y verificación (puerto – puerto) para el manejo de la movilidad de la información.
	E.18	Destrucción de información	El departamento de sistemas cuenta con copias de seguridad periódicas

Tabla 71. Estimación de la vulnerabilidad activo internet movistar. (Continuación)

	E.19	Fugas de información	Las personas contratadas están atadas a cláusulas de confidencialidad.
	E.24	Caída del sistema por agotamiento de recursos	Saturación del sistema informático.
ATAQUES INTENCIONADOS	**A.5**	Suplantación de la identidad del usuario	Acceso a personas que no cuenten con los permisos necesarios o con las credenciales necesarias.
	A.6	Abuso de privilegios de acceso	Abuso de cada uno de los derechos otorgados.
	A.7	Uso no previsto	Implementación de recursos (económicos y de tiempo) en actividades no relacionadas.
	A.9	[Re-]encaminamiento de mensajes	La dependencia cuenta con sistemas de cifrado y verificación (puerto – puerto) para el manejo de la movilidad de la información.
	A.10	Alteración de secuencia	Alteración de datos.
	A.11	Acceso no autorizado	Uso ilícito del internet movistar
	A.12	Análisis de trafico	Análisis de cada uno de los datos transitados por la red interna de la institución.
	A.14	Interceptación de información (escucha)	Escucha pasiva.
	A.15	Modificación deliberada de la información	Datos erróneos en el momento de la movilización de la información.

Tabla 71. Estimación de la vulnerabilidad activo internet movistar. (Continuación)

	A.19	Divulgación de información	Información filtrada abiertamente a personas no correspondientes.
	A.24	Denegación de servicio	Saturación del sistema de información.

Fuente: Autoría propia

Tabla 72. Estimación de la vulnerabilidad activo red LAN

ACTIVO TI	RED LAN		
ADMINISTRADOR	PIMIENTO CARDENAS WILSON MAURICIO		
TIPO DE ACTIVO	REDES DE COMUNICACIÓN		
Tipo	**ID**	**Amenaza**	**Exposición/Vulnerabilidad**
DE ORIGEN INDUSTRIAL	**I.8**	Fallo de servicios de comunicaciones	Atentados externos por parte de grupos ha margen de la ley que puedan atentar contra la infraestructura que trasmite cada uno de los servicios.
ERRORES Y FALLOS NO INTENCIONADOS	**E.2**	Errores del administrador	Pérdida total o parcial del tiempo de ejecución de sus actividades, dependiendo de la gravedad del asunto.
	E.9	Errores de [re-] encaminamiento	La dependencia cuenta con sistemas de cifrado y verificación (puerto – puerto) para el manejo de la movilidad de la información.
	E.10	Errores de secuencia	La dependencia cuenta con sistemas de cifrado y verificación (puerto – puerto) para el manejo de la movilidad de la información.
	E.15	Alteración accidental de la información	La dependencia cuenta con sistemas de cifrado y verificación (puerto – puerto) para el manejo de la movilidad de la información.
	E.18	Destrucción de información	El departamento de sistemas cuenta con copias de seguridad periódicas

Tabla 72. Estimación de la vulnerabilidad activo red LAN. (Continuación)

	E.19	Fugas de información	Las personas contratadas están atadas a cláusulas de confidencialidad.
	E.24	Caída del sistema por agotamiento de recursos	Saturación del sistema informático.
ATAQUES INTENCIONADOS	**A.5**	Suplantación de la identidad del usuario	Acceso a personas que no cuenten con los permisos necesarios o con las credenciales necesarias.
	A.6	Abuso de privilegios de acceso	Abuso de cada uno de los derechos otorgados.
	A.7	Uso no previsto	Implementación de recursos (económicos y de tiempo) en actividades no relacionadas.
	A.9	[Re-]encaminamiento de mensajes	La dependencia cuenta con sistemas de cifrado y verificación (puerto – puerto) para el manejo de la movilidad de la información.
	A.10	Alteración de secuencia	Alteración de datos.
	A.11	Acceso no autorizado	Uso ilícito de la red LAN
	A.12	Análisis de trafico	Análisis de cada uno de los datos transitados por la red interna de la institución.
	A.14	Interceptación de información (escucha)	Escucha pasiva.
	A.15	Modificación deliberada de la información	Datos erróneos en el momento de la movilización de la información.

Tabla 72. Estimación de la vulnerabilidad activo red LAN. (Continuación)

	A.19	Divulgación de información	Información filtrada abiertamente a personas no correspondientes.
	A.24	Denegación de servicio	Saturación del sistema de información.

Fuente: Autoría propia

Tabla 73. Estimación de la vulnerabilidad activo red WIFI

ACTIVO TI	RED WIFI
ADMINISTRADOR	PIMIENTO CARDENAS WILSON MAURICIO
TIPO DE ACTIVO	REDES DE COMUNICACIÓN

Tipo	ID	Amenaza	Exposición/Vulnerabilidad
DE ORIGEN INDUSTRIAL	**I.8**	Fallo de servicios de comunicaciones	Atentados externos por parte de grupos ha margen de la ley que puedan atentar contra la infraestructura que trasmite cada uno de los servicios.
ERRORES Y FALLOS NO INTENCIONADOS	**E.2**	Errores del administrador	Pérdida total o parcial del tiempo de ejecución de sus actividades, dependiendo de la gravedad del asunto.
	E.9	Errores de [re-] encaminamiento	La dependencia cuenta con sistemas de cifrado y verificación (puerto – puerto) para el manejo de la movilidad de la información.
	E.10	Errores de secuencia	La dependencia cuenta con sistemas de cifrado y verificación (puerto – puerto) para el manejo de la movilidad de la información.
	E.15	Alteración accidental de la información	La dependencia cuenta con sistemas de cifrado y verificación (puerto – puerto) para el manejo de la movilidad de la información.
	E.18	Destrucción de información	El departamento de sistemas cuenta con copias de seguridad periódicas

Tabla 73. Estimación de la vulnerabilidad activo red WIFI. (Continuación)

	E.19	Fugas de información	Las personas contratadas están atadas a cláusulas de confidencialidad.
	E.24	Caída del sistema por agotamiento de recursos	Saturación del sistema informático.
ATAQUES INTENCIONADOS	**A.5**	Suplantación de la identidad del usuario	Acceso a personas que no cuenten con los permisos necesarios o con las credenciales necesarias.
	A.6	Abuso de privilegios de acceso	Abuso de cada uno de los derechos otorgados.
	A.7	Uso no previsto	Implementación de recursos (económicos y de tiempo) en actividades no relacionadas.
	A.9	[Re-]encaminamiento de mensajes	La dependencia cuenta con sistemas de cifrado y verificación (puerto – puerto) para el manejo de la movilidad de la información.
	A.10	Alteración de secuencia	Alteración de datos.
	A.11	Acceso no autorizado	Uso ilícito de la red WIFI
	A.12	Análisis de trafico	Análisis de cada uno de los datos transitados por la red interna de la institución.
	A.14	Interceptación de información (escucha)	Escucha pasiva.
	A.15	Modificación deliberada de la información	Datos erróneos en el momento de la movilización de la información.

Tabla 73. Estimación de la vulnerabilidad activo red WIFI. (Continuación)

	A.19	Divulgación de información	Información filtrada abiertamente a personas no correspondientes.
	A.24	Denegación de servicio	Saturación del sistema de información.

Fuente: Autoría propia

Tabla 74. Estimación de la vulnerabilidad activo red de datos

ACTIVO TI	RED DE DATOS		
ADMINISTRADOR	PIMIENTO CARDENAS WILSON MAURICIO		
TIPO DE ACTIVO	REDES DE COMUNICACIÓN		
Tipo	**ID**	**Amenaza**	**Exposición/Vulnerabilidad**
DE ORIGEN INDUSTRIAL	**I.8**	Fallo de servicios de comunicaciones	Atentados externos por parte de grupos ha margen de la ley que puedan atentar contra la infraestructura que trasmite cada uno de los servicios.
ERRORES Y FALLOS NO INTENCIONADOS	**E.2**	Errores del administrador	Pérdida total o parcial del tiempo de ejecución de sus actividades, dependiendo de la gravedad del asunto.
	E.9	Errores de [re-] encaminamiento	La dependencia cuenta con sistemas de cifrado y verificación (puerto – puerto) para el manejo de la movilidad de la información.
	E.10	Errores de secuencia	La dependencia cuenta con sistemas de cifrado y verificación (puerto – puerto) para el manejo de la movilidad de la información.
	E.15	Alteración accidental de la información	La dependencia cuenta con sistemas de cifrado y verificación (puerto – puerto) para el manejo de la movilidad de la información.
	E.18	Destrucción de información	El departamento de sistemas cuenta con copias de seguridad periódicas

Tabla 74. Estimación de la vulnerabilidad activo red de datos. (Continuación)

	E.19	Fugas de información	Las personas contratadas están atadas a cláusulas de confidencialidad.
	E.24	Caída del sistema por agotamiento de recursos	Saturación del sistema informático.
ATAQUES INTENCIONADOS	**A.5**	Suplantación de la identidad del usuario	Acceso a personas que no cuenten con los permisos necesarios o con las credenciales necesarias.
	A.6	Abuso de privilegios de acceso	Abuso de cada uno de los derechos otorgados.
	A.7	Uso no previsto	Implementación de recursos (económicos y de tiempo) en actividades no relacionadas.
	A.9	[Re-]encaminamiento de mensajes	La dependencia cuenta con sistemas de cifrado y verificación (puerto – puerto) para el manejo de la movilidad de la información.
	A.10	Alteración de secuencia	Alteración de datos.
	A.11	Acceso no autorizado	Uso ilícito de la red de datos
	A.12	Análisis de trafico	Análisis de cada uno de los datos transitados por la red interna de la institución.
	A.14	Interceptación de información (escucha)	Escucha pasiva.
	A.15	Modificación deliberada de la información	Datos erróneos en el momento de la movilización de la información.

Tabla 74. Estimación de la vulnerabilidad activo red de datos. (Continuación)

	A.19	Divulgación de información	Información filtrada abiertamente a personas no correspondientes.
	A.24	Denegación de servicio	Saturación del sistema de información.

Fuente: Autoría propia

Tabla 75. Estimación de la vulnerabilidad activo DDS 1TB

ACTIVO TI		DDS 1TB	
ADMINISTRADOR		PIMIENTO CARDENAS WILSON MAURICIO	
TIPO DE ACTIVO		SOPORTES DE INFORMACIÓN	
Tipo	ID	Amenaza	Exposición/Vulnerabilidad
DESASTRES NATURALES	**N.1**	Fuego	No existe sistema de alarma contra incendios. Se posee un solo extintor de solkaflam (clase c) recomendados para incendios en lugares donde se encuentren equipos eléctricos.
	N.2	Daños por agua	La infraestructura está expuesta a goteras, cuenta con averías en el techo en donde el agua de las lluvias
	N.*	Desastres naturales	La oficina de la dependencia de sistemas se encuentra en zona baja de riesgo de desastre natural de origen volcánico debido a su cercanía con el volcán nevado del Tolima.
DE ORIGEN INDUSTRIAL	**I.1**	Fuego	No existe sistema de alarma contra incendios. Se posee un solo extintor de solkaflam (clase c) recomendados para incendios en lugares donde se encuentren equipos eléctricos.
	I.2	Daños por agua	La concentración del líquido sobrante por parte del aire acondicionado causaría daños en los equipos.
	I.*	Desastres industriales	No hay exposición o vulnerabilidad, por parte de esta amenaza.

Tabla 75. Estimación de la vulnerabilidad activo DDS 1TB. (Continuación)

	I.3	Contaminación mecánica	No hay exposición o vulnerabilidad, por parte de esta amenaza.
	I.4	Contaminación electromagnética	No hay exposición o vulnerabilidad, por parte de esta amenaza.
	I.5	Avería de origen físico o lógico	La manipulación por parte de cada uno de los componentes encontrados en la dependencia, como también por defectos de los componentes desde fabrica
	I.6	Corte del suministro eléctrico	Amenaza debida a factores externos, a clemencias de tipo naturales como lluvias u otros.
	I.7	Condiciones inadecuadas de temperatura o humedad	No se cuenta con una infraestructura adecuada para soportar los defectos del sistema de refrigeración.
	I.10	Degradación de los soportes de almacén amiento de la información	Pérdida gradual de cada uno de los registros históricos de la dependencia.
	I.11	Emanaciones electromagnéticas	No hay exposición o vulnerabilidad, por parte de esta amenaza.
ERRORES Y FALLOS NO INTENCIONADOS	**E.1**	Errores de los usuarios	Pérdida total o parcial del tiempo de ejecución de sus actividades, dependiendo de la gravedad del asunto.
	E.2	Errores del administrador	Pérdida total o parcial del tiempo de ejecución de sus actividades, dependiendo de la gravedad del asunto.
	E.15	Alteración accidental de la información	La dependencia cuenta con sistemas de cifrado y verificación (puerto – puerto) para el manejo de la movilidad de la información.

Tabla 75. Estimación de la vulnerabilidad activo DDS 1TB. (Continuación)

	E.18	Destrucción de información	El departamento de sistemas cuenta con copias de seguridad periódicas
	E.19	Fugas de información	Las personas contratadas están atadas a cláusulas de confidencialidad.
	E.23	Errores de mantenimiento / actualización de equipos(hardware)	Perjuicio a la mantenibilidad del sistema de información.
	E.25	Perdida de equipos (Robo)	Recuperación de soportes reciclados o desechados.
ATAQUES INTENCIONADOS	**A.7**	Uso no previsto	Implementación de recursos (económicos y de tiempo) en actividades no relacionadas.
	A.11	Acceso no autorizado	Uso ilícito del DDS 1TB
	A.15	Modificación deliberada de la información	Datos erróneos en el momento de la movilización de la información.
	A.18	Destrucción de información	Perdida de la información.
	A.19	Divulgación de información	Información filtrada abiertamente a personas no correspondientes.
	A.23	Manipulación de los equipos	Sabotaje del hardware y software conteniente.
	A.25	Robo	Robo de porte de la información, puede esta ser física o digital.
	A.26	Ataque destructivo	Destrucción de los contenedores de la información, en recipientes físicos y lógicos.

Fuente: Autoría propia

Tabla 76. Estimación de la vulnerabilidad activo materiales físicos

ACTIVO TI		MATERIALES FÍSICOS	
ADMINISTRADOR		PIMIENTO CARDENAS WILSON MAURICIO	
TIPO DE ACTIVO		SOPORTES DE INFORMACIÓN	
Tipo	**ID**	**Amenaza**	**Exposición/Vulnerabilidad**
DESASTRES NATURALES	**N.1**	Fuego	No existe sistema de alarma contra incendios. Se posee un solo extintor de solkaflam (clase c) recomendados para incendios en lugares donde se encuentren equipos eléctricos.
	N.2	Daños por agua	La infraestructura está expuesta a goteras, cuenta con averías en el techo en donde el agua de las lluvias
	N.*	Desastres naturales	La oficina de la dependencia de sistemas se encuentra en zona baja de riesgo de desastre natural de origen volcánico debido a su cercanía con el volcán nevado del Tolima.
DE ORIGEN INDUSTRIAL	**I.1**	Fuego	No existe sistema de alarma contra incendios. Se posee un solo extintor de solkaflam (clase c) recomendados para incendios en lugares donde se encuentren equipos eléctricos.
	I.2	Daños por agua	La concentración del líquido sobrante por parte del aire acondicionado causaría daños en los equipos.
	I.*	Desastres industriales	No hay exposición o vulnerabilidad, por parte de esta amenaza.
	I.3	Contaminación mecánica	No hay exposición o vulnerabilidad, por parte de esta amenaza.
	I.4	Contaminación electromagnética	No hay exposición o vulnerabilidad, por parte de esta amenaza.

Tabla 76. Estimación de la vulnerabilidad activo materiales físicos. (Continuación)

	I.5	Avería de origen físico o lógico	La manipulación por parte de cada uno de los componentes encontrados en la dependencia, como también por defectos de los componentes desde fabrica
	I.6	Corte del suministro eléctrico	Amenaza debida a factores externos, a clemencias de tipo naturales como lluvias u otros.
	I.7	Condiciones inadecuadas de temperatura o humedad	No se cuenta con una infraestructura adecuada para soportar los defectos del sistema de refrigeración.
	I.10	Degradación de los soportes de almacén amiento de la información	Pérdida gradual de cada uno de los registros históricos de la dependencia.
	I.11	Emanaciones electromagnéticas	No hay exposición o vulnerabilidad, por parte de esta amenaza.
ERRORES Y FALLOS NO INTENCIONADOS	**E.1**	Errores de los usuarios	Pérdida total o parcial del tiempo de ejecución de sus actividades, dependiendo de la gravedad del asunto.
	E.2	Errores del administrador	Pérdida total o parcial del tiempo de ejecución de sus actividades, dependiendo de la gravedad del asunto.
	E.15	Alteración accidental de la información	La dependencia cuenta con sistemas de cifrado y verificación (puerto – puerto) para el manejo de la movilidad de la información.
	E.18	Destrucción de información	El departamento de sistemas cuenta con copias de seguridad periódicas
	E.19	Fugas de información	Las personas contratadas están atadas a cláusulas de confidencialidad.

Tabla 76. Estimación de la vulnerabilidad activo materiales físicos. (Continuación)

	E.23	Errores de mantenimiento / actualización de equipos(hardware)	Perjuicio a la mantenibilidad del sistema de información.
	E.25	Perdida de equipos (Robo)	Recuperación de soportes reciclados o desechados.
ATAQUES INTENCIONADOS	**A.7**	Uso no previsto	Implementación de recursos (económicos y de tiempo) en actividades no relacionadas.
	A.11	Acceso no autorizado	Uso ilícito del hardware
	A.15	Modificación deliberada de la información	Datos erróneos en el momento de la movilización de la información.
	A.18	Destrucción de información	Perdida de la información.
	A.19	Divulgación de información	Información filtrada abiertamente a personas no correspondientes.
	A.23	Manipulación de los equipos	Sabotaje del hardware y software conteniente.
	A.25	Robo	Robo de porte de la información, puede esta ser física o digital.
	A.26	Ataque destructivo	Destrucción de los contenedores de la información, en recipientes físicos y lógicos.

Fuente: Autoría propia

Tabla 77. Estimación de la vulnerabilidad activo UPS 10 KVA 9578

ACTIVO TI		UPS 10 KVA 9578	
ADMINISTRADOR		PIMIENTO CARDENAS WILSON MAURICIO	
TIPO DE ACTIVO		EQUIPAMIENTO AUXILIAR	
Tipo	**ID**	**Amenaza**	**Exposición/Vulnerabilidad**

Tabla 77. Estimación de la vulnerabilidad activo UPS 10 KVA 9578. (Continuación)

DESASTRES NATURALES	**N.1**	Fuego	No existe sistema de alarma contra incendios. Se posee un solo extintor de solkaflam (clase c) recomendados para incendios en lugares donde se encuentren equipos eléctricos.
	N.2	Daños por agua	La infraestructura está expuesta a goteras, cuenta con averías en el techo en donde el agua de las lluvias
	N.*	Desastres naturales	La oficina de la dependencia de sistemas se encuentra en zona baja de riesgo de desastre natural de origen volcánico debido a su cercanía con el volcán nevado del Tolima.
DE ORIGEN INDUSTRIAL	**I.1**	Fuego	No existe sistema de alarma contra incendios. Se posee un solo extintor de solkaflam (clase c) recomendados para incendios en lugares donde se encuentren equipos eléctricos.
	I.2	Daños por agua	La concentración del líquido sobrante por parte del aire acondicionado causaría daños en los equipos.
	I.*	Desastres industriales	No hay exposición o vulnerabilidad, por parte de esta amenaza.
	I.3	Contaminación mecánica	No hay exposición o vulnerabilidad, por parte de esta amenaza.
	I.4	Contaminación electromagnética	No hay exposición o vulnerabilidad, por parte de esta amenaza.
	I.5	Avería de origen físico o lógico	La manipulación por parte de cada uno de los componentes encontrados en la dependencia, como también por defectos de los componentes desde fabrica

Tabla 77. Estimación de la vulnerabilidad activo UPS 10 KVA 9578. (Continuación)

	I.6	Corte del suministro eléctrico	Amenaza debida a factores externos, a clemencias de tipo naturales como lluvias u otros.
	I.7	Condiciones inadecuadas de temperatura o humedad	No se cuenta con una infraestructura adecuada para soportar los defectos del sistema de refrigeración.
	I.9	Interrupción de otros servicios y suministros esenciales	No hay exposición o vulnerabilidad, por parte de esta amenaza.
	I.11	Emanaciones electromagnéticas	No hay exposición o vulnerabilidad, por parte de esta amenaza.
ERRORES Y FALLOS NO INTENCIONADOS	**E.23**	Errores de mantenimiento / actualización de equipos(hardware)	Perjuicio a la mantenibilidad del sistema de información.
	E.25	Perdida de equipos (Robo)	Recuperación de soportes reciclados o desechados.
ATAQUES INTENCIONADOS	**A.7**	Uso no previsto	Implementación de recursos (económicos y de tiempo) en actividades no relacionadas.
	A.11	Acceso no autorizado	Uso ilícito del hardware
	A.23	Manipulación de los equipos	Sabotaje del hardware y software conteniente.
	A.25	Robo	Robo de porte de la información, puede esta ser física o digital.
	A.26	Ataque destructivo	Destrucción de los contenedores de la información, en recipientes físicos y lógicos.

Fuente: Autoría propia

Tabla 78. Estimación de la vulnerabilidad activo UPS 10 KVA 9579

ACTIVO TI		UPS 10 KVA 9579	
ADMINISTRADOR		PIMIENTO CARDENAS WILSON MAURICIO	
TIPO DE ACTIVO		EQUIPAMIENTO AUXILIAR	
Tipo	**ID**	**Amenaza**	**Exposición/Vulnerabilidad**
DESASTRES NATURALES	**N.1**	Fuego	No existe sistema de alarma contra incendios. Se posee un solo extintor de solkaflam (clase c) recomendados para incendios en lugares donde se encuentren equipos eléctricos.
	N.2	Daños por agua	La infraestructura está expuesta a goteras, cuenta con averías en el techo en donde el agua de las lluvias
	N.*	Desastres naturales	La oficina de la dependencia de sistemas se encuentra en zona baja de riesgo de desastre natural de origen volcánico debido a su cercanía con el volcán nevado del Tolima.
DE ORIGEN INDUSTRIAL	**I.1**	Fuego	No existe sistema de alarma contra incendios. Se posee un solo extintor de solkaflam (clase c) recomendados para incendios en lugares donde se encuentren equipos eléctricos.
	I.2	Daños por agua	La concentración del líquido sobrante por parte del aire acondicionado causaría daños en los equipos.
	I.*	Desastres industriales	No hay exposición o vulnerabilidad, por parte de esta amenaza.
	I.3	Contaminación mecánica	No hay exposición o vulnerabilidad, por parte de esta amenaza.
	I.4	Contaminación electromagnética	No hay exposición o vulnerabilidad, por parte de esta amenaza.

Tabla 78. Estimación de la vulnerabilidad activo UPS 10 KVA 9579. (Continuación)

	I.5	Avería de origen físico o lógico	La manipulación por parte de cada uno de los componentes encontrados en la dependencia, como también por defectos de los componentes desde fabrica
	I.6	Corte del suministro eléctrico	Amenaza debida a factores externos, a clemencias de tipo naturales como lluvias u otros.
	I.7	Condiciones inadecuadas de temperatura o humedad	No se cuenta con una infraestructura adecuada para soportar los defectos del sistema de refrigeración.
	I.9	Interrupción de otros servicios y suministros esenciales	No hay exposición o vulnerabilidad, por parte de esta amenaza.
	I.11	Emanaciones electromagnéticas	No hay exposición o vulnerabilidad, por parte de esta amenaza.
ERRORES Y FALLOS NO INTENCIONADOS	**E.23**	Errores de mantenimiento / actualización de equipos(hardware)	Perjuicio a la mantenibilidad del sistema de información.
	E.25	Perdida de equipos (Robo)	Recuperación de soportes reciclados o desechados.
ATAQUES INTENCIONADOS	**A.7**	Uso no previsto	Implementación de recursos (económicos y de tiempo) en actividades no relacionadas.
	A.11	Acceso no autorizado	Uso ilícito del hardware
	A.23	Manipulación de los equipos	Sabotaje del hardware y software conteniente.

Tabla 78. Estimación de la vulnerabilidad activo UPS 10 KVA 9579. (Continuación)

	A.25	Robo	Robo de porte de la información, puede esta ser física o digital.
	A.26	Ataque destructivo	Destrucción de los contenedores de la información, en recipientes físicos y lógicos.

Fuente: Autoría propia

Tabla 79. Estimación de la vulnerabilidad activo UPS 10 KVA 9580

ACTIVO TI		UPS 10 KVA 9580	
ADMINISTRADOR		PIMIENTO CARDENAS WILSON MAURICIO	
TIPO DE ACTIVO		EQUIPAMIENTO AUXILIAR	
Tipo	**ID**	**Amenaza**	**Exposición/Vulnerabilidad**
DESASTRES NATURALES	**N.1**	Fuego	No existe sistema de alarma contra incendios. Se posee un solo extintor de solkaflam (clase c) recomendados para incendios en lugares donde se encuentren equipos eléctricos.
	N.2	Daños por agua	La infraestructura está expuesta a goteras, cuenta con averías en el techo en donde el agua de las lluvias
	N.*	Desastres naturales	La oficina de la dependencia de sistemas se encuentra en zona baja de riesgo de desastre natural de origen volcánico debido a su cercanía con el volcán nevado del Tolima.
ORIGEN DE INDUSTRIAL	**I.1**	Fuego	No existe sistema de alarma contra incendios. Se posee un solo extintor de solkaflam (clase c) recomendados para incendios en lugares donde se encuentren equipos eléctricos.
	I.2	Daños por agua	La concentración del líquido sobrante por parte del aire acondicionado causaría daños en los equipos.

Tabla 79. Estimación de la vulnerabilidad activo UPS 10 KVA 9580. (Continuación)

	I.*	Desastres industriales	No hay exposición o vulnerabilidad, por parte de esta amenaza.
	I.3	Contaminación mecánica	No hay exposición o vulnerabilidad, por parte de esta amenaza.
	I.4	Contaminación electromagnética	No hay exposición o vulnerabilidad, por parte de esta amenaza.
	I.5	Avería de origen físico o lógico	La manipulación por parte de cada uno de los componentes encontrados en la dependencia, como también por defectos de los componentes desde fabrica
	I.6	Corte del suministro eléctrico	Amenaza debida a factores externos, a clemencias de tipo naturales como lluvias u otros.
	I.7	Condiciones inadecuadas de temperatura o humedad	No se cuenta con una infraestructura adecuada para soportar los defectos del sistema de refrigeración.
	I.9	Interrupción de otros servicios y suministros esenciales	No hay exposición o vulnerabilidad, por parte de esta amenaza.
	I.11	Emanaciones electromagnéticas	No hay exposición o vulnerabilidad, por parte de esta amenaza.
ERRORES Y FALLOS NO INTENCIONADOS	**E.23**	Errores de mantenimiento / actualización de equipos(hardware)	Perjuicio a la mantenibilidad del sistema de información.
	E.25	Perdida de equipos (Robo)	Recuperación de soportes reciclados o desechados.

Tabla 79. Estimación de la vulnerabilidad activo UPS 10 KVA 9580. (Continuación)

ATAQUES INTENCIONADOS	**A.7**	Uso no previsto	Implementación de recursos (económicos y de tiempo) en actividades no relacionadas.
	A.11	Acceso no autorizado	Uso ilícito del hardware
	A.23	Manipulación de los equipos	Sabotaje del hardware y software conteniente.
	A.25	Robo	Robo de porte de la información, puede esta ser física o digital.
	A.26	Ataque destructivo	Destrucción de los contenedores de la información, en recipientes físicos y lógicos.

Fuente: Autoría propia

Tabla 80. Estimación de la vulnerabilidad activo cuarto o recinto (oficina)

ACTIVO TI	CUARTO O RECINTO (OFICINA)		
ADMINISTRADOR	PIMIENTO CARDENAS WILSON MAURICIO		
TIPO DE ACTIVO	INSTALACIONES		
Tipo	**ID**	**Amenaza**	**Exposición/Vulnerabilidad**
DESASTRES NATURALES	**N.1**	Fuego	No existe sistema de alarma contra incendios. Se posee un solo extintor de solkaflam (clase c) recomendados para incendios en lugares donde se encuentren equipos eléctricos.
	N.2	Daños por agua	La infraestructura está expuesta a goteras, cuenta con averías en el techo en donde el agua de las lluvias
	N.*	Desastres naturales	La oficina de la dependencia de sistemas se encuentra en zona baja de riesgo de desastre natural de origen volcánico debido a su cercanía con el volcán nevado del Tolima.

Tabla 80. Estimación de la vulnerabilidad activo cuarto o recinto (oficina) . (Continuación)

DE ORIGEN INDUSTRIAL	**I.1**	Fuego	No existe sistema de alarma contra incendios. Se posee un solo extintor de solkaflam (clase c) recomendados para incendios en lugares donde se encuentren equipos eléctricos.
	I.2	Daños por agua	La concentración del líquido sobrante por parte del aire acondicionado causaría daños en los equipos.
	I.*	Desastres industriales	No hay exposición o vulnerabilidad, por parte de esta amenaza.
	I.11	Emanaciones electromagnéticas	No hay exposición o vulnerabilidad, por parte de esta amenaza.
ERRORES Y FALLOS NO INTENCIONADOS	**E.15**	Alteración accidental de la información	La dependencia cuenta con sistemas de cifrado y verificación (puerto – puerto) para el manejo de la movilidad de la información.
	E.18	Destrucción de información	El departamento de sistemas cuenta con copias de seguridad periódicas
	E.19	Fugas de información	Las personas contratadas están atadas a cláusulas de confidencialidad.
ATAQUES INTENCIONADOS	**A.7**	Uso no previsto	Implementación de recursos (económicos y de tiempo) en actividades no relacionadas.
	A.11	Acceso no autorizado	Uso ilícito del hardware
	A.15	Modificación deliberada de la información	Datos erróneos en el momento de la movilización de la información.
	A.18	Destrucción de información	Perdida de la información.

Tabla 80. Estimación de la vulnerabilidad activo cuarto o recinto (oficina) . (Continuación)

	A.19	Divulgación de información	Información filtrada abiertamente a personas no correspondientes.
	A.26	Ataque destructivo	Destrucción de los contenedores de la información, en recipientes físicos y lógicos.
	A.27	Ocupación enemiga	Divulgación de información no consentida.

Fuente: Autoría propia

Tabla 81. Estimación de la vulnerabilidad activo coordinador de sistemas

ACTIVO TI		COORDINADOR DE SISTEMAS	
ADMINISTRADOR		PIMIENTO CARDENAS WILSON MAURICIO	
TIPO DE ACTIVO		PERSONAL	
Tipo	**ID**	**Amenaza**	**Exposición/Vulnerabilidad**
ERRORES Y FALLOS NO INTENCIONADOS	**E.7**	Deficiencias en la organización	No hay exposición o vulnerabilidad, por parte de esta amenaza.
	E.19	Fugas de información	Las personas contratadas están atadas a cláusulas de confidencialidad.
	E.28	Indisponibilidad del personal	Daño a la disponibilidad de cada una de las personas influyentes en la dependencia.
ATAQUES INTENCIONADOS	**A.28**	Indisponibilidad del personal	Daño a la disponibilidad de la información.
	A.29	Extorsión	Influenciarían al personal capacitado.
	A.30	Ingeniería social (picaresca)	Intervención de personas con fines no éticas.

Fuente: Autoría propia

Tabla 82. Estimación de la vulnerabilidad activo programador

ACTIVO TI		PROGRAMADOR	
ADMINISTRADOR		PIMIENTO CARDENAS WILSON MAURICIO	
TIPO DE ACTIVO		PERSONAL	
Tipo	**ID**	**Amenaza**	**Exposición/Vulnerabilidad**

Tabla 82. Estimación de la vulnerabilidad activo programador. (Continuación)

ERRORES Y FALLOS NO INTENCIONADOS	**E.7**	Deficiencias en la organización	No hay exposición o vulnerabilidad, por parte de esta amenaza.
	E.19	Fugas de información	Las personas contratadas están atadas a cláusulas de confidencialidad.
	E.28	Indisponibilidad del personal	Daño a la disponibilidad de cada una de las personas influyentes en la dependencia.
ATAQUES INTENCIONADOS	**A.28**	Indisponibilidad del personal	Daño a la disponibilidad de la información.
	A.29	Extorsión	Influenciarían al personal capacitado.
	A.30	Ingeniería social (picaresca)	Intervención de personas con fines no éticas.

Fuente: Autoría propia

Tabla 83. Estimación de la vulnerabilidad activo ingeniero auxiliar/ soporte técnico

ACTIVO TI	INGENIERO AUXILIAR/ SOPORTE TÉCNICO		
ADMINISTRADOR	PIMIENTO CARDENAS WILSON MAURICIO		
TIPO DE ACTIVO	PERSONAL		
Tipo	**ID**	**Amenaza**	**Exposición/Vulnerabilidad**
ERRORES Y FALLOS NO INTENCIONADOS	**E.7**	Deficiencias en la organización	No hay exposición o vulnerabilidad, por parte de esta amenaza.
	E.19	Fugas de información	Las personas contratadas están atadas a cláusulas de confidencialidad.
	E.28	Indisponibilidad del personal	Daño a la disponibilidad de cada una de las personas influyentes en la dependencia.
ATAQUES INTENCIONADOS	**A.28**	Indisponibilidad del personal	Daño a la disponibilidad de la información.
	A.29	Extorsión	Influenciarían al personal capacitado.
	A.30	Ingeniería social (picaresca)	Intervención de personas con fines no éticas.

Fuente: Autoría propia

ANEXO 4

CONTENIDO

LISTA DE TABLAS

1. ESTIMACIÓN DEL IMPACTO QUE CAUSARÍA LA PÉRDIDA DE CADA ACTIVO

Tabla 1. Estimación del impacto en cada uno de los activos.

ID	CANTIDAD	ACTIVO	DISPONIBILIDAD	INTEGRIDAD	CONFIDENCIALIDAD	Valoración del activo	
						NIVEL	VALOR
I-DU	N	Inventario de usuarios	Muy bajo	Alto	Muy alto	Muy alto	5
E-ORG	N	estructura organizacional	Muy bajo	Alto	Muy alto	Muy alto	5
I-DC	N	Inventario de contratos	Muy bajo	Alto	Muy alto	Muy alto	5
R-DA	N	Registro de actividades	Muy bajo	Alto	Muy alto	Muy alto	5
R-ME	N	Registro Mantenimiento equipos	Muy bajo	Alto	Muy alto	Muy alto	5
R-AE	N	Registro de la arquitectura de los equipos	Muy bajo	Alto	Muy alto	Muy alto	5
S-EC	N	Soporte equipos de computo	Muy alto	Muy alto	Muy bajo	Muy alto	5
S-PV	N	Soporte de plataformas virtuales	Muy alto	Muy alto	Muy bajo	Muy alto	5

Tabla 1. Estimación del impacto en cada uno de los activos. (Continuación)

VLAN-ADMON	1	Vlan de administración	Alto	Muy alto	Bajo	Muy alto	5
VLAN-FINAN	1	Vlan de financiera	Alto	Muy alto	Bajo	Muy alto	5
VLAN-TESO	1	Vlan de tesorería	Alto	Muy alto	Bajo	Muy alto	5
VLAN-EST	1	Vlan de estudiantes	Alto	Muy alto	Bajo	Muy alto	5
V-WIFI	1	Vlan de wifi	Alto	Muy alto	Bajo	Muy alto	5
VLAN-CONF	1	Vlan de configuración	Alto	Muy alto	Bajo	Muy alto	5
VLAN-SIS	1	Vlan de sistemas	Alto	Muy alto	Bajo	Muy alto	5
VLAN-RYCA	1	Vlan de registro y control	Alto	Muy alto	Bajo	Muy alto	5
VLAN-ALMA	1	Vlan de almacén	Alto	Muy alto	Bajo	Muy alto	5
VLAN-TALEN	1	Vlan de talento humano	Alto	Muy alto	Bajo	Muy alto	5
BACK UP-SISTEMAS	N	Copias de seguridad de cada pc de la dependencia de sistemas	Muy alto	Muy alto	Alto	Muy alto	5
BACK UP-ITFIP	N	Copias de seguridad de cada pc de las dependencias de la institución	Muy alto	Muy alto	Alto	Muy alto	5
BACK UP-SERVER'S	N	Copia de seguridad de las configuraciones de los servidores	Muy alto	Muy alto	Alto	Muy alto	5
PASS-BIO	N	Contraseña biométrica para acceso a la sala del servidor	Muy bajo	Alto	Muy alto	Muy alto	5
PASS-SERVER	N	Contraseña de los usuarios que acceden a los servidores	Muy bajo	Alto	Muy alto	Muy alto	5

Tabla 1. Estimación del impacto en cada uno de los activos. (Continuación)

PASS-SERVER-BACK UP	N	Contraseña del servidor de copias de seguridad	Muy bajo	Alto	Muy alto	Muy alto	5
PASS-PC-ITFIP	N	Contraseña de usuarios de los Pc de las demás dependencias	bajo	Muy alto	Muy alto	Muy alto	5
PASS-S-BIO	N	Contraseña sensor biométrico	bajo	Alto	Alto	Alto	5
C-CASERVER	N	Código de acceso a la sala de servidor	bajo	Muy alto	Muy alto	Muy alto	5
S-RYCA1	1	Sistema de Registro y Control Académico (RYCA) V.1	alto	Alto	Alto	Alto	5
S-RYCA2	1	Sistema de Registro y Control Académico (RYCA) V.2.0	alto	Alto	Alto	Alto	5
P-ITFIP	1	Página Oficial del ITFIP	Muy alto	Alto	Bajo	Alto	3
G-CHROME	N	Navegador Google Chrome	Muy alto	Muy alto	Muy alto	Muy alto	1
M-F	N	Navegador Mozilla Firefox	Muy alto	Muy alto	Muy alto	Muy alto	1
SAFI	N	Navegador Safari	Muy alto	Muy alto	Muy alto	Muy alto	1
M-OFFICE	N	Microsoft Office 2013	Alto	Alto	Muy alto	Alto	3
O-OLINUX	N	Open Office Linux 2017	Alto	Alto	Muy alto	Alto	2
S-CENTER	N	Antivirus System Center	Muy alto	Muy alto	Muy alto	Muy alto	2
W-DEFEN	N	Antivirus Windows Defender	Muy alto	Muy alto	Muy alto	Muy alto	2
W-8	N	Sistema Operativo Windows 8	Muy alto	Muy alto	Muy alto	Muy alto	3
W-SER09	N	Sistema Operativo Windows Server 2009	Muy alto	Muy alto	Muy alto	Muy alto	5

Tabla 1. Estimación del impacto en cada uno de los activos. (Continuación)

W-SER12	N	Sistema Operativo Windows Server 2012	Muy alto	Muy alto	Muy alto	Muy alto	5
C-5	N	Sistema Operativo CentOS 5	Muy alto	Muy alto	Muy alto	Muy alto	5
D-7	N	Sistema Operativo Debian 7	Muy alto	Muy alto	Muy alto	Muy alto	5
U-14	N	Sistema Operativo Ubuntu 14	Muy alto	Muy alto	Muy alto	Muy alto	2
M-OSX	N	Sistema Operativo Mac OS X	Muy alto	Muy alto	Muy alto	Muy alto	5
CMD	N	Terminal CoMmanD (CMD)	Muy alto	Muy alto	Muy alto	Muy alto	2
C-LMAC	N	Terminal CoMmanD line (Mac)	Muy alto	Muy alto	Muy alto	Muy alto	3
TERM	N	Terminal Linux	Muy alto	Muy alto	Muy alto	Muy alto	2
S-DNS	N	Servidor DNS y DHCP	Alto	Muy alto	Muy alto	Muy alto	8
S-RYCA2	N	Servidor Plataforma RYCA V.2.0	Alto	Muy alto	Muy alto	Muy alto	8
S-RYCA1	N	Servidor Plataforma RYCA V.1	Muy alto	Muy alto	Muy alto	Muy alto	8
S-BD	N	Servidor de Base de Datos ITFIP	Alto	Muy alto	Muy alto	Muy alto	8
S-FIREW	N	Servidor Firewall Fortigate	alto	Muy alto	Muy alto	Muy alto	8
S-SIIGO	N	Servidor Contable SIIGO	Muy alto	Muy alto	Muy alto	Muy alto	8
S-PDESA	N	Servidor de Pruebas “Desarrollito”	Alto	Muy alto	Muy alto	Muy alto	3

Tabla 1. Estimación del impacto en cada uno de los activos. (Continuación)

S-CSECURITY	N	Servidor de Copias de seguridad de la información del ITFIP	Muy alto	Muy alto	Muy alto	Muy alto	8
022400532 AL 022400534	3	Computador IMAC APPLE	Medio	Alto	Medio	Medio	5
022400570 AL 022400192	18	Computadores HP all-one Pro	Medio	Alto	Medio	Medio	3
022400540 AL 022400565	16	Portátil Toshiba	Alto	Alto	Muy bajo	Alto	3
022400675	1	Tablet negra 9”	Muy alto	Medio	Muy bajo	Muy bajo	2
022400534 AL 022400537	3	Computador IMAC APPLE	Muy alto	Alto	Muy bajo	Muy bajo	5
MUSB234	N	Memoria USB	Medio	Bajo	Bajo	Bajo	2
DD234	N	Discos duros	Medio	Bajo	Bajo	Bajo	3
DDX334	N	Discos duros externos	Medio	Bajo	Bajo	Bajo	3
020700059	1	SWITCH ALCATEL LUCEN 9553	Muy alto	Alto	bajo	Muy alto	5
020700130	1	SWITCH 24 10/100/1000 BASE T C SWITCH 24 10/100/1000 BASE T C	Muy alto	Alto	Alto	Alto	5
020700158	1	SWITCH 24/10/100/1000 BASE T4S	Muy alto	Alto	Alto	Alto	5
020700136	1	SWITCH 24/10/100/1000PWR CORD	Muy alto	Alto	Alto	Alto	5
020700067	1	SWITCH ALCATEL LUCEN 9561	Muy alto	Alto	Alto	Alto	5

Tabla 1. Estimación del impacto en cada uno de los activos. (Continuación)

020700062	1	SWITCH ALCATEL LUCEN 9556	Muy alto	Alto	Alto	Alto	5
020700063	1	SWITCH ALCATEL LUCEN 9557	Muy alto	Alto	Alto	Alto	5
020700064	1	SWITCH ALCATEL LUCEN 9558	Muy alto	Alto	Alto	Alto	5
020700065	1	SWITCH ALCATEL LUCEN 9559	Muy alto	Alto	Alto	Alto	5
020700049	1	SWITCH ALCATEL LUCEN 9543	Muy alto	Alto	Alto	Alto	5
020700050	1	SWITCH ALCATEL LUCEN 9544	Muy alto	Alto	Alto	Alto	5
020700051	1	SWITCH ALCATEL LUCEN 9545	Muy alto	Alto	Alto	Alto	5
020700054	1	SWITCH ALCATEL LUCEN 9548	Muy alto	Alto	Alto	Alto	5
020700056	1	SWITCH ALCATEL LUCEN 9550	Muy alto	Alto	Alto	Alto	5
020700057	1	SWITCH ALCATEL LUCEN 9551	Muy alto	Alto	Alto	Alto	5
020700058	1	SWITCH ALCATEL LUCEN 9552	Muy alto	Alto	Alto	Alto	5
020700060	1	SWITCH ALCATEL LUCEN 9554	Muy alto	Alto	Alto	Alto	5
020700061	1	SWITCH ALCATEL LUCEN 9555	Muy alto	Alto	Alto	Alto	5
020700066	1	SWITCH ALCATEL LUCEN 9560	Muy alto	Alto	Alto	Alto	5
020700080	1	SWITCH LAYER 3 9574	Muy alto	Alto	Alto	Alto	5

Tabla 1. Estimación del impacto en cada uno de los activos. (Continuación)

020700082	1	SWITCH LAYER 3 9576	Muy alto	Alto	Alto	Alto	5
020700083	1	SWITCH LAYER 3 9577	Muy alto	Alto	Alto	Alto	5
020700081	1	SWITCH LAYER 3 9575	Muy alto	Alto	Alto	Alto	5
	1	ROUTER CISCO MODELO 1800 4781	Alto	Medio	Medio	Medio	5
	1	Red Wi-fi ITFIP	Muy alto	Medio	Medio	Medio	2
	1	Red Wi-fi ITFIP 2	Muy alto	Medio	Medio	Medio	2
	1	Red Wi-fi ITFIP_P1	Muy alto	Medio	Medio	Medio	2
	1	Red Wi-fi ITFIP_FUNCIONARIOS_P1	Bajo	Medio	Medio	Medio	2
	1	Red Wi-fi Salas1y2	Muy alto	Medio	Medio	Medio	2
	1	Red Wi-fi Salas_Sis2	Muy alto	Medio	Medio	Medio	2
	1	Red Wi-fi Rectoría	Bajo	Medio	Medio	Medio	2
DSK1024	5	DDS 1TB	Muy bajo	Muy alto	Muy alto	Muy alto	3
022400526	1	UPS 10 KVA 9578	Muy alto	Medio	Medio	Medio	5
022400527	1	UPS 10 KVA 9579	Muy alto	Medio	Medio	Medio	5
022400528	1	UPS 10 KVA 9580	Muy alto	Medio	Medio	Medio	5

Fuente: Autoría propia

2. ESTIMACIÓN DE LA PROBABILIDAD DE QUE OCURRA PERDIDA DEL ACTIVO

Tabla 2. Estimación de la probabilidad activo de cada pc de la dependencia de sistemas

ACTIVO TI	COPIAS DE SEGURIDAD DE CADA PC DE LA DEPENDENCIA DE SISTEMAS
ADMINISTRADOR	PIMIENTO CARDENAS WILSON MAURICIO
DEGRADACIÓN	80%
IMPACTO	5
TIPO DE ACTIVO	DATOS/INFORMACIÓN

Tipo	ID	Amenaza	Exposición/Vulnerabilidad	Frecuencia (F)	
ERRORES Y FALLOS NO INTENCIONADOS	**E.1**	Errores de los usuarios	Pérdida total o parcial del tiempo de ejecución de sus actividades, dependiendo de la gravedad del asunto.	Baja	3
	E.2	Errores del administrador	Pérdida total o parcial del tiempo de ejecución de sus actividades, dependiendo de la gravedad del asunto.	Baja	3
	E.15	Alteración accidental de la información	La dependencia cuenta con sistemas de cifrado y verificación (puerto – puerto) para el manejo de la movilidad de la información.	Baja	3
	E.18	Destrucción de información	El departamento de sistemas cuenta con copias de seguridad periódicas	Media	4
	E.19	Fugas de información	Las personas contratadas están atadas a cláusulas de confidencialidad.	Media	4
ATAQUES INTENCIO	**A.5**	Suplantación de la identidad del usuario	Acceso a personas que no cuenten con los permisos necesarios o con las credenciales necesarias.	Media	4

Tabla 2. Estimación de la probabilidad activo de cada pc de la dependencia de sistemas. (Continuación)

	A.6	Abuso de privilegios de acceso	Abuso de cada uno de los derechos otorgados.	Media	4
	A.11	Acceso no autorizado	Uso ilícito del hardware	Media	4
	A.15	Modificación deliberada de la información	Datos erróneos en el momento de la movilización de la información.	Media	4
	A.18	Destrucción de información	Perdida de la información.	Media	4
	A.19	Divulgación de información	Información filtrada abiertamente a personas no correspondientes.	Media	4

Fuente: Autoría propia

Tabla 3. Estimación de la probabilidad activo de cada pc de las dependencias de la institución

ACTIVO TI	COPIAS DE SEGURIDAD DE CADA PC DE LAS DEPENDENCIAS DE LA INSTITUCIÓN
ADMINISTRADOR	PIMIENTO CARDENAS WILSON MAURICIO
DEGRADACIÓN	80%
IMPACTO	5
TIPO DE ACTIVO	DATOS/INFORMACIÓN

Tipo	**ID**	**Amenaza**	**Exposición/Vulnerabilidad**	**Frecuencia (F)**	
ERRORES Y FALLOS NO INTENCIONADOS	**E.1**	Errores de los usuarios	Pérdida total o parcial del tiempo de ejecución de sus actividades, dependiendo de la gravedad del asunto.	Baja	3
	E.2	Errores del administrador	Pérdida total o parcial del tiempo de ejecución de sus actividades, dependiendo de la gravedad del asunto.	Baja	3
	E.15	Alteración accidental de la información	La dependencia cuenta con sistemas de cifrado y verificación (puerto – puerto)	Baja	3

Tabla 3. Estimación de la probabilidad activo de cada pc de las dependencias de la institución. (Continuación)

			para el manejo de la movilidad de la información.		
	E.18	Destrucción de información	El departamento de sistemas cuenta con copias de seguridad periódicas	Media	4
	E.19	Fugas de información	Las personas contratadas están atadas a cláusulas de confidencialidad.	Media	4
ATAQUES INTENCIONAD	**A.5**	Suplantación de la identidad del usuario	Acceso a personas que no cuenten con los permisos necesarios o con las credenciales necesarias.	Media	4
	A.6	Abuso de privilegios de acceso	Abuso de cada uno de los derechos otorgados.	Media	4
	A.11	Acceso no autorizado	Uso ilícito del hardware	Media	4
	A.15	Modificación deliberada de la información	Datos erróneos en el momento de la movilización de la información.	Media	4
	A.18	Destrucción de información	Perdida de la información.	Media	4
	A.19	Divulgación de información	Información filtrada abiertamente a personas no correspondientes.	Media	4

Fuente: Autoría propia

Tabla 4. Estimación de la probabilidad activo de las configuraciones de los servidores

ACTIVO TI	COPIAS DE SEGURIDAD DE LAS CONFIGURACIONES DE LOS SERVIDORES
ADMINISTRADOR	PIMIENTO CARDENAS WILSON MAURICIO
DEGRADACIÓN	90%
IMPACTO	5
TIPO DE ACTIVO	DATOS/INFORMACIÓN

Tabla 4. Estimación de la probabilidad activo de las configuraciones de los servidores. (Continuación)

Tipo	ID	Amenaza	Exposición/Vulnerabilidad	Frecuencia (F)	
ERRORES Y FALLOS NO INTENCIONADOS	**E.1**	Errores de los usuarios	Pérdida total o parcial del tiempo de ejecución de sus actividades, dependiendo de la gravedad del asunto.	Baja	3
	E.2	Errores del administrador	Pérdida total o parcial del tiempo de ejecución de sus actividades, dependiendo de la gravedad del asunto.	Baja	3
	E.15	Alteración accidental de la información	La dependencia cuenta con sistemas de cifrado y verificación (puerto – puerto) para el manejo de la movilidad de la información.	Baja	3
	E.18	Destrucción de información	El departamento de sistemas cuenta con copias de seguridad periódicas	Media	4
	E.19	Fugas de información	Las personas contratadas están atadas a cláusulas de confidencialidad.	Media	4
ATAQUES INTENCIONAD	**A.5**	Suplantación de la identidad del usuario	Acceso a personas que no cuenten con los permisos necesarios o con las credenciales necesarias.	Media	4
	A.6	Abuso de privilegios de acceso	Abuso de cada uno de los derechos otorgados.	Media	4
	A.11	Acceso no autorizado	Uso ilícito del hardware	Media	4
	A.15	Modificación deliberada de la información	Datos erróneos en el momento de la movilización de la información.	Media	4

Tabla 4. Estimación de la probabilidad activo de las configuraciones de los servidores. (Continuación)

	A.18	Destrucción de información	Perdida de la información.	Media	4
	A.19	Divulgación de información	Información filtrada abiertamente a personas no correspondientes.	Media	4

Fuente: Autoría propia

Tabla 5. Estimación de la probabilidad activo biométricas para acceso a la sala de servidor

ACTIVO TI	CONTRASEÑAS BIOMÉTRICAS PARA ACCESO A LA SALA DE SERVIDOR
ADMINISTRADOR	PIMIENTO CARDENAS WILSON MAURICIO
DEGRACIÓN	100%
IMPACTO	5
TIPO DE ACTIVO	DATOS/INFORMACIÓN

Tipo	**ID**	**Amenaza**	**Exposición/Vulnerabilidad**	**Frecuencia (F)**	
ERRORES Y FALLOS NO INTENCIONADOS	**E.1**	Errores de los usuarios	Pérdida total o parcial del tiempo de ejecución de sus actividades, dependiendo de la gravedad del asunto.	Baja	3
	E.2	Errores del administrador	Pérdida total o parcial del tiempo de ejecución de sus actividades, dependiendo de la gravedad del asunto.	Baja	3
	E.15	Alteración accidental de la información	La dependencia cuenta con sistemas de cifrado y verificación (puerto – puerto) para el manejo de la movilidad de la información.	Baja	3
	E.18	Destrucción de información	El departamento de sistemas cuenta con copias de seguridad periódicas	Media	4
	E.19	Fugas de información	Las personas contratadas están atadas a cláusulas de confidencialidad.	Media	4

Tabla 5. Estimación de la probabilidad activo biométricas para acceso a la sala de servidor. (Continuación)

ATAQUES INTENCIONAD	**A.5**	Suplantación de la identidad del usuario	Acceso a personas que no cuenten con los permisos necesarios o con las credenciales necesarias.	Media	4
	A.6	Abuso de privilegios de acceso	Abuso de cada uno de los derechos otorgados.	Media	4
	A.11	Acceso no autorizado	Uso ilícito del hardware	Media	4
	A.15	Modificación deliberada de la información	Datos erróneos en el momento de la movilización de la información.	Media	4
	A.18	Destrucción de información	Perdida de la información.	Media	4
	A.19	Divulgación de información	Información filtrada abiertamente a personas no correspondientes.	Media	4

Fuente: Autoría propia

Tabla 6. Estimación de la probabilidad activo de los usuarios que acceden a los servidores

ACTIVO TI		CONTRASEÑAS DE LOS USUARIOS QUE ACCEDEN A LOS SERVIDORES			
ADMINISTRADOR		PIMIENTO CARDENAS WILSON MAURICIO			
DEGRACIÓN		100%			
IMPACTO		5			
TIPO DE ACTIVO		DATOS/INFORMACIÓN			
Tipo	**ID**	**Amenaza**	**Exposición/Vulnerabilidad**	**Frecuencia (F)**	
ERRORES Y FALLOS NO	**E.1**	Errores de los usuarios	Pérdida total o parcial del tiempo de ejecución de sus actividades, dependiendo de la gravedad del asunto.	Baja	3
	E.2	Errores del administrador	Pérdida total o parcial del tiempo de ejecución de sus	Baja	3

Tabla 6. Estimación de la probabilidad activo de los usuarios que acceden a los servidores. (Continuación)

			actividades, dependiendo de la gravedad del asunto.		
	E.15	Alteración accidental de la información	La dependencia cuenta con sistemas de cifrado y verificación (puerto – puerto) para el manejo de la movilidad de la información.	Baja	3
	E.18	Destrucción de información	El departamento de sistemas cuenta con copias de seguridad periódicas	Media	4
	E.19	Fugas de información	Las personas contratadas están atadas a cláusulas de confidencialidad.	Media	4
ATAQUES INTENCIONAD	**A.5**	Suplantación de la identidad del usuario	Acceso a personas que no cuenten con los permisos necesarios o con las credenciales necesarias.	Media	4
	A.6	Abuso de privilegios de acceso	Abuso de cada uno de los derechos otorgados.	Media	4
	A.11	Acceso no autorizado	Uso ilícito del hardware	Media	4
	A.15	Modificación deliberada de la información	Datos erróneos en el momento de la movilización de la información.	Media	4
	A.18	Destrucción de información	Perdida de la información.	Media	4
	A.19	Divulgación de información	Información filtrada abiertamente a personas no correspondientes.	Media	4

Fuente: Autoría propia

Tabla 7. Estimación de la probabilidad activo servidor de copias de seguridad

ACTIVO TI		CONTRASEÑAS DEL SERVIDOR DE COPIAS DE SEGURIDAD			
ADMINISTRADOR		PIMIENTO CARDENAS WILSON MAURICIO			
DEGRADACIÓN		100%			
IMPACTO		5			
TIPO DE ACTIVO		DATOS/INFORMACIÓN			
Tipo	**ID**	**Amenaza**	**Exposición/Vulnerabilidad**	**Frecuencia (F)**	
ERRORES Y FALLOS NO INTENCIONADOS	**E.1**	Errores de los usuarios	Pérdida total o parcial del tiempo de ejecución de sus actividades, dependiendo de la gravedad del asunto.	Baja	3
	E.2	Errores del administrador	Pérdida total o parcial del tiempo de ejecución de sus actividades, dependiendo de la gravedad del asunto.	Baja	3
	E.15	Alteración accidental de la información	La dependencia cuenta con sistemas de cifrado y verificación (puerto – puerto) para el manejo de la movilidad de la información.	Baja	3
	E.18	Destrucción de información	El departamento de sistemas cuenta con copias de seguridad periódicas	Media	4
	E.19	Fugas de información	Las personas contratadas están atadas a cláusulas de confidencialidad.	Media	4
ATAQUES INTENCIO	**A.5**	Suplantación de la identidad del usuario	Acceso a personas que no cuenten con los permisos necesarios o con las credenciales necesarias.	Media	4

Tabla 7. Estimación de la probabilidad activo servidor de copias de seguridad. (Continuación)

	A.6	Abuso de privilegios de acceso	Abuso de cada uno de los derechos otorgados.	Media	4
	A.11	Acceso no autorizado	Uso ilícito del hardware	Media	4
	A.15	Modificación deliberada de la información	Datos erróneos en el momento de la movilización de la información.	Media	4
	A.18	Destrucción de información	Perdida de la información.	Media	4
	A.19	Divulgación de información	Información filtrada abiertamente a personas no correspondientes.	Media	4

Fuente: Autoría propia

Tabla 8. Estimación de la probabilidad activo usuarios de los pc de las demás dependencias

ACTIVO TI	CONTRASEÑAS DE LOS USUARIOS DE LOS PC DE LAS DEMÁS DEPENDENCIAS
ADMINISTRADOR	PIMIENTO CARDENAS WILSON MAURICIO
DEGRACIÓN	85%
IMPACTO	5
TIPO DE ACTIVO	CLAVES CRIPTOGRÁFICAS

Tipo	**ID**	**Amenaza**	**Exposición/Vulnerabilidad**	**Frecuencia (F)**	
ERRORES Y FALLOS NO INTENCIONADOS	**E.1**	Errores de los usuarios	Pérdida total o parcial del tiempo de ejecución de sus actividades, dependiendo de la gravedad del asunto.	Muy baja	2
	E.2	Errores del administrador	Pérdida total o parcial del tiempo de ejecución de sus actividades, dependiendo de la gravedad del asunto.	Muy baja	2

Tabla 8. Estimación de la probabilidad activo usuarios de los pc de las demás dependencias. (Continuación)

	E.15	Alteración accidental de la información	La dependencia cuenta con sistemas de cifrado y verificación (puerto – puerto) para el manejo de la movilidad de la información.	Media	4
	E.18	Destrucción de información	El departamento de sistemas cuenta con copias de seguridad periódicas	Media	4
	E.19	Fugas de información	Las personas contratadas están atadas a cláusulas de confidencialidad.	Media	4
ATAQUES INTENCIONAD	**A.5**	Suplantación de la identidad del usuario	Acceso a personas que no cuenten con los permisos necesarios o con las credenciales necesarias.	Media	4
	A.6	Abuso de privilegios de acceso	Abuso de cada uno de los derechos otorgados.	Media	4
	A.11	Acceso no autorizado	Uso ilícito del hardware	Media	4
	A.15	Modificación deliberada de la información	Datos erróneos en el momento de la movilización de la información.	Media	4
	A.18	Destrucción de información	Perdida de la información.	Media	4
	A.19	Divulgación de información	Información filtrada abiertamente a personas no correspondientes.	Media	4

Fuente: Autoría propia

Tabla 9. Estimación de la probabilidad activo sensor biométrico

ACTIVO TI	CONTRASEÑA SENSOR BIOMÉTRICO
ADMINISTRADOR	PIMIENTO CARDENAS WILSON MAURICIO
DEGRADACIÓN	100%
IMPACTO	5
TIPO DE ACTIVO	CLAVES CRIPTOGRÁFICAS

Tipo	ID	Amenaza	Exposición/Vulnerabilidad	Frecuencia (F)	
ERRORES Y FALLOS NO INTENCIONADOS	**E.1**	Errores de los usuarios	Pérdida total o parcial del tiempo de ejecución de sus actividades, dependiendo de la gravedad del asunto.	Muy baja	2
	E.2	Errores del administrador	Pérdida total o parcial del tiempo de ejecución de sus actividades, dependiendo de la gravedad del asunto.	Muy baja	2
	E.15	Alteración accidental de la información	La dependencia cuenta con sistemas de cifrado y verificación (puerto – puerto) para el manejo de la movilidad de la información.	Media	4
	E.18	Destrucción de información	El departamento de sistemas cuenta con copias de seguridad periódicas	Media	4
	E.19	Fugas de información	Las personas contratadas están atadas a cláusulas de confidencialidad.	Media	4
ATAQUES INTENCIONAD	**A.5**	Suplantación de la identidad del usuario	Acceso a personas que no cuenten con los permisos necesarios o con las credenciales necesarias.	Media	4
	A.6	Abuso de privilegios de acceso	Abuso de cada uno de los derechos otorgados.	Media	4

Tabla 9. Estimación de la probabilidad activo sensor biométrico. (Continuación)

	A.11	Acceso no autorizado	Uso ilícito del hardware	Media	4
	A.15	Modificación deliberada de la información	Datos erróneos en el momento de la movilización de la información.	Media	4
	A.18	Destrucción de información	Perdida de la información.	Media	4
	A.19	Divulgación de información	Información filtrada abiertamente a personas no correspondientes.	Media	4

Fuente: Autoría propia

Tabla 10. Estimación de la probabilidad activo código de confirmación para acceso a la sala de servidor

ACTIVO TI	CÓDIGO DE ACCESO A LA SALA DEL SERVIDOR
ADMINISTRADOR	PIMIENTO CARDENAS WILSON MAURICIO
DEGRACIÓN	100%
IMPACTO	5
TIPO DE ACTIVO	CLAVES CRIPTOGRÁFICAS

Tipo	**ID**	**Amenaza**	**Exposición/Vulnerabilidad**	**Frecuencia (F)**	
ERRORES Y FALLOS NO INTENCIONADOS	**E.1**	Errores de los usuarios	Pérdida total o parcial del tiempo de ejecución de sus actividades, dependiendo de la gravedad del asunto.	Muy baja	2
	E.2	Errores del administrador	Pérdida total o parcial del tiempo de ejecución de sus actividades, dependiendo de la gravedad del asunto.	Muy baja	2
	E.15	Alteración accidental de la información	La dependencia cuenta con sistemas de cifrado y verificación (puerto – puerto) para el manejo de la movilidad de la información.	Media	4

Tabla 10. Estimación de la probabilidad activo código confirmación acceso a la sala servidor. (Continuación)

	E.18	Destrucción de información	El departamento de sistemas cuenta con copias de seguridad periódicas	Media	4
	E.19	Fugas de información	Las personas contratadas están atadas a cláusulas de confidencialidad.	Media	4
ATAQUES INTENCIONAD	**A.5**	Suplantación de la identidad del usuario	Acceso a personas que no cuenten con los permisos necesarios o con las credenciales necesarias.	Media	4
	A.6	Abuso de privilegios de acceso	Abuso de cada uno de los derechos otorgados.	Media	4
	A.11	Acceso no autorizado	Uso ilícito del hardware	Media	4
	A.15	Modificación deliberada de la información	Datos erróneos en el momento de la movilización de la información.	Media	4
	A.18	Destrucción de información	Perdida de la información.	Media	4
	A.19	Divulgación de información	Información filtrada abiertamente a personas no correspondientes.	Media	4

Fuente: Autoría propia

Tabla 11. Estimación de la probabilidad activo sistema de registro y control académico (RYCA) V.1

ACTIVO TI	SISTEMA DE REGISTRO Y CONTROL ACADÉMICO (RYCA) V.1			
ADMINISTRADOR	PIMIENTO CARDENAS WILSON MAURICIO			
DEGRADACIÓN	90%			
IMPACTO	5			
TIPO DE ACTIVO	SOFTWARE			
Tipo	**ID**	**Amenaza**	**Exposición/Vulnerabilidad**	**Frecuencia (F)**

Tabla 11. Estimación de la probabilidad activo sistema (RYCA) V.1. (Continuación)

DE ORIGEN INDUSTRIAL	**I.5**	Avería de origen físico o lógico	La manipulación por parte de cada uno de los componentes encontrados en la dependencia, como también por defectos de los componentes desde fabrica	Baja	**3**
ERRORES Y FALLOS NO INTENCIONADOS	**E.1**	Errores de los usuarios	Pérdida total o parcial del tiempo de ejecución de sus actividades, dependiendo de la gravedad del asunto.	Baja	**3**
	E.2	Errores del administrador	Pérdida total o parcial del tiempo de ejecución de sus actividades, dependiendo de la gravedad del asunto.	Baja	**3**
	E.8	Difusión de software dañino	La dependencia cuenta con antivirus capaces de controlar software malicioso	Baja	**3**
	E.9	Errores de [re-] encaminamiento	La dependencia cuenta con sistemas de cifrado y verificación (puerto – puerto) para el manejo de la movilidad de la información.	Baja	**3**
	E.10	Errores de secuencia	La dependencia cuenta con sistemas de cifrado y verificación (puerto – puerto) para el manejo de la movilidad de la información.	Baja	**3**
	E.15	Alteración accidental de la información	La dependencia cuenta con sistemas de cifrado y verificación (puerto – puerto) para el manejo de la movilidad de la información.	Baja	**3**

Tabla 11. Estimación de la probabilidad activo sistema (RYCA) V.1. (Continuación)

	E.18	Destrucción de información	El departamento de sistemas cuenta con copias de seguridad periódicas	Baja	**3**
	E.19	Fugas de información	Las personas contratadas están atadas a cláusulas de confidencialidad.	Baja	**3**
	E.20	Vulnerabilidades de los programas (software)	La dependencia cuenta con un servidor (personal) para llevar a cabo cada uno de los softwares empleados para la institución.	Baja	**3**
	E.21	Errores de mantenimiento / actualización de programas (software)	Falla de funcionamiento del software.	Baja	**3**
ATAQUES INTENCIONAD	**A.5**	Suplantación de la identidad del usuario	Acceso a personas que no cuenten con los permisos necesarios o con las credenciales necesarias.	Baja	**3**
	A.6	Abuso de privilegios de acceso	Abuso de cada uno de los derechos otorgados.	Baja	**3**
	A.7	Uso no previsto	Implementación de recursos (económicos y de tiempo) en actividades no relacionadas.	Baja	**3**
	A.8	Difusión de software dañino	Afectación en los sistemas de información y los procesos que ello conlleva.	Baja	**3**
	A.9	[Re-]encaminamiento de mensajes	La dependencia cuenta con sistemas de cifrado y verificación (puerto –	Baja	**3**

Tabla 11. Estimación de la probabilidad activo sistema (RYCA) V.1. (Continuación)

			puerto) para el manejo de la movilidad de la información.		
	A.10	Alteración de secuencia	Alteración de datos.	Baja	**3**
	A.11	Acceso no autorizado	Uso ilícito del hardware	Baja	**3**
	A.15	Modificación deliberada de la información	Datos erróneos en el momento de la movilización de la información.	Baja	**3**
	A.18	Destrucción de información	Perdida de la información.	Baja	**3**
	A.19	Divulgación de información	Información filtrada abiertamente a personas no correspondientes.	Baja	**3**
	A.22	Manipulación de programas	Alteración del funcionamiento de cada uno de los programas de la dependencia.	Baja	**3**

Fuente: Autoría propia

Tabla 12. Estimación de la probabilidad activo sistema de registro y control académico (RYCA) V.2.0

ACTIVO TI	SISTEMA DE REGISTRO Y CONTROL ACADÉMICO (RYCA) V.2.0
ADMINISTRADOR	PIMIENTO CARDENAS WILSON MAURICIO
DEGRADACIÓN	90%
IMPACTO	5
TIPO DE ACTIVO	SOFTWARE

Tipo	**ID**	**Amenaza**	**Exposición/Vulnerabilidad**	**Frecuencia (F)**	
DE ORIGEN INDUSTRIAL	**I.5**	Avería de origen físico o lógico	La manipulación por parte de cada uno de los componentes encontrados en la dependencia, como también por defectos de los componentes desde fabrica	Baja	**3**

Tabla 12. Estimación de la probabilidad activo (RYCA) V.2.0. (Continuación)

ERRORES Y FALLOS NO INTENCIONADOS	**E.1**	Errores de los usuarios	Pérdida total o parcial del tiempo de ejecución de sus actividades, dependiendo de la gravedad del asunto.	Baja	**3**
	E.2	Errores del administrador	Pérdida total o parcial del tiempo de ejecución de sus actividades, dependiendo de la gravedad del asunto.	Baja	**3**
	E.8	Difusión de software dañino	La dependencia cuenta con antivirus capaces de controlar software malicioso	Baja	**3**
	E.9	Errores de [re-] encaminamiento	La dependencia cuenta con sistemas de cifrado y verificación (puerto – puerto) para el manejo de la movilidad de la información.	Baja	**3**
	E.10	Errores de secuencia	La dependencia cuenta con sistemas de cifrado y verificación (puerto – puerto) para el manejo de la movilidad de la información.	Baja	**3**
	E.15	Alteración accidental de la información	La dependencia cuenta con sistemas de cifrado y verificación (puerto – puerto) para el manejo de la movilidad de la información.	Baja	**3**
	E.18	Destrucción de información	El departamento de sistemas cuenta con copias de seguridad periódicas	Baja	**3**
	E.19	Fugas de información	Las personas contratadas están atadas a cláusulas de confidencialidad.	Baja	**3**

Tabla 12. Estimación de la probabilidad activo (RYCA) V.2.0. (Continuación)

	E.20	Vulnerabilidades de los programas (software)	La dependencia cuenta con un servidor (personal) para llevar a cabo cada uno de los softwares empleados para la institución.	Baja	**3**
	E.21	Errores de mantenimiento / actualización de programas (software)	Falla de funcionamiento del software.	Baja	**3**
ATAQUES INTENCIONAD	**A.5**	Suplantación de la identidad del usuario	Acceso a personas que no cuenten con los permisos necesarios o con las credenciales necesarias.	Baja	**3**
	A.6	Abuso de privilegios de acceso	Abuso de cada uno de los derechos otorgados.	Baja	**3**
	A.7	Uso no previsto	Implementación de recursos (económicos y de tiempo) en actividades no relacionadas.	Baja	**3**
	A.8	Difusión de software dañino	Afectación en los sistemas de información y los procesos que ello conlleva.	Baja	**3**
	A.9	[Re-]encaminamiento de mensajes	La dependencia cuenta con sistemas de cifrado y verificación (puerto – puerto) para el manejo de la movilidad de la información.	Baja	**3**
	A.10	Alteración de secuencia	Alteración de datos.	Baja	**3**
	A.11	Acceso no autorizado	Uso ilícito del hardware	Baja	**3**

Tabla 12. Estimación de la probabilidad activo (RYCA) V.2.0. (Continuación)

	A.15	Modificación deliberada de la información	Datos erróneos en el momento de la movilización de la información.	Baja	**3**
	A.18	Destrucción de información	Perdida de la información.	Baja	**3**
	A.19	Divulgación de información	Información filtrada abiertamente a personas no correspondientes.	Baja	**3**
	A.22	Manipulación de programas	Alteración del funcionamiento de cada uno de los programas de la dependencia.	Baja	**3**

Fuente: Autoría propia

Tabla 13. Estimación de la probabilidad activo página oficial del ITFIP

ACTIVO TI	PÁGINA OFICIAL DEL ITFIP				
ADMINISTRADOR	PIMIENTO CARDENAS WILSON MAURICIO				
DEGRADACIÓN	50%				
IMPACTO	3				
TIPO DE ACTIVO	SOFTWARE				
Tipo	**ID**	**Amenaza**	**Exposición/Vulnerabilidad**	**Frecuencia (F)**	
DE ORIGEN INDUSTRIAL	**I.5**	Avería de origen físico o lógico	La manipulación por parte de cada uno de los componentes encontrados en la dependencia, como también por defectos de los componentes desde fabrica	Baja	**3**
Y NO ERRORES FALLOS	**E.1**	Errores de los usuarios	Pérdida total o parcial del tiempo de ejecución de sus actividades, dependiendo de la gravedad del asunto.	Baja	**3**
	E.2	Errores del administrador	Pérdida total o parcial del tiempo de ejecución de sus	Baja	**3**

Tabla 13. Estimación de la probabilidad activo página oficial del ITFIP. (Continuación)

			actividades, dependiendo de la gravedad del asunto.		
	E.8	Difusión de software dañino	La dependencia cuenta con antivirus capaces de controlar software malicioso	Baja	**3**
	E.9	Errores de [re-] encaminamiento	La dependencia cuenta con sistemas de cifrado y verificación (puerto – puerto) para el manejo de la movilidad de la información.	Baja	**3**
	E.10	Errores de secuencia	La dependencia cuenta con sistemas de cifrado y verificación (puerto – puerto) para el manejo de la movilidad de la información.	Baja	**3**
	E.15	Alteración accidental de la información	La dependencia cuenta con sistemas de cifrado y verificación (puerto – puerto) para el manejo de la movilidad de la información.	Baja	**3**
	E.18	Destrucción de información	El departamento de sistemas cuenta con copias de seguridad periódicas	Baja	**3**
	E.19	Fugas de información	Las personas contratadas están atadas a cláusulas de confidencialidad.	Baja	**3**
	E.20	Vulnerabilidades de los programas (software)	La dependencia cuenta con un servidor (personal) para llevar a cabo cada uno de los softwares empleados para la institución.	Baja	**3**
	E.21	Errores de mantenimiento /	Falla de funcionamiento del software.	Baja	**3**

Tabla 13. Estimación de la probabilidad activo página oficial del ITFIP. (Continuación)

		actualización de programas (software)			
ATAQUES INTENCIONAD	**A.5**	Suplantación de la identidad del usuario	Acceso a personas que no cuenten con los permisos necesarios o con las credenciales necesarias.	Baja	**3**
	A.6	Abuso de privilegios de acceso	Abuso de cada uno de los derechos otorgados.	Baja	**3**
	A.7	Uso no previsto	Implementación de recursos (económicos y de tiempo) en actividades no relacionadas.	Baja	**3**
	A.8	Difusión de software dañino	Afectación en los sistemas de información y los procesos que ello conlleva.	Baja	**3**
	A.9	[Re-]encaminamiento de mensajes	La dependencia cuenta con sistemas de cifrado y verificación (puerto – puerto) para el manejo de la movilidad de la información.	Baja	**3**
	A.10	Alteración de secuencia	Alteración de datos.	Baja	**3**
	A.11	Acceso no autorizado	Uso ilícito del hardware	Baja	**3**
	A.15	Modificación deliberada de la información	Datos erróneos en el momento de la movilización de la información.	Baja	**3**
	A.18	Destrucción de información	Perdida de la información.	Baja	**3**

Tabla 13. Estimación de la probabilidad activo página oficial del ITFIP. (Continuación)

	A.19	Divulgación de información	Información filtrada abiertamente a personas no correspondientes.	Baja	**3**
	A.22	Manipulación de programas	Alteración del funcionamiento de cada uno de los programas de la dependencia.	Baja	**3**

Fuente: Autoría propia

Tabla 14. Estimación de la probabilidad activo Google Chrome

ACTIVO TI	NAVEGADOR GOOGLE CHROME
ADMINISTRADOR	PIMIENTO CARDENAS WILSON MAURICIO
DEGRADACIÓN	10%
IMPACTO	1
TIPO DE ACTIVO	SOFTWARE

Tipo	**ID**	**Amenaza**	**Exposición/Vulnerabilidad**	**Frecuencia (F)**	
DE ORIGEN INDUSTRIAL	**I.5**	Avería de origen físico o lógico	La manipulación por parte de cada uno de los componentes encontrados en la dependencia, como también por defectos de los componentes desde fabrica	Baja	**3**
ERRORES Y FALLOS NO INTENCIONADOS	**E.1**	Errores de los usuarios	Pérdida total o parcial del tiempo de ejecución de sus actividades, dependiendo de la gravedad del asunto.	Baja	**3**
	E.2	Errores del administrador	Pérdida total o parcial del tiempo de ejecución de sus actividades, dependiendo de la gravedad del asunto.	Baja	**3**
	E.8	Difusión de software dañino	La dependencia cuenta con antivirus capaces de controlar software malicioso	Baja	**3**

Tabla 14. Estimación de la probabilidad activo Google Chrome. (Continuación)

	E.9	Errores de [re-] encaminamiento	La dependencia cuenta con sistemas de cifrado y verificación (puerto – puerto) para el manejo de la movilidad de la información.	Baja	**3**
	E.10	Errores de secuencia	La dependencia cuenta con sistemas de cifrado y verificación (puerto – puerto) para el manejo de la movilidad de la información.	Baja	**3**
	E.15	Alteración accidental de la información	La dependencia cuenta con sistemas de cifrado y verificación (puerto – puerto) para el manejo de la movilidad de la información.	Baja	**3**
	E.18	Destrucción de información	El departamento de sistemas cuenta con copias de seguridad periódicas	Baja	**3**
	E.19	Fugas de información	Las personas contratadas están atadas a cláusulas de confidencialidad.	Baja	**3**
	E.20	Vulnerabilidades de los programas (software)	La dependencia cuenta con un servidor (personal) para llevar a cabo cada uno de los softwares empleados para la institución.	Baja	**3**
	E.21	Errores de mantenimiento / actualización de programas (software)	Falla de funcionamiento del software.	Baja	**3**

Tabla 14. Estimación de la probabilidad activo Google Chrome. (Continuación)

ATAQUES INTENCIONAD	**A.5**	Suplantación de la identidad del usuario	Acceso a personas que no cuenten con los permisos necesarios o con las credenciales necesarias.	Baja	**3**
	A.6	Abuso de privilegios de acceso	Abuso de cada uno de los derechos otorgados.	Baja	**3**
	A.7	Uso no previsto	Implementación de recursos (económicos y de tiempo) en actividades no relacionadas.	Baja	**3**
	A.8	Difusión de software dañino	Afectación en los sistemas de información y los procesos que ello conlleva.	Baja	**3**
	A.9	[Re-]encaminamiento de mensajes	La dependencia cuenta con sistemas de cifrado y verificación (puerto – puerto) para el manejo de la movilidad de la información.	Baja	**3**
	A.10	Alteración de secuencia	Alteración de datos.	Baja	**3**
	A.11	Acceso no autorizado	Uso ilícito del hardware	Baja	**3**
	A.15	Modificación deliberada de la información	Datos erróneos en el momento de la movilización de la información.	Baja	**3**
	A.18	Destrucción de información	Perdida de la información.	Baja	**3**
	A.19	Divulgación de información	Información filtrada abiertamente a personas no correspondientes.	Baja	**3**

Tabla 14. Estimación de la probabilidad activo Google Chrome. (Continuación)

	A.22	Manipulación de programas	Alteración del funcionamiento de cada uno de los programas de la dependencia.	Baja	**3**

Fuente: Autoría propia

Tabla 15. Estimación de la probabilidad activo Mozilla Firefox

ACTIVO TI	NAVEGADOR MOZILLA FIREFOX
ADMINISTRADOR	PIMIENTO CARDENAS WILSON MAURICIO
DEGRADACIÓN	15%
IMPACTO	1
TIPO DE ACTIVO	SOFTWARE

Tipo	**ID**	**Amenaza**	**Exposición/Vulnerabilidad**	**Frecuencia (F)**	
DE ORIGEN INDUSTRIAL	**I.5**	Avería de origen físico o lógico	La manipulación por parte de cada uno de los componentes encontrados en la dependencia, como también por defectos de los componentes desde fabrica	Baja	**3**
ERRORES Y FALLOS NO INTENCIONADOS	**E.1**	Errores de los usuarios	Pérdida total o parcial del tiempo de ejecución de sus actividades, dependiendo de la gravedad del asunto.	Baja	**3**
	E.2	Errores del administrador	Pérdida total o parcial del tiempo de ejecución de sus actividades, dependiendo de la gravedad del asunto.	Baja	**3**
	E.8	Difusión de software dañino	La dependencia cuenta con antivirus capaces de controlar software malicioso	Baja	**3**
	E.9	Errores de [re-] encaminamiento	La dependencia cuenta con sistemas de cifrado y verificación (puerto – puerto) para el manejo de la movilidad de la información.	Baja	**3**

Tabla 15. Estimación de la probabilidad activo Mozilla Firefox. (Continuación)

	E.10	Errores de secuencia	La dependencia cuenta con sistemas de cifrado y verificación (puerto – puerto) para el manejo de la movilidad de la información.	Baja	**3**
	E.15	Alteración accidental de la información	La dependencia cuenta con sistemas de cifrado y verificación (puerto – puerto) para el manejo de la movilidad de la información.	Baja	**3**
	E.18	Destrucción de información	El departamento de sistemas cuenta con copias de seguridad periódicas	Baja	**3**
	E.19	Fugas de información	Las personas contratadas están atadas a cláusulas de confidencialidad.	Baja	**3**
	E.20	Vulnerabilidades de los programas (software)	La dependencia cuenta con un servidor (personal) para llevar a cabo cada uno de los softwares empleados para la institución.	Baja	**3**
	E.21	Errores de mantenimiento / actualización de programas (software)	Falla de funcionamiento del software.	Baja	**3**
ATAQUES INTENCIONAD	**A.5**	Suplantación de la identidad del usuario	Acceso a personas que no cuenten con los permisos necesarios o con las credenciales necesarias.	Baja	**3**
	A.6	Abuso de privilegios de acceso	Abuso de cada uno de los derechos otorgados.	Baja	**3**

Tabla 15. Estimación de la probabilidad activo Mozilla Firefox. (Continuación)

	A.7	Uso no previsto	Implementación de recursos (económicos y de tiempo) en actividades no relacionadas.	Baja	**3**
	A.8	Difusión de software dañino	Afectación en los sistemas de información y los procesos que ello conlleva.	Baja	**3**
	A.9	[Re-]encaminamiento de mensajes	La dependencia cuenta con sistemas de cifrado y verificación (puerto – puerto) para el manejo de la movilidad de la información.	Baja	**3**
	A.10	Alteración de secuencia	Alteración de datos.	Baja	**3**
	A.11	Acceso no autorizado	Uso ilícito del hardware	Baja	**3**
	A.15	Modificación deliberada de la información	Datos erróneos en el momento de la movilización de la información.	Baja	**3**
	A.18	Destrucción de información	Perdida de la información.	Baja	**3**
	A.19	Divulgación de información	Información filtrada abiertamente a personas no correspondientes.	Baja	**3**
	A.22	Manipulación de programas	Alteración del funcionamiento de cada uno de los programas de la dependencia.	Baja	**3**

Fuente: Autoría propia

Tabla 16. Estimación de la probabilidad activo safari

ACTIVO TI	NAVEGADOR SAFARI
ADMINISTRADOR	PIMIENTO CARDENAS WILSON MAURICIO
DEGRADACIÓN	10%
IMPACTO	1
TIPO DE ACTIVO	SOFTWARE

Tipo	ID	Amenaza	Exposición/Vulnerabilidad	Frecuencia (F)	
DE ORIGEN INDUSTRIAL	**I.5**	Avería de origen físico o lógico	La manipulación por parte de cada uno de los componentes encontrados en la dependencia, como también por defectos de los componentes desde fabrica	Baja	**3**
ERRORES Y FALLOS NO INTENCIONADOS	**E.1**	Errores de los usuarios	Pérdida total o parcial del tiempo de ejecución de sus actividades, dependiendo de la gravedad del asunto.	Baja	**3**
	E.2	Errores del administrador	Pérdida total o parcial del tiempo de ejecución de sus actividades, dependiendo de la gravedad del asunto.	Baja	**3**
	E.8	Difusión de software dañino	La dependencia cuenta con antivirus capaces de controlar software malicioso	Baja	**3**
	E.9	Errores de [re-] encaminamiento	La dependencia cuenta con sistemas de cifrado y verificación (puerto – puerto) para el manejo de la movilidad de la información.	Baja	**3**
	E.10	Errores de secuencia	La dependencia cuenta con sistemas de cifrado y verificación (puerto – puerto) para el manejo de la movilidad de la información.	Baja	**3**

Tabla 16. Estimación de la probabilidad activo safari. (Continuación)

	E.15	Alteración accidental de la información	La dependencia cuenta con sistemas de cifrado y verificación (puerto – puerto) para el manejo de la movilidad de la información.	Baja	**3**
	E.18	Destrucción de información	El departamento de sistemas cuenta con copias de seguridad periódicas	Baja	**3**
	E.19	Fugas de información	Las personas contratadas están atadas a cláusulas de confidencialidad.	Baja	**3**
	E.20	Vulnerabilidades de los programas (software)	La dependencia cuenta con un servidor (personal) para llevar a cabo cada uno de los softwares empleados para la institución.	Baja	**3**
	E.21	Errores de mantenimiento / actualización de programas (software)	Falla de funcionamiento del software.	Baja	**3**
ATAQUES INTENCIONAD	**A.5**	Suplantación de la identidad del usuario	Acceso a personas que no cuenten con los permisos necesarios o con las credenciales necesarias.	Baja	**3**
	A.6	Abuso de privilegios de acceso	Abuso de cada uno de los derechos otorgados.	Baja	**3**
	A.7	Uso no previsto	Implementación de recursos (económicos y de tiempo) en actividades no relacionadas.	Baja	**3**

Tabla 16. Estimación de la probabilidad activo safari. (Continuación)

	A.8	Difusión de software dañino	Afectación en los sistemas de información y los procesos que ello conlleva.	Baja	**3**
	A.9	[Re-]encaminamiento de mensajes	La dependencia cuenta con sistemas de cifrado y verificación (puerto – puerto) para el manejo de la movilidad de la información.	Baja	**3**
	A.10	Alteración de secuencia	Alteración de datos.	Baja	**3**
	A.11	Acceso no autorizado	Uso ilícito del hardware	Baja	**3**
	A.15	Modificación deliberada de la información	Datos erróneos en el momento de la movilización de la información.	Baja	**3**
	A.18	Destrucción de información	Perdida de la información.	Baja	**3**
	A.19	Divulgación de información	Información filtrada abiertamente a personas no correspondientes.	Baja	**3**
	A.22	Manipulación de programas	Alteración del funcionamiento de cada uno de los programas de la dependencia.	Baja	**3**

Fuente: Autoría propia

Tabla 17. Estimación de la probabilidad activo Microsoft office 2013

ACTIVO TI	MICROSOFT OFFICE 2013			
ADMINISTRADOR	PIMIENTO CARDENAS WILSON MAURICIO			
DEGRADACIÓN	20%			
IMPACTO	3			
TIPO DE ACTIVO	SOFTWARE			
Tipo	**ID**	**Amenaza**	**Exposición/Vulnerabilidad**	**Frecuencia (F)**

Tabla 17. Estimación de la probabilidad activo Microsoft office 2013. (Continuación)

DE ORIGEN INDUSTRIAL	**I.5**	Avería de origen físico o lógico	La manipulación por parte de cada uno de los componentes encontrados en la dependencia, como también por defectos de los componentes desde fabrica	Baja	**3**
ERRORES Y FALLOS NO INTENCIONADOS	**E.1**	Errores de los usuarios	Pérdida total o parcial del tiempo de ejecución de sus actividades, dependiendo de la gravedad del asunto.	Baja	**3**
	E.2	Errores del administrador	Pérdida total o parcial del tiempo de ejecución de sus actividades, dependiendo de la gravedad del asunto.	Baja	**3**
	E.8	Difusión de software dañino	La dependencia cuenta con antivirus capaces de controlar software malicioso	Baja	**3**
	E.9	Errores de [re-] encaminamiento	La dependencia cuenta con sistemas de cifrado y verificación (puerto – puerto) para el manejo de la movilidad de la información.	Baja	**3**
	E.10	Errores de secuencia	La dependencia cuenta con sistemas de cifrado y verificación (puerto – puerto) para el manejo de la movilidad de la información.	Baja	**3**
	E.15	Alteración accidental de la información	La dependencia cuenta con sistemas de cifrado y verificación (puerto – puerto) para el manejo de la movilidad de la información.	Baja	**3**

Tabla 17. Estimación de la probabilidad activo Microsoft office 2013. (Continuación)

	E.18	Destrucción de información	El departamento de sistemas cuenta con copias de seguridad periódicas	Baja	**3**
	E.19	Fugas de información	Las personas contratadas están atadas a cláusulas de confidencialidad.	Baja	**3**
	E.20	Vulnerabilidades de los programas (software)	La dependencia cuenta con un servidor (personal) para llevar a cabo cada uno de los softwares empleados para la institución.	Baja	**3**
	E.21	Errores de mantenimiento / actualización de programas (software)	Falla de funcionamiento del software.	Baja	**3**
ATAQUES INTENCIONAD	**A.5**	Suplantación de la identidad del usuario	Acceso a personas que no cuenten con los permisos necesarios o con las credenciales necesarias.	Baja	**3**
	A.6	Abuso de privilegios de acceso	Abuso de cada uno de los derechos otorgados.	Baja	**3**
	A.7	Uso no previsto	Implementación de recursos (económicos y de tiempo) en actividades no relacionadas.	Baja	**3**
	A.8	Difusión de software dañino	Afectación en los sistemas de información y los procesos que ello conlleva.	Baja	**3**
	A.9	[Re-]encaminamiento de mensajes	La dependencia cuenta con sistemas de cifrado y verificación (puerto –	Baja	**3**

Tabla 17. Estimación de la probabilidad activo Microsoft office 2013. (Continuación)

			puerto) para el manejo de la movilidad de la información.		
	A.10	Alteración de secuencia	Alteración de datos.	Baja	**3**
	A.11	Acceso no autorizado	Uso ilícito del hardware	Baja	**3**
	A.15	Modificación deliberada de la información	Datos erróneos en el momento de la movilización de la información.	Baja	**3**
	A.18	Destrucción de información	Perdida de la información.	Baja	**3**
	A.19	Divulgación de información	Información filtrada abiertamente a personas no correspondientes.	Baja	**3**
	A.22	Manipulación de programas	Alteración del funcionamiento de cada uno de los programas de la dependencia.	Baja	**3**

Fuente: Autoría propia

Tabla 18. Estimación de la probabilidad activo open office Linux 2017

ACTIVO TI	OPEN OFFICE LINUX 2017				
ADMINISTRADOR	PIMIENTO CARDENAS WILSON MAURICIO				
DEGRADACIÓN	15%				
IMPACTO	2				
TIPO DE ACTIVO	SOFTWARE				
Tipo	**ID**	**Amenaza**	**Exposición/Vulnerabilidad**	**Frecuencia (F)**	
DE ORIGEN INDUSTRIAL	**I.5**	Avería de origen físico o lógico	La manipulación por parte de cada uno de los componentes encontrados en la dependencia, como también por defectos de los componentes desde fabrica	Baja	**3**

Tabla 18. Estimación de la probabilidad activo open office Linux 2017. (Continuación)

ERRORES Y FALLOS NO INTENCIONADOS	**E.1**	Errores de los usuarios	Pérdida total o parcial del tiempo de ejecución de sus actividades, dependiendo de la gravedad del asunto.	Baja	**3**
	E.2	Errores del administrador	Pérdida total o parcial del tiempo de ejecución de sus actividades, dependiendo de la gravedad del asunto.	Baja	**3**
	E.8	Difusión de software dañino	La dependencia cuenta con antivirus capaces de controlar software malicioso	Baja	**3**
	E.9	Errores de [re-] encaminamiento	La dependencia cuenta con sistemas de cifrado y verificación (puerto – puerto) para el manejo de la movilidad de la información.	Baja	**3**
	E.10	Errores de secuencia	La dependencia cuenta con sistemas de cifrado y verificación (puerto – puerto) para el manejo de la movilidad de la información.	Baja	**3**
	E.15	Alteración accidental de la información	La dependencia cuenta con sistemas de cifrado y verificación (puerto – puerto) para el manejo de la movilidad de la información.	Baja	**3**
	E.18	Destrucción de información	El departamento de sistemas cuenta con copias de seguridad periódicas	Baja	**3**
	E.19	Fugas de información	Las personas contratadas están atadas a cláusulas de confidencialidad.	Baja	**3**

Tabla 18. Estimación de la probabilidad activo open office Linux 2017. (Continuación)

	E.20	Vulnerabilidades de los programas (software)	La dependencia cuenta con un servidor (personal) para llevar a cabo cada uno de los softwares empleados para la institución.	Baja	**3**
	E.21	Errores de mantenimiento / actualización de programas (software)	Falla de funcionamiento del software.	Baja	**3**
ATAQUES INTENCIONAD	**A.5**	Suplantación de la identidad del usuario	Acceso a personas que no cuenten con los permisos necesarios o con las credenciales necesarias.	Baja	**3**
	A.6	Abuso de privilegios de acceso	Abuso de cada uno de los derechos otorgados.	Baja	**3**
	A.7	Uso no previsto	Implementación de recursos (económicos y de tiempo) en actividades no relacionadas.	Baja	**3**
	A.8	Difusión de software dañino	Afectación en los sistemas de información y los procesos que ello conlleva.	Baja	**3**
	A.9	[Re-]encaminamiento de mensajes	La dependencia cuenta con sistemas de cifrado y verificación (puerto – puerto) para el manejo de la movilidad de la información.	Baja	**3**
	A.10	Alteración de secuencia	Alteración de datos.	Baja	**3**
	A.11	Acceso no autorizado	Uso ilícito del hardware	Baja	**3**

Tabla 18. Estimación de la probabilidad activo open office Linux 2017. (Continuación)

	A.15	Modificación deliberada de la información	Datos erróneos en el momento de la movilización de la información.	Baja	**3**
	A.18	Destrucción de información	Perdida de la información.	Baja	**3**
	A.19	Divulgación de información	Información filtrada abiertamente a personas no correspondientes.	Baja	**3**
	A.22	Manipulación de programas	Alteración del funcionamiento de cada uno de los programas de la dependencia.	Baja	**3**

Fuente: Autoría propia

Tabla 19. Estimación de la probabilidad activo *System center*

ACTIVO TI	ANTIVIRUS SYSTEM CENTER				
ADMINISTRADOR	PIMIENTO CARDENAS WILSON MAURICIO				
DEGRADACIÓN	20%				
IMPACTO	2				
TIPO DE ACTIVO	SOFTWARE				
Tipo	**ID**	**Amenaza**	**Exposición/Vulnerabilidad**	**Frecuencia (F)**	
DE ORIGEN INDUSTRIAL	**I.5**	Avería de origen físico o lógico	La manipulación por parte de cada uno de los componentes encontrados en la dependencia, como también por defectos de los componentes desde fabrica	Baja	**3**
ERRORES Y NO FALLOS	**E.1**	Errores de los usuarios	Pérdida total o parcial del tiempo de ejecución de sus actividades, dependiendo de la gravedad del asunto.	Baja	**3**
	E.2	Errores del administrador	Pérdida total o parcial del tiempo de ejecución de sus	Baja	**3**

Tabla 19. Estimación de la probabilidad activo *System center*. (Continuación)

			actividades, dependiendo de la gravedad del asunto.		
	E.8	Difusión de software dañino	La dependencia cuenta con antivirus capaces de controlar software malicioso	Baja	**3**
	E.9	Errores de [re-] encaminamiento	La dependencia cuenta con sistemas de cifrado y verificación (puerto – puerto) para el manejo de la movilidad de la información.	Baja	**3**
	E.10	Errores de secuencia	La dependencia cuenta con sistemas de cifrado y verificación (puerto – puerto) para el manejo de la movilidad de la información.	Baja	**3**
	E.15	Alteración accidental de la información	La dependencia cuenta con sistemas de cifrado y verificación (puerto – puerto) para el manejo de la movilidad de la información.	Baja	**3**
	E.18	Destrucción de información	El departamento de sistemas cuenta con copias de seguridad periódicas	Baja	**3**
	E.19	Fugas de información	Las personas contratadas están atadas a cláusulas de confidencialidad.	Baja	**3**
	E.20	Vulnerabilidades de los programas (software)	La dependencia cuenta con un servidor (personal) para llevar a cabo cada uno de los softwares empleados para la institución.	Baja	**3**
	E.21	Errores de mantenimiento /	Falla de funcionamiento del software.	Baja	**3**

Tabla 19. Estimación de la probabilidad activo *System center*. (Continuación)

		actualización de programas (software)			
ATAQUES INTENCIONAD	**A.5**	Suplantación de la identidad del usuario	Acceso a personas que no cuenten con los permisos necesarios o con las credenciales necesarias.	Baja	**3**
	A.6	Abuso de privilegios de acceso	Abuso de cada uno de los derechos otorgados.	Baja	**3**
	A.7	Uso no previsto	Implementación de recursos (económicos y de tiempo) en actividades no relacionadas.	Baja	**3**
	A.8	Difusión de software dañino	Afectación en los sistemas de información y los procesos que ello conlleva.	Baja	**3**
	A.9	[Re-]encaminamiento de mensajes	La dependencia cuenta con sistemas de cifrado y verificación (puerto – puerto) para el manejo de la movilidad de la información.	Baja	**3**
	A.10	Alteración de secuencia	Alteración de datos.	Baja	**3**
	A.11	Acceso no autorizado	Uso ilícito del hardware	Baja	**3**
	A.15	Modificación deliberada de la información	Datos erróneos en el momento de la movilización de la información.	Baja	**3**
	A.18	Destrucción de información	Perdida de la información.	Baja	**3**

Tabla 19. Estimación de la probabilidad activo *System center*.

	A.19	Divulgación de información	Información filtrada abiertamente a personas no correspondientes.	Baja	**3**
	A.22	Manipulación de programas	Alteración del funcionamiento de cada uno de los programas de la dependencia.	Baja	**3**

Fuente: Autoría propia

Tabla 20. Estimación de la probabilidad activo Windows *defender*

ACTIVO TI	ANTIVIRUS WINDOWS DEFENDER
ADMINISTRADOR	PIMIENTO CARDENAS WILSON MAURICIO
DEGRADACIÓN	20%
IMPACTO	2
TIPO DE ACTIVO	SOFTWARE

Tipo	**ID**	**Amenaza**	**Exposición/Vulnerabilidad**	**Frecuencia (F)**	
DE ORIGEN INDUSTRIAL	**I.5**	Avería de origen físico o lógico	La manipulación por parte de cada uno de los componentes encontrados en la dependencia, como también por defectos de los componentes desde fabrica	Baja	**3**
ERRORES Y FALLOS NO INTENCIONADOS	**E.1**	Errores de los usuarios	Pérdida total o parcial del tiempo de ejecución de sus actividades, dependiendo de la gravedad del asunto.	Baja	**3**
	E.2	Errores del administrador	Pérdida total o parcial del tiempo de ejecución de sus actividades, dependiendo de la gravedad del asunto.	Baja	**3**
	E.8	Difusión de software dañino	La dependencia cuenta con antivirus capaces de controlar software malicioso	Baja	**3**

Tabla 20. Estimación de la probabilidad activo Windows *defender*. (Continuación)

	E.9	Errores de [re-] encaminamiento	La dependencia cuenta con sistemas de cifrado y verificación (puerto – puerto) para el manejo de la movilidad de la información.	Baja	**3**
	E.10	Errores de secuencia	La dependencia cuenta con sistemas de cifrado y verificación (puerto – puerto) para el manejo de la movilidad de la información.	Baja	**3**
	E.15	Alteración accidental de la información	La dependencia cuenta con sistemas de cifrado y verificación (puerto – puerto) para el manejo de la movilidad de la información.	Baja	**3**
	E.18	Destrucción de información	El departamento de sistemas cuenta con copias de seguridad periódicas	Baja	**3**
	E.19	Fugas de información	Las personas contratadas están atadas a cláusulas de confidencialidad.	Baja	**3**
	E.20	Vulnerabilidades de los programas (software)	La dependencia cuenta con un servidor (personal) para llevar a cabo cada uno de los softwares empleados para la institución.	Baja	**3**
	E.21	Errores de mantenimiento / actualización de programas (software)	Falla de funcionamiento del software.	Baja	**3**

Tabla 20. Estimación de la probabilidad activo Windows *defender*. (Continuación)

ATAQUES INTENCIONAD	**A.5**	Suplantación de la identidad del usuario	Acceso a personas que no cuenten con los permisos necesarios o con las credenciales necesarias.	Baja	**3**
	A.6	Abuso de privilegios de acceso	Abuso de cada uno de los derechos otorgados.	Baja	**3**
	A.7	Uso no previsto	Implementación de recursos (económicos y de tiempo) en actividades no relacionadas.	Baja	**3**
	A.8	Difusión de software dañino	Afectación en los sistemas de información y los procesos que ello conlleva.	Baja	**3**
	A.9	[Re-]encaminamiento de mensajes	La dependencia cuenta con sistemas de cifrado y verificación (puerto – puerto) para el manejo de la movilidad de la información.	Baja	**3**
	A.10	Alteración de secuencia	Alteración de datos.	Baja	**3**
	A.11	Acceso no autorizado	Uso ilícito del hardware	Baja	**3**
	A.15	Modificación deliberada de la información	Datos erróneos en el momento de la movilización de la información.	Baja	**3**
	A.18	Destrucción de información	Perdida de la información.	Baja	**3**
	A.19	Divulgación de información	Información filtrada abiertamente a personas no correspondientes.	Baja	**3**

Tabla 20. Estimación de la probabilidad activo Windows *defender*. (Continuación)

	A.22	Manipulación de programas	Alteración del funcionamiento de cada uno de los programas de la dependencia.	Baja	**3**

Fuente: Autoría propia

Tabla 21. Estimación de la probabilidad activo Windows 8

ACTIVO TI	SISTEMA OPERATIVO WINDOWS 8
ADMINISTRADOR	PIMIENTO CARDENAS WILSON MAURICIO
DEGRADACIÓN	35%
IMPACTO	3
TIPO DE ACTIVO	SOFTWARE

Tipo	**ID**	**Amenaza**	**Exposición/Vulnerabilidad**	**Frecuencia (F)**	
DE ORIGEN INDUSTRIAL	**I.5**	Avería de origen físico o lógico	La manipulación por parte de cada uno de los componentes encontrados en la dependencia, como también por defectos de los componentes desde fabrica	Baja	**3**
ERRORES Y FALLOS NO INTENCIONADOS	**E.1**	Errores de los usuarios	Pérdida total o parcial del tiempo de ejecución de sus actividades, dependiendo de la gravedad del asunto.	Baja	**3**
	E.2	Errores del administrador	Pérdida total o parcial del tiempo de ejecución de sus actividades, dependiendo de la gravedad del asunto.	Baja	**3**
	E.8	Difusión de software dañino	La dependencia cuenta con antivirus capaces de controlar software malicioso	Baja	**3**
	E.9	Errores de [re-] encaminamiento	La dependencia cuenta con sistemas de cifrado y verificación (puerto – puerto) para el manejo de la movilidad de la información.	Baja	**3**

Tabla 21. Estimación de la probabilidad activo Windows 8. (Continuación)

	E.10	Errores de secuencia	La dependencia cuenta con sistemas de cifrado y verificación (puerto – puerto) para el manejo de la movilidad de la información.	Baja	**3**
	E.15	Alteración accidental de la información	La dependencia cuenta con sistemas de cifrado y verificación (puerto – puerto) para el manejo de la movilidad de la información.	Baja	**3**
	E.18	Destrucción de información	El departamento de sistemas cuenta con copias de seguridad periódicas	Baja	**3**
	E.19	Fugas de información	Las personas contratadas están atadas a cláusulas de confidencialidad.	Baja	**3**
	E.20	Vulnerabilidades de los programas (software)	La dependencia cuenta con un servidor (personal) para llevar a cabo cada uno de los softwares empleados para la institución.	Baja	**3**
	E.21	Errores de mantenimiento / actualización de programas (software)	Falla de funcionamiento del software.	Baja	**3**
ATAQUES INTENCIONAD	**A.5**	Suplantación de la identidad del usuario	Acceso a personas que no cuenten con los permisos necesarios o con las credenciales necesarias.	Baja	**3**
	A.6	Abuso de privilegios de acceso	Abuso de cada uno de los derechos otorgados.	Baja	**3**

Tabla 21. Estimación de la probabilidad activo Windows 8. (Continuación)

	A.7	Uso no previsto	Implementación de recursos (económicos y de tiempo) en actividades no relacionadas.	Baja	**3**
	A.8	Difusión de software dañino	Afectación en los sistemas de información y los procesos que ello conlleva.	Baja	**3**
	A.9	[Re-]encaminamiento de mensajes	La dependencia cuenta con sistemas de cifrado y verificación (puerto – puerto) para el manejo de la movilidad de la información.	Baja	**3**
	A.10	Alteración de secuencia	Alteración de datos.	Baja	**3**
	A.11	Acceso no autorizado	Uso ilícito del hardware	Baja	**3**
	A.15	Modificación deliberada de la información	Datos erróneos en el momento de la movilización de la información.	Baja	**3**
	A.18	Destrucción de información	Perdida de la información.	Baja	**3**
	A.19	Divulgación de información	Información filtrada abiertamente a personas no correspondientes.	Baja	**3**
	A.22	Manipulación de programas	Alteración del funcionamiento de cada uno de los programas de la dependencia.	Baja	**3**

Fuente: Autoría propia

Tabla 22. Estimación de la probabilidad activo Windows server 2009

ACTIVO TI	SISTEMA OPERATIVO WINDOWS SERVER 2009				
ADMINISTRADOR	PIMIENTO CARDENAS WILSON MAURICIO				
DEGRADACIÓN	60%				
IMPACTO	5				
TIPO DE ACTIVO	SOFTWARE				
Tipo	**ID**	**Amenaza**	**Exposición/Vulnerabilidad**	**Frecuencia (F)**	
DE ORIGEN INDUSTRIAL	**I.5**	Avería de origen físico o lógico	La manipulación por parte de cada uno de los componentes encontrados en la dependencia, como también por defectos de los componentes desde fabrica	Baja	**3**
ERRORES Y FALLOS NO INTENCIONADOS	**E.1**	Errores de los usuarios	Pérdida total o parcial del tiempo de ejecución de sus actividades, dependiendo de la gravedad del asunto.	Baja	**3**
	E.2	Errores del administrador	Pérdida total o parcial del tiempo de ejecución de sus actividades, dependiendo de la gravedad del asunto.	Baja	**3**
	E.8	Difusión de software dañino	La dependencia cuenta con antivirus capaces de controlar software malicioso	Baja	**3**
	E.9	Errores de [re-] encaminamiento	La dependencia cuenta con sistemas de cifrado y verificación (puerto – puerto) para el manejo de la movilidad de la información.	Baja	**3**
	E.10	Errores de secuencia	La dependencia cuenta con sistemas de cifrado y verificación (puerto – puerto) para el manejo de la movilidad de la información.	Baja	**3**

Tabla 22. Estimación de la probabilidad activo Windows server 2009. (Continuación)

	E.15	Alteración accidental de la información	La dependencia cuenta con sistemas de cifrado y verificación (puerto – puerto) para el manejo de la movilidad de la información.	Baja	**3**
	E.18	Destrucción de información	El departamento de sistemas cuenta con copias de seguridad periódicas	Baja	**3**
	E.19	Fugas de información	Las personas contratadas están atadas a cláusulas de confidencialidad.	Baja	**3**
	E.20	Vulnerabilidades de los programas (software)	La dependencia cuenta con un servidor (personal) para llevar a cabo cada uno de los softwares empleados para la institución.	Baja	**3**
	E.21	Errores de mantenimiento / actualización de programas (software)	Falla de funcionamiento del software.	Baja	**3**
ATAQUES INTENCIONAD	**A.5**	Suplantación de la identidad del usuario	Acceso a personas que no cuenten con los permisos necesarios o con las credenciales necesarias.	Baja	**3**
	A.6	Abuso de privilegios de acceso	Abuso de cada uno de los derechos otorgados.	Baja	**3**
	A.7	Uso no previsto	Implementación de recursos (económicos y de tiempo) en actividades no relacionadas.	Baja	**3**

Tabla 22. Estimación de la probabilidad activo Windows server 2009. (Continuación)

	A.8	Difusión de software dañino	Afectación en los sistemas de información y los procesos que ello conlleva.	Baja	**3**
	A.9	[Re-]encaminamiento de mensajes	La dependencia cuenta con sistemas de cifrado y verificación (puerto – puerto) para el manejo de la movilidad de la información.	Baja	**3**
	A.10	Alteración de secuencia	Alteración de datos.	Baja	**3**
	A.11	Acceso no autorizado	Uso ilícito del hardware	Baja	**3**
	A.15	Modificación deliberada de la información	Datos erróneos en el momento de la movilización de la información.	Baja	**3**
	A.18	Destrucción de información	Perdida de la información.	Baja	**3**
	A.19	Divulgación de información	Información filtrada abiertamente a personas no correspondientes.	Baja	**3**
	A.22	Manipulación de programas	Alteración del funcionamiento de cada uno de los programas de la dependencia.	Baja	**3**

Fuente: Autoría propia

Tabla 23. Estimación de la probabilidad activo Windows server 2012

ACTIVO TI	SISTEMA OPERATIVO WINDOWS SERVER 2012			
ADMINISTRADOR	PIMIENTO CARDENAS WILSON MAURICIO			
DEGRADACIÓN	60%			
IMPACTO	5			
TIPO DE ACTIVO	SOFTWARE			
Tipo	**ID**	**Amenaza**	**Exposición/Vulnerabilidad**	**Frecuencia (F)**

Tabla 23. Estimación de la probabilidad activo Windows server 2012. (Continuación)

DE ORIGEN INDUSTRIAL	**I.5**	Avería de origen físico o lógico	La manipulación por parte de cada uno de los componentes encontrados en la dependencia, como también por defectos de los componentes desde fabrica	Baja	**3**
ERRORES Y FALLOS NO INTENCIONADOS	**E.1**	Errores de los usuarios	Pérdida total o parcial del tiempo de ejecución de sus actividades, dependiendo de la gravedad del asunto.	Baja	**3**
	E.2	Errores del administrador	Pérdida total o parcial del tiempo de ejecución de sus actividades, dependiendo de la gravedad del asunto.	Baja	**3**
	E.8	Difusión de software dañino	La dependencia cuenta con antivirus capaces de controlar software malicioso	Baja	**3**
	E.9	Errores de [re-] encaminamiento	La dependencia cuenta con sistemas de cifrado y verificación (puerto – puerto) para el manejo de la movilidad de la información.	Baja	**3**
	E.10	Errores de secuencia	La dependencia cuenta con sistemas de cifrado y verificación (puerto – puerto) para el manejo de la movilidad de la información.	Baja	**3**
	E.15	Alteración accidental de la información	La dependencia cuenta con sistemas de cifrado y verificación (puerto – puerto) para el manejo de la movilidad de la información.	Baja	**3**

Tabla 23. Estimación de la probabilidad activo Windows server 2012. (Continuación)

	E.18	Destrucción de información	El departamento de sistemas cuenta con copias de seguridad periódicas	Baja	**3**
	E.19	Fugas de información	Las personas contratadas están atadas a cláusulas de confidencialidad.	Baja	**3**
	E.20	Vulnerabilidades de los programas (software)	La dependencia cuenta con un servidor (personal) para llevar a cabo cada uno de los *softwares* empleados para la institución.	Baja	**3**
	E.21	Errores de mantenimiento / actualización de programas (software)	Falla de funcionamiento del software.	Baja	**3**
ATAQUES INTENCIONAD	**A.5**	Suplantación de la identidad del usuario	Acceso a personas que no cuenten con los permisos necesarios o con las credenciales necesarias.	Baja	**3**
	A.6	Abuso de privilegios de acceso	Abuso de cada uno de los derechos otorgados.	Baja	**3**
	A.7	Uso no previsto	Implementación de recursos (económicos y de tiempo) en actividades no relacionadas.	Baja	**3**
	A.8	Difusión de software dañino	Afectación en los sistemas de información y los procesos que ello conlleva.	Baja	**3**
	A.9	[Re-]encaminamiento de mensajes	La dependencia cuenta con sistemas de cifrado y verificación (puerto –	Baja	**3**

Tabla 23. Estimación de la probabilidad activo Windows server 2012. (Continuación)

			puerto) para el manejo de la movilidad de la información.		
	A.10	Alteración de secuencia	Alteración de datos.	Baja	**3**
	A.11	Acceso no autorizado	Uso ilícito del hardware	Baja	**3**
	A.15	Modificación deliberada de la información	Datos erróneos en el momento de la movilización de la información.	Baja	**3**
	A.18	Destrucción de información	Perdida de la información.	Baja	**3**
	A.19	Divulgación de información	Información filtrada abiertamente a personas no correspondientes.	Baja	**3**
	A.22	Manipulación de programas	Alteración del funcionamiento de cada uno de los programas de la dependencia.	Baja	**3**

Fuente: Autoría propia

Tabla 24. Estimación de la probabilidad activo CentOS 5

ACTIVO TI	SISTEMA OPERATIVO CentOS 5				
ADMINISTRADOR	PIMIENTO CARDENAS WILSON MAURICIO				
DEGRADACIÓN	60%				
IMPACTO	5				
TIPO DE ACTIVO	SOFTWARE				
Tipo	**ID**	**Amenaza**	**Exposición/Vulnerabilidad**	**Frecuencia (F)**	
DE ORIGEN INDUSTRIAL	**I.5**	Avería de origen físico o lógico	La manipulación por parte de cada uno de los componentes encontrados en la dependencia, como también por defectos de los componentes desde fabrica	Baja	**3**

Tabla 24. Estimación de la probabilidad activo CentOS 5. (Continuación)

ERRORES Y FALLOS NO INTENCIONADOS	**E.1**	Errores de los usuarios	Pérdida total o parcial del tiempo de ejecución de sus actividades, dependiendo de la gravedad del asunto.	Baja	**3**
	E.2	Errores del administrador	Pérdida total o parcial del tiempo de ejecución de sus actividades, dependiendo de la gravedad del asunto.	Baja	**3**
	E.8	Difusión de software dañino	La dependencia cuenta con antivirus capaces de controlar software malicioso	Baja	**3**
	E.9	Errores de [re-] encaminamiento	La dependencia cuenta con sistemas de cifrado y verificación (puerto – puerto) para el manejo de la movilidad de la información.	Baja	**3**
	E.10	Errores de secuencia	La dependencia cuenta con sistemas de cifrado y verificación (puerto – puerto) para el manejo de la movilidad de la información.	Baja	**3**
	E.15	Alteración accidental de la información	La dependencia cuenta con sistemas de cifrado y verificación (puerto – puerto) para el manejo de la movilidad de la información.	Baja	**3**
	E.18	Destrucción de información	El departamento de sistemas cuenta con copias de seguridad periódicas	Baja	**3**
	E.19	Fugas de información	Las personas contratadas están atadas a cláusulas de confidencialidad.	Baja	**3**

Tabla 24. Estimación de la probabilidad activo CentOS 5. (Continuación)

	E.20	Vulnerabilidades de los programas (software)	La dependencia cuenta con un servidor (personal) para llevar a cabo cada uno de los softwares empleados para la institución.	Baja	**3**
	E.21	Errores de mantenimiento / actualización de programas (software)	Falla de funcionamiento del software.	Baja	**3**
ATAQUES INTENCIONAD	**A.5**	Suplantación de la identidad del usuario	Acceso a personas que no cuenten con los permisos necesarios o con las credenciales necesarias.	Baja	**3**
	A.6	Abuso de privilegios de acceso	Abuso de cada uno de los derechos otorgados.	Baja	**3**
	A.7	Uso no previsto	Implementación de recursos (económicos y de tiempo) en actividades no relacionadas.	Baja	**3**
	A.8	Difusión de software dañino	Afectación en los sistemas de información y los procesos que ello conlleva.	Baja	**3**
	A.9	[Re-]encaminamiento de mensajes	La dependencia cuenta con sistemas de cifrado y verificación (puerto – puerto) para el manejo de la movilidad de la información.	Baja	**3**
	A.10	Alteración de secuencia	Alteración de datos.	Baja	**3**
	A.11	Acceso no autorizado	Uso ilícito del hardware	Baja	**3**

Tabla 24. Estimación de la probabilidad activo CentOS 5. (Continuación)

	A.15	Modificación deliberada de la información	Datos erróneos en el momento de la movilización de la información.	Baja	**3**
	A.18	Destrucción de información	Perdida de la información.	Baja	**3**
	A.19	Divulgación de información	Información filtrada abiertamente a personas no correspondientes.	Baja	**3**
	A.22	Manipulación de programas	Alteración del funcionamiento de cada uno de los programas de la dependencia.	Baja	**3**

Fuente: Autoría propia

Tabla 25. Estimación de la probabilidad activo Debian 7

ACTIVO TI	SISTEMA OPERATIVO DEBIAN 7				
ADMINISTRADOR	PIMIENTO CARDENAS WILSON MAURICIO				
DEGRADACIÓN	60%				
IMPACTO	5				
TIPO DE ACTIVO	SOFTWARE				
Tipo	**ID**	**Amenaza**	**Exposición/Vulnerabilidad**	**Frecuencia (F)**	
DE ORIGEN INDUSTRIAL	**I.5**	Avería de origen físico o lógico	La manipulación por parte de cada uno de los componentes encontrados en la dependencia, como también por defectos de los componentes desde fabrica	Baja	**3**
ERRORES Y NO FALLOS	**E.1**	Errores de los usuarios	Pérdida total o parcial del tiempo de ejecución de sus actividades, dependiendo de la gravedad del asunto.	Baja	**3**
	E.2	Errores del administrador	Pérdida total o parcial del tiempo de ejecución de sus	Baja	**3**

Tabla 25. Estimación de la probabilidad activo Debian 7. (Continuación)

			actividades, dependiendo de la gravedad del asunto.		
	E.8	Difusión de software dañino	La dependencia cuenta con antivirus capaces de controlar software malicioso	Baja	**3**
	E.9	Errores de [re-] encaminamiento	La dependencia cuenta con sistemas de cifrado y verificación (puerto – puerto) para el manejo de la movilidad de la información.	Baja	**3**
	E.10	Errores de secuencia	La dependencia cuenta con sistemas de cifrado y verificación (puerto – puerto) para el manejo de la movilidad de la información.	Baja	**3**
	E.15	Alteración accidental de la información	La dependencia cuenta con sistemas de cifrado y verificación (puerto – puerto) para el manejo de la movilidad de la información.	Baja	**3**
	E.18	Destrucción de información	El departamento de sistemas cuenta con copias de seguridad periódicas	Baja	**3**
	E.19	Fugas de información	Las personas contratadas están atadas a cláusulas de confidencialidad.	Baja	**3**
	E.20	Vulnerabilidades de los programas (software)	La dependencia cuenta con un servidor (personal) para llevar a cabo cada uno de los softwares empleados para la institución.	Baja	**3**
	E.21	Errores de mantenimiento /	Falla de funcionamiento del software.	Baja	**3**

Tabla 25. Estimación de la probabilidad activo Debian 7. (Continuación)

		actualización de programas (software)			
ATAQUES INTENCIONAD	**A.5**	Suplantación de la identidad del usuario	Acceso a personas que no cuenten con los permisos necesarios o con las credenciales necesarias.	Baja	**3**
	A.6	Abuso de privilegios de acceso	Abuso de cada uno de los derechos otorgados.	Baja	**3**
	A.7	Uso no previsto	Implementación de recursos (económicos y de tiempo) en actividades no relacionadas.	Baja	**3**
	A.8	Difusión de software dañino	Afectación en los sistemas de información y los procesos que ello conlleva.	Baja	**3**
	A.9	[Re-]encaminamiento de mensajes	La dependencia cuenta con sistemas de cifrado y verificación (puerto – puerto) para el manejo de la movilidad de la información.	Baja	**3**
	A.10	Alteración de secuencia	Alteración de datos.	Baja	**3**
	A.11	Acceso no autorizado	Uso ilícito del hardware	Baja	**3**
	A.15	Modificación deliberada de la información	Datos erróneos en el momento de la movilización de la información.	Baja	**3**
	A.18	Destrucción de información	Perdida de la información.	Baja	**3**

Tabla 25. Estimación de la probabilidad activo Debian 7. (Continuación)

	A.19	Divulgación de información	Información filtrada abiertamente a personas no correspondientes.	Baja	**3**
	A.22	Manipulación de programas	Alteración del funcionamiento de cada uno de los programas de la dependencia.	Baja	**3**

Fuente: Autoría propia

Tabla 26. Estimación de la probabilidad activo Ubuntu 14

ACTIVO TI	SISTEMA OPERATIVO UBUNTU 14
ADMINISTRADOR	PIMIENTO CARDENAS WILSON MAURICIO
DEGRADACIÓN	20%
IMPACTO	2
TIPO DE ACTIVO	SOFTWARE

Tipo	**ID**	**Amenaza**	**Exposición/Vulnerabilidad**	**Frecuencia (F)**	
DE ORIGEN INDUSTRIAL	**I.5**	Avería de origen físico o lógico	La manipulación por parte de cada uno de los componentes encontrados en la dependencia, como también por defectos de los componentes desde fabrica	Baja	**3**
ERRORES Y FALLOS NO INTENCIONADOS	**E.1**	Errores de los usuarios	Pérdida total o parcial del tiempo de ejecución de sus actividades, dependiendo de la gravedad del asunto.	Baja	**3**
	E.2	Errores del administrador	Pérdida total o parcial del tiempo de ejecución de sus actividades, dependiendo de la gravedad del asunto.	Baja	**3**
	E.8	Difusión de software dañino	La dependencia cuenta con antivirus capaces de controlar software malicioso	Baja	**3**

Tabla 26. Estimación de la probabilidad activo Ubuntu 14. (Continuación)

	E.9	Errores de [re-] encaminamiento	La dependencia cuenta con sistemas de cifrado y verificación (puerto – puerto) para el manejo de la movilidad de la información.	Baja	**3**
	E.10	Errores de secuencia	La dependencia cuenta con sistemas de cifrado y verificación (puerto – puerto) para el manejo de la movilidad de la información.	Baja	**3**
	E.15	Alteración accidental de la información	La dependencia cuenta con sistemas de cifrado y verificación (puerto – puerto) para el manejo de la movilidad de la información.	Baja	**3**
	E.18	Destrucción de información	El departamento de sistemas cuenta con copias de seguridad periódicas	Baja	**3**
	E.19	Fugas de información	Las personas contratadas están atadas a cláusulas de confidencialidad.	Baja	**3**
	E.20	Vulnerabilidades de los programas (software)	La dependencia cuenta con un servidor (personal) para llevar a cabo cada uno de los softwares empleados para la institución.	Baja	**3**
	E.21	Errores de mantenimiento / actualización de programas (software)	Falla de funcionamiento del software.	Baja	**3**

Tabla 26. Estimación de la probabilidad activo Ubuntu 14. (Continuación)

ATAQUES INTENCIONAD	**A.5**	Suplantación de la identidad del usuario	Acceso a personas que no cuenten con los permisos necesarios o con las credenciales necesarias.	Baja	**3**
	A.6	Abuso de privilegios de acceso	Abuso de cada uno de los derechos otorgados.	Baja	**3**
	A.7	Uso no previsto	Implementación de recursos (económicos y de tiempo) en actividades no relacionadas.	Baja	**3**
	A.8	Difusión de software dañino	Afectación en los sistemas de información y los procesos que ello conlleva.	Baja	**3**
	A.9	[Re-]encaminamiento de mensajes	La dependencia cuenta con sistemas de cifrado y verificación (puerto – puerto) para el manejo de la movilidad de la información.	Baja	**3**
	A.10	Alteración de secuencia	Alteración de datos.	Baja	**3**
	A.11	Acceso no autorizado	Uso ilícito del hardware	Baja	**3**
	A.15	Modificación deliberada de la información	Datos erróneos en el momento de la movilización de la información.	Baja	**3**
	A.18	Destrucción de información	Perdida de la información.	Baja	**3**
	A.19	Divulgación de información	Información filtrada abiertamente a personas no correspondientes.	Baja	**3**

Tabla 26. Estimación de la probabilidad activo Ubuntu 14. (Continuación)

	A.22	Manipulación de programas	Alteración del funcionamiento de cada uno de los programas de la dependencia.	Baja	**3**

Fuente: Autoría propia

Tabla 27. Estimación de la probabilidad activo Mac os x

ACTIVO TI	SISTEMA OPERATIVO MAC OS X
ADMINISTRADOR	PIMIENTO CARDENAS WILSON MAURICIO
DEGRADACIÓN	60%
IMPACTO	5
TIPO DE ACTIVO	SOFTWARE

Tipo	**ID**	**Amenaza**	**Exposición/Vulnerabilidad**	**Frecuencia (F)**	
DE ORIGEN INDUSTRIAL	**I.5**	Avería de origen físico o lógico	La manipulación por parte de cada uno de los componentes encontrados en la dependencia, como también por defectos de los componentes desde fabrica	Baja	**3**
ERRORES Y FALLOS NO INTENCIONADOS	**E.1**	Errores de los usuarios	Pérdida total o parcial del tiempo de ejecución de sus actividades, dependiendo de la gravedad del asunto.	Baja	**3**
	E.2	Errores del administrador	Pérdida total o parcial del tiempo de ejecución de sus actividades, dependiendo de la gravedad del asunto.	Baja	**3**
	E.8	Difusión de software dañino	La dependencia cuenta con antivirus capaces de controlar software malicioso	Baja	**3**
	E.9	Errores de [re-] encaminamiento	La dependencia cuenta con sistemas de cifrado y verificación (puerto – puerto) para el manejo de la movilidad de la información.	Baja	**3**

Tabla 27. Estimación de la probabilidad activo Mac os x. (Continuación)

	E.10	Errores de secuencia	La dependencia cuenta con sistemas de cifrado y verificación (puerto – puerto) para el manejo de la movilidad de la información.	Baja	**3**
	E.15	Alteración accidental de la información	La dependencia cuenta con sistemas de cifrado y verificación (puerto – puerto) para el manejo de la movilidad de la información.	Baja	**3**
	E.18	Destrucción de información	El departamento de sistemas cuenta con copias de seguridad periódicas	Baja	**3**
	E.19	Fugas de información	Las personas contratadas están atadas a cláusulas de confidencialidad.	Baja	**3**
	E.20	Vulnerabilidades de los programas (software)	La dependencia cuenta con un servidor (personal) para llevar a cabo cada uno de los softwares empleados para la institución.	Baja	**3**
	E.21	Errores de mantenimiento / actualización de programas (software)	Falla de funcionamiento del software.	Baja	**3**
ATAQUES INTENCIONAD	**A.5**	Suplantación de la identidad del usuario	Acceso a personas que no cuenten con los permisos necesarios o con las credenciales necesarias.	Baja	**3**
	A.6	Abuso de privilegios de acceso	Abuso de cada uno de los derechos otorgados.	Baja	**3**

Tabla 27. Estimación de la probabilidad activo Mac os x. (Continuación)

	A.7	Uso no previsto	Implementación de recursos (económicos y de tiempo) en actividades no relacionadas.	Baja	**3**
	A.8	Difusión de software dañino	Afectación en los sistemas de información y los procesos que ello conlleva.	Baja	**3**
	A.9	[Re-]encaminamiento de mensajes	La dependencia cuenta con sistemas de cifrado y verificación (puerto – puerto) para el manejo de la movilidad de la información.	Baja	**3**
	A.10	Alteración de secuencia	Alteración de datos.	Baja	**3**
	A.11	Acceso no autorizado	Uso ilícito del hardware	Baja	**3**
	A.15	Modificación deliberada de la información	Datos erróneos en el momento de la movilización de la información.	Baja	**3**
	A.18	Destrucción de información	Perdida de la información.	Baja	**3**
	A.19	Divulgación de información	Información filtrada abiertamente a personas no correspondientes.	Baja	**3**
	A.22	Manipulación de programas	Alteración del funcionamiento de cada uno de los programas de la dependencia.	Baja	**3**

Fuente: Autoría propia

Tabla 28. Estimación de la probabilidad activo COMMAND (CMD)

ACTIVO TI	TERMINAL COMMAND (CMD)
ADMINISTRADOR	PIMIENTO CARDENAS WILSON MAURICIO
DEGRADACIÓN	25%
IMPACTO	2
TIPO DE ACTIVO	SOFTWARE

Tipo	ID	Amenaza	Exposición/Vulnerabilidad	Frecuencia (F)	
DE ORIGEN INDUSTRIAL	**I.5**	Avería de origen físico o lógico	La manipulación por parte de cada uno de los componentes encontrados en la dependencia, como también por defectos de los componentes desde fabrica	Baja	**3**
ERRORES Y FALLOS NO INTENCIONADOS	**E.1**	Errores de los usuarios	Pérdida total o parcial del tiempo de ejecución de sus actividades, dependiendo de la gravedad del asunto.	Baja	**3**
	E.2	Errores del administrador	Pérdida total o parcial del tiempo de ejecución de sus actividades, dependiendo de la gravedad del asunto.	Baja	**3**
	E.8	Difusión de software dañino	La dependencia cuenta con antivirus capaces de controlar software malicioso	Baja	**3**
	E.9	Errores de [re-] encaminamiento	La dependencia cuenta con sistemas de cifrado y verificación (puerto – puerto) para el manejo de la movilidad de la información.	Baja	**3**
	E.10	Errores de secuencia	La dependencia cuenta con sistemas de cifrado y verificación (puerto – puerto) para el manejo de la movilidad de la información.	Baja	**3**

Tabla 28. Estimación de la probabilidad activo COMMAND (CMD). (Continuación)

	E.15	Alteración accidental de la información	La dependencia cuenta con sistemas de cifrado y verificación (puerto – puerto) para el manejo de la movilidad de la información.	Baja	**3**
	E.18	Destrucción de información	El departamento de sistemas cuenta con copias de seguridad periódicas	Baja	**3**
	E.19	Fugas de información	Las personas contratadas están atadas a cláusulas de confidencialidad.	Baja	**3**
	E.20	Vulnerabilidades de los programas (software)	La dependencia cuenta con un servidor (personal) para llevar a cabo cada uno de los softwares empleados para la institución.	Baja	**3**
	E.21	Errores de mantenimiento / actualización de programas (software)	Falla de funcionamiento del software.	Baja	**3**
ATAQUES INTENCIONAD	**A.5**	Suplantación de la identidad del usuario	Acceso a personas que no cuenten con los permisos necesarios o con las credenciales necesarias.	Baja	**3**
	A.6	Abuso de privilegios de acceso	Abuso de cada uno de los derechos otorgados.	Baja	**3**
	A.7	Uso no previsto	Implementación de recursos (económicos y de tiempo) en actividades no relacionadas.	Baja	**3**

Tabla 28. Estimación de la probabilidad activo COMMAND (CMD). (Continuación)

	A.8	Difusión de software dañino	Afectación en los sistemas de información y los procesos que ello conlleva.	Baja	**3**
	A.9	[Re-]encaminamiento de mensajes	La dependencia cuenta con sistemas de cifrado y verificación (puerto – puerto) para el manejo de la movilidad de la información.	Baja	**3**
	A.10	Alteración de secuencia	Alteración de datos.	Baja	**3**
	A.11	Acceso no autorizado	Uso ilícito del hardware	Baja	**3**
	A.15	Modificación deliberada de la información	Datos erróneos en el momento de la movilización de la información.	Baja	**3**
	A.18	Destrucción de información	Perdida de la información.	Baja	**3**
	A.19	Divulgación de información	Información filtrada abiertamente a personas no correspondientes.	Baja	**3**
	A.22	Manipulación de programas	Alteración del funcionamiento de cada uno de los programas de la dependencia.	Baja	**3**

Fuente: Autoría propia

Tabla 29. Estimación de la probabilidad activo CoMmanD line (Mac)

ACTIVO TI	TERMINAL COMMAND LINE (MAC)			
ADMINISTRADOR	PIMIENTO CARDENAS WILSON MAURICIO			
DEGRADACIÓN	45%			
IMPACTO	3			
TIPO DE ACTIVO	SOFTWARE			
Tipo	**ID**	**Amenaza**	**Exposición/Vulnerabilidad**	**Frecuencia (F)**

Tabla 29. Estimación de la probabilidad activo CoMmanD line (Mac). (Continuación)

DE ORIGEN INDUSTRIAL	**I.5**	Avería de origen físico o lógico	La manipulación por parte de cada uno de los componentes encontrados en la dependencia, como también por defectos de los componentes desde fabrica	Baja	**3**
ERRORES Y FALLOS NO INTENCIONADOS	**E.1**	Errores de los usuarios	Pérdida total o parcial del tiempo de ejecución de sus actividades, dependiendo de la gravedad del asunto.	Baja	**3**
	E.2	Errores del administrador	Pérdida total o parcial del tiempo de ejecución de sus actividades, dependiendo de la gravedad del asunto.	Baja	**3**
	E.8	Difusión de software dañino	La dependencia cuenta con antivirus capaces de controlar software malicioso	Baja	**3**
	E.9	Errores de [re-] encaminamiento	La dependencia cuenta con sistemas de cifrado y verificación (puerto – puerto) para el manejo de la movilidad de la información.	Baja	**3**
	E.10	Errores de secuencia	La dependencia cuenta con sistemas de cifrado y verificación (puerto – puerto) para el manejo de la movilidad de la información.	Baja	**3**
	E.15	Alteración accidental de la información	La dependencia cuenta con sistemas de cifrado y verificación (puerto – puerto) para el manejo de la movilidad de la información.	Baja	**3**

Tabla 29. Estimación de la probabilidad activo CoMmanD line (Mac). (Continuación)

	E.18	Destrucción de información	El departamento de sistemas cuenta con copias de seguridad periódicas	Baja	**3**
	E.19	Fugas de información	Las personas contratadas están atadas a cláusulas de confidencialidad.	Baja	**3**
	E.20	Vulnerabilidades de los programas (software)	La dependencia cuenta con un servidor (personal) para llevar a cabo cada uno de los softwares empleados para la institución.	Baja	**3**
	E.21	Errores de mantenimiento / actualización de programas (software)	Falla de funcionamiento del software.	Baja	**3**
ATAQUES INTENCIONAD	**A.5**	Suplantación de la identidad del usuario	Acceso a personas que no cuenten con los permisos necesarios o con las credenciales necesarias.	Baja	**3**
	A.6	Abuso de privilegios de acceso	Abuso de cada uno de los derechos otorgados.	Baja	**3**
	A.7	Uso no previsto	Implementación de recursos (económicos y de tiempo) en actividades no relacionadas.	Baja	**3**
	A.8	Difusión de software dañino	Afectación en los sistemas de información y los procesos que ello conlleva.	Baja	**3**
	A.9	[Re-]encaminamiento de mensajes	La dependencia cuenta con sistemas de cifrado y verificación (puerto –	Baja	**3**

Tabla 29. Estimación de la probabilidad activo CoMmanD line (Mac). (Continuación)

			puerto) para el manejo de la movilidad de la información.		
	A.10	Alteración de secuencia	Alteración de datos.	Baja	**3**
	A.11	Acceso no autorizado	Uso ilícito del hardware	Baja	**3**
	A.15	Modificación deliberada de la información	Datos erróneos en el momento de la movilización de la información.	Baja	**3**
	A.18	Destrucción de información	Perdida de la información.	Baja	**3**
	A.19	Divulgación de información	Información filtrada abiertamente a personas no correspondientes.	Baja	**3**
	A.22	Manipulación de programas	Alteración del funcionamiento de cada uno de los programas de la dependencia.	Baja	**3**

Fuente: Autoría propia

Tabla 30. Estimación de la probabilidad activo terminal

ACTIVO TI	TERMINAL LINUX				
ADMINISTRADOR	PIMIENTO CARDENAS WILSON MAURICIO				
DEGRADACIÓN	30%				
IMPACTO	2				
TIPO DE ACTIVO	SOFTWARE				
Tipo	**ID**	**Amenaza**	**Exposición/Vulnerabilidad**	**Frecuencia (F)**	
DE ORIGEN INDUSTRIAL	**I.5**	Avería de origen físico o lógico	La manipulación por parte de cada uno de los componentes encontrados en la dependencia, como también por defectos de los componentes desde fabrica	Baja	**3**

Tabla 30. Estimación de la probabilidad activo terminal. (Continuación)

ERRORES Y FALLOS NO INTENCIONADOS	**E.1**	Errores de los usuarios	Pérdida total o parcial del tiempo de ejecución de sus actividades, dependiendo de la gravedad del asunto.	Baja	**3**
	E.2	Errores del administrador	Pérdida total o parcial del tiempo de ejecución de sus actividades, dependiendo de la gravedad del asunto.	Baja	**3**
	E.8	Difusión de software dañino	La dependencia cuenta con antivirus capaces de controlar software malicioso	Baja	**3**
	E.9	Errores de [re-] encaminamiento	La dependencia cuenta con sistemas de cifrado y verificación (puerto – puerto) para el manejo de la movilidad de la información.	Baja	**3**
	E.10	Errores de secuencia	La dependencia cuenta con sistemas de cifrado y verificación (puerto – puerto) para el manejo de la movilidad de la información.	Baja	**3**
	E.15	Alteración accidental de la información	La dependencia cuenta con sistemas de cifrado y verificación (puerto – puerto) para el manejo de la movilidad de la información.	Baja	**3**
	E.18	Destrucción de información	El departamento de sistemas cuenta con copias de seguridad periódicas	Baja	**3**
	E.19	Fugas de información	Las personas contratadas están atadas a cláusulas de confidencialidad.	Baja	**3**

Tabla 30. Estimación de la probabilidad activo terminal. (Continuación)

	E.20	Vulnerabilidades de los programas (software)	La dependencia cuenta con un servidor (personal) para llevar a cabo cada uno de los softwares empleados para la institución.	Baja	**3**
	E.21	Errores de mantenimiento / actualización de programas (software)	Falla de funcionamiento del software.	Baja	**3**
ATAQUES INTENCIONAD	**A.5**	Suplantación de la identidad del usuario	Acceso a personas que no cuenten con los permisos necesarios o con las credenciales necesarias.	Baja	**3**
	A.6	Abuso de privilegios de acceso	Abuso de cada uno de los derechos otorgados.	Baja	**3**
	A.7	Uso no previsto	Implementación de recursos (económicos y de tiempo) en actividades no relacionadas.	Baja	**3**
	A.8	Difusión de software dañino	Afectación en los sistemas de información y los procesos que ello conlleva.	Baja	**3**
	A.9	[Re-]encaminamiento de mensajes	La dependencia cuenta con sistemas de cifrado y verificación (puerto – puerto) para el manejo de la movilidad de la información.	Baja	**3**
	A.10	Alteración de secuencia	Alteración de datos.	Baja	**3**
	A.11	Acceso no autorizado	Uso ilícito del hardware	Baja	**3**

Tabla 30. Estimación de la probabilidad activo terminal. (Continuación)

	A.15	Modificación deliberada de la información	Datos erróneos en el momento de la movilización de la información.	Baja	**3**
	A.18	Destrucción de información	Perdida de la información.	Baja	**3**
	A.19	Divulgación de información	Información filtrada abiertamente a personas no correspondientes.	Baja	**3**
	A.22	Manipulación de programas	Alteración del funcionamiento de cada uno de los programas de la dependencia.	Baja	**3**

Fuente: Autoría propia

Tabla 31. Estimación de la probabilidad activo servidor DNS y DHCP

ACTIVO TI	SERVIDOR DNS Y DHCP				
ADMINISTRADOR	PIMIENTO CARDENAS WILSON MAURICIO				
DEGRADACIÓN	90%				
IMPACTO	8				
TIPO DE ACTIVO	HARDWARE				
Tipo	**ID**	**Amenaza**	**Exposición/Vulnerabilidad**	**Frecuencia (F)**	
DESASTRES NATURALES	**N.1**	Fuego	No existe sistema de alarma contra incendios. Se posee un solo extintor de solkaflam (clase c) recomendados para incendios en lugares donde se encuentren equipos eléctricos.	Muy baja	**2**
	N.2	Daños por agua	La infraestructura está expuesta a goteras, cuenta con averías en el techo en donde el agua de las lluvias	Muy baja	**2**

Tabla 31. Estimación de la probabilidad activo servidor DNS y DHCP. (Continuación)

	N.*	Desastres naturales	La oficina de la dependencia de sistemas se encuentra en zona baja de riesgo de desastre natural de origen volcánico debido a su cercanía con el volcán nevado del Tolima.	Raro	**1**
DE ORIGEN INDUSTRIAL	**I.1**	Fuego	No existe sistema de alarma contra incendios. Se posee un solo extintor de solkaflam (clase c) recomendados para incendios en lugares donde se encuentren equipos eléctricos.	Muy baja	**2**
	I.2	Daños por agua	La concentración del líquido sobrante por parte del aire acondicionado causaría daños en los equipos.	Muy baja	**2**
	I.*	Desastres industriales	No hay exposición o vulnerabilidad, por parte de esta amenaza.	Muy baja	**2**
	I.3	Contaminación mecánica	No hay exposición o vulnerabilidad, por parte de esta amenaza.	Muy baja	**2**
	I.4	Contaminación electromagnética	No hay exposición o vulnerabilidad, por parte de esta amenaza.	Muy baja	**2**
	I.5	Avería de origen físico o lógico	La manipulación por parte de cada uno de los componentes encontrados en la dependencia, como también por defectos de los componentes desde fabrica	Muy baja	**2**

Tabla 31. Estimación de la probabilidad activo servidor DNS y DHCP. (Continuación)

	I.6	Corte del suministro eléctrico	Amenaza debida a factores externos, a clemencias de tipo naturales como lluvias u otros.	Muy baja	**2**
	I.7	Condiciones inadecuadas de temperatura o humedad	No se cuenta con una infraestructura adecuada para soportar los defectos del sistema de refrigeración.	Muy baja	**2**
	I.11	Emanaciones electromagnéticas	No hay exposición o vulnerabilidad, por parte de esta amenaza.	Muy baja	**2**
ERRORES Y FALLOS NO INTENCIONADOS	**E.2**	Errores del administrador	Pérdida total o parcial del tiempo de ejecución de sus actividades, dependiendo de la gravedad del asunto.	Muy baja	**2**
	E.23	Errores de mantenimiento / actualización de equipos(hardware)	Perjuicio a la mantenibilidad del sistema de información.	Muy baja	**2**
	E.24	Caída del sistema por agotamiento de recursos	Saturación del sistema informático.	Muy baja	**2**
	E.25	Perdida de equipos (Robo)	Recuperación de soportes reciclados o desechados.	Muy baja	**2**
ATAQUES INTENCIONADOS	**A.6**	Abuso de privilegios de acceso	Abuso de cada uno de los derechos otorgados.	Muy baja	**2**
	A.7	Uso no previsto	Implementación de recursos (económicos y de tiempo) en actividades no relacionadas.	Muy baja	**2**

Tabla 31. Estimación de la probabilidad activo servidor DNS y DHCP. (Continuación)

	A.11	Acceso no autorizado	Uso ilícito del hardware	Muy baja	**2**
	A.23	Manipulación de los equipos	Sabotaje del hardware y software conteniente.	Muy baja	**2**
	A.24	Denegación de servicio	Saturación del sistema de información.	Muy baja	**2**
	A.25	Robo	Robo de porte de la información, puede esta ser física o digital.	Muy baja	**2**
	A.26	Ataque destructivo	Destrucción de los contenedores de la información, en recipientes físicos y lógicos.	Muy baja	**2**

Fuente: Autoría propia

Tabla 32. Estimación de la probabilidad activo servidor plataforma RYCA V.2.0

ACTIVO TI	SERVIDOR PLATAFORMA RYCA V.2.0				
ADMINISTRADOR	PIMIENTO CARDENAS WILSON MAURICIO				
DEGRADACIÓN	90%				
IMPACTO	8				
TIPO DE ACTIVO	HARDWARE				
Tipo	**ID**	**Amenaza**	**Exposición/Vulnerabilidad**	**Frecuencia (F)**	
DESASTRES NATURALES	**N.1**	Fuego	No existe sistema de alarma contra incendios. Se posee un solo extintor de solkaflam (clase c) recomendados para incendios en lugares donde se encuentren equipos eléctricos.	Muy baja	**2**
	N.2	Daños por agua	La infraestructura está expuesta a goteras, cuenta con averías en el techo en donde el agua de las lluvias	Muy baja	**2**

Tabla 32. Estimación de la probabilidad activo servidor plataforma RYCA V.2.0. (Continuación)

	N.*	Desastres naturales	La oficina de la dependencia de sistemas se encuentra en zona baja de riesgo de desastre natural de origen volcánico debido a su cercanía con el volcán nevado del Tolima.	Raro	**1**
DE ORIGEN INDUSTRIAL	**I.1**	Fuego	No existe sistema de alarma contra incendios. Se posee un solo extintor de solkaflam (clase c) recomendados para incendios en lugares donde se encuentren equipos eléctricos.	Muy baja	**2**
	I.2	Daños por agua	La concentración del líquido sobrante por parte del aire acondicionado causaría daños en los equipos.	Muy baja	**2**
	I.*	Desastres industriales	No hay exposición o vulnerabilidad, por parte de esta amenaza.	Muy baja	**2**
	I.3	Contaminación mecánica	No hay exposición o vulnerabilidad, por parte de esta amenaza.	Muy baja	**2**
	I.4	Contaminación electromagnética	No hay exposición o vulnerabilidad, por parte de esta amenaza.	Muy baja	**2**
	I.5	Avería de origen físico o lógico	La manipulación por parte de cada uno de los componentes encontrados en la dependencia, como también por defectos de los componentes desde fabrica	Muy baja	**2**

Tabla 32. Estimación de la probabilidad activo servidor plataforma RYCA V.2.0. (Continuación)

	I.6	Corte del suministro eléctrico	Amenaza debida a factores externos, a clemencias de tipo naturales como lluvias u otros.	Muy baja	**2**
	I.7	Condiciones inadecuadas de temperatura o humedad	No se cuenta con una infraestructura adecuada para soportar los defectos del sistema de refrigeración.	Muy baja	**2**
	I.11	Emanaciones electromagnéticas	No hay exposición o vulnerabilidad, por parte de esta amenaza.	Muy baja	**2**
ERRORES Y FALLOS NO INTENCIONADOS	**E.2**	Errores del administrador	Pérdida total o parcial del tiempo de ejecución de sus actividades, dependiendo de la gravedad del asunto.	Muy baja	**2**
	E.23	Errores de mantenimiento / actualización de equipos(hardware)	Perjuicio a la mantenibilidad del sistema de información.	Muy baja	**2**
	E.24	Caída del sistema por agotamiento de recursos	Saturación del sistema informático.	Muy baja	**2**
	E.25	Perdida de equipos (Robo)	Recuperación de soportes reciclados o desechados.	Muy baja	**2**
ATAQUES INTENCIONADOS	**A.6**	Abuso de privilegios de acceso	Abuso de cada uno de los derechos otorgados.	Muy baja	**2**
	A.7	Uso no previsto	Implementación de recursos (económicos y de tiempo) en actividades no relacionadas.	Muy baja	**2**

Tabla 32. Estimación de la probabilidad activo servidor plataforma RYCA V.2.0. (Continuación)

	A.11	Acceso no autorizado	Uso ilícito del hardware	Muy baja	**2**
	A.23	Manipulación de los equipos	Sabotaje del hardware y software conteniente.	Muy baja	**2**
	A.24	Denegación de servicio	Saturación del sistema de información.	Muy baja	**2**
	A.25	Robo	Robo de porte de la información, puede esta ser física o digital.	Muy baja	**2**
	A.26	Ataque destructivo	Destrucción de los contenedores de la información, en recipientes físicos y lógicos.	Muy baja	**2**

Fuente: Autoría propia

Tabla 33. Estimación de la probabilidad activo servidor plataforma RYCA V.1

ACTIVO TI	SERVIDOR PLATAFORMA RYCA V.1
ADMINISTRADOR	PIMIENTO CARDENAS WILSON MAURICIO
DEGRADACIÓN	90%
IMPACTO	8
TIPO DE ACTIVO	HARDWARE

Tipo	**ID**	**Amenaza**	**Exposición/Vulnerabilidad**	**Frecuencia (F)**	
DESASTRES NATURALES	**N.1**	Fuego	No existe sistema de alarma contra incendios. Se posee un solo extintor de solkaflam (clase c) recomendados para incendios en lugares donde se encuentren equipos eléctricos.	Muy baja	**2**
	N.2	Daños por agua	La infraestructura está expuesta a goteras, cuenta con averías en el techo en donde el agua de las lluvias	Muy baja	**2**

Tabla 33. Estimación de la probabilidad activo servidor plataforma RYCA V.1. (Continuación)

	N.*	Desastres naturales	La oficina de la dependencia de sistemas se encuentra en zona baja de riesgo de desastre natural de origen volcánico debido a su cercanía con el volcán nevado del Tolima.	Raro	**1**
DE ORIGEN INDUSTRIAL	**I.1**	Fuego	No existe sistema de alarma contra incendios. Se posee un solo extintor de solkaflam (clase c) recomendados para incendios en lugares donde se encuentren equipos eléctricos.	Muy baja	**2**
	I.2	Daños por agua	La concentración del líquido sobrante por parte del aire acondicionado causaría daños en los equipos.	Muy baja	**2**
	I.*	Desastres industriales	No hay exposición o vulnerabilidad, por parte de esta amenaza.	Muy baja	**2**
	I.3	Contaminación mecánica	No hay exposición o vulnerabilidad, por parte de esta amenaza.	Muy baja	**2**
	I.4	Contaminación electromagnética	No hay exposición o vulnerabilidad, por parte de esta amenaza.	Muy baja	**2**
	I.5	Avería de origen físico o lógico	La manipulación por parte de cada uno de los componentes encontrados en la dependencia, como también por defectos de los componentes desde fabrica	Muy baja	**2**

Tabla 33. Estimación de la probabilidad activo servidor plataforma RYCA V.1. (Continuación)

	I.6	Corte del suministro eléctrico	Amenaza debida a factores externos, a clemencias de tipo naturales como lluvias u otros.	Muy baja	**2**
	I.7	Condiciones inadecuadas de temperatura o humedad	No se cuenta con una infraestructura adecuada para soportar los defectos del sistema de refrigeración.	Muy baja	**2**
	I.11	Emanaciones electromagnéticas	No hay exposición o vulnerabilidad, por parte de esta amenaza.	Muy baja	**2**
ERRORES Y FALLOS NO INTENCIONADOS	**E.2**	Errores del administrador	Pérdida total o parcial del tiempo de ejecución de sus actividades, dependiendo de la gravedad del asunto.	Muy baja	**2**
	E.23	Errores de mantenimiento / actualización de equipos(hardware)	Perjuicio a la mantenibilidad del sistema de información.	Muy baja	**2**
	E.24	Caída del sistema por agotamiento de recursos	Saturación del sistema informático.	Muy baja	**2**
	E.25	Perdida de equipos (Robo)	Recuperación de soportes reciclados o desechados.	Muy baja	**2**
ATAQUES INTENCIONADOS	**A.6**	Abuso de privilegios de acceso	Abuso de cada uno de los derechos otorgados.	Muy baja	**2**
	A.7	Uso no previsto	Implementación de recursos (económicos y de tiempo) en actividades no relacionadas.	Muy baja	**2**

Tabla 33. Estimación de la probabilidad activo servidor plataforma RYCA V.1. (Continuación)

	A.11	Acceso no autorizado	Uso ilícito del hardware	Muy baja	**2**
	A.23	Manipulación de los equipos	Sabotaje del hardware y software conteniente.	Muy baja	**2**
	A.24	Denegación de servicio	Saturación del sistema de información.	Muy baja	**2**
	A.25	Robo	Robo de porte de la información, puede esta ser física o digital.	Muy baja	**2**
	A.26	Ataque destructivo	Destrucción de los contenedores de la información, en recipientes físicos y lógicos.	Muy baja	**2**

Fuente: Autoría propia

Tabla 34. Estimación de la probabilidad activo servidor de base de datos ITFIP

ACTIVO TI	SERVIDOR DE BASE DE DATOS ITFIP
ADMINISTRADOR	PIMIENTO CARDENAS WILSON MAURICIO
DEGRADACIÓN	90%
IMPACTO	8
TIPO DE ACTIVO	HARDWARE

Tipo	**ID**	**Amenaza**	**Exposición/Vulnerabilidad**	**Frecuencia (F)**	
DESASTRES NATURALES	**N.1**	Fuego	No existe sistema de alarma contra incendios. Se posee un solo extintor de solkaflam (clase c) recomendados para incendios en lugares donde se encuentren equipos eléctricos.	Muy baja	**2**
	N.2	Daños por agua	La infraestructura está expuesta a goteras, cuenta con averías en el techo en donde el agua de las lluvias	Muy baja	**2**

Tabla 34. Estimación de la probabilidad activo servidor de base de datos ITFIP. (Continuación)

	N.*	Desastres naturales	La oficina de la dependencia de sistemas se encuentra en zona baja de riesgo de desastre natural de origen volcánico debido a su cercanía con el volcán nevado del Tolima.	Raro	**1**
DE ORIGEN INDUSTRIAL	**I.1**	Fuego	No existe sistema de alarma contra incendios. Se posee un solo extintor de solkaflam (clase c) recomendados para incendios en lugares donde se encuentren equipos eléctricos.	Muy baja	**2**
	I.2	Daños por agua	La concentración del líquido sobrante por parte del aire acondicionado causaría daños en los equipos.	Muy baja	**2**
	I.*	Desastres industriales	No hay exposición o vulnerabilidad, por parte de esta amenaza.	Muy baja	**2**
	I.3	Contaminación mecánica	No hay exposición o vulnerabilidad, por parte de esta amenaza.	Muy baja	**2**
	I.4	Contaminación electromagnética	No hay exposición o vulnerabilidad, por parte de esta amenaza.	Muy baja	**2**
	I.5	Avería de origen físico o lógico	La manipulación por parte de cada uno de los componentes encontrados en la dependencia, como también por defectos de los componentes desde fabrica	Muy baja	**2**

Tabla 34. Estimación de la probabilidad activo servidor de base de datos ITFIP. (Continuación)

	I.6	Corte del suministro eléctrico	Amenaza debida a factores externos, a clemencias de tipo naturales como lluvias u otros.	Muy baja	**2**
	I.7	Condiciones inadecuadas de temperatura o humedad	No se cuenta con una infraestructura adecuada para soportar los defectos del sistema de refrigeración.	Muy baja	**2**
	I.11	Emanaciones electromagnéticas	No hay exposición o vulnerabilidad, por parte de esta amenaza.	Muy baja	**2**
ERRORES Y FALLOS NO INTENCIONADOS	**E.2**	Errores del administrador	Pérdida total o parcial del tiempo de ejecución de sus actividades, dependiendo de la gravedad del asunto.	Muy baja	**2**
	E.23	Errores de mantenimiento / actualización de equipos(hardware)	Perjuicio a la mantenibilidad del sistema de información.	Muy baja	**2**
	E.24	Caída del sistema por agotamiento de recursos	Saturación del sistema informático.	Muy baja	**2**
	E.25	Perdida de equipos (Robo)	Recuperación de soportes reciclados o desechados.	Muy baja	**2**
ATAQUES INTENCIONADOS	**A.6**	Abuso de privilegios de acceso	Abuso de cada uno de los derechos otorgados.	Muy baja	**2**
	A.7	Uso no previsto	Implementación de recursos (económicos y de tiempo) en actividades no relacionadas.	Muy baja	**2**

Tabla 34.Estimación de la probabilidad activo servidor de base de datos ITFIP. (Continuación)

	A.11	Acceso no autorizado	Uso ilícito del hardware	Muy baja	**2**
	A.23	Manipulación de los equipos	Sabotaje del hardware y software conteniente.	Muy baja	**2**
	A.24	Denegación de servicio	Saturación del sistema de información.	Muy baja	**2**
	A.25	Robo	Robo de porte de la información, puede esta ser física o digital.	Muy baja	**2**
	A.26	Ataque destructivo	Destrucción de los contenedores de la información, en recipientes físicos y lógicos.	Muy baja	**2**

Fuente: Autoría propia

Tabla 35. Estimación de la probabilidad activo servidor *firewall* FORTIGATE

ACTIVO TI	SERVIDOR FIREWALL FORTIGATE
ADMINISTRADOR	PIMIENTO CARDENAS WILSON MAURICIO
DEGRADACIÓN	90%
IMPACTO	8
TIPO DE ACTIVO	HARDWARE

Tipo	**ID**	**Amenaza**	**Exposición/Vulnerabilidad**	**Frecuencia (F)**	
DESASTRES NATURALES	**N.1**	Fuego	No existe sistema de alarma contra incendios. Se posee un solo extintor de solkaflam (clase c) recomendados para incendios en lugares donde se encuentren equipos eléctricos.	Muy baja	**2**
	N.2	Daños por agua	La infraestructura está expuesta a goteras, cuenta con averías en el techo en donde el agua de las lluvias	Muy baja	**2**

Tabla 35. Estimación de la probabilidad activo servidor *firewall* FORTIGATE. (Continuación)

	N.*	Desastres naturales	La oficina de la dependencia de sistemas se encuentra en zona baja de riesgo de desastre natural de origen volcánico debido a su cercanía con el volcán nevado del Tolima.	Raro	**1**
DE ORIGEN INDUSTRIAL	**I.1**	Fuego	No existe sistema de alarma contra incendios. Se posee un solo extintor de solkaflam (clase c) recomendados para incendios en lugares donde se encuentren equipos eléctricos.	Muy baja	**2**
	I.2	Daños por agua	La concentración del líquido sobrante por parte del aire acondicionado causaría daños en los equipos.	Muy baja	**2**
	I.*	Desastres industriales	No hay exposición o vulnerabilidad, por parte de esta amenaza.	Muy baja	**2**
	I.3	Contaminación mecánica	No hay exposición o vulnerabilidad, por parte de esta amenaza.	Muy baja	**2**
	I.4	Contaminación electromagnética	No hay exposición o vulnerabilidad, por parte de esta amenaza.	Muy baja	**2**
	I.5	Avería de origen físico o lógico	La manipulación por parte de cada uno de los componentes encontrados en la dependencia, como también por defectos de los componentes desde fabrica	Muy baja	**2**

Tabla 35. Estimación de la probabilidad activo servidor *firewall* FORTIGATE. (Continuación)

	I.6	Corte del suministro eléctrico	Amenaza debida a factores externos, a clemencias de tipo naturales como lluvias u otros.	Muy baja	**2**
	I.7	Condiciones inadecuadas de temperatura o humedad	No se cuenta con una infraestructura adecuada para soportar los defectos del sistema de refrigeración.	Muy baja	**2**
	I.11	Emanaciones electromagnéticas	No hay exposición o vulnerabilidad, por parte de esta amenaza.	Muy baja	**2**
ERRORES Y FALLOS NO INTENCIONADOS	**E.2**	Errores del administrador	Pérdida total o parcial del tiempo de ejecución de sus actividades, dependiendo de la gravedad del asunto.	Muy baja	**2**
	E.23	Errores de mantenimiento / actualización de equipos(hardware)	Perjuicio a la mantenibilidad del sistema de información.	Muy baja	**2**
	E.24	Caída del sistema por agotamiento de recursos	Saturación del sistema informático.	Muy baja	**2**
	E.25	Perdida de equipos (Robo)	Recuperación de soportes reciclados o desechados.	Muy baja	**2**
ATAQUES INTENCIONADOS	**A.6**	Abuso de privilegios de acceso	Abuso de cada uno de los derechos otorgados.	Muy baja	**2**
	A.7	Uso no previsto	Implementación de recursos (económicos y de tiempo) en actividades no relacionadas.	Muy baja	**2**

Tabla 35. Estimación de la probabilidad activo servidor *firewall* FORTIGATE. (Continuación)

	A.11	Acceso no autorizado	Uso ilícito del hardware	Muy baja	**2**
	A.23	Manipulación de los equipos	Sabotaje del hardware y software conteniente.	Muy baja	**2**
	A.24	Denegación de servicio	Saturación del sistema de información.	Muy baja	**2**
	A.25	Robo	Robo de porte de la información, puede esta ser física o digital.	Muy baja	**2**
	A.26	Ataque destructivo	Destrucción de los contenedores de la información, en recipientes físicos y lógicos.	Muy baja	**2**

Fuente: Autoría propia

Tabla 36. Estimación de la probabilidad activo servidor contable SIIGO

ACTIVO TI	SERVIDOR CONTABLE SIIGO
ADMINISTRADOR	PIMIENTO CARDENAS WILSON MAURICIO
DEGRADACIÓN	90%
IMPACTO	8
TIPO DE ACTIVO	HARDWARE

Tipo	**ID**	**Amenaza**	**Exposición/Vulnerabilidad**	**Frecuencia (F)**	
DESASTRES NATURALES	**N.1**	Fuego	No existe sistema de alarma contra incendios. Se posee un solo extintor de solkaflam (clase c) recomendados para incendios en lugares donde se encuentren equipos eléctricos.	Muy baja	**2**
	N.2	Daños por agua	La infraestructura está expuesta a goteras, cuenta con averías en el techo en donde el agua de las lluvias	Muy baja	**2**

Tabla 36. Estimación de la probabilidad activo servidor contable SIIGO. (Continuación)

	N.*	Desastres naturales	La oficina de la dependencia de sistemas se encuentra en zona baja de riesgo de desastre natural de origen volcánico debido a su cercanía con el volcán nevado del Tolima.	Raro	**1**
DE ORIGEN INDUSTRIAL	**I.1**	Fuego	No existe sistema de alarma contra incendios. Se posee un solo extintor de solkaflam (clase c) recomendados para incendios en lugares donde se encuentren equipos eléctricos.	Muy baja	**2**
	I.2	Daños por agua	La concentración del líquido sobrante por parte del aire acondicionado causaría daños en los equipos.	Muy baja	**2**
	I.*	Desastres industriales	No hay exposición o vulnerabilidad, por parte de esta amenaza.	Muy baja	**2**
	I.3	Contaminación mecánica	No hay exposición o vulnerabilidad, por parte de esta amenaza.	Muy baja	**2**
	I.4	Contaminación electromagnética	No hay exposición o vulnerabilidad, por parte de esta amenaza.	Muy baja	**2**
	I.5	Avería de origen físico o lógico	La manipulación por parte de cada uno de los componentes encontrados en la dependencia, como también por defectos de los componentes desde fabrica	Muy baja	**2**

Tabla 36. Estimación de la probabilidad activo servidor contable SIIGO. (Continuación)

	I.6	Corte del suministro eléctrico	Amenaza debida a factores externos, a clemencias de tipo naturales como lluvias u otros.	Muy baja	**2**
	I.7	Condiciones inadecuadas de temperatura o humedad	No se cuenta con una infraestructura adecuada para soportar los defectos del sistema de refrigeración.	Muy baja	**2**
	I.11	Emanaciones electromagnéticas	No hay exposición o vulnerabilidad, por parte de esta amenaza.	Muy baja	**2**
ERRORES Y FALLOS NO INTENCIONADOS	**E.2**	Errores del administrador	Pérdida total o parcial del tiempo de ejecución de sus actividades, dependiendo de la gravedad del asunto.	Muy baja	**2**
	E.23	Errores de mantenimiento / actualización de equipos(hardware)	Perjuicio a la mantenibilidad del sistema de información.	Muy baja	**2**
	E.24	Caída del sistema por agotamiento de recursos	Saturación del sistema informático.	Muy baja	**2**
	E.25	Perdida de equipos (Robo)	Recuperación de soportes reciclados o desechados.	Muy baja	**2**
ATAQUES INTENCIONADOS	**A.6**	Abuso de privilegios de acceso	Abuso de cada uno de los derechos otorgados.	Muy baja	**2**
	A.7	Uso no previsto	Implementación de recursos (económicos y de tiempo) en actividades no relacionadas.	Muy baja	**2**

Tabla 36. Estimación de la probabilidad activo servidor contable SIIGO. (Continuación)

	A.11	Acceso no autorizado	Uso ilícito del hardware	Muy baja	**2**
	A.23	Manipulación de los equipos	Sabotaje del hardware y software conteniente.	Muy baja	**2**
	A.24	Denegación de servicio	Saturación del sistema de información.	Muy baja	**2**
	A.25	Robo	Robo de porte de la información, puede esta ser física o digital.	Muy baja	**2**
	A.26	Ataque destructivo	Destrucción de los contenedores de la información, en recipientes físicos y lógicos.	Muy baja	**2**

Fuente: Autoría propia

Tabla 37. Estimación de la probabilidad activo servidor de pruebas “desarrollito”

ACTIVO TI	SERVIDOR DE PRUEBAS “DESARROLLITO”
ADMINISTRADOR	PIMIENTO CARDENAS WILSON MAURICIO
DEGRADACIÓN	45%
IMPACTO	3
TIPO DE ACTIVO	HARDWARE

Tipo	**ID**	**Amenaza**	**Exposición/Vulnerabilidad**	**Frecuencia (F)**	
DESASTRES NATURALES	**N.1**	Fuego	No existe sistema de alarma contra incendios. Se posee un solo extintor de solkaflam (clase c) recomendados para incendios en lugares donde se encuentren equipos eléctricos.	Muy baja	**2**
	N.2	Daños por agua	La infraestructura está expuesta a goteras, cuenta con averías en el techo en donde el agua de las lluvias	Muy baja	**2**

Tabla 37. Estimación de la probabilidad activo servidor de pruebas “desarrollito”. (Continuación)

	N.*	Desastres naturales	La oficina de la dependencia de sistemas se encuentra en zona baja de riesgo de desastre natural de origen volcánico debido a su cercanía con el volcán nevado del Tolima.	Raro	**1**
DE ORIGEN INDUSTRIAL	**I.1**	Fuego	No existe sistema de alarma contra incendios. Se posee un solo extintor de solkaflam (clase c) recomendados para incendios en lugares donde se encuentren equipos eléctricos.	Muy baja	**2**
	I.2	Daños por agua	La concentración del líquido sobrante por parte del aire acondicionado causaría daños en los equipos.	Muy baja	**2**
	I.*	Desastres industriales	No hay exposición o vulnerabilidad, por parte de esta amenaza.	Muy baja	**2**
	I.3	Contaminación mecánica	No hay exposición o vulnerabilidad, por parte de esta amenaza.	Muy baja	**2**
	I.4	Contaminación electromagnética	No hay exposición o vulnerabilidad, por parte de esta amenaza.	Muy baja	**2**
	I.5	Avería de origen físico o lógico	La manipulación por parte de cada uno de los componentes encontrados en la dependencia, como también por defectos de los componentes desde fabrica	Muy baja	**2**

Tabla 37. Estimación de la probabilidad activo servidor de pruebas “desarrollito”. (Continuación)

	I.6	Corte del suministro eléctrico	Amenaza debida a factores externos, a clemencias de tipo naturales como lluvias u otros.	Muy baja	**2**
	I.7	Condiciones inadecuadas de temperatura o humedad	No se cuenta con una infraestructura adecuada para soportar los defectos del sistema de refrigeración.	Muy baja	**2**
	I.11	Emanaciones electromagnéticas	No hay exposición o vulnerabilidad, por parte de esta amenaza.	Muy baja	**2**
ERRORES Y FALLOS NO INTENCIONADOS	**E.2**	Errores del administrador	Pérdida total o parcial del tiempo de ejecución de sus actividades, dependiendo de la gravedad del asunto.	Muy baja	**2**
	E.23	Errores de mantenimiento / actualización de equipos(hardware)	Perjuicio a la mantenibilidad del sistema de información.	Muy baja	**2**
	E.24	Caída del sistema por agotamiento de recursos	Saturación del sistema informático.	Muy baja	**2**
	E.25	Perdida de equipos (Robo)	Recuperación de soportes reciclados o desechados.	Muy baja	**2**
ATAQUES INTENCIONADOS	**A.6**	Abuso de privilegios de acceso	Abuso de cada uno de los derechos otorgados.	Muy baja	**2**
	A.7	Uso no previsto	Implementación de recursos (económicos y de tiempo) en actividades no relacionadas.	Muy baja	**2**

Tabla 37. Estimación de la probabilidad activo servidor de pruebas “desarrollito”. (Continuación)

	A.11	Acceso no autorizado	Uso ilícito del hardware	Muy baja	**2**
	A.23	Manipulación de los equipos	Sabotaje del hardware y software conteniente.	Muy baja	**2**
	A.24	Denegación de servicio	Saturación del sistema de información.	Muy baja	**2**
	A.25	Robo	Robo de porte de la información, puede esta ser física o digital.	Muy baja	**2**
	A.26	Ataque destructivo	Destrucción de los contenedores de la información, en recipientes físicos y lógicos.	Muy baja	**2**

Fuente: Autoría propia

Tabla 38. Estimación de la probabilidad activo servidor de copias de seguridad de la información del ITFIP

ACTIVO TI	SERVIDOR DE COPIAS DE SEGURIDAD DE LA INFORMACIÓN DEL ITFIP
ADMINISTRADOR	PIMIENTO CARDENAS WILSON MAURICIO
DEGRADACIÓN	90%
IMPACTO	8
TIPO DE ACTIVO	HARDWARE

Tipo	**ID**	**Amenaza**	**Exposición/Vulnerabilidad**	**Frecuencia (F)**	
DESASTRES NATURALES	**N.1**	Fuego	No existe sistema de alarma contra incendios. Se posee un solo extintor de solkaflam (clase c) recomendados para incendios en lugares donde se encuentren equipos eléctricos.	Muy baja	**2**
	N.2	Daños por agua	La infraestructura está expuesta a goteras, cuenta con averías en el techo en donde el agua de las lluvias	Muy baja	**2**

Tabla 38. Estimación de la probabilidad activo servidor *backup* de información del ITFIP. Continuación)

	N.*	Desastres naturales	La oficina de la dependencia de sistemas se encuentra en zona baja de riesgo de desastre natural de origen volcánico debido a su cercanía con el volcán nevado del Tolima.	Raro	**1**
DE ORIGEN INDUSTRIAL	**I.1**	Fuego	No existe sistema de alarma contra incendios. Se posee un solo extintor de solkaflam (clase c) recomendados para incendios en lugares donde se encuentren equipos eléctricos.	Muy baja	**2**
	I.2	Daños por agua	La concentración del líquido sobrante por parte del aire acondicionado causaría daños en los equipos.	Muy baja	**2**
	I.*	Desastres industriales	No hay exposición o vulnerabilidad, por parte de esta amenaza.	Muy baja	**2**
	I.3	Contaminación mecánica	No hay exposición o vulnerabilidad, por parte de esta amenaza.	Muy baja	**2**
	I.4	Contaminación electromagnética	No hay exposición o vulnerabilidad, por parte de esta amenaza.	Muy baja	**2**
	I.5	Avería de origen físico o lógico	La manipulación por parte de cada uno de los componentes encontrados en la dependencia, como también por defectos de los componentes desde fabrica	Muy baja	**2**

Tabla 38. Estimación de la probabilidad activo servidor *backup* de información del ITFIP. Continuación)

	I.6	Corte del suministro eléctrico	Amenaza debida a factores externos, a clemencias de tipo naturales como lluvias u otros.	Muy baja	**2**
	I.7	Condiciones inadecuadas de temperatura o humedad	No se cuenta con una infraestructura adecuada para soportar los defectos del sistema de refrigeración.	Muy baja	**2**
	I.11	Emanaciones electromagnéticas	No hay exposición o vulnerabilidad, por parte de esta amenaza.	Muy baja	**2**
ERRORES Y FALLOS NO INTENCIONADOS	**E.2**	Errores del administrador	Pérdida total o parcial del tiempo de ejecución de sus actividades, dependiendo de la gravedad del asunto.	Muy baja	**2**
	E.23	Errores de mantenimiento / actualización de equipos(hardware)	Perjuicio a la mantenibilidad del sistema de información.	Muy baja	**2**
	E.24	Caída del sistema por agotamiento de recursos	Saturación del sistema informático.	Muy baja	**2**
	E.25	Perdida de equipos (Robo)	Recuperación de soportes reciclados o desechados.	Muy baja	**2**
ATAQUES INTENCIONADOS	**A.6**	Abuso de privilegios de acceso	Abuso de cada uno de los derechos otorgados.	Muy baja	**2**
	A.7	Uso no previsto	Implementación de recursos (económicos y de tiempo) en actividades no relacionadas.	Muy baja	**2**

Tabla 38. Estimación de la probabilidad activo servidor *backup* de información del ITFIP. Continuación)

	A.11	Acceso no autorizado	Uso ilícito del hardware	Muy baja	**2**
	A.23	Manipulación de los equipos	Sabotaje del hardware y software conteniente.	Muy baja	**2**
	A.24	Denegación de servicio	Saturación del sistema de información.	Muy baja	**2**
	A.25	Robo	Robo de porte de la información, puede esta ser física o digital.	Muy baja	**2**
	A.26	Ataque destructivo	Destrucción de los contenedores de la información, en recipientes físicos y lógicos.	Muy baja	**2**

Fuente: Autoría propia

Tabla 39. Estimación de la probabilidad activo computador iMac Apple (3 equipos)

ACTIVO TI	COMPUTADOR IMAC APPLE (3 EQUIPOS)
ADMINISTRADOR	PIMIENTO CARDENAS WILSON MAURICIO
DEGRADACIÓN	50%
IMPACTO	5
TIPO DE ACTIVO	HARDWARE

Tipo	**ID**	**Amenaza**	**Exposición/Vulnerabilidad**	**Frecuencia (F)**	
DESASTRES NATURALES	**N.1**	Fuego	No existe sistema de alarma contra incendios. Se posee un solo extintor de solkaflam (clase c) recomendados para incendios en lugares donde se encuentren equipos eléctricos.	Muy baja	**2**
	N.2	Daños por agua	La infraestructura está expuesta a goteras, cuenta con averías en el techo en donde el agua de las lluvias	Muy baja	**2**

Tabla 39. Estimación de la probabilidad activo computador iMac Apple (3 equipos). (Continuación)

	N.*	Desastres naturales	La oficina de la dependencia de sistemas se encuentra en zona baja de riesgo de desastre natural de origen volcánico debido a su cercanía con el volcán nevado del Tolima.	Raro	**1**
DE ORIGEN INDUSTRIAL	**I.1**	Fuego	No existe sistema de alarma contra incendios. Se posee un solo extintor de solkaflam (clase c) recomendados para incendios en lugares donde se encuentren equipos eléctricos.	Muy baja	**2**
	I.2	Daños por agua	La concentración del líquido sobrante por parte del aire acondicionado causaría daños en los equipos.	Muy baja	**2**
	I.*	Desastres industriales	No hay exposición o vulnerabilidad, por parte de esta amenaza.	Muy baja	**2**
	I.3	Contaminación mecánica	No hay exposición o vulnerabilidad, por parte de esta amenaza.	Muy baja	**2**
	I.4	Contaminación electromagnética	No hay exposición o vulnerabilidad, por parte de esta amenaza.	Muy baja	**2**
	I.5	Avería de origen físico o lógico	La manipulación por parte de cada uno de los componentes encontrados en la dependencia, como también por defectos de los componentes desde fabrica	Muy baja	**2**

Tabla 39. Estimación de la probabilidad activo computador iMac Apple (3 equipos). (Continuación)

	I.6	Corte del suministro eléctrico	Amenaza debida a factores externos, a clemencias de tipo naturales como lluvias u otros.	Muy baja	**2**
	I.7	Condiciones inadecuadas de temperatura o humedad	No se cuenta con una infraestructura adecuada para soportar los defectos del sistema de refrigeración.	Muy baja	**2**
	I.11	Emanaciones electromagnéticas	No hay exposición o vulnerabilidad, por parte de esta amenaza.	Muy baja	**2**
ERRORES Y FALLOS NO INTENCIONADOS	**E.2**	Errores del administrador	Pérdida total o parcial del tiempo de ejecución de sus actividades, dependiendo de la gravedad del asunto.	Muy baja	**2**
	E.23	Errores de mantenimiento / actualización de equipos(hardware)	Perjuicio a la mantenibilidad del sistema de información.	Muy baja	**2**
	E.24	Caída del sistema por agotamiento de recursos	Saturación del sistema informático.	Muy baja	**2**
	E.25	Perdida de equipos (Robo)	Recuperación de soportes reciclados o desechados.	Muy baja	**2**
ATAQUES INTENCIONADOS	**A.6**	Abuso de privilegios de acceso	Abuso de cada uno de los derechos otorgados.	Muy baja	**2**
	A.7	Uso no previsto	Implementación de recursos (económicos y de tiempo) en actividades no relacionadas.	Muy baja	**2**

Tabla 39. Estimación de la probabilidad activo computador iMac Apple (3 equipos). (Continuación)

	A.11	Acceso no autorizado	Uso ilícito del hardware	Muy baja	**2**
	A.23	Manipulación de los equipos	Sabotaje del hardware y software conteniente.	Muy baja	**2**
	A.24	Denegación de servicio	Saturación del sistema de información.	Muy baja	**2**
	A.25	Robo	Robo de porte de la información, puede esta ser física o digital.	Muy baja	**2**
	A.26	Ataque destructivo	Destrucción de los contenedores de la información, en recipientes físicos y lógicos.	Muy baja	**2**

Fuente: Autoría propia

Tabla 40. Estimación de la probabilidad activo computadores hp all-one pro (18 equipos)

ACTIVO TI	COMPUTADORES HP ALL-ONE PRO (18 EQUIPOS)
ADMINISTRADOR	PIMIENTO CARDENAS WILSON MAURICIO
DEGRADACIÓN	30%
IMPACTO	3
TIPO DE ACTIVO	HARDWARE

Tipo	**ID**	**Amenaza**	**Exposición/Vulnerabilidad**	**Frecuencia (F)**	
DESASTRES NATURALES	**N.1**	Fuego	No existe sistema de alarma contra incendios. Se posee un solo extintor de solkaflam (clase c) recomendados para incendios en lugares donde se encuentren equipos eléctricos.	Muy baja	**2**
	N.2	Daños por agua	La infraestructura está expuesta a goteras, cuenta con averías en el techo en donde el agua de las lluvias	Muy baja	**2**

Tabla 40. Estimación de la probabilidad activo computadores hp all-one pro (18 equipos). (Continuación)

	N.*	Desastres naturales	La oficina de la dependencia de sistemas se encuentra en zona baja de riesgo de desastre natural de origen volcánico debido a su cercanía con el volcán nevado del Tolima.	Raro	**1**
DE ORIGEN INDUSTRIAL	**I.1**	Fuego	No existe sistema de alarma contra incendios. Se posee un solo extintor de solkaflam (clase c) recomendados para incendios en lugares donde se encuentren equipos eléctricos.	Muy baja	**2**
	I.2	Daños por agua	La concentración del líquido sobrante por parte del aire acondicionado causaría daños en los equipos.	Muy baja	**2**
	I.*	Desastres industriales	No hay exposición o vulnerabilidad, por parte de esta amenaza.	Muy baja	**2**
	I.3	Contaminación mecánica	No hay exposición o vulnerabilidad, por parte de esta amenaza.	Muy baja	**2**
	I.4	Contaminación electromagnética	No hay exposición o vulnerabilidad, por parte de esta amenaza.	Muy baja	**2**
	I.5	Avería de origen físico o lógico	La manipulación por parte de cada uno de los componentes encontrados en la dependencia, como también por defectos de los componentes desde fabrica	Muy baja	**2**

Tabla 40. Estimación de la probabilidad activo computadores hp all-one pro (18 equipos). (Continuación)

	I.6	Corte del suministro eléctrico	Amenaza debida a factores externos, a clemencias de tipo naturales como lluvias u otros.	Muy baja	**2**
	I.7	Condiciones inadecuadas de temperatura o humedad	No se cuenta con una infraestructura adecuada para soportar los defectos del sistema de refrigeración.	Muy baja	**2**
	I.11	Emanaciones electromagnéticas	No hay exposición o vulnerabilidad, por parte de esta amenaza.	Muy baja	**2**
ERRORES Y FALLOS NO INTENCIONADOS	**E.2**	Errores del administrador	Pérdida total o parcial del tiempo de ejecución de sus actividades, dependiendo de la gravedad del asunto.	Muy baja	**2**
	E.23	Errores de mantenimiento / actualización de equipos(hardware)	Perjuicio a la mantenibilidad del sistema de información.	Muy baja	**2**
	E.24	Caída del sistema por agotamiento de recursos	Saturación del sistema informático.	Muy baja	**2**
	E.25	Perdida de equipos (Robo)	Recuperación de soportes reciclados o desechados.	Muy baja	**2**
ATAQUES INTENCIONADOS	**A.6**	Abuso de privilegios de acceso	Abuso de cada uno de los derechos otorgados.	Muy baja	**2**
	A.7	Uso no previsto	Implementación de recursos (económicos y de tiempo) en actividades no relacionadas.	Muy baja	**2**

Tabla 40. Estimación de la probabilidad activo computadores hp all-one pro (18 equipos). (Continuación)

	A.11	Acceso no autorizado	Uso ilícito del hardware	Muy baja	**2**
	A.23	Manipulación de los equipos	Sabotaje del hardware y software conteniente.	Muy baja	**2**
	A.24	Denegación de servicio	Saturación del sistema de información.	Muy baja	**2**
	A.25	Robo	Robo de porte de la información, puede esta ser física o digital.	Muy baja	**2**
	A.26	Ataque destructivo	Destrucción de los contenedores de la información, en recipientes físicos y lógicos.	Muy baja	**2**

Fuente: Autoría propia

Tabla 41. Estimación de la probabilidad activo portátil Toshiba (16 equipos)

ACTIVO TI	PORTÁTIL TOSHIBA (16 EQUIPOS)
ADMINISTRADOR	PIMIENTO CARDENAS WILSON MAURICIO
DEGRADACIÓN	30%
IMPACTO	3
TIPO DE ACTIVO	HARDWARE

Tipo	**ID**	**Amenaza**	**Exposición/Vulnerabilidad**	**Frecuencia (F)**	
DESASTRES NATURALES	**N.1**	Fuego	No existe sistema de alarma contra incendios. Se posee un solo extintor de solkaflam (clase c) recomendados para incendios en lugares donde se encuentren equipos eléctricos.	Muy baja	**2**
	N.2	Daños por agua	La infraestructura está expuesta a goteras, cuenta con averías en el techo en donde el agua de las lluvias	Muy baja	**2**

Tabla 41. Estimación de la probabilidad activo portátil Toshiba (16 equipos). (Continuación)

	N.*	Desastres naturales	La oficina de la dependencia de sistemas se encuentra en zona baja de riesgo de desastre natural de origen volcánico debido a su cercanía con el volcán nevado del Tolima.	Raro	**1**
DE ORIGEN INDUSTRIAL	**I.1**	Fuego	No existe sistema de alarma contra incendios. Se posee un solo extintor de solkaflam (clase c) recomendados para incendios en lugares donde se encuentren equipos eléctricos.	Muy baja	**2**
	I.2	Daños por agua	La concentración del líquido sobrante por parte del aire acondicionado causaría daños en los equipos.	Muy baja	**2**
	I.*	Desastres industriales	No hay exposición o vulnerabilidad, por parte de esta amenaza.	Muy baja	**2**
	I.3	Contaminación mecánica	No hay exposición o vulnerabilidad, por parte de esta amenaza.	Muy baja	**2**
	I.4	Contaminación electromagnética	No hay exposición o vulnerabilidad, por parte de esta amenaza.	Muy baja	**2**
	I.5	Avería de origen físico o lógico	La manipulación por parte de cada uno de los componentes encontrados en la dependencia, como también por defectos de los componentes desde fabrica	Muy baja	**2**

Tabla 41. Estimación de la probabilidad activo portátil Toshiba (16 equipos). (Continuación)

	I.6	Corte del suministro eléctrico	Amenaza debida a factores externos, a clemencias de tipo naturales como lluvias u otros.	Muy baja	**2**
	I.7	Condiciones inadecuadas de temperatura o humedad	No se cuenta con una infraestructura adecuada para soportar los defectos del sistema de refrigeración.	Muy baja	**2**
	I.11	Emanaciones electromagnéticas	No hay exposición o vulnerabilidad, por parte de esta amenaza.	Muy baja	**2**
ERRORES Y FALLOS NO INTENCIONADOS	**E.2**	Errores del administrador	Pérdida total o parcial del tiempo de ejecución de sus actividades, dependiendo de la gravedad del asunto.	Muy baja	**2**
	E.23	Errores de mantenimiento / actualización de equipos(hardware)	Perjuicio a la mantenibilidad del sistema de información.	Muy baja	**2**
	E.24	Caída del sistema por agotamiento de recursos	Saturación del sistema informático.	Muy baja	**2**
	E.25	Perdida de equipos (Robo)	Recuperación de soportes reciclados o desechados.	Muy baja	**2**
ATAQUES INTENCIONADOS	**A.6**	Abuso de privilegios de acceso	Abuso de cada uno de los derechos otorgados.	Muy baja	**2**
	A.7	Uso no previsto	Implementación de recursos (económicos y de tiempo) en actividades no relacionadas.	Muy baja	**2**

Tabla 41. Estimación de la probabilidad activo portátil Toshiba (16 equipos). (Continuación)

	A.11	Acceso no autorizado	Uso ilícito del hardware	Muy baja	**2**
	A.23	Manipulación de los equipos	Sabotaje del hardware y software conteniente.	Muy baja	**2**
	A.24	Denegación de servicio	Saturación del sistema de información.	Muy baja	**2**
	A.25	Robo	Robo de porte de la información, puede esta ser física o digital.	Muy baja	**2**
	A.26	Ataque destructivo	Destrucción de los contenedores de la información, en recipientes físicos y lógicos.	Muy baja	**2**

Fuente: Autoría propia

Tabla 42. Estimación de la probabilidad activo Tablet negra 9" (1 equipo)

ACTIVO TI	TABLET NEGRA 9" (1 EQUIPO)
ADMINISTRADOR	PIMIENTO CARDENAS WILSON MAURICIO
DEGRADACIÓN	20%
IMPACTO	2
TIPO DE ACTIVO	HARDWARE

Tipo	**ID**	**Amenaza**	**Exposición/Vulnerabilidad**	**Frecuencia (F)**	
DESASTRES NATURALES	**N.1**	Fuego	No existe sistema de alarma contra incendios. Se posee un solo extintor de solkaflam (clase c) recomendados para incendios en lugares donde se encuentren equipos eléctricos.	Muy baja	**2**
	N.2	Daños por agua	La infraestructura está expuesta a goteras, cuenta con averías en el techo en donde el agua de las lluvias	Muy baja	**2**

Tabla 42. Estimación de la probabilidad activo Tablet negra 9” (1 equipo). (Continuación)

	N.*	Desastres naturales	La oficina de la dependencia de sistemas se encuentra en zona baja de riesgo de desastre natural de origen volcánico debido a su cercanía con el volcán nevado del Tolima.	Raro	**1**
DE ORIGEN INDUSTRIAL	**I.1**	Fuego	No existe sistema de alarma contra incendios. Se posee un solo extintor de solkaflam (clase c) recomendados para incendios en lugares donde se encuentren equipos eléctricos.	Muy baja	**2**
	I.2	Daños por agua	La concentración del líquido sobrante por parte del aire acondicionado causaría daños en los equipos.	Muy baja	**2**
	I.*	Desastres industriales	No hay exposición o vulnerabilidad, por parte de esta amenaza.	Muy baja	**2**
	I.3	Contaminación mecánica	No hay exposición o vulnerabilidad, por parte de esta amenaza.	Muy baja	**2**
	I.4	Contaminación electromagnética	No hay exposición o vulnerabilidad, por parte de esta amenaza.	Muy baja	**2**
	I.5	Avería de origen físico o lógico	La manipulación por parte de cada uno de los componentes encontrados en la dependencia, como también por defectos de los componentes desde fabrica	Muy baja	**2**

Tabla 42. Estimación de la probabilidad activo Tablet negra 9" (1 equipo). (Continuación)

	I.6	Corte del suministro eléctrico	Amenaza debida a factores externos, a clemencias de tipo naturales como lluvias u otros.	Muy baja	**2**
	I.7	Condiciones inadecuadas de temperatura o humedad	No se cuenta con una infraestructura adecuada para soportar los defectos del sistema de refrigeración.	Muy baja	**2**
	I.11	Emanaciones electromagnéticas	No hay exposición o vulnerabilidad, por parte de esta amenaza.	Muy baja	**2**
ERRORES Y FALLOS NO INTENCIONADOS	**E.2**	Errores del administrador	Pérdida total o parcial del tiempo de ejecución de sus actividades, dependiendo de la gravedad del asunto.	Muy baja	**2**
	E.23	Errores de mantenimiento / actualización de equipos(hardware)	Perjuicio a la mantenibilidad del sistema de información.	Muy baja	**2**
	E.24	Caída del sistema por agotamiento de recursos	Saturación del sistema informático.	Muy baja	**2**
	E.25	Perdida de equipos (Robo)	Recuperación de soportes reciclados o desechados.	Muy baja	**2**
ATAQUES INTENCIONADOS	**A.6**	Abuso de privilegios de acceso	Abuso de cada uno de los derechos otorgados.	Muy baja	**2**
	A.7	Uso no previsto	Implementación de recursos (económicos y de tiempo) en actividades no relacionadas.	Muy baja	**2**

Tabla 42. Estimación de la probabilidad activo Tablet negra 9" (1 equipo). (Continuación)

	A.11	Acceso no autorizado	Uso ilícito del hardware	Muy baja	**2**
	A.23	Manipulación de los equipos	Sabotaje del hardware y software conteniente.	Muy baja	**2**
	A.24	Denegación de servicio	Saturación del sistema de información.	Muy baja	**2**
	A.25	Robo	Robo de porte de la información, puede esta ser física o digital.	Muy baja	**2**
	A.26	Ataque destructivo	Destrucción de los contenedores de la información, en recipientes físicos y lógicos.	Muy baja	**2**

Fuente: Autoría propia

Tabla 43. Estimación de la probabilidad activo computador iMac Apple (3 equipos)

ACTIVO TI	COMPUTADOR IMAC APPLE (3 EQUIPOS)				
ADMINISTRADOR	PIMIENTO CARDENAS WILSON MAURICIO				
DEGRADACIÓN	50%				
IMPACTO	5				
TIPO DE ACTIVO	HARDWARE				
Tipo	**ID**	**Amenaza**	**Exposición/Vulnerabilidad**	**Frecuencia (F)**	
DESASTRES NATURALES	**N.1**	Fuego	No existe sistema de alarma contra incendios. Se posee un solo extintor de solkaflam (clase c) recomendados para incendios en lugares donde se encuentren equipos eléctricos.	Muy baja	**2**
	N.2	Daños por agua	La infraestructura está expuesta a goteras, cuenta con averías en el techo en donde el agua de las lluvias	Muy baja	**2**

Tabla 43. Estimación de la probabilidad activo computador iMac Apple (3 equipos). (Continuación)

	N.*	Desastres naturales	La oficina de la dependencia de sistemas se encuentra en zona baja de riesgo de desastre natural de origen volcánico debido a su cercanía con el volcán nevado del Tolima.	Raro	**1**
DE ORIGEN INDUSTRIAL	**I.1**	Fuego	No existe sistema de alarma contra incendios. Se posee un solo extintor de solkaflam (clase c) recomendados para incendios en lugares donde se encuentren equipos eléctricos.	Muy baja	**2**
	I.2	Daños por agua	La concentración del líquido sobrante por parte del aire acondicionado causaría daños en los equipos.	Muy baja	**2**
	I.*	Desastres industriales	No hay exposición o vulnerabilidad, por parte de esta amenaza.	Muy baja	**2**
	I.3	Contaminación mecánica	No hay exposición o vulnerabilidad, por parte de esta amenaza.	Muy baja	**2**
	I.4	Contaminación electromagnética	No hay exposición o vulnerabilidad, por parte de esta amenaza.	Muy baja	**2**
	I.5	Avería de origen físico o lógico	La manipulación por parte de cada uno de los componentes encontrados en la dependencia, como también por defectos de los componentes desde fabrica	Muy baja	**2**

Tabla 43. Estimación de la probabilidad activo computador iMac Apple (3 equipos). (Continuación)

	I.6	Corte del suministro eléctrico	Amenaza debida a factores externos, a clemencias de tipo naturales como lluvias u otros.	Muy baja	**2**
	I.7	Condiciones inadecuadas de temperatura o humedad	No se cuenta con una infraestructura adecuada para soportar los defectos del sistema de refrigeración.	Muy baja	**2**
	I.11	Emanaciones electromagnéticas	No hay exposición o vulnerabilidad, por parte de esta amenaza.	Muy baja	**2**
ERRORES Y FALLOS NO INTENCIONADOS	**E.2**	Errores del administrador	Pérdida total o parcial del tiempo de ejecución de sus actividades, dependiendo de la gravedad del asunto.	Muy baja	**2**
	E.23	Errores de mantenimiento / actualización de equipos(hardware)	Perjuicio a la mantenibilidad del sistema de información.	Muy baja	**2**
	E.24	Caída del sistema por agotamiento de recursos	Saturación del sistema informático.	Muy baja	**2**
	E.25	Perdida de equipos (Robo)	Recuperación de soportes reciclados o desechados.	Muy baja	**2**
ATAQUES INTENCIONADOS	**A.6**	Abuso de privilegios de acceso	Abuso de cada uno de los derechos otorgados.	Muy baja	**2**
	A.7	Uso no previsto	Implementación de recursos (económicos y de tiempo) en actividades no relacionadas.	Muy baja	**2**

Tabla 43. Estimación de la probabilidad activo computador iMac Apple (3 equipos). (Continuación)

	A.11	Acceso no autorizado	Uso ilícito del hardware	Muy baja	**2**
	A.23	Manipulación de los equipos	Sabotaje del hardware y software conteniente.	Muy baja	**2**
	A.24	Denegación de servicio	Saturación del sistema de información.	Muy baja	**2**
	A.25	Robo	Robo de porte de la información, puede esta ser física o digital.	Muy baja	**2**
	A.26	Ataque destructivo	Destrucción de los contenedores de la información, en recipientes físicos y lógicos.	Muy baja	**2**

Fuente: Autoría propia

Tabla 44. Estimación de la probabilidad activo memoria USB

ACTIVO TI	MEMORIA USB
ADMINISTRADOR	PIMIENTO CARDENAS WILSON MAURICIO
DEGRADACIÓN	20%
IMPACTO	2
TIPO DE ACTIVO	HARDWARE

Tipo	**ID**	**Amenaza**	**Exposición/Vulnerabilidad**	**Frecuencia (F)**	
DESASTRES NATURALES	**N.1**	Fuego	No existe sistema de alarma contra incendios. Se posee un solo extintor de solkaflam (clase c) recomendados para incendios en lugares donde se encuentren equipos eléctricos.	Muy baja	**2**
	N.2	Daños por agua	La infraestructura está expuesta a goteras, cuenta con averías en el techo en donde el agua de las lluvias	Muy baja	**2**

Tabla 44. Estimación de la probabilidad activo memoria USB. (Continuación)

	N.*	Desastres naturales	La oficina de la dependencia de sistemas se encuentra en zona baja de riesgo de desastre natural de origen volcánico debido a su cercanía con el volcán nevado del Tolima.	Raro	**1**
DE ORIGEN INDUSTRIAL	**I.1**	Fuego	No existe sistema de alarma contra incendios. Se posee un solo extintor de solkaflam (clase c) recomendados para incendios en lugares donde se encuentren equipos eléctricos.	Muy baja	**2**
	I.2	Daños por agua	La concentración del líquido sobrante por parte del aire acondicionado causaría daños en los equipos.	Muy baja	**2**
	I.*	Desastres industriales	No hay exposición o vulnerabilidad, por parte de esta amenaza.	Muy baja	**2**
	I.3	Contaminación mecánica	No hay exposición o vulnerabilidad, por parte de esta amenaza.	Muy baja	**2**
	I.4	Contaminación electromagnética	No hay exposición o vulnerabilidad, por parte de esta amenaza.	Muy baja	**2**
	I.5	Avería de origen físico o lógico	La manipulación por parte de cada uno de los componentes encontrados en la dependencia, como también por defectos de los componentes desde fabrica	Muy baja	**2**

Tabla 44. Estimación de la probabilidad activo memoria USB. (Continuación)

	I.6	Corte del suministro eléctrico	Amenaza debida a factores externos, a clemencias de tipo naturales como lluvias u otros.	Muy baja	**2**
	I.7	Condiciones inadecuadas de temperatura o humedad	No se cuenta con una infraestructura adecuada para soportar los defectos del sistema de refrigeración.	Muy baja	**2**
	I.11	Emanaciones electromagnéticas	No hay exposición o vulnerabilidad, por parte de esta amenaza.	Muy baja	**2**
ERRORES Y FALLOS NO INTENCIONADOS	**E.2**	Errores del administrador	Pérdida total o parcial del tiempo de ejecución de sus actividades, dependiendo de la gravedad del asunto.	Muy baja	**2**
	E.23	Errores de mantenimiento / actualización de equipos(hardware)	Perjuicio a la mantenibilidad del sistema de información.	Muy baja	**2**
	E.24	Caída del sistema por agotamiento de recursos	Saturación del sistema informático.	Muy baja	**2**
	E.25	Perdida de equipos (Robo)	Recuperación de soportes reciclados o desechados.	Muy baja	**2**
ATAQUES INTENCIONADOS	**A.6**	Abuso de privilegios de acceso	Abuso de cada uno de los derechos otorgados.	Muy baja	**2**
	A.7	Uso no previsto	Implementación de recursos (económicos y de tiempo) en actividades no relacionadas.	Muy baja	**2**

Tabla 44. Estimación de la probabilidad activo memoria USB. (Continuación)

	A.11	Acceso no autorizado	Uso ilícito del hardware	Muy baja	**2**
	A.23	Manipulación de los equipos	Sabotaje del hardware y software conteniente.	Muy baja	**2**
	A.24	Denegación de servicio	Saturación del sistema de información.	Muy baja	**2**
	A.25	Robo	Robo de porte de la información, puede esta ser física o digital.	Muy baja	**2**
	A.26	Ataque destructivo	Destrucción de los contenedores de la información, en recipientes físicos y lógicos.	Muy baja	**2**

Fuente: Autoría propia

Tabla 45. Estimación de la probabilidad activo discos duros

ACTIVO TI	DISCOS DUROS
ADMINISTRADOR	PIMIENTO CARDENAS WILSON MAURICIO
DEGRADACIÓN	35%
IMPACTO	3
TIPO DE ACTIVO	HARDWARE

Tipo	**ID**	**Amenaza**	**Exposición/Vulnerabilidad**	**Frecuencia (F)**	
DESASTRES NATURALES	**N.1**	Fuego	No existe sistema de alarma contra incendios. Se posee un solo extintor de solkaflam (clase c) recomendados para incendios en lugares donde se encuentren equipos eléctricos.	Muy baja	**2**
	N.2	Daños por agua	La infraestructura está expuesta a goteras, cuenta con averías en el techo en donde el agua de las lluvias	Muy baja	**2**

Tabla 45. Estimación de la probabilidad activo discos duros. (Continuación)

	N.*	Desastres naturales	La oficina de la dependencia de sistemas se encuentra en zona baja de riesgo de desastre natural de origen volcánico debido a su cercanía con el volcán nevado del Tolima.	Raro	**1**
DE ORIGEN INDUSTRIAL	**I.1**	Fuego	No existe sistema de alarma contra incendios. Se posee un solo extintor de solkaflam (clase c) recomendados para incendios en lugares donde se encuentren equipos eléctricos.	Muy baja	**2**
	I.2	Daños por agua	La concentración del líquido sobrante por parte del aire acondicionado causaría daños en los equipos.	Muy baja	**2**
	I.*	Desastres industriales	No hay exposición o vulnerabilidad, por parte de esta amenaza.	Muy baja	**2**
	I.3	Contaminación mecánica	No hay exposición o vulnerabilidad, por parte de esta amenaza.	Muy baja	**2**
	I.4	Contaminación electromagnética	No hay exposición o vulnerabilidad, por parte de esta amenaza.	Muy baja	**2**
	I.5	Avería de origen físico o lógico	La manipulación por parte de cada uno de los componentes encontrados en la dependencia, como también por defectos de los componentes desde fabrica	Muy baja	**2**

Tabla 45. Estimación de la probabilidad activo discos duros. (Continuación)

	I.6	Corte del suministro eléctrico	Amenaza debida a factores externos, a clemencias de tipo naturales como lluvias u otros.	Muy baja	**2**
	I.7	Condiciones inadecuadas de temperatura o humedad	No se cuenta con una infraestructura adecuada para soportar los defectos del sistema de refrigeración.	Muy baja	**2**
	I.11	Emanaciones electromagnéticas	No hay exposición o vulnerabilidad, por parte de esta amenaza.	Muy baja	**2**
ERRORES Y FALLOS NO INTENCIONADOS	**E.2**	Errores del administrador	Pérdida total o parcial del tiempo de ejecución de sus actividades, dependiendo de la gravedad del asunto.	Muy baja	**2**
	E.23	Errores de mantenimiento / actualización de equipos(hardware)	Perjuicio a la mantenibilidad del sistema de información.	Muy baja	**2**
	E.24	Caída del sistema por agotamiento de recursos	Saturación del sistema informático.	Muy baja	**2**
	E.25	Perdida de equipos (Robo)	Recuperación de soportes reciclados o desechados.	Muy baja	**2**
ATAQUES INTENCIONADOS	**A.6**	Abuso de privilegios de acceso	Abuso de cada uno de los derechos otorgados.	Muy baja	**2**
	A.7	Uso no previsto	Implementación de recursos (económicos y de tiempo) en actividades no relacionadas.	Muy baja	**2**

Tabla 45. Estimación de la probabilidad activo discos duros. (Continuación)

	A.11	Acceso no autorizado	Uso ilícito del hardware	Muy baja	**2**
	A.23	Manipulación de los equipos	Sabotaje del hardware y software conteniente.	Muy baja	**2**
	A.24	Denegación de servicio	Saturación del sistema de información.	Muy baja	**2**
	A.25	Robo	Robo de porte de la información, puede esta ser física o digital.	Muy baja	**2**
	A.26	Ataque destructivo	Destrucción de los contenedores de la información, en recipientes físicos y lógicos.	Muy baja	**2**

Fuente: Autoría propia

Tabla 46. Estimación de la probabilidad activo discos duros externos

ACTIVO TI	DISCOS DUROS EXTERNOS
ADMINISTRADOR	PIMIENTO CARDENAS WILSON MAURICIO
DEGRADACIÓN	45%
IMPACTO	3
TIPO DE ACTIVO	HARDWARE

Tipo	**ID**	**Amenaza**	**Exposición/Vulnerabilidad**	**Frecuencia (F)**	
DESASTRES NATURALES	**N.1**	Fuego	No existe sistema de alarma contra incendios. Se posee un solo extintor de solkaflam (clase c) recomendados para incendios en lugares donde se encuentren equipos eléctricos.	Muy baja	**2**
	N.2	Daños por agua	La infraestructura está expuesta a goteras, cuenta con averías en el techo en donde el agua de las lluvias	Muy baja	**2**

Tabla 46. Estimación de la probabilidad activo discos duros externos. (Continuación)

	N.*	Desastres naturales	La oficina de la dependencia de sistemas se encuentra en zona baja de riesgo de desastre natural de origen volcánico debido a su cercanía con el volcán nevado del Tolima.	Raro	**1**
DE ORIGEN INDUSTRIAL	**I.1**	Fuego	No existe sistema de alarma contra incendios. Se posee un solo extintor de solkaflam (clase c) recomendados para incendios en lugares donde se encuentren equipos eléctricos.	Muy baja	**2**
	I.2	Daños por agua	La concentración del líquido sobrante por parte del aire acondicionado causaría daños en los equipos.	Muy baja	**2**
	I.*	Desastres industriales	No hay exposición o vulnerabilidad, por parte de esta amenaza.	Muy baja	**2**
	I.3	Contaminación mecánica	No hay exposición o vulnerabilidad, por parte de esta amenaza.	Muy baja	**2**
	I.4	Contaminación electromagnética	No hay exposición o vulnerabilidad, por parte de esta amenaza.	Muy baja	**2**
	I.5	Avería de origen físico o lógico	La manipulación por parte de cada uno de los componentes encontrados en la dependencia, como también por defectos de los componentes desde fabrica	Muy baja	**2**

Tabla 46. Estimación de la probabilidad activo discos duros externos. (Continuación)

	I.6	Corte del suministro eléctrico	Amenaza debida a factores externos, a clemencias de tipo naturales como lluvias u otros.	Muy baja	**2**
	I.7	Condiciones inadecuadas de temperatura o humedad	No se cuenta con una infraestructura adecuada para soportar los defectos del sistema de refrigeración.	Muy baja	**2**
	I.11	Emanaciones electromagnéticas	No hay exposición o vulnerabilidad, por parte de esta amenaza.	Muy baja	**2**
ERRORES Y FALLOS NO INTENCIONADOS	**E.2**	Errores del administrador	Pérdida total o parcial del tiempo de ejecución de sus actividades, dependiendo de la gravedad del asunto.	Muy baja	**2**
	E.23	Errores de mantenimiento / actualización de equipos(hardware)	Perjuicio a la mantenibilidad del sistema de información.	Muy baja	**2**
	E.24	Caída del sistema por agotamiento de recursos	Saturación del sistema informático.	Muy baja	**2**
	E.25	Perdida de equipos (Robo)	Recuperación de soportes reciclados o desechados.	Muy baja	**2**
ATAQUES INTENCIONADOS	**A.6**	Abuso de privilegios de acceso	Abuso de cada uno de los derechos otorgados.	Muy baja	**2**
	A.7	Uso no previsto	Implementación de recursos (económicos y de tiempo) en actividades no relacionadas.	Muy baja	**2**

Tabla 46. Estimación de la probabilidad activo discos duros externos. (Continuación)

	A.11	Acceso no autorizado	Uso ilícito del hardware	Muy baja	**2**
	A.23	Manipulación de los equipos	Sabotaje del hardware y software conteniente.	Muy baja	**2**
	A.24	Denegación de servicio	Saturación del sistema de información.	Muy baja	**2**
	A.25	Robo	Robo de porte de la información, puede esta ser física o digital.	Muy baja	**2**
	A.26	Ataque destructivo	Destrucción de los contenedores de la información, en recipientes físicos y lógicos.	Muy baja	**2**

Fuente: Autoría propia

Tabla 47. Estimación de la probabilidad activo switch ALCATEL LUCEN 9553

ACTIVO TI	SWITCH ALCATEL LUCEN 9553
ADMINISTRADOR	PIMIENTO CARDENAS WILSON MAURICIO
DEGRADACIÓN	60%
IMPACTO	5
TIPO DE ACTIVO	HARDWARE

Tipo	**ID**	**Amenaza**	**Exposición/Vulnerabilidad**	**Frecuencia (F)**	
DESASTRES NATURALES	**N.1**	Fuego	No existe sistema de alarma contra incendios. Se posee un solo extintor de solkaflam (clase c) recomendados para incendios en lugares donde se encuentren equipos eléctricos.	Muy baja	**2**
	N.2	Daños por agua	La infraestructura está expuesta a goteras, cuenta con averías en el techo en donde el agua de las lluvias	Muy baja	**2**

Tabla 47. Estimación de la probabilidad activo switch ALCATEL LUCEN 9553. (Continuación)

	N.*	Desastres naturales	La oficina de la dependencia de sistemas se encuentra en zona baja de riesgo de desastre natural de origen volcánico debido a su cercanía con el volcán nevado del Tolima.	Raro	**1**
DE ORIGEN INDUSTRIAL	**I.1**	Fuego	No existe sistema de alarma contra incendios. Se posee un solo extintor de solkaflam (clase c) recomendados para incendios en lugares donde se encuentren equipos eléctricos.	Muy baja	**2**
	I.2	Daños por agua	La concentración del líquido sobrante por parte del aire acondicionado causaría daños en los equipos.	Muy baja	**2**
	I.*	Desastres industriales	No hay exposición o vulnerabilidad, por parte de esta amenaza.	Muy baja	**2**
	I.3	Contaminación mecánica	No hay exposición o vulnerabilidad, por parte de esta amenaza.	Muy baja	**2**
	I.4	Contaminación electromagnética	No hay exposición o vulnerabilidad, por parte de esta amenaza.	Muy baja	**2**
	I.5	Avería de origen físico o lógico	La manipulación por parte de cada uno de los componentes encontrados en la dependencia, como también por defectos de los componentes desde fabrica	Muy baja	**2**

Tabla 47. Estimación de la probabilidad activo switch ALCATEL LUCEN 9553. (Continuación)

	I.6	Corte del suministro eléctrico	Amenaza debida a factores externos, a clemencias de tipo naturales como lluvias u otros.	Muy baja	**2**
	I.7	Condiciones inadecuadas de temperatura o humedad	No se cuenta con una infraestructura adecuada para soportar los defectos del sistema de refrigeración.	Muy baja	**2**
	I.11	Emanaciones electromagnéticas	No hay exposición o vulnerabilidad, por parte de esta amenaza.	Muy baja	**2**
ERRORES Y FALLOS NO INTENCIONADOS	**E.2**	Errores del administrador	Pérdida total o parcial del tiempo de ejecución de sus actividades, dependiendo de la gravedad del asunto.	Muy baja	**2**
	E.23	Errores de mantenimiento / actualización de equipos(hardware)	Perjuicio a la mantenibilidad del sistema de información.	Muy baja	**2**
	E.24	Caída del sistema por agotamiento de recursos	Saturación del sistema informático.	Muy baja	**2**
	E.25	Perdida de equipos (Robo)	Recuperación de soportes reciclados o desechados.	Muy baja	**2**
ATAQUES INTENCIONADOS	**A.6**	Abuso de privilegios de acceso	Abuso de cada uno de los derechos otorgados.	Muy baja	**2**
	A.7	Uso no previsto	Implementación de recursos (económicos y de tiempo) en actividades no relacionadas.	Muy baja	**2**

Tabla 47. Estimación de la probabilidad activo switch ALCATEL LUCEN 9553. (Continuación)

	A.11	Acceso no autorizado	Uso ilícito del hardware	Muy baja	**2**
	A.23	Manipulación de los equipos	Sabotaje del hardware y software conteniente.	Muy baja	**2**
	A.24	Denegación de servicio	Saturación del sistema de información.	Muy baja	**2**
	A.25	Robo	Robo de porte de la información, puede esta ser física o digital.	Muy baja	**2**
	A.26	Ataque destructivo	Destrucción de los contenedores de la información, en recipientes físicos y lógicos.	Muy baja	**2**

Fuente: Autoría propia

Tabla 48. Estimación de la probabilidad activo switch 24 10/100/1000 base t c

ACTIVO TI	SWITCH 24 10/100/1000 BASE T C
ADMINISTRADOR	PIMIENTO CARDENAS WILSON MAURICIO
DEGRADACIÓN	60%
IMPACTO	5
TIPO DE ACTIVO	HARDWARE

Tipo	**ID**	**Amenaza**	**Exposición/Vulnerabilidad**	**Frecuencia (F)**	
DESASTRES NATURALES	**N.1**	Fuego	No existe sistema de alarma contra incendios. Se posee un solo extintor de solkaflam (clase c) recomendados para incendios en lugares donde se encuentren equipos eléctricos.	Muy baja	**2**
	N.2	Daños por agua	La infraestructura está expuesta a goteras, cuenta con averías en el techo en donde el agua de las lluvias	Muy baja	**2**

Tabla 48. Estimación de la probabilidad activo switch 24 10/100/1000 base t c. (Continuación)

	N.*	Desastres naturales	La oficina de la dependencia de sistemas se encuentra en zona baja de riesgo de desastre natural de origen volcánico debido a su cercanía con el volcán nevado del Tolima.	Raro	**1**
DE ORIGEN INDUSTRIAL	**I.1**	Fuego	No existe sistema de alarma contra incendios. Se posee un solo extintor de solkaflam (clase c) recomendados para incendios en lugares donde se encuentren equipos eléctricos.	Muy baja	**2**
	I.2	Daños por agua	La concentración del líquido sobrante por parte del aire acondicionado causaría daños en los equipos.	Muy baja	**2**
	I.*	Desastres industriales	No hay exposición o vulnerabilidad, por parte de esta amenaza.	Muy baja	**2**
	I.3	Contaminación mecánica	No hay exposición o vulnerabilidad, por parte de esta amenaza.	Muy baja	**2**
	I.4	Contaminación electromagnética	No hay exposición o vulnerabilidad, por parte de esta amenaza.	Muy baja	**2**
	I.5	Avería de origen físico o lógico	La manipulación por parte de cada uno de los componentes encontrados en la dependencia, como también por defectos de los componentes desde fabrica	Muy baja	**2**

Tabla 48. Estimación de la probabilidad activo switch 24 10/100/1000 base t c. (Continuación)

	I.6	Corte del suministro eléctrico	Amenaza debida a factores externos, a clemencias de tipo naturales como lluvias u otros.	Muy baja	**2**
	I.7	Condiciones inadecuadas de temperatura o humedad	No se cuenta con una infraestructura adecuada para soportar los defectos del sistema de refrigeración.	Muy baja	**2**
	I.11	Emanaciones electromagnéticas	No hay exposición o vulnerabilidad, por parte de esta amenaza.	Muy baja	**2**
ERRORES Y FALLOS NO INTENCIONADOS	**E.2**	Errores del administrador	Pérdida total o parcial del tiempo de ejecución de sus actividades, dependiendo de la gravedad del asunto.	Muy baja	**2**
	E.23	Errores de mantenimiento / actualización de equipos(hardware)	Perjuicio a la mantenibilidad del sistema de información.	Muy baja	**2**
	E.24	Caída del sistema por agotamiento de recursos	Saturación del sistema informático.	Muy baja	**2**
	E.25	Perdida de equipos (Robo)	Recuperación de soportes reciclados o desechados.	Muy baja	**2**
ATAQUES INTENCIONADOS	**A.6**	Abuso de privilegios de acceso	Abuso de cada uno de los derechos otorgados.	Muy baja	**2**
	A.7	Uso no previsto	Implementación de recursos (económicos y de tiempo) en actividades no relacionadas.	Muy baja	**2**

Tabla 48. Estimación de la probabilidad activo switch 24 10/100/1000 base t c. (Continuación)

	A.11	Acceso no autorizado	Uso ilícito del hardware	Muy baja	**2**
	A.23	Manipulación de los equipos	Sabotaje del hardware y software conteniente.	Muy baja	**2**
	A.24	Denegación de servicio	Saturación del sistema de información.	Muy baja	**2**
	A.25	Robo	Robo de porte de la información, puede esta ser física o digital.	Muy baja	**2**
	A.26	Ataque destructivo	Destrucción de los contenedores de la información, en recipientes físicos y lógicos.	Muy baja	**2**

Fuente: Autoría propia

Tabla 49. Estimación de la probabilidad activo switch 24/10/100/1000 base t4s

ACTIVO TI	SWITCH 24/10/100/1000 BASE T4S
ADMINISTRADOR	PIMIENTO CARDENAS WILSON MAURICIO
DEGRADACIÓN	60%
IMPACTO	5
TIPO DE ACTIVO	HARDWARE

Tipo	**ID**	**Amenaza**	**Exposición/Vulnerabilidad**	**Frecuencia (F)**	
DESASTRES NATURALES	**N.1**	Fuego	No existe sistema de alarma contra incendios. Se posee un solo extintor de solkaflam (clase c) recomendados para incendios en lugares donde se encuentren equipos eléctricos.	Muy baja	**2**
	N.2	Daños por agua	La infraestructura está expuesta a goteras, cuenta con averías en el techo en donde el agua de las lluvias	Muy baja	**2**

Tabla 49. Estimación de la probabilidad activo switch 24/10/100/1000 base t4s. (Continuación)

	N.*	Desastres naturales	La oficina de la dependencia de sistemas se encuentra en zona baja de riesgo de desastre natural de origen volcánico debido a su cercanía con el volcán nevado del Tolima.	Raro	**1**
DE ORIGEN INDUSTRIAL	**I.1**	Fuego	No existe sistema de alarma contra incendios. Se posee un solo extintor de solkaflam (clase c) recomendados para incendios en lugares donde se encuentren equipos eléctricos.	Muy baja	**2**
	I.2	Daños por agua	La concentración del líquido sobrante por parte del aire acondicionado causaría daños en los equipos.	Muy baja	**2**
	I.*	Desastres industriales	No hay exposición o vulnerabilidad, por parte de esta amenaza.	Muy baja	**2**
	I.3	Contaminación mecánica	No hay exposición o vulnerabilidad, por parte de esta amenaza.	Muy baja	**2**
	I.4	Contaminación electromagnética	No hay exposición o vulnerabilidad, por parte de esta amenaza.	Muy baja	**2**
	I.5	Avería de origen físico o lógico	La manipulación por parte de cada uno de los componentes encontrados en la dependencia, como también por defectos de los componentes desde fabrica	Muy baja	**2**

Tabla 49. Estimación de la probabilidad activo switch 24/10/100/1000 base t4s. (Continuación)

	I.6	Corte del suministro eléctrico	Amenaza debida a factores externos, a clemencias de tipo naturales como lluvias u otros.	Muy baja	**2**
	I.7	Condiciones inadecuadas de temperatura o humedad	No se cuenta con una infraestructura adecuada para soportar los defectos del sistema de refrigeración.	Muy baja	**2**
	I.11	Emanaciones electromagnéticas	No hay exposición o vulnerabilidad, por parte de esta amenaza.	Muy baja	**2**
ERRORES Y FALLOS NO INTENCIONADOS	**E.2**	Errores del administrador	Pérdida total o parcial del tiempo de ejecución de sus actividades, dependiendo de la gravedad del asunto.	Muy baja	**2**
	E.23	Errores de mantenimiento / actualización de equipos(hardware)	Perjuicio a la mantenibilidad del sistema de información.	Muy baja	**2**
	E.24	Caída del sistema por agotamiento de recursos	Saturación del sistema informático.	Muy baja	**2**
	E.25	Perdida de equipos (Robo)	Recuperación de soportes reciclados o desechados.	Muy baja	**2**
ATAQUES INTENCIONADOS	**A.6**	Abuso de privilegios de acceso	Abuso de cada uno de los derechos otorgados.	Muy baja	**2**
	A.7	Uso no previsto	Implementación de recursos (económicos y de tiempo) en actividades no relacionadas.	Muy baja	**2**

Tabla 49. Estimación de la probabilidad activo switch 24/10/100/1000 base t4s. (Continuación)

	A.11	Acceso no autorizado	Uso ilícito del hardware	Muy baja	**2**
	A.23	Manipulación de los equipos	Sabotaje del hardware y software conteniente.	Muy baja	**2**
	A.24	Denegación de servicio	Saturación del sistema de información.	Muy baja	**2**
	A.25	Robo	Robo de porte de la información, puede esta ser física o digital.	Muy baja	**2**
	A.26	Ataque destructivo	Destrucción de los contenedores de la información, en recipientes físicos y lógicos.	Muy baja	**2**

Fuente: Autoría propia

Tabla 50. Estimación de la probabilidad activo switch 24/10/100/1000pwr cord

ACTIVO TI	SWITCH 24/10/100/1000PWR CORD
ADMINISTRADOR	PIMIENTO CARDENAS WILSON MAURICIO
DEGRADACIÓN	60%
IMPACTO	5
TIPO DE ACTIVO	HARDWARE

Tipo	**ID**	**Amenaza**	**Exposición/Vulnerabilidad**	**Frecuencia (F)**	
DESASTRES NATURALES	**N.1**	Fuego	No existe sistema de alarma contra incendios. Se posee un solo extintor de solkaflam (clase c) recomendados para incendios en lugares donde se encuentren equipos eléctricos.	Muy baja	**2**
	N.2	Daños por agua	La infraestructura está expuesta a goteras, cuenta con averías en el techo en donde el agua de las lluvias	Muy baja	**2**

Tabla 50. Estimación de la probabilidad activo switch 24/10/100/1000pwr cord. (Continuación)

	N.*	Desastres naturales	La oficina de la dependencia de sistemas se encuentra en zona baja de riesgo de desastre natural de origen volcánico debido a su cercanía con el volcán nevado del Tolima.	Raro	**1**
DE ORIGEN INDUSTRIAL	**I.1**	Fuego	No existe sistema de alarma contra incendios. Se posee un solo extintor de solkaflam (clase c) recomendados para incendios en lugares donde se encuentren equipos eléctricos.	Muy baja	**2**
	I.2	Daños por agua	La concentración del líquido sobrante por parte del aire acondicionado causaría daños en los equipos.	Muy baja	**2**
	I.*	Desastres industriales	No hay exposición o vulnerabilidad, por parte de esta amenaza.	Muy baja	**2**
	I.3	Contaminación mecánica	No hay exposición o vulnerabilidad, por parte de esta amenaza.	Muy baja	**2**
	I.4	Contaminación electromagnética	No hay exposición o vulnerabilidad, por parte de esta amenaza.	Muy baja	**2**
	I.5	Avería de origen físico o lógico	La manipulación por parte de cada uno de los componentes encontrados en la dependencia, como también por defectos de los componentes desde fabrica	Muy baja	**2**

Tabla 50. Estimación de la probabilidad activo switch 24/10/100/1000pwr cord. (Continuación)

	I.6	Corte del suministro eléctrico	Amenaza debida a factores externos, a clemencias de tipo naturales como lluvias u otros.	Muy baja	**2**
	I.7	Condiciones inadecuadas de temperatura o humedad	No se cuenta con una infraestructura adecuada para soportar los defectos del sistema de refrigeración.	Muy baja	**2**
	I.11	Emanaciones electromagnéticas	No hay exposición o vulnerabilidad, por parte de esta amenaza.	Muy baja	**2**
ERRORES Y FALLOS NO INTENCIONADOS	**E.2**	Errores del administrador	Pérdida total o parcial del tiempo de ejecución de sus actividades, dependiendo de la gravedad del asunto.	Muy baja	**2**
	E.23	Errores de mantenimiento / actualización de equipos(hardware)	Perjuicio a la mantenibilidad del sistema de información.	Muy baja	**2**
	E.24	Caída del sistema por agotamiento de recursos	Saturación del sistema informático.	Muy baja	**2**
	E.25	Perdida de equipos (Robo)	Recuperación de soportes reciclados o desechados.	Muy baja	**2**
ATAQUES INTENCIONADOS	**A.6**	Abuso de privilegios de acceso	Abuso de cada uno de los derechos otorgados.	Muy baja	**2**
	A.7	Uso no previsto	Implementación de recursos (económicos y de tiempo) en actividades no relacionadas.	Muy baja	**2**

Tabla 50. Estimación de la probabilidad activo switch 24/10/100/1000pwr cord. (Continuación)

	A.11	Acceso no autorizado	Uso ilícito del hardware	Muy baja	**2**
	A.23	Manipulación de los equipos	Sabotaje del hardware y software conteniente.	Muy baja	**2**
	A.24	Denegación de servicio	Saturación del sistema de información.	Muy baja	**2**
	A.25	Robo	Robo de porte de la información, puede esta ser física o digital.	Muy baja	**2**
	A.26	Ataque destructivo	Destrucción de los contenedores de la información, en recipientes físicos y lógicos.	Muy baja	**2**

Fuente: Autoría propia

Tabla 51. Estimación de la probabilidad activo switch ALCATEL LUCEN 9561

ACTIVO TI	SWITCH ALCATEL LUCEN 9561
ADMINISTRADOR	PIMIENTO CARDENAS WILSON MAURICIO
DEGRADACIÓN	60%
IMPACTO	5
TIPO DE ACTIVO	HARDWARE

Tipo	**ID**	**Amenaza**	**Exposición/Vulnerabilidad**	**Frecuencia (F)**	
DESASTRES NATURALES	**N.1**	Fuego	No existe sistema de alarma contra incendios. Se posee un solo extintor de solkaflam (clase c) recomendados para incendios en lugares donde se encuentren equipos eléctricos.	Muy baja	**2**
	N.2	Daños por agua	La infraestructura está expuesta a goteras, cuenta con averías en el techo en donde el agua de las lluvias	Muy baja	**2**

Tabla 51. Estimación de la probabilidad activo switch ALCATEL LUCEN 9561. (Continuación)

	N.*	Desastres naturales	La oficina de la dependencia de sistemas se encuentra en zona baja de riesgo de desastre natural de origen volcánico debido a su cercanía con el volcán nevado del Tolima.	Raro	**1**
DE ORIGEN INDUSTRIAL	**I.1**	Fuego	No existe sistema de alarma contra incendios. Se posee un solo extintor de solkaflam (clase c) recomendados para incendios en lugares donde se encuentren equipos eléctricos.	Muy baja	**2**
	I.2	Daños por agua	La concentración del líquido sobrante por parte del aire acondicionado causaría daños en los equipos.	Muy baja	**2**
	I.*	Desastres industriales	No hay exposición o vulnerabilidad, por parte de esta amenaza.	Muy baja	**2**
	I.3	Contaminación mecánica	No hay exposición o vulnerabilidad, por parte de esta amenaza.	Muy baja	**2**
	I.4	Contaminación electromagnética	No hay exposición o vulnerabilidad, por parte de esta amenaza.	Muy baja	**2**
	I.5	Avería de origen físico o lógico	La manipulación por parte de cada uno de los componentes encontrados en la dependencia, como también por defectos de los componentes desde fabrica	Muy baja	**2**

Tabla 51. Estimación de la probabilidad activo switch ALCATEL LUCEN 9561. (Continuación)

	I.6	Corte del suministro eléctrico	Amenaza debida a factores externos, a clemencias de tipo naturales como lluvias u otros.	Muy baja	**2**
	I.7	Condiciones inadecuadas de temperatura o humedad	No se cuenta con una infraestructura adecuada para soportar los defectos del sistema de refrigeración.	Muy baja	**2**
	I.11	Emanaciones electromagnéticas	No hay exposición o vulnerabilidad, por parte de esta amenaza.	Muy baja	**2**
ERRORES Y FALLOS NO INTENCIONADOS	**E.2**	Errores del administrador	Pérdida total o parcial del tiempo de ejecución de sus actividades, dependiendo de la gravedad del asunto.	Muy baja	**2**
	E.23	Errores de mantenimiento / actualización de equipos(hardware)	Perjuicio a la mantenibilidad del sistema de información.	Muy baja	**2**
	E.24	Caída del sistema por agotamiento de recursos	Saturación del sistema informático.	Muy baja	**2**
	E.25	Perdida de equipos (Robo)	Recuperación de soportes reciclados o desechados.	Muy baja	**2**
ATAQUES INTENCIONADOS	**A.6**	Abuso de privilegios de acceso	Abuso de cada uno de los derechos otorgados.	Muy baja	**2**
	A.7	Uso no previsto	Implementación de recursos (económicos y de tiempo) en actividades no relacionadas.	Muy baja	**2**

Tabla 51. Estimación de la probabilidad activo switch ALCATEL LUCEN 9561. (Continuación)

	A.11	Acceso no autorizado	Uso ilícito del hardware	Muy baja	**2**
	A.23	Manipulación de los equipos	Sabotaje del hardware y software conteniente.	Muy baja	**2**
	A.24	Denegación de servicio	Saturación del sistema de información.	Muy baja	**2**
	A.25	Robo	Robo de porte de la información, puede esta ser física o digital.	Muy baja	**2**
	A.26	Ataque destructivo	Destrucción de los contenedores de la información, en recipientes físicos y lógicos.	Muy baja	**2**

Fuente: Autoría propia

Tabla 52. Estimación de la probabilidad activo switch ALCATEL LUCEN 9556

ACTIVO TI	SWITCH ALCATEL LUCEN 9556
ADMINISTRADOR	PIMIENTO CARDENAS WILSON MAURICIO
DEGRADACIÓN	60%
IMPACTO	5
TIPO DE ACTIVO	HARDWARE

Tipo	**ID**	**Amenaza**	**Exposición/Vulnerabilidad**	**Frecuencia (F)**	
DESASTRES NATURALES	**N.1**	Fuego	No existe sistema de alarma contra incendios. Se posee un solo extintor de solkaflam (clase c) recomendados para incendios en lugares donde se encuentren equipos eléctricos.	Muy baja	**2**
	N.2	Daños por agua	La infraestructura está expuesta a goteras, cuenta con averías en el techo en donde el agua de las lluvias	Muy baja	**2**

Tabla 52. Estimación de la probabilidad activo switch ALCATEL LUCEN 9556. (Continuación)

	N.*	Desastres naturales	La oficina de la dependencia de sistemas se encuentra en zona baja de riesgo de desastre natural de origen volcánico debido a su cercanía con el volcán nevado del Tolima.	Raro	**1**
DE ORIGEN INDUSTRIAL	**I.1**	Fuego	No existe sistema de alarma contra incendios. Se posee un solo extintor de solkaflam (clase c) recomendados para incendios en lugares donde se encuentren equipos eléctricos.	Muy baja	**2**
	I.2	Daños por agua	La concentración del líquido sobrante por parte del aire acondicionado causaría daños en los equipos.	Muy baja	**2**
	I.*	Desastres industriales	No hay exposición o vulnerabilidad, por parte de esta amenaza.	Muy baja	**2**
	I.3	Contaminación mecánica	No hay exposición o vulnerabilidad, por parte de esta amenaza.	Muy baja	**2**
	I.4	Contaminación electromagnética	No hay exposición o vulnerabilidad, por parte de esta amenaza.	Muy baja	**2**
	I.5	Avería de origen físico o lógico	La manipulación por parte de cada uno de los componentes encontrados en la dependencia, como también por defectos de los componentes desde fabrica	Muy baja	**2**

Tabla 52. Estimación de la probabilidad activo switch ALCATEL LUCEN 9556. (Continuación)

	I.6	Corte del suministro eléctrico	Amenaza debida a factores externos, a clemencias de tipo naturales como lluvias u otros.	Muy baja	**2**
	I.7	Condiciones inadecuadas de temperatura o humedad	No se cuenta con una infraestructura adecuada para soportar los defectos del sistema de refrigeración.	Muy baja	**2**
	I.11	Emanaciones electromagnéticas	No hay exposición o vulnerabilidad, por parte de esta amenaza.	Muy baja	**2**
ERRORES Y FALLOS NO INTENCIONADOS	**E.2**	Errores del administrador	Pérdida total o parcial del tiempo de ejecución de sus actividades, dependiendo de la gravedad del asunto.	Muy baja	**2**
	E.23	Errores de mantenimiento / actualización de equipos(hardware)	Perjuicio a la mantenibilidad del sistema de información.	Muy baja	**2**
	E.24	Caída del sistema por agotamiento de recursos	Saturación del sistema informático.	Muy baja	**2**
	E.25	Perdida de equipos (Robo)	Recuperación de soportes reciclados o desechados.	Muy baja	**2**
ATAQUES INTENCIONADOS	**A.6**	Abuso de privilegios de acceso	Abuso de cada uno de los derechos otorgados.	Muy baja	**2**
	A.7	Uso no previsto	Implementación de recursos (económicos y de tiempo) en actividades no relacionadas.	Muy baja	**2**

Tabla 52. Estimación de la probabilidad activo switch ALCATEL LUCEN 9556. (Continuación)

	A.11	Acceso no autorizado	Uso ilícito del hardware	Muy baja	**2**
	A.23	Manipulación de los equipos	Sabotaje del hardware y software conteniente.	Muy baja	**2**
	A.24	Denegación de servicio	Saturación del sistema de información.	Muy baja	**2**
	A.25	Robo	Robo de porte de la información, puede esta ser física o digital.	Muy baja	**2**
	A.26	Ataque destructivo	Destrucción de los contenedores de la información, en recipientes físicos y lógicos.	Muy baja	**2**

Fuente: Autoría propia

Tabla 53. Estimación de la probabilidad activo switch ALCATEL LUCEN 9557

ACTIVO TI	SWITCH ALCATEL LUCEN 9557
ADMINISTRADOR	PIMIENTO CARDENAS WILSON MAURICIO
DEGRADACIÓN	60%
IMPACTO	5
TIPO DE ACTIVO	HARDWARE

Tipo	**ID**	**Amenaza**	**Exposición/Vulnerabilidad**	**Frecuencia (F)**	
DESASTRES NATURALES	**N.1**	Fuego	No existe sistema de alarma contra incendios. Se posee un solo extintor de solkaflam (clase c) recomendados para incendios en lugares donde se encuentren equipos eléctricos.	Muy baja	**2**
	N.2	Daños por agua	La infraestructura está expuesta a goteras, cuenta con averías en el techo en donde el agua de las lluvias	Muy baja	**2**

Tabla 53. Estimación de la probabilidad activo switch ALCATEL LUCEN 9557. (Continuación)

	N.*	Desastres naturales	La oficina de la dependencia de sistemas se encuentra en zona baja de riesgo de desastre natural de origen volcánico debido a su cercanía con el volcán nevado del Tolima.	Raro	**1**
DE ORIGEN INDUSTRIAL	**I.1**	Fuego	No existe sistema de alarma contra incendios. Se posee un solo extintor de solkaflam (clase c) recomendados para incendios en lugares donde se encuentren equipos eléctricos.	Muy baja	**2**
	I.2	Daños por agua	La concentración del líquido sobrante por parte del aire acondicionado causaría daños en los equipos.	Muy baja	**2**
	I.*	Desastres industriales	No hay exposición o vulnerabilidad, por parte de esta amenaza.	Muy baja	**2**
	I.3	Contaminación mecánica	No hay exposición o vulnerabilidad, por parte de esta amenaza.	Muy baja	**2**
	I.4	Contaminación electromagnética	No hay exposición o vulnerabilidad, por parte de esta amenaza.	Muy baja	**2**
	I.5	Avería de origen físico o lógico	La manipulación por parte de cada uno de los componentes encontrados en la dependencia, como también por defectos de los componentes desde fabrica	Muy baja	**2**

Tabla 53. Estimación de la probabilidad activo switch ALCATEL LUCEN 9557. (Continuación)

	I.6	Corte del suministro eléctrico	Amenaza debida a factores externos, a clemencias de tipo naturales como lluvias u otros.	Muy baja	**2**
	I.7	Condiciones inadecuadas de temperatura o humedad	No se cuenta con una infraestructura adecuada para soportar los defectos del sistema de refrigeración.	Muy baja	**2**
	I.11	Emanaciones electromagnéticas	No hay exposición o vulnerabilidad, por parte de esta amenaza.	Muy baja	**2**
ERRORES Y FALLOS NO INTENCIONADOS	**E.2**	Errores del administrador	Pérdida total o parcial del tiempo de ejecución de sus actividades, dependiendo de la gravedad del asunto.	Muy baja	**2**
	E.23	Errores de mantenimiento / actualización de equipos(hardware)	Perjuicio a la mantenibilidad del sistema de información.	Muy baja	**2**
	E.24	Caída del sistema por agotamiento de recursos	Saturación del sistema informático.	Muy baja	**2**
	E.25	Perdida de equipos (Robo)	Recuperación de soportes reciclados o desechados.	Muy baja	**2**
ATAQUES INTENCIONADOS	**A.6**	Abuso de privilegios de acceso	Abuso de cada uno de los derechos otorgados.	Muy baja	**2**
	A.7	Uso no previsto	Implementación de recursos (económicos y de tiempo) en actividades no relacionadas.	Muy baja	**2**

Tabla 53. Estimación de la probabilidad activo switch ALCATEL LUCEN 9557. (Continuación)

	A.11	Acceso no autorizado	Uso ilícito del hardware	Muy baja	**2**
	A.23	Manipulación de los equipos	Sabotaje del hardware y software conteniente.	Muy baja	**2**
	A.24	Denegación de servicio	Saturación del sistema de información.	Muy baja	**2**
	A.25	Robo	Robo de porte de la información, puede esta ser física o digital.	Muy baja	**2**
	A.26	Ataque destructivo	Destrucción de los contenedores de la información, en recipientes físicos y lógicos.	Muy baja	**2**

Fuente: Autoría propia

Tabla 54. Estimación de la probabilidad activo switch ALCATEL LUCEN 9558

ACTIVO TI	SWITCH ALCATEL LUCEN 9558
ADMINISTRADOR	PIMIENTO CARDENAS WILSON MAURICIO
DEGRADACIÓN	60%
IMPACTO	5
TIPO DE ACTIVO	HARDWARE

Tipo	**ID**	**Amenaza**	**Exposición/Vulnerabilidad**	**Frecuencia (F)**	
DESASTRES NATURALES	**N.1**	Fuego	No existe sistema de alarma contra incendios. Se posee un solo extintor de solkaflam (clase c) recomendados para incendios en lugares donde se encuentren equipos eléctricos.	Muy baja	**2**
	N.2	Daños por agua	La infraestructura está expuesta a goteras, cuenta con averías en el techo en donde el agua de las lluvias	Muy baja	**2**

Tabla 54. Estimación de la probabilidad activo switch ALCATEL LUCEN 9558. (Continuación)

	N.*	Desastres naturales	La oficina de la dependencia de sistemas se encuentra en zona baja de riesgo de desastre natural de origen volcánico debido a su cercanía con el volcán nevado del Tolima.	Raro	**1**
DE ORIGEN INDUSTRIAL	**I.1**	Fuego	No existe sistema de alarma contra incendios. Se posee un solo extintor de solkaflam (clase c) recomendados para incendios en lugares donde se encuentren equipos eléctricos.	Muy baja	**2**
	I.2	Daños por agua	La concentración del líquido sobrante por parte del aire acondicionado causaría daños en los equipos.	Muy baja	**2**
	I.*	Desastres industriales	No hay exposición o vulnerabilidad, por parte de esta amenaza.	Muy baja	**2**
	I.3	Contaminación mecánica	No hay exposición o vulnerabilidad, por parte de esta amenaza.	Muy baja	**2**
	I.4	Contaminación electromagnética	No hay exposición o vulnerabilidad, por parte de esta amenaza.	Muy baja	**2**
	I.5	Avería de origen físico o lógico	La manipulación por parte de cada uno de los componentes encontrados en la dependencia, como también por defectos de los componentes desde fabrica	Muy baja	**2**

Tabla 54. Estimación de la probabilidad activo switch ALCATEL LUCEN 9558. (Continuación)

	I.6	Corte del suministro eléctrico	Amenaza debida a factores externos, a clemencias de tipo naturales como lluvias u otros.	Muy baja	**2**
	I.7	Condiciones inadecuadas de temperatura o humedad	No se cuenta con una infraestructura adecuada para soportar los defectos del sistema de refrigeración.	Muy baja	**2**
	I.11	Emanaciones electromagnéticas	No hay exposición o vulnerabilidad, por parte de esta amenaza.	Muy baja	**2**
ERRORES Y FALLOS NO INTENCIONADOS	**E.2**	Errores del administrador	Pérdida total o parcial del tiempo de ejecución de sus actividades, dependiendo de la gravedad del asunto.	Muy baja	**2**
	E.23	Errores de mantenimiento / actualización de equipos(hardware)	Perjuicio a la mantenibilidad del sistema de información.	Muy baja	**2**
	E.24	Caída del sistema por agotamiento de recursos	Saturación del sistema informático.	Muy baja	**2**
	E.25	Perdida de equipos (Robo)	Recuperación de soportes reciclados o desechados.	Muy baja	**2**
ATAQUES INTENCIONADOS	**A.6**	Abuso de privilegios de acceso	Abuso de cada uno de los derechos otorgados.	Muy baja	**2**
	A.7	Uso no previsto	Implementación de recursos (económicos y de tiempo) en actividades no relacionadas.	Muy baja	**2**

Tabla 54. Estimación de la probabilidad activo switch ALCATEL LUCEN 9558. (Continuación)

	A.11	Acceso no autorizado	Uso ilícito del hardware	Muy baja	**2**
	A.23	Manipulación de los equipos	Sabotaje del hardware y software conteniente.	Muy baja	**2**
	A.24	Denegación de servicio	Saturación del sistema de información.	Muy baja	**2**
	A.25	Robo	Robo de porte de la información, puede esta ser física o digital.	Muy baja	**2**
	A.26	Ataque destructivo	Destrucción de los contenedores de la información, en recipientes físicos y lógicos.	Muy baja	**2**

Fuente: Autoría propia

Tabla 55. Estimación de la probabilidad activo switch ALCATEL LUCEN 9559

ACTIVO TI	SWITCH ALCATEL LUCEN 9559
ADMINISTRADOR	PIMIENTO CARDENAS WILSON MAURICIO
DEGRADACIÓN	60%
IMPACTO	5
TIPO DE ACTIVO	HARDWARE

Tipo	**ID**	**Amenaza**	**Exposición/Vulnerabilidad**	**Frecuencia (F)**	
DESASTRES NATURALES	**N.1**	Fuego	No existe sistema de alarma contra incendios. Se posee un solo extintor de solkaflam (clase c) recomendados para incendios en lugares donde se encuentren equipos eléctricos.	Muy baja	**2**
	N.2	Daños por agua	La infraestructura está expuesta a goteras, cuenta con averías en el techo en donde el agua de las lluvias	Muy baja	**2**

Tabla 55. Estimación de la probabilidad activo switch ALCATEL LUCEN 9559. (Continuación)

	N.*	Desastres naturales	La oficina de la dependencia de sistemas se encuentra en zona baja de riesgo de desastre natural de origen volcánico debido a su cercanía con el volcán nevado del Tolima.	Raro	**1**
DE ORIGEN INDUSTRIAL	**I.1**	Fuego	No existe sistema de alarma contra incendios. Se posee un solo extintor de solkaflam (clase c) recomendados para incendios en lugares donde se encuentren equipos eléctricos.	Muy baja	**2**
	I.2	Daños por agua	La concentración del líquido sobrante por parte del aire acondicionado causaría daños en los equipos.	Muy baja	**2**
	I.*	Desastres industriales	No hay exposición o vulnerabilidad, por parte de esta amenaza.	Muy baja	**2**
	I.3	Contaminación mecánica	No hay exposición o vulnerabilidad, por parte de esta amenaza.	Muy baja	**2**
	I.4	Contaminación electromagnética	No hay exposición o vulnerabilidad, por parte de esta amenaza.	Muy baja	**2**
	I.5	Avería de origen físico o lógico	La manipulación por parte de cada uno de los componentes encontrados en la dependencia, como también por defectos de los componentes desde fabrica	Muy baja	**2**

Tabla 55. Estimación de la probabilidad activo switch ALCATEL LUCEN 9559. (Continuación)

	I.6	Corte del suministro eléctrico	Amenaza debida a factores externos, a clemencias de tipo naturales como lluvias u otros.	Muy baja	**2**
	I.7	Condiciones inadecuadas de temperatura o humedad	No se cuenta con una infraestructura adecuada para soportar los defectos del sistema de refrigeración.	Muy baja	**2**
	I.11	Emanaciones electromagnéticas	No hay exposición o vulnerabilidad, por parte de esta amenaza.	Muy baja	**2**
ERRORES Y FALLOS NO INTENCIONADOS	**E.2**	Errores del administrador	Pérdida total o parcial del tiempo de ejecución de sus actividades, dependiendo de la gravedad del asunto.	Muy baja	**2**
	E.23	Errores de mantenimiento / actualización de equipos(hardware)	Perjuicio a la mantenibilidad del sistema de información.	Muy baja	**2**
	E.24	Caída del sistema por agotamiento de recursos	Saturación del sistema informático.	Muy baja	**2**
	E.25	Perdida de equipos (Robo)	Recuperación de soportes reciclados o desechados.	Muy baja	**2**
ATAQUES INTENCIONADOS	**A.6**	Abuso de privilegios de acceso	Abuso de cada uno de los derechos otorgados.	Muy baja	**2**
	A.7	Uso no previsto	Implementación de recursos (económicos y de tiempo) en actividades no relacionadas.	Muy baja	**2**

Tabla 55. Estimación de la probabilidad activo switch ALCATEL LUCEN 9559. (Continuación)

	A.11	Acceso no autorizado	Uso ilícito del hardware	Muy baja	**2**
	A.23	Manipulación de los equipos	Sabotaje del hardware y software conteniente.	Muy baja	**2**
	A.24	Denegación de servicio	Saturación del sistema de información.	Muy baja	**2**
	A.25	Robo	Robo de porte de la información, puede esta ser física o digital.	Muy baja	**2**
	A.26	Ataque destructivo	Destrucción de los contenedores de la información, en recipientes físicos y lógicos.	Muy baja	**2**

Fuente: Autoría propia

Tabla 56. Estimación de la probabilidad activo switch ALCATEL LUCEN 9543

ACTIVO TI	SWITCH ALCATEL LUCEN 9543
ADMINISTRADOR	PIMIENTO CARDENAS WILSON MAURICIO
DEGRADACIÓN	60%
IMPACTO	5
TIPO DE ACTIVO	HARDWARE

Tipo	**ID**	**Amenaza**	**Exposición/Vulnerabilidad**	**Frecuencia (F)**	
DESASTRES NATURALES	**N.1**	Fuego	No existe sistema de alarma contra incendios. Se posee un solo extintor de solkaflam (clase c) recomendados para incendios en lugares donde se encuentren equipos eléctricos.	Muy baja	**2**
	N.2	Daños por agua	La infraestructura está expuesta a goteras, cuenta con averías en el techo en donde el agua de las lluvias	Muy baja	**2**

Tabla 56. Estimación de la probabilidad activo switch ALCATEL LUCEN 9543. (Continuación)

	N.*	Desastres naturales	La oficina de la dependencia de sistemas se encuentra en zona baja de riesgo de desastre natural de origen volcánico debido a su cercanía con el volcán nevado del Tolima.	Raro	**1**
DE ORIGEN INDUSTRIAL	**I.1**	Fuego	No existe sistema de alarma contra incendios. Se posee un solo extintor de solkaflam (clase c) recomendados para incendios en lugares donde se encuentren equipos eléctricos.	Muy baja	**2**
	I.2	Daños por agua	La concentración del líquido sobrante por parte del aire acondicionado causaría daños en los equipos.	Muy baja	**2**
	I.*	Desastres industriales	No hay exposición o vulnerabilidad, por parte de esta amenaza.	Muy baja	**2**
	I.3	Contaminación mecánica	No hay exposición o vulnerabilidad, por parte de esta amenaza.	Muy baja	**2**
	I.4	Contaminación electromagnética	No hay exposición o vulnerabilidad, por parte de esta amenaza.	Muy baja	**2**
	I.5	Avería de origen físico o lógico	La manipulación por parte de cada uno de los componentes encontrados en la dependencia, como también por defectos de los componentes desde fabrica	Muy baja	**2**

Tabla 56. Estimación de la probabilidad activo switch ALCATEL LUCEN 9543. (Continuación)

	I.6	Corte del suministro eléctrico	Amenaza debida a factores externos, a clemencias de tipo naturales como lluvias u otros.	Muy baja	**2**
	I.7	Condiciones inadecuadas de temperatura o humedad	No se cuenta con una infraestructura adecuada para soportar los defectos del sistema de refrigeración.	Muy baja	**2**
	I.11	Emanaciones electromagnéticas	No hay exposición o vulnerabilidad, por parte de esta amenaza.	Muy baja	**2**
ERRORES Y FALLOS NO INTENCIONADOS	**E.2**	Errores del administrador	Pérdida total o parcial del tiempo de ejecución de sus actividades, dependiendo de la gravedad del asunto.	Muy baja	**2**
	E.23	Errores de mantenimiento / actualización de equipos(hardware)	Perjuicio a la mantenibilidad del sistema de información.	Muy baja	**2**
	E.24	Caída del sistema por agotamiento de recursos	Saturación del sistema informático.	Muy baja	**2**
	E.25	Perdida de equipos (Robo)	Recuperación de soportes reciclados o desechados.	Muy baja	**2**
ATAQUES INTENCIONADOS	**A.6**	Abuso de privilegios de acceso	Abuso de cada uno de los derechos otorgados.	Muy baja	**2**
	A.7	Uso no previsto	Implementación de recursos (económicos y de tiempo) en actividades no relacionadas.	Muy baja	**2**

Tabla 56. Estimación de la probabilidad activo switch ALCATEL LUCEN 9543. (Continuación)

	A.11	Acceso no autorizado	Uso ilícito del hardware	Muy baja	**2**
	A.23	Manipulación de los equipos	Sabotaje del hardware y software conteniente.	Muy baja	**2**
	A.24	Denegación de servicio	Saturación del sistema de información.	Muy baja	**2**
	A.25	Robo	Robo de porte de la información, puede esta ser física o digital.	Muy baja	**2**
	A.26	Ataque destructivo	Destrucción de los contenedores de la información, en recipientes físicos y lógicos.	Muy baja	**2**

Fuente: Autoría propia

Tabla 57. Estimación de la probabilidad activo switch ALCATEL LUCEN 9544

ACTIVO TI	SWITCH ALCATEL LUCEN 9544
ADMINISTRADOR	PIMIENTO CARDENAS WILSON MAURICIO
DEGRADACIÓN	60%
IMPACTO	5
TIPO DE ACTIVO	HARDWARE

Tipo	**ID**	**Amenaza**	**Exposición/Vulnerabilidad**	**Frecuencia (F)**	
DESASTRES NATURALES	**N.1**	Fuego	No existe sistema de alarma contra incendios. Se posee un solo extintor de solkaflam (clase c) recomendados para incendios en lugares donde se encuentren equipos eléctricos.	Muy baja	**2**
	N.2	Daños por agua	La infraestructura está expuesta a goteras, cuenta con averías en el techo en donde el agua de las lluvias	Muy baja	**2**

Tabla 57. Estimación de la probabilidad activo switch ALCATEL LUCEN 9544. (Continuación)

	N.*	Desastres naturales	La oficina de la dependencia de sistemas se encuentra en zona baja de riesgo de desastre natural de origen volcánico debido a su cercanía con el volcán nevado del Tolima.	Raro	**1**
DE ORIGEN INDUSTRIAL	**I.1**	Fuego	No existe sistema de alarma contra incendios. Se posee un solo extintor de solkaflam (clase c) recomendados para incendios en lugares donde se encuentren equipos eléctricos.	Muy baja	**2**
	I.2	Daños por agua	La concentración del líquido sobrante por parte del aire acondicionado causaría daños en los equipos.	Muy baja	**2**
	I.*	Desastres industriales	No hay exposición o vulnerabilidad, por parte de esta amenaza.	Muy baja	**2**
	I.3	Contaminación mecánica	No hay exposición o vulnerabilidad, por parte de esta amenaza.	Muy baja	**2**
	I.4	Contaminación electromagnética	No hay exposición o vulnerabilidad, por parte de esta amenaza.	Muy baja	**2**
	I.5	Avería de origen físico o lógico	La manipulación por parte de cada uno de los componentes encontrados en la dependencia, como también por defectos de los componentes desde fabrica	Muy baja	**2**

Tabla 57. Estimación de la probabilidad activo switch ALCATEL LUCEN 9544. (Continuación)

	I.6	Corte del suministro eléctrico	Amenaza debida a factores externos, a clemencias de tipo naturales como lluvias u otros.	Muy baja	**2**
	I.7	Condiciones inadecuadas de temperatura o humedad	No se cuenta con una infraestructura adecuada para soportar los defectos del sistema de refrigeración.	Muy baja	**2**
	I.11	Emanaciones electromagnéticas	No hay exposición o vulnerabilidad, por parte de esta amenaza.	Muy baja	**2**
ERRORES Y FALLOS NO INTENCIONADOS	**E.2**	Errores del administrador	Pérdida total o parcial del tiempo de ejecución de sus actividades, dependiendo de la gravedad del asunto.	Muy baja	**2**
	E.23	Errores de mantenimiento / actualización de equipos(hardware)	Perjuicio a la mantenibilidad del sistema de información.	Muy baja	**2**
	E.24	Caída del sistema por agotamiento de recursos	Saturación del sistema informático.	Muy baja	**2**
	E.25	Perdida de equipos (Robo)	Recuperación de soportes reciclados o desechados.	Muy baja	**2**
ATAQUES INTENCIONADOS	**A.6**	Abuso de privilegios de acceso	Abuso de cada uno de los derechos otorgados.	Muy baja	**2**
	A.7	Uso no previsto	Implementación de recursos (económicos y de tiempo) en actividades no relacionadas.	Muy baja	**2**

Tabla 57. Estimación de la probabilidad activo switch ALCATEL LUCEN 9544. (Continuación)

	A.11	Acceso no autorizado	Uso ilícito del hardware	Muy baja	**2**
	A.23	Manipulación de los equipos	Sabotaje del hardware y software conteniente.	Muy baja	**2**
	A.24	Denegación de servicio	Saturación del sistema de información.	Muy baja	**2**
	A.25	Robo	Robo de porte de la información, puede esta ser física o digital.	Muy baja	**2**
	A.26	Ataque destructivo	Destrucción de los contenedores de la información, en recipientes físicos y lógicos.	Muy baja	**2**

Fuente: Autoría propia

Tabla 58. Estimación de la probabilidad activo switch ALCATEL LUCEN 9545

ACTIVO TI	SWITCH ALCATEL LUCEN 9545
ADMINISTRADOR	PIMIENTO CARDENAS WILSON MAURICIO
DEGRADACIÓN	60%
IMPACTO	5
TIPO DE ACTIVO	HARDWARE

Tipo	**ID**	**Amenaza**	**Exposición/Vulnerabilidad**	**Frecuencia (F)**	
DESASTRES NATURALES	**N.1**	Fuego	No existe sistema de alarma contra incendios. Se posee un solo extintor de solkaflam (clase c) recomendados para incendios en lugares donde se encuentren equipos eléctricos.	Muy baja	**2**
	N.2	Daños por agua	La infraestructura está expuesta a goteras, cuenta con averías en el techo en donde el agua de las lluvias	Muy baja	**2**

Tabla 58. Estimación de la probabilidad activo switch ALCATEL LUCEN 9545. (Continuación)

	N.*	Desastres naturales	La oficina de la dependencia de sistemas se encuentra en zona baja de riesgo de desastre natural de origen volcánico debido a su cercanía con el volcán nevado del Tolima.	Raro	**1**
DE ORIGEN INDUSTRIAL	**I.1**	Fuego	No existe sistema de alarma contra incendios. Se posee un solo extintor de solkaflam (clase c) recomendados para incendios en lugares donde se encuentren equipos eléctricos.	Muy baja	**2**
	I.2	Daños por agua	La concentración del líquido sobrante por parte del aire acondicionado causaría daños en los equipos.	Muy baja	**2**
	I.*	Desastres industriales	No hay exposición o vulnerabilidad, por parte de esta amenaza.	Muy baja	**2**
	I.3	Contaminación mecánica	No hay exposición o vulnerabilidad, por parte de esta amenaza.	Muy baja	**2**
	I.4	Contaminación electromagnética	No hay exposición o vulnerabilidad, por parte de esta amenaza.	Muy baja	**2**
	I.5	Avería de origen físico o lógico	La manipulación por parte de cada uno de los componentes encontrados en la dependencia, como también por defectos de los componentes desde fabrica	Muy baja	**2**

Tabla 58. Estimación de la probabilidad activo switch ALCATEL LUCEN 9545. (Continuación)

	I.6	Corte del suministro eléctrico	Amenaza debida a factores externos, a clemencias de tipo naturales como lluvias u otros.	Muy baja	**2**
	I.7	Condiciones inadecuadas de temperatura o humedad	No se cuenta con una infraestructura adecuada para soportar los defectos del sistema de refrigeración.	Muy baja	**2**
	I.11	Emanaciones electromagnéticas	No hay exposición o vulnerabilidad, por parte de esta amenaza.	Muy baja	**2**
ERRORES Y FALLOS NO INTENCIONADOS	**E.2**	Errores del administrador	Pérdida total o parcial del tiempo de ejecución de sus actividades, dependiendo de la gravedad del asunto.	Muy baja	**2**
	E.23	Errores de mantenimiento / actualización de equipos(hardware)	Perjuicio a la mantenibilidad del sistema de información.	Muy baja	**2**
	E.24	Caída del sistema por agotamiento de recursos	Saturación del sistema informático.	Muy baja	**2**
	E.25	Perdida de equipos (Robo)	Recuperación de soportes reciclados o desechados.	Muy baja	**2**
ATAQUES INTENCIONADOS	**A.6**	Abuso de privilegios de acceso	Abuso de cada uno de los derechos otorgados.	Muy baja	**2**
	A.7	Uso no previsto	Implementación de recursos (económicos y de tiempo) en actividades no relacionadas.	Muy baja	**2**

Tabla 58. Estimación de la probabilidad activo switch ALCATEL LUCEN 9545. (Continuación)

	A.11	Acceso no autorizado	Uso ilícito del hardware	Muy baja	**2**
	A.23	Manipulación de los equipos	Sabotaje del hardware y software conteniente.	Muy baja	**2**
	A.24	Denegación de servicio	Saturación del sistema de información.	Muy baja	**2**
	A.25	Robo	Robo de porte de la información, puede esta ser física o digital.	Muy baja	**2**
	A.26	Ataque destructivo	Destrucción de los contenedores de la información, en recipientes físicos y lógicos.	Muy baja	**2**

Fuente: Autoría propia

Tabla 59. Estimación de la probabilidad activo switch ALCATEL LUCEN 9548

ACTIVO TI	SWITCH ALCATEL LUCEN 9548
ADMINISTRADOR	PIMIENTO CARDENAS WILSON MAURICIO
DEGRADACIÓN	60%
IMPACTO	5
TIPO DE ACTIVO	HARDWARE

Tipo	**ID**	**Amenaza**	**Exposición/Vulnerabilidad**	**Frecuencia (F)**	
DESASTRES NATURALES	**N.1**	Fuego	No existe sistema de alarma contra incendios. Se posee un solo extintor de solkaflam (clase c) recomendados para incendios en lugares donde se encuentren equipos eléctricos.	Muy baja	**2**
	N.2	Daños por agua	La infraestructura está expuesta a goteras, cuenta con averías en el techo en donde el agua de las lluvias	Muy baja	**2**

Tabla 59. Estimación de la probabilidad activo switch ALCATEL LUCEN 9548. (Continuación)

	N.*	Desastres naturales	La oficina de la dependencia de sistemas se encuentra en zona baja de riesgo de desastre natural de origen volcánico debido a su cercanía con el volcán nevado del Tolima.	Raro	**1**
DE ORIGEN INDUSTRIAL	**I.1**	Fuego	No existe sistema de alarma contra incendios. Se posee un solo extintor de solkaflam (clase c) recomendados para incendios en lugares donde se encuentren equipos eléctricos.	Muy baja	**2**
	I.2	Daños por agua	La concentración del líquido sobrante por parte del aire acondicionado causaría daños en los equipos.	Muy baja	**2**
	I.*	Desastres industriales	No hay exposición o vulnerabilidad, por parte de esta amenaza.	Muy baja	**2**
	I.3	Contaminación mecánica	No hay exposición o vulnerabilidad, por parte de esta amenaza.	Muy baja	**2**
	I.4	Contaminación electromagnética	No hay exposición o vulnerabilidad, por parte de esta amenaza.	Muy baja	**2**
	I.5	Avería de origen físico o lógico	La manipulación por parte de cada uno de los componentes encontrados en la dependencia, como también por defectos de los componentes desde fabrica	Muy baja	**2**

Tabla 59. Estimación de la probabilidad activo switch ALCATEL LUCEN 9548. (Continuación)

	I.6	Corte del suministro eléctrico	Amenaza debida a factores externos, a clemencias de tipo naturales como lluvias u otros.	Muy baja	**2**
	I.7	Condiciones inadecuadas de temperatura o humedad	No se cuenta con una infraestructura adecuada para soportar los defectos del sistema de refrigeración.	Muy baja	**2**
	I.11	Emanaciones electromagnéticas	No hay exposición o vulnerabilidad, por parte de esta amenaza.	Muy baja	**2**
ERRORES Y FALLOS NO INTENCIONADOS	**E.2**	Errores del administrador	Pérdida total o parcial del tiempo de ejecución de sus actividades, dependiendo de la gravedad del asunto.	Muy baja	**2**
	E.23	Errores de mantenimiento / actualización de equipos(hardware)	Perjuicio a la mantenibilidad del sistema de información.	Muy baja	**2**
	E.24	Caída del sistema por agotamiento de recursos	Saturación del sistema informático.	Muy baja	**2**
	E.25	Perdida de equipos (Robo)	Recuperación de soportes reciclados o desechados.	Muy baja	**2**
ATAQUES INTENCIONADOS	**A.6**	Abuso de privilegios de acceso	Abuso de cada uno de los derechos otorgados.	Muy baja	**2**
	A.7	Uso no previsto	Implementación de recursos (económicos y de tiempo) en actividades no relacionadas.	Muy baja	**2**

Tabla 59. Estimación de la probabilidad activo switch ALCATEL LUCEN 9548. (Continuación)

	A.11	Acceso no autorizado	Uso ilícito del hardware	Muy baja	**2**
	A.23	Manipulación de los equipos	Sabotaje del hardware y software conteniente.	Muy baja	**2**
	A.24	Denegación de servicio	Saturación del sistema de información.	Muy baja	**2**
	A.25	Robo	Robo de porte de la información, puede esta ser física o digital.	Muy baja	**2**
	A.26	Ataque destructivo	Destrucción de los contenedores de la información, en recipientes físicos y lógicos.	Muy baja	**2**

Fuente: Autoría propia

Tabla 60. Estimación de la probabilidad activo switch ALCATEL LUCEN 9550

ACTIVO TI	SWITCH ALCATEL LUCEN 9550
ADMINISTRADOR	PIMIENTO CARDENAS WILSON MAURICIO
DEGRADACIÓN	60%
IMPACTO	5
TIPO DE ACTIVO	HARDWARE

Tipo	**ID**	**Amenaza**	**Exposición/Vulnerabilidad**	**Frecuencia (F)**	
DESASTRES NATURALES	**N.1**	Fuego	No existe sistema de alarma contra incendios. Se posee un solo extintor de solkaflam (clase c) recomendados para incendios en lugares donde se encuentren equipos eléctricos.	Muy baja	**2**
	N.2	Daños por agua	La infraestructura está expuesta a goteras, cuenta con averías en el techo en donde el agua de las lluvias	Muy baja	**2**

Tabla 60. Estimación de la probabilidad activo switch ALCATEL LUCEN 9550. (Continuación)

	N.*	Desastres naturales	La oficina de la dependencia de sistemas se encuentra en zona baja de riesgo de desastre natural de origen volcánico debido a su cercanía con el volcán nevado del Tolima.	Raro	**1**
DE ORIGEN INDUSTRIAL	**I.1**	Fuego	No existe sistema de alarma contra incendios. Se posee un solo extintor de solkaflam (clase c) recomendados para incendios en lugares donde se encuentren equipos eléctricos.	Muy baja	**2**
	I.2	Daños por agua	La concentración del líquido sobrante por parte del aire acondicionado causaría daños en los equipos.	Muy baja	**2**
	I.*	Desastres industriales	No hay exposición o vulnerabilidad, por parte de esta amenaza.	Muy baja	**2**
	I.3	Contaminación mecánica	No hay exposición o vulnerabilidad, por parte de esta amenaza.	Muy baja	**2**
	I.4	Contaminación electromagnética	No hay exposición o vulnerabilidad, por parte de esta amenaza.	Muy baja	**2**
	I.5	Avería de origen físico o lógico	La manipulación por parte de cada uno de los componentes encontrados en la dependencia, como también por defectos de los componentes desde fabrica	Muy baja	**2**

Tabla 60. Estimación de la probabilidad activo switch ALCATEL LUCEN 9550. (Continuación)

	I.6	Corte del suministro eléctrico	Amenaza debida a factores externos, a clemencias de tipo naturales como lluvias u otros.	Muy baja	**2**
	I.7	Condiciones inadecuadas de temperatura o humedad	No se cuenta con una infraestructura adecuada para soportar los defectos del sistema de refrigeración.	Muy baja	**2**
	I.11	Emanaciones electromagnéticas	No hay exposición o vulnerabilidad, por parte de esta amenaza.	Muy baja	**2**
ERRORES Y FALLOS NO INTENCIONADOS	**E.2**	Errores del administrador	Pérdida total o parcial del tiempo de ejecución de sus actividades, dependiendo de la gravedad del asunto.	Muy baja	**2**
	E.23	Errores de mantenimiento / actualización de equipos(hardware)	Perjuicio a la mantenibilidad del sistema de información.	Muy baja	**2**
	E.24	Caída del sistema por agotamiento de recursos	Saturación del sistema informático.	Muy baja	**2**
	E.25	Perdida de equipos (Robo)	Recuperación de soportes reciclados o desechados.	Muy baja	**2**
ATAQUES INTENCIONADOS	**A.6**	Abuso de privilegios de acceso	Abuso de cada uno de los derechos otorgados.	Muy baja	**2**
	A.7	Uso no previsto	Implementación de recursos (económicos y de tiempo) en actividades no relacionadas.	Muy baja	**2**

Tabla 60. Estimación de la probabilidad activo switch ALCATEL LUCEN 9550. (Continuación)

	A.11	Acceso no autorizado	Uso ilícito del hardware	Muy baja	**2**
	A.23	Manipulación de los equipos	Sabotaje del hardware y software conteniente.	Muy baja	**2**
	A.24	Denegación de servicio	Saturación del sistema de información.	Muy baja	**2**
	A.25	Robo	Robo de porte de la información, puede esta ser física o digital.	Muy baja	**2**
	A.26	Ataque destructivo	Destrucción de los contenedores de la información, en recipientes físicos y lógicos.	Muy baja	**2**

Fuente: Autoría propia

Tabla 61. Estimación de la probabilidad activo switch ALCATEL LUCEN 9551

ACTIVO TI	SWITCH ALCATEL LUCEN 9551
ADMINISTRADOR	PIMIENTO CARDENAS WILSON MAURICIO
DEGRADACIÓN	60%
IMPACTO	5
TIPO DE ACTIVO	HARDWARE

Tipo	**ID**	**Amenaza**	**Exposición/Vulnerabilidad**	**Frecuencia (F)**	
DESASTRES NATURALES	**N.1**	Fuego	No existe sistema de alarma contra incendios. Se posee un solo extintor de solkaflam (clase c) recomendados para incendios en lugares donde se encuentren equipos eléctricos.	Muy baja	**2**
	N.2	Daños por agua	La infraestructura está expuesta a goteras, cuenta con averías en el techo en donde el agua de las lluvias	Muy baja	**2**

Tabla 61. Estimación de la probabilidad activo switch ALCATEL LUCEN 9551. (Continuación)

	N.*	Desastres naturales	La oficina de la dependencia de sistemas se encuentra en zona baja de riesgo de desastre natural de origen volcánico debido a su cercanía con el volcán nevado del Tolima.	Raro	**1**
DE ORIGEN INDUSTRIAL	**I.1**	Fuego	No existe sistema de alarma contra incendios. Se posee un solo extintor de solkaflam (clase c) recomendados para incendios en lugares donde se encuentren equipos eléctricos.	Muy baja	**2**
	I.2	Daños por agua	La concentración del líquido sobrante por parte del aire acondicionado causaría daños en los equipos.	Muy baja	**2**
	I.*	Desastres industriales	No hay exposición o vulnerabilidad, por parte de esta amenaza.	Muy baja	**2**
	I.3	Contaminación mecánica	No hay exposición o vulnerabilidad, por parte de esta amenaza.	Muy baja	**2**
	I.4	Contaminación electromagnética	No hay exposición o vulnerabilidad, por parte de esta amenaza.	Muy baja	**2**
	I.5	Avería de origen físico o lógico	La manipulación por parte de cada uno de los componentes encontrados en la dependencia, como también por defectos de los componentes desde fabrica	Muy baja	**2**

Tabla 61. Estimación de la probabilidad activo switch ALCATEL LUCEN 9551. (Continuación)

	I.6	Corte del suministro eléctrico	Amenaza debida a factores externos, a clemencias de tipo naturales como lluvias u otros.	Muy baja	**2**
	I.7	Condiciones inadecuadas de temperatura o humedad	No se cuenta con una infraestructura adecuada para soportar los defectos del sistema de refrigeración.	Muy baja	**2**
	I.11	Emanaciones electromagnéticas	No hay exposición o vulnerabilidad, por parte de esta amenaza.	Muy baja	**2**
ERRORES Y FALLOS NO INTENCIONADOS	**E.2**	Errores del administrador	Pérdida total o parcial del tiempo de ejecución de sus actividades, dependiendo de la gravedad del asunto.	Muy baja	**2**
	E.23	Errores de mantenimiento / actualización de equipos(hardware)	Perjuicio a la mantenibilidad del sistema de información.	Muy baja	**2**
	E.24	Caída del sistema por agotamiento de recursos	Saturación del sistema informático.	Muy baja	**2**
	E.25	Perdida de equipos (Robo)	Recuperación de soportes reciclados o desechados.	Muy baja	**2**
ATAQUES INTENCIONADOS	**A.6**	Abuso de privilegios de acceso	Abuso de cada uno de los derechos otorgados.	Muy baja	**2**
	A.7	Uso no previsto	Implementación de recursos (económicos y de tiempo) en actividades no relacionadas.	Muy baja	**2**

Tabla 61. Estimación de la probabilidad activo switch ALCATEL LUCEN 9551. (Continuación)

	A.11	Acceso no autorizado	Uso ilícito del hardware	Muy baja	**2**
	A.23	Manipulación de los equipos	Sabotaje del hardware y software conteniente.	Muy baja	**2**
	A.24	Denegación de servicio	Saturación del sistema de información.	Muy baja	**2**
	A.25	Robo	Robo de porte de la información, puede esta ser física o digital.	Muy baja	**2**
	A.26	Ataque destructivo	Destrucción de los contenedores de la información, en recipientes físicos y lógicos.	Muy baja	**2**

Fuente: Autoría propia

Tabla 62. Estimación de la probabilidad activo switch ALCATEL LUCEN 9552

ACTIVO TI	SWITCH ALCATEL LUCEN 9552
ADMINISTRADOR	PIMIENTO CARDENAS WILSON MAURICIO
DEGRADACIÓN	60%
IMPACTO	5
TIPO DE ACTIVO	HARDWARE

Tipo	**ID**	**Amenaza**	**Exposición/Vulnerabilidad**	**Frecuencia (F)**	
DESASTRES NATURALES	**N.1**	Fuego	No existe sistema de alarma contra incendios. Se posee un solo extintor de solkaflam (clase c) recomendados para incendios en lugares donde se encuentren equipos eléctricos.	Muy baja	**2**
	N.2	Daños por agua	La infraestructura está expuesta a goteras, cuenta con averías en el techo en donde el agua de las lluvias	Muy baja	**2**

Tabla 62. Estimación de la probabilidad activo switch ALCATEL LUCEN 9552. (Continuación)

	N.*	Desastres naturales	La oficina de la dependencia de sistemas se encuentra en zona baja de riesgo de desastre natural de origen volcánico debido a su cercanía con el volcán nevado del Tolima.	Raro	**1**
DE ORIGEN INDUSTRIAL	**I.1**	Fuego	No existe sistema de alarma contra incendios. Se posee un solo extintor de solkaflam (clase c) recomendados para incendios en lugares donde se encuentren equipos eléctricos.	Muy baja	**2**
	I.2	Daños por agua	La concentración del líquido sobrante por parte del aire acondicionado causaría daños en los equipos.	Muy baja	**2**
	I.*	Desastres industriales	No hay exposición o vulnerabilidad, por parte de esta amenaza.	Muy baja	**2**
	I.3	Contaminación mecánica	No hay exposición o vulnerabilidad, por parte de esta amenaza.	Muy baja	**2**
	I.4	Contaminación electromagnética	No hay exposición o vulnerabilidad, por parte de esta amenaza.	Muy baja	**2**
	I.5	Avería de origen físico o lógico	La manipulación por parte de cada uno de los componentes encontrados en la dependencia, como también por defectos de los componentes desde fabrica	Muy baja	**2**

Tabla 62. Estimación de la probabilidad activo switch ALCATEL LUCEN 9552. (Continuación)

	I.6	Corte del suministro eléctrico	Amenaza debida a factores externos, a clemencias de tipo naturales como lluvias u otros.	Muy baja	**2**
	I.7	Condiciones inadecuadas de temperatura o humedad	No se cuenta con una infraestructura adecuada para soportar los defectos del sistema de refrigeración.	Muy baja	**2**
	I.11	Emanaciones electromagnéticas	No hay exposición o vulnerabilidad, por parte de esta amenaza.	Muy baja	**2**
ERRORES Y FALLOS NO INTENCIONADOS	**E.2**	Errores del administrador	Pérdida total o parcial del tiempo de ejecución de sus actividades, dependiendo de la gravedad del asunto.	Muy baja	**2**
	E.23	Errores de mantenimiento / actualización de equipos(hardware)	Perjuicio a la mantenibilidad del sistema de información.	Muy baja	**2**
	E.24	Caída del sistema por agotamiento de recursos	Saturación del sistema informático.	Muy baja	**2**
	E.25	Perdida de equipos (Robo)	Recuperación de soportes reciclados o desechados.	Muy baja	**2**
ATAQUES INTENCIONADOS	**A.6**	Abuso de privilegios de acceso	Abuso de cada uno de los derechos otorgados.	Muy baja	**2**
	A.7	Uso no previsto	Implementación de recursos (económicos y de tiempo) en actividades no relacionadas.	Muy baja	**2**

Tabla 62. Estimación de la probabilidad activo switch ALCATEL LUCEN 9552. (Continuación)

	A.11	Acceso no autorizado	Uso ilícito del hardware	Muy baja	**2**
	A.23	Manipulación de los equipos	Sabotaje del hardware y software conteniente.	Muy baja	**2**
	A.24	Denegación de servicio	Saturación del sistema de información.	Muy baja	**2**
	A.25	Robo	Robo de porte de la información, puede esta ser física o digital.	Muy baja	**2**
	A.26	Ataque destructivo	Destrucción de los contenedores de la información, en recipientes físicos y lógicos.	Muy baja	**2**

Fuente: Autoría propia

Tabla 63. Estimación de la probabilidad activo switch ALCATEL LUCEN 9554

ACTIVO TI	SWITCH ALCATEL LUCEN 9554
ADMINISTRADOR	PIMIENTO CARDENAS WILSON MAURICIO
DEGRADACIÓN	60%
IMPACTO	5
TIPO DE ACTIVO	HARDWARE

Tipo	**ID**	**Amenaza**	**Exposición/Vulnerabilidad**	**Frecuencia (F)**	
DESASTRES NATURALES	**N.1**	Fuego	No existe sistema de alarma contra incendios. Se posee un solo extintor de solkaflam (clase c) recomendados para incendios en lugares donde se encuentren equipos eléctricos.	Muy baja	**2**
	N.2	Daños por agua	La infraestructura está expuesta a goteras, cuenta con averías en el techo en donde el agua de las lluvias	Muy baja	**2**

Tabla 63. Estimación de la probabilidad activo switch ALCATEL LUCEN 9554. (Continuación)

	N.*	Desastres naturales	La oficina de la dependencia de sistemas se encuentra en zona baja de riesgo de desastre natural de origen volcánico debido a su cercanía con el volcán nevado del Tolima.	Raro	**1**
DE ORIGEN INDUSTRIAL	**I.1**	Fuego	No existe sistema de alarma contra incendios. Se posee un solo extintor de solkaflam (clase c) recomendados para incendios en lugares donde se encuentren equipos eléctricos.	Muy baja	**2**
	I.2	Daños por agua	La concentración del líquido sobrante por parte del aire acondicionado causaría daños en los equipos.	Muy baja	**2**
	I.*	Desastres industriales	No hay exposición o vulnerabilidad, por parte de esta amenaza.	Muy baja	**2**
	I.3	Contaminación mecánica	No hay exposición o vulnerabilidad, por parte de esta amenaza.	Muy baja	**2**
	I.4	Contaminación electromagnética	No hay exposición o vulnerabilidad, por parte de esta amenaza.	Muy baja	**2**
	I.5	Avería de origen físico o lógico	La manipulación por parte de cada uno de los componentes encontrados en la dependencia, como también por defectos de los componentes desde fabrica	Muy baja	**2**

Tabla 63. Estimación de la probabilidad activo switch ALCATEL LUCEN 9554. (Continuación)

	I.6	Corte del suministro eléctrico	Amenaza debida a factores externos, a clemencias de tipo naturales como lluvias u otros.	Muy baja	**2**
	I.7	Condiciones inadecuadas de temperatura o humedad	No se cuenta con una infraestructura adecuada para soportar los defectos del sistema de refrigeración.	Muy baja	**2**
	I.11	Emanaciones electromagnéticas	No hay exposición o vulnerabilidad, por parte de esta amenaza.	Muy baja	**2**
ERRORES Y FALLOS NO INTENCIONADOS	**E.2**	Errores del administrador	Pérdida total o parcial del tiempo de ejecución de sus actividades, dependiendo de la gravedad del asunto.	Muy baja	**2**
	E.23	Errores de mantenimiento / actualización de equipos(hardware)	Perjuicio a la mantenibilidad del sistema de información.	Muy baja	**2**
	E.24	Caída del sistema por agotamiento de recursos	Saturación del sistema informático.	Muy baja	**2**
	E.25	Perdida de equipos (Robo)	Recuperación de soportes reciclados o desechados.	Muy baja	**2**
ATAQUES INTENCIONADOS	**A.6**	Abuso de privilegios de acceso	Abuso de cada uno de los derechos otorgados.	Muy baja	**2**
	A.7	Uso no previsto	Implementación de recursos (económicos y de tiempo) en actividades no relacionadas.	Muy baja	**2**

Tabla 63. Estimación de la probabilidad activo switch ALCATEL LUCEN 9554. (Continuación)

	A.11	Acceso no autorizado	Uso ilícito del hardware	Muy baja	**2**
	A.23	Manipulación de los equipos	Sabotaje del hardware y software conteniente.	Muy baja	**2**
	A.24	Denegación de servicio	Saturación del sistema de información.	Muy baja	**2**
	A.25	Robo	Robo de porte de la información, puede esta ser física o digital.	Muy baja	**2**
	A.26	Ataque destructivo	Destrucción de los contenedores de la información, en recipientes físicos y lógicos.	Muy baja	**2**

Fuente: Autoría propia

Tabla 64. Estimación de la probabilidad activo switch ALCATEL LUCEN 9555

ACTIVO TI	SWITCH ALCATEL LUCEN 9555
ADMINISTRADOR	PIMIENTO CARDENAS WILSON MAURICIO
DEGRADACIÓN	60%
IMPACTO	5
TIPO DE ACTIVO	HARDWARE

Tipo	**ID**	**Amenaza**	**Exposición/Vulnerabilidad**	**Frecuencia (F)**	
DESASTRES NATURALES	**N.1**	Fuego	No existe sistema de alarma contra incendios. Se posee un solo extintor de solkaflam (clase c) recomendados para incendios en lugares donde se encuentren equipos eléctricos.	Muy baja	**2**
	N.2	Daños por agua	La infraestructura está expuesta a goteras, cuenta con averías en el techo en donde el agua de las lluvias	Muy baja	**2**

Tabla 64. Estimación de la probabilidad activo switch ALCATEL LUCEN 9555. (Continuación)

	N.*	Desastres naturales	La oficina de la dependencia de sistemas se encuentra en zona baja de riesgo de desastre natural de origen volcánico debido a su cercanía con el volcán nevado del Tolima.	Raro	**1**
DE ORIGEN INDUSTRIAL	**I.1**	Fuego	No existe sistema de alarma contra incendios. Se posee un solo extintor de solkaflam (clase c) recomendados para incendios en lugares donde se encuentren equipos eléctricos.	Muy baja	**2**
	I.2	Daños por agua	La concentración del líquido sobrante por parte del aire acondicionado causaría daños en los equipos.	Muy baja	**2**
	I.*	Desastres industriales	No hay exposición o vulnerabilidad, por parte de esta amenaza.	Muy baja	**2**
	I.3	Contaminación mecánica	No hay exposición o vulnerabilidad, por parte de esta amenaza.	Muy baja	**2**
	I.4	Contaminación electromagnética	No hay exposición o vulnerabilidad, por parte de esta amenaza.	Muy baja	**2**
	I.5	Avería de origen físico o lógico	La manipulación por parte de cada uno de los componentes encontrados en la dependencia, como también por defectos de los componentes desde fabrica	Muy baja	**2**

Tabla 64. Estimación de la probabilidad activo switch ALCATEL LUCEN 9555. (Continuación)

	I.6	Corte del suministro eléctrico	Amenaza debida a factores externos, a clemencias de tipo naturales como lluvias u otros.	Muy baja	**2**
	I.7	Condiciones inadecuadas de temperatura o humedad	No se cuenta con una infraestructura adecuada para soportar los defectos del sistema de refrigeración.	Muy baja	**2**
	I.11	Emanaciones electromagnéticas	No hay exposición o vulnerabilidad, por parte de esta amenaza.	Muy baja	**2**
ERRORES Y FALLOS NO INTENCIONADOS	**E.2**	Errores del administrador	Pérdida total o parcial del tiempo de ejecución de sus actividades, dependiendo de la gravedad del asunto.	Muy baja	**2**
	E.23	Errores de mantenimiento / actualización de equipos(hardware)	Perjuicio a la mantenibilidad del sistema de información.	Muy baja	**2**
	E.24	Caída del sistema por agotamiento de recursos	Saturación del sistema informático.	Muy baja	**2**
	E.25	Perdida de equipos (Robo)	Recuperación de soportes reciclados o desechados.	Muy baja	**2**
ATAQUES INTENCIONADOS	**A.6**	Abuso de privilegios de acceso	Abuso de cada uno de los derechos otorgados.	Muy baja	**2**
	A.7	Uso no previsto	Implementación de recursos (económicos y de tiempo) en actividades no relacionadas.	Muy baja	**2**

Tabla 64. Estimación de la probabilidad activo switch ALCATEL LUCEN 9555. (Continuación)

	A.11	Acceso no autorizado	Uso ilícito del hardware	Muy baja	**2**
	A.23	Manipulación de los equipos	Sabotaje del hardware y software conteniente.	Muy baja	**2**
	A.24	Denegación de servicio	Saturación del sistema de información.	Muy baja	**2**
	A.25	Robo	Robo de porte de la información, puede esta ser física o digital.	Muy baja	**2**
	A.26	Ataque destructivo	Destrucción de los contenedores de la información, en recipientes físicos y lógicos.	Muy baja	**2**

Fuente: Autoría propia

Tabla 65. Estimación de la probabilidad activo switch ALCATEL LUCEN 9560

ACTIVO TI	SWITCH ALCATEL LUCEN 9560
ADMINISTRADOR	PIMIENTO CARDENAS WILSON MAURICIO
DEGRADACIÓN	60%
IMPACTO	5
TIPO DE ACTIVO	HARDWARE

Tipo	**ID**	**Amenaza**	**Exposición/Vulnerabilidad**	**Frecuencia (F)**	
DESASTRES NATURALES	**N.1**	Fuego	No existe sistema de alarma contra incendios. Se posee un solo extintor de solkaflam (clase c) recomendados para incendios en lugares donde se encuentren equipos eléctricos.	Muy baja	**2**
	N.2	Daños por agua	La infraestructura está expuesta a goteras, cuenta con averías en el techo en donde el agua de las lluvias	Muy baja	**2**

Tabla 65. Estimación de la probabilidad activo switch ALCATEL LUCEN 9560. (Continuación)

	N.*	Desastres naturales	La oficina de la dependencia de sistemas se encuentra en zona baja de riesgo de desastre natural de origen volcánico debido a su cercanía con el volcán nevado del Tolima.	Raro	**1**
DE ORIGEN INDUSTRIAL	**I.1**	Fuego	No existe sistema de alarma contra incendios. Se posee un solo extintor de solkaflam (clase c) recomendados para incendios en lugares donde se encuentren equipos eléctricos.	Muy baja	**2**
	I.2	Daños por agua	La concentración del líquido sobrante por parte del aire acondicionado causaría daños en los equipos.	Muy baja	**2**
	I.*	Desastres industriales	No hay exposición o vulnerabilidad, por parte de esta amenaza.	Muy baja	**2**
	I.3	Contaminación mecánica	No hay exposición o vulnerabilidad, por parte de esta amenaza.	Muy baja	**2**
	I.4	Contaminación electromagnética	No hay exposición o vulnerabilidad, por parte de esta amenaza.	Muy baja	**2**
	I.5	Avería de origen físico o lógico	La manipulación por parte de cada uno de los componentes encontrados en la dependencia, como también por defectos de los componentes desde fabrica	Muy baja	**2**

Tabla 65. Estimación de la probabilidad activo switch ALCATEL LUCEN 9560. (Continuación)

	I.6	Corte del suministro eléctrico	Amenaza debida a factores externos, a clemencias de tipo naturales como lluvias u otros.	Muy baja	**2**
	I.7	Condiciones inadecuadas de temperatura o humedad	No se cuenta con una infraestructura adecuada para soportar los defectos del sistema de refrigeración.	Muy baja	**2**
	I.11	Emanaciones electromagnéticas	No hay exposición o vulnerabilidad, por parte de esta amenaza.	Muy baja	**2**
ERRORES Y FALLOS NO INTENCIONADOS	**E.2**	Errores del administrador	Pérdida total o parcial del tiempo de ejecución de sus actividades, dependiendo de la gravedad del asunto.	Muy baja	**2**
	E.23	Errores de mantenimiento / actualización de equipos(hardware)	Perjuicio a la mantenibilidad del sistema de información.	Muy baja	**2**
	E.24	Caída del sistema por agotamiento de recursos	Saturación del sistema informático.	Muy baja	**2**
	E.25	Perdida de equipos (Robo)	Recuperación de soportes reciclados o desechados.	Muy baja	**2**
ATAQUES INTENCIONADOS	**A.6**	Abuso de privilegios de acceso	Abuso de cada uno de los derechos otorgados.	Muy baja	**2**
	A.7	Uso no previsto	Implementación de recursos (económicos y de tiempo) en actividades no relacionadas.	Muy baja	**2**

Tabla 65. Estimación de la probabilidad activo switch ALCATEL LUCEN 9560. (Continuación)

	A.11	Acceso no autorizado	Uso ilícito del hardware	Muy baja	**2**
	A.23	Manipulación de los equipos	Sabotaje del hardware y software conteniente.	Muy baja	**2**
	A.24	Denegación de servicio	Saturación del sistema de información.	Muy baja	**2**
	A.25	Robo	Robo de porte de la información, puede esta ser física o digital.	Muy baja	**2**
	A.26	Ataque destructivo	Destrucción de los contenedores de la información, en recipientes físicos y lógicos.	Muy baja	**2**

Fuente: Autoría propia

Tabla 66. Estimación de la probabilidad activo switch layer 3 9574

ACTIVO TI	SWITCH LAYER 3 9574
ADMINISTRADOR	PIMIENTO CARDENAS WILSON MAURICIO
DEGRADACIÓN	60%
IMPACTO	5
TIPO DE ACTIVO	HARDWARE

Tipo	**ID**	**Amenaza**	**Exposición/Vulnerabilidad**	**Frecuencia (F)**	
DESASTRES NATURALES	**N.1**	Fuego	No existe sistema de alarma contra incendios. Se posee un solo extintor de solkaflam (clase c) recomendados para incendios en lugares donde se encuentren equipos eléctricos.	Muy baja	**2**
	N.2	Daños por agua	La infraestructura está expuesta a goteras, cuenta con averías en el techo en donde el agua de las lluvias	Muy baja	**2**

Tabla 66. Estimación de la probabilidad activo switch layer 3 9574. (Continuación)

	N.*	Desastres naturales	La oficina de la dependencia de sistemas se encuentra en zona baja de riesgo de desastre natural de origen volcánico debido a su cercanía con el volcán nevado del Tolima.	Raro	**1**
DE ORIGEN INDUSTRIAL	**I.1**	Fuego	No existe sistema de alarma contra incendios. Se posee un solo extintor de solkaflam (clase c) recomendados para incendios en lugares donde se encuentren equipos eléctricos.	Muy baja	**2**
	I.2	Daños por agua	La concentración del líquido sobrante por parte del aire acondicionado causaría daños en los equipos.	Muy baja	**2**
	I.*	Desastres industriales	No hay exposición o vulnerabilidad, por parte de esta amenaza.	Muy baja	**2**
	I.3	Contaminación mecánica	No hay exposición o vulnerabilidad, por parte de esta amenaza.	Muy baja	**2**
	I.4	Contaminación electromagnética	No hay exposición o vulnerabilidad, por parte de esta amenaza.	Muy baja	**2**
	I.5	Avería de origen físico o lógico	La manipulación por parte de cada uno de los componentes encontrados en la dependencia, como también por defectos de los componentes desde fabrica	Muy baja	**2**

Tabla 66. Estimación de la probabilidad activo switch layer 3 9574. (Continuación)

	I.6	Corte del suministro eléctrico	Amenaza debida a factores externos, a clemencias de tipo naturales como lluvias u otros.	Muy baja	**2**
	I.7	Condiciones inadecuadas de temperatura o humedad	No se cuenta con una infraestructura adecuada para soportar los defectos del sistema de refrigeración.	Muy baja	**2**
	I.11	Emanaciones electromagnéticas	No hay exposición o vulnerabilidad, por parte de esta amenaza.	Muy baja	**2**
ERRORES Y FALLOS NO INTENCIONADOS	**E.2**	Errores del administrador	Pérdida total o parcial del tiempo de ejecución de sus actividades, dependiendo de la gravedad del asunto.	Muy baja	**2**
	E.23	Errores de mantenimiento / actualización de equipos(hardware)	Perjuicio a la mantenibilidad del sistema de información.	Muy baja	**2**
	E.24	Caída del sistema por agotamiento de recursos	Saturación del sistema informático.	Muy baja	**2**
	E.25	Perdida de equipos (Robo)	Recuperación de soportes reciclados o desechados.	Muy baja	**2**
ATAQUES INTENCIONADOS	**A.6**	Abuso de privilegios de acceso	Abuso de cada uno de los derechos otorgados.	Muy baja	**2**
	A.7	Uso no previsto	Implementación de recursos (económicos y de tiempo) en actividades no relacionadas.	Muy baja	**2**

Tabla 66. Estimación de la probabilidad activo switch layer 3 9574. (Continuación)

	A.11	Acceso no autorizado	Uso ilícito del hardware	Muy baja	**2**
	A.23	Manipulación de los equipos	Sabotaje del hardware y software conteniente.	Muy baja	**2**
	A.24	Denegación de servicio	Saturación del sistema de información.	Muy baja	**2**
	A.25	Robo	Robo de porte de la información, puede esta ser física o digital.	Muy baja	**2**
	A.26	Ataque destructivo	Destrucción de los contenedores de la información, en recipientes físicos y lógicos.	Muy baja	**2**

Fuente: Autoría propia

Tabla 67. Estimación de la probabilidad activo switch layer 3 9576

ACTIVO TI	SWITCH LAYER 3 9576
ADMINISTRADOR	PIMIENTO CARDENAS WILSON MAURICIO
DEGRADACIÓN	60%
IMPACTO	5
TIPO DE ACTIVO	HARDWARE

Tipo	**ID**	**Amenaza**	**Exposición/Vulnerabilidad**	**Frecuencia (F)**	
DESASTRES NATURALES	**N.1**	Fuego	No existe sistema de alarma contra incendios. Se posee un solo extintor de solkaflam (clase c) recomendados para incendios en lugares donde se encuentren equipos eléctricos.	Muy baja	**2**
	N.2	Daños por agua	La infraestructura está expuesta a goteras, cuenta con averías en el techo en donde el agua de las lluvias	Muy baja	**2**

Tabla 67. Estimación de la probabilidad activo switch layer 3 9576. (Continuación)

	N.*	Desastres naturales	La oficina de la dependencia de sistemas se encuentra en zona baja de riesgo de desastre natural de origen volcánico debido a su cercanía con el volcán nevado del Tolima.	Raro	**1**
DE ORIGEN INDUSTRIAL	**I.1**	Fuego	No existe sistema de alarma contra incendios. Se posee un solo extintor de solkaflam (clase c) recomendados para incendios en lugares donde se encuentren equipos eléctricos.	Muy baja	**2**
	I.2	Daños por agua	La concentración del líquido sobrante por parte del aire acondicionado causaría daños en los equipos.	Muy baja	**2**
	I.*	Desastres industriales	No hay exposición o vulnerabilidad, por parte de esta amenaza.	Muy baja	**2**
	I.3	Contaminación mecánica	No hay exposición o vulnerabilidad, por parte de esta amenaza.	Muy baja	**2**
	I.4	Contaminación electromagnética	No hay exposición o vulnerabilidad, por parte de esta amenaza.	Muy baja	**2**
	I.5	Avería de origen físico o lógico	La manipulación por parte de cada uno de los componentes encontrados en la dependencia, como también por defectos de los componentes desde fabrica	Muy baja	**2**

Tabla 67. Estimación de la probabilidad activo switch layer 3 9576. (Continuación)

	I.6	Corte del suministro eléctrico	Amenaza debida a factores externos, a clemencias de tipo naturales como lluvias u otros.	Muy baja	**2**
	I.7	Condiciones inadecuadas de temperatura o humedad	No se cuenta con una infraestructura adecuada para soportar los defectos del sistema de refrigeración.	Muy baja	**2**
	I.11	Emanaciones electromagnéticas	No hay exposición o vulnerabilidad, por parte de esta amenaza.	Muy baja	**2**
ERRORES Y FALLOS NO INTENCIONADOS	**E.2**	Errores del administrador	Pérdida total o parcial del tiempo de ejecución de sus actividades, dependiendo de la gravedad del asunto.	Muy baja	**2**
	E.23	Errores de mantenimiento / actualización de equipos(hardware)	Perjuicio a la mantenibilidad del sistema de información.	Muy baja	**2**
	E.24	Caída del sistema por agotamiento de recursos	Saturación del sistema informático.	Muy baja	**2**
	E.25	Perdida de equipos (Robo)	Recuperación de soportes reciclados o desechados.	Muy baja	**2**
ATAQUES INTENCIONADOS	**A.6**	Abuso de privilegios de acceso	Abuso de cada uno de los derechos otorgados.	Muy baja	**2**
	A.7	Uso no previsto	Implementación de recursos (económicos y de tiempo) en actividades no relacionadas.	Muy baja	**2**

Tabla 67. Estimación de la probabilidad activo switch layer 3 9576. (Continuación)

	A.11	Acceso no autorizado	Uso ilícito del hardware	Muy baja	**2**
	A.23	Manipulación de los equipos	Sabotaje del hardware y software conteniente.	Muy baja	**2**
	A.24	Denegación de servicio	Saturación del sistema de información.	Muy baja	**2**
	A.25	Robo	Robo de porte de la información, puede esta ser física o digital.	Muy baja	**2**
	A.26	Ataque destructivo	Destrucción de los contenedores de la información, en recipientes físicos y lógicos.	Muy baja	**2**

Fuente: Autoría propia

Tabla 68. Estimación de la probabilidad activo switch layer 3 9577

ACTIVO TI	SWITCH LAYER 3 9577
ADMINISTRADOR	PIMIENTO CARDENAS WILSON MAURICIO
DEGRADACIÓN	60%
IMPACTO	5
TIPO DE ACTIVO	HARDWARE

Tipo	**ID**	**Amenaza**	**Exposición/Vulnerabilidad**	**Frecuencia (F)**	
DESASTRES NATURALES	**N.1**	Fuego	No existe sistema de alarma contra incendios. Se posee un solo extintor de solkaflam (clase c) recomendados para incendios en lugares donde se encuentren equipos eléctricos.	Muy baja	**2**
	N.2	Daños por agua	La infraestructura está expuesta a goteras, cuenta con averías en el techo en donde el agua de las lluvias	Muy baja	**2**

Tabla 68. Estimación de la probabilidad activo switch layer 3 9577. (Continuación)

	N.*	Desastres naturales	La oficina de la dependencia de sistemas se encuentra en zona baja de riesgo de desastre natural de origen volcánico debido a su cercanía con el volcán nevado del Tolima.	Raro	**1**
DE ORIGEN INDUSTRIAL	**I.1**	Fuego	No existe sistema de alarma contra incendios. Se posee un solo extintor de solkaflam (clase c) recomendados para incendios en lugares donde se encuentren equipos eléctricos.	Muy baja	**2**
	I.2	Daños por agua	La concentración del líquido sobrante por parte del aire acondicionado causaría daños en los equipos.	Muy baja	**2**
	I.*	Desastres industriales	No hay exposición o vulnerabilidad, por parte de esta amenaza.	Muy baja	**2**
	I.3	Contaminación mecánica	No hay exposición o vulnerabilidad, por parte de esta amenaza.	Muy baja	**2**
	I.4	Contaminación electromagnética	No hay exposición o vulnerabilidad, por parte de esta amenaza.	Muy baja	**2**
	I.5	Avería de origen físico o lógico	La manipulación por parte de cada uno de los componentes encontrados en la dependencia, como también por defectos de los componentes desde fabrica	Muy baja	**2**

Tabla 68. Estimación de la probabilidad activo switch layer 3 9577. (Continuación)

	I.6	Corte del suministro eléctrico	Amenaza debida a factores externos, a clemencias de tipo naturales como lluvias u otros.	Muy baja	**2**
	I.7	Condiciones inadecuadas de temperatura o humedad	No se cuenta con una infraestructura adecuada para soportar los defectos del sistema de refrigeración.	Muy baja	**2**
	I.11	Emanaciones electromagnéticas	No hay exposición o vulnerabilidad, por parte de esta amenaza.	Muy baja	**2**
ERRORES Y FALLOS NO INTENCIONADOS	**E.2**	Errores del administrador	Pérdida total o parcial del tiempo de ejecución de sus actividades, dependiendo de la gravedad del asunto.	Muy baja	**2**
	E.23	Errores de mantenimiento / actualización de equipos(hardware)	Perjuicio a la mantenibilidad del sistema de información.	Muy baja	**2**
	E.24	Caída del sistema por agotamiento de recursos	Saturación del sistema informático.	Muy baja	**2**
	E.25	Perdida de equipos (Robo)	Recuperación de soportes reciclados o desechados.	Muy baja	**2**
ATAQUES INTENCIONADOS	**A.6**	Abuso de privilegios de acceso	Abuso de cada uno de los derechos otorgados.	Muy baja	**2**
	A.7	Uso no previsto	Implementación de recursos (económicos y de tiempo) en actividades no relacionadas.	Muy baja	**2**

Tabla 68. Estimación de la probabilidad activo switch layer 3 9577. (Continuación)

	A.11	Acceso no autorizado	Uso ilícito del hardware	Muy baja	**2**
	A.23	Manipulación de los equipos	Sabotaje del hardware y software conteniente.	Muy baja	**2**
	A.24	Denegación de servicio	Saturación del sistema de información.	Muy baja	**2**
	A.25	Robo	Robo de porte de la información, puede esta ser física o digital.	Muy baja	**2**
	A.26	Ataque destructivo	Destrucción de los contenedores de la información, en recipientes físicos y lógicos.	Muy baja	**2**

Fuente: Autoría propia

ANEXO 5

CONTENIDO

LISTA DE TABLAS

1. CONTINUACIÓN DE LA ESTIMACIÓN DE LA PROBABILIDAD DE QUE OCURRA PERDIDA DEL ACTIVO

Tabla 1. Estimación de la probabilidad activo *switch layer* 3 9575

ACTIVO TI	**SWITCH LAYER 3 9575**
ADMINISTRADOR	PIMIENTO CARDENAS WILSON MAURICIO
DEGRADACIÓN	60%
IMPACTO	5
TIPO DE ACTIVO	HARDWARE

Tipo	ID	Amenaza	Exposición/Vulnerabilidad	Frecuencia (F)	
DESASTRES NATURALES	**N.1**	Fuego	No existe sistema de alarma contra incendios. Se posee un solo extintor de solkaflam (clase c) recomendados para incendios en lugares donde se encuentren equipos eléctricos.	Muy baja	**2**
	N.2	Daños por agua	La infraestructura está expuesta a goteras, cuenta con averías en el techo en donde el agua de las lluvias	Muy baja	**2**
	N.*	Desastres naturales	La oficina de la dependencia de sistemas se encuentra en zona baja de riesgo de desastre natural de origen volcánico debido a su cercanía con el volcán nevado del Tolima.	Raro	**1**
DE ORIGEN INDUSTRIA	**I.1**	Fuego	No existe sistema de alarma contra incendios. Se posee un solo extintor de solkaflam (clase c) recomendados para incendios en lugares	Muy baja	**2**

Tabla 1. Estimación de la probabilidad activo switch layer 3 9575 (continuación)

			donde se encuentren equipos eléctricos.		
	I.2	Daños por agua	La concentración del líquido sobrante por parte del aire acondicionado causaría daños en los equipos.	Muy baja	**2**
	I.*	Desastres industriales	No hay exposición o vulnerabilidad, por parte de esta amenaza.	Muy baja	**2**
	I.3	Contaminación mecánica	No hay exposición o vulnerabilidad, por parte de esta amenaza.	Muy baja	**2**
	I.4	Contaminación electromagnética	No hay exposición o vulnerabilidad, por parte de esta amenaza.	Muy baja	**2**
	I.5	Avería de origen físico o lógico	La manipulación por parte de cada uno de los componentes encontrados en la dependencia, como también por defectos de los componentes desde fabrica	Muy baja	**2**
	I.6	Corte del suministro eléctrico	Amenaza debida a factores externos, a clemencias de tipo naturales como lluvias u otros.	Muy baja	**2**
	I.7	Condiciones inadecuadas de temperatura o humedad	No se cuenta con una infraestructura adecuada para soportar los defectos del sistema de refrigeración.	Muy baja	**2**

Tabla 1. Estimación de la probabilidad activo switch layer 3 9575 (continuación)

	I.11	Emanaciones electromagnéticas	No hay exposición o vulnerabilidad, por parte de esta amenaza.	Muy baja	**2**
ERRORES Y FALLOS NO INTENCIONADOS	**E.2**	Errores del administrador	Pérdida total o parcial del tiempo de ejecución de sus actividades, dependiendo de la gravedad del asunto.	Muy baja	**2**
	E.23	Errores de mantenimiento / actualización de equipos(hardware)	Perjuicio a la mantenibilidad del sistema de información.	Muy baja	**2**
	E.24	Caída del sistema por agotamiento de recursos	Saturación del sistema informático.	Muy baja	**2**
	E.25	Perdida de equipos (Robo)	Recuperación de soportes reciclados o desechados.	Muy baja	**2**
ATAQUES INTENCIONADOS	**A.6**	Abuso de privilegios de acceso	Abuso de cada uno de los derechos otorgados.	Muy baja	**2**
	A.7	Uso no previsto	Implementación de recursos (económicos y de tiempo) en actividades no relacionadas.	Muy baja	**2**
	A.11	Acceso no autorizado	Uso ilícito del hardware	Muy baja	**2**
	A.23	Manipulación de los equipos	Sabotaje del hardware y software conteniente.	Muy baja	**2**
	A.24	Denegación de servicio	Saturación del sistema de información.	Muy baja	**2**

Tabla 1. Estimación de la probabilidad activo switch layer 3 9575 (continuación)

	A.25	Robo	Robo de porte de la información, puede esta ser física o digital.	Muy baja	**2**
	A.26	Ataque destructivo	Destrucción de los contenedores de la información, en recipientes físicos y lógicos.	Muy baja	**2**

Fuente: Autoría propia

Tabla 2. Estimación de la probabilidad activo *router* cisco modelo 1800 4781

ACTIVO TI	**ROUTER CISCO MODELO 1800 4781**
ADMINISTRADOR	PIMIENTO CARDENAS WILSON MAURICIO
DEGRADACIÓN	70%
IMPACTO	5
TIPO DE ACTIVO	HARDWARE

Tipo	ID	Amenaza	Exposición/Vulnerabilidad	Frecuencia (F)	
DESASTRES NATURALES	**N.1**	Fuego	No existe sistema de alarma contra incendios. Se posee un solo extintor de solkaflam (clase c) recomendados para incendios en lugares donde se encuentren equipos eléctricos.	Muy baja	**2**
	N.2	Daños por agua	La infraestructura está expuesta a goteras, cuenta con averías en el techo en donde el agua de las lluvias	Muy baja	**2**
	N.*	Desastres naturales	La oficina de la dependencia de sistemas se encuentra en zona baja de riesgo de desastre natural de origen volcánico debido a su cercanía con el volcán nevado del Tolima.	Raro	**1**

Tabla 2. Estimación de la probabilidad activo router cisco modelo 1800 4781 (continuación)

DE ORIGEN INDUSTRIAL	**I.1**	Fuego	No existe sistema de alarma contra incendios. Se posee un solo extintor de solkaflam (clase c) recomendados para incendios en lugares donde se encuentren equipos eléctricos.	Muy baja	**2**
	I.2	Daños por agua	La concentración del líquido sobrante por parte del aire acondicionado causaría daños en los equipos.	Muy baja	**2**
	I.*	Desastres industriales	No hay exposición o vulnerabilidad, por parte de esta amenaza.	Muy baja	**2**
	I.3	Contaminación mecánica	No hay exposición o vulnerabilidad, por parte de esta amenaza.	Muy baja	**2**
	I.4	Contaminación electromagnética	No hay exposición o vulnerabilidad, por parte de esta amenaza.	Muy baja	**2**
	I.5	Avería de origen físico o lógico	La manipulación por parte de cada uno de los componentes encontrados en la dependencia, como también por defectos de los componentes desde fabrica	Muy baja	**2**
	I.6	Corte del suministro eléctrico	Amenaza debida a factores externos, a clemencias de tipo naturales como lluvias u otros.	Muy baja	**2**
	I.7	Condiciones inadecuadas de	No se cuenta con una infraestructura adecuada	Muy baja	**2**

Tabla 2. Estimación de la probabilidad activo router cisco modelo 1800 4781 (continuación)

		temperatura o humedad	para soportar los defectos del sistema de refrigeración.		
	I.11	Emanaciones electromagnéticas	No hay exposición o vulnerabilidad, por parte de esta amenaza.	Muy baja	**2**
ERRORES Y FALLOS NO INTENCIONADOS	**E.2**	Errores del administrador	Pérdida total o parcial del tiempo de ejecución de sus actividades, dependiendo de la gravedad del asunto.	Muy baja	**2**
	E.23	Errores de mantenimiento / actualización de equipos(hardware)	Perjuicio a la mantenibilidad del sistema de información.	Muy baja	**2**
	E.24	Caída del sistema por agotamiento de recursos	Saturación del sistema informático.	Muy baja	**2**
	E.25	Perdida de equipos (Robo)	Recuperación de soportes reciclados o desechados.	Muy baja	**2**
ATAQUES INTENCIONADOS	**A.6**	Abuso de privilegios de acceso	Abuso de cada uno de los derechos otorgados.	Muy baja	**2**
	A.7	Uso no previsto	Implementación de recursos (económicos y de tiempo) en actividades no relacionadas.	Muy baja	**2**
	A.11	Acceso no autorizado	Uso ilícito del hardware	Muy baja	**2**
	A.23	Manipulación de los equipos	Sabotaje del hardware y software conteniente.	Muy baja	**2**
	A.24	Denegación de servicio	Saturación del sistema de información.	Muy baja	**2**

Tabla 2. Estimación de la probabilidad activo *route*r cisco modelo 1800 4781. (Continuación)

	A.25	Robo	Robo de porte de la información, puede esta ser física o digital.	Muy baja	**2**
	A.26	Ataque destructivo	Destrucción de los contenedores de la información, en recipientes físicos y lógicos.	Muy baja	**2**

Fuente: Autoría propia

Tabla 3. Estimación de la probabilidad activo red telefónica

ACTIVO TI	**RED TELEFÓNICA**
ADMINISTRADOR	PIMIENTO CARDENAS WILSON MAURICIO
DEGRADACIÓN	60%
IMPACTO	5
TIPO DE ACTIVO	REDES DE COMUNICACIÓN

Tipo	ID	Amenaza	Exposición/Vulnerabilidad	Frecuencia (F)	
DE ORIGEN INDUSTRIAL	**I.8**	Fallo de servicios de comunicaciones	Atentados externos por parte de grupos ha margen de la ley que puedan atentar contra la infraestructura que trasmite cada uno de los servicios.	Media	4
ERRORES Y FALLOS NO INTENCIONADOS	**E.2**	Errores del administrador	Pérdida total o parcial del tiempo de ejecución de sus actividades, dependiendo de la gravedad del asunto.	Media	4
	E.9	Errores de [re-] encaminamiento	La dependencia cuenta con sistemas de cifrado y verificación (puerto – puerto) para el manejo de la movilidad de la información.	Media	4
	E.10	Errores de secuencia	La dependencia cuenta con sistemas de cifrado y verificación (puerto –	Media	4

Tabla 3. Estimación de la probabilidad activo red telefónica (continuación)

			puerto) para el manejo de la movilidad de la información.		
	E.15	Alteración accidental de la información	La dependencia cuenta con sistemas de cifrado y verificación (puerto – puerto) para el manejo de la movilidad de la información.	Media	4
	E.18	Destrucción de información	El departamento de sistemas cuenta con copias de seguridad periódicas	Media	4
	E.19	Fugas de información	Las personas contratadas están atadas a cláusulas de confidencialidad.	Media	4
	E.24	Caída del sistema por agotamiento de recursos	Saturación del sistema informático.	Media	4
ATAQUES INTENCIONADOS	**A.5**	Suplantación de la identidad del usuario	Acceso a personas que no cuenten con los permisos necesarios o con las credenciales necesarias.	Media	4
	A.6	Abuso de privilegios de acceso	Abuso de cada uno de los derechos otorgados.	Media	4
	A.7	Uso no previsto	Implementación de recursos (económicos y de tiempo) en actividades no relacionadas.	Media	4
	A.9	[Re-]encaminamiento de mensajes	La dependencia cuenta con sistemas de cifrado y verificación (puerto – puerto) para el manejo de la movilidad de la información.	Media	4

Tabla 3. Estimación de la probabilidad activo red telefónica (continuación)

	A.10	Alteración de secuencia	Alteración de datos.	Media	4
	A.11	Acceso no autorizado	Uso ilícito del hardware	Media	4
	A.12	Análisis de trafico	Análisis de cada uno de los datos transitados por la red interna de la institución.	Media	4
	A.14	Interceptación de información (escucha)	Escucha pasiva.	Media	4
	A.15	Modificación deliberada de la información	Datos erróneos en el momento de la movilización de la información.	Media	4
	A.19	Divulgación de información	Información filtrada abiertamente a personas no correspondientes.	Media	4
	A.24	Denegación de servicio	Saturación del sistema de información.	Media	4

Fuente: Autoría propia

Tabla 4 . Estimación de la probabilidad activo internet movistar

ACTIVO TI	**INTERNET MOVISTAR**			
ADMINISTRADOR	PIMIENTO CARDENAS WILSON MAURICIO			
DEGRADACIÓN	90%			
IMPACTO	8			
TIPO DE ACTIVO	REDES DE COMUNICACIÓN			
Tipo	**ID**	**Amenaza**	**Exposición/Vulnerabilidad**	**Frecuencia (F)**	
DE ORIGEN INDUSTRIAL	**I.8**	Fallo de servicios de comunicaciones	Atentados externos por parte de grupos ha margen de la ley que puedan atentar contra la infraestructura que trasmite cada uno de los servicios.	Media	4

Tabla 4. Estimación de la probabilidad activo internet movistar. (Continuación)

ERRORES Y FALLOS NO INTENCIONADOS	**E.2**	Errores del administrador	Pérdida total o parcial del tiempo de ejecución de sus actividades, dependiendo de la gravedad del asunto.	Media	4
	E.9	Errores de [re-] encaminamiento	La dependencia cuenta con sistemas de cifrado y verificación (puerto – puerto) para el manejo de la movilidad de la información.	Media	4
	E.10	Errores de secuencia	La dependencia cuenta con sistemas de cifrado y verificación (puerto – puerto) para el manejo de la movilidad de la información.	Media	4
	E.15	Alteración accidental de la información	La dependencia cuenta con sistemas de cifrado y verificación (puerto – puerto) para el manejo de la movilidad de la información.	Media	4
	E.18	Destrucción de información	El departamento de sistemas cuenta con copias de seguridad periódicas	Media	4
	E.19	Fugas de información	Las personas contratadas están atadas a cláusulas de confidencialidad.	Media	4
	E.24	Caída del sistema por agotamiento de recursos	Saturación del sistema informático.	Media	4
ATAQUES INTENCIO	**A.5**	Suplantación de la identidad del usuario	Acceso a personas que no cuenten con los permisos necesarios o con las credenciales necesarias.	Media	4

Tabla 4. Estimación de la probabilidad activo internet movistar. (Continuación)

	A.6	Abuso de privilegios de acceso	Abuso de cada uno de los derechos otorgados.	Media	4
	A.7	Uso no previsto	Implementación de recursos (económicos y de tiempo) en actividades no relacionadas.	Media	4
	A.9	[Re-]encaminamiento de mensajes	La dependencia cuenta con sistemas de cifrado y verificación (puerto – puerto) para el manejo de la movilidad de la información.	Media	4
	A.10	Alteración de secuencia	Alteración de datos.	Media	4
	A.11	Acceso no autorizado	Uso ilícito del hardware	Media	4
	A.12	Análisis de trafico	Análisis de cada uno de los datos transitados por la red interna de la institución.	Media	4
	A.14	Interceptación de información (escucha)	Escucha pasiva.	Media	4
	A.15	Modificación deliberada de la información	Datos erróneos en el momento de la movilización de la información.	Media	4
	A.19	Divulgación de información	Información filtrada abiertamente a personas no correspondientes.	Media	4
	A.24	Denegación de servicio	Saturación del sistema de información.	Media	4

Fuente: Autoría propia

Tabla 5. Estimación de la probabilidad activo red LAN

ACTIVO TI	**RED LAN**
ADMINISTRADOR	PIMIENTO CARDENAS WILSON MAURICIO
DEGRADACIÓN	90%
IMPACTO	8
TIPO DE ACTIVO	REDES DE COMUNICACIÓN

Tipo	ID	Amenaza	Exposición/Vulnerabilidad	Frecuencia (F)	
DE ORIGEN INDUSTRIAL	**I.8**	Fallo de servicios de comunicaciones	Atentados externos por parte de grupos ha margen de la ley que puedan atentar contra la infraestructura que trasmite cada uno de los servicios.	Media	4
ERRORES Y FALLOS NO INTENCIONADOS	**E.2**	Errores del administrador	Pérdida total o parcial del tiempo de ejecución de sus actividades, dependiendo de la gravedad del asunto.	Media	4
	E.9	Errores de [re-] encaminamiento	La dependencia cuenta con sistemas de cifrado y verificación (puerto – puerto) para el manejo de la movilidad de la información.	Media	4
	E.10	Errores de secuencia	La dependencia cuenta con sistemas de cifrado y verificación (puerto – puerto) para el manejo de la movilidad de la información.	Media	4
	E.15	Alteración accidental de la información	La dependencia cuenta con sistemas de cifrado y verificación (puerto – puerto) para el manejo de la movilidad de la información.	Media	4

Tabla 5. Estimación de la probabilidad activo red LAN. (Continuación)

	E.18	Destrucción de información	El departamento de sistemas cuenta con copias de seguridad periódicas	Media	4
	E.19	Fugas de información	Las personas contratadas están atadas a cláusulas de confidencialidad.	Media	4
	E.24	Caída del sistema por agotamiento de recursos	Saturación del sistema informático.	Media	4
ATAQUES INTENCIONADOS	**A.5**	Suplantación de la identidad del usuario	Acceso a personas que no cuenten con los permisos necesarios o con las credenciales necesarias.	Media	4
	A.6	Abuso de privilegios de acceso	Abuso de cada uno de los derechos otorgados.	Media	4
	A.7	Uso no previsto	Implementación de recursos (económicos y de tiempo) en actividades no relacionadas.	Media	4
	A.9	[Re-]encaminamiento de mensajes	La dependencia cuenta con sistemas de cifrado y verificación (puerto – puerto) para el manejo de la movilidad de la información.	Media	4
	A.10	Alteración de secuencia	Alteración de datos.	Media	4
	A.11	Acceso no autorizado	Uso ilícito del hardware	Media	4
	A.12	Análisis de trafico	Análisis de cada uno de los datos transitados por la red interna de la institución.	Media	4

Tabla 5. Estimación de la probabilidad activo red LAN. (Continuación)

	A.14	Interceptación de información (escucha)	Escucha pasiva.	Media	4
	A.15	Modificación deliberada de la información	Datos erróneos en el momento de la movilización de la información.	Media	4
	A.19	Divulgación de información	Información filtrada abiertamente a personas no correspondientes.	Media	4
	A.24	Denegación de servicio	Saturación del sistema de información.	Media	4

Fuente: Autoría propia

Tabla 6. Estimación de la probabilidad activo red WIFI

ACTIVO TI	**RED WIFI**
ADMINISTRADOR	PIMIENTO CARDENAS WILSON MAURICIO
DEGRADACIÓN	70%
IMPACTO	5
TIPO DE ACTIVO	REDES DE COMUNICACIÓN

Tipo	ID	Amenaza	Exposición/Vulnerabilidad	Frecuencia (F)	
DE ORIGEN INDUSTRIAL	**I.8**	Fallo de servicios de comunicaciones	Atentados externos por parte de grupos ha margen de la ley que puedan atentar contra la infraestructura que trasmite cada uno de los servicios.	Media	4
ERRORES Y FALLOS NO	**E.2**	Errores del administrador	Pérdida total o parcial del tiempo de ejecución de sus actividades, dependiendo de la gravedad del asunto.	Media	4
	E.9	Errores de [re-] encaminamiento	La dependencia cuenta con sistemas de cifrado y verificación (puerto –	Media	4

Tabla 6. Estimación de la probabilidad activo red WIFI. (Continuación)

			puerto) para el manejo de la movilidad de la información.		
	E.10	Errores de secuencia	La dependencia cuenta con sistemas de cifrado y verificación (puerto – puerto) para el manejo de la movilidad de la información.	Media	4
	E.15	Alteración accidental de la información	La dependencia cuenta con sistemas de cifrado y verificación (puerto – puerto) para el manejo de la movilidad de la información.	Media	4
	E.18	Destrucción de información	El departamento de sistemas cuenta con copias de seguridad periódicas	Media	4
	E.19	Fugas de información	Las personas contratadas están atadas a cláusulas de confidencialidad.	Media	4
	E.24	Caída del sistema por agotamiento de recursos	Saturación del sistema informático.	Media	4
ATAQUES INTENCIONADOS	**A.5**	Suplantación de la identidad del usuario	Acceso a personas que no cuenten con los permisos necesarios o con las credenciales necesarias.	Media	4
	A.6	Abuso de privilegios de acceso	Abuso de cada uno de los derechos otorgados.	Media	4
	A.7	Uso no previsto	Implementación de recursos (económicos y de tiempo) en actividades no relacionadas.	Media	4

Tabla 6. Estimación de la probabilidad activo red WIFI. (Continuación)

	A.9	[Re-]encaminamiento de mensajes	La dependencia cuenta con sistemas de cifrado y verificación (puerto – puerto) para el manejo de la movilidad de la información.	Media	4
	A.10	Alteración de secuencia	Alteración de datos.	Media	4
	A.11	Acceso no autorizado	Uso ilícito del hardware	Media	4
	A.12	Análisis de trafico	Análisis de cada uno de los datos transitados por la red interna de la institución.	Media	4
	A.14	Interceptación de información (escucha)	Escucha pasiva.	Media	4
	A.15	Modificación deliberada de la información	Datos erróneos en el momento de la movilización de la información.	Media	4
	A.19	Divulgación de información	Información filtrada abiertamente a personas no correspondientes.	Media	4
	A.24	Denegación de servicio	Saturación del sistema de información.	Media	4

Fuente: Autoría propia

Tabla 7. Estimación de la probabilidad activo red de datos

ACTIVO TI	**RED DE DATOS**			
ADMINISTRADOR	PIMIENTO CARDENAS WILSON MAURICIO			
DEGRADACIÓN	70%			
IMPACTO	5			
TIPO DE ACTIVO	REDES DE COMUNICACIÓN			
Tipo	**ID**	**Amenaza**	**Exposición/Vulnerabilidad**	**Frecuencia (F)**

Tabla 7. Estimación de la probabilidad activo red de datos. (Continuación)

DE ORIGEN INDUSTRIAL	**I.8**	Fallo de servicios de comunicaciones	Atentados externos por parte de grupos ha margen de la ley que puedan atentar contra la infraestructura que trasmite cada uno de los servicios.	Media	4
ERRORES Y FALLOS NO INTENCIONADOS	**E.2**	Errores del administrador	Pérdida total o parcial del tiempo de ejecución de sus actividades, dependiendo de la gravedad del asunto.	Media	4
	E.9	Errores de [re-] encaminamiento	La dependencia cuenta con sistemas de cifrado y verificación (puerto – puerto) para el manejo de la movilidad de la información.	Media	4
	E.10	Errores de secuencia	La dependencia cuenta con sistemas de cifrado y verificación (puerto – puerto) para el manejo de la movilidad de la información.	Media	4
	E.15	Alteración accidental de la información	La dependencia cuenta con sistemas de cifrado y verificación (puerto – puerto) para el manejo de la movilidad de la información.	Media	4
	E.18	Destrucción de información	El departamento de sistemas cuenta con copias de seguridad periódicas	Media	4
	E.19	Fugas de información	Las personas contratadas están atadas a cláusulas de confidencialidad.	Media	4

Tabla 7. Estimación de la probabilidad activo red de datos. (Continuación)

	E.24	Caída del sistema por agotamiento de recursos	Saturación del sistema informático.	Media	4
ATAQUES INTENCIONADOS	**A.5**	Suplantación de la identidad del usuario	Acceso a personas que no cuenten con los permisos necesarios o con las credenciales necesarias.	Media	4
	A.6	Abuso de privilegios de acceso	Abuso de cada uno de los derechos otorgados.	Media	4
	A.7	Uso no previsto	Implementación de recursos (económicos y de tiempo) en actividades no relacionadas.	Media	4
	A.9	[Re-]encaminamiento de mensajes	La dependencia cuenta con sistemas de cifrado y verificación (puerto – puerto) para el manejo de la movilidad de la información.	Media	4
	A.10	Alteración de secuencia	Alteración de datos.	Media	4
	A.11	Acceso no autorizado	Uso ilícito del hardware	Media	4
	A.12	Análisis de trafico	Análisis de cada uno de los datos transitados por la red interna de la institución.	Media	4
	A.14	Interceptación de información (escucha)	Escucha pasiva.	Media	4
	A.15	Modificación deliberada de la información	Datos erróneos en el momento de la movilización de la información.	Media	4

Tabla 7. Estimación de la probabilidad activo red de datos. (Continuación)

	A.19	Divulgación de información	Información filtrada abiertamente a personas no correspondientes.	Media	4
	A.24	Denegación de servicio	Saturación del sistema de información.	Media	4

Fuente: Autoría propia

Tabla 8. Estimación de la probabilidad activo DDS 1TB

ACTIVO TI	**DDS 1TB**
ADMINISTRADOR	PIMIENTO CARDENAS WILSON MAURICIO
DEGRADACIÓN	35%
IMPACTO	3
TIPO DE ACTIVO	SOPORTES DE INFORMACIÓN

Tipo	ID	Amenaza	Exposición/Vulnerabilidad	Frecuencia (F)	
DESASTRES NATURALES	**N.1**	Fuego	No existe sistema de alarma contra incendios. Se posee un solo extintor de solkaflam (clase c) recomendados para incendios en lugares donde se encuentren equipos eléctricos.	Baja	**3**
	N.2	Daños por agua	La infraestructura está expuesta a goteras, cuenta con averías en el techo en donde el agua de las lluvias	Baja	**3**
	N.*	Desastres naturales	La oficina de la dependencia de sistemas se encuentra en zona baja de riesgo de desastre natural de origen volcánico debido a su cercanía con el volcán nevado del Tolima.	Baja	**3**

Tabla 8. Estimación de la probabilidad activo DDS 1TB. (Continuación)

DE ORIGEN INDUSTRIAL	**I.1**	Fuego	No existe sistema de alarma contra incendios. Se posee un solo extintor de solkaflam (clase c) recomendados para incendios en lugares donde se encuentren equipos eléctricos.	Baja	**3**
	I.2	Daños por agua	La concentración del líquido sobrante por parte del aire acondicionado causaría daños en los equipos.	Baja	**3**
	I.*	Desastres industriales	No hay exposición o vulnerabilidad, por parte de esta amenaza.	Baja	**3**
	I.3	Contaminación mecánica	No hay exposición o vulnerabilidad, por parte de esta amenaza.	Baja	**3**
	I.4	Contaminación electromagnética	No hay exposición o vulnerabilidad, por parte de esta amenaza.	Baja	**3**
	I.5	Avería de origen físico o lógico	La manipulación por parte de cada uno de los componentes encontrados en la dependencia, como también por defectos de los componentes desde fabrica	Baja	**3**
	I.6	Corte del suministro eléctrico	Amenaza debida a factores externos, a clemencias de tipo naturales como lluvias u otros.	Baja	**3**
	I.7	Condiciones inadecuadas de	No se cuenta con una infraestructura adecuada	Baja	**3**

Tabla 8. Estimación de la probabilidad activo DDS 1TB. (Continuación)

		temperatura o humedad	para soportar los defectos del sistema de refrigeración.		
	I.10	Degradación de los soportes de almacén amiento de la información	Pérdida gradual de cada uno de los registros históricos de la dependencia.	Baja	**3**
	I.11	Emanaciones electromagnéticas	No hay exposición o vulnerabilidad, por parte de esta amenaza.	Baja	**3**
ERRORES Y FALLOS NO INTENCIONADOS	**E.1**	Errores de los usuarios	Pérdida total o parcial del tiempo de ejecución de sus actividades, dependiendo de la gravedad del asunto.	Baja	**3**
	E.2	Errores del administrador	Pérdida total o parcial del tiempo de ejecución de sus actividades, dependiendo de la gravedad del asunto.	Baja	**3**
	E.15	Alteración accidental de la información	La dependencia cuenta con sistemas de cifrado y verificación (puerto – puerto) para el manejo de la movilidad de la información.	Baja	**3**
	E.18	Destrucción de información	El departamento de sistemas cuenta con copias de seguridad periódicas	Baja	**3**
	E.19	Fugas de información	Las personas contratadas están atadas a cláusulas de confidencialidad.	Baja	**3**
	E.23	Errores de mantenimiento / actualización de equipos(hardware)	Perjuicio a la mantenibilidad del sistema de información.	Baja	**3**

Tabla 8. Estimación de la probabilidad activo DDS 1TB. (Continuación)

	E.25	Perdida de equipos (Robo)	Recuperación de soportes reciclados o desechados.	Baja	**3**
ATAQUES INTENCIONADOS	**A.7**	Uso no previsto	Implementación de recursos (económicos y de tiempo) en actividades no relacionadas.	Baja	**3**
	A.11	Acceso no autorizado	Uso ilícito del hardware	Baja	**3**
	A.15	Modificación deliberada de la información	Datos erróneos en el momento de la movilización de la información.	Baja	**3**
	A.18	Destrucción de información	Perdida de la información.	Baja	**3**
	A.19	Divulgación de información	Información filtrada abiertamente a personas no correspondientes.	Baja	**3**
	A.23	Manipulación de los equipos	Sabotaje del hardware y software conteniente.	Baja	**3**
	A.25	Robo	Robo de porte de la información, puede esta ser física o digital.	Baja	**3**
	A.26	Ataque destructivo	Destrucción de los contenedores de la información, en recipientes físicos y lógicos.	Baja	**3**

Fuente: Autoría propia

Tabla 9. Estimación de la probabilidad activo materiales físicos

ACTIVO TI	**MATERIALES FÍSICOS**
ADMINISTRADOR	PIMIENTO CARDENAS WILSON MAURICIO
DEGRACIÓN	25%
IMPACTO	2
TIPO DE ACTIVO	SOPORTES DE INFORMACIÓN

Tabla 9. Estimación de la probabilidad activo materiales físicos. (Continuación)

Tipo	ID	Amenaza	Exposición/Vulnerabilidad	Frecuencia (F)	
DESASTRES NATURALES	**N.1**	Fuego	No existe sistema de alarma contra incendios. Se posee un solo extintor de solkaflam (clase c) recomendados para incendios en lugares donde se encuentren equipos eléctricos.	Baja	**3**
	N.2	Daños por agua	La infraestructura está expuesta a goteras, cuenta con averías en el techo en donde el agua de las lluvias	Baja	**3**
	N.*	Desastres naturales	La oficina de la dependencia de sistemas se encuentra en zona baja de riesgo de desastre natural de origen volcánico debido a su cercanía con el volcán nevado del Tolima.	Baja	**3**
DE ORIGEN INDUSTRIAL	**I.1**	Fuego	No existe sistema de alarma contra incendios. Se posee un solo extintor de solkaflam (clase c) recomendados para incendios en lugares donde se encuentren equipos eléctricos.	Baja	**3**
	I.2	Daños por agua	La concentración del líquido sobrante por parte del aire acondicionado causaría daños en los equipos.	Baja	**3**
	I.*	Desastres industriales	No hay exposición o vulnerabilidad, por parte de esta amenaza.	Baja	**3**

Tabla 9. Estimación de la probabilidad activo materiales físicos. (Continuación)

	I.3	Contaminación mecánica	No hay exposición o vulnerabilidad, por parte de esta amenaza.	Baja	**3**
	I.4	Contaminación electromagnética	No hay exposición o vulnerabilidad, por parte de esta amenaza.	Baja	**3**
	I.5	Avería de origen físico o lógico	La manipulación por parte de cada uno de los componentes encontrados en la dependencia, como también por defectos de los componentes desde fabrica	Baja	**3**
	I.6	Corte del suministro eléctrico	Amenaza debida a factores externos, a clemencias de tipo naturales como lluvias u otros.	Baja	**3**
	I.7	Condiciones inadecuadas de temperatura o humedad	No se cuenta con una infraestructura adecuada para soportar los defectos del sistema de refrigeración.	Baja	**3**
	I.10	Degradación de los soportes de almacén amiento de la información	Pérdida gradual de cada uno de los registros históricos de la dependencia.	Baja	**3**
	I.11	Emanaciones electromagnéticas	No hay exposición o vulnerabilidad, por parte de esta amenaza.	Baja	**3**
ERRORES Y FALLOS NO	**E.1**	Errores de los usuarios	Pérdida total o parcial del tiempo de ejecución de sus actividades, dependiendo de la gravedad del asunto.	Baja	**3**
	E.2	Errores del administrador	Pérdida total o parcial del tiempo de ejecución de sus	Baja	**3**

Tabla 9. Estimación de la probabilidad activo materiales físicos. (Continuación)

			actividades, dependiendo de la gravedad del asunto.		
	E.15	Alteración accidental de la información	La dependencia cuenta con sistemas de cifrado y verificación (puerto – puerto) para el manejo de la movilidad de la información.	Baja	**3**
	E.18	Destrucción de información	El departamento de sistemas cuenta con copias de seguridad periódicas	Baja	**3**
	E.19	Fugas de información	Las personas contratadas están atadas a cláusulas de confidencialidad.	Baja	**3**
	E.23	Errores de mantenimiento / actualización de equipos(hardware)	Perjuicio a la mantenibilidad del sistema de información.	Baja	**3**
	E.25	Perdida de equipos (Robo)	Recuperación de soportes reciclados o desechados.	Baja	**3**
ATAQUES INTENCIONADOS	**A.7**	Uso no previsto	Implementación de recursos (económicos y de tiempo) en actividades no relacionadas.	Baja	**3**
	A.11	Acceso no autorizado	Uso ilícito del hardware	Baja	**3**
	A.15	Modificación deliberada de la información	Datos erróneos en el momento de la movilización de la información.	Baja	**3**
	A.18	Destrucción de información	Perdida de la información.	Baja	**3**

Tabla 9. Estimación de la probabilidad activo materiales físicos. (Continuación)

	A.19	Divulgación de información	Información filtrada abiertamente a personas no correspondientes.	Baja	**3**
	A.23	Manipulación de los equipos	Sabotaje del hardware y software conteniente.	Baja	**3**
	A.25	Robo	Robo de porte de la información, puede esta ser física o digital.	Baja	**3**
	A.26	Ataque destructivo	Destrucción de los contenedores de la información, en recipientes físicos y lógicos.	Baja	**3**

Fuente: Autoría propia

Tabla 10. Estimación de la probabilidad activo UPS 10 KVA 9578

ACTIVO TI	**UPS 10 KVA 9578**
ADMINISTRADOR	PIMIENTO CARDENAS WILSON MAURICIO
DEGRADACIÓN	70%
IMPACTO	5
TIPO DE ACTIVO	EQUIPAMIENTO AUXILIAR

Tipo	**ID**	**Amenaza**	**Exposición/Vulnerabilidad**	**Frecuencia (F)**	
DESASTRES NATURALES	**N.1**	Fuego	No existe sistema de alarma contra incendios. Se posee un solo extintor de solkaflam (clase c) recomendados para incendios en lugares donde se encuentren equipos eléctricos.	Muy baja	**2**
	N.2	Daños por agua	La infraestructura está expuesta a goteras, cuenta con averías en el techo en donde el agua de las lluvias	Muy baja	**2**

Tabla 10. Estimación de la probabilidad activo UPS 10 KVA 9578. (Continuación)

	N.*	Desastres naturales	La oficina de la dependencia de sistemas se encuentra en zona baja de riesgo de desastre natural de origen volcánico debido a su cercanía con el volcán nevado del Tolima.	Muy baja	**2**
DE ORIGEN INDUSTRIAL	**I.1**	Fuego	No existe sistema de alarma contra incendios. Se posee un solo extintor de solkaflam (clase c) recomendados para incendios en lugares donde se encuentren equipos eléctricos.	Muy baja	**2**
	I.2	Daños por agua	La concentración del líquido sobrante por parte del aire acondicionado causaría daños en los equipos.	Muy baja	**2**
	I.*	Desastres industriales	No hay exposición o vulnerabilidad, por parte de esta amenaza.	Muy baja	**2**
	I.3	Contaminación mecánica	No hay exposición o vulnerabilidad, por parte de esta amenaza.	Muy baja	**2**
	I.4	Contaminación electromagnética	No hay exposición o vulnerabilidad, por parte de esta amenaza.	Muy baja	**2**
	I.5	Avería de origen físico o lógico	La manipulación por parte de cada uno de los componentes encontrados en la dependencia, como también por defectos de los componentes desde fabrica	Muy baja	**2**

Tabla 10. Estimación de la probabilidad activo UPS 10 KVA 9578. (Continuación)

	I.6	Corte del suministro eléctrico	Amenaza debida a factores externos, a clemencias de tipo naturales como lluvias u otros.	Muy baja	**2**
	I.7	Condiciones inadecuadas de temperatura o humedad	No se cuenta con una infraestructura adecuada para soportar los defectos del sistema de refrigeración.	Muy baja	**2**
	I.9	Interrupción de otros servicios y suministros esenciales	No hay exposición o vulnerabilidad, por parte de esta amenaza.	Muy baja	**2**
	I.11	Emanaciones electromagnéticas	No hay exposición o vulnerabilidad, por parte de esta amenaza.	Muy baja	**2**
ERRORES Y FALLOS NO	**E.23**	Errores de mantenimiento / actualización de equipos(hardware)	Perjuicio a la mantenibilidad del sistema de información.	Baja	3
	E.25	Perdida de equipos (Robo)	Recuperación de soportes reciclados o desechados.	Baja	3
ATAQUES INTENCIONADOS	**A.7**	Uso no previsto	Implementación de recursos (económicos y de tiempo) en actividades no relacionadas.	Baja	3
	A.11	Acceso no autorizado	Uso ilícito del hardware	Baja	3
	A.23	Manipulación de los equipos	Sabotaje del hardware y software conteniente.	Baja	3
	A.25	Robo	Robo de porte de la información, puede esta ser física o digital.	Baja	3

Tabla 10. Estimación de la probabilidad activo UPS 10 KVA 9578. (Continuación)

	A.26	Ataque destructivo	Destrucción de los contenedores de la información, en recipientes físicos y lógicos.	Baja	3

Fuente: Autoría propia

Tabla 11. Estimación de la probabilidad activo UPS 10 KVA 9579

ACTIVO TI	**UPS 10 KVA 9579**
ADMINISTRADOR	PIMIENTO CARDENAS WILSON MAURICIO
DEGRADACIÓN	70%
IMPACTO	5
TIPO DE ACTIVO	EQUIPAMIENTO AUXILIAR

Tipo	ID	Amenaza	Exposición/Vulnerabilidad	Frecuencia (F)	
DESASTRES NATURALES	**N.1**	Fuego	No existe sistema de alarma contra incendios. Se posee un solo extintor de solkaflam (clase c) recomendados para incendios en lugares donde se encuentren equipos eléctricos.	Muy baja	**2**
	N.2	Daños por agua	La infraestructura está expuesta a goteras, cuenta con averías en el techo en donde el agua de las lluvias	Muy baja	**2**
	N.*	Desastres naturales	La oficina de la dependencia de sistemas se encuentra en zona baja de riesgo de desastre natural de origen volcánico debido a su cercanía con el volcán nevado del Tolima.	Muy baja	**2**
DE ORIGEN INDUSTRIA	**I.1**	Fuego	No existe sistema de alarma contra incendios. Se posee un solo extintor de solkaflam (clase c) recomendados para incendios en lugares	Muy baja	**2**

Tabla 11. Estimación de la probabilidad activo UPS 10 KVA 9579. (Continuación)

			donde se encuentren equipos eléctricos.		
	I.2	Daños por agua	La concentración del líquido sobrante por parte del aire acondicionado causaría daños en los equipos.	Muy baja	**2**
	I.*	Desastres industriales	No hay exposición o vulnerabilidad, por parte de esta amenaza.	Muy baja	**2**
	I.3	Contaminación mecánica	No hay exposición o vulnerabilidad, por parte de esta amenaza.	Muy baja	**2**
	I.4	Contaminación electromagnética	No hay exposición o vulnerabilidad, por parte de esta amenaza.	Muy baja	**2**
	I.5	Avería de origen físico o lógico	La manipulación por parte de cada uno de los componentes encontrados en la dependencia, como también por defectos de los componentes desde fabrica	Muy baja	**2**
	I.6	Corte del suministro eléctrico	Amenaza debida a factores externos, a clemencias de tipo naturales como lluvias u otros.	Muy baja	**2**
	I.7	Condiciones inadecuadas de temperatura o humedad	No se cuenta con una infraestructura adecuada para soportar los defectos del sistema de refrigeración.	Muy baja	**2**

Tabla 11. Estimación de la probabilidad activo UPS 10 KVA 9579. (Continuación)

	I.9	Interrupción de otros servicios y suministros esenciales	No hay exposición o vulnerabilidad, por parte de esta amenaza.	Muy baja	**2**
	I.11	Emanaciones electromagnéticas	No hay exposición o vulnerabilidad, por parte de esta amenaza.	Muy baja	**2**
ERRORES Y NO FALLOS	**E.23**	Errores de mantenimiento / actualización de equipos(hardware)	Perjuicio a la mantenibilidad del sistema de información.	Baja	3
	E.25	Perdida de equipos (Robo)	Recuperación de soportes reciclados o desechados.	Baja	3
ATAQUES INTENCIONADOS	**A.7**	Uso no previsto	Implementación de recursos (económicos y de tiempo) en actividades no relacionadas.	Baja	3
	A.11	Acceso no autorizado	Uso ilícito del hardware	Baja	3
	A.23	Manipulación de los equipos	Sabotaje del hardware y software conteniente.	Baja	3
	A.25	Robo	Robo de porte de la información, puede esta ser física o digital.	Baja	3
	A.26	Ataque destructivo	Destrucción de los contenedores de la información, en recipientes físicos y lógicos.	Baja	3

Fuente: Autoría propia

Tabla 12. Estimación de la probabilidad activo UPS 10 KVA 9580

ACTIVO TI	**UPS 10 KVA 9580**
ADMINISTRADOR	PIMIENTO CARDENAS WILSON MAURICIO
DEGRADACIÓN	70%

Tabla 12. Estimación de la probabilidad activo UPS 10 KVA 9580. (Continuación)

IMPACTO	5				
TIPO DE ACTIVO	EQUIPAMIENTO AUXILIAR				
Tipo	**ID**	**Amenaza**	**Exposición/Vulnerabilidad**	**Frecuencia (F)**	
DESASTRES NATURALES	**N.1**	Fuego	No existe sistema de alarma contra incendios. Se posee un solo extintor de solkaflam (clase c) recomendados para incendios en lugares donde se encuentren equipos eléctricos.	Muy baja	**2**
	N.2	Daños por agua	La infraestructura está expuesta a goteras, cuenta con averías en el techo en donde el agua de las lluvias	Muy baja	**2**
	N.*	Desastres naturales	La oficina de la dependencia de sistemas se encuentra en zona baja de riesgo de desastre natural de origen volcánico debido a su cercanía con el volcán nevado del Tolima.	Muy baja	**2**
DE ORIGEN INDUSTRIAL	**I.1**	Fuego	No existe sistema de alarma contra incendios. Se posee un solo extintor de solkaflam (clase c) recomendados para incendios en lugares donde se encuentren equipos eléctricos.	Muy baja	**2**
	I.2	Daños por agua	La concentración del líquido sobrante por parte del aire acondicionado causaría daños en los equipos.	Muy baja	**2**

Tabla 12. Estimación de la probabilidad activo UPS 10 KVA 9580. (Continuación)

	I.*	Desastres industriales	No hay exposición o vulnerabilidad, por parte de esta amenaza.	Muy baja	**2**
	I.3	Contaminación mecánica	No hay exposición o vulnerabilidad, por parte de esta amenaza.	Muy baja	**2**
	I.4	Contaminación electromagnética	No hay exposición o vulnerabilidad, por parte de esta amenaza.	Muy baja	**2**
	I.5	Avería de origen físico o lógico	La manipulación por parte de cada uno de los componentes encontrados en la dependencia, como también por defectos de los componentes desde fabrica	Muy baja	**2**
	I.6	Corte del suministro eléctrico	Amenaza debida a factores externos, a clemencias de tipo naturales como lluvias u otros.	Muy baja	**2**
	I.7	Condiciones inadecuadas de temperatura o humedad	No se cuenta con una infraestructura adecuada para soportar los defectos del sistema de refrigeración.	Muy baja	**2**
	I.9	Interrupción de otros servicios y suministros esenciales	No hay exposición o vulnerabilidad, por parte de esta amenaza.	Muy baja	**2**
	I.11	Emanaciones electromagnéticas	No hay exposición o vulnerabilidad, por parte de esta amenaza.	Muy baja	**2**
ERRORE	**E.23**	Errores de mantenimiento /	Perjuicio a la mantenibilidad del sistema de información.	Baja	3

Tabla 12. Estimación de la probabilidad activo UPS 10 KVA 9580. (Continuación)

		actualización de equipos(hardware)			
	E.25	Perdida de equipos (Robo)	Recuperación de soportes reciclados o desechados.	Baja	3
ATAQUES INTENCIONADOS	**A.7**	Uso no previsto	Implementación de recursos (económicos y de tiempo) en actividades no relacionadas.	Baja	3
	A.11	Acceso no autorizado	Uso ilícito del hardware	Baja	3
	A.23	Manipulación de los equipos	Sabotaje del hardware y software conteniente.	Baja	3
	A.25	Robo	Robo de porte de la información, puede esta ser física o digital.	Baja	3
	A.26	Ataque destructivo	Destrucción de los contenedores de la información, en recipientes físicos y lógicos.	Baja	3

Fuente: Autoría propia

Tabla 12. Estimación de la probabilidad activo cuarto o recinto (oficina)

ACTIVO TI	**CUARTO O RECINTO (OFICINA)**
ADMINISTRADOR	PIMIENTO CARDENAS WILSON MAURICIO
DEGRADACIÓN	90%
IMPACTO	8
TIPO DE ACTIVO	INSTALACIONES

Tipo	**ID**	**Amenaza**	**Exposición/Vulnerabilidad**	**Frecuencia (F)**	
DESASTRES	**N.1**	Fuego	No existe sistema de alarma contra incendios. Se posee un solo extintor de solkaflam (clase c) recomendados para incendios en lugares	Raro	**1**

Tabla 12. Estimación de la probabilidad activo cuarto o recinto (oficina). (Continuación)

			donde se encuentren equipos eléctricos.		
	N.2	Daños por agua	La infraestructura está expuesta a goteras, cuenta con averías en el techo en donde el agua de las lluvias	Raro	**1**
	N.*	Desastres naturales	La oficina de la dependencia de sistemas se encuentra en zona baja de riesgo de desastre natural de origen volcánico debido a su cercanía con el volcán nevado del Tolima.	Raro	**1**
DE ORIGEN INDUSTRIAL	**I.1**	Fuego	No existe sistema de alarma contra incendios. Se posee un solo extintor de solkaflam (clase c) recomendados para incendios en lugares donde se encuentren equipos eléctricos.	Raro	**1**
	I.2	Daños por agua	La concentración del líquido sobrante por parte del aire acondicionado causaría daños en los equipos.	Raro	**1**
	I.*	Desastres industriales	No hay exposición o vulnerabilidad, por parte de esta amenaza.	Raro	**1**
	I.11	Emanaciones electromagnéticas	No hay exposición o vulnerabilidad, por parte de esta amenaza.	Raro	**1**

Tabla 12. Estimación de la probabilidad activo cuarto o recinto (oficina). (Continuación)

ERRORES Y FALLOS NO INTENCIONADOS	**E.15**	Alteración accidental de la información	La dependencia cuenta con sistemas de cifrado y verificación (puerto – puerto) para el manejo de la movilidad de la información.	Muy bajo	**2**
	E.18	Destrucción de información	El departamento de sistemas cuenta con copias de seguridad periódicas	Muy bajo	**2**
	E.19	Fugas de información	Las personas contratadas están atadas a cláusulas de confidencialidad.	Muy bajo	**2**
ATAQUES INTENCIONADOS	**A.7**	Uso no previsto	Implementación de recursos (económicos y de tiempo) en actividades no relacionadas.	Muy bajo	**2**
	A.11	Acceso no autorizado	Uso ilícito del hardware	Muy bajo	**2**
	A.15	Modificación deliberada de la información	Datos erróneos en el momento de la movilización de la información.	Muy bajo	**2**
	A.18	Destrucción de información	Perdida de la información.	Muy bajo	**2**
	A.19	Divulgación de información	Información filtrada abiertamente a personas no correspondientes.	Muy bajo	**2**
	A.26	Ataque destructivo	Destrucción de los contenedores de la información, en recipientes físicos y lógicos.	Muy bajo	**2**
	A.27	Ocupación enemiga	Divulgación de información no consentida.	Muy bajo	**2**

Fuente: Autoría propia

Tabla 13. Estimación de la probabilidad activo coordinador de sistemas

ACTIVO TI	**COORDINADOR DE SISTEMAS**				
ADMINISTRADOR	PIMIENTO CARDENAS WILSON MAURICIO				
DEGRADACIÓN	70%				
IMPACTO	5				
TIPO DE ACTIVO	PERSONAL				
Tipo	**ID**	**Amenaza**	**Exposición/Vulnerabilidad**	**Frecuencia (F)**	
ERRORES Y FALLOS NO INTENCIONADOS	**E.7**	Deficiencias en la organización	No hay exposición o vulnerabilidad, por parte de esta amenaza.	Baja	3
	E.19	Fugas de información	Las personas contratadas están atadas a cláusulas de confidencialidad.	Baja	3
	E.28	Indisponibilidad del personal	Daño a la disponibilidad de cada una de las personas influyentes en la dependencia.	Baja	3
ATAQUES INTENCIONADOS	**A.28**	Indisponibilidad del personal	Daño a la disponibilidad de la información.	Baja	3
	A.29	Extorsión	Influenciarían al personal capacitado.	Baja	3
	A.30	Ingeniería social (picaresca)	Intervención de personas con fines no éticas.	Baja	3

Fuente: Autoría propia

Tabla 14. Estimación de la probabilidad activo programador

ACTIVO TI	**PROGRAMADOR**			
ADMINISTRADOR	PIMIENTO CARDENAS WILSON MAURICIO			
DEGRADACIÓN	70%			
IMPACTO	5			
TIPO DE ACTIVO	PERSONAL			
Tipo	**ID**	**Amenaza**	**Exposición/Vulnerabilidad**	**Frecuencia (F)**

Tabla 14. Estimación de la probabilidad activo programador. (Continuación)

ERRORES Y FALLOS NO INTENCIONADOS	**E.7**	Deficiencias en la organización	No hay exposición o vulnerabilidad, por parte de esta amenaza.	Baja	3
	E.19	Fugas de información	Las personas contratadas están atadas a cláusulas de confidencialidad.	Baja	3
	E.28	Indisponibilidad del personal	Daño a la disponibilidad de cada una de las personas influyentes en la dependencia.	Baja	3
ATAQUES INTENCIONADOS	**A.28**	Indisponibilidad del personal	Daño a la disponibilidad de la información.	Baja	3
	A.29	Extorsión	Influenciarían al personal capacitado.	Baja	3
	A.30	Ingeniería social (picaresca)	Intervención de personas con fines no éticas.	Baja	3

Fuente: Autoría propia

Tabla 15. Estimación de la probabilidad activo ingeniero auxiliar/ soporte técnico

ACTIVO TI	**INGENIERO AUXILIAR/ SOPORTE TÉCNICO**
ADMINISTRADOR	PIMIENTO CARDENAS WILSON MAURICIO
DEGRADACIÓN	40%
IMPACTO	3
TIPO DE ACTIVO	PERSONAL

Tipo	**ID**	**Amenaza**	**Exposición/Vulnerabilidad**	**Frecuencia (F)**	
ERRORES Y FALLOS NO INTENCIONADOS	**E.7**	Deficiencias en la organización	No hay exposición o vulnerabilidad, por parte de esta amenaza.	Baja	3
	E.19	Fugas de información	Las personas contratadas están atadas a cláusulas de confidencialidad.	Baja	3
	E.28	Indisponibilidad del personal	Daño a la disponibilidad de cada una de las personas	Baja	3

Tabla 15. Estimación de la probabilidad activo ingeniero auxiliar/ soporte técnico. (Continuación)

			influyentes en la dependencia.		
ATAQUES INTENCIONADOS	**A.28**	Indisponibilidad del personal	Daño a la disponibilidad de la información.	Baja	3
	A.29	Extorsión	Influenciarían al personal capacitado.	Baja	3
	A.30	Ingeniería social (picaresca)	Intervención de personas con fines no éticas.	Baja	3

Fuente: Autoría propia

1. ESTIMACIÓN DEL RIESGO

Tabla 16. Nivel de aceptación / tolerancia según MAGERIT

Aceptable	**Retenido.**
Tolerable	Para activos no críticos, y tratado como intolerable en caso de críticos.
Intolerable	Atención inmediata y monitoreo permanente.
Extremo	Tratado en forma similar al intolerable, pero a nivel de Gerencia General.

Fuente: MAGERIT V3.0

ACTIVO TI	**COPIAS DE SEGURIDAD DE CADA PC DE LA DEPENDENCIA DE SISTEMAS**
ADMINISTRADOR	PIMIENTO CARDENAS WILSON MAURICIO
DEGRADACIÓN	80%
IMPACTO	5
TIPO DE ACTIVO	DATOS/INFORMACIÓN

Tipo	ID	Amenaza	Exposición/Vulnerabilidad	RIESGO ACTUAL				
							4	Extremo
				Frecuencia (F)		R	NR	
ERRORES Y FALLOS NO INTENCIONADOS	**E.1**	Errores de los usuarios	Pérdida total o parcial del tiempo de ejecución de sus actividades, dependiendo de la gravedad del asunto.	Baja	3	15	4	Extremo
	E.2	Errores del administrador	Pérdida total o parcial del tiempo de ejecución de sus actividades, dependiendo de la gravedad del asunto.	Baja	3	15	4	Extremo
	E.15	Alteración accidental de la información	La dependencia cuenta con sistemas de cifrado y verificación (puerto – puerto) para el manejo de la movilidad de la información.	Baja	3	15	4	Extremo

Tabla 16. Nivel de aceptación / tolerancia según MAGERIT. (Continuación)

	E.18	Destrucción de información	El departamento de sistemas cuenta con copias de seguridad periódicas	Media	4	20	4	Extremo
	E.19	Fugas de información	Las personas contratadas están atadas a cláusulas de confidencialidad.	Media	4	20	4	Extremo
ATAQUES INTENCIONAD	**A.5**	Suplantación de la identidad del usuario	Acceso a personas que no cuenten con los permisos necesarios o con las credenciales necesarias.	Media	4	20	4	Extremo
	A.6	Abuso de privilegios de acceso	Abuso de cada uno de los derechos otorgados.	Media	4	20	4	Extremo
	A.11	Acceso no autorizado	Uso ilícito del hardware	Media	4	20	4	Extremo
	A.15	Modificación deliberada de la información	Datos erróneos en el momento de la movilización de la información.	Media	4	20	4	Extremo
	A.18	Destrucción de información	Perdida de la información.	Media	4	20	4	Extremo
	A.19	Divulgación de información	Información filtrada abiertamente a personas no correspondientes.	Media	4	20	4	Extremo

Fuente: Autoría propia

Tabla 17. Estimación del riesgo activo copias de seguridad de cada pc de las dependencias de la institución

ACTIVO TI	**COPIAS DE SEGURIDAD DE CADA PC DE LAS DEPENDENCIAS DE LA INSTITUCIÓN**							
ADMINISTRADOR	PIMIENTO CARDENAS WILSON MAURICIO							
DEGRADACIÓN	80%							
IMPACTO	5							
TIPO DE ACTIVO	DATOS/INFORMACIÓN							
Tipo	**ID**	**Amenaza**	**Exposición/Vulnerabilidad**	**RIESGO ACTUAL**				
							4	Extremo
				Frecuencia (F)		**R**	**NR**	
ERRORES Y FALLOS NO INTENCIONADOS	**E.1**	Errores de los usuarios	Pérdida total o parcial del tiempo de ejecución de sus actividades, dependiendo de la gravedad del asunto.	Baja	3	15	4	Extremo
	E.2	Errores del administrador	Pérdida total o parcial del tiempo de ejecución de sus actividades, dependiendo de la gravedad del asunto.	Baja	3	15	4	Extremo
	E.15	Alteración accidental de la información	La dependencia cuenta con sistemas de cifrado y verificación (puerto – puerto) para el manejo de la movilidad de la información.	Baja	3	15	4	Extremo
	E.18	Destrucción de información	El departamento de sistemas cuenta con copias de seguridad periódicas	Media	4	20	4	Extremo
	E.19	Fugas de información	Las personas contratadas están atadas a cláusulas de confidencialidad.	Media	4	20	4	Extremo

Tabla 17. Estimación del riesgo activo copias de seguridad de cada pc de las dependencias de la institución. (Continuación)

ATAQUES INTENCIONAD	**A.5**	Suplantación de la identidad del usuario	Acceso a personas que no cuenten con los permisos necesarios o con las credenciales necesarias.	Media	4	20	4	Extremo
	A.6	Abuso de privilegios de acceso	Abuso de cada uno de los derechos otorgados.	Media	4	20	4	Extremo
	A.11	Acceso no autorizado	Uso ilícito del hardware	Media	4	20	4	Extremo
	A.15	Modificación deliberada de la información	Datos erróneos en el momento de la movilización de la información.	Media	4	20	4	Extremo
	A.18	Destrucción de información	Perdida de la información.	Media	4	20	4	Extremo
	A.19	Divulgación de información	Información filtrada abiertamente a personas no correspondientes.	Media	4	20	4	Extremo

Fuente: Autoría propia

Tabla 18. Estimación del riesgo activo copias de seguridad de las configuraciones de los servidores

ACTIVO TI			COPIAS DE SEGURIDAD DE LAS CONFIGURACIONES DE LOS SERVIDORES					
ADMINISTRADOR			PIMIENTO CARDENAS WILSON MAURICIO					
DEGRADACIÓN			90%					
IMPACTO			5					
TIPO DE ACTIVO			DATOS/INFORMACIÓN					
Tipo	**ID**	**Amenaza**	**Exposición/Vulnerabilidad**	**RIESGO ACTUAL**				
							4	Extremo

Tabla 18. Estimación del riesgo activo copias de seguridad de las configuraciones de los servidores. (Continuación)

				Frecuencia (F)		R	NR	
ERRORES Y FALLOS NO INTENCIONADOS	**E.1**	Errores de los usuarios	Pérdida total o parcial del tiempo de ejecución de sus actividades, dependiendo de la gravedad del asunto.	Baja	3	15	4	Extremo
	E.2	Errores del administrador	Pérdida total o parcial del tiempo de ejecución de sus actividades, dependiendo de la gravedad del asunto.	Baja	3	15	4	Extremo
	E.15	Alteración accidental de la información	La dependencia cuenta con sistemas de cifrado y verificación (puerto – puerto) para el manejo de la movilidad de la información.	Baja	3	15	4	Extremo
	E.18	Destrucción de información	El departamento de sistemas cuenta con copias de seguridad periódicas	Media	4	20	4	Extremo
	E.19	Fugas de información	Las personas contratadas están atadas a cláusulas de confidencialidad.	Media	4	20	4	Extremo
ATAQUES INTENCIONAD	**A.5**	Suplantación de la identidad del usuario	Acceso a personas que no cuenten con los permisos necesarios o con las credenciales necesarias.	Media	4	20	4	Extremo
	A.6	Abuso de privilegios de acceso	Abuso de cada uno de los derechos otorgados.	Media	4	20	4	Extremo
	A.11	Acceso no autorizado	Uso ilícito del hardware	Media	4	20	4	Extremo
	A.15	Modificación deliberada de la información	Datos erróneos en el momento de la movilización de la información.	Media	4	20	4	Extremo
	A.18	Destrucción de información	Perdida de la información.	Media	4	20	4	Extremo
	A.19	Divulgación de información	Información filtrada abiertamente a personas no correspondientes.	Media	4	20	4	Extremo

Fuente: Autoría propia

Tabla 19. Estimación del riesgo activo contraseñas biométricas para acceso a la sala de servidor

ACTIVO TI	**CONTRASEÑAS BIOMÉTRICAS PARA ACCESO A LA SALA DE SERVIDOR**
ADMINISTRADOR	PIMIENTO CARDENAS WILSON MAURICIO
DEGRACIÓN	100%
IMPACTO	5
TIPO DE ACTIVO	DATOS/INFORMACIÓN

Tipo	ID	Amenaza	Exposición/Vulnerabilidad	RIESGO ACTUAL				
							4	Extremo
				Frecuencia (F)		R	NR	
ERRORES Y FALLOS NO INTENCIONADOS	**E.1**	Errores de los usuarios	Pérdida total o parcial del tiempo de ejecución de sus actividades, dependiendo de la gravedad del asunto.	Baja	3	15	4	Extremo
	E.2	Errores del administrador	Pérdida total o parcial del tiempo de ejecución de sus actividades, dependiendo de la gravedad del asunto.	Baja	3	15	4	Extremo
	E.15	Alteración accidental de la información	La dependencia cuenta con sistemas de cifrado y verificación (puerto – puerto) para el manejo de la movilidad de la información.	Baja	3	15	4	Extremo
	E.18	Destrucción de información	El departamento de sistemas cuenta con copias de seguridad periódicas	Media	4	20	4	Extremo
	E.19	Fugas de información	Las personas contratadas están atadas a cláusulas de confidencialidad.	Media	4	20	4	Extremo

Tabla 19. Estimación del riesgo activo contraseñas biométricas para acceso a la sala de servidor. (Continuación)

ATAQUES INTENCIONAD	**A.5**	Suplantación de la identidad del usuario	Acceso a personas que no cuenten con los permisos necesarios o con las credenciales necesarias.	Media	4	20	4	Extremo
	A.6	Abuso de privilegios de acceso	Abuso de cada uno de los derechos otorgados.	Media	4	20	4	Extremo
	A.11	Acceso no autorizado	Uso ilícito del hardware	Media	4	20	4	Extremo
	A.15	Modificación deliberada de la información	Datos erróneos en el momento de la movilización de la información.	Media	4	20	4	Extremo
	A.18	Destrucción de información	Perdida de la información.	Media	4	20	4	Extremo
	A.19	Divulgación de información	Información filtrada abiertamente a personas no correspondientes.	Media	4	20	4	Extremo

Fuente: Autoría propia

Tabla 20. Estimación del riesgo activo contraseñas de los usuarios que acceden a los servidores

ACTIVO TI	**CONTRASEÑAS DE LOS USUARIOS QUE ACCEDEN A LOS SERVIDORES**							
ADMINISTRADOR	PIMIENTO CARDENAS WILSON MAURICIO							
DEGRACIÓN	100%							
IMPACTO	5							
TIPO DE ACTIVO	DATOS/INFORMACIÓN							
Tipo	**ID**	**Amenaza**	**Exposición/Vulnerabilidad**	**RIESGO ACTUAL**				
							4	Extremo

Tabla 20. Estimación del riesgo activo contraseñas de los usuarios que acceden a los servidores. (Continuación)

				Frecuencia (F)		R	NR	
ERRORES Y FALLOS NO INTENCIONADOS	**E.1**	Errores de los usuarios	Pérdida total o parcial del tiempo de ejecución de sus actividades, dependiendo de la gravedad del asunto.	Baja	3	15	4	Extremo
	E.2	Errores del administrador	Pérdida total o parcial del tiempo de ejecución de sus actividades, dependiendo de la gravedad del asunto.	Baja	3	15	4	Extremo
	E.15	Alteración accidental de la información	La dependencia cuenta con sistemas de cifrado y verificación (puerto – puerto) para el manejo de la movilidad de la información.	Baja	3	15	4	Extremo
	E.18	Destrucción de información	El departamento de sistemas cuenta con copias de seguridad periódicas	Media	4	20	4	Extremo
	E.19	Fugas de información	Las personas contratadas están atadas a cláusulas de confidencialidad.	Media	4	20	4	Extremo
ATAQUES INTENCIONAD	**A.5**	Suplantación de la identidad del usuario	Acceso a personas que no cuenten con los permisos necesarios o con las credenciales necesarias.	Media	4	20	4	Extremo
	A.6	Abuso de privilegios de acceso	Abuso de cada uno de los derechos otorgados.	Media	4	20	4	Extremo

Tabla 20. Estimación del riesgo activo contraseñas de los usuarios que acceden a los servidores. (Continuación)

	A.11	Acceso no autorizado	Uso ilícito del hardware	Media	4	20	4	Extremo
	A.15	Modificación deliberada de la información	Datos erróneos en el momento de la movilización de la información.	Media	4	20	4	Extremo
	A.18	Destrucción de información	Perdida de la información.	Media	4	20	4	Extremo
	A.19	Divulgación de información	Información filtrada abiertamente a personas no correspondientes.	Media	4	20	4	Extremo

Fuente: Autoría propia

Tabla 21. Estimación del riesgo activo contraseñas del servidor de copias de seguridad

ACTIVO TI	**CONTRASEÑAS DEL SERVIDOR DE COPIAS DE SEGURIDAD**
ADMINISTRADOR	PIMIENTO CARDENAS WILSON MAURICIO
DEGRADACIÓN	100%
IMPACTO	5
TIPO DE ACTIVO	DATOS/INFORMACIÓN

Tipo	**ID**	**Amenaza**	**Exposición/Vulnerabilidad**	**RIESGO ACTUAL**				
							4	Extremo
				Frecuencia (F)		**R**	**NR**	
ERRORES Y FALLOS	**E.1**	Errores de los usuarios	Pérdida total o parcial del tiempo de ejecución de sus actividades, dependiendo de la gravedad del asunto.	Baja	3	15	4	Extremo

Tabla 21. Estimación del riesgo activo contraseñas del servidor de copias de seguridad. (Continuación)

	E.2	Errores del administrador	Pérdida total o parcial del tiempo de ejecución de sus actividades, dependiendo de la gravedad del asunto.	Baja	3	15	4	Extremo
	E.15	Alteración accidental de la información	La dependencia cuenta con sistemas de cifrado y verificación (puerto – puerto) para el manejo de la movilidad de la información.	Baja	3	15	4	Extremo
	E.18	Destrucción de información	El departamento de sistemas cuenta con copias de seguridad periódicas	Media	4	20	4	Extremo
	E.19	Fugas de información	Las personas contratadas están atadas a cláusulas de confidencialidad.	Media	4	20	4	Extremo
ATAQUES INTENCIONAD	**A.5**	Suplantación de la identidad del usuario	Acceso a personas que no cuenten con los permisos necesarios o con las credenciales necesarias.	Media	4	20	4	Extremo
	A.6	Abuso de privilegios de acceso	Abuso de cada uno de los derechos otorgados.	Media	4	20	4	Extremo
	A.11	Acceso no autorizado	Uso ilícito del hardware	Media	4	20	4	Extremo
	A.15	Modificación deliberada de la información	Datos erróneos en el momento de la movilización de la información.	Media	4	20	4	Extremo

Tabla 21. Estimación del riesgo activo contraseñas del servidor de copias de seguridad. (Continuación)

	A.18	Destrucción de información	Perdida de la información.	Media	4	20	4	Extremo
	A.19	Divulgación de información	Información filtrada abiertamente a personas no correspondientes.	Media	4	20	4	Extremo

Fuente: Autoría propia

Tabla 22. Estimación del riesgo activo contraseñas del usuario de los pc de las demás dependencias

ACTIVO TI	**CONTRASEÑAS DE LOS USUARIOS DE LOS PC DE LAS DEMÁS DEPENDENCIAS**
ADMINISTRADOR	PIMIENTO CARDENAS WILSON MAURICIO
DEGRACIÓN	85%
IMPACTO	5
TIPO DE ACTIVO	CLAVES CRIPTOGRÁFICAS

Tipo	**ID**	**Amenaza**	**Exposición/Vulnerabilidad**	**RIESGO ACTUAL**				
							3.81	Intolerable
				Frecuencia (F)		**R**	**NR**	
ERRORES Y FALLOS NO INTENCIONADOS	**E.1**	Errores de los usuarios	Pérdida total o parcial del tiempo de ejecución de sus actividades, dependiendo de la gravedad del asunto.	Muy baja	2	10	3	Intolerable
	E.2	Errores del administrador	Pérdida total o parcial del tiempo de ejecución de sus actividades, dependiendo de la gravedad del asunto.	Muy baja	2	10	3	Intolerable

Tabla 22. Estimación del riesgo activo contraseñas del usuario de los pc de las demás dependencias. (Continuación)

	E.15	Alteración accidental de la información	La dependencia cuenta con sistemas de cifrado y verificación (puerto – puerto) para el manejo de la movilidad de la información.	Media	4	20	4	Extremo
	E.18	Destrucción de información	El departamento de sistemas cuenta con copias de seguridad periódicas	Media	4	20	4	Extremo
	E.19	Fugas de información	Las personas contratadas están atadas a cláusulas de confidencialidad.	Media	4	20	4	Extremo
ATAQUES INTENCIONAD	**A.5**	Suplantación de la identidad del usuario	Acceso a personas que no cuenten con los permisos necesarios o con las credenciales necesarias.	Media	4	20	4	Extremo
	A.6	Abuso de privilegios de acceso	Abuso de cada uno de los derechos otorgados.	Media	4	20	4	Extremo
	A.11	Acceso no autorizado	Uso ilícito del hardware	Media	4	20	4	Extremo
	A.15	Modificación deliberada de la información	Datos erróneos en el momento de la movilización de la información.	Media	4	20	4	Extremo
	A.18	Destrucción de información	Perdida de la información.	Media	4	20	4	Extremo

Tabla 22. Estimación del riesgo activo contraseñas del usuario de los pc de las demás dependencias. (Continuación)

	A.19	Divulgación de información	Información filtrada abiertamente a personas no correspondientes.	Media	4	20	4	Extremo

Fuente: Autoría propia

Tabla 23. Estimación del riesgo activo contraseña sensor biométrico

ACTIVO TI	**CONTRASEÑA SENSOR BIOMÉTRICO**
ADMINISTRADOR	PIMIENTO CARDENAS WILSON MAURICIO
DEGRADACIÓN	100%
IMPACTO	5
TIPO DE ACTIVO	CLAVES CRIPTOGRÁFICAS

Tipo	ID	Amenaza	Exposición/Vulnerabilidad	RIESGO ACTUAL				
							3.81	Intolerable
				Frecuencia (F)		R	NR	
ERRORES Y FALLOS NO INTENCIONADOS	**E.1**	Errores de los usuarios	Pérdida total o parcial del tiempo de ejecución de sus actividades, dependiendo de la gravedad del asunto.	Muy baja	2	10	3	Intolerable
	E.2	Errores del administrador	Pérdida total o parcial del tiempo de ejecución de sus actividades, dependiendo de la gravedad del asunto.	Muy baja	2	10	3	Intolerable
	E.15	Alteración accidental de la información	La dependencia cuenta con sistemas de cifrado y verificación (puerto – puerto) para el manejo de la movilidad de la información.	Media	4	20	4	Extremo
	E.18	Destrucción de información	El departamento de sistemas cuenta con copias de seguridad periódicas	Media	4	20	4	Extremo

Tabla 23. Estimación del riesgo activo contraseña sensor biométrico. (Continuación)

	E.19	Fugas de información	Las personas contratadas están atadas a cláusulas de confidencialidad.	Media	4	20	4	Extremo
ATAQUES INTENCIONAD	**A.5**	Suplantación de la identidad del usuario	Acceso a personas que no cuenten con los permisos necesarios o con las credenciales necesarias.	Media	4	20	4	Extremo
	A.6	Abuso de privilegios de acceso	Abuso de cada uno de los derechos otorgados.	Media	4	20	4	Extremo
	A.11	Acceso no autorizado	Uso ilícito del hardware	Media	4	20	4	Extremo
	A.15	Modificación deliberada de la información	Datos erróneos en el momento de la movilización de la información.	Media	4	20	4	Extremo
	A.18	Destrucción de información	Perdida de la información.	Media	4	20	4	Extremo
	A.19	Divulgación de información	Información filtrada abiertamente a personas no correspondientes.	Media	4	20	4	Extremo

Fuente: Autoría propia

Tabla 24. Estimación del riesgo activo código de confirmación para acceso a la sala de servidor

ACTIVO TI	**CÓDIGO DE ACCESO A LA SALA DEL SERVIDOR**
ADMINISTRADOR	PIMIENTO CARDENAS WILSON MAURICIO

Tabla 24. Estimación del riesgo activo código de confirmación para acceso a la sala de servidor. (Continuación)

DEGRACIÓN	100%
IMPACTO	5
TIPO DE ACTIVO	CLAVES CRIPTOGRÁFICAS

Tipo	ID	Amenaza	Exposición/Vulnerabilidad	RIESGO ACTUAL				
							3.81	Intolerable
				Frecuencia (F)		R	NR	
ERRORES Y FALLOS NO INTENCIONADOS	**E.1**	Errores de los usuarios	Pérdida total o parcial del tiempo de ejecución de sus actividades, dependiendo de la gravedad del asunto.	Muy baja	2	10	3	Intolerable
	E.2	Errores del administrador	Pérdida total o parcial del tiempo de ejecución de sus actividades, dependiendo de la gravedad del asunto.	Muy baja	2	10	3	Intolerable
	E.15	Alteración accidental de la información	La dependencia cuenta con sistemas de cifrado y verificación (puerto – puerto) para el manejo de la movilidad de la información.	Media	4	20	4	Extremo
	E.18	Destrucción de información	El departamento de sistemas cuenta con copias de seguridad periódicas	Media	4	20	4	Extremo
	E.19	Fugas de información	Las personas contratadas están atadas a cláusulas de confidencialidad.	Media	4	20	4	Extremo

Tabla 24. Estimación del riesgo activo código de confirmación para acceso a la sala de servidor. (Continuación)

ATAQUES INTENCIONAD	**A.5**	Suplantación de la identidad del usuario	Acceso a personas que no cuenten con los permisos necesarios o con las credenciales necesarias.	Media	4	20	4	Extremo
	A.6	Abuso de privilegios de acceso	Abuso de cada uno de los derechos otorgados.	Media	4	20	4	Extremo
	A.11	Acceso no autorizado	Uso ilícito del hardware	Media	4	20	4	Extremo
	A.15	Modificación deliberada de la información	Datos erróneos en el momento de la movilización de la información.	Media	4	20	4	Extremo
	A.18	Destrucción de información	Perdida de la información.	Media	4	20	4	Extremo
	A.19	Divulgación de información	Información filtrada abiertamente a personas no correspondientes.	Media	4	20	4	Extremo

Fuente: Autoría propia

Tabla 25. Estimación del riesgo activo sistema de registro y control académico (RYCA) V.1

ACTIVO TI	**SISTEMA DE REGISTRO Y CONTROL ACADÉMICO (RYCA) V.1**							
ADMINISTRADOR	PIMIENTO CARDENAS WILSON MAURICIO							
DEGRADACIÓN	90%							
IMPACTO	5							
TIPO DE ACTIVO	SOFTWARE							
Tipo	**ID**	**Amenaza**	**Exposición/Vulnerabilidad**	**RIESGO ACTUAL**				
							4	Extremo

Tabla 25. Estimación del riesgo activo sistema de registro y control académico (RYCA) V.1. (Continuación)

				Frecuencia (F)		R	NR	
DE ORIGEN INDUSTRIAL	**I.5**	Avería de origen físico o lógico	La manipulación por parte de cada uno de los componentes encontrados en la dependencia, como también por defectos de los componentes desde fabrica	Baja	3	15	4	Extremo
ERRORES Y FALLOS NO INTENCIONADOS	**E.1**	Errores de los usuarios	Pérdida total o parcial del tiempo de ejecución de sus actividades, dependiendo de la gravedad del asunto.	Baja	3	15	4	Extremo
	E.2	Errores del administrador	Pérdida total o parcial del tiempo de ejecución de sus actividades, dependiendo de la gravedad del asunto.	Baja	3	15	4	Extremo
	E.8	Difusión de software dañino	La dependencia cuenta con antivirus capaces de controlar software malicioso	Baja	3	15	4	Extremo
	E.9	Errores de [re-] encaminamiento	La dependencia cuenta con sistemas de cifrado y verificación (puerto – puerto) para el manejo de la movilidad de la información.	Baja	3	15	4	Extremo
	E.10	Errores de secuencia	La dependencia cuenta con sistemas de cifrado y verificación (puerto – puerto) para el manejo de la movilidad de la información.	Baja	3	15	4	Extremo

Tabla 25. Estimación del riesgo activo sistema de registro y control académico (RYCA) V.1. (Continuación)

	E.15	Alteración accidental de la información	La dependencia cuenta con sistemas de cifrado y verificación (puerto – puerto) para el manejo de la movilidad de la información.	Baja	3	15	4	Extremo
	E.18	Destrucción de información	El departamento de sistemas cuenta con copias de seguridad periódicas	Baja	3	15	4	Extremo
	E.19	Fugas de información	Las personas contratadas están atadas a cláusulas de confidencialidad.	Baja	3	15	4	Extremo
	E.20	Vulnerabilidades de los programas (software)	La dependencia cuenta con un servidor (personal) para llevar a cabo cada uno de los softwares empleados para la institución.	Baja	3	15	4	Extremo
	E.21	Errores de mantenimiento / actualización de programas (software)	Falla de funcionamiento del software.	Baja	3	15	4	Extremo
ATAQUES INTENCIONAD	**A.5**	Suplantación de la identidad del usuario	Acceso a personas que no cuenten con los permisos necesarios o con las credenciales necesarias.	Baja	3	15	4	Extremo
	A.6	Abuso de privilegios de acceso	Abuso de cada uno de los derechos otorgados.	Baja	3	15	4	Extremo

Tabla 25. Estimación del riesgo activo sistema de registro y control académico (RYCA) V.1. (Continuación)

	A.7	Uso no previsto	Implementación de recursos (económicos y de tiempo) en actividades no relacionadas.	Baja	3	15	4	Extremo
	A.8	Difusión de software dañino	Afectación en los sistemas de información y los procesos que ello conlleva.	Baja	3	15	4	Extremo
	A.9	[Re-]encaminamiento de mensajes	La dependencia cuenta con sistemas de cifrado y verificación (puerto – puerto) para el manejo de la movilidad de la información.	Baja	3	15	4	Extremo
	A.10	Alteración de secuencia	Alteración de datos.	Baja	3	15	4	Extremo
	A.11	Acceso no autorizado	Uso ilícito del hardware	Baja	3	15	4	Extremo
	A.15	Modificación deliberada de la información	Datos erróneos en el momento de la movilización de la información.	Baja	3	15	4	Extremo
	A.18	Destrucción de información	Perdida de la información.	Baja	3	15	4	Extremo
	A.19	Divulgación de información	Información filtrada abiertamente a personas no correspondientes.	Baja	3	15	4	Extremo

Tabla 25. Estimación del riesgo activo sistema de registro y control académico (RYCA) V.1. (Continuación)

	A.22	Manipulación de programas	Alteración del funcionamiento de cada uno de los programas de la dependencia.	Baja	3	15	4	Extremo

Fuente: Autoría propia

Tabla 26. Estimación del riesgo activo sistema de registro y control académico (RYCA) V.2.0

ACTIVO TI	**SISTEMA DE REGISTRO Y CONTROL ACADÉMICO (RYCA) V.2.0**
ADMINISTRADOR	PIMIENTO CARDENAS WILSON MAURICIO
DEGRADACIÓN	90%
IMPACTO	5
TIPO DE ACTIVO	SOFTWARE

Tipo	ID	Amenaza	Exposición/Vulnerabilidad	RIESGO ACTUAL				
							4	Extremo
				Frecuencia (F)		**R**	**NR**	
DE ORIGEN INDUSTRIAL	**I.5**	Avería de origen físico o lógico	La manipulación por parte de cada uno de los componentes encontrados en la dependencia, como también por defectos de los componentes desde fabrica	Baja	3	15	4	Extremo
ERRORES Y FALLOS NO INTENCIONADOS	**E.1**	Errores de los usuarios	Pérdida total o parcial del tiempo de ejecución de sus actividades, dependiendo de la gravedad del asunto.	Baja	3	15	4	Extremo
	E.2	Errores del administrador	Pérdida total o parcial del tiempo de ejecución de sus actividades, dependiendo de la gravedad del asunto.	Baja	3	15	4	Extremo

Tabla 26. Estimación del riesgo activo sistema de registro y control académico (RYCA) V.2.0. (Continuación)

	E.8	Difusión de software dañino	La dependencia cuenta con antivirus capaces de controlar software malicioso	Baja	3	15	4	Extremo
	E.9	Errores de [re-] encaminamiento	La dependencia cuenta con sistemas de cifrado y verificación (puerto – puerto) para el manejo de la movilidad de la información.	Baja	3	15	4	Extremo
	E.10	Errores de secuencia	La dependencia cuenta con sistemas de cifrado y verificación (puerto – puerto) para el manejo de la movilidad de la información.	Baja	3	15	4	Extremo
	E.15	Alteración accidental de la información	La dependencia cuenta con sistemas de cifrado y verificación (puerto – puerto) para el manejo de la movilidad de la información.	Baja	3	15	4	Extremo
	E.18	Destrucción de información	El departamento de sistemas cuenta con copias de seguridad periódicas	Baja	3	15	4	Extremo
	E.19	Fugas de información	Las personas contratadas están atadas a cláusulas de confidencialidad.	Baja	3	15	4	Extremo
	E.20	Vulnerabilidades de los programas (software)	La dependencia cuenta con un servidor (personal) para llevar a cabo cada uno de los softwares empleados para la institución.	Baja	3	15	4	Extremo

Tabla 26. Estimación del riesgo activo sistema de registro y control académico (RYCA) V.2.0. (Continuación)

	E.21	Errores de mantenimiento / actualización de programas (software)	Falla de funcionamiento del software.	Baja	3	15	4	Extremo
ATAQUES INTENCIONAD	**A.5**	Suplantación de la identidad del usuario	Acceso a personas que no cuenten con los permisos necesarios o con las credenciales necesarias.	Baja	3	15	4	Extremo
	A.6	Abuso de privilegios de acceso	Abuso de cada uno de los derechos otorgados.	Baja	3	15	4	Extremo
	A.7	Uso no previsto	Implementación de recursos (económicos y de tiempo) en actividades no relacionadas.	Baja	3	15	4	Extremo
	A.8	Difusión de software dañino	Afectación en los sistemas de información y los procesos que ello conlleva.	Baja	3	15	4	Extremo
	A.9	[Re-]encaminamiento de mensajes	La dependencia cuenta con sistemas de cifrado y verificación (puerto – puerto) para el manejo de la movilidad de la información.	Baja	3	15	4	Extremo
	A.10	Alteración de secuencia	Alteración de datos.	Baja	3	15	4	Extremo
	A.11	Acceso no autorizado	Uso ilícito del hardware	Baja	3	15	4	Extremo

Tabla 26. Estimación del riesgo activo sistema de registro y control académico (RYCA) V.2.0. (Continuación)

	A.15	Modificación deliberada de la información	Datos erróneos en el momento de la movilización de la información.	Baja	3	15	4	Extremo
	A.18	Destrucción de información	Perdida de la información.	Baja	3	15	4	Extremo
	A.19	Divulgación de información	Información filtrada abiertamente a personas no correspondientes.	Baja	3	15	4	Extremo
	A.22	Manipulación de programas	Alteración del funcionamiento de cada uno de los programas de la dependencia.	Baja	3	15	4	Extremo

Fuente: Autoría propia

Tabla 27. Estimación del riesgo activo página oficial del ITFIP

ACTIVO TI	**PÁGINA OFICIAL DEL ITFIP**
ADMINISTRADOR	PIMIENTO CARDENAS WILSON MAURICIO
DEGRADACIÓN	50%
IMPACTO	3
TIPO DE ACTIVO	SOFTWARE

Tipo	**ID**	**Amenaza**	**Exposición/Vulnerabilidad**	**RIESGO ACTUAL**				
							3	Intolerable
				Frecuencia (F)		**R**	**NR**	
DE ORIGEN	**I.5**	Avería de origen físico o lógico	La manipulación por parte de cada uno de los componentes encontrados en la dependencia, como también por	Baja	3	9	3	Intolerable

Tabla 27. Estimación del riesgo activo página oficial del ITFIP. (Continuación)

			defectos de los componentes desde fabrica					
ERRORES Y FALLOS NO INTENCIONADOS	**E.1**	Errores de los usuarios	Pérdida total o parcial del tiempo de ejecución de sus actividades, dependiendo de la gravedad del asunto.	Baja	3	9	3	Intolerable
	E.2	Errores del administrador	Pérdida total o parcial del tiempo de ejecución de sus actividades, dependiendo de la gravedad del asunto.	Baja	3	9	3	Intolerable
	E.8	Difusión de software dañino	La dependencia cuenta con antivirus capaces de controlar software malicioso	Baja	3	9	3	Intolerable
	E.9	Errores de [re-] encaminamiento	La dependencia cuenta con sistemas de cifrado y verificación (puerto – puerto) para el manejo de la movilidad de la información.	Baja	3	9	3	Intolerable
	E.10	Errores de secuencia	La dependencia cuenta con sistemas de cifrado y verificación (puerto – puerto) para el manejo de la movilidad de la información.	Baja	3	9	3	Intolerable

Tabla 27. Estimación del riesgo activo página oficial del ITFIP. (Continuación)

	E.15	Alteración accidental de la información	La dependencia cuenta con sistemas de cifrado y verificación (puerto – puerto) para el manejo de la movilidad de la información.	Baja	3	9	3	Intolerable
	E.18	Destrucción de información	El departamento de sistemas cuenta con copias de seguridad periódicas	Baja	3	9	3	Intolerable
	E.19	Fugas de información	Las personas contratadas están atadas a cláusulas de confidencialidad.	Baja	3	9	3	Intolerable
	E.20	Vulnerabilidades de los programas (software)	La dependencia cuenta con un servidor (personal) para llevar a cabo cada uno de los softwares empleados para la institución.	Baja	3	9	3	Intolerable
	E.21	Errores de mantenimiento / actualización de programas (software)	Falla de funcionamiento del software.	Baja	3	9	3	Intolerable
ATAQUES INTENCIONAD	**A.5**	Suplantación de la identidad del usuario	Acceso a personas que no cuenten con los permisos necesarios o con las credenciales necesarias.	Baja	3	9	3	Intolerable
	A.6	Abuso de privilegios de acceso	Abuso de cada uno de los derechos otorgados.	Baja	3	9	3	Intolerable

Tabla 27. Estimación del riesgo activo página oficial del ITFIP. (Continuación)

	A.7	Uso no previsto	Implementación de recursos (económicos y de tiempo) en actividades no relacionadas.	Baja	3	9	3	Intolerable
	A.8	Difusión de software dañino	Afectación en los sistemas de información y los procesos que ello conlleva.	Baja	3	9	3	Intolerable
	A.9	[Re-]encaminamiento de mensajes	La dependencia cuenta con sistemas de cifrado y verificación (puerto – puerto) para el manejo de la movilidad de la información.	Baja	3	9	3	Intolerable
	A.10	Alteración de secuencia	Alteración de datos.	Baja	3	9	3	Intolerable
	A.11	Acceso no autorizado	Uso ilícito del hardware	Baja	3	9	3	Intolerable
	A.15	Modificación deliberada de la información	Datos erróneos en el momento de la movilización de la información.	Baja	3	9	3	Intolerable
	A.18	Destrucción de información	Perdida de la información.	Baja	3	9	3	Intolerable
	A.19	Divulgación de información	Información filtrada abiertamente a personas no correspondientes.	Baja	3	9	3	Intolerable

Tabla 27. Estimación del riesgo activo página oficial del ITFIP. (Continuación)

	A.22	Manipulación de programas	Alteración del funcionamiento de cada uno de los programas de la dependencia.	Baja	3	9	3	Intolerable

Fuente: Autoría propia

Tabla 28. Estimación del riesgo activo Google Chrome

ACTIVO TI	**NAVEGADOR GOOGLE CHROME**
ADMINISTRADOR	PIMIENTO CARDENAS WILSON MAURICIO
DEGRADACIÓN	10%
IMPACTO	1
TIPO DE ACTIVO	SOFTWARE

Tipo	ID	Amenaza	Exposición/Vulnerabilidad	RIESGO ACTUAL				
							2	Tolerable
				Frecuencia (F)		**R**	**NR**	
DE ORIGEN INDUSTRIAL	**I.5**	Avería de origen físico o lógico	La manipulación por parte de cada uno de los componentes encontrados en la dependencia, como también por defectos de los componentes desde fabrica	Baja	3	3	2	Tolerable
ERRORES Y FALLOS NO INTENCIONADOS	**E.1**	Errores de los usuarios	Pérdida total o parcial del tiempo de ejecución de sus actividades, dependiendo de la gravedad del asunto.	Baja	3	3	2	Tolerable
	E.2	Errores del administrador	Pérdida total o parcial del tiempo de ejecución de sus actividades, dependiendo de la gravedad del asunto.	Baja	3	3	2	Tolerable

Tabla 28. Estimación del riesgo activo Google Chrome. (Continuación)

	E.8	Difusión de software dañino	La dependencia cuenta con antivirus capaces de controlar software malicioso	Baja	3	3	2	Tolerable
	E.9	Errores de [re-] encaminamiento	La dependencia cuenta con sistemas de cifrado y verificación (puerto – puerto) para el manejo de la movilidad de la información.	Baja	3	3	2	Tolerable
	E.10	Errores de secuencia	La dependencia cuenta con sistemas de cifrado y verificación (puerto – puerto) para el manejo de la movilidad de la información.	Baja	3	3	2	Tolerable
	E.15	Alteración accidental de la información	La dependencia cuenta con sistemas de cifrado y verificación (puerto – puerto) para el manejo de la movilidad de la información.	Baja	3	3	2	Tolerable
	E.18	Destrucción de información	El departamento de sistemas cuenta con copias de seguridad periódicas	Baja	3	3	2	Tolerable
	E.19	Fugas de información	Las personas contratadas están atadas a cláusulas de confidencialidad.	Baja	3	3	2	Tolerable
	E.20	Vulnerabilidades de los programas (software)	La dependencia cuenta con un servidor (personal) para llevar a cabo cada uno de los softwares empleados para la institución.	Baja	3	3	2	Tolerable

Tabla 28. Estimación del riesgo activo Google Chrome. (Continuación)

	E.21	Errores de mantenimiento / actualización de programas (software)	Falla de funcionamiento del software.	Baja	3	3	2	Tolerable
ATAQUES INTENCIONAD	**A.5**	Suplantación de la identidad del usuario	Acceso a personas que no cuenten con los permisos necesarios o con las credenciales necesarias.	Baja	3	3	2	Tolerable
	A.6	Abuso de privilegios de acceso	Abuso de cada uno de los derechos otorgados.	Baja	3	3	2	Tolerable
	A.7	Uso no previsto	Implementación de recursos (económicos y de tiempo) en actividades no relacionadas.	Baja	3	3	2	Tolerable
	A.8	Difusión de software dañino	Afectación en los sistemas de información y los procesos que ello conlleva.	Baja	3	3	2	Tolerable
	A.9	[Re-]encaminamiento de mensajes	La dependencia cuenta con sistemas de cifrado y verificación (puerto – puerto) para el manejo de la movilidad de la información.	Baja	3	3	2	Tolerable
	A.10	Alteración de secuencia	Alteración de datos.	Baja	3	3	2	Tolerable
	A.11	Acceso no autorizado	Uso ilícito del hardware	Baja	3	3	2	Tolerable

Tabla 28. Estimación del riesgo activo Google Chrome. (Continuación)

	A.15	Modificación deliberada de la información	Datos erróneos en el momento de la movilización de la información.	Baja	3	3	2	Tolerable
	A.18	Destrucción de información	Perdida de la información.	Baja	3	3	2	Tolerable
	A.19	Divulgación de información	Información filtrada abiertamente a personas no correspondientes.	Baja	3	3	2	Tolerable
	A.22	Manipulación de programas	Alteración del funcionamiento de cada uno de los programas de la dependencia.	Baja	3	3	2	Tolerable

Fuente: Autoría propia

Tabla 29. Estimación del riesgo activo Mozilla Firefox

ACTIVO TI	**NAVEGADOR MOZILLA FIREFOX**							
ADMINISTRADOR	PIMIENTO CARDENAS WILSON MAURICIO							
DEGRADACIÓN	15%							
IMPACTO	1							
TIPO DE ACTIVO	SOFTWARE							
Tipo	**ID**	**Amenaza**	**Exposición/Vulnerabilidad**	**RIESGO ACTUAL**				
							2	Tolerable
				Frecuencia (F)		**R**	**NR**	
DE ORIGEN	**I.5**	Avería de origen físico o lógico	La manipulación por parte de cada uno de los componentes encontrados en la dependencia, como también por	Baja	**3**	**3**	2	Tolerable

Tabla 29. Estimación del riesgo activo Mozilla Firefox. (Continuación)

			defectos de los componentes desde fabrica					
ERRORES Y FALLOS NO INTENCIONADOS	**E.1**	Errores de los usuarios	Pérdida total o parcial del tiempo de ejecución de sus actividades, dependiendo de la gravedad del asunto.	Baja	**3**	**3**	2	Tolerable
	E.2	Errores del administrador	Pérdida total o parcial del tiempo de ejecución de sus actividades, dependiendo de la gravedad del asunto.	Baja	**3**	**3**	2	Tolerable
	E.8	Difusión de software dañino	La dependencia cuenta con antivirus capaces de controlar software malicioso	Baja	**3**	**3**	2	Tolerable
	E.9	Errores de [re-] encaminamiento	La dependencia cuenta con sistemas de cifrado y verificación (puerto – puerto) para el manejo de la movilidad de la información.	Baja	**3**	**3**	2	Tolerable
	E.10	Errores de secuencia	La dependencia cuenta con sistemas de cifrado y verificación (puerto – puerto) para el manejo de la movilidad de la información.	Baja	**3**	**3**	2	Tolerable
	E.15	Alteración accidental de la información	La dependencia cuenta con sistemas de cifrado y verificación (puerto – puerto) para el manejo de la movilidad de la información.	Baja	**3**	**3**	2	Tolerable

Tabla 29. Estimación del riesgo activo Mozilla Firefox. (Continuación)

	E.18	Destrucción de información	El departamento de sistemas cuenta con copias de seguridad periódicas	Baja	**3**	**3**	2	Tolerable
	E.19	Fugas de información	Las personas contratadas están atadas a cláusulas de confidencialidad.	Baja	**3**	**3**	2	Tolerable
	E.20	Vulnerabilidades de los programas (software)	La dependencia cuenta con un servidor (personal) para llevar a cabo cada uno de los softwares empleados para la institución.	Baja	**3**	**3**	2	Tolerable
	E.21	Errores de mantenimiento / actualización de programas (software)	Falla de funcionamiento del software.	Baja	**3**	**3**	2	Tolerable
ATAQUES INTENCIONAD	**A.5**	Suplantación de la identidad del usuario	Acceso a personas que no cuenten con los permisos necesarios o con las credenciales necesarias.	Baja	**3**	**3**	2	Tolerable
	A.6	Abuso de privilegios de acceso	Abuso de cada uno de los derechos otorgados.	Baja	**3**	**3**	2	Tolerable
	A.7	Uso no previsto	Implementación de recursos (económicos y de tiempo) en actividades no relacionadas.	Baja	**3**	**3**	2	Tolerable

Tabla 29. Estimación del riesgo activo Mozilla Firefox. (Continuación)

	A.8	Difusión de software dañino	Afectación en los sistemas de información y los procesos que ello conlleva.	Baja	**3**	**3**	2	Tolerable
	A.9	[Re-]encaminamiento de mensajes	La dependencia cuenta con sistemas de cifrado y verificación (puerto – puerto) para el manejo de la movilidad de la información.	Baja	**3**	**3**	2	Tolerable
	A.10	Alteración de secuencia	Alteración de datos.	Baja	**3**	**3**	2	Tolerable
	A.11	Acceso no autorizado	Uso ilícito del hardware	Baja	**3**	**3**	2	Tolerable
	A.15	Modificación deliberada de la información	Datos erróneos en el momento de la movilización de la información.	Baja	**3**	**3**	2	Tolerable
	A.18	Destrucción de información	Perdida de la información.	Baja	**3**	**3**	2	Tolerable
	A.19	Divulgación de información	Información filtrada abiertamente a personas no correspondientes.	Baja	**3**	**3**	2	Tolerable
	A.22	Manipulación de programas	Alteración del funcionamiento de cada uno de los programas de la dependencia.	Baja	**3**	**3**	2	Tolerable

Fuente: Autoría propia

Tabla 30. Estimación del riesgo activo safari

ACTIVO TI	**NAVEGADOR SAFARI**
ADMINISTRADOR	PIMIENTO CARDENAS WILSON MAURICIO

Tabla 30. Estimación del riesgo activo safari. (Continuación)

DEGRADACIÓN	10%
IMPACTO	1
TIPO DE ACTIVO	SOFTWARE

Tipo	ID	Amenaza	Exposición/Vulnerabilidad	RIESGO ACTUAL				
							2	Tolerable
				Frecuencia (F)		R	NR	
DE ORIGEN INDUSTRIAL	**I.5**	Avería de origen físico o lógico	La manipulación por parte de cada uno de los componentes encontrados en la dependencia, como también por defectos de los componentes desde fabrica	Baja	3	3	2	Tolerable
ERRORES Y FALLOS NO INTENCIONADOS	**E.1**	Errores de los usuarios	Pérdida total o parcial del tiempo de ejecución de sus actividades, dependiendo de la gravedad del asunto.	Baja	3	3	2	Tolerable
	E.2	Errores del administrador	Pérdida total o parcial del tiempo de ejecución de sus actividades, dependiendo de la gravedad del asunto.	Baja	3	3	2	Tolerable
	E.8	Difusión de software dañino	La dependencia cuenta con antivirus capaces de controlar software malicioso	Baja	3	3	2	Tolerable
	E.9	Errores de [re-] encaminamiento	La dependencia cuenta con sistemas de cifrado y verificación (puerto – puerto) para el manejo de la movilidad de la información.	Baja	3	3	2	Tolerable

Tabla 30. Estimación del riesgo activo safari. (Continuación)

	E.10	Errores de secuencia	La dependencia cuenta con sistemas de cifrado y verificación (puerto – puerto) para el manejo de la movilidad de la información.	Baja	3	3	2	Tolerable
	E.15	Alteración accidental de la información	La dependencia cuenta con sistemas de cifrado y verificación (puerto – puerto) para el manejo de la movilidad de la información.	Baja	3	3	2	Tolerable
	E.18	Destrucción de información	El departamento de sistemas cuenta con copias de seguridad periódicas	Baja	3	3	2	Tolerable
	E.19	Fugas de información	Las personas contratadas están atadas a cláusulas de confidencialidad.	Baja	3	3	2	Tolerable
	E.20	Vulnerabilidades de los programas (software)	La dependencia cuenta con un servidor (personal) para llevar a cabo cada uno de los softwares empleados para la institución.	Baja	3	3	2	Tolerable
	E.21	Errores de mantenimiento / actualización de programas (software)	Falla de funcionamiento del software.	Baja	3	3	2	Tolerable
ATAQUES INTENC	**A.5**	Suplantación de la identidad del usuario	Acceso a personas que no cuenten con los permisos necesarios o con las credenciales necesarias.	Baja	3	3	2	Tolerable

Tabla 30. Estimación del riesgo activo safari. (Continuación)

	A.6	Abuso de privilegios de acceso	Abuso de cada uno de los derechos otorgados.	Baja	3	3	2	Tolerable
	A.7	Uso no previsto	Implementación de recursos (económicos y de tiempo) en actividades no relacionadas.	Baja	3	3	2	Tolerable
	A.8	Difusión de software dañino	Afectación en los sistemas de información y los procesos que ello conlleva.	Baja	3	3	2	Tolerable
	A.9	[Re-]encaminamiento de mensajes	La dependencia cuenta con sistemas de cifrado y verificación (puerto – puerto) para el manejo de la movilidad de la información.	Baja	3	3	2	Tolerable
	A.10	Alteración de secuencia	Alteración de datos.	Baja	3	3	2	Tolerable
	A.11	Acceso no autorizado	Uso ilícito del hardware	Baja	3	3	2	Tolerable
	A.15	Modificación deliberada de la información	Datos erróneos en el momento de la movilización de la información.	Baja	3	3	2	Tolerable
	A.18	Destrucción de información	Perdida de la información.	Baja	3	3	2	Tolerable
	A.19	Divulgación de información	Información filtrada abiertamente a personas no correspondientes.	Baja	3	3	2	Tolerable

Tabla 30. Estimación del riesgo activo safari. (Continuación)

	A.22	Manipulación de programas	Alteración del funcionamiento de cada uno de los programas de la dependencia.	Baja	3	3	2	Tolerable

Fuente: Autoría propia

Tabla 31. Estimación del riesgo activo Microsoft office 2013

ACTIVO TI	**MICROSOFT OFFICE 2013**
ADMINISTRADOR	PIMIENTO CARDENAS WILSON MAURICIO
DEGRADACIÓN	20%
IMPACTO	3
TIPO DE ACTIVO	SOFTWARE

Tipo	ID	Amenaza	Exposición/Vulnerabilidad	RIESGO ACTUAL				
							3	Intolerable
				Frecuencia (F)		**R**	**NR**	
DE ORIGEN INDUSTRIAL	**I.5**	Avería de origen físico o lógico	La manipulación por parte de cada uno de los componentes encontrados en la dependencia, como también por defectos de los componentes desde fabrica	Baja	3	9	3	Intolerable
ERRORES Y FALLOS NO INTENCIONADOS	**E.1**	Errores de los usuarios	Pérdida total o parcial del tiempo de ejecución de sus actividades, dependiendo de la gravedad del asunto.	Baja	3	9	3	Intolerable
	E.2	Errores del administrador	Pérdida total o parcial del tiempo de ejecución de sus actividades,	Baja	3	9	3	Intolerable

Tabla 31. Estimación del riesgo activo Microsoft office 2013. (Continuación)

			dependiendo de la gravedad del asunto.					
	E.8	Difusión de software dañino	La dependencia cuenta con antivirus capaces de controlar software malicioso	Baja	3	9	3	Intolerable
	E.9	Errores de [re-] encaminamiento	La dependencia cuenta con sistemas de cifrado y verificación (puerto – puerto) para el manejo de la movilidad de la información.	Baja	3	9	3	Intolerable
	E.10	Errores de secuencia	La dependencia cuenta con sistemas de cifrado y verificación (puerto – puerto) para el manejo de la movilidad de la información.	Baja	3	9	3	Intolerable
	E.15	Alteración accidental de la información	La dependencia cuenta con sistemas de cifrado y verificación (puerto – puerto) para el manejo de la movilidad de la información.	Baja	3	9	3	Intolerable
	E.18	Destrucción de información	El departamento de sistemas cuenta con copias de seguridad periódicas	Baja	3	9	3	Intolerable
	E.19	Fugas de información	Las personas contratadas están atadas a cláusulas de confidencialidad.	Baja	3	9	3	Intolerable

Tabla 31. Estimación del riesgo activo Microsoft office 2013. (Continuación)

	E.20	Vulnerabilidades de los programas (software)	La dependencia cuenta con un servidor (personal) para llevar a cabo cada uno de los softwares empleados para la institución.	Baja	3	9	3	Intolerable
	E.21	Errores de mantenimiento / actualización de programas (software)	Falla de funcionamiento del software.	Baja	3	9	3	Intolerable
ATAQUES INTENCIONAD	**A.5**	Suplantación de la identidad del usuario	Acceso a personas que no cuenten con los permisos necesarios o con las credenciales necesarias.	Baja	3	9	3	Intolerable
	A.6	Abuso de privilegios de acceso	Abuso de cada uno de los derechos otorgados.	Baja	3	9	3	Intolerable
	A.7	Uso no previsto	Implementación de recursos (económicos y de tiempo) en actividades no relacionadas.	Baja	3	9	3	Intolerable
	A.8	Difusión de software dañino	Afectación en los sistemas de información y los procesos que ello conlleva.	Baja	3	9	3	Intolerable
	A.9	[Re-]encaminamiento de mensajes	La dependencia cuenta con sistemas de cifrado y verificación (puerto – puerto) para el manejo de la movilidad de la información.	Baja	3	9	3	Intolerable

Tabla 31. Estimación del riesgo activo Microsoft office 2013. (Continuación)

	A.10	Alteración de secuencia	Alteración de datos.	Baja	3	9	3	Intolerable
	A.11	Acceso no autorizado	Uso ilícito del hardware	Baja	3	9	3	Intolerable
	A.15	Modificación deliberada de la información	Datos erróneos en el momento de la movilización de la información.	Baja	3	9	3	Intolerable
	A.18	Destrucción de información	Perdida de la información.	Baja	3	9	3	Intolerable
	A.19	Divulgación de información	Información filtrada abiertamente a personas no correspondientes.	Baja	3	9	3	Intolerable
	A.22	Manipulación de programas	Alteración del funcionamiento de cada uno de los programas de la dependencia.	Baja	3	9	3	Intolerable

Fuente: Autoría propia

Tabla 32. Estimación del riesgo activo open office Linux 2017

ACTIVO TI	**OPEN OFFICE LINUX 2017**						
ADMINISTRADOR	PIMIENTO CARDENAS WILSON MAURICIO						
DEGRADACIÓN	15%						
IMPACTO	2						
TIPO DE ACTIVO	SOFTWARE						
Tipo	**ID**	**Amenaza**	**Exposición/Vulnerabilidad**	**RIESGO ACTUAL**			
						2	Tolerable

Tabla 32. Estimación del riesgo activo open office Linux 2017. (Continuación)

				Frecuencia (F)		R	NR	
DE ORIGEN INDUSTRIAL	**I.5**	Avería de origen físico o lógico	La manipulación por parte de cada uno de los componentes encontrados en la dependencia, como también por defectos de los componentes desde fabrica	Baja	3	6	2	Tolerable
ERRORES Y FALLOS NO INTENCIONADOS	**E.1**	Errores de los usuarios	Pérdida total o parcial del tiempo de ejecución de sus actividades, dependiendo de la gravedad del asunto.	Baja	3	6	2	Tolerable
	E.2	Errores del administrador	Pérdida total o parcial del tiempo de ejecución de sus actividades, dependiendo de la gravedad del asunto.	Baja	3	6	2	Tolerable
	E.8	Difusión de software dañino	La dependencia cuenta con antivirus capaces de controlar software malicioso	Baja	3	6	2	Tolerable
	E.9	Errores de [re-] encaminamiento	La dependencia cuenta con sistemas de cifrado y verificación (puerto – puerto) para el manejo de la movilidad de la información.	Baja	3	6	2	Tolerable
	E.10	Errores de secuencia	La dependencia cuenta con sistemas de cifrado y verificación (puerto – puerto) para el manejo de la movilidad de la información.	Baja	3	6	2	Tolerable

Tabla 32. Estimación del riesgo activo open office Linux 2017. (Continuación)

	E.15	Alteración accidental de la información	La dependencia cuenta con sistemas de cifrado y verificación (puerto – puerto) para el manejo de la movilidad de la información.	Baja	3	6	2	Tolerable
	E.18	Destrucción de información	El departamento de sistemas cuenta con copias de seguridad periódicas	Baja	3	6	2	Tolerable
	E.19	Fugas de información	Las personas contratadas están atadas a cláusulas de confidencialidad.	Baja	3	6	2	Tolerable
	E.20	Vulnerabilidades de los programas (software)	La dependencia cuenta con un servidor (personal) para llevar a cabo cada uno de los softwares empleados para la institución.	Baja	3	6	2	Tolerable
	E.21	Errores de mantenimiento / actualización de programas (software)	Falla de funcionamiento del software.	Baja	3	6	2	Tolerable
ATAQUES INTENCIONAD	**A.5**	Suplantación de la identidad del usuario	Acceso a personas que no cuenten con los permisos necesarios o con las credenciales necesarias.	Baja	3	6	2	Tolerable
	A.6	Abuso de privilegios de acceso	Abuso de cada uno de los derechos otorgados.	Baja	3	6	2	Tolerable

Tabla 32. Estimación del riesgo activo open office Linux 2017. (Continuación)

	A.7	Uso no previsto	Implementación de recursos (económicos y de tiempo) en actividades no relacionadas.	Baja	3	6	2	Tolerable
	A.8	Difusión de software dañino	Afectación en los sistemas de información y los procesos que ello conlleva.	Baja	3	6	2	Tolerable
	A.9	[Re-]encaminamiento de mensajes	La dependencia cuenta con sistemas de cifrado y verificación (puerto – puerto) para el manejo de la movilidad de la información.	Baja	3	6	2	Tolerable
	A.10	Alteración de secuencia	Alteración de datos.	Baja	3	6	2	Tolerable
	A.11	Acceso no autorizado	Uso ilícito del hardware	Baja	3	6	2	Tolerable
	A.15	Modificación deliberada de la información	Datos erróneos en el momento de la movilización de la información.	Baja	3	6	2	Tolerable
	A.18	Destrucción de información	Perdida de la información.	Baja	3	6	2	Tolerable
	A.19	Divulgación de información	Información filtrada abiertamente a personas no correspondientes.	Baja	3	6	2	Tolerable
	A.22	Manipulación de programas	Alteración del funcionamiento de cada uno de los programas de la dependencia.	Baja	3	6	2	Tolerable

Fuente: Autoría propia

Tabla 33. Estimación del riesgo activo *System center*

ACTIVO TI	**ANTIVIRUS SYSTEM CENTER**
ADMINISTRADOR	PIMIENTO CARDENAS WILSON MAURICIO
DEGRADACIÓN	20%
IMPACTO	2
TIPO DE ACTIVO	SOFTWARE

Tipo	ID	Amenaza	Exposición/Vulnerabilidad	RIESGO ACTUAL				
							2	Tolerable
				Frecuencia (F)		R	NR	
DE ORIGEN INDUSTRIAL	**I.5**	Avería de origen físico o lógico	La manipulación por parte de cada uno de los componentes encontrados en la dependencia, como también por defectos de los componentes desde fabrica	Baja	3	6	2	Tolerable
ERRORES Y FALLOS NO INTENCIONADOS	**E.1**	Errores de los usuarios	Pérdida total o parcial del tiempo de ejecución de sus actividades, dependiendo de la gravedad del asunto.	Baja	3	6	2	Tolerable
	E.2	Errores del administrador	Pérdida total o parcial del tiempo de ejecución de sus actividades, dependiendo de la gravedad del asunto.	Baja	3	6	2	Tolerable
	E.8	Difusión de software dañino	La dependencia cuenta con antivirus capaces de controlar software malicioso	Baja	3	6	2	Tolerable

Tabla 33. Estimación del riesgo activo *System center*. (Continuación)

	E.9	Errores de [re-] encaminamiento	La dependencia cuenta con sistemas de cifrado y verificación (puerto – puerto) para el manejo de la movilidad de la información.	Baja	3	6	2	Tolerable
	E.10	Errores de secuencia	La dependencia cuenta con sistemas de cifrado y verificación (puerto – puerto) para el manejo de la movilidad de la información.	Baja	3	6	2	Tolerable
	E.15	Alteración accidental de la información	La dependencia cuenta con sistemas de cifrado y verificación (puerto – puerto) para el manejo de la movilidad de la información.	Baja	3	6	2	Tolerable
	E.18	Destrucción de información	El departamento de sistemas cuenta con copias de seguridad periódicas	Baja	3	6	2	Tolerable
	E.19	Fugas de información	Las personas contratadas están atadas a cláusulas de confidencialidad.	Baja	3	6	2	Tolerable
	E.20	Vulnerabilidades de los programas (software)	La dependencia cuenta con un servidor (personal) para llevar a cabo cada uno de los softwares empleados para la institución.	Baja	3	6	2	Tolerable
	E.21	Errores de mantenimiento /	Falla de funcionamiento del software.	Baja	3	6	2	Tolerable

Tabla 33. Estimación del riesgo activo *System center.* (Continuación)

		actualización de programas (software)						
ATAQUES INTENCIONAD	**A.5**	Suplantación de la identidad del usuario	Acceso a personas que no cuenten con los permisos necesarios o con las credenciales necesarias.	Baja	3	6	2	Tolerable
	A.6	Abuso de privilegios de acceso	Abuso de cada uno de los derechos otorgados.	Baja	3	6	2	Tolerable
	A.7	Uso no previsto	Implementación de recursos (económicos y de tiempo) en actividades no relacionadas.	Baja	3	6	2	Tolerable
	A.8	Difusión de software dañino	Afectación en los sistemas de información y los procesos que ello conlleva.	Baja	3	6	2	Tolerable
	A.9	[Re-]encaminamiento de mensajes	La dependencia cuenta con sistemas de cifrado y verificación (puerto – puerto) para el manejo de la movilidad de la información.	Baja	3	6	2	Tolerable
	A.10	Alteración de secuencia	Alteración de datos.	Baja	3	6	2	Tolerable
	A.11	Acceso no autorizado	Uso ilícito del hardware	Baja	3	6	2	Tolerable
	A.15	Modificación deliberada de la información	Datos erróneos en el momento de la movilización de la información.	Baja	3	6	2	Tolerable

Tabla 33. Estimación del riesgo activo *System center*. (Continuación)

	A.18	Destrucción de información	Perdida de la información.	Baja	3	6	2	Tolerable
	A.19	Divulgación de información	Información filtrada abiertamente a personas no correspondientes.	Baja	3	6	2	Tolerable
	A.22	Manipulación de programas	Alteración del funcionamiento de cada uno de los programas de la dependencia.	Baja	3	6	2	Tolerable

Fuente: Autoría propia

Tabla 34. Estimación del riesgo activo Windows defender

ACTIVO TI	**ANTIVIRUS WINDOWS DEFENDER**							
ADMINISTRADOR	PIMIENTO CARDENAS WILSON MAURICIO							
DEGRADACIÓN	20%							
IMPACTO	2							
TIPO DE ACTIVO	SOFTWARE							
Tipo	**ID**	**Amenaza**	**Exposición/Vulnerabilidad**	**RIESGO ACTUAL**				
							2	Tolerable
				Frecuencia (F)		**R**	**NR**	
DE ORIGEN INDUSTRIAL	**I.5**	Avería de origen físico o lógico	La manipulación por parte de cada uno de los componentes encontrados en la dependencia, como también por defectos de los componentes desde fabrica	Baja	3	6	2	Tolerable

Tabla 34. Estimación del riesgo activo Windows defender. (Continuación)

ERRORES Y FALLOS NO INTENCIONADOS	**E.1**	Errores de los usuarios	Pérdida total o parcial del tiempo de ejecución de sus actividades, dependiendo de la gravedad del asunto.	Baja	3	6	2	Tolerable
	E.2	Errores del administrador	Pérdida total o parcial del tiempo de ejecución de sus actividades, dependiendo de la gravedad del asunto.	Baja	3	6	2	Tolerable
	E.8	Difusión de software dañino	La dependencia cuenta con antivirus capaces de controlar software malicioso	Baja	3	6	2	Tolerable
	E.9	Errores de [re-] encaminamiento	La dependencia cuenta con sistemas de cifrado y verificación (puerto – puerto) para el manejo de la movilidad de la información.	Baja	3	6	2	Tolerable
	E.10	Errores de secuencia	La dependencia cuenta con sistemas de cifrado y verificación (puerto – puerto) para el manejo de la movilidad de la información.	Baja	3	6	2	Tolerable
	E.15	Alteración accidental de la información	La dependencia cuenta con sistemas de cifrado y verificación (puerto – puerto) para el manejo de la movilidad de la información.	Baja	3	6	2	Tolerable
	E.18	Destrucción de información	El departamento de sistemas cuenta con copias de seguridad periódicas	Baja	3	6	2	Tolerable

Tabla 34. Estimación del riesgo activo Windows defender. (Continuación)

	E.19	Fugas de información	Las personas contratadas están atadas a cláusulas de confidencialidad.	Baja	3	6	2	Tolerable
	E.20	Vulnerabilidades de los programas (software)	La dependencia cuenta con un servidor (personal) para llevar a cabo cada uno de los softwares empleados para la institución.	Baja	3	6	2	Tolerable
	E.21	Errores de mantenimiento / actualización de programas (software)	Falla de funcionamiento del software.	Baja	3	6	2	Tolerable
ATAQUES INTENCIONAD	**A.5**	Suplantación de la identidad del usuario	Acceso a personas que no cuenten con los permisos necesarios o con las credenciales necesarias.	Baja	3	6	2	Tolerable
	A.6	Abuso de privilegios de acceso	Abuso de cada uno de los derechos otorgados.	Baja	3	6	2	Tolerable
	A.7	Uso no previsto	Implementación de recursos (económicos y de tiempo) en actividades no relacionadas.	Baja	3	6	2	Tolerable
	A.8	Difusión de software dañino	Afectación en los sistemas de información y los procesos que ello conlleva.	Baja	3	6	2	Tolerable

Tabla 34. Estimación del riesgo activo Windows defender. (Continuación)

	A.9	[Re-]encaminamiento de mensajes	La dependencia cuenta con sistemas de cifrado y verificación (puerto – puerto) para el manejo de la movilidad de la información.	Baja	3	6	2	Tolerable
	A.10	Alteración de secuencia	Alteración de datos.	Baja	3	6	2	Tolerable
	A.11	Acceso no autorizado	Uso ilícito del hardware	Baja	3	6	2	Tolerable
	A.15	Modificación deliberada de la información	Datos erróneos en el momento de la movilización de la información.	Baja	3	6	2	Tolerable
	A.18	Destrucción de información	Perdida de la información.	Baja	3	6	2	Tolerable
	A.19	Divulgación de información	Información filtrada abiertamente a personas no correspondientes.	Baja	3	6	2	Tolerable
	A.22	Manipulación de programas	Alteración del funcionamiento de cada uno de los programas de la dependencia.	Baja	3	6	2	Tolerable

Fuente: Autoría propia

Tabla 35. Estimación del riesgo activo Windows 8

ACTIVO TI	**SISTEMA OPERATIVO WINDOWS 8**
ADMINISTRADOR	PIMIENTO CARDENAS WILSON MAURICIO
DEGRADACIÓN	35%
IMPACTO	3
TIPO DE ACTIVO	SOFTWARE

Tabla 35. Estimación del riesgo activo Windows 8. (Continuación)

Tipo	ID	Amenaza	Exposición/Vulnerabilidad	RIESGO ACTUAL				
							3	Intolerable
				Frecuencia (F)		R	NR	
DE ORIGEN INDUSTRIAL	**I.5**	Avería de origen físico o lógico	La manipulación por parte de cada uno de los componentes encontrados en la dependencia, como también por defectos de los componentes desde fabrica	Baja	3	9	3	Intolerable
ERRORES Y FALLOS NO INTENCIONADOS	**E.1**	Errores de los usuarios	Pérdida total o parcial del tiempo de ejecución de sus actividades, dependiendo de la gravedad del asunto.	Baja	3	9	3	Intolerable
	E.2	Errores del administrador	Pérdida total o parcial del tiempo de ejecución de sus actividades, dependiendo de la gravedad del asunto.	Baja	3	9	3	Intolerable
	E.8	Difusión de software dañino	La dependencia cuenta con antivirus capaces de controlar software malicioso	Baja	3	9	3	Intolerable
	E.9	Errores de [re-] encaminamiento	La dependencia cuenta con sistemas de cifrado y verificación (puerto – puerto) para el manejo de la movilidad de la información.	Baja	3	9	3	Intolerable

Tabla 35. Estimación del riesgo activo Windows 8. (Continuación)

	E.10	Errores de secuencia	La dependencia cuenta con sistemas de cifrado y verificación (puerto – puerto) para el manejo de la movilidad de la información.	Baja	3	9	3	Intolerable
	E.15	Alteración accidental de la información	La dependencia cuenta con sistemas de cifrado y verificación (puerto – puerto) para el manejo de la movilidad de la información.	Baja	3	9	3	Intolerable
	E.18	Destrucción de información	El departamento de sistemas cuenta con copias de seguridad periódicas	Baja	3	9	3	Intolerable
	E.19	Fugas de información	Las personas contratadas están atadas a cláusulas de confidencialidad.	Baja	3	9	3	Intolerable
	E.20	Vulnerabilidades de los programas (software)	La dependencia cuenta con un servidor (personal) para llevar a cabo cada uno de los softwares empleados para la institución.	Baja	3	9	3	Intolerable
	E.21	Errores de mantenimiento / actualización de programas (software)	Falla de funcionamiento del software.	Baja	3	9	3	Intolerable
ATAQUES INTENC	**A.5**	Suplantación de la identidad del usuario	Acceso a personas que no cuenten con los permisos necesarios o con las credenciales necesarias.	Baja	3	9	3	Intolerable

Tabla 35. Estimación del riesgo activo Windows 8. (Continuación)

	A.6	Abuso de privilegios de acceso	Abuso de cada uno de los derechos otorgados.	Baja	3	9	3	Intolerable
	A.7	Uso no previsto	Implementación de recursos (económicos y de tiempo) en actividades no relacionadas.	Baja	3	9	3	Intolerable
	A.8	Difusión de software dañino	Afectación en los sistemas de información y los procesos que ello conlleva.	Baja	3	9	3	Intolerable
	A.9	[Re-]encaminamiento de mensajes	La dependencia cuenta con sistemas de cifrado y verificación (puerto – puerto) para el manejo de la movilidad de la información.	Baja	3	9	3	Intolerable
	A.10	Alteración de secuencia	Alteración de datos.	Baja	3	9	3	Intolerable
	A.11	Acceso no autorizado	Uso ilícito del hardware	Baja	3	9	3	Intolerable
	A.15	Modificación deliberada de la información	Datos erróneos en el momento de la movilización de la información.	Baja	3	9	3	Intolerable
	A.18	Destrucción de información	Perdida de la información.	Baja	3	9	3	Intolerable
	A.19	Divulgación de información	Información filtrada abiertamente a personas no correspondientes.	Baja	3	9	3	Intolerable

Tabla 35. Estimación del riesgo activo Windows 8. (Continuación)

	A.22	Manipulación de programas	Alteración del funcionamiento de cada uno de los programas de la dependencia.	Baja	3	9	3	Intolerable

Fuente: Autoría propia

Tabla 36. Estimación del riesgo activo Windows *server* 2009

ACTIVO TI	**SISTEMA OPERATIVO WINDOWS SERVER 2009**
ADMINISTRADOR	PIMIENTO CARDENAS WILSON MAURICIO
DEGRADACIÓN	60%
IMPACTO	5
TIPO DE ACTIVO	SOFTWARE

Tipo	**ID**	**Amenaza**	**Exposición/Vulnerabilidad**	**RIESGO ACTUAL**				
							4	Extremo
				Frecuencia (F)		**R**	**NR**	
DE ORIGEN INDUSTRIAL	**I.5**	Avería de origen físico o lógico	La manipulación por parte de cada uno de los componentes encontrados en la dependencia, como también por defectos de los componentes desde fabrica	Baja	3	15	4	Extremo
ERRORES Y FALLOS NO INTENCIONADOS	**E.1**	Errores de los usuarios	Pérdida total o parcial del tiempo de ejecución de sus actividades, dependiendo de la gravedad del asunto.	Baja	3	15	4	Extremo
	E.2	Errores del administrador	Pérdida total o parcial del tiempo de ejecución de sus actividades, dependiendo de la gravedad del asunto.	Baja	3	15	4	Extremo

Tabla 36. Estimación del riesgo activo Windows *server* 2009. (Continuación)

	E.8	Difusión de software dañino	La dependencia cuenta con antivirus capaces de controlar software malicioso	Baja	3	15	4	Extremo
	E.9	Errores de [re-] encaminamiento	La dependencia cuenta con sistemas de cifrado y verificación (puerto – puerto) para el manejo de la movilidad de la información.	Baja	3	15	4	Extremo
	E.10	Errores de secuencia	La dependencia cuenta con sistemas de cifrado y verificación (puerto – puerto) para el manejo de la movilidad de la información.	Baja	3	15	4	Extremo
	E.15	Alteración accidental de la información	La dependencia cuenta con sistemas de cifrado y verificación (puerto – puerto) para el manejo de la movilidad de la información.	Baja	3	15	4	Extremo
	E.18	Destrucción de información	El departamento de sistemas cuenta con copias de seguridad periódicas	Baja	3	15	4	Extremo
	E.19	Fugas de información	Las personas contratadas están atadas a cláusulas de confidencialidad.	Baja	3	15	4	Extremo
	E.20	Vulnerabilidades de los programas (software)	La dependencia cuenta con un servidor (personal) para llevar a cabo cada uno de los softwares empleados para la institución.	Baja	3	15	4	Extremo

Tabla 36. Estimación del riesgo activo Windows *server* 2009. (Continuación)

	E.21	Errores de mantenimiento / actualización de programas (software)	Falla de funcionamiento del software.	Baja	3	15	4	Extremo
ATAQUES INTENCIONAD	**A.5**	Suplantación de la identidad del usuario	Acceso a personas que no cuenten con los permisos necesarios o con las credenciales necesarias.	Baja	3	15	4	Extremo
	A.6	Abuso de privilegios de acceso	Abuso de cada uno de los derechos otorgados.	Baja	3	15	4	Extremo
	A.7	Uso no previsto	Implementación de recursos (económicos y de tiempo) en actividades no relacionadas.	Baja	3	15	4	Extremo
	A.8	Difusión de software dañino	Afectación en los sistemas de información y los procesos que ello conlleva.	Baja	3	15	4	Extremo
	A.9	[Re-]encaminamiento de mensajes	La dependencia cuenta con sistemas de cifrado y verificación (puerto – puerto) para el manejo de la movilidad de la información.	Baja	3	15	4	Extremo
	A.10	Alteración de secuencia	Alteración de datos.	Baja	3	15	4	Extremo
	A.11	Acceso no autorizado	Uso ilícito del hardware	Baja	3	15	4	Extremo

Tabla 36. Estimación del riesgo activo Windows *server* 2009. (Continuación)

	A.15	Modificación deliberada de la información	Datos erróneos en el momento de la movilización de la información.	Baja	3	15	4	Extremo
	A.18	Destrucción de información	Perdida de la información.	Baja	3	15	4	Extremo
	A.19	Divulgación de información	Información filtrada abiertamente a personas no correspondientes.	Baja	3	15	4	Extremo
	A.22	Manipulación de programas	Alteración del funcionamiento de cada uno de los programas de la dependencia.	Baja	3	15	4	Extremo

Fuente: Autoría propia

Tabla 37. Estimación del riesgo activo Windows *server* 2012

ACTIVO TI	**SISTEMA OPERATIVO WINDOWS SERVER 2012**							
ADMINISTRADOR	PIMIENTO CARDENAS WILSON MAURICIO							
DEGRADACIÓN	60%							
IMPACTO	5							
TIPO DE ACTIVO	SOFTWARE							
Tipo	**ID**	**Amenaza**	**Exposición/Vulnerabilidad**	**RIESGO ACTUAL**				
							4	Extremo
				Frecuencia (F)		**R**	**NR**	
DE ORIGEN	**I.5**	Avería de origen físico o lógico	La manipulación por parte de cada uno de los componentes encontrados en la dependencia, como también por	Baja	3	15	4	Extremo

Tabla 37. Estimación del riesgo activo Windows *server* 2012. (Continuación)

			defectos de los componentes desde fabrica					
ERRORES Y FALLOS NO INTENCIONADOS	**E.1**	Errores de los usuarios	Pérdida total o parcial del tiempo de ejecución de sus actividades, dependiendo de la gravedad del asunto.	Baja	3	15	4	Extremo
	E.2	Errores del administrador	Pérdida total o parcial del tiempo de ejecución de sus actividades, dependiendo de la gravedad del asunto.	Baja	3	15	4	Extremo
	E.8	Difusión de software dañino	La dependencia cuenta con antivirus capaces de controlar software malicioso	Baja	3	15	4	Extremo
	E.9	Errores de [re-] encaminamiento	La dependencia cuenta con sistemas de cifrado y verificación (puerto – puerto) para el manejo de la movilidad de la información.	Baja	3	15	4	Extremo
	E.10	Errores de secuencia	La dependencia cuenta con sistemas de cifrado y verificación (puerto – puerto) para el manejo de la movilidad de la información.	Baja	3	15	4	Extremo
	E.15	Alteración accidental de la información	La dependencia cuenta con sistemas de cifrado y verificación (puerto – puerto) para el manejo de la movilidad de la información.	Baja	3	15	4	Extremo

Tabla 37. Estimación del riesgo activo Windows *server* 2012. (Continuación)

	E.18	Destrucción de información	El departamento de sistemas cuenta con copias de seguridad periódicas	Baja	3	15	4	Extremo
	E.19	Fugas de información	Las personas contratadas están atadas a cláusulas de confidencialidad.	Baja	3	15	4	Extremo
	E.20	Vulnerabilidades de los programas (software)	La dependencia cuenta con un servidor (personal) para llevar a cabo cada uno de los softwares empleados para la institución.	Baja	3	15	4	Extremo
	E.21	Errores de mantenimiento / actualización de programas (software)	Falla de funcionamiento del software.	Baja	3	15	4	Extremo
ATAQUES INTENCIONAD	**A.5**	Suplantación de la identidad del usuario	Acceso a personas que no cuenten con los permisos necesarios o con las credenciales necesarias.	Baja	3	15	4	Extremo
	A.6	Abuso de privilegios de acceso	Abuso de cada uno de los derechos otorgados.	Baja	3	15	4	Extremo
	A.7	Uso no previsto	Implementación de recursos (económicos y de tiempo) en actividades no relacionadas.	Baja	3	15	4	Extremo

Tabla 37. Estimación del riesgo activo Windows *server* 2012. (Continuación)

	A.8	Difusión de software dañino	Afectación en los sistemas de información y los procesos que ello conlleva.	Baja	3	15	4	Extremo
	A.9	[Re-]encaminamiento de mensajes	La dependencia cuenta con sistemas de cifrado y verificación (puerto – puerto) para el manejo de la movilidad de la información.	Baja	3	15	4	Extremo
	A.10	Alteración de secuencia	Alteración de datos.	Baja	3	15	4	Extremo
	A.11	Acceso no autorizado	Uso ilícito del hardware	Baja	3	15	4	Extremo
	A.15	Modificación deliberada de la información	Datos erróneos en el momento de la movilización de la información.	Baja	3	15	4	Extremo
	A.18	Destrucción de información	Perdida de la información.	Baja	3	15	4	Extremo
	A.19	Divulgación de información	Información filtrada abiertamente a personas no correspondientes.	Baja	3	15	4	Extremo
	A.22	Manipulación de programas	Alteración del funcionamiento de cada uno de los programas de la dependencia.	Baja	3	15	4	Extremo

Fuente: Autoría propia

Tabla 38. Estimación del riesgo activo CentOS 5

ACTIVO TI	**SISTEMA OPERATIVO CentOS 5**

Tabla 38. Estimación del riesgo activo CentOS 5. (Continuación)

ADMINISTRADOR	PIMIENTO CARDENAS WILSON MAURICIO
DEGRADACIÓN	60%
IMPACTO	5
TIPO DE ACTIVO	SOFTWARE

Tipo	ID	Amenaza	Exposición/Vulnerabilidad	RIESGO ACTUAL				
							4	Extremo
				Frecuencia (F)		R	NR	
DE ORIGEN INDUSTRIAL	**I.5**	Avería de origen físico o lógico	La manipulación por parte de cada uno de los componentes encontrados en la dependencia, como también por defectos de los componentes desde fabrica	Baja	3	15	4	Extremo
ERRORES Y FALLOS NO INTENCIONADOS	**E.1**	Errores de los usuarios	Pérdida total o parcial del tiempo de ejecución de sus actividades, dependiendo de la gravedad del asunto.	Baja	3	15	4	Extremo
	E.2	Errores del administrador	Pérdida total o parcial del tiempo de ejecución de sus actividades, dependiendo de la gravedad del asunto.	Baja	3	15	4	Extremo
	E.8	Difusión de software dañino	La dependencia cuenta con antivirus capaces de controlar software malicioso	Baja	3	15	4	Extremo
	E.9	Errores de [re-] encaminamiento	La dependencia cuenta con sistemas de cifrado y verificación (puerto – puerto)	Baja	3	15	4	Extremo

Tabla 38. Estimación del riesgo activo CentOS 5. (Continuación)

			para el manejo de la movilidad de la información.					
	E.10	Errores de secuencia	La dependencia cuenta con sistemas de cifrado y verificación (puerto – puerto) para el manejo de la movilidad de la información.	Baja	3	15	4	Extremo
	E.15	Alteración accidental de la información	La dependencia cuenta con sistemas de cifrado y verificación (puerto – puerto) para el manejo de la movilidad de la información.	Baja	3	15	4	Extremo
	E.18	Destrucción de información	El departamento de sistemas cuenta con copias de seguridad periódicas	Baja	3	15	4	Extremo
	E.19	Fugas de información	Las personas contratadas están atadas a cláusulas de confidencialidad.	Baja	3	15	4	Extremo
	E.20	Vulnerabilidades de los programas (software)	La dependencia cuenta con un servidor (personal) para llevar a cabo cada uno de los softwares empleados para la institución.	Baja	3	15	4	Extremo
	E.21	Errores de mantenimiento / actualización de programas (software)	Falla de funcionamiento del software.	Baja	3	15	4	Extremo

Tabla 38. Estimación del riesgo activo CentOS 5. (Continuación)

ATAQUES INTENCIONAD	**A.5**	Suplantación de la identidad del usuario	Acceso a personas que no cuenten con los permisos necesarios o con las credenciales necesarias.	Baja	3	15	4	Extremo
	A.6	Abuso de privilegios de acceso	Abuso de cada uno de los derechos otorgados.	Baja	3	15	4	Extremo
	A.7	Uso no previsto	Implementación de recursos (económicos y de tiempo) en actividades no relacionadas.	Baja	3	15	4	Extremo
	A.8	Difusión de software dañino	Afectación en los sistemas de información y los procesos que ello conlleva.	Baja	3	15	4	Extremo
	A.9	[Re-]encaminamiento de mensajes	La dependencia cuenta con sistemas de cifrado y verificación (puerto – puerto) para el manejo de la movilidad de la información.	Baja	3	15	4	Extremo
	A.10	Alteración de secuencia	Alteración de datos.	Baja	3	15	4	Extremo
	A.11	Acceso no autorizado	Uso ilícito del hardware	Baja	3	15	4	Extremo
	A.15	Modificación deliberada de la información	Datos erróneos en el momento de la movilización de la información.	Baja	3	15	4	Extremo
	A.18	Destrucción de información	Perdida de la información.	Baja	3	15	4	Extremo

Tabla 39. Estimación del riesgo activo CentOS 5. (Continuación)

	A.19	Divulgación de información	Información filtrada abiertamente a personas no correspondientes.	Baja	3	15	4	Extremo
	A.22	Manipulación de programas	Alteración del funcionamiento de cada uno de los programas de la dependencia.	Baja	3	15	4	Extremo

Fuente: Autoría propia

Tabla 40. Estimación del riesgo activo Debian 7

ACTIVO TI	**SISTEMA OPERATIVO DEBIAN 7**							
ADMINISTRADOR	PIMIENTO CARDENAS WILSON MAURICIO							
DEGRADACIÓN	60%							
IMPACTO	5							
TIPO DE ACTIVO	SOFTWARE							
Tipo	**ID**	**Amenaza**	**Exposición/Vulnerabilidad**	**RIESGO ACTUAL**				
							4	Extremo
				Frecuencia (F)		**R**	**NR**	
DE ORIGEN INDUSTRIAL	**I.5**	Avería de origen físico o lógico	La manipulación por parte de cada uno de los componentes encontrados en la dependencia, como también por defectos de los componentes desde fabrica	Baja	3	15	4	Extremo
ERRORES Y FALLOS	**E.1**	Errores de los usuarios	Pérdida total o parcial del tiempo de ejecución de sus actividades, dependiendo de la gravedad del asunto.	Baja	3	15	4	Extremo

Tabla 40. Estimación del riesgo activo Debian 7. (Continuación)

	E.2	Errores del administrador	Pérdida total o parcial del tiempo de ejecución de sus actividades, dependiendo de la gravedad del asunto.	Baja	3	15	4	Extremo
	E.8	Difusión de software dañino	La dependencia cuenta con antivirus capaces de controlar software malicioso	Baja	3	15	4	Extremo
	E.9	Errores de [re-] encaminamiento	La dependencia cuenta con sistemas de cifrado y verificación (puerto – puerto) para el manejo de la movilidad de la información.	Baja	3	15	4	Extremo
	E.10	Errores de secuencia	La dependencia cuenta con sistemas de cifrado y verificación (puerto – puerto) para el manejo de la movilidad de la información.	Baja	3	15	4	Extremo
	E.15	Alteración accidental de la información	La dependencia cuenta con sistemas de cifrado y verificación (puerto – puerto) para el manejo de la movilidad de la información.	Baja	3	15	4	Extremo
	E.18	Destrucción de información	El departamento de sistemas cuenta con copias de seguridad periódicas	Baja	3	15	4	Extremo
	E.19	Fugas de información	Las personas contratadas están atadas a cláusulas de confidencialidad.	Baja	3	15	4	Extremo

Tabla 40. Estimación del riesgo activo Debian 7. (Continuación)

	E.20	Vulnerabilidades de los programas (software)	La dependencia cuenta con un servidor (personal) para llevar a cabo cada uno de los softwares empleados para la institución.	Baja	3	15	4	Extremo
	E.21	Errores de mantenimiento / actualización de programas (software)	Falla de funcionamiento del software.	Baja	3	15	4	Extremo
ATAQUES INTENCIONAD	**A.5**	Suplantación de la identidad del usuario	Acceso a personas que no cuenten con los permisos necesarios o con las credenciales necesarias.	Baja	3	15	4	Extremo
	A.6	Abuso de privilegios de acceso	Abuso de cada uno de los derechos otorgados.	Baja	3	15	4	Extremo
	A.7	Uso no previsto	Implementación de recursos (económicos y de tiempo) en actividades no relacionadas.	Baja	3	15	4	Extremo
	A.8	Difusión de software dañino	Afectación en los sistemas de información y los procesos que ello conlleva.	Baja	3	15	4	Extremo
	A.9	[Re-]encaminamiento de mensajes	La dependencia cuenta con sistemas de cifrado y verificación (puerto – puerto) para el manejo de la movilidad de la información.	Baja	3	15	4	Extremo

Tabla 40. Estimación del riesgo activo Debian 7. (Continuación)

	A.10	Alteración de secuencia	Alteración de datos.	Baja	3	15	4	Extremo
	A.11	Acceso no autorizado	Uso ilícito del hardware	Baja	3	15	4	Extremo
	A.15	Modificación deliberada de la información	Datos erróneos en el momento de la movilización de la información.	Baja	3	15	4	Extremo
	A.18	Destrucción de información	Perdida de la información.	Baja	3	15	4	Extremo
	A.19	Divulgación de información	Información filtrada abiertamente a personas no correspondientes.	Baja	3	15	4	Extremo
	A.22	Manipulación de programas	Alteración del funcionamiento de cada uno de los programas de la dependencia.	Baja	3	15	4	Extremo

Fuente: Autoría propia

Tabla 41. Estimación del riesgo activo Ubuntu 14

ACTIVO TI	**SISTEMA OPERATIVO UBUNTU 14**						
ADMINISTRADOR	PIMIENTO CARDENAS WILSON MAURICIO						
DEGRADACIÓN	20%						
IMPACTO	2						
TIPO DE ACTIVO	SOFTWARE						
Tipo	**ID**	**Amenaza**	**Exposición/Vulnerabilidad**	**RIESGO ACTUAL**			
						2	Tolerable

Tabla 41. Estimación del riesgo activo Ubuntu 14. (Continuación)

				Frecuencia (F)		R	NR	
DE ORIGEN INDUSTRIAL	**I.5**	Avería de origen físico o lógico	La manipulación por parte de cada uno de los componentes encontrados en la dependencia, como también por defectos de los componentes desde fabrica	Baja	3	6	2	Tolerable
ERRORES Y FALLOS NO INTENCIONADOS	**E.1**	Errores de los usuarios	Pérdida total o parcial del tiempo de ejecución de sus actividades, dependiendo de la gravedad del asunto.	Baja	3	6	2	Tolerable
	E.2	Errores del administrador	Pérdida total o parcial del tiempo de ejecución de sus actividades, dependiendo de la gravedad del asunto.	Baja	3	6	2	Tolerable
	E.8	Difusión de software dañino	La dependencia cuenta con antivirus capaces de controlar software malicioso	Baja	3	6	2	Tolerable
	E.9	Errores de [re-] encaminamiento	La dependencia cuenta con sistemas de cifrado y verificación (puerto – puerto) para el manejo de la movilidad de la información.	Baja	3	6	2	Tolerable
	E.10	Errores de secuencia	La dependencia cuenta con sistemas de cifrado y verificación (puerto – puerto) para el manejo de la movilidad de la información.	Baja	3	6	2	Tolerable

Tabla 41. Estimación del riesgo activo Ubuntu 14. (Continuación)

	E.15	Alteración accidental de la información	La dependencia cuenta con sistemas de cifrado y verificación (puerto – puerto) para el manejo de la movilidad de la información.	Baja	3	6	2	Tolerable
	E.18	Destrucción de información	El departamento de sistemas cuenta con copias de seguridad periódicas	Baja	3	6	2	Tolerable
	E.19	Fugas de información	Las personas contratadas están atadas a cláusulas de confidencialidad.	Baja	3	6	2	Tolerable
	E.20	Vulnerabilidades de los programas (software)	La dependencia cuenta con un servidor (personal) para llevar a cabo cada uno de los softwares empleados para la institución.	Baja	3	6	2	Tolerable
	E.21	Errores de mantenimiento / actualización de programas (software)	Falla de funcionamiento del software.	Baja	3	6	2	Tolerable
ATAQUES INTENCIONAD	**A.5**	Suplantación de la identidad del usuario	Acceso a personas que no cuenten con los permisos necesarios o con las credenciales necesarias.	Baja	3	6	2	Tolerable
	A.6	Abuso de privilegios de acceso	Abuso de cada uno de los derechos otorgados.	Baja	3	6	2	Tolerable

Tabla 41. Estimación del riesgo activo Ubuntu 14. (Continuación)

	A.7	Uso no previsto	Implementación de recursos (económicos y de tiempo) en actividades no relacionadas.	Baja	3	6	2	Tolerable
	A.8	Difusión de software dañino	Afectación en los sistemas de información y los procesos que ello conlleva.	Baja	3	6	2	Tolerable
	A.9	[Re-]encaminamiento de mensajes	La dependencia cuenta con sistemas de cifrado y verificación (puerto – puerto) para el manejo de la movilidad de la información.	Baja	3	6	2	Tolerable
	A.10	Alteración de secuencia	Alteración de datos.	Baja	3	6	2	Tolerable
	A.11	Acceso no autorizado	Uso ilícito del hardware	Baja	3	6	2	Tolerable
	A.15	Modificación deliberada de la información	Datos erróneos en el momento de la movilización de la información.	Baja	3	6	2	Tolerable
	A.18	Destrucción de información	Perdida de la información.	Baja	3	6	2	Tolerable
	A.19	Divulgación de información	Información filtrada abiertamente a personas no correspondientes.	Baja	3	6	2	Tolerable
	A.22	Manipulación de programas	Alteración del funcionamiento de cada uno de los programas de la dependencia.	Baja	3	6	2	Tolerable

Fuente: Autoría propia

Tabla 42. Estimación del riesgo activo Mac os x

ACTIVO TI	**SISTEMA OPERATIVO MAC OS X**							
ADMINISTRADOR	PIMIENTO CARDENAS WILSON MAURICIO							
DEGRADACIÓN	60%							
IMPACTO	5							
TIPO DE ACTIVO	SOFTWARE							
Tipo	**ID**	**Amenaza**	**Exposición/Vulnerabilidad**	**RIESGO ACTUAL**				
							4	Extremo
				Frecuencia (F)		**R**	**NR**	
DE ORIGEN INDUSTRIAL	**I.5**	Avería de origen físico o lógico	La manipulación por parte de cada uno de los componentes encontrados en la dependencia, como también por defectos de los componentes desde fabrica	Baja	3	15	4	Extremo
ERRORES Y FALLOS NO INTENCIONADOS	**E.1**	Errores de los usuarios	Pérdida total o parcial del tiempo de ejecución de sus actividades, dependiendo de la gravedad del asunto.	Baja	3	15	4	Extremo
	E.2	Errores del administrador	Pérdida total o parcial del tiempo de ejecución de sus actividades, dependiendo de la gravedad del asunto.	Baja	3	15	4	Extremo
	E.8	Difusión de software dañino	La dependencia cuenta con antivirus capaces de controlar software malicioso	Baja	3	15	4	Extremo

Tabla 42. Estimación del riesgo activo Mac os x. (Continuación)

	E.9	Errores de [re-] encaminamiento	La dependencia cuenta con sistemas de cifrado y verificación (puerto – puerto) para el manejo de la movilidad de la información.	Baja	3	15	4	Extremo
	E.10	Errores de secuencia	La dependencia cuenta con sistemas de cifrado y verificación (puerto – puerto) para el manejo de la movilidad de la información.	Baja	3	15	4	Extremo
	E.15	Alteración accidental de la información	La dependencia cuenta con sistemas de cifrado y verificación (puerto – puerto) para el manejo de la movilidad de la información.	Baja	3	15	4	Extremo
	E.18	Destrucción de información	El departamento de sistemas cuenta con copias de seguridad periódicas	Baja	3	15	4	Extremo
	E.19	Fugas de información	Las personas contratadas están atadas a cláusulas de confidencialidad.	Baja	3	15	4	Extremo
	E.20	Vulnerabilidades de los programas (software)	La dependencia cuenta con un servidor (personal) para llevar a cabo cada uno de los softwares empleados para la institución.	Baja	3	15	4	Extremo
	E.21	Errores de mantenimiento /	Falla de funcionamiento del software.	Baja	3	15	4	Extremo

Tabla 42. Estimación del riesgo activo Mac os x. (Continuación)

		actualización de programas (software)						
ATAQUES INTENCIONAD	**A.5**	Suplantación de la identidad del usuario	Acceso a personas que no cuenten con los permisos necesarios o con las credenciales necesarias.	Baja	3	15	4	Extremo
	A.6	Abuso de privilegios de acceso	Abuso de cada uno de los derechos otorgados.	Baja	3	15	4	Extremo
	A.7	Uso no previsto	Implementación de recursos (económicos y de tiempo) en actividades no relacionadas.	Baja	3	15	4	Extremo
	A.8	Difusión de software dañino	Afectación en los sistemas de información y los procesos que ello conlleva.	Baja	3	15	4	Extremo
	A.9	[Re-]encaminamiento de mensajes	La dependencia cuenta con sistemas de cifrado y verificación (puerto – puerto) para el manejo de la movilidad de la información.	Baja	3	15	4	Extremo
	A.10	Alteración de secuencia	Alteración de datos.	Baja	3	15	4	Extremo
	A.11	Acceso no autorizado	Uso ilícito del hardware	Baja	3	15	4	Extremo
	A.15	Modificación deliberada de la información	Datos erróneos en el momento de la movilización de la información.	Baja	3	15	4	Extremo

Tabla 42. Estimación del riesgo activo Mac os x. (Continuación)

	A.18	Destrucción de información	Perdida de la información.	Baja	3	15	4	Extremo
	A.19	Divulgación de información	Información filtrada abiertamente a personas no correspondientes.	Baja	3	15	4	Extremo
	A.22	Manipulación de programas	Alteración del funcionamiento de cada uno de los programas de la dependencia.	Baja	3	15	4	Extremo

Fuente: Autoría propia

Tabla 43. Estimación del riesgo activo COMMAND (CMD)

ACTIVO TI	**TERMINAL COMMAND (CMD)**							
ADMINISTRADOR	PIMIENTO CARDENAS WILSON MAURICIO							
DEGRADACIÓN	25%							
IMPACTO	2							
TIPO DE ACTIVO	SOFTWARE							
Tipo	**ID**	**Amenaza**	**Exposición/Vulnerabilidad**	**RIESGO ACTUAL**				
							2	Tolerable
				Frecuencia (F)		**R**	**NR**	
DE ORIGEN INDUSTRIAL	**I.5**	Avería de origen físico o lógico	La manipulación por parte de cada uno de los componentes encontrados en la dependencia, como también por defectos de los componentes desde fabrica	Baja	3	6	2	Tolerable

Tabla 43. Estimación del riesgo activo COMMAND (CMD). (Continuación)

ERRORES Y FALLOS NO INTENCIONADOS	**E.1**	Errores de los usuarios	Pérdida total o parcial del tiempo de ejecución de sus actividades, dependiendo de la gravedad del asunto.	Baja	3	6	2	Tolerable
	E.2	Errores del administrador	Pérdida total o parcial del tiempo de ejecución de sus actividades, dependiendo de la gravedad del asunto.	Baja	3	6	2	Tolerable
	E.8	Difusión de software dañino	La dependencia cuenta con antivirus capaces de controlar software malicioso	Baja	3	6	2	Tolerable
	E.9	Errores de [re-] encaminamiento	La dependencia cuenta con sistemas de cifrado y verificación (puerto – puerto) para el manejo de la movilidad de la información.	Baja	3	6	2	Tolerable
	E.10	Errores de secuencia	La dependencia cuenta con sistemas de cifrado y verificación (puerto – puerto) para el manejo de la movilidad de la información.	Baja	3	6	2	Tolerable
	E.15	Alteración accidental de la información	La dependencia cuenta con sistemas de cifrado y verificación (puerto – puerto) para el manejo de la movilidad de la información.	Baja	3	6	2	Tolerable
	E.18	Destrucción de información	El departamento de sistemas cuenta con copias de seguridad periódicas	Baja	3	6	2	Tolerable

Tabla 43. Estimación del riesgo activo COMMAND (CMD). (Continuación)

	E.19	Fugas de información	Las personas contratadas están atadas a cláusulas de confidencialidad.	Baja	3	6	2	Tolerable
	E.20	Vulnerabilidades de los programas (software)	La dependencia cuenta con un servidor (personal) para llevar a cabo cada uno de los softwares empleados para la institución.	Baja	3	6	2	Tolerable
	E.21	Errores de mantenimiento / actualización de programas (software)	Falla de funcionamiento del software.	Baja	3	6	2	Tolerable
ATAQUES INTENCIONAD	**A.5**	Suplantación de la identidad del usuario	Acceso a personas que no cuenten con los permisos necesarios o con las credenciales necesarias.	Baja	3	6	2	Tolerable
	A.6	Abuso de privilegios de acceso	Abuso de cada uno de los derechos otorgados.	Baja	3	6	2	Tolerable
	A.7	Uso no previsto	Implementación de recursos (económicos y de tiempo) en actividades no relacionadas.	Baja	3	6	2	Tolerable
	A.8	Difusión de software dañino	Afectación en los sistemas de información y los procesos que ello conlleva.	Baja	3	6	2	Tolerable

Tabla 43. Estimación del riesgo activo COMMAND (CMD). (Continuación)

	A.9	[Re-]encaminamiento de mensajes	La dependencia cuenta con sistemas de cifrado y verificación (puerto – puerto) para el manejo de la movilidad de la información.	Baja	3	6	2	Tolerable
	A.10	Alteración de secuencia	Alteración de datos.	Baja	3	6	2	Tolerable
	A.11	Acceso no autorizado	Uso ilícito del hardware	Baja	3	6	2	Tolerable
	A.15	Modificación deliberada de la información	Datos erróneos en el momento de la movilización de la información.	Baja	3	6	2	Tolerable
	A.18	Destrucción de información	Perdida de la información.	Baja	3	6	2	Tolerable
	A.19	Divulgación de información	Información filtrada abiertamente a personas no correspondientes.	Baja	3	6	2	Tolerable
	A.22	Manipulación de programas	Alteración del funcionamiento de cada uno de los programas de la dependencia.	Baja	3	6	2	Tolerable

Fuente: Autoría propia

Tabla 44. Estimación del riesgo activo *CoMmanD line* (Mac)

ACTIVO TI	**TERMINAL COMMAND LINE (MAC)**
ADMINISTRADOR	PIMIENTO CARDENAS WILSON MAURICIO
DEGRADACIÓN	45%
IMPACTO	3
TIPO DE ACTIVO	SOFTWARE

Tabla 44. Estimación del riesgo activo *Command line* (Mac). (Continuación)

Tipo	ID	Amenaza	Exposición/Vulnerabilidad	RIESGO ACTUAL				
							3	Intolerable
				Frecuencia (F)		R	NR	
DE ORIGEN INDUSTRIAL	**I.5**	Avería de origen físico o lógico	La manipulación por parte de cada uno de los componentes encontrados en la dependencia, como también por defectos de los componentes desde fabrica	Baja	3	9	3	Intolerable
ERRORES Y FALLOS NO INTENCIONADOS	**E.1**	Errores de los usuarios	Pérdida total o parcial del tiempo de ejecución de sus actividades, dependiendo de la gravedad del asunto.	Baja	3	9	3	Intolerable
	E.2	Errores del administrador	Pérdida total o parcial del tiempo de ejecución de sus actividades, dependiendo de la gravedad del asunto.	Baja	3	9	3	Intolerable
	E.8	Difusión de software dañino	La dependencia cuenta con antivirus capaces de controlar software malicioso	Baja	3	9	3	Intolerable
	E.9	Errores de [re-] encaminamiento	La dependencia cuenta con sistemas de cifrado y verificación (puerto – puerto) para el manejo de la movilidad de la información.	Baja	3	9	3	Intolerable

Tabla 44. Estimación del riesgo activo *Command line* (Mac). (Continuación)

	E.10	Errores de secuencia	La dependencia cuenta con sistemas de cifrado y verificación (puerto – puerto) para el manejo de la movilidad de la información.	Baja	3	9	3	Intolerable
	E.15	Alteración accidental de la información	La dependencia cuenta con sistemas de cifrado y verificación (puerto – puerto) para el manejo de la movilidad de la información.	Baja	3	9	3	Intolerable
	E.18	Destrucción de información	El departamento de sistemas cuenta con copias de seguridad periódicas	Baja	3	9	3	Intolerable
	E.19	Fugas de información	Las personas contratadas están atadas a cláusulas de confidencialidad.	Baja	3	9	3	Intolerable
	E.20	Vulnerabilidades de los programas (software)	La dependencia cuenta con un servidor (personal) para llevar a cabo cada uno de los softwares empleados para la institución.	Baja	3	9	3	Intolerable
	E.21	Errores de mantenimiento / actualización de programas (software)	Falla de funcionamiento del software.	Baja	3	9	3	Intolerable
ATAQUES INTENC	**A.5**	Suplantación de la identidad del usuario	Acceso a personas que no cuenten con los permisos necesarios o con las credenciales necesarias.	Baja	3	9	3	Intolerable

Tabla 44. Estimación del riesgo activo *Command line* (Mac). (Continuación)

	A.6	Abuso de privilegios de acceso	Abuso de cada uno de los derechos otorgados.	Baja	3	9	3	Intolerable
	A.7	Uso no previsto	Implementación de recursos (económicos y de tiempo) en actividades no relacionadas.	Baja	3	9	3	Intolerable
	A.8	Difusión de software dañino	Afectación en los sistemas de información y los procesos que ello conlleva.	Baja	3	9	3	Intolerable
	A.9	[Re-]encaminamiento de mensajes	La dependencia cuenta con sistemas de cifrado y verificación (puerto – puerto) para el manejo de la movilidad de la información.	Baja	3	9	3	Intolerable
	A.10	Alteración de secuencia	Alteración de datos.	Baja	3	9	3	Intolerable
	A.11	Acceso no autorizado	Uso ilícito del hardware	Baja	3	9	3	Intolerable
	A.15	Modificación deliberada de la información	Datos erróneos en el momento de la movilización de la información.	Baja	3	9	3	Intolerable
	A.18	Destrucción de información	Perdida de la información.	Baja	3	9	3	Intolerable
	A.19	Divulgación de información	Información filtrada abiertamente a personas no correspondientes.	Baja	3	9	3	Intolerable

Tabla 44. Estimación del riesgo activo *Command line* (Mac). (Continuación)

	A.22	Manipulación de programas	Alteración del funcionamiento de cada uno de los programas de la dependencia.	Baja	3	9	3	Intolerable

Fuente: Autoría propia

Tabla 45. Estimación del riesgo activo terminal

ACTIVO TI	**TERMINAL LINUX**							
ADMINISTRADOR	PIMIENTO CARDENAS WILSON MAURICIO							
DEGRADACIÓN	30%							
IMPACTO	2							
TIPO DE ACTIVO	SOFTWARE							
Tipo	**ID**	**Amenaza**	**Exposición/Vulnerabilidad**	**RIESGO ACTUAL**				
							2	Tolerable
				Frecuencia (F)		**R**	**NR**	
DE ORIGEN INDUSTRIAL	**I.5**	Avería de origen físico o lógico	La manipulación por parte de cada uno de los componentes encontrados en la dependencia, como también por defectos de los componentes desde fabrica	Baja	3	6	2	Tolerable
ERRORES Y FALLOS NO INTENCIONADOS	**E.1**	Errores de los usuarios	Pérdida total o parcial del tiempo de ejecución de sus actividades, dependiendo de la gravedad del asunto.	Baja	3	6	2	Tolerable
	E.2	Errores del administrador	Pérdida total o parcial del tiempo de ejecución de sus actividades, dependiendo de la gravedad del asunto.	Baja	3	6	2	Tolerable

Tabla 45. Estimación del riesgo activo terminal. (Continuación)

	E.8	Difusión de software dañino	La dependencia cuenta con antivirus capaces de controlar software malicioso	Baja	3	6	2	Tolerable
	E.9	Errores de [re-] encaminamiento	La dependencia cuenta con sistemas de cifrado y verificación (puerto – puerto) para el manejo de la movilidad de la información.	Baja	3	6	2	Tolerable
	E.10	Errores de secuencia	La dependencia cuenta con sistemas de cifrado y verificación (puerto – puerto) para el manejo de la movilidad de la información.	Baja	3	6	2	Tolerable
	E.15	Alteración accidental de la información	La dependencia cuenta con sistemas de cifrado y verificación (puerto – puerto) para el manejo de la movilidad de la información.	Baja	3	6	2	Tolerable
	E.18	Destrucción de información	El departamento de sistemas cuenta con copias de seguridad periódicas	Baja	3	6	2	Tolerable
	E.19	Fugas de información	Las personas contratadas están atadas a cláusulas de confidencialidad.	Baja	3	6	2	Tolerable
	E.20	Vulnerabilidades de los programas (software)	La dependencia cuenta con un servidor (personal) para llevar a cabo cada uno de los softwares empleados para la institución.	Baja	3	6	2	Tolerable

Tabla 45. Estimación del riesgo activo terminal. (Continuación)

	E.21	Errores de mantenimiento / actualización de programas (software)	Falla de funcionamiento del software.	Baja	3	6	2	Tolerable
ATAQUES INTENCIONAD	**A.5**	Suplantación de la identidad del usuario	Acceso a personas que no cuenten con los permisos necesarios o con las credenciales necesarias.	Baja	3	6	2	Tolerable
	A.6	Abuso de privilegios de acceso	Abuso de cada uno de los derechos otorgados.	Baja	3	6	2	Tolerable
	A.7	Uso no previsto	Implementación de recursos (económicos y de tiempo) en actividades no relacionadas.	Baja	3	6	2	Tolerable
	A.8	Difusión de software dañino	Afectación en los sistemas de información y los procesos que ello conlleva.	Baja	3	6	2	Tolerable
	A.9	[Re-]encaminamiento de mensajes	La dependencia cuenta con sistemas de cifrado y verificación (puerto – puerto) para el manejo de la movilidad de la información.	Baja	3	6	2	Tolerable
	A.10	Alteración de secuencia	Alteración de datos.	Baja	3	6	2	Tolerable
	A.11	Acceso no autorizado	Uso ilícito del hardware	Baja	3	6	2	Tolerable

Tabla 45. Estimación del riesgo activo terminal. (Continuación)

	A.15	Modificación deliberada de la información	Datos erróneos en el momento de la movilización de la información.	Baja	3	6	2	Tolerable
	A.18	Destrucción de información	Perdida de la información.	Baja	3	6	2	Tolerable
	A.19	Divulgación de información	Información filtrada abiertamente a personas no correspondientes.	Baja	3	6	2	Tolerable
	A.22	Manipulación de programas	Alteración del funcionamiento de cada uno de los programas de la dependencia.	Baja	3	6	2	Tolerable

Fuente: Autoría propia

Tabla 46. Estimación del riesgo activo servidor DNS y DHCP

ACTIVO TI	**SERVIDOR DNS Y DHCP**							
ADMINISTRADOR	PIMIENTO CARDENAS WILSON MAURICIO							
DEGRADACIÓN	90%							
IMPACTO	8							
TIPO DE ACTIVO	HARDWARE							
Tipo	**ID**	**Amenaza**	**Exposición/Vulnerabilidad**	**RIESGO ACTUAL**				
							3.92	Intolerable
				Frecuencia (F)		**R**	**NR**	
DESASTRES NATURA	**N.1**	Fuego	No existe sistema de alarma contra incendios. Se posee un solo extintor de solkaflam (clase c) recomendados para incendios en	Muy baja	2	16	4	Extremo

Tabla 46. Estimación del riesgo activo servidor DNS y DHCP. (Continuación)

			lugares donde se encuentren equipos eléctricos.					
	N.2	Daños por agua	La infraestructura está expuesta a goteras, cuenta con averías en el techo en donde el agua de las lluvias	Muy baja	2	16	4	Extremo
	N.*	Desastres naturales	La oficina de la dependencia de sistemas se encuentra en zona baja de riesgo de desastre natural de origen volcánico debido a su cercanía con el volcán nevado del Tolima.	Raro	1	8	3	Intolerable
DE ORIGEN INDUSTRIAL	**I.1**	Fuego	No existe sistema de alarma contra incendios. Se posee un solo extintor de solkaflam (clase c) recomendados para incendios en lugares donde se encuentren equipos eléctricos.	Muy baja	2	16	4	Extremo
	I.2	Daños por agua	La concentración del líquido sobrante por parte del aire acondicionado causaría daños en los equipos.	Muy baja	2	16	4	Extremo

Tabla 46. Estimación del riesgo activo servidor DNS y DHCP. (Continuación)

	I.*	Desastres industriales	No hay exposición o vulnerabilidad, por parte de esta amenaza.	Muy baja	2	16	4	Extremo
	I.3	Contaminación mecánica	No hay exposición o vulnerabilidad, por parte de esta amenaza.	Muy baja	2	16	4	Extremo
	I.4	Contaminación electromagnética	No hay exposición o vulnerabilidad, por parte de esta amenaza.	Muy baja	2	16	4	Extremo
	I.5	Avería de origen físico o lógico	La manipulación por parte de cada uno de los componentes encontrados en la dependencia, como también por defectos de los componentes desde fabrica	Muy baja	2	16	4	Extremo
	I.6	Corte del suministro eléctrico	Amenaza debida a factores externos, a clemencias de tipo naturales como lluvias u otros.	Muy baja	2	16	4	Extremo
	I.7	Condiciones inadecuadas de temperatura o humedad	No se cuenta con una infraestructura adecuada para soportar los defectos del sistema de refrigeración.	Muy baja	2	16	4	Extremo
	I.11	Emanaciones electromagnéticas	No hay exposición o vulnerabilidad, por parte de esta amenaza.	Muy baja	2	16	4	Extremo

Tabla 46. Estimación del riesgo activo servidor DNS y DHCP. (Continuación)

ERRORES Y FALLOS NO INTENCIONADOS	**E.2**	Errores del administrador	Pérdida total o parcial del tiempo de ejecución de sus actividades, dependiendo de la gravedad del asunto.	Muy baja	2	16	4	Extremo
	E.23	Errores de mantenimiento / actualización de equipos(hardware)	Perjuicio a la mantenibilidad del sistema de información.	Muy baja	2	16	4	Extremo
	E.24	Caída del sistema por agotamiento de recursos	Saturación del sistema informático.	Muy baja	2	16	4	Extremo
	E.25	Perdida de equipos (Robo)	Recuperación de soportes reciclados o desechados.	Muy baja	2	16	4	Extremo
ATAQUES INTENCIONADOS	**A.6**	Abuso de privilegios de acceso	Abuso de cada uno de los derechos otorgados.	Muy baja	2	16	4	Extremo
	A.7	Uso no previsto	Implementación de recursos (económicos y de tiempo) en actividades no relacionadas.	Muy baja	2	16	4	Extremo
	A.11	Acceso no autorizado	Uso ilícito del hardware	Muy baja	2	16	4	Extremo
	A.23	Manipulación de los equipos	Sabotaje del hardware y software conteniente.	Muy baja	2	16	4	Extremo

Tabla 46. Estimación del riesgo activo servidor DNS y DHCP. (Continuación)

	A.24	Denegación de servicio	Saturación del sistema de información.	Muy baja	2	16	4	Extremo
	A.25	Robo	Robo de porte de la información, puede esta ser física o digital.	Muy baja	2	16	4	Extremo
	A.26	Ataque destructivo	Destrucción de los contenedores de la información, en recipientes físicos y lógicos.	Muy baja	2	16	4	Extremo

Fuente: Autoría propia

Tabla 47. Estimación del riesgo activo servidor plataforma RYCA V.2.0

ACTIVO TI	**SERVIDOR PLATAFORMA RYCA V.2.0**							
ADMINISTRADOR	PIMIENTO CARDENAS WILSON MAURICIO							
DEGRADACIÓN	90%							
IMPACTO	8							
TIPO DE ACTIVO	HARDWARE							
Tipo	**ID**	**Amenaza**	**Exposición/Vulnerabilidad**	**RIESGO ACTUAL**				
							4	Extremo
				Frecuencia (F)		**R**	**NR**	
DESASTRES NATURALES	**N.1**	Fuego	No existe sistema de alarma contra incendios. Se posee un solo extintor de solkaflam (clase c) recomendados para incendios en lugares donde se encuentren equipos eléctricos.	Muy baja	2	16	4	Extremo

Tabla 47. Estimación del riesgo activo servidor plataforma RYCA V.2.0. (Continuación)

	N.2	Daños por agua	La infraestructura está expuesta a goteras, cuenta con averías en el techo en donde el agua de las lluvias	Muy baja	2	16	4	Extremo
	N.*	Desastres naturales	La oficina de la dependencia de sistemas se encuentra en zona baja de riesgo de desastre natural de origen volcánico debido a su cercanía con el volcán nevado del Tolima.	Raro	1	16	4	Extremo
DE ORIGEN INDUSTRIAL	**I.1**	Fuego	No existe sistema de alarma contra incendios. Se posee un solo extintor de solkaflam (clase c) recomendados para incendios en lugares donde se encuentren equipos eléctricos.	Muy baja	2	16	4	Extremo
	I.2	Daños por agua	La concentración del líquido sobrante por parte del aire acondicionado causaría daños en los equipos.	Muy baja	2	16	4	Extremo
	I.*	Desastres industriales	No hay exposición o vulnerabilidad, por parte de esta amenaza.	Muy baja	2	16	4	Extremo
	I.3	Contaminación mecánica	No hay exposición o vulnerabilidad, por parte de esta amenaza.	Muy baja	2	16	4	Extremo
	I.4	Contaminación electromagnética	No hay exposición o vulnerabilidad, por parte de esta amenaza.	Muy baja	2	16	4	Extremo

Tabla 47. Estimación del riesgo activo servidor plataforma RYCA V.2.0. (Continuación)

	I.5	Avería de origen físico o lógico	La manipulación por parte de cada uno de los componentes encontrados en la dependencia, como también por defectos de los componentes desde fabrica	Muy baja	2	16	4	Extremo
	I.6	Corte del suministro eléctrico	Amenaza debida a factores externos, a clemencias de tipo naturales como lluvias u otros.	Muy baja	2	16	4	Extremo
	I.7	Condiciones inadecuadas de temperatura o humedad	No se cuenta con una infraestructura adecuada para soportar los defectos del sistema de refrigeración.	Muy baja	2	16	4	Extremo
	I.11	Emanaciones electromagnéticas	No hay exposición o vulnerabilidad, por parte de esta amenaza.	Muy baja	2	16	4	Extremo
ERRORES Y FALLOS NO INTENCIONADOS	**E.2**	Errores del administrador	Pérdida total o parcial del tiempo de ejecución de sus actividades, dependiendo de la gravedad del asunto.	Muy baja	2	16	4	Extremo
	E.23	Errores de mantenimiento / actualización de equipos(hardware)	Perjuicio a la mantenibilidad del sistema de información.	Muy baja	2	16	4	Extremo

Tabla 47. Estimación del riesgo activo servidor plataforma RYCA V.2.0. (Continuación)

	E.24	Caída del sistema por agotamiento de recursos	Saturación del sistema informático.	Muy baja	2	16	4	Extremo
	E.25	Perdida de equipos (Robo)	Recuperación de soportes reciclados o desechados.	Muy baja	2	16	4	Extremo
ATAQUES INTENCIONADOS	**A.6**	Abuso de privilegios de acceso	Abuso de cada uno de los derechos otorgados.	Muy baja	2	16	4	Extremo
	A.7	Uso no previsto	Implementación de recursos (económicos y de tiempo) en actividades no relacionadas.	Muy baja	2	16	4	Extremo
	A.11	Acceso no autorizado	Uso ilícito del hardware	Muy baja	2	16	4	Extremo
	A.23	Manipulación de los equipos	Sabotaje del hardware y software conteniente.	Muy baja	2	16	4	Extremo
	A.24	Denegación de servicio	Saturación del sistema de información.	Muy baja	2	16	4	Extremo
	A.25	Robo	Robo de porte de la información, puede esta ser física o digital.	Muy baja	2	16	4	Extremo
	A.26	Ataque destructivo	Destrucción de los contenedores de la información, en recipientes físicos y lógicos.	Muy baja	2	16	4	Extremo

Fuente: Autoría propia

Tabla 48. Estimación del riesgo activo servidor plataforma RYCA V.1

ACTIVO TI	**SERVIDOR PLATAFORMA RYCA V.1**							
ADMINISTRADOR	PIMIENTO CARDENAS WILSON MAURICIO							
DEGRADACIÓN	90%							
IMPACTO	8							
TIPO DE ACTIVO	HARDWARE							
Tipo	**ID**	**Amenaza**	**Exposición/Vulnerabilidad**	**RIESGO ACTUAL**				
							3.96	Intolerable
				Frecuencia (F)		**R**	**NR**	
DESASTRES NATURALES	**N.1**	Fuego	No existe sistema de alarma contra incendios. Se posee un solo extintor de solkaflam (clase c) recomendados para incendios en lugares donde se encuentren equipos eléctricos.	Muy baja	2	16	4	Extremo
	N.2	Daños por agua	La infraestructura está expuesta a goteras, cuenta con averías en el techo en donde el agua de las lluvias	Muy baja	2	16	4	Extremo
	N.*	Desastres naturales	La oficina de la dependencia de sistemas se encuentra en zona baja de riesgo de desastre natural de origen volcánico debido a su cercanía con el volcán nevado del Tolima.	Raro	1	8	3	Intolerable

Tabla 48. Estimación del riesgo activo servidor plataforma RYCA V.1. (Continuación)

DE ORIGEN INDUSTRIAL	**I.1**	Fuego	No existe sistema de alarma contra incendios. Se posee un solo extintor de solkaflam (clase c) recomendados para incendios en lugares donde se encuentren equipos eléctricos.	Muy baja	2	16	4	Extremo
	I.2	Daños por agua	La concentración del líquido sobrante por parte del aire acondicionado causaría daños en los equipos.	Muy baja	2	16	4	Extremo
	I.*	Desastres industriales	No hay exposición o vulnerabilidad, por parte de esta amenaza.	Muy baja	2	16	4	Extremo
	I.3	Contaminación mecánica	No hay exposición o vulnerabilidad, por parte de esta amenaza.	Muy baja	2	16	4	Extremo
	I.4	Contaminación electromagnética	No hay exposición o vulnerabilidad, por parte de esta amenaza.	Muy baja	2	16	4	Extremo
	I.5	Avería de origen físico o lógico	La manipulación por parte de cada uno de los componentes encontrados en la dependencia, como también por defectos de los componentes desde fabrica	Muy baja	2	16	4	Extremo

Tabla 48. Estimación del riesgo activo servidor plataforma RYCA V.1. (Continuación)

	I.6	Corte del suministro eléctrico	Amenaza debida a factores externos, a clemencias de tipo naturales como lluvias u otros.	Muy baja	2	16	4	Extremo
	I.7	Condiciones inadecuadas de temperatura o humedad	No se cuenta con una infraestructura adecuada para soportar los defectos del sistema de refrigeración.	Muy baja	2	16	4	Extremo
	I.11	Emanaciones electromagnéticas	No hay exposición o vulnerabilidad, por parte de esta amenaza.	Muy baja	2	16	4	Extremo
ERRORES Y FALLOS NO INTENCIONADOS	**E.2**	Errores del administrador	Pérdida total o parcial del tiempo de ejecución de sus actividades, dependiendo de la gravedad del asunto.	Muy baja	2	16	4	Extremo
	E.23	Errores de mantenimiento / actualización de equipos(hardware)	Perjuicio a la mantenibilidad del sistema de información.	Muy baja	2	16	4	Extremo
	E.24	Caída del sistema por agotamiento de recursos	Saturación del sistema informático.	Muy baja	2	16	4	Extremo
	E.25	Perdida de equipos (Robo)	Recuperación de soportes reciclados o desechados.	Muy baja	2	16	4	Extremo

Tabla 48. Estimación del riesgo activo servidor plataforma RYCA V.1. (Continuación)

ATAQUES INTENCIONADOS	**A.6**	Abuso de privilegios de acceso	Abuso de cada uno de los derechos otorgados.	Muy baja	2	16	4	Extremo
	A.7	Uso no previsto	Implementación de recursos (económicos y de tiempo) en actividades no relacionadas.	Muy baja	2	16	4	Extremo
	A.11	Acceso no autorizado	Uso ilícito del hardware	Muy baja	2	16	4	Extremo
	A.23	Manipulación de los equipos	Sabotaje del hardware y software conteniente.	Muy baja	2	16	4	Extremo
	A.24	Denegación de servicio	Saturación del sistema de información.	Muy baja	2	16	4	Extremo
	A.25	Robo	Robo de porte de la información, puede esta ser física o digital.	Muy baja	2	16	4	Extremo
	A.26	Ataque destructivo	Destrucción de los contenedores de la información, en recipientes físicos y lógicos.	Muy baja	2	16	4	Extremo

Fuente: Autoría propia

Tabla 49. Estimación del riesgo activo servidor de base de datos ITFIP

ACTIVO TI	**SERVIDOR DE BASE DE DATOS ITFIP**
ADMINISTRADOR	PIMIENTO CARDENAS WILSON MAURICIO
DEGRADACIÓN	90%
IMPACTO	8

Tabla 49. Estimación del riesgo activo servidor de base de datos ITFIP. (Continuación)

TIPO DE ACTIVO		HARDWARE						
Tipo	**ID**	**Amenaza**	**Exposición/Vulnerabilidad**	**RIESGO ACTUAL**				
							3.96	Intolerable
				Frecuencia (F)		**R**	**NR**	
DESASTRES NATURALES	**N.1**	Fuego	No existe sistema de alarma contra incendios. Se posee un solo extintor de solkaflam (clase c) recomendados para incendios en lugares donde se encuentren equipos eléctricos.	Muy baja	2	16	4	Extremo
	N.2	Daños por agua	La infraestructura está expuesta a goteras, cuenta con averías en el techo en donde el agua de las lluvias	Muy baja	2	16	4	Extremo
	N.*	Desastres naturales	La oficina de la dependencia de sistemas se encuentra en zona baja de riesgo de desastre natural de origen volcánico debido a su cercanía con el volcán nevado del Tolima.	Raro	1	8	3	Intolerable
DE ORIGEN INDUSTRIAL	**I.1**	Fuego	No existe sistema de alarma contra incendios. Se posee un solo extintor de solkaflam (clase c) recomendados para incendios en lugares donde se encuentren equipos eléctricos.	Muy baja	2	16	4	Extremo

Tabla 49. Estimación del riesgo activo servidor de base de datos ITFIP. (Continuación)

	I.2	Daños por agua	La concentración del líquido sobrante por parte del aire acondicionado causaría daños en los equipos.	Muy baja	2	16	4	Extremo
	I.*	Desastres industriales	No hay exposición o vulnerabilidad, por parte de esta amenaza.	Muy baja	2	16	4	Extremo
	I.3	Contaminación mecánica	No hay exposición o vulnerabilidad, por parte de esta amenaza.	Muy baja	2	16	4	Extremo
	I.4	Contaminación electromagnética	No hay exposición o vulnerabilidad, por parte de esta amenaza.	Muy baja	2	16	4	Extremo
	I.5	Avería de origen físico o lógico	La manipulación por parte de cada uno de los componentes encontrados en la dependencia, como también por defectos de los componentes desde fabrica	Muy baja	2	16	4	Extremo
	I.6	Corte del suministro eléctrico	Amenaza debida a factores externos, a clemencias de tipo naturales como lluvias u otros.	Muy baja	2	16	4	Extremo
	I.7	Condiciones inadecuadas de temperatura o humedad	No se cuenta con una infraestructura adecuada para soportar los defectos del sistema de refrigeración.	Muy baja	2	16	4	Extremo

Tabla 49. Estimación del riesgo activo servidor de base de datos ITFIP. (Continuación)

	I.11	Emanaciones electromagnéticas	No hay exposición o vulnerabilidad, por parte de esta amenaza.	Muy baja	2	16	4	Extremo
NO FALLOS Y ERRORES INTENCIONADOS	**E.2**	Errores del administrador	Pérdida total o parcial del tiempo de ejecución de sus actividades, dependiendo de la gravedad del asunto.	Muy baja	2	16	4	Extremo
	E.23	Errores de mantenimiento / actualización de equipos(hardware)	Perjuicio a la mantenibilidad del sistema de información.	Muy baja	2	16	4	Extremo
	E.24	Caída del sistema por agotamiento de recursos	Saturación del sistema informático.	Muy baja	2	16	4	Extremo
	E.25	Perdida de equipos (Robo)	Recuperación de soportes reciclados o desechados.	Muy baja	2	16	4	Extremo
ATAQUES INTENCIONADOS	**A.6**	Abuso de privilegios de acceso	Abuso de cada uno de los derechos otorgados.	Muy baja	2	16	4	Extremo
	A.7	Uso no previsto	Implementación de recursos (económicos y de tiempo) en actividades no relacionadas.	Muy baja	2	16	4	Extremo
	A.11	Acceso no autorizado	Uso ilícito del hardware	Muy baja	2	16	4	Extremo

Tabla 49. Estimación del riesgo activo servidor de base de datos ITFIP. (Continuación)

	A.23	Manipulación de los equipos	Sabotaje del hardware y software conteniente.	Muy baja	2	16	4	Extremo
	A.24	Denegación de servicio	Saturación del sistema de información.	Muy baja	2	16	4	Extremo
	A.25	Robo	Robo de porte de la información, puede esta ser física o digital.	Muy baja	2	16	4	Extremo
	A.26	Ataque destructivo	Destrucción de los contenedores de la información, en recipientes físicos y lógicos.	Muy baja	2	16	4	Extremo

Fuente: Autoría propia

Tabla 50. Estimación del riesgo activo servidor firewall FORTIGATE

ACTIVO TI	**SERVIDOR FIREWALL FORTIGATE**							
ADMINISTRADOR	PIMIENTO CARDENAS WILSON MAURICIO							
DEGRADACIÓN	90%							
IMPACTO	8							
TIPO DE ACTIVO	HARDWARE							
Tipo	**ID**	**Amenaza**	**Exposición/Vulnerabilidad**	**RIESGO ACTUAL**				
							3.96	Intolerable
				Frecuencia (F)		**R**	**NR**	
DESASTRES NATURA	**N.1**	Fuego	No existe sistema de alarma contra incendios. Se posee un solo extintor de solkaflam (clase c) recomendados para incendios en	Muy baja	2	16	4	Extremo

Tabla 50. Estimación del riesgo activo servidor *firewall* FORTIGATE. (Continuación)

			lugares donde se encuentren equipos eléctricos.					
	N.2	Daños por agua	La infraestructura está expuesta a goteras, cuenta con averías en el techo en donde el agua de las lluvias	Muy baja	2	16	4	Extremo
	N.*	Desastres naturales	La oficina de la dependencia de sistemas se encuentra en zona baja de riesgo de desastre natural de origen volcánico debido a su cercanía con el volcán nevado del Tolima.	Raro	1	8	3	Intolerable
DE ORIGEN INDUSTRIAL	**I.1**	Fuego	No existe sistema de alarma contra incendios. Se posee un solo extintor de solkaflam (clase c) recomendados para incendios en lugares donde se encuentren equipos eléctricos.	Muy baja	2	16	4	Extremo
	I.2	Daños por agua	La concentración del líquido sobrante por parte del aire acondicionado causaría daños en los equipos.	Muy baja	2	16	4	Extremo

Tabla 50. Estimación del riesgo activo servidor *firewall* FORTIGATE. (Continuación)

	I.*	Desastres industriales	No hay exposición o vulnerabilidad, por parte de esta amenaza.	Muy baja	2	16	4	Extremo
	I.3	Contaminación mecánica	No hay exposición o vulnerabilidad, por parte de esta amenaza.	Muy baja	2	16	4	Extremo
	I.4	Contaminación electromagnética	No hay exposición o vulnerabilidad, por parte de esta amenaza.	Muy baja	2	16	4	Extremo
	I.5	Avería de origen físico o lógico	La manipulación por parte de cada uno de los componentes encontrados en la dependencia, como también por defectos de los componentes desde fabrica	Muy baja	2	16	4	Extremo
	I.6	Corte del suministro eléctrico	Amenaza debida a factores externos, a clemencias de tipo naturales como lluvias u otros.	Muy baja	2	16	4	Extremo
	I.7	Condiciones inadecuadas de temperatura o humedad	No se cuenta con una infraestructura adecuada para soportar los defectos del sistema de refrigeración.	Muy baja	2	16	4	Extremo
	I.11	Emanaciones electromagnéticas	No hay exposición o vulnerabilidad, por parte de esta amenaza.	Muy baja	2	16	4	Extremo

Tabla 50. Estimación del riesgo activo servidor *firewall* FORTIGATE. (Continuación)

ERRORES Y FALLOS NO INTENCIONADOS	**E.2**	Errores del administrador	Pérdida total o parcial del tiempo de ejecución de sus actividades, dependiendo de la gravedad del asunto.	Muy baja	2	16	4	Extremo
	E.23	Errores de mantenimiento / actualización de equipos(hardware)	Perjuicio a la mantenibilidad del sistema de información.	Muy baja	2	16	4	Extremo
	E.24	Caída del sistema por agotamiento de recursos	Saturación del sistema informático.	Muy baja	2	16	4	Extremo
	E.25	Perdida de equipos (Robo)	Recuperación de soportes reciclados o desechados.	Muy baja	2	16	4	Extremo
ATAQUES INTENCIONADOS	**A.6**	Abuso de privilegios de acceso	Abuso de cada uno de los derechos otorgados.	Muy baja	2	16	4	Extremo
	A.7	Uso no previsto	Implementación de recursos (económicos y de tiempo) en actividades no relacionadas.	Muy baja	2	16	4	Extremo
	A.11	Acceso no autorizado	Uso ilícito del hardware	Muy baja	2	16	4	Extremo
	A.23	Manipulación de los equipos	Sabotaje del hardware y software conteniente.	Muy baja	2	16	4	Extremo

Tabla 50. Estimación del riesgo activo servidor *firewall* FORTIGATE. (Continuación)

	A.24	Denegación de servicio	Saturación del sistema de información.	Muy baja	2	16	4	Extremo
	A.25	Robo	Robo de porte de la información, puede esta ser física o digital.	Muy baja	2	16	4	Extremo
	A.26	Ataque destructivo	Destrucción de los contenedores de la información, en recipientes físicos y lógicos.	Muy baja	2	16	4	Extremo

Fuente: Autoría propia

Tabla 51. Estimación del riesgo activo servidor contable SIIGO

ACTIVO TI	**SERVIDOR CONTABLE SIIGO**							
ADMINISTRADOR	PIMIENTO CARDENAS WILSON MAURICIO							
DEGRADACIÓN	90%							
IMPACTO	8							
TIPO DE ACTIVO	HARDWARE							
Tipo	**ID**	**Amenaza**	**Exposición/Vulnerabilidad**	**RIESGO ACTUAL**				
							3.96	Intolerable
				Frecuencia (F)		**R**	**NR**	
DESASTRES NATURALES	**N.1**	Fuego	No existe sistema de alarma contra incendios. Se posee un solo extintor de solkaflam (clase c) recomendados para incendios en lugares donde se encuentren equipos eléctricos.	Muy baja	2	16	4	Extremo

Tabla 51. Estimación del riesgo activo servidor contable SIIGO. (Continuación)

	N.2	Daños por agua	La infraestructura está expuesta a goteras, cuenta con averías en el techo en donde el agua de las lluvias	Muy baja	2	16	4	Extremo
	N.*	Desastres naturales	La oficina de la dependencia de sistemas se encuentra en zona baja de riesgo de desastre natural de origen volcánico debido a su cercanía con el volcán nevado del Tolima.	Raro	1	8	3	Intolerable
DE ORIGEN INDUSTRIAL	**I.1**	Fuego	No existe sistema de alarma contra incendios. Se posee un solo extintor de solkaflam (clase c) recomendados para incendios en lugares donde se encuentren equipos eléctricos.	Muy baja	2	16	4	Extremo
	I.2	Daños por agua	La concentración del líquido sobrante por parte del aire acondicionado causaría daños en los equipos.	Muy baja	2	16	4	Extremo
	I.*	Desastres industriales	No hay exposición o vulnerabilidad, por parte de esta amenaza.	Muy baja	2	16	4	Extremo
	I.3	Contaminación mecánica	No hay exposición o vulnerabilidad, por parte de esta amenaza.	Muy baja	2	16	4	Extremo

Tabla 51. Estimación del riesgo activo servidor contable SIIGO. (Continuación)

	I.4	Contaminación electromagnética	No hay exposición o vulnerabilidad, por parte de esta amenaza.	Muy baja	2	16	4	Extremo
	I.5	Avería de origen físico o lógico	La manipulación por parte de cada uno de los componentes encontrados en la dependencia, como también por defectos de los componentes desde fabrica	Muy baja	2	16	4	Extremo
	I.6	Corte del suministro eléctrico	Amenaza debida a factores externos, a clemencias de tipo naturales como lluvias u otros.	Muy baja	2	16	4	Extremo
	I.7	Condiciones inadecuadas de temperatura o humedad	No se cuenta con una infraestructura adecuada para soportar los defectos del sistema de refrigeración.	Muy baja	2	16	4	Extremo
	I.11	Emanaciones electromagnéticas	No hay exposición o vulnerabilidad, por parte de esta amenaza.	Muy baja	2	16	4	Extremo
ERRORES Y FALLOS NO INTENCIONADOS	**E.2**	Errores del administrador	Pérdida total o parcial del tiempo de ejecución de sus actividades, dependiendo de la gravedad del asunto.	Muy baja	2	16	4	Extremo
	E.23	Errores de mantenimiento /	Perjuicio a la mantenibilidad del sistema de información.	Muy baja	2	16	4	Extremo

Tabla 51. Estimación del riesgo activo servidor contable SIIGO. (Continuación)

		actualización de equipos(hardware)						
	E.24	Caída del sistema por agotamiento de recursos	Saturación del sistema informático.	Muy baja	2	16	4	Extremo
	E.25	Perdida de equipos (Robo)	Recuperación de soportes reciclados o desechados.	Muy baja	2	16	4	Extremo
ATAQUES INTENCIONADOS	**A.6**	Abuso de privilegios de acceso	Abuso de cada uno de los derechos otorgados.	Muy baja	2	16	4	Extremo
	A.7	Uso no previsto	Implementación de recursos (económicos y de tiempo) en actividades no relacionadas.	Muy baja	2	16	4	Extremo
	A.11	Acceso no autorizado	Uso ilícito del hardware	Muy baja	2	16	4	Extremo
	A.23	Manipulación de los equipos	Sabotaje del hardware y software conteniente.	Muy baja	2	16	4	Extremo
	A.24	Denegación de servicio	Saturación del sistema de información.	Muy baja	2	16	4	Extremo
	A.25	Robo	Robo de porte de la información, puede esta ser física o digital.	Muy baja	2	16	4	Extremo

Tabla 51. Estimación del riesgo activo servidor contable SIIGO. (Continuación)

	A.26	Ataque destructivo	Destrucción de los contenedores de la información, en recipientes físicos y lógicos.	Muy baja	2	16	4	Extremo

Fuente: Autoría propia

Tabla 52. Estimación del riesgo activo servidor de pruebas “desarrollito”

ACTIVO TI	**SERVIDOR DE PRUEBAS “DESARROLLITO”**
ADMINISTRADOR	PIMIENTO CARDENAS WILSON MAURICIO
DEGRADACIÓN	45%
IMPACTO	3
TIPO DE ACTIVO	HARDWARE

Tipo	ID	Amenaza	Exposición/Vulnerabilidad	RIESGO ACTUAL				
							2	Tolerable
				Frecuencia (F)		**R**	**NR**	
DESASTRES NATURALES	**N.1**	Fuego	No existe sistema de alarma contra incendios. Se posee un solo extintor de solkaflam (clase c) recomendados para incendios en lugares donde se encuentren equipos eléctricos.	Muy baja	2	6	2	Tolerable
	N.2	Daños por agua	La infraestructura está expuesta a goteras, cuenta con averías en el techo en donde el agua de las lluvias	Muy baja	2	6	2	Tolerable

Tabla 52. Estimación del riesgo activo servidor de pruebas “desarrollito”. (Continuación)

	N.*	Desastres naturales	La oficina de la dependencia de sistemas se encuentra en zona baja de riesgo de desastre natural de origen volcánico debido a su cercanía con el volcán nevado del Tolima.	Raro	1	3	2	Tolerable
DE ORIGEN INDUSTRIAL	**I.1**	Fuego	No existe sistema de alarma contra incendios. Se posee un solo extintor de solkaflam (clase c) recomendados para incendios en lugares donde se encuentren equipos eléctricos.	Muy baja	2	6	2	Tolerable
	I.2	Daños por agua	La concentración del líquido sobrante por parte del aire acondicionado causaría daños en los equipos.	Muy baja	2	6	2	Tolerable
	I.*	Desastres industriales	No hay exposición o vulnerabilidad, por parte de esta amenaza.	Muy baja	2	6	2	Tolerable
	I.3	Contaminación mecánica	No hay exposición o vulnerabilidad, por parte de esta amenaza.	Muy baja	2	6	2	Tolerable
	I.4	Contaminación electromagnética	No hay exposición o vulnerabilidad, por parte de esta amenaza.	Muy baja	2	6	2	Tolerable
	I.5	Avería de origen físico o lógico	La manipulación por parte de cada uno de los componentes encontrados en la dependencia, como también por	Muy baja	2	6	2	Tolerable

Tabla 52. Estimación del riesgo activo servidor de pruebas “desarrollito”. (Continuación)

			defectos de los componentes desde fabrica					
	I.6	Corte del suministro eléctrico	Amenaza debida a factores externos, a clemencias de tipo naturales como lluvias u otros.	Muy baja	2	6	2	Tolerable
	I.7	Condiciones inadecuadas de temperatura o humedad	No se cuenta con una infraestructura adecuada para soportar los defectos del sistema de refrigeración.	Muy baja	2	6	2	Tolerable
	I.11	Emanaciones electromagnéticas	No hay exposición o vulnerabilidad, por parte de esta amenaza.	Muy baja	2	6	2	Tolerable
ERRORES Y FALLOS NO INTENCIONADOS	**E.2**	Errores del administrador	Pérdida total o parcial del tiempo de ejecución de sus actividades, dependiendo de la gravedad del asunto.	Muy baja	2	6	2	Tolerable
	E.23	Errores de mantenimiento / actualización de equipos(hardware)	Perjuicio a la mantenibilidad del sistema de información.	Muy baja	2	6	2	Tolerable
	E.24	Caída del sistema por agotamiento de recursos	Saturación del sistema informático.	Muy baja	2	6	2	Tolerable

Tabla 52. Estimación del riesgo activo servidor de pruebas “desarrollito”. (Continuación)

	E.25	Perdida de equipos (Robo)	Recuperación de soportes reciclados o desechados.	Muy baja	2	6	2	Tolerable
ATAQUES INTENCIONADOS	**A.6**	Abuso de privilegios de acceso	Abuso de cada uno de los derechos otorgados.	Muy baja	2	6	2	Tolerable
	A.7	Uso no previsto	Implementación de recursos (económicos y de tiempo) en actividades no relacionadas.	Muy baja	2	6	2	Tolerable
	A.11	Acceso no autorizado	Uso ilícito del hardware	Muy baja	2	6	2	Tolerable
	A.23	Manipulación de los equipos	Sabotaje del hardware y software conteniente.	Muy baja	2	6	2	Tolerable
	A.24	Denegación de servicio	Saturación del sistema de información.	Muy baja	2	6	2	Tolerable
	A.25	Robo	Robo de porte de la información, puede esta ser física o digital.	Muy baja	2	6	2	Tolerable
	A.26	Ataque destructivo	Destrucción de los contenedores de la información, en recipientes físicos y lógicos.	Muy baja	2	6	2	Tolerable

Fuente: Autoría propia

Tabla 52. Estimación del riesgo activo servidor de copias de seguridad de la información del ITFIP

ACTIVO TI	**SERVIDOR DE COPIAS DE SEGURIDAD DE LA INFORMACIÓN DEL ITFIP**
ADMINISTRADOR	PIMIENTO CARDENAS WILSON MAURICIO
DEGRADACIÓN	90%
IMPACTO	8
TIPO DE ACTIVO	HARDWARE

Tipo	ID	Amenaza	Exposición/Vulnerabilidad	RIESGO ACTUAL				
							4	Extremo
				Frecuencia (F)		R	NR	
DESASTRES NATURALES	**N.1**	Fuego	No existe sistema de alarma contra incendios. Se posee un solo extintor de solkaflam (clase c) recomendados para incendios en lugares donde se encuentren equipos eléctricos.	Muy baja	2	16	4	Extremo
	N.2	Daños por agua	La infraestructura está expuesta a goteras, cuenta con averías en el techo en donde el agua de las lluvias	Muy baja	2	16	4	Extremo
	N.*	Desastres naturales	La oficina de la dependencia de sistemas se encuentra en zona baja de riesgo de desastre natural de origen volcánico debido a su cercanía con el volcán nevado del Tolima.	Raro	1			
DE ORIGEN INDUST	**I.1**	Fuego	No existe sistema de alarma contra incendios. Se posee un solo extintor de solkaflam (clase c) recomendados para	Muy baja	2	16	4	Extremo

Tabla 52. Estimación del riesgo activo servidor de copias de seguridad de la información del ITFIP. (Continuación)

			incendios en lugares donde se encuentren equipos eléctricos.					
	I.2	Daños por agua	La concentración del líquido sobrante por parte del aire acondicionado causaría daños en los equipos.	Muy baja	2	16	4	Extremo
	I.*	Desastres industriales	No hay exposición o vulnerabilidad, por parte de esta amenaza.	Muy baja	2	16	4	Extremo
	I.3	Contaminación mecánica	No hay exposición o vulnerabilidad, por parte de esta amenaza.	Muy baja	2	16	4	Extremo
	I.4	Contaminación electromagnética	No hay exposición o vulnerabilidad, por parte de esta amenaza.	Muy baja	2	16	4	Extremo
	I.5	Avería de origen físico o lógico	La manipulación por parte de cada uno de los componentes encontrados en la dependencia, como también por defectos de los componentes desde fabrica	Muy baja	2	16	4	Extremo
	I.6	Corte del suministro eléctrico	Amenaza debida a factores externos, a clemencias de tipo naturales como lluvias u otros.	Muy baja	2	16	4	Extremo

Tabla 52. Estimación del riesgo activo servidor de copias de seguridad de la información del ITFIP. (Continuación)

	I.7	Condiciones inadecuadas de temperatura o humedad	No se cuenta con una infraestructura adecuada para soportar los defectos del sistema de refrigeración.	Muy baja	2	16	4	Extremo
	I.11	Emanaciones electromagnéticas	No hay exposición o vulnerabilidad, por parte de esta amenaza.	Muy baja	2	16	4	Extremo
ERRORES Y FALLOS NO INTENCIONADOS	**E.2**	Errores del administrador	Pérdida total o parcial del tiempo de ejecución de sus actividades, dependiendo de la gravedad del asunto.	Muy baja	2	16	4	Extremo
	E.23	Errores de mantenimiento / actualización de equipos(hardware)	Perjuicio a la mantenibilidad del sistema de información.	Muy baja	2	16	4	Extremo
	E.24	Caída del sistema por agotamiento de recursos	Saturación del sistema informático.	Muy baja	2	16	4	Extremo
	E.25	Perdida de equipos (Robo)	Recuperación de soportes reciclados o desechados.	Muy baja	2	16	4	Extremo
ATAQUES	**A.6**	Abuso de privilegios de acceso	Abuso de cada uno de los derechos otorgados.	Muy baja	2	16	4	Extremo

Tabla 52. Estimación del riesgo activo servidor de copias de seguridad de la información del ITFIP. (Continuación)

	A.7	Uso no previsto	Implementación de recursos (económicos y de tiempo) en actividades no relacionadas.	Muy baja	2	16	4	Extremo
	A.11	Acceso no autorizado	Uso ilícito del hardware	Muy baja	2	16	4	Extremo
	A.23	Manipulación de los equipos	Sabotaje del hardware y software conteniente.	Muy baja	2	16	4	Extremo
	A.24	Denegación de servicio	Saturación del sistema de información.	Muy baja	2	16	4	Extremo
	A.25	Robo	Robo de porte de la información, puede esta ser física o digital.	Muy baja	2	16	4	Extremo
	A.26	Ataque destructivo	Destrucción de los contenedores de la información, en recipientes físicos y lógicos.	Muy baja	2	16	4	Extremo

Fuente: Autoría propia

Tabla 53. Estimación del riesgo activo computador iMac Apple (3 equipos)

ACTIVO TI	**COMPUTADOR IMAC APPLE (3 EQUIPOS)**						
ADMINISTRADOR	PIMIENTO CARDENAS WILSON MAURICIO						
DEGRADACIÓN	50%						
IMPACTO	5						
TIPO DE ACTIVO	HARDWARE						
Tipo	**ID**	**Amenaza**	**Exposición/Vulnerabilidad**	**RIESGO ACTUAL**			
						2.95	Tolerable

Tabla 53. Estimación del riesgo activo computador iMac Apple (3 equipos). (Continuación)

				Frecuencia (F)		R	NR	
DESASTRES NATURALES	**N.1**	Fuego	No existe sistema de alarma contra incendios. Se posee un solo extintor de solkaflam (clase c) recomendados para incendios en lugares donde se encuentren equipos eléctricos.	Muy baja	2	10	3	Intolerable
	N.2	Daños por agua	La infraestructura está expuesta a goteras, cuenta con averías en el techo en donde el agua de las lluvias	Muy baja	2	10	3	Intolerable
	N.*	Desastres naturales	La oficina de la dependencia de sistemas se encuentra en zona baja de riesgo de desastre natural de origen volcánico debido a su cercanía con el volcán nevado del Tolima.	Raro	1	5	2	Tolerable
DE ORIGEN INDUSTRIAL	**I.1**	Fuego	No existe sistema de alarma contra incendios. Se posee un solo extintor de solkaflam (clase c) recomendados para incendios en lugares donde se encuentren equipos eléctricos.	Muy baja	2	10	3	Intolerable
	I.2	Daños por agua	La concentración del líquido sobrante por parte del aire	Muy baja	2	10	3	Intolerable

Tabla 53. Estimación del riesgo activo computador iMac Apple (3 equipos). (Continuación)

			acondicionado causaría daños en los equipos.					
	I.*	Desastres industriales	No hay exposición o vulnerabilidad, por parte de esta amenaza.	Muy baja	2	10	3	Intolerable
	I.3	Contaminación mecánica	No hay exposición o vulnerabilidad, por parte de esta amenaza.	Muy baja	2	10	3	Intolerable
	I.4	Contaminación electromagnética	No hay exposición o vulnerabilidad, por parte de esta amenaza.	Muy baja	2	10	3	Intolerable
	I.5	Avería de origen físico o lógico	La manipulación por parte de cada uno de los componentes encontrados en la dependencia, como también por defectos de los componentes desde fabrica	Muy baja	2	10	3	Intolerable
	I.6	Corte del suministro eléctrico	Amenaza debida a factores externos, a clemencias de tipo naturales como lluvias u otros.	Muy baja	2	10	3	Intolerable
	I.7	Condiciones inadecuadas de temperatura o humedad	No se cuenta con una infraestructura adecuada para soportar los defectos del sistema de refrigeración.	Muy baja	2	10	3	Intolerable
	I.11	Emanaciones electromagnéticas	No hay exposición o vulnerabilidad, por parte de esta amenaza.	Muy baja	2	10	3	Intolerable

Tabla 53. Estimación del riesgo activo computador iMac Apple (3 equipos). (Continuación)

ERRORES Y FALLOS NO INTENCIONADOS	**E.2**	Errores del administrador	Pérdida total o parcial del tiempo de ejecución de sus actividades, dependiendo de la gravedad del asunto.	Muy baja	2	10	3	Intolerable
	E.23	Errores de mantenimiento / actualización de equipos(hardware)	Perjuicio a la mantenibilidad del sistema de información.	Muy baja	2	10	3	Intolerable
	E.24	Caída del sistema por agotamiento de recursos	Saturación del sistema informático.	Muy baja	2	10	3	Intolerable
	E.25	Perdida de equipos (Robo)	Recuperación de soportes reciclados o desechados.	Muy baja	2	10	3	Intolerable
ATAQUES INTENCIONADOS	**A.6**	Abuso de privilegios de acceso	Abuso de cada uno de los derechos otorgados.	Muy baja	2	10	3	Intolerable
	A.7	Uso no previsto	Implementación de recursos (económicos y de tiempo) en actividades no relacionadas.	Muy baja	2	10	3	Intolerable
	A.11	Acceso no autorizado	Uso ilícito del hardware	Muy baja	2	10	3	Intolerable
	A.23	Manipulación de los equipos	Sabotaje del hardware y software conteniente.	Muy baja	2	10	3	Intolerable

Tabla 53. Estimación del riesgo activo computador iMac Apple (3 equipos). (Continuación)

	A.24	Denegación de servicio	Saturación del sistema de información.	Muy baja	2	10	3	Intolerable
	A.25	Robo	Robo de porte de la información, puede esta ser física o digital.	Muy baja	2	10	3	Intolerable
	A.26	Ataque destructivo	Destrucción de los contenedores de la información, en recipientes físicos y lógicos.	Muy baja	2	10	3	Intolerable

Fuente: Autoría propia

Tabla 54. Estimación del riesgo activo computadores hp all-one pro (18 equipos)

ACTIVO TI	**COMPUTADORES HP ALL-ONE PRO (18 EQUIPOS)**							
ADMINISTRADOR	PIMIENTO CARDENAS WILSON MAURICIO							
DEGRADACIÓN	30%							
IMPACTO	3							
TIPO DE ACTIVO	HARDWARE							
Tipo	**ID**	**Amenaza**	**Exposición/Vulnerabilidad**	**RIESGO ACTUAL**				
							2	Tolerable
				Frecuencia (F)		**R**	**NR**	
DESASTRES NATURALES	**N.1**	Fuego	No existe sistema de alarma contra incendios. Se posee un solo extintor de solkaflam (clase c) recomendados para incendios en lugares donde se encuentren equipos eléctricos.	Muy baja	2	6	2	Tolerable

Tabla 54. Estimación del riesgo activo computadores hp all-one pro (18 equipos). (Continuación)

	N.2	Daños por agua	La infraestructura está expuesta a goteras, cuenta con averías en el techo en donde el agua de las lluvias	Muy baja	2	6	2	Tolerable
	N.*	Desastres naturales	La oficina de la dependencia de sistemas se encuentra en zona baja de riesgo de desastre natural de origen volcánico debido a su cercanía con el volcán nevado del Tolima.	Raro	1	3	2	Tolerable
DE ORIGEN INDUSTRIAL	**I.1**	Fuego	No existe sistema de alarma contra incendios. Se posee un solo extintor de solkaflam (clase c) recomendados para incendios en lugares donde se encuentren equipos eléctricos.	Muy baja	2	6	2	Tolerable
	I.2	Daños por agua	La concentración del líquido sobrante por parte del aire acondicionado causaría daños en los equipos.	Muy baja	2	6	2	Tolerable
	I.*	Desastres industriales	No hay exposición o vulnerabilidad, por parte de esta amenaza.	Muy baja	2	6	2	Tolerable
	I.3	Contaminación mecánica	No hay exposición o vulnerabilidad, por parte de esta amenaza.	Muy baja	2	6	2	Tolerable
	I.4	Contaminación electromagnética	No hay exposición o vulnerabilidad, por parte de esta amenaza.	Muy baja	2	6	2	Tolerable

Tabla 54. Estimación del riesgo activo computadores hp all-one pro (18 equipos). (Continuación)

	I.5	Avería de origen físico o lógico	La manipulación por parte de cada uno de los componentes encontrados en la dependencia, como también por defectos de los componentes desde fabrica	Muy baja	2	6	2	Tolerable
	I.6	Corte del suministro eléctrico	Amenaza debida a factores externos, a clemencias de tipo naturales como lluvias u otros.	Muy baja	2	6	2	Tolerable
	I.7	Condiciones inadecuadas de temperatura o humedad	No se cuenta con una infraestructura adecuada para soportar los defectos del sistema de refrigeración.	Muy baja	2	6	2	Tolerable
	I.11	Emanaciones electromagnéticas	No hay exposición o vulnerabilidad, por parte de esta amenaza.	Muy baja	2	6	2	Tolerable
ERRORES Y FALLOS NO INTENCIONADOS	**E.2**	Errores del administrador	Pérdida total o parcial del tiempo de ejecución de sus actividades, dependiendo de la gravedad del asunto.	Muy baja	2	6	2	Tolerable
	E.23	Errores de mantenimiento / actualización de equipos(hardware)	Perjuicio a la mantenibilidad del sistema de información.	Muy baja	2	6	2	Tolerable

Tabla 54. Estimación del riesgo activo computadores hp all-one pro (18 equipos). (Continuación)

	E.24	Caída del sistema por agotamiento de recursos	Saturación del sistema informático.	Muy baja	2	6	2	Tolerable
	E.25	Perdida de equipos (Robo)	Recuperación de soportes reciclados o desechados.	Muy baja	2	6	2	Tolerable
ATAQUES INTENCIONADOS	**A.6**	Abuso de privilegios de acceso	Abuso de cada uno de los derechos otorgados.	Muy baja	2	6	2	Tolerable
	A.7	Uso no previsto	Implementación de recursos (económicos y de tiempo) en actividades no relacionadas.	Muy baja	2	6	2	Tolerable
	A.11	Acceso no autorizado	Uso ilícito del hardware	Muy baja	2	6	2	Tolerable
	A.23	Manipulación de los equipos	Sabotaje del hardware y software conteniente.	Muy baja	2	6	2	Tolerable
	A.24	Denegación de servicio	Saturación del sistema de información.	Muy baja	2	6	2	Tolerable
	A.25	Robo	Robo de porte de la información, puede esta ser física o digital.	Muy baja	2	6	2	Tolerable
	A.26	Ataque destructivo	Destrucción de los contenedores de la información, en recipientes físicos y lógicos.	Muy baja	2	6	2	Tolerable

Fuente: Autoría propia

Tabla 55. Estimación del riesgo activo portátil Toshiba (16 equipos)

ACTIVO TI	**PORTÁTIL TOSHIBA (16 EQUIPOS)**
ADMINISTRADOR	PIMIENTO CARDENAS WILSON MAURICIO
DEGRADACIÓN	30%
IMPACTO	3
TIPO DE ACTIVO	HARDWARE

Tipo	ID	Amenaza	Exposición/Vulnerabilidad	RIESGO ACTUAL				
							2	Tolerable
				Frecuencia (F)		R	NR	
DESASTRES NATURALES	**N.1**	Fuego	No existe sistema de alarma contra incendios. Se posee un solo extintor de solkaflam (clase c) recomendados para incendios en lugares donde se encuentren equipos eléctricos.	Muy baja	2	6	2	Tolerable
	N.2	Daños por agua	La infraestructura está expuesta a goteras, cuenta con averías en el techo en donde el agua de las lluvias	Muy baja	2	6	2	Tolerable
	N.*	Desastres naturales	La oficina de la dependencia de sistemas se encuentra en zona baja de riesgo de desastre natural de origen volcánico debido a su cercanía con el volcán nevado del Tolima.	Raro	1	3	2	Tolerable

Tabla 55. Estimación del riesgo activo portátil Toshiba (16 equipos). (Continuación)

DE ORIGEN INDUSTRIAL	**I.1**	Fuego	No existe sistema de alarma contra incendios. Se posee un solo extintor de solkaflam (clase c) recomendados para incendios en lugares donde se encuentren equipos eléctricos.	Muy baja	2	6	2	Tolerable
	I.2	Daños por agua	La concentración del líquido sobrante por parte del aire acondicionado causaría daños en los equipos.	Muy baja	2	6	2	Tolerable
	I.*	Desastres industriales	No hay exposición o vulnerabilidad, por parte de esta amenaza.	Muy baja	2	6	2	Tolerable
	I.3	Contaminación mecánica	No hay exposición o vulnerabilidad, por parte de esta amenaza.	Muy baja	2	6	2	Tolerable
	I.4	Contaminación electromagnética	No hay exposición o vulnerabilidad, por parte de esta amenaza.	Muy baja	2	6	2	Tolerable
	I.5	Avería de origen físico o lógico	La manipulación por parte de cada uno de los componentes encontrados en la dependencia, como también por defectos de los componentes desde fabrica	Muy baja	2	6	2	Tolerable
	I.6	Corte del suministro eléctrico	Amenaza debida a factores externos, a clemencias de tipo naturales como lluvias u otros.	Muy baja	2	6	2	Tolerable

Tabla 55. Estimación del riesgo activo portátil Toshiba (16 equipos). (Continuación)

	I.7	Condiciones inadecuadas de temperatura o humedad	No se cuenta con una infraestructura adecuada para soportar los defectos del sistema de refrigeración.	Muy baja	2	6	2	Tolerable
	I.11	Emanaciones electromagnéticas	No hay exposición o vulnerabilidad, por parte de esta amenaza.	Muy baja	2	6	2	Tolerable
ERRORES Y FALLOS NO INTENCIONADOS	**E.2**	Errores del administrador	Pérdida total o parcial del tiempo de ejecución de sus actividades, dependiendo de la gravedad del asunto.	Muy baja	2	6	2	Tolerable
	E.23	Errores de mantenimiento / actualización de equipos(hardware)	Perjuicio a la mantenibilidad del sistema de información.	Muy baja	2	6	2	Tolerable
	E.24	Caída del sistema por agotamiento de recursos	Saturación del sistema informático.	Muy baja	2	6	2	Tolerable
	E.25	Perdida de equipos (Robo)	Recuperación de soportes reciclados o desechados.	Muy baja	2	6	2	Tolerable
ATAQUES	**A.6**	Abuso de privilegios de acceso	Abuso de cada uno de los derechos otorgados.	Muy baja	2	6	2	Tolerable

Tabla 55. Estimación del riesgo activo portátil Toshiba (16 equipos). (Continuación)

	A.7	Uso no previsto	Implementación de recursos (económicos y de tiempo) en actividades no relacionadas.	Muy baja	2	6	2	Tolerable
	A.11	Acceso no autorizado	Uso ilícito del hardware	Muy baja	2	6	2	Tolerable
	A.23	Manipulación de los equipos	Sabotaje del hardware y software conteniente.	Muy baja	2	6	2	Tolerable
	A.24	Denegación de servicio	Saturación del sistema de información.	Muy baja	2	6	2	Tolerable
	A.25	Robo	Robo de porte de la información, puede esta ser física o digital.	Muy baja	2	6	2	Tolerable
	A.26	Ataque destructivo	Destrucción de los contenedores de la información, en recipientes físicos y lógicos.	Muy baja	2	6	2	Tolerable

Fuente: Autoría propia

Tabla 56. Estimación del riesgo activo Tablet negra 9" (1 equipo)

ACTIVO TI	**TABLET NEGRA 9" (1 EQUIPO)**						
ADMINISTRADOR	PIMIENTO CARDENAS WILSON MAURICIO						
DEGRADACIÓN	20%						
IMPACTO	2						
TIPO DE ACTIVO	HARDWARE						
Tipo	**ID**	**Amenaza**	**Exposición/Vulnerabilidad**	**RIESGO ACTUAL**			
						1.95	Aceptable

Tabla 56. Estimación del riesgo activo Tablet negra 9” (1 equipo). (Continuación)

				Frecuencia (F)		R	NR	
DESASTRES NATURALES	**N.1**	Fuego	No existe sistema de alarma contra incendios. Se posee un solo extintor de solkaflam (clase c) recomendados para incendios en lugares donde se encuentren equipos eléctricos.	Muy baja	2	4	2	Tolerable
	N.2	Daños por agua	La infraestructura está expuesta a goteras, cuenta con averías en el techo en donde el agua de las lluvias	Muy baja	2	4	2	Tolerable
	N.*	Desastres naturales	La oficina de la dependencia de sistemas se encuentra en zona baja de riesgo de desastre natural de origen volcánico debido a su cercanía con el volcán nevado del Tolima.	Raro	1	2	1	Aceptable
DE ORIGEN INDUSTRIAL	**I.1**	Fuego	No existe sistema de alarma contra incendios. Se posee un solo extintor de solkaflam (clase c) recomendados para incendios en lugares donde se encuentren equipos eléctricos.	Muy baja	2	4	2	Tolerable
	I.2	Daños por agua	La concentración del líquido sobrante por parte del aire acondicionado causaría daños en los equipos.	Muy baja	2	4	2	Tolerable

Tabla 56. Estimación del riesgo activo Tablet negra 9" (1 equipo). (Continuación)

	I.*	Desastres industriales	No hay exposición o vulnerabilidad, por parte de esta amenaza.	Muy baja	2	4	2	Tolerable
	I.3	Contaminación mecánica	No hay exposición o vulnerabilidad, por parte de esta amenaza.	Muy baja	2	4	2	Tolerable
	I.4	Contaminación electromagnética	No hay exposición o vulnerabilidad, por parte de esta amenaza.	Muy baja	2	4	2	Tolerable
	I.5	Avería de origen físico o lógico	La manipulación por parte de cada uno de los componentes encontrados en la dependencia, como también por defectos de los componentes desde fabrica	Muy baja	2	4	2	Tolerable
	I.6	Corte del suministro eléctrico	Amenaza debida a factores externos, a clemencias de tipo naturales como lluvias u otros.	Muy baja	2	4	2	Tolerable
	I.7	Condiciones inadecuadas de temperatura o humedad	No se cuenta con una infraestructura adecuada para soportar los defectos del sistema de refrigeración.	Muy baja	2	4	2	Tolerable
	I.11	Emanaciones electromagnéticas	No hay exposición o vulnerabilidad, por parte de esta amenaza.	Muy baja	2	4	2	Tolerable

Tabla 56. Estimación del riesgo activo Tablet negra 9" (1 equipo). (Continuación)

ERRORES Y FALLOS NO INTENCIONADOS	**E.2**	Errores del administrador	Pérdida total o parcial del tiempo de ejecución de sus actividades, dependiendo de la gravedad del asunto.	Muy baja	2	4	2	Tolerable
	E.23	Errores de mantenimiento / actualización de equipos(hardware)	Perjuicio a la mantenibilidad del sistema de información.	Muy baja	2	4	2	Tolerable
	E.24	Caída del sistema por agotamiento de recursos	Saturación del sistema informático.	Muy baja	2	4	2	Tolerable
	E.25	Perdida de equipos (Robo)	Recuperación de soportes reciclados o desechados.	Muy baja	2	4	2	Tolerable
ATAQUES INTENCIONADOS	**A.6**	Abuso de privilegios de acceso	Abuso de cada uno de los derechos otorgados.	Muy baja	2	4	2	Tolerable
	A.7	Uso no previsto	Implementación de recursos (económicos y de tiempo) en actividades no relacionadas.	Muy baja	2	4	2	Tolerable
	A.11	Acceso no autorizado	Uso ilícito del hardware	Muy baja	2	4	2	Tolerable
	A.23	Manipulación de los equipos	Sabotaje del hardware y software conteniente.	Muy baja	2	4	2	Tolerable

Tabla 56. Estimación del riesgo activo Tablet negra 9" (1 equipo). (Continuación)

	A.24	Denegación de servicio	Saturación del sistema de información.	Muy baja	2	4	2	Tolerable
	A.25	Robo	Robo de porte de la información, puede esta ser física o digital.	Muy baja	2	4	2	Tolerable
	A.26	Ataque destructivo	Destrucción de los contenedores de la información, en recipientes físicos y lógicos.	Muy baja	2	4	2	Tolerable

Fuente: Autoría propia

Tabla 57. Estimación del riesgo activo computador iMac *Apple* (3 equipos)

ACTIVO TI	**COMPUTADOR IMAC APPLE (3 EQUIPOS)**							
ADMINISTRADOR	PIMIENTO CARDENAS WILSON MAURICIO							
DEGRADACIÓN	50%							
IMPACTO	5							
TIPO DE ACTIVO	HARDWARE							
Tipo	**ID**	**Amenaza**	**Exposición/Vulnerabilidad**	**RIESGO ACTUAL**				
							2.95	Tolerable
				Frecuencia (F)		**R**	**NR**	
DESASTRES NATURALES	**N.1**	Fuego	No existe sistema de alarma contra incendios. Se posee un solo extintor de solkaflam (clase c) recomendados para incendios en lugares donde se encuentren equipos eléctricos.	Muy baja	2	10	3	Intolerable

Tabla 57. Estimación del riesgo activo computador iMac *Apple* (3 equipos). (Continuación)

	N.2	Daños por agua	La infraestructura está expuesta a goteras, cuenta con averías en el techo en donde el agua de las lluvias	Muy baja	2	10	3	Intolerable
	N.*	Desastres naturales	La oficina de la dependencia de sistemas se encuentra en zona baja de riesgo de desastre natural de origen volcánico debido a su cercanía con el volcán nevado del Tolima.	Raro	1	5	2	Tolerable
DE ORIGEN INDUSTRIAL	**I.1**	Fuego	No existe sistema de alarma contra incendios. Se posee un solo extintor de solkaflam (clase c) recomendados para incendios en lugares donde se encuentren equipos eléctricos.	Muy baja	2	10	3	Intolerable
	I.2	Daños por agua	La concentración del líquido sobrante por parte del aire acondicionado causaría daños en los equipos.	Muy baja	2	10	3	Intolerable
	I.*	Desastres industriales	No hay exposición o vulnerabilidad, por parte de esta amenaza.	Muy baja	2	10	3	Intolerable
	I.3	Contaminación mecánica	No hay exposición o vulnerabilidad, por parte de esta amenaza.	Muy baja	2	10	3	Intolerable

Tabla 57. Estimación del riesgo activo computador iMac *Apple* (3 equipos). (Continuación)

	I.4	Contaminación electromagnética	No hay exposición o vulnerabilidad, por parte de esta amenaza.	Muy baja	2	10	3	Intolerable
	I.5	Avería de origen físico o lógico	La manipulación por parte de cada uno de los componentes encontrados en la dependencia, como también por defectos de los componentes desde fabrica	Muy baja	2	10	3	Intolerable
	I.6	Corte del suministro eléctrico	Amenaza debida a factores externos, a clemencias de tipo naturales como lluvias u otros.	Muy baja	2	10	3	Intolerable
	I.7	Condiciones inadecuadas de temperatura o humedad	No se cuenta con una infraestructura adecuada para soportar los defectos del sistema de refrigeración.	Muy baja	2	10	3	Intolerable
	I.11	Emanaciones electromagnéticas	No hay exposición o vulnerabilidad, por parte de esta amenaza.	Muy baja	2	10	3	Intolerable
ERRORES Y FALLOS NO INTENCIONADOS	**E.2**	Errores del administrador	Pérdida total o parcial del tiempo de ejecución de sus actividades, dependiendo de la gravedad del asunto.	Muy baja	2	10	3	Intolerable
	E.23	Errores de mantenimiento /	Perjuicio a la mantenibilidad del sistema de información.	Muy baja	2	10	3	Intolerable

Tabla 57. Estimación del riesgo activo computador iMac *Apple* (3 equipos). (Continuación)

		actualización de equipos(hardware)						
	E.24	Caída del sistema por agotamiento de recursos	Saturación del sistema informático.	Muy baja	2	10	3	Intolerable
	E.25	Perdida de equipos (Robo)	Recuperación de soportes reciclados o desechados.	Muy baja	2	10	3	Intolerable
ATAQUES INTENCIONADOS	**A.6**	Abuso de privilegios de acceso	Abuso de cada uno de los derechos otorgados.	Muy baja	2	10	3	Intolerable
	A.7	Uso no previsto	Implementación de recursos (económicos y de tiempo) en actividades no relacionadas.	Muy baja	2	10	3	Intolerable
	A.11	Acceso no autorizado	Uso ilícito del hardware	Muy baja	2	10	3	Intolerable
	A.23	Manipulación de los equipos	Sabotaje del hardware y software conteniente.	Muy baja	2	10	3	Intolerable
	A.24	Denegación de servicio	Saturación del sistema de información.	Muy baja	2	10	3	Intolerable
	A.25	Robo	Robo de porte de la información, puede esta ser física o digital.	Muy baja	2	10	3	Intolerable

Tabla 57. Estimación del riesgo activo computador iMac *Apple* (3 equipos). (Continuación)

	A.26	Ataque destructivo	Destrucción de los contenedores de la información, en recipientes físicos y lógicos.	Muy baja	2	10	3	Intolerable

Fuente: Autoría propia

Tabla 58. Estimación del riesgo activo memoria USB

ACTIVO TI	**MEMORIA USB**
ADMINISTRADOR	PIMIENTO CARDENAS WILSON MAURICIO
DEGRADACIÓN	20%
IMPACTO	2
TIPO DE ACTIVO	HARDWARE

Tipo	ID	Amenaza	Exposición/Vulnerabilidad	RIESGO ACTUAL				
							1.95	Aceptable
				Frecuencia (F)		**R**	**NR**	
DESASTRES NATURALES	**N.1**	Fuego	No existe sistema de alarma contra incendios. Se posee un solo extintor de solkaflam (clase c) recomendados para incendios en lugares donde se encuentren equipos eléctricos.	Muy baja	2	4	2	Tolerable
	N.2	Daños por agua	La infraestructura está expuesta a goteras, cuenta con averías en el techo en donde el agua de las lluvias	Muy baja	2	4	2	Tolerable
	N.*	Desastres naturales	La oficina de la dependencia de sistemas se encuentra en zona baja de riesgo de desastre natural de	Raro	1	2	1	Aceptable

Tabla 58. Estimación del riesgo activo memoria USB. (Continuación)

			origen volcánico debido a su cercanía con el volcán nevado del Tolima.					
DE ORIGEN INDUSTRIAL	**I.1**	Fuego	No existe sistema de alarma contra incendios. Se posee un solo extintor de solkaflam (clase c) recomendados para incendios en lugares donde se encuentren equipos eléctricos.	Muy baja	2	4	2	Tolerable
	I.2	Daños por agua	La concentración del líquido sobrante por parte del aire acondicionado causaría daños en los equipos.	Muy baja	2	4	2	Tolerable
	I.*	Desastres industriales	No hay exposición o vulnerabilidad, por parte de esta amenaza.	Muy baja	2	4	2	Tolerable
	I.3	Contaminación mecánica	No hay exposición o vulnerabilidad, por parte de esta amenaza.	Muy baja	2	4	2	Tolerable
	I.4	Contaminación electromagnética	No hay exposición o vulnerabilidad, por parte de esta amenaza.	Muy baja	2	4	2	Tolerable
	I.5	Avería de origen físico o lógico	La manipulación por parte de cada uno de los componentes encontrados en la dependencia, como también por defectos de los componentes desde fabrica	Muy baja	2	4	2	Tolerable

Tabla 58. Estimación del riesgo activo memoria USB. (Continuación)

	I.6	Corte del suministro eléctrico	Amenaza debida a factores externos, a clemencias de tipo naturales como lluvias u otros.	Muy baja	2	4	2	Tolerable
	I.7	Condiciones inadecuadas de temperatura o humedad	No se cuenta con una infraestructura adecuada para soportar los defectos del sistema de refrigeración.	Muy baja	2	4	2	Tolerable
	I.11	Emanaciones electromagnéticas	No hay exposición o vulnerabilidad, por parte de esta amenaza.	Muy baja	2	4	2	Tolerable
ERRORES Y FALLOS NO INTENCIONADOS	**E.2**	Errores del administrador	Pérdida total o parcial del tiempo de ejecución de sus actividades, dependiendo de la gravedad del asunto.	Muy baja	2	4	2	Tolerable
	E.23	Errores de mantenimiento / actualización de equipos(hardware)	Perjuicio a la mantenibilidad del sistema de información.	Muy baja	2	4	2	Tolerable
	E.24	Caída del sistema por agotamiento de recursos	Saturación del sistema informático.	Muy baja	2	4	2	Tolerable
	E.25	Perdida de equipos (Robo)	Recuperación de soportes reciclados o desechados.	Muy baja	2	4	2	Tolerable

Tabla 58. Estimación del riesgo activo memoria USB. (Continuación)

ATAQUES INTENCIONADOS	**A.6**	Abuso de privilegios de acceso	Abuso de cada uno de los derechos otorgados.	Muy baja	2	4	2	Tolerable
	A.7	Uso no previsto	Implementación de recursos (económicos y de tiempo) en actividades no relacionadas.	Muy baja	2	4	2	Tolerable
	A.11	Acceso no autorizado	Uso ilícito del hardware	Muy baja	2	4	2	Tolerable
	A.23	Manipulación de los equipos	Sabotaje del hardware y software conteniente.	Muy baja	2	4	2	Tolerable
	A.24	Denegación de servicio	Saturación del sistema de información.	Muy baja	2	4	2	Tolerable
	A.25	Robo	Robo de porte de la información, puede esta ser física o digital.	Muy baja	2	4	2	Tolerable
	A.26	Ataque destructivo	Destrucción de los contenedores de la información, en recipientes físicos y lógicos.	Muy baja	2	4	2	Tolerable

Fuente: Autoría propia

Tabla 59. Estimación del riesgo activo discos duros

ACTIVO TI	**DISCOS DUROS**
ADMINISTRADOR	PIMIENTO CARDENAS WILSON MAURICIO
DEGRADACIÓN	35%
IMPACTO	3

Tabla 59. Estimación del riesgo activo discos duros. (Continuación)

TIPO DE ACTIVO		HARDWARE						
Tipo	**ID**	**Amenaza**	**Exposición/Vulnerabilidad**	**RIESGO ACTUAL**				
							2	Tolerable
				Frecuencia (F)		**R**	**NR**	
DESASTRES NATURALES	**N.1**	Fuego	No existe sistema de alarma contra incendios. Se posee un solo extintor de solkaflam (clase c) recomendados para incendios en lugares donde se encuentren equipos eléctricos.	Muy baja	2	6	2	Tolerable
	N.2	Daños por agua	La infraestructura está expuesta a goteras, cuenta con averías en el techo en donde el agua de las lluvias	Muy baja	2	6	2	Tolerable
	N.*	Desastres naturales	La oficina de la dependencia de sistemas se encuentra en zona baja de riesgo de desastre natural de origen volcánico debido a su cercanía con el volcán nevado del Tolima.	Raro	1	3	2	Tolerable
DE ORIGEN INDUSTRIAL	**I.1**	Fuego	No existe sistema de alarma contra incendios. Se posee un solo extintor de solkaflam (clase c) recomendados para incendios en lugares donde se encuentren equipos eléctricos.	Muy baja	2	6	2	Tolerable

Tabla 59. Estimación del riesgo activo discos duros. (Continuación)

	I.2	Daños por agua	La concentración del líquido sobrante por parte del aire acondicionado causaría daños en los equipos.	Muy baja	2	6	2	Tolerable
	I.*	Desastres industriales	No hay exposición o vulnerabilidad, por parte de esta amenaza.	Muy baja	2	6	2	Tolerable
	I.3	Contaminación mecánica	No hay exposición o vulnerabilidad, por parte de esta amenaza.	Muy baja	2	6	2	Tolerable
	I.4	Contaminación electromagnética	No hay exposición o vulnerabilidad, por parte de esta amenaza.	Muy baja	2	6	2	Tolerable
	I.5	Avería de origen físico o lógico	La manipulación por parte de cada uno de los componentes encontrados en la dependencia, como también por defectos de los componentes desde fabrica	Muy baja	2	6	2	Tolerable
	I.6	Corte del suministro eléctrico	Amenaza debida a factores externos, a clemencias de tipo naturales como lluvias u otros.	Muy baja	2	6	2	Tolerable
	I.7	Condiciones inadecuadas de temperatura o humedad	No se cuenta con una infraestructura adecuada para soportar los defectos del sistema de refrigeración.	Muy baja	2	6	2	Tolerable

Tabla 59. Estimación del riesgo activo discos duros. (Continuación)

	I.11	Emanaciones electromagnéticas	No hay exposición o vulnerabilidad, por parte de esta amenaza.	Muy baja	2	6	2	Tolerable
ERRORES Y FALLOS NO INTENCIONADOS	**E.2**	Errores del administrador	Pérdida total o parcial del tiempo de ejecución de sus actividades, dependiendo de la gravedad del asunto.	Muy baja	2	6	2	Tolerable
	E.23	Errores de mantenimiento / actualización de equipos(hardware)	Perjuicio a la mantenibilidad del sistema de información.	Muy baja	2	6	2	Tolerable
	E.24	Caída del sistema por agotamiento de recursos	Saturación del sistema informático.	Muy baja	2	6	2	Tolerable
	E.25	Perdida de equipos (Robo)	Recuperación de soportes reciclados o desechados.	Muy baja	2	6	2	Tolerable
ATAQUES INTENCIONADOS	**A.6**	Abuso de privilegios de acceso	Abuso de cada uno de los derechos otorgados.	Muy baja	2	6	2	Tolerable
	A.7	Uso no previsto	Implementación de recursos (económicos y de tiempo) en actividades no relacionadas.	Muy baja	2	6	2	Tolerable
	A.11	Acceso no autorizado	Uso ilícito del hardware	Muy baja	2	6	2	Tolerable

Tabla 59. Estimación del riesgo activo discos duros. (Continuación)

	A.23	Manipulación de los equipos	Sabotaje del hardware y software conteniente.	Muy baja	2	6	2	Tolerable
	A.24	Denegación de servicio	Saturación del sistema de información.	Muy baja	2	6	2	Tolerable
	A.25	Robo	Robo de porte de la información, puede esta ser física o digital.	Muy baja	2	6	2	Tolerable
	A.26	Ataque destructivo	Destrucción de los contenedores de la información, en recipientes físicos y lógicos.	Muy baja	2	6	2	Tolerable

Fuente: Autoría propia

Tabla 60. Estimación del riesgo activo discos duros externos

ACTIVO TI	**DISCOS DUROS EXTERNOS**							
ADMINISTRADOR	PIMIENTO CARDENAS WILSON MAURICIO							
DEGRADACIÓN	45%							
IMPACTO	3							
TIPO DE ACTIVO	HARDWARE							
Tipo	**ID**	**Amenaza**	**Exposición/Vulnerabilidad**	**RIESGO ACTUAL**				
							2	Tolerable
				Frecuencia (F)		**R**	**NR**	
DESASTRES	**N.1**	Fuego	No existe sistema de alarma contra incendios. Se posee un solo extintor de solkaflam (clase c) recomendados para	Muy baja	2	6	2	Tolerable

Tabla 60. Estimación del riesgo activo discos duros externos. (Continuación)

			incendios en lugares donde se encuentren equipos eléctricos.					
	N.2	Daños por agua	La infraestructura está expuesta a goteras, cuenta con averías en el techo en donde el agua de las lluvias	Muy baja	2	6	2	Tolerable
	N.*	Desastres naturales	La oficina de la dependencia de sistemas se encuentra en zona baja de riesgo de desastre natural de origen volcánico debido a su cercanía con el volcán nevado del Tolima.	Raro	1	3	2	Tolerable
DE ORIGEN INDUSTRIAL	**I.1**	Fuego	No existe sistema de alarma contra incendios. Se posee un solo extintor de solkaflam (clase c) recomendados para incendios en lugares donde se encuentren equipos eléctricos.	Muy baja	2	6	2	Tolerable
	I.2	Daños por agua	La concentración del líquido sobrante por parte del aire acondicionado causaría daños en los equipos.	Muy baja	2	6	2	Tolerable
	I.*	Desastres industriales	No hay exposición o vulnerabilidad, por parte de esta amenaza.	Muy baja	2	6	2	Tolerable
	I.3	Contaminación mecánica	No hay exposición o vulnerabilidad, por parte de esta amenaza.	Muy baja	2	6	2	Tolerable

Tabla 60. Estimación del riesgo activo discos duros externos. (Continuación)

	I.4	Contaminación electromagnética	No hay exposición o vulnerabilidad, por parte de esta amenaza.	Muy baja	2	6	2	Tolerable
	I.5	Avería de origen físico o lógico	La manipulación por parte de cada uno de los componentes encontrados en la dependencia, como también por defectos de los componentes desde fabrica	Muy baja	2	6	2	Tolerable
	I.6	Corte del suministro eléctrico	Amenaza debida a factores externos, a clemencias de tipo naturales como lluvias u otros.	Muy baja	2	6	2	Tolerable
	I.7	Condiciones inadecuadas de temperatura o humedad	No se cuenta con una infraestructura adecuada para soportar los defectos del sistema de refrigeración.	Muy baja	2	6	2	Tolerable
	I.11	Emanaciones electromagnéticas	No hay exposición o vulnerabilidad, por parte de esta amenaza.	Muy baja	2	6	2	Tolerable
ERRORES Y FALLOS NO INTENCIONADOS	**E.2**	Errores del administrador	Pérdida total o parcial del tiempo de ejecución de sus actividades, dependiendo de la gravedad del asunto.	Muy baja	2	6	2	Tolerable
	E.23	Errores de mantenimiento / actualización de equipos(hardware)	Perjuicio a la mantenibilidad del sistema de información.	Muy baja	2	6	2	Tolerable

Tabla 60. Estimación del riesgo activo discos duros externos. (Continuación)

	E.24	Caída del sistema por agotamiento de recursos	Saturación del sistema informático.	Muy baja	2	6	2	Tolerable
	E.25	Perdida de equipos (Robo)	Recuperación de soportes reciclados o desechados.	Muy baja	2	6	2	Tolerable
ATAQUES INTENCIONADOS	**A.6**	Abuso de privilegios de acceso	Abuso de cada uno de los derechos otorgados.	Muy baja	2	6	2	Tolerable
	A.7	Uso no previsto	Implementación de recursos (económicos y de tiempo) en actividades no relacionadas.	Muy baja	2	6	2	Tolerable
	A.11	Acceso no autorizado	Uso ilícito del hardware	Muy baja	2	6	2	Tolerable
	A.23	Manipulación de los equipos	Sabotaje del hardware y software conteniente.	Muy baja	2	6	2	Tolerable
	A.24	Denegación de servicio	Saturación del sistema de información.	Muy baja	2	6	2	Tolerable
	A.25	Robo	Robo de porte de la información, puede esta ser física o digital.	Muy baja	2	6	2	Tolerable
	A.26	Ataque destructivo	Destrucción de los contenedores de la información, en recipientes físicos y lógicos.	Muy baja	2	6	2	Tolerable

Fuente: Autoría propia

Tabla 61. Estimación del riesgo activo switch ALCATEL LUCEN 9553

ACTIVO TI	**SWITCH ALCATEL LUCEN 9553**
ADMINISTRADOR	PIMIENTO CARDENAS WILSON MAURICIO
DEGRADACIÓN	60%
IMPACTO	5
TIPO DE ACTIVO	HARDWARE

Tipo	ID	Amenaza	Exposición/Vulnerabilidad	RIESGO ACTUAL				
							3.04	Intolerable
				Frecuencia (F)		**R**	**NR**	
DESASTRES NATURALES	**N.1**	Fuego	No existe sistema de alarma contra incendios. Se posee un solo extintor de solkaflam (clase c) recomendados para incendios en lugares donde se encuentren equipos eléctricos.	Muy baja	2	10	3	Intolerable
	N.2	Daños por agua	La infraestructura está expuesta a goteras, cuenta con averías en el techo en donde el agua de las lluvias	Muy baja	2	10	3	Intolerable
	N.*	Desastres naturales	La oficina de la dependencia de sistemas se encuentra en zona baja de riesgo de desastre natural de origen volcánico debido a su cercanía con el volcán nevado del Tolima.	Raro	1	5	2	Tolerable

Tabla 61. Estimación del riesgo activo switch ALCATEL LUCEN 9553. (Continuación)

DE ORIGEN INDUSTRIAL	**I.1**	Fuego	No existe sistema de alarma contra incendios. Se posee un solo extintor de solkaflam (clase c) recomendados para incendios en lugares donde se encuentren equipos eléctricos.	Muy baja	2	10	3	Intolerable
	I.2	Daños por agua	La concentración del líquido sobrante por parte del aire acondicionado causaría daños en los equipos.	Muy baja	2	10	3	Intolerable
	I.*	Desastres industriales	No hay exposición o vulnerabilidad, por parte de esta amenaza.	Muy baja	2	10	3	Intolerable
	I.3	Contaminación mecánica	No hay exposición o vulnerabilidad, por parte de esta amenaza.	Muy baja	2	10	3	Intolerable
	I.4	Contaminación electromagnética	No hay exposición o vulnerabilidad, por parte de esta amenaza.	Muy baja	2	10	3	Intolerable
	I.5	Avería de origen físico o lógico	La manipulación por parte de cada uno de los componentes encontrados en la dependencia, como también por defectos de los componentes desde fabrica	Muy baja	2	10	3	Intolerable

Tabla 61. Estimación del riesgo activo switch ALCATEL LUCEN 9553. (Continuación)

	I.6	Corte del suministro eléctrico	Amenaza debida a factores externos, a clemencias de tipo naturales como lluvias u otros.	Muy baja	2	10	3	Intolerable
	I.7	Condiciones inadecuadas de temperatura o humedad	No se cuenta con una infraestructura adecuada para soportar los defectos del sistema de refrigeración.	Muy baja	2	10	3	Intolerable
	I.11	Emanaciones electromagnéticas	No hay exposición o vulnerabilidad, por parte de esta amenaza.	Muy baja	2	10	3	Intolerable
ERRORES Y FALLOS NO INTENCIONADOS	**E.2**	Errores del administrador	Pérdida total o parcial del tiempo de ejecución de sus actividades, dependiendo de la gravedad del asunto.	Muy baja	2	10	3	Intolerable
	E.23	Errores de mantenimiento / actualización de equipos(hardware)	Perjuicio a la mantenibilidad del sistema de información.	Muy baja	2	10	3	Intolerable
	E.24	Caída del sistema por agotamiento de recursos	Saturación del sistema informático.	Muy baja	2	10	3	Intolerable
	E.25	Perdida de equipos (Robo)	Recuperación de soportes reciclados o desechados.	Muy baja	2	10	3	Intolerable

Tabla 61. Estimación del riesgo activo switch ALCATEL LUCEN 9553. (Continuación)

ATAQUES INTENCIONADOS	**A.6**	Abuso de privilegios de acceso	Abuso de cada uno de los derechos otorgados.	Muy baja	2	10	3	Intolerable
	A.7	Uso no previsto	Implementación de recursos (económicos y de tiempo) en actividades no relacionadas.	Muy baja	2	10	3	Intolerable
	A.11	Acceso no autorizado	Uso ilícito del hardware	Muy baja	2	10	3	Intolerable
	A.23	Manipulación de los equipos	Sabotaje del hardware y software conteniente.	Muy baja	2	10	3	Intolerable
	A.24	Denegación de servicio	Saturación del sistema de información.	Muy baja	2	10	3	Intolerable
	A.25	Robo	Robo de porte de la información, puede esta ser física o digital.	Muy baja	2	10	3	Intolerable
	A.26	Ataque destructivo	Destrucción de los contenedores de la información, en recipientes físicos y lógicos.	Muy baja	2	10	3	Intolerable

Fuente: Autoría propia

Tabla 62. Estimación del riesgo activo switch 24 10/100/1000 base t c

ACTIVO TI	**SWITCH 24 10/100/1000 BASE T C**
ADMINISTRADOR	PIMIENTO CARDENAS WILSON MAURICIO
DEGRADACIÓN	60%
IMPACTO	5

Tabla 62. Estimación del riesgo activo switch 24 10/100/1000 base t c. (Continuación)

TIPO DE ACTIVO		HARDWARE						
Tipo	**ID**	**Amenaza**	**Exposición/Vulnerabilidad**	**RIESGO ACTUAL**				
							3.04	Intolerable
				Frecuencia (F)		**R**	**NR**	
DESASTRES NATURALES	**N.1**	Fuego	No existe sistema de alarma contra incendios. Se posee un solo extintor de solkaflam (clase c) recomendados para incendios en lugares donde se encuentren equipos eléctricos.	Muy baja	2	10	3	Intolerable
	N.2	Daños por agua	La infraestructura está expuesta a goteras, cuenta con averías en el techo en donde el agua de las lluvias	Muy baja	2	10	3	Intolerable
	N.*	Desastres naturales	La oficina de la dependencia de sistemas se encuentra en zona baja de riesgo de desastre natural de origen volcánico debido a su cercanía con el volcán nevado del Tolima.	Raro	1	5	2	Tolerable
DE ORIGEN INDUST	**I.1**	Fuego	No existe sistema de alarma contra incendios. Se posee un solo extintor de solkaflam (clase c) recomendados para incendios en	Muy baja	2	10	3	Intolerable

Tabla 62. Estimación del riesgo activo switch 24 10/100/1000 base t c. (Continuación)

			lugares donde se encuentren equipos eléctricos.					
	I.2	Daños por agua	La concentración del líquido sobrante por parte del aire acondicionado causaría daños en los equipos.	Muy baja	2	10	3	Intolerable
	I.*	Desastres industriales	No hay exposición o vulnerabilidad, por parte de esta amenaza.	Muy baja	2	10	3	Intolerable
	I.3	Contaminación mecánica	No hay exposición o vulnerabilidad, por parte de esta amenaza.	Muy baja	2	10	3	Intolerable
	I.4	Contaminación electromagnética	No hay exposición o vulnerabilidad, por parte de esta amenaza.	Muy baja	2	10	3	Intolerable
	I.5	Avería de origen físico o lógico	La manipulación por parte de cada uno de los componentes encontrados en la dependencia, como también por defectos de los componentes desde fabrica	Muy baja	2	10	3	Intolerable
	I.6	Corte del suministro eléctrico	Amenaza debida a factores externos, a clemencias de tipo naturales como lluvias u otros.	Muy baja	2	10	3	Intolerable

Tabla 62. Estimación del riesgo activo switch 24 10/100/1000 base t c. (Continuación)

	I.7	Condiciones inadecuadas de temperatura o humedad	No se cuenta con una infraestructura adecuada para soportar los defectos del sistema de refrigeración.	Muy baja	2	10	3	Intolerable
	I.11	Emanaciones electromagnéticas	No hay exposición o vulnerabilidad, por parte de esta amenaza.	Muy baja	2	10	3	Intolerable
ERRORES Y FALLOS NO INTENCIONADOS	**E.2**	Errores del administrador	Pérdida total o parcial del tiempo de ejecución de sus actividades, dependiendo de la gravedad del asunto.	Muy baja	2	10	3	Intolerable
	E.23	Errores de mantenimiento / actualización de equipos(hardware)	Perjuicio a la mantenibilidad del sistema de información.	Muy baja	2	10	3	Intolerable
	E.24	Caída del sistema por agotamiento de recursos	Saturación del sistema informático.	Muy baja	2	10	3	Intolerable
	E.25	Perdida de equipos (Robo)	Recuperación de soportes reciclados o desechados.	Muy baja	2	10	3	Intolerable
ATAQUES	**A.6**	Abuso de privilegios de acceso	Abuso de cada uno de los derechos otorgados.	Muy baja	2	10	3	Intolerable

Tabla 62. Estimación del riesgo activo switch 24 10/100/1000 base t c. (Continuación)

	A.7	Uso no previsto	Implementación de recursos (económicos y de tiempo) en actividades no relacionadas.	Muy baja	2	10	3	Intolerable
	A.11	Acceso no autorizado	Uso ilícito del hardware	Muy baja	2	10	3	Intolerable
	A.23	Manipulación de los equipos	Sabotaje del hardware y software conteniente.	Muy baja	2	10	3	Intolerable
	A.24	Denegación de servicio	Saturación del sistema de información.	Muy baja	2	10	3	Intolerable
	A.25	Robo	Robo de porte de la información, puede esta ser física o digital.	Muy baja	2	10	3	Intolerable
	A.26	Ataque destructivo	Destrucción de los contenedores de la información, en recipientes físicos y lógicos.	Muy baja	2	10	3	Intolerable

Fuente: Autoría propia

ANEXO 6

CONTENIDO

LISTA DE TABLAS

1. CONTINUACIÓN DE LA ESTIMACIÓN DE RIESGO DE CADA ACTIVO

Tabla 1. Estimación del riesgo activo switch 24/10/100/1000 base t4s

ACTIVO TI	**SWITCH 24/10/100/1000 BASE T4S**
ADMINISTRADOR	PIMIENTO CARDENAS WILSON MAURICIO
DEGRADACIÓN	60%
IMPACTO	5
TIPO DE ACTIVO	HARDWARE

Tipo	ID	Amenaza	Exposición/Vulnerabilidad	RIESGO ACTUAL				
							3.04	Intolerable
				Frecuencia (F)		**R**	**NR**	
DESASTRES NATURALES	**N.1**	Fuego	No existe sistema de alarma contra incendios. Se posee un solo extintor de solkaflam (clase c) recomendados para incendios en lugares donde se encuentren equipos eléctricos.	Muy baja	2	10	3	Intolerable
	N.2	Daños por agua	La infraestructura está expuesta a goteras, cuenta con averías en el techo en donde el agua de las lluvias	Muy baja	2	10	3	Intolerable
	N.*	Desastres naturales	La oficina de la dependencia de sistemas se encuentra en zona baja de riesgo de desastre natural de origen volcánico debido a su cercanía con el volcán nevado del Tolima.	Raro	1	5	2	Tolerable

Tabla 1. Estimación del riesgo activo switch 24/10/100/1000 base t4s. (Continuación)

DE ORIGEN INDUSTRIAL	**I.1**	Fuego	No existe sistema de alarma contra incendios. Se posee un solo extintor de solkaflam (clase c) recomendados para incendios en lugares donde se encuentren equipos eléctricos.	Muy baja	2	10	3	Intolerable
	I.2	Daños por agua	La concentración del líquido sobrante por parte del aire acondicionado causaría daños en los equipos.	Muy baja	2	10	3	Intolerable
	I.*	Desastres industriales	No hay exposición o vulnerabilidad, por parte de esta amenaza.	Muy baja	2	10	3	Intolerable
	I.3	Contaminación mecánica	No hay exposición o vulnerabilidad, por parte de esta amenaza.	Muy baja	2	10	3	Intolerable
	I.4	Contaminación electromagnética	No hay exposición o vulnerabilidad, por parte de esta amenaza.	Muy baja	2	10	3	Intolerable
	I.5	Avería de origen físico o lógico	La manipulación por parte de cada uno de los componentes encontrados en la dependencia, como también por defectos de los componentes desde fabrica	Muy baja	2	10	3	Intolerable

Tabla 1. Estimación del riesgo activo switch 24/10/100/1000 base t4s. (Continuación)

	I.6	Corte del suministro eléctrico	Amenaza debida a factores externos, a clemencias de tipo naturales como lluvias u otros.	Muy baja	2	10	3	Intolerable
	I.7	Condiciones inadecuadas de temperatura o humedad	No se cuenta con una infraestructura adecuada para soportar los defectos del sistema de refrigeración.	Muy baja	2	10	3	Intolerable
	I.11	Emanaciones electromagnéticas	No hay exposición o vulnerabilidad, por parte de esta amenaza.	Muy baja	2	10	3	Intolerable
ERRORES Y FALLOS NO INTENCIONADOS	**E.2**	Errores del administrador	Pérdida total o parcial del tiempo de ejecución de sus actividades, dependiendo de la gravedad del asunto.	Muy baja	2	10	3	Intolerable
	E.23	Errores de mantenimiento / actualización de equipos(hardware)	Perjuicio a la mantenibilidad del sistema de información.	Muy baja	2	10	3	Intolerable
	E.24	Caída del sistema por agotamiento de recursos	Saturación del sistema informático.	Muy baja	2	10	3	Intolerable
	E.25	Perdida de equipos (Robo)	Recuperación de soportes reciclados o desechados.	Muy baja	2	10	3	Intolerable

Tabla 1. Estimación del riesgo activo switch 24/10/100/1000 base t4s. (Continuación)

ATAQUES INTENCIONADOS	**A.6**	Abuso de privilegios de acceso	Abuso de cada uno de los derechos otorgados.	Muy baja	2	10	3	Intolerable
	A.7	Uso no previsto	Implementación de recursos (económicos y de tiempo) en actividades no relacionadas.	Muy baja	2	10	3	Intolerable
	A.11	Acceso no autorizado	Uso ilícito del hardware	Muy baja	2	10	3	Intolerable
	A.23	Manipulación de los equipos	Sabotaje del hardware y software conteniente.	Muy baja	2	10	3	Intolerable
	A.24	Denegación de servicio	Saturación del sistema de información.	Muy baja	2	10	3	Intolerable
	A.25	Robo	Robo de porte de la información, puede esta ser física o digital.	Muy baja	2	10	3	Intolerable
	A.26	Ataque destructivo	Destrucción de los contenedores de la información, en recipientes físicos y lógicos.	Muy baja	2	10	3	Intolerable

Fuente: Autoría propia

Tabla 2. Estimación del riesgo activo switch 24/10/100/1000pwr cord

ACTIVO TI	**SWITCH 24/10/100/1000PWR CORD**
ADMINISTRADOR	PIMIENTO CARDENAS WILSON MAURICIO
DEGRADACIÓN	60%
IMPACTO	5

Tabla 2. Estimación del riesgo activo switch 24/10/100/1000pwr cord. (Continuación)

TIPO DE ACTIVO	HARDWARE							
Tipo	**ID**	**Amenaza**	**Exposición/Vulnerabilidad**	**RIESGO ACTUAL**				
							3.04	Intolerable
				Frecuencia (F)		**R**	**NR**	
DESASTRES NATURALES	**N.1**	Fuego	No existe sistema de alarma contra incendios. Se posee un solo extintor de solkaflam (clase c) recomendados para incendios en lugares donde se encuentren equipos eléctricos.	Muy baja	2	10	3	Intolerable
	N.2	Daños por agua	La infraestructura está expuesta a goteras, cuenta con averías en el techo en donde el agua de las lluvias	Muy baja	2	10	3	Intolerable
	N.*	Desastres naturales	La oficina de la dependencia de sistemas se encuentra en zona baja de riesgo de desastre natural de origen volcánico debido a su cercanía con el volcán nevado del Tolima.	Raro	1	5	2	Tolerable
DE ORIGEN INDUSTRIAL	**I.1**	Fuego	No existe sistema de alarma contra incendios. Se posee un solo extintor de solkaflam (clase c) recomendados para incendios en lugares donde se encuentren equipos eléctricos.	Muy baja	2	10	3	Intolerable

Tabla 2. Estimación del riesgo activo switch 24/10/100/1000pwr cord. (Continuación)

	I.2	Daños por agua	La concentración del líquido sobrante por parte del aire acondicionado causaría daños en los equipos.	Muy baja	2	10	3	Intolerable
	I.*	Desastres industriales	No hay exposición o vulnerabilidad, por parte de esta amenaza.	Muy baja	2	10	3	Intolerable
	I.3	Contaminación mecánica	No hay exposición o vulnerabilidad, por parte de esta amenaza.	Muy baja	2	10	3	Intolerable
	I.4	Contaminación electromagnética	No hay exposición o vulnerabilidad, por parte de esta amenaza.	Muy baja	2	10	3	Intolerable
	I.5	Avería de origen físico o lógico	La manipulación por parte de cada uno de los componentes encontrados en la dependencia, como también por defectos de los componentes desde fabrica	Muy baja	2	10	3	Intolerable
	I.6	Corte del suministro eléctrico	Amenaza debida a factores externos, a clemencias de tipo naturales como lluvias u otros.	Muy baja	2	10	3	Intolerable
	I.7	Condiciones inadecuadas de temperatura o humedad	No se cuenta con una infraestructura adecuada para soportar los defectos del sistema de refrigeración.	Muy baja	2	10	3	Intolerable

Tabla 2. Estimación del riesgo activo switch 24/10/100/1000pwr cord. (Continuación)

	I.11	Emanaciones electromagnéticas	No hay exposición o vulnerabilidad, por parte de esta amenaza.	Muy baja	2	10	3	Intolerable
ERRORES Y FALLOS NO INTENCIONADOS	**E.2**	Errores del administrador	Pérdida total o parcial del tiempo de ejecución de sus actividades, dependiendo de la gravedad del asunto.	Muy baja	2	10	3	Intolerable
	E.23	Errores de mantenimiento / actualización de equipos(hardware)	Perjuicio a la mantenibilidad del sistema de información.	Muy baja	2	10	3	Intolerable
	E.24	Caída del sistema por agotamiento de recursos	Saturación del sistema informático.	Muy baja	2	10	3	Intolerable
	E.25	Perdida de equipos (Robo)	Recuperación de soportes reciclados o desechados.	Muy baja	2	10	3	Intolerable
ATAQUES INTENCIONADOS	**A.6**	Abuso de privilegios de acceso	Abuso de cada uno de los derechos otorgados.	Muy baja	2	10	3	Intolerable
	A.7	Uso no previsto	Implementación de recursos (económicos y de tiempo) en actividades no relacionadas.	Muy baja	2	10	3	Intolerable
	A.11	Acceso no autorizado	Uso ilícito del hardware	Muy baja	2	10	3	Intolerable

Tabla 2. Estimación del riesgo activo switch 24/10/100/1000pwr cord. (Continuación)

	A.23	Manipulación de los equipos	Sabotaje del hardware y software conteniente.	Muy baja	2	10	3	Intolerable
	A.24	Denegación de servicio	Saturación del sistema de información.	Muy baja	2	10	3	Intolerable
	A.25	Robo	Robo de porte de la información, puede esta ser física o digital.	Muy baja	2	10	3	Intolerable
	A.26	Ataque destructivo	Destrucción de los contenedores de la información, en recipientes físicos y lógicos.	Muy baja	2	10	3	Intolerable

Fuente: Autoría propia

Tabla 3. Estimación del riesgo activo switch ALCATEL LUCEN 9561

ACTIVO TI	**SWITCH ALCATEL LUCEN 9561**							
ADMINISTRADOR	PIMIENTO CARDENAS WILSON MAURICIO							
DEGRADACIÓN	60%							
IMPACTO	5							
TIPO DE ACTIVO	HARDWARE							
Tipo	**ID**	**Amenaza**	**Exposición/Vulnerabilidad**	**RIESGO ACTUAL**				
							3.04	Intolerable
				Frecuencia (F)		**R**	**NR**	
DESASTRES NATURA	**N.1**	Fuego	No existe sistema de alarma contra incendios. Se posee un solo extintor de solkaflam (clase c) recomendados para incendios en	Muy baja	2	10	3	Intolerable

Tabla 3. Estimación del riesgo activo switch ALCATEL LUCEN 9561. (Continuación)

			lugares donde se encuentren equipos eléctricos.					
	N.2	Daños por agua	La infraestructura está expuesta a goteras, cuenta con averías en el techo en donde el agua de las lluvias	Muy baja	2	10	3	Intolerable
	N.*	Desastres naturales	La oficina de la dependencia de sistemas se encuentra en zona baja de riesgo de desastre natural de origen volcánico debido a su cercanía con el volcán nevado del Tolima.	Raro	1	5	2	Tolerable
DE ORIGEN INDUSTRIAL	**I.1**	Fuego	No existe sistema de alarma contra incendios. Se posee un solo extintor de solkaflam (clase c) recomendados para incendios en lugares donde se encuentren equipos eléctricos.	Muy baja	2	10	3	Intolerable
	I.2	Daños por agua	La concentración del líquido sobrante por parte del aire acondicionado causaría daños en los equipos.	Muy baja	2	10	3	Intolerable
	I.*	Desastres industriales	No hay exposición o vulnerabilidad, por parte de esta amenaza.	Muy baja	2	10	3	Intolerable

Tabla 3. Estimación del riesgo activo switch ALCATEL LUCEN 9561. (Continuación)

	I.3	Contaminación mecánica	No hay exposición o vulnerabilidad, por parte de esta amenaza.	Muy baja	2	10	3	Intolerable
	I.4	Contaminación electromagnética	No hay exposición o vulnerabilidad, por parte de esta amenaza.	Muy baja	2	10	3	Intolerable
	I.5	Avería de origen físico o lógico	La manipulación por parte de cada uno de los componentes encontrados en la dependencia, como también por defectos de los componentes desde fabrica	Muy baja	2	10	3	Intolerable
	I.6	Corte del suministro eléctrico	Amenaza debida a factores externos, a clemencias de tipo naturales como lluvias u otros.	Muy baja	2	10	3	Intolerable
	I.7	Condiciones inadecuadas de temperatura o humedad	No se cuenta con una infraestructura adecuada para soportar los defectos del sistema de refrigeración.	Muy baja	2	10	3	Intolerable
	I.11	Emanaciones electromagnéticas	No hay exposición o vulnerabilidad, por parte de esta amenaza.	Muy baja	2	10	3	Intolerable
ERRORES Y FALLOS NO	**E.2**	Errores del administrador	Pérdida total o parcial del tiempo de ejecución de sus actividades, dependiendo de la gravedad del asunto.	Muy baja	2	10	3	Intolerable

Tabla 3. Estimación del riesgo activo switch ALCATEL LUCEN 9561. (Continuación)

	E.23	Errores de mantenimiento / actualización de equipos(hardware)	Perjuicio a la mantenibilidad del sistema de información.	Muy baja	2	10	3	Intolerable
	E.24	Caída del sistema por agotamiento de recursos	Saturación del sistema informático.	Muy baja	2	10	3	Intolerable
	E.25	Perdida de equipos (Robo)	Recuperación de soportes reciclados o desechados.	Muy baja	2	10	3	Intolerable
ATAQUES INTENCIONADOS	**A.6**	Abuso de privilegios de acceso	Abuso de cada uno de los derechos otorgados.	Muy baja	2	10	3	Intolerable
	A.7	Uso no previsto	Implementación de recursos (económicos y de tiempo) en actividades no relacionadas.	Muy baja	2	10	3	Intolerable
	A.11	Acceso no autorizado	Uso ilícito del hardware	Muy baja	2	10	3	Intolerable
	A.23	Manipulación de los equipos	Sabotaje del hardware y software conteniente.	Muy baja	2	10	3	Intolerable
	A.24	Denegación de servicio	Saturación del sistema de información.	Muy baja	2	10	3	Intolerable

Tabla 3. Estimación del riesgo activo switch ALCATEL LUCEN 9561. (Continuación)

	A.25	Robo	Robo de porte de la información, puede esta ser física o digital.	Muy baja	2	10	3	Intolerable
	A.26	Ataque destructivo	Destrucción de los contenedores de la información, en recipientes físicos y lógicos.	Muy baja	2	10	3	Intolerable

Fuente: Autoría propia

Tabla 4. Estimación del riesgo activo switch ALCATEL LUCEN 9556

ACTIVO TI	**SWITCH ALCATEL LUCEN 9556**							
ADMINISTRADOR	PIMIENTO CARDENAS WILSON MAURICIO							
DEGRADACIÓN	60%							
IMPACTO	5							
TIPO DE ACTIVO	HARDWARE							
Tipo	**ID**	**Amenaza**	**Exposición/Vulnerabilidad**	**RIESGO ACTUAL**				
							3.04	Intolerable
				Frecuencia (F)		**R**	**NR**	
DESASTRES NATURALES	**N.1**	Fuego	No existe sistema de alarma contra incendios. Se posee un solo extintor de solkaflam (clase c) recomendados para incendios en lugares donde se encuentren equipos eléctricos.	Muy baja	2	10	3	Intolerable
	N.2	Daños por agua	La infraestructura está expuesta a goteras, cuenta con averías en el techo en donde el agua de las lluvias	Muy baja	2	10	3	Intolerable

Tabla 4. Estimación del riesgo activo switch ALCATEL LUCEN 9556. (Continuación)

	N.*	Desastres naturales	La oficina de la dependencia de sistemas se encuentra en zona baja de riesgo de desastre natural de origen volcánico debido a su cercanía con el volcán nevado del Tolima.	Raro	1	5	2	Tolerable
DE ORIGEN INDUSTRIAL	**I.1**	Fuego	No existe sistema de alarma contra incendios. Se posee un solo extintor de solkaflam (clase c) recomendados para incendios en lugares donde se encuentren equipos eléctricos.	Muy baja	2	10	3	Intolerable
	I.2	Daños por agua	La concentración del líquido sobrante por parte del aire acondicionado causaría daños en los equipos.	Muy baja	2	10	3	Intolerable
	I.*	Desastres industriales	No hay exposición o vulnerabilidad, por parte de esta amenaza.	Muy baja	2	10	3	Intolerable
	I.3	Contaminación mecánica	No hay exposición o vulnerabilidad, por parte de esta amenaza.	Muy baja	2	10	3	Intolerable
	I.4	Contaminación electromagnética	No hay exposición o vulnerabilidad, por parte de esta amenaza.	Muy baja	2	10	3	Intolerable

Tabla 4. Estimación del riesgo activo switch ALCATEL LUCEN 9556. (Continuación)

	I.5	Avería de origen físico o lógico	La manipulación por parte de cada uno de los componentes encontrados en la dependencia, como también por defectos de los componentes desde fabrica	Muy baja	2	10	3	Intolerable
	I.6	Corte del suministro eléctrico	Amenaza debida a factores externos, a clemencias de tipo naturales como lluvias u otros.	Muy baja	2	10	3	Intolerable
	I.7	Condiciones inadecuadas de temperatura o humedad	No se cuenta con una infraestructura adecuada para soportar los defectos del sistema de refrigeración.	Muy baja	2	10	3	Intolerable
	I.11	Emanaciones electromagnéticas	No hay exposición o vulnerabilidad, por parte de esta amenaza.	Muy baja	2	10	3	Intolerable
ERRORES Y FALLOS NO INTENCIONADOS	**E.2**	Errores del administrador	Pérdida total o parcial del tiempo de ejecución de sus actividades, dependiendo de la gravedad del asunto.	Muy baja	2	10	3	Intolerable
	E.23	Errores de mantenimiento / actualización de equipos(hardware)	Perjuicio a la mantenibilidad del sistema de información.	Muy baja	2	10	3	Intolerable

Tabla 4. Estimación del riesgo activo switch ALCATEL LUCEN 9556. (Continuación)

	E.24	Caída del sistema por agotamiento de recursos	Saturación del sistema informático.	Muy baja	2	10	3	Intolerable
	E.25	Perdida de equipos (Robo)	Recuperación de soportes reciclados o desechados.	Muy baja	2	10	3	Intolerable
ATAQUES INTENCIONADOS	**A.6**	Abuso de privilegios de acceso	Abuso de cada uno de los derechos otorgados.	Muy baja	2	10	3	Intolerable
	A.7	Uso no previsto	Implementación de recursos (económicos y de tiempo) en actividades no relacionadas.	Muy baja	2	10	3	Intolerable
	A.11	Acceso no autorizado	Uso ilícito del hardware	Muy baja	2	10	3	Intolerable
	A.23	Manipulación de los equipos	Sabotaje del hardware y software conteniente.	Muy baja	2	10	3	Intolerable
	A.24	Denegación de servicio	Saturación del sistema de información.	Muy baja	2	10	3	Intolerable
	A.25	Robo	Robo de porte de la información, puede esta ser física o digital.	Muy baja	2	10	3	Intolerable
	A.26	Ataque destructivo	Destrucción de los contenedores de la información, en recipientes físicos y lógicos.	Muy baja	2	10	3	Intolerable

Fuente: Autoría propia

Tabla 5. Estimación del riesgo activo switch Alcatel lucent 9557

ACTIVO TI	**SWITCH ALCATEL LUCENT 9557**
ADMINISTRADOR	PIMIENTO CARDENAS WILSON MAURICIO
DEGRADACIÓN	60%
IMPACTO	5
TIPO DE ACTIVO	HARDWARE

Tipo	ID	Amenaza	Exposición/Vulnerabilidad	RIESGO ACTUAL				
							3.04	Intolerable
				Frecuencia (F)		**R**	**NR**	
DESASTRES NATURALES	**N.1**	Fuego	No existe sistema de alarma contra incendios. Se posee un solo extintor de solkaflam (clase c) recomendados para incendios en lugares donde se encuentren equipos eléctricos.	Muy baja	2	10	3	Intolerable
	N.2	Daños por agua	La infraestructura está expuesta a goteras, cuenta con averías en el techo en donde el agua de las lluvias	Muy baja	2	10	3	Intolerable
	N.*	Desastres naturales	La oficina de la dependencia de sistemas se encuentra en zona baja de riesgo de desastre natural de origen volcánico debido a su cercanía con el volcán nevado del Tolima.	Raro	1	5	2	Tolerable

Tabla 5. Estimación del riesgo activo switch Alcatel lucent 9557. (Continuación)

DE ORIGEN INDUSTRIAL	**I.1**	Fuego	No existe sistema de alarma contra incendios. Se posee un solo extintor de solkaflam (clase c) recomendados para incendios en lugares donde se encuentren equipos eléctricos.	Muy baja	2	10	3	Intolerable
	I.2	Daños por agua	La concentración del líquido sobrante por parte del aire acondicionado causaría daños en los equipos.	Muy baja	2	10	3	Intolerable
	I.*	Desastres industriales	No hay exposición o vulnerabilidad, por parte de esta amenaza.	Muy baja	2	10	3	Intolerable
	I.3	Contaminación mecánica	No hay exposición o vulnerabilidad, por parte de esta amenaza.	Muy baja	2	10	3	Intolerable
	I.4	Contaminación electromagnética	No hay exposición o vulnerabilidad, por parte de esta amenaza.	Muy baja	2	10	3	Intolerable
	I.5	Avería de origen físico o lógico	La manipulación por parte de cada uno de los componentes encontrados en la dependencia, como también por defectos de los componentes desde fabrica	Muy baja	2	10	3	Intolerable

Tabla 5. Estimación del riesgo activo switch Alcatel lucent 9557. (Continuación)

	I.6	Corte del suministro eléctrico	Amenaza debida a factores externos, a clemencias de tipo naturales como lluvias u otros.	Muy baja	2	10	3	Intolerable
	I.7	Condiciones inadecuadas de temperatura o humedad	No se cuenta con una infraestructura adecuada para soportar los defectos del sistema de refrigeración.	Muy baja	2	10	3	Intolerable
	I.11	Emanaciones electromagnéticas	No hay exposición o vulnerabilidad, por parte de esta amenaza.	Muy baja	2	10	3	Intolerable
ERRORES Y FALLOS NO INTENCIONADOS	**E.2**	Errores del administrador	Pérdida total o parcial del tiempo de ejecución de sus actividades, dependiendo de la gravedad del asunto.	Muy baja	2	10	3	Intolerable
	E.23	Errores de mantenimiento / actualización de equipos(hardware)	Perjuicio a la mantenibilidad del sistema de información.	Muy baja	2	10	3	Intolerable
	E.24	Caída del sistema por agotamiento de recursos	Saturación del sistema informático.	Muy baja	2	10	3	Intolerable
	E.25	Perdida de equipos (Robo)	Recuperación de soportes reciclados o desechados.	Muy baja	2	10	3	Intolerable

Tabla 5. Estimación del riesgo activo switch Alcatel lucent 9557. (Continuación)

ATAQUES INTENCIONADOS	**A.6**	Abuso de privilegios de acceso	Abuso de cada uno de los derechos otorgados.	Muy baja	2	10	3	Intolerable
	A.7	Uso no previsto	Implementación de recursos (económicos y de tiempo) en actividades no relacionadas.	Muy baja	2	10	3	Intolerable
	A.11	Acceso no autorizado	Uso ilícito del hardware	Muy baja	2	10	3	Intolerable
	A.23	Manipulación de los equipos	Sabotaje del hardware y software conteniente.	Muy baja	2	10	3	Intolerable
	A.24	Denegación de servicio	Saturación del sistema de información.	Muy baja	2	10	3	Intolerable
	A.25	Robo	Robo de porte de la información, puede esta ser física o digital.	Muy baja	2	10	3	Intolerable
	A.26	Ataque destructivo	Destrucción de los contenedores de la información, en recipientes físicos y lógicos.	Muy baja	2	10	3	Intolerable

Fuente: Autoría propia

Tabla 6. Estimación del riesgo activo switch Alcatel lucent 9558

ACTIVO TI	**SWITCH ALCATEL LUCENT 9558**
ADMINISTRADOR	PIMIENTO CARDENAS WILSON MAURICIO
DEGRADACIÓN	60%
IMPACTO	5

Tabla 6. Estimación del riesgo activo switch Alcatel lucent 9558. (Continuación)

TIPO DE ACTIVO	HARDWARE							
Tipo	**ID**	**Amenaza**	**Exposición/Vulnerabilidad**	**RIESGO ACTUAL**				
							3.04	Intolerable
				Frecuencia (F)		**R**	**NR**	
DESASTRES NATURALES	**N.1**	Fuego	No existe sistema de alarma contra incendios. Se posee un solo extintor de solkaflam (clase c) recomendados para incendios en lugares donde se encuentren equipos eléctricos.	Muy baja	2	10	3	Intolerable
	N.2	Daños por agua	La infraestructura está expuesta a goteras, cuenta con averías en el techo en donde el agua de las lluvias	Muy baja	2	10	3	Intolerable
	N.*	Desastres naturales	La oficina de la dependencia de sistemas se encuentra en zona baja de riesgo de desastre natural de origen volcánico debido a su cercanía con el volcán nevado del Tolima.	Raro	1	5	2	Tolerable
DE ORIGEN INDUST	**I.1**	Fuego	No existe sistema de alarma contra incendios. Se posee un solo extintor de solkaflam (clase c) recomendados para incendios en	Muy baja	2	10	3	Intolerable

Tabla 6. Estimación del riesgo activo switch Alcatel lucent 9558. (Continuación)

			lugares donde se encuentren equipos eléctricos.					
	I.2	Daños por agua	La concentración del líquido sobrante por parte del aire acondicionado causaría daños en los equipos.	Muy baja	2	10	3	Intolerable
	I.*	Desastres industriales	No hay exposición o vulnerabilidad, por parte de esta amenaza.	Muy baja	2	10	3	Intolerable
	I.3	Contaminación mecánica	No hay exposición o vulnerabilidad, por parte de esta amenaza.	Muy baja	2	10	3	Intolerable
	I.4	Contaminación electromagnética	No hay exposición o vulnerabilidad, por parte de esta amenaza.	Muy baja	2	10	3	Intolerable
	I.5	Avería de origen físico o lógico	La manipulación por parte de cada uno de los componentes encontrados en la dependencia, como también por defectos de los componentes desde fabrica	Muy baja	2	10	3	Intolerable
	I.6	Corte del suministro eléctrico	Amenaza debida a factores externos, a clemencias de tipo naturales como lluvias u otros.	Muy baja	2	10	3	Intolerable

Tabla 6. Estimación del riesgo activo switch Alcatel lucent 9558. (Continuación)

	I.7	Condiciones inadecuadas de temperatura o humedad	No se cuenta con una infraestructura adecuada para soportar los defectos del sistema de refrigeración.	Muy baja	2	10	3	Intolerable
	I.11	Emanaciones electromagnéticas	No hay exposición o vulnerabilidad, por parte de esta amenaza.	Muy baja	2	10	3	Intolerable
ERRORES Y FALLOS NO INTENCIONADOS	**E.2**	Errores del administrador	Pérdida total o parcial del tiempo de ejecución de sus actividades, dependiendo de la gravedad del asunto.	Muy baja	2	10	3	Intolerable
	E.23	Errores de mantenimiento / actualización de equipos(hardware)	Perjuicio a la mantenibilidad del sistema de información.	Muy baja	2	10	3	Intolerable
	E.24	Caída del sistema por agotamiento de recursos	Saturación del sistema informático.	Muy baja	2	10	3	Intolerable
	E.25	Perdida de equipos (Robo)	Recuperación de soportes reciclados o desechados.	Muy baja	2	10	3	Intolerable
ATAQUES	**A.6**	Abuso de privilegios de acceso	Abuso de cada uno de los derechos otorgados.	Muy baja	2	10	3	Intolerable

Tabla 6. Estimación del riesgo activo switch Alcatel lucent 9558. (Continuación)

	A.7	Uso no previsto	Implementación de recursos (económicos y de tiempo) en actividades no relacionadas.	Muy baja	2	10	3	Intolerable
	A.11	Acceso no autorizado	Uso ilícito del hardware	Muy baja	2	10	3	Intolerable
	A.23	Manipulación de los equipos	Sabotaje del hardware y software conteniente.	Muy baja	2	10	3	Intolerable
	A.24	Denegación de servicio	Saturación del sistema de información.	Muy baja	2	10	3	Intolerable
	A.25	Robo	Robo de porte de la información, puede esta ser física o digital.	Muy baja	2	10	3	Intolerable
	A.26	Ataque destructivo	Destrucción de los contenedores de la información, en recipientes físicos y lógicos.	Muy baja	2	10	3	Intolerable

Fuente: Autoría propia

Tabla 7. Estimación del riesgo activo switch Alcatel lucent 9559

ACTIVO TI	**SWITCH ALCATEL LUCENT 9559**						
ADMINISTRADOR	PIMIENTO CARDENAS WILSON MAURICIO						
DEGRADACIÓN	60%						
IMPACTO	5						
TIPO DE ACTIVO	HARDWARE						
Tipo	**ID**	**Amenaza**	**Exposición/Vulnerabilidad**	**RIESGO ACTUAL**			
						3.04	Intolerable

Tabla 7. Estimación del riesgo activo switch Alcatel lucent 9559. (Continuación)

				Frecuencia (F)		R	NR	
DESASTRES NATURALES	**N.1**	Fuego	No existe sistema de alarma contra incendios. Se posee un solo extintor de solkaflam (clase c) recomendados para incendios en lugares donde se encuentren equipos eléctricos.	Muy baja	2	10	3	Intolerable
	N.2	Daños por agua	La infraestructura está expuesta a goteras, cuenta con averías en el techo en donde el agua de las lluvias	Muy baja	2	10	3	Intolerable
	N.*	Desastres naturales	La oficina de la dependencia de sistemas se encuentra en zona baja de riesgo de desastre natural de origen volcánico debido a su cercanía con el volcán nevado del Tolima.	Raro	1	5	2	Tolerable
DE ORIGEN INDUSTRIAL	**I.1**	Fuego	No existe sistema de alarma contra incendios. Se posee un solo extintor de solkaflam (clase c) recomendados para incendios en lugares donde se encuentren equipos eléctricos.	Muy baja	2	10	3	Intolerable
	I.2	Daños por agua	La concentración del líquido sobrante por parte del aire	Muy baja	2	10	3	Intolerable

Tabla 7. Estimación del riesgo activo switch Alcatel lucent 9559. (Continuación)

			acondicionado causaría daños en los equipos.					
	I.*	Desastres industriales	No hay exposición o vulnerabilidad, por parte de esta amenaza.	Muy baja	2	10	3	Intolerable
	I.3	Contaminación mecánica	No hay exposición o vulnerabilidad, por parte de esta amenaza.	Muy baja	2	10	3	Intolerable
	I.4	Contaminación electromagnética	No hay exposición o vulnerabilidad, por parte de esta amenaza.	Muy baja	2	10	3	Intolerable
	I.5	Avería de origen físico o lógico	La manipulación por parte de cada uno de los componentes encontrados en la dependencia, como también por defectos de los componentes desde fabrica	Muy baja	2	10	3	Intolerable
	I.6	Corte del suministro eléctrico	Amenaza debida a factores externos, a clemencias de tipo naturales como lluvias u otros.	Muy baja	2	10	3	Intolerable
	I.7	Condiciones inadecuadas de temperatura o humedad	No se cuenta con una infraestructura adecuada para soportar los defectos del sistema de refrigeración.	Muy baja	2	10	3	Intolerable
	I.11	Emanaciones electromagnéticas	No hay exposición o vulnerabilidad, por parte de esta amenaza.	Muy baja	2	10	3	Intolerable

Tabla 7. Estimación del riesgo activo switch Alcatel lucent 9559. (Continuación)

ERRORES Y FALLOS NO INTENCIONADOS	**E.2**	Errores del administrador	Pérdida total o parcial del tiempo de ejecución de sus actividades, dependiendo de la gravedad del asunto.	Muy baja	2	10	3	Intolerable
	E.23	Errores de mantenimiento / actualización de equipos(hardware)	Perjuicio a la mantenibilidad del sistema de información.	Muy baja	2	10	3	Intolerable
	E.24	Caída del sistema por agotamiento de recursos	Saturación del sistema informático.	Muy baja	2	10	3	Intolerable
	E.25	Perdida de equipos (Robo)	Recuperación de soportes reciclados o desechados.	Muy baja	2	10	3	Intolerable
ATAQUES INTENCIONADOS	**A.6**	Abuso de privilegios de acceso	Abuso de cada uno de los derechos otorgados.	Muy baja	2	10	3	Intolerable
	A.7	Uso no previsto	Implementación de recursos (económicos y de tiempo) en actividades no relacionadas.	Muy baja	2	10	3	Intolerable
	A.11	Acceso no autorizado	Uso ilícito del hardware	Muy baja	2	10	3	Intolerable
	A.23	Manipulación de los equipos	Sabotaje del hardware y software conteniente.	Muy baja	2	10	3	Intolerable

Tabla 7. Estimación del riesgo activo switch Alcatel lucent 9559. (Continuación)

	A.24	Denegación de servicio	Saturación del sistema de información.	Muy baja	2	10	3	Intolerable
	A.25	Robo	Robo de porte de la información, puede esta ser física o digital.	Muy baja	2	10	3	Intolerable
	A.26	Ataque destructivo	Destrucción de los contenedores de la información, en recipientes físicos y lógicos.	Muy baja	2	10	3	Intolerable

Fuente: Autoría propia

Tabla 8. Estimación del riesgo activo switch Alcatel lucent 9543

ACTIVO TI	**SWITCH ALCATEL LUCENT 9543**							
ADMINISTRADOR	PIMIENTO CARDENAS WILSON MAURICIO							
DEGRADACIÓN	60%							
IMPACTO	5							
TIPO DE ACTIVO	HARDWARE							
Tipo	**ID**	**Amenaza**	**Exposición/Vulnerabilidad**	**RIESGO ACTUAL**				
							3.04	Intolerable
				Frecuencia (F)		**R**	**NR**	
DESASTRES NATURALES	**N.1**	Fuego	No existe sistema de alarma contra incendios. Se posee un solo extintor de solkaflam (clase c) recomendados para incendios en lugares donde se encuentren equipos eléctricos.	Muy baja	2	10	3	Intolerable

Tabla 8. Estimación del riesgo activo switch Alcatel lucent 9543. (Continuación)

	N.2	Daños por agua	La infraestructura está expuesta a goteras, cuenta con averías en el techo en donde el agua de las lluvias	Muy baja	2	10	3	Intolerable
	N.*	Desastres naturales	La oficina de la dependencia de sistemas se encuentra en zona baja de riesgo de desastre natural de origen volcánico debido a su cercanía con el volcán nevado del Tolima.	Raro	1	5	2	Tolerable
DE ORIGEN INDUSTRIAL	**I.1**	Fuego	No existe sistema de alarma contra incendios. Se posee un solo extintor de solkaflam (clase c) recomendados para incendios en lugares donde se encuentren equipos eléctricos.	Muy baja	2	10	3	Intolerable
	I.2	Daños por agua	La concentración del líquido sobrante por parte del aire acondicionado causaría daños en los equipos.	Muy baja	2	10	3	Intolerable
	I.*	Desastres industriales	No hay exposición o vulnerabilidad, por parte de esta amenaza.	Muy baja	2	10	3	Intolerable
	I.3	Contaminación mecánica	No hay exposición o vulnerabilidad, por parte de esta amenaza.	Muy baja	2	10	3	Intolerable

Tabla 8. Estimación del riesgo activo switch Alcatel lucent 9543. (Continuación)

	I.4	Contaminación electromagnética	No hay exposición o vulnerabilidad, por parte de esta amenaza.	Muy baja	2	10	3	Intolerable
	I.5	Avería de origen físico o lógico	La manipulación por parte de cada uno de los componentes encontrados en la dependencia, como también por defectos de los componentes desde fabrica	Muy baja	2	10	3	Intolerable
	I.6	Corte del suministro eléctrico	Amenaza debida a factores externos, a clemencias de tipo naturales como lluvias u otros.	Muy baja	2	10	3	Intolerable
	I.7	Condiciones inadecuadas de temperatura o humedad	No se cuenta con una infraestructura adecuada para soportar los defectos del sistema de refrigeración.	Muy baja	2	10	3	Intolerable
	I.11	Emanaciones electromagnéticas	No hay exposición o vulnerabilidad, por parte de esta amenaza.	Muy baja	2	10	3	Intolerable
ERRORES Y FALLOS NO INTENCIONADOS	**E.2**	Errores del administrador	Pérdida total o parcial del tiempo de ejecución de sus actividades, dependiendo de la gravedad del asunto.	Muy baja	2	10	3	Intolerable
	E.23	Errores de mantenimiento /	Perjuicio a la mantenibilidad del sistema de información.	Muy baja	2	10	3	Intolerable

Tabla 8. Estimación del riesgo activo switch Alcatel lucent 9543. (Continuación)

		actualización de equipos(hardware)						
	E.24	Caída del sistema por agotamiento de recursos	Saturación del sistema informático.	Muy baja	2	10	3	Intolerable
	E.25	Perdida de equipos (Robo)	Recuperación de soportes reciclados o desechados.	Muy baja	2	10	3	Intolerable
ATAQUES INTENCIONADOS	**A.6**	Abuso de privilegios de acceso	Abuso de cada uno de los derechos otorgados.	Muy baja	2	10	3	Intolerable
	A.7	Uso no previsto	Implementación de recursos (económicos y de tiempo) en actividades no relacionadas.	Muy baja	2	10	3	Intolerable
	A.11	Acceso no autorizado	Uso ilícito del hardware	Muy baja	2	10	3	Intolerable
	A.23	Manipulación de los equipos	Sabotaje del hardware y software conteniente.	Muy baja	2	10	3	Intolerable
	A.24	Denegación de servicio	Saturación del sistema de información.	Muy baja	2	10	3	Intolerable
	A.25	Robo	Robo de porte de la información, puede esta ser física o digital.	Muy baja	2	10	3	Intolerable

Tabla 8. Estimación del riesgo activo switch Alcatel lucent 9543. (Continuación)

	A.26	Ataque destructivo	Destrucción de los contenedores de la información, en recipientes físicos y lógicos.	Muy baja	2	10	3	Intolerable

Fuente: Autoría propia

Tabla 9. Estimación del riesgo activo switch Alcatel lucent 9544

ACTIVO TI			**SWITCH ALCATEL LUCENT 9544**					
ADMINISTRADOR			PIMIENTO CARDENAS WILSON MAURICIO					
DEGRADACIÓN			60%					
IMPACTO			5					
TIPO DE ACTIVO			HARDWARE					
Tipo	**ID**	**Amenaza**	**Exposición/Vulnerabilidad**	**RIESGO ACTUAL**				
							3.04	Intolerable
				Frecuencia (F)		**R**	**NR**	
DESASTRES NATURALES	**N.1**	Fuego	No existe sistema de alarma contra incendios. Se posee un solo extintor de solkaflam (clase c) recomendados para incendios en lugares donde se encuentren equipos eléctricos.	Muy baja	2	10	3	Intolerable
	N.2	Daños por agua	La infraestructura está expuesta a goteras, cuenta con averías en el techo en donde el agua de las lluvias	Muy baja	2	10	3	Intolerable

Tabla 9. Estimación del riesgo activo switch Alcatel lucent 9544. (Continuación)

	N.*	Desastres naturales	La oficina de la dependencia de sistemas se encuentra en zona baja de riesgo de desastre natural de origen volcánico debido a su cercanía con el volcán nevado del Tolima.	Raro	1	5	2	Tolerable
DE ORIGEN INDUSTRIAL	**I.1**	Fuego	No existe sistema de alarma contra incendios. Se posee un solo extintor de solkaflam (clase c) recomendados para incendios en lugares donde se encuentren equipos eléctricos.	Muy baja	2	10	3	Intolerable
	I.2	Daños por agua	La concentración del líquido sobrante por parte del aire acondicionado causaría daños en los equipos.	Muy baja	2	10	3	Intolerable
	I.*	Desastres industriales	No hay exposición o vulnerabilidad, por parte de esta amenaza.	Muy baja	2	10	3	Intolerable
	I.3	Contaminación mecánica	No hay exposición o vulnerabilidad, por parte de esta amenaza.	Muy baja	2	10	3	Intolerable
	I.4	Contaminación electromagnética	No hay exposición o vulnerabilidad, por parte de esta amenaza.	Muy baja	2	10	3	Intolerable

Tabla 9. Estimación del riesgo activo switch Alcatel lucent 9544. (Continuación)

	I.5	Avería de origen físico o lógico	La manipulación por parte de cada uno de los componentes encontrados en la dependencia, como también por defectos de los componentes desde fabrica	Muy baja	2	10	3	Intolerable
	I.6	Corte del suministro eléctrico	Amenaza debida a factores externos, a clemencias de tipo naturales como lluvias u otros.	Muy baja	2	10	3	Intolerable
	I.7	Condiciones inadecuadas de temperatura o humedad	No se cuenta con una infraestructura adecuada para soportar los defectos del sistema de refrigeración.	Muy baja	2	10	3	Intolerable
	I.11	Emanaciones electromagnéticas	No hay exposición o vulnerabilidad, por parte de esta amenaza.	Muy baja	2	10	3	Intolerable
ERRORES Y FALLOS NO INTENCIONADOS	**E.2**	Errores del administrador	Pérdida total o parcial del tiempo de ejecución de sus actividades, dependiendo de la gravedad del asunto.	Muy baja	2	10	3	Intolerable
	E.23	Errores de mantenimiento / actualización de equipos(hardware)	Perjuicio a la mantenibilidad del sistema de información.	Muy baja	2	10	3	Intolerable

Tabla 9. Estimación del riesgo activo switch Alcatel lucent 9544. (Continuación)

	E.24	Caída del sistema por agotamiento de recursos	Saturación del sistema informático.	Muy baja	2	10	3	Intolerable
	E.25	Perdida de equipos (Robo)	Recuperación de soportes reciclados o desechados.	Muy baja	2	10	3	Intolerable
ATAQUES INTENCIONADOS	**A.6**	Abuso de privilegios de acceso	Abuso de cada uno de los derechos otorgados.	Muy baja	2	10	3	Intolerable
	A.7	Uso no previsto	Implementación de recursos (económicos y de tiempo) en actividades no relacionadas.	Muy baja	2	10	3	Intolerable
	A.11	Acceso no autorizado	Uso ilícito del hardware	Muy baja	2	10	3	Intolerable
	A.23	Manipulación de los equipos	Sabotaje del hardware y software conteniente.	Muy baja	2	10	3	Intolerable
	A.24	Denegación de servicio	Saturación del sistema de información.	Muy baja	2	10	3	Intolerable
	A.25	Robo	Robo de porte de la información, puede esta ser física o digital.	Muy baja	2	10	3	Intolerable
	A.26	Ataque destructivo	Destrucción de los contenedores de la información, en recipientes físicos y lógicos.	Muy baja	2	10	3	Intolerable

Fuente: Autoría propia

Tabla 10. Estimación del riesgo activo switch Alcatel lucent 9545

ACTIVO TI	**SWITCH ALCATEL LUCENT 9545**
ADMINISTRADOR	PIMIENTO CARDENAS WILSON MAURICIO
DEGRADACIÓN	60%
IMPACTO	5
TIPO DE ACTIVO	HARDWARE

Tipo	ID	Amenaza	Exposición/Vulnerabilidad	RIESGO ACTUAL				
							3.04	Intolerable
				Frecuencia (F)		**R**	**NR**	
DESASTRES NATURALES	**N.1**	Fuego	No existe sistema de alarma contra incendios. Se posee un solo extintor de solkaflam (clase c) recomendados para incendios en lugares donde se encuentren equipos eléctricos.	Muy baja	2	10	3	Intolerable
	N.2	Daños por agua	La infraestructura está expuesta a goteras, cuenta con averías en el techo en donde el agua de las lluvias	Muy baja	2	10	3	Intolerable
	N.*	Desastres naturales	La oficina de la dependencia de sistemas se encuentra en zona baja de riesgo de desastre natural de origen volcánico debido a su cercanía con el volcán nevado del Tolima.	Raro	1	5	2	Tolerable

Tabla 10. Estimación del riesgo activo switch Alcatel lucent 9545. (Continuación)

DE ORIGEN INDUSTRIAL	**I.1**	Fuego	No existe sistema de alarma contra incendios. Se posee un solo extintor de solkaflam (clase c) recomendados para incendios en lugares donde se encuentren equipos eléctricos.	Muy baja	2	10	3	Intolerable
	I.2	Daños por agua	La concentración del líquido sobrante por parte del aire acondicionado causaría daños en los equipos.	Muy baja	2	10	3	Intolerable
	I.*	Desastres industriales	No hay exposición o vulnerabilidad, por parte de esta amenaza.	Muy baja	2	10	3	Intolerable
	I.3	Contaminación mecánica	No hay exposición o vulnerabilidad, por parte de esta amenaza.	Muy baja	2	10	3	Intolerable
	I.4	Contaminación electromagnética	No hay exposición o vulnerabilidad, por parte de esta amenaza.	Muy baja	2	10	3	Intolerable
	I.5	Avería de origen físico o lógico	La manipulación por parte de cada uno de los componentes encontrados en la dependencia, como también por defectos de los componentes desde fabrica	Muy baja	2	10	3	Intolerable

Tabla 10. Estimación del riesgo activo switch Alcatel lucent 9545. (Continuación)

	I.6	Corte del suministro eléctrico	Amenaza debida a factores externos, a clemencias de tipo naturales como lluvias u otros.	Muy baja	2	10	3	Intolerable
	I.7	Condiciones inadecuadas de temperatura o humedad	No se cuenta con una infraestructura adecuada para soportar los defectos del sistema de refrigeración.	Muy baja	2	10	3	Intolerable
	I.11	Emanaciones electromagnéticas	No hay exposición o vulnerabilidad, por parte de esta amenaza.	Muy baja	2	10	3	Intolerable
ERRORES Y FALLOS NO INTENCIONADOS	**E.2**	Errores del administrador	Pérdida total o parcial del tiempo de ejecución de sus actividades, dependiendo de la gravedad del asunto.	Muy baja	2	10	3	Intolerable
	E.23	Errores de mantenimiento / actualización de equipos(hardware)	Perjuicio a la mantenibilidad del sistema de información.	Muy baja	2	10	3	Intolerable
	E.24	Caída del sistema por agotamiento de recursos	Saturación del sistema informático.	Muy baja	2	10	3	Intolerable
	E.25	Perdida de equipos (Robo)	Recuperación de soportes reciclados o desechados.	Muy baja	2	10	3	Intolerable

Tabla 10. Estimación del riesgo activo switch Alcatel lucent 9545. (Continuación)

ATAQUES INTENCIONADOS	**A.6**	Abuso de privilegios de acceso	Abuso de cada uno de los derechos otorgados.	Muy baja	2	10	3	Intolerable
	A.7	Uso no previsto	Implementación de recursos (económicos y de tiempo) en actividades no relacionadas.	Muy baja	2	10	3	Intolerable
	A.11	Acceso no autorizado	Uso ilícito del hardware	Muy baja	2	10	3	Intolerable
	A.23	Manipulación de los equipos	Sabotaje del hardware y software conteniente.	Muy baja	2	10	3	Intolerable
	A.24	Denegación de servicio	Saturación del sistema de información.	Muy baja	2	10	3	Intolerable
	A.25	Robo	Robo de porte de la información, puede esta ser física o digital.	Muy baja	2	10	3	Intolerable
	A.26	Ataque destructivo	Destrucción de los contenedores de la información, en recipientes físicos y lógicos.	Muy baja	2	10	3	Intolerable

Fuente: Autoría propia

Tabla 11. Estimación del riesgo activo switch Alcatel lucent 9548

ACTIVO TI	**SWITCH ALCATEL LUCENT 9548**
ADMINISTRADOR	PIMIENTO CARDENAS WILSON MAURICIO
DEGRADACIÓN	60%
IMPACTO	5

Tabla 11. Estimación del riesgo activo switch Alcatel lucent 9548. (Continuación)

TIPO DE ACTIVO		HARDWARE						
Tipo	**ID**	**Amenaza**	**Exposición/Vulnerabilidad**	**RIESGO ACTUAL**				
							3.04	Intolerable
				Frecuencia (F)		**R**	**NR**	
DESASTRES NATURALES	**N.1**	Fuego	No existe sistema de alarma contra incendios. Se posee un solo extintor de solkaflam (clase c) recomendados para incendios en lugares donde se encuentren equipos eléctricos.	Muy baja	2	10	3	Intolerable
	N.2	Daños por agua	La infraestructura está expuesta a goteras, cuenta con averías en el techo en donde el agua de las lluvias	Muy baja	2	10	3	Intolerable
	N.*	Desastres naturales	La oficina de la dependencia de sistemas se encuentra en zona baja de riesgo de desastre natural de origen volcánico debido a su cercanía con el volcán nevado del Tolima.	Raro	1	5	2	Tolerable
DE ORIGEN INDUSTRIAL	**I.1**	Fuego	No existe sistema de alarma contra incendios. Se posee un solo extintor de solkaflam (clase c) recomendados para incendios en lugares donde se encuentren equipos eléctricos.	Muy baja	2	10	3	Intolerable

Tabla 11. Estimación del riesgo activo switch Alcatel lucent 9548. (Continuación)

	I.2	Daños por agua	La concentración del líquido sobrante por parte del aire acondicionado causaría daños en los equipos.	Muy baja	2	10	3	Intolerable
	I.*	Desastres industriales	No hay exposición o vulnerabilidad, por parte de esta amenaza.	Muy baja	2	10	3	Intolerable
	I.3	Contaminación mecánica	No hay exposición o vulnerabilidad, por parte de esta amenaza.	Muy baja	2	10	3	Intolerable
	I.4	Contaminación electromagnética	No hay exposición o vulnerabilidad, por parte de esta amenaza.	Muy baja	2	10	3	Intolerable
	I.5	Avería de origen físico o lógico	La manipulación por parte de cada uno de los componentes encontrados en la dependencia, como también por defectos de los componentes desde fabrica	Muy baja	2	10	3	Intolerable
	I.6	Corte del suministro eléctrico	Amenaza debida a factores externos, a clemencias de tipo naturales como lluvias u otros.	Muy baja	2	10	3	Intolerable
	I.7	Condiciones inadecuadas de temperatura o humedad	No se cuenta con una infraestructura adecuada para soportar los defectos del sistema de refrigeración.	Muy baja	2	10	3	Intolerable

Tabla 11. Estimación del riesgo activo switch Alcatel lucent 9548. (Continuación)

	I.11	Emanaciones electromagnéticas	No hay exposición o vulnerabilidad, por parte de esta amenaza.	Muy baja	2	10	3	Intolerable
ERRORES Y FALLOS NO INTENCIONADOS	**E.2**	Errores del administrador	Pérdida total o parcial del tiempo de ejecución de sus actividades, dependiendo de la gravedad del asunto.	Muy baja	2	10	3	Intolerable
	E.23	Errores de mantenimiento / actualización de equipos(hardware)	Perjuicio a la mantenibilidad del sistema de información.	Muy baja	2	10	3	Intolerable
	E.24	Caída del sistema por agotamiento de recursos	Saturación del sistema informático.	Muy baja	2	10	3	Intolerable
	E.25	Perdida de equipos (Robo)	Recuperación de soportes reciclados o desechados.	Muy baja	2	10	3	Intolerable
ATAQUES INTENCIONADOS	**A.6**	Abuso de privilegios de acceso	Abuso de cada uno de los derechos otorgados.	Muy baja	2	10	3	Intolerable
	A.7	Uso no previsto	Implementación de recursos (económicos y de tiempo) en actividades no relacionadas.	Muy baja	2	10	3	Intolerable
	A.11	Acceso no autorizado	Uso ilícito del hardware	Muy baja	2	10	3	Intolerable

Tabla 11. Estimación del riesgo activo switch Alcatel lucent 9548. (Continuación)

	A.23	Manipulación de los equipos	Sabotaje del hardware y software conteniente.	Muy baja	2	10	3	Intolerable
	A.24	Denegación de servicio	Saturación del sistema de información.	Muy baja	2	10	3	Intolerable
	A.25	Robo	Robo de porte de la información, puede esta ser física o digital.	Muy baja	2	10	3	Intolerable
	A.26	Ataque destructivo	Destrucción de los contenedores de la información, en recipientes físicos y lógicos.	Muy baja	2	10	3	Intolerable

Fuente: Autoría propia

Tabla 12. Estimación del riesgo activo switch Alcatel lucent 9550

ACTIVO TI	**SWITCH ALCATEL LUCENT 9550**							
ADMINISTRADOR	PIMIENTO CARDENAS WILSON MAURICIO							
DEGRADACIÓN	60%							
IMPACTO	5							
TIPO DE ACTIVO	HARDWARE							
Tipo	**ID**	**Amenaza**	**Exposición/Vulnerabilidad**	**RIESGO ACTUAL**				
							3.04	Intolerable
				Frecuencia (F)		**R**	**NR**	
DESASTRES NATURA	**N.1**	Fuego	No existe sistema de alarma contra incendios. Se posee un solo extintor de solkaflam (clase c) recomendados para incendios en	Muy baja	2	10	3	Intolerable

Tabla 12. Estimación del riesgo activo switch Alcatel lucent 9550. (Continuación)

			lugares donde se encuentren equipos eléctricos.					
	N.2	Daños por agua	La infraestructura está expuesta a goteras, cuenta con averías en el techo en donde el agua de las lluvias	Muy baja	2	10	3	Intolerable
	N.*	Desastres naturales	La oficina de la dependencia de sistemas se encuentra en zona baja de riesgo de desastre natural de origen volcánico debido a su cercanía con el volcán nevado del Tolima.	Raro	1	5	2	Tolerable
DE ORIGEN INDUSTRIAL	**I.1**	Fuego	No existe sistema de alarma contra incendios. Se posee un solo extintor de solkaflam (clase c) recomendados para incendios en lugares donde se encuentren equipos eléctricos.	Muy baja	2	10	3	Intolerable
	I.2	Daños por agua	La concentración del líquido sobrante por parte del aire acondicionado causaría daños en los equipos.	Muy baja	2	10	3	Intolerable
	I.*	Desastres industriales	No hay exposición o vulnerabilidad, por parte de esta amenaza.	Muy baja	2	10	3	Intolerable

Tabla 12. Estimación del riesgo activo switch Alcatel lucent 9550. (Continuación)

	I.3	Contaminación mecánica	No hay exposición o vulnerabilidad, por parte de esta amenaza.	Muy baja	2	10	3	Intolerable
	I.4	Contaminación electromagnética	No hay exposición o vulnerabilidad, por parte de esta amenaza.	Muy baja	2	10	3	Intolerable
	I.5	Avería de origen físico o lógico	La manipulación por parte de cada uno de los componentes encontrados en la dependencia, como también por defectos de los componentes desde fabrica	Muy baja	2	10	3	Intolerable
	I.6	Corte del suministro eléctrico	Amenaza debida a factores externos, a clemencias de tipo naturales como lluvias u otros.	Muy baja	2	10	3	Intolerable
	I.7	Condiciones inadecuadas de temperatura o humedad	No se cuenta con una infraestructura adecuada para soportar los defectos del sistema de refrigeración.	Muy baja	2	10	3	Intolerable
	I.11	Emanaciones electromagnéticas	No hay exposición o vulnerabilidad, por parte de esta amenaza.	Muy baja	2	10	3	Intolerable
ERRORES Y FALLOS NO	**E.2**	Errores del administrador	Pérdida total o parcial del tiempo de ejecución de sus actividades, dependiendo de la gravedad del asunto.	Muy baja	2	10	3	Intolerable

Tabla 12. Estimación del riesgo activo switch Alcatel lucent 9550. (Continuación)

	E.23	Errores de mantenimiento / actualización de equipos(hardware)	Perjuicio a la mantenibilidad del sistema de información.	Muy baja	2	10	3	Intolerable
	E.24	Caída del sistema por agotamiento de recursos	Saturación del sistema informático.	Muy baja	2	10	3	Intolerable
	E.25	Perdida de equipos (Robo)	Recuperación de soportes reciclados o desechados.	Muy baja	2	10	3	Intolerable
ATAQUES INTENCIONADOS	**A.6**	Abuso de privilegios de acceso	Abuso de cada uno de los derechos otorgados.	Muy baja	2	10	3	Intolerable
	A.7	Uso no previsto	Implementación de recursos (económicos y de tiempo) en actividades no relacionadas.	Muy baja	2	10	3	Intolerable
	A.11	Acceso no autorizado	Uso ilícito del hardware	Muy baja	2	10	3	Intolerable
	A.23	Manipulación de los equipos	Sabotaje del hardware y software conteniente.	Muy baja	2	10	3	Intolerable
	A.24	Denegación de servicio	Saturación del sistema de información.	Muy baja	2	10	3	Intolerable

Tabla 12. Estimación del riesgo activo switch Alcatel lucent 9550. (Continuación)

	A.25	Robo	Robo de porte de la información, puede esta ser física o digital.	Muy baja	2	10	3	Intolerable
	A.26	Ataque destructivo	Destrucción de los contenedores de la información, en recipientes físicos y lógicos.	Muy baja	2	10	3	Intolerable

Fuente: Autoría propia

Tabla 13. Estimación del riesgo activo switch Alcatel lucent 9551

ACTIVO TI	**SWITCH ALCATEL LUCENT 9551**							
ADMINISTRADOR	PIMIENTO CARDENAS WILSON MAURICIO							
DEGRADACIÓN	60%							
IMPACTO	5							
TIPO DE ACTIVO	HARDWARE							
Tipo	**ID**	**Amenaza**	**Exposición/Vulnerabilidad**	**RIESGO ACTUAL**				
							3.04	Intolerable
				Frecuencia (F)		**R**	**NR**	
DESASTRES NATURALES	**N.1**	Fuego	No existe sistema de alarma contra incendios. Se posee un solo extintor de solkaflam (clase c) recomendados para incendios en lugares donde se encuentren equipos eléctricos.	Muy baja	2	10	3	Intolerable
	N.2	Daños por agua	La infraestructura está expuesta a goteras, cuenta con averías en el techo en donde el agua de las lluvias	Muy baja	2	10	3	Intolerable

Tabla 13. Estimación del riesgo activo switch Alcatel lucent 9551. (Continuación)

	N.*	Desastres naturales	La oficina de la dependencia de sistemas se encuentra en zona baja de riesgo de desastre natural de origen volcánico debido a su cercanía con el volcán nevado del Tolima.	Raro	1	5	2	Tolerable
DE ORIGEN INDUSTRIAL	**I.1**	Fuego	No existe sistema de alarma contra incendios. Se posee un solo extintor de solkaflam (clase c) recomendados para incendios en lugares donde se encuentren equipos eléctricos.	Muy baja	2	10	3	Intolerable
	I.2	Daños por agua	La concentración del líquido sobrante por parte del aire acondicionado causaría daños en los equipos.	Muy baja	2	10	3	Intolerable
	I.*	Desastres industriales	No hay exposición o vulnerabilidad, por parte de esta amenaza.	Muy baja	2	10	3	Intolerable
	I.3	Contaminación mecánica	No hay exposición o vulnerabilidad, por parte de esta amenaza.	Muy baja	2	10	3	Intolerable
	I.4	Contaminación electromagnética	No hay exposición o vulnerabilidad, por parte de esta amenaza.	Muy baja	2	10	3	Intolerable

Tabla 13. Estimación del riesgo activo switch Alcatel lucent 9551. (Continuación)

	I.5	Avería de origen físico o lógico	La manipulación por parte de cada uno de los componentes encontrados en la dependencia, como también por defectos de los componentes desde fabrica	Muy baja	2	10	3	Intolerable
	I.6	Corte del suministro eléctrico	Amenaza debida a factores externos, a clemencias de tipo naturales como lluvias u otros.	Muy baja	2	10	3	Intolerable
	I.7	Condiciones inadecuadas de temperatura o humedad	No se cuenta con una infraestructura adecuada para soportar los defectos del sistema de refrigeración.	Muy baja	2	10	3	Intolerable
	I.11	Emanaciones electromagnéticas	No hay exposición o vulnerabilidad, por parte de esta amenaza.	Muy baja	2	10	3	Intolerable
ERRORES Y FALLOS NO INTENCIONADOS	**E.2**	Errores del administrador	Pérdida total o parcial del tiempo de ejecución de sus actividades, dependiendo de la gravedad del asunto.	Muy baja	2	10	3	Intolerable
	E.23	Errores de mantenimiento / actualización de equipos(hardware)	Perjuicio a la mantenibilidad del sistema de información.	Muy baja	2	10	3	Intolerable

Tabla 13. Estimación del riesgo activo switch Alcatel lucent 9551. (Continuación)

	E.24	Caída del sistema por agotamiento de recursos	Saturación del sistema informático.	Muy baja	2	10	3	Intolerable
	E.25	Perdida de equipos (Robo)	Recuperación de soportes reciclados o desechados.	Muy baja	2	10	3	Intolerable
ATAQUES INTENCIONADOS	**A.6**	Abuso de privilegios de acceso	Abuso de cada uno de los derechos otorgados.	Muy baja	2	10	3	Intolerable
	A.7	Uso no previsto	Implementación de recursos (económicos y de tiempo) en actividades no relacionadas.	Muy baja	2	10	3	Intolerable
	A.11	Acceso no autorizado	Uso ilícito del hardware	Muy baja	2	10	3	Intolerable
	A.23	Manipulación de los equipos	Sabotaje del hardware y software conteniente.	Muy baja	2	10	3	Intolerable
	A.24	Denegación de servicio	Saturación del sistema de información.	Muy baja	2	10	3	Intolerable
	A.25	Robo	Robo de porte de la información, puede esta ser física o digital.	Muy baja	2	10	3	Intolerable
	A.26	Ataque destructivo	Destrucción de los contenedores de la información, en recipientes físicos y lógicos.	Muy baja	2	10	3	Intolerable

Fuente: Autoría propia

Tabla 14. Estimación del riesgo activo switch Alcatel lucent 9552

ACTIVO TI	**SWITCH ALCATEL LUCENT 9552**
ADMINISTRADOR	PIMIENTO CARDENAS WILSON MAURICIO
DEGRADACIÓN	60%
IMPACTO	5
TIPO DE ACTIVO	HARDWARE

Tipo	ID	Amenaza	Exposición/Vulnerabilidad	RIESGO ACTUAL				
							3.04	Intolerable
				Frecuencia (F)		**R**	**NR**	
DESASTRES NATURALES	**N.1**	Fuego	No existe sistema de alarma contra incendios. Se posee un solo extintor de solkaflam (clase c) recomendados para incendios en lugares donde se encuentren equipos eléctricos.	Muy baja	2	10	3	Intolerable
	N.2	Daños por agua	La infraestructura está expuesta a goteras, cuenta con averías en el techo en donde el agua de las lluvias	Muy baja	2	10	3	Intolerable
	N.*	Desastres naturales	La oficina de la dependencia de sistemas se encuentra en zona baja de riesgo de desastre natural de origen volcánico debido a su cercanía con el volcán nevado del Tolima.	Raro	1	5	2	Tolerable

Tabla 14. Estimación del riesgo activo switch Alcatel lucent 9552. (Continuación)

DE ORIGEN INDUSTRIAL	**I.1**	Fuego	No existe sistema de alarma contra incendios. Se posee un solo extintor de solkaflam (clase c) recomendados para incendios en lugares donde se encuentren equipos eléctricos.	Muy baja	2	10	3	Intolerable
	I.2	Daños por agua	La concentración del líquido sobrante por parte del aire acondicionado causaría daños en los equipos.	Muy baja	2	10	3	Intolerable
	I.*	Desastres industriales	No hay exposición o vulnerabilidad, por parte de esta amenaza.	Muy baja	2	10	3	Intolerable
	I.3	Contaminación mecánica	No hay exposición o vulnerabilidad, por parte de esta amenaza.	Muy baja	2	10	3	Intolerable
	I.4	Contaminación electromagnética	No hay exposición o vulnerabilidad, por parte de esta amenaza.	Muy baja	2	10	3	Intolerable
	I.5	Avería de origen físico o lógico	La manipulación por parte de cada uno de los componentes encontrados en la dependencia, como también por defectos de los componentes desde fabrica	Muy baja	2	10	3	Intolerable

Tabla 14. Estimación del riesgo activo switch Alcatel lucent 9552. (Continuación)

	I.6	Corte del suministro eléctrico	Amenaza debida a factores externos, a clemencias de tipo naturales como lluvias u otros.	Muy baja	2	10	3	Intolerable
	I.7	Condiciones inadecuadas de temperatura o humedad	No se cuenta con una infraestructura adecuada para soportar los defectos del sistema de refrigeración.	Muy baja	2	10	3	Intolerable
	I.11	Emanaciones electromagnéticas	No hay exposición o vulnerabilidad, por parte de esta amenaza.	Muy baja	2	10	3	Intolerable
ERRORES Y FALLOS NO INTENCIONADOS	**E.2**	Errores del administrador	Pérdida total o parcial del tiempo de ejecución de sus actividades, dependiendo de la gravedad del asunto.	Muy baja	2	10	3	Intolerable
	E.23	Errores de mantenimiento / actualización de equipos(hardware)	Perjuicio a la mantenibilidad del sistema de información.	Muy baja	2	10	3	Intolerable
	E.24	Caída del sistema por agotamiento de recursos	Saturación del sistema informático.	Muy baja	2	10	3	Intolerable
	E.25	Perdida de equipos (Robo)	Recuperación de soportes reciclados o desechados.	Muy baja	2	10	3	Intolerable

Tabla 14. Estimación del riesgo activo switch Alcatel lucent 9552. (Continuación)

ATAQUES INTENCIONADOS	**A.6**	Abuso de privilegios de acceso	Abuso de cada uno de los derechos otorgados.	Muy baja	2	10	3	Intolerable
	A.7	Uso no previsto	Implementación de recursos (económicos y de tiempo) en actividades no relacionadas.	Muy baja	2	10	3	Intolerable
	A.11	Acceso no autorizado	Uso ilícito del hardware	Muy baja	2	10	3	Intolerable
	A.23	Manipulación de los equipos	Sabotaje del hardware y software conteniente.	Muy baja	2	10	3	Intolerable
	A.24	Denegación de servicio	Saturación del sistema de información.	Muy baja	2	10	3	Intolerable
	A.25	Robo	Robo de porte de la información, puede esta ser física o digital.	Muy baja	2	10	3	Intolerable
	A.26	Ataque destructivo	Destrucción de los contenedores de la información, en recipientes físicos y lógicos.	Muy baja	2	10	3	Intolerable

Fuente: Autoría propia

Tabla 15. Estimación del riesgo activo switch Alcatel lucent 9554

ACTIVO TI	**SWITCH ALCATEL LUCENT 9554**
ADMINISTRADOR	PIMIENTO CARDENAS WILSON MAURICIO
DEGRADACIÓN	60%
IMPACTO	5

Tabla 15. Estimación del riesgo activo switch Alcatel lucent 9554. (Continuación)

TIPO DE ACTIVO		HARDWARE						
Tipo	**ID**	**Amenaza**	**Exposición/Vulnerabilidad**	**RIESGO ACTUAL**				
							3.04	Intolerable
				Frecuencia (F)		**R**	**NR**	
DESASTRES NATURALES	**N.1**	Fuego	No existe sistema de alarma contra incendios. Se posee un solo extintor de solkaflam (clase c) recomendados para incendios en lugares donde se encuentren equipos eléctricos.	Muy baja	2	10	3	Intolerable
	N.2	Daños por agua	La infraestructura está expuesta a goteras, cuenta con averías en el techo en donde el agua de las lluvias	Muy baja	2	10	3	Intolerable
	N.*	Desastres naturales	La oficina de la dependencia de sistemas se encuentra en zona baja de riesgo de desastre natural de origen volcánico debido a su cercanía con el volcán nevado del Tolima.	Raro	1	5	2	Tolerable
DE ORIGEN INDUSTRIAL	**I.1**	Fuego	No existe sistema de alarma contra incendios. Se posee un solo extintor de solkaflam (clase c) recomendados para incendios en lugares donde se encuentren equipos eléctricos.	Muy baja	2	10	3	Intolerable

Tabla 15. Estimación del riesgo activo switch Alcatel lucent 9554. (Continuación)

	I.2	Daños por agua	La concentración del líquido sobrante por parte del aire acondicionado causaría daños en los equipos.	Muy baja	2	10	3	Intolerable
	I.*	Desastres industriales	No hay exposición o vulnerabilidad, por parte de esta amenaza.	Muy baja	2	10	3	Intolerable
	I.3	Contaminación mecánica	No hay exposición o vulnerabilidad, por parte de esta amenaza.	Muy baja	2	10	3	Intolerable
	I.4	Contaminación electromagnética	No hay exposición o vulnerabilidad, por parte de esta amenaza.	Muy baja	2	10	3	Intolerable
	I.5	Avería de origen físico o lógico	La manipulación por parte de cada uno de los componentes encontrados en la dependencia, como también por defectos de los componentes desde fabrica	Muy baja	2	10	3	Intolerable
	I.6	Corte del suministro eléctrico	Amenaza debida a factores externos, a clemencias de tipo naturales como lluvias u otros.	Muy baja	2	10	3	Intolerable
	I.7	Condiciones inadecuadas de temperatura o humedad	No se cuenta con una infraestructura adecuada para soportar los defectos del sistema de refrigeración.	Muy baja	2	10	3	Intolerable

Tabla 15. Estimación del riesgo activo switch Alcatel lucent 9554. (Continuación)

	I.11	Emanaciones electromagnéticas	No hay exposición o vulnerabilidad, por parte de esta amenaza.	Muy baja	2	10	3	Intolerable
ERRORES Y FALLOS NO INTENCIONADOS	**E.2**	Errores del administrador	Pérdida total o parcial del tiempo de ejecución de sus actividades, dependiendo de la gravedad del asunto.	Muy baja	2	10	3	Intolerable
	E.23	Errores de mantenimiento / actualización de equipos(hardware)	Perjuicio a la mantenibilidad del sistema de información.	Muy baja	2	10	3	Intolerable
	E.24	Caída del sistema por agotamiento de recursos	Saturación del sistema informático.	Muy baja	2	10	3	Intolerable
	E.25	Perdida de equipos (Robo)	Recuperación de soportes reciclados o desechados.	Muy baja	2	10	3	Intolerable
ATAQUES INTENCIONADOS	**A.6**	Abuso de privilegios de acceso	Abuso de cada uno de los derechos otorgados.	Muy baja	2	10	3	Intolerable
	A.7	Uso no previsto	Implementación de recursos (económicos y de tiempo) en actividades no relacionadas.	Muy baja	2	10	3	Intolerable
	A.11	Acceso no autorizado	Uso ilícito del hardware	Muy baja	2	10	3	Intolerable

Tabla 15. Estimación del riesgo activo switch Alcatel lucent 9554. (Continuación)

	A.23	Manipulación de los equipos	Sabotaje del hardware y software conteniente.	Muy baja	2	10	3	Intolerable
	A.24	Denegación de servicio	Saturación del sistema de información.	Muy baja	2	10	3	Intolerable
	A.25	Robo	Robo de porte de la información, puede esta ser física o digital.	Muy baja	2	10	3	Intolerable
	A.26	Ataque destructivo	Destrucción de los contenedores de la información, en recipientes físicos y lógicos.	Muy baja	2	10	3	Intolerable

Fuente: Autoría propia

Tabla 16. Estimación del riesgo activo switch Alcatel lucent 9555

ACTIVO TI	**SWITCH ALCATEL LUCENT 9555**							
ADMINISTRADOR	PIMIENTO CARDENAS WILSON MAURICIO							
DEGRADACIÓN	60%							
IMPACTO	5							
TIPO DE ACTIVO	HARDWARE							
Tipo	**ID**	**Amenaza**	**Exposición/Vulnerabilidad**	**RIESGO ACTUAL**				
							3.04	Intolerable
				Frecuencia (F)		**R**	**NR**	
DESASTRES NATURA	**N.1**	Fuego	No existe sistema de alarma contra incendios. Se posee un solo extintor de solkaflam (clase c) recomendados para incendios en	Muy baja	2	10	3	Intolerable

Tabla 16. Estimación del riesgo activo switch Alcatel lucent 9555. (Continuación)

			lugares donde se encuentren equipos eléctricos.					
	N.2	Daños por agua	La infraestructura está expuesta a goteras, cuenta con averías en el techo en donde el agua de las lluvias	Muy baja	2	10	3	Intolerable
	N.*	Desastres naturales	La oficina de la dependencia de sistemas se encuentra en zona baja de riesgo de desastre natural de origen volcánico debido a su cercanía con el volcán nevado del Tolima.	Raro	1	5	2	Tolerable
DE ORIGEN INDUSTRIAL	**I.1**	Fuego	No existe sistema de alarma contra incendios. Se posee un solo extintor de solkaflam (clase c) recomendados para incendios en lugares donde se encuentren equipos eléctricos.	Muy baja	2	10	3	Intolerable
	I.2	Daños por agua	La concentración del líquido sobrante por parte del aire acondicionado causaría daños en los equipos.	Muy baja	2	10	3	Intolerable
	I.*	Desastres industriales	No hay exposición o vulnerabilidad, por parte de esta amenaza.	Muy baja	2	10	3	Intolerable

Tabla 16. Estimación del riesgo activo switch Alcatel lucent 9555. (Continuación)

	I.3	Contaminación mecánica	No hay exposición o vulnerabilidad, por parte de esta amenaza.	Muy baja	2	10	3	Intolerable
	I.4	Contaminación electromagnética	No hay exposición o vulnerabilidad, por parte de esta amenaza.	Muy baja	2	10	3	Intolerable
	I.5	Avería de origen físico o lógico	La manipulación por parte de cada uno de los componentes encontrados en la dependencia, como también por defectos de los componentes desde fabrica	Muy baja	2	10	3	Intolerable
	I.6	Corte del suministro eléctrico	Amenaza debida a factores externos, a clemencias de tipo naturales como lluvias u otros.	Muy baja	2	10	3	Intolerable
	I.7	Condiciones inadecuadas de temperatura o humedad	No se cuenta con una infraestructura adecuada para soportar los defectos del sistema de refrigeración.	Muy baja	2	10	3	Intolerable
	I.11	Emanaciones electromagnéticas	No hay exposición o vulnerabilidad, por parte de esta amenaza.	Muy baja	2	10	3	Intolerable
ERRORES Y FALLOS NO	**E.2**	Errores del administrador	Pérdida total o parcial del tiempo de ejecución de sus actividades, dependiendo de la gravedad del asunto.	Muy baja	2	10	3	Intolerable

Tabla 16. Estimación del riesgo activo switch Alcatel lucent 9555. (Continuación)

	E.23	Errores de mantenimiento / actualización de equipos(hardware)	Perjuicio a la mantenibilidad del sistema de información.	Muy baja	2	10	3	Intolerable
	E.24	Caída del sistema por agotamiento de recursos	Saturación del sistema informático.	Muy baja	2	10	3	Intolerable
	E.25	Perdida de equipos (Robo)	Recuperación de soportes reciclados o desechados.	Muy baja	2	10	3	Intolerable
ATAQUES INTENCIONADOS	**A.6**	Abuso de privilegios de acceso	Abuso de cada uno de los derechos otorgados.	Muy baja	2	10	3	Intolerable
	A.7	Uso no previsto	Implementación de recursos (económicos y de tiempo) en actividades no relacionadas.	Muy baja	2	10	3	Intolerable
	A.11	Acceso no autorizado	Uso ilícito del hardware	Muy baja	2	10	3	Intolerable
	A.23	Manipulación de los equipos	Sabotaje del hardware y software conteniente.	Muy baja	2	10	3	Intolerable
	A.24	Denegación de servicio	Saturación del sistema de información.	Muy baja	2	10	3	Intolerable

Tabla 16. Estimación del riesgo activo switch Alcatel lucent 9555. (Continuación)

	A.25	Robo	Robo de porte de la información, puede esta ser física o digital.	Muy baja	2	10	3	Intolerable
	A.26	Ataque destructivo	Destrucción de los contenedores de la información, en recipientes físicos y lógicos.	Muy baja	2	10	3	Intolerable

Fuente: Autoría propia

Tabla 17. Estimación del riesgo activo switch Alcatel lucent 9560

ACTIVO TI	**SWITCH ALCATEL LUCENT 9560**							
ADMINISTRADOR	PIMIENTO CARDENAS WILSON MAURICIO							
DEGRADACIÓN	60%							
IMPACTO	5							
TIPO DE ACTIVO	HARDWARE							
Tipo	**ID**	**Amenaza**	**Exposición/Vulnerabilidad**	**RIESGO ACTUAL**				
							3.04	Intolerable
				Frecuencia (F)		**R**	**NR**	
DESASTRES NATURALES	**N.1**	Fuego	No existe sistema de alarma contra incendios. Se posee un solo extintor de solkaflam (clase c) recomendados para incendios en lugares donde se encuentren equipos eléctricos.	Muy baja	2	10	3	Intolerable
	N.2	Daños por agua	La infraestructura está expuesta a goteras, cuenta con averías en el techo en donde el agua de las lluvias	Muy baja	2	10	3	Intolerable

Tabla 17. Estimación del riesgo activo switch Alcatel lucent 9560. (Continuación)

	N.*	Desastres naturales	La oficina de la dependencia de sistemas se encuentra en zona baja de riesgo de desastre natural de origen volcánico debido a su cercanía con el volcán nevado del Tolima.	Raro	1	5	2	Tolerable
DE ORIGEN INDUSTRIAL	**I.1**	Fuego	No existe sistema de alarma contra incendios. Se posee un solo extintor de solkaflam (clase c) recomendados para incendios en lugares donde se encuentren equipos eléctricos.	Muy baja	2	10	3	Intolerable
	I.2	Daños por agua	La concentración del líquido sobrante por parte del aire acondicionado causaría daños en los equipos.	Muy baja	2	10	3	Intolerable
	I.*	Desastres industriales	No hay exposición o vulnerabilidad, por parte de esta amenaza.	Muy baja	2	10	3	Intolerable
	I.3	Contaminación mecánica	No hay exposición o vulnerabilidad, por parte de esta amenaza.	Muy baja	2	10	3	Intolerable
	I.4	Contaminación electromagnética	No hay exposición o vulnerabilidad, por parte de esta amenaza.	Muy baja	2	10	3	Intolerable

Tabla 17. Estimación del riesgo activo switch Alcatel lucent 9560. (Continuación)

	I.5	Avería de origen físico o lógico	La manipulación por parte de cada uno de los componentes encontrados en la dependencia, como también por defectos de los componentes desde fabrica	Muy baja	2	10	3	Intolerable
	I.6	Corte del suministro eléctrico	Amenaza debida a factores externos, a clemencias de tipo naturales como lluvias u otros.	Muy baja	2	10	3	Intolerable
	I.7	Condiciones inadecuadas de temperatura o humedad	No se cuenta con una infraestructura adecuada para soportar los defectos del sistema de refrigeración.	Muy baja	2	10	3	Intolerable
	I.11	Emanaciones electromagnéticas	No hay exposición o vulnerabilidad, por parte de esta amenaza.	Muy baja	2	10	3	Intolerable
ERRORES Y FALLOS NO INTENCIONADOS	**E.2**	Errores del administrador	Pérdida total o parcial del tiempo de ejecución de sus actividades, dependiendo de la gravedad del asunto.	Muy baja	2	10	3	Intolerable
	E.23	Errores de mantenimiento / actualización de equipos(hardware)	Perjuicio a la mantenibilidad del sistema de información.	Muy baja	2	10	3	Intolerable

Tabla 17. Estimación del riesgo activo switch Alcatel lucent 9560. (Continuación)

	E.24	Caída del sistema por agotamiento de recursos	Saturación del sistema informático.	Muy baja	2	10	3	Intolerable
	E.25	Perdida de equipos (Robo)	Recuperación de soportes reciclados o desechados.	Muy baja	2	10	3	Intolerable
ATAQUES INTENCIONADOS	**A.6**	Abuso de privilegios de acceso	Abuso de cada uno de los derechos otorgados.	Muy baja	2	10	3	Intolerable
	A.7	Uso no previsto	Implementación de recursos (económicos y de tiempo) en actividades no relacionadas.	Muy baja	2	10	3	Intolerable
	A.11	Acceso no autorizado	Uso ilícito del hardware	Muy baja	2	10	3	Intolerable
	A.23	Manipulación de los equipos	Sabotaje del hardware y software conteniente.	Muy baja	2	10	3	Intolerable
	A.24	Denegación de servicio	Saturación del sistema de información.	Muy baja	2	10	3	Intolerable
	A.25	Robo	Robo de porte de la información, puede esta ser física o digital.	Muy baja	2	10	3	Intolerable
	A.26	Ataque destructivo	Destrucción de los contenedores de la información, en recipientes físicos y lógicos.	Muy baja	2	10	3	Intolerable

Fuente: Autoría propia

Tabla 18. Estimación del riesgo activo switch layer 3 9574

ACTIVO TI	**SWITCH LAYER 3 9574**
ADMINISTRADOR	PIMIENTO CARDENAS WILSON MAURICIO
DEGRADACIÓN	60%
IMPACTO	5
TIPO DE ACTIVO	HARDWARE

Tipo	ID	Amenaza	Exposición/Vulnerabilidad	RIESGO ACTUAL				
							3.04	Intolerable
				Frecuencia (F)		**R**	**NR**	
DESASTRES NATURALES	**N.1**	Fuego	No existe sistema de alarma contra incendios. Se posee un solo extintor de solkaflam (clase c) recomendados para incendios en lugares donde se encuentren equipos eléctricos.	Muy baja	2	10	3	Intolerable
	N.2	Daños por agua	La infraestructura está expuesta a goteras, cuenta con averías en el techo en donde el agua de las lluvias	Muy baja	2	10	3	Intolerable
	N.*	Desastres naturales	La oficina de la dependencia de sistemas se encuentra en zona baja de riesgo de desastre natural de origen volcánico debido a su cercanía con el volcán nevado del Tolima.	Raro	1	5	2	Tolerable

Tabla 18. Estimación del riesgo activo switch layer 3 9574. (Continuación)

DE ORIGEN INDUSTRIAL	**I.1**	Fuego	No existe sistema de alarma contra incendios. Se posee un solo extintor de solkaflam (clase c) recomendados para incendios en lugares donde se encuentren equipos eléctricos.	Muy baja	2	10	3	Intolerable
	I.2	Daños por agua	La concentración del líquido sobrante por parte del aire acondicionado causaría daños en los equipos.	Muy baja	2	10	3	Intolerable
	I.*	Desastres industriales	No hay exposición o vulnerabilidad, por parte de esta amenaza.	Muy baja	2	10	3	Intolerable
	I.3	Contaminación mecánica	No hay exposición o vulnerabilidad, por parte de esta amenaza.	Muy baja	2	10	3	Intolerable
	I.4	Contaminación electromagnética	No hay exposición o vulnerabilidad, por parte de esta amenaza.	Muy baja	2	10	3	Intolerable
	I.5	Avería de origen físico o lógico	La manipulación por parte de cada uno de los componentes encontrados en la dependencia, como también por defectos de los componentes desde fabrica	Muy baja	2	10	3	Intolerable

Tabla 18. Estimación del riesgo activo switch layer 3 9574. (Continuación)

	I.6	Corte del suministro eléctrico	Amenaza debida a factores externos, a clemencias de tipo naturales como lluvias u otros.	Muy baja	2	10	3	Intolerable
	I.7	Condiciones inadecuadas de temperatura o humedad	No se cuenta con una infraestructura adecuada para soportar los defectos del sistema de refrigeración.	Muy baja	2	10	3	Intolerable
	I.11	Emanaciones electromagnéticas	No hay exposición o vulnerabilidad, por parte de esta amenaza.	Muy baja	2	10	3	Intolerable
ERRORES Y FALLOS NO INTENCIONADOS	**E.2**	Errores del administrador	Pérdida total o parcial del tiempo de ejecución de sus actividades, dependiendo de la gravedad del asunto.	Muy baja	2	10	3	Intolerable
	E.23	Errores de mantenimiento / actualización de equipos(hardware)	Perjuicio a la mantenibilidad del sistema de información.	Muy baja	2	10	3	Intolerable
	E.24	Caída del sistema por agotamiento de recursos	Saturación del sistema informático.	Muy baja	2	10	3	Intolerable
	E.25	Perdida de equipos (Robo)	Recuperación de soportes reciclados o desechados.	Muy baja	2	10	3	Intolerable

Tabla 18. Estimación del riesgo activo switch layer 3 9574. (Continuación)

ATAQUES INTENCIONADOS	**A.6**	Abuso de privilegios de acceso	Abuso de cada uno de los derechos otorgados.	Muy baja	2	10	3	Intolerable
	A.7	Uso no previsto	Implementación de recursos (económicos y de tiempo) en actividades no relacionadas.	Muy baja	2	10	3	Intolerable
	A.11	Acceso no autorizado	Uso ilícito del hardware	Muy baja	2	10	3	Intolerable
	A.23	Manipulación de los equipos	Sabotaje del hardware y software conteniente.	Muy baja	2	10	3	Intolerable
	A.24	Denegación de servicio	Saturación del sistema de información.	Muy baja	2	10	3	Intolerable
	A.25	Robo	Robo de porte de la información, puede esta ser física o digital.	Muy baja	2	10	3	Intolerable
	A.26	Ataque destructivo	Destrucción de los contenedores de la información, en recipientes físicos y lógicos.	Muy baja	2	10	3	Intolerable

Fuente: Autoría propia

Tabla 19. Estimación del riesgo activo switch layer 3 9576

ACTIVO TI	**SWITCH LAYER 3 9576**
ADMINISTRADOR	PIMIENTO CARDENAS WILSON MAURICIO
DEGRADACIÓN	60%
IMPACTO	5

Tabla 19. Estimación del riesgo activo switch layer 3 9576. (Continuación)

TIPO DE ACTIVO		HARDWARE						
Tipo	**ID**	**Amenaza**	**Exposición/Vulnerabilidad**	**RIESGO ACTUAL**				
							3.04	Intolerable
				Frecuencia (F)		**R**	**NR**	
DESASTRES NATURALES	**N.1**	Fuego	No existe sistema de alarma contra incendios. Se posee un solo extintor de solkaflam (clase c) recomendados para incendios en lugares donde se encuentren equipos eléctricos.	Muy baja	2	10	3	Intolerable
	N.2	Daños por agua	La infraestructura está expuesta a goteras, cuenta con averías en el techo en donde el agua de las lluvias	Muy baja	2	10	3	Intolerable
	N.*	Desastres naturales	La oficina de la dependencia de sistemas se encuentra en zona baja de riesgo de desastre natural de origen volcánico debido a su cercanía con el volcán nevado del Tolima.	Raro	1	5	2	Tolerable
DE ORIGEN INDUSTRIAL	**I.1**	Fuego	No existe sistema de alarma contra incendios. Se posee un solo extintor de solkaflam (clase c) recomendados para incendios en lugares donde se encuentren equipos eléctricos.	Muy baja	2	10	3	Intolerable

Tabla 19. Estimación del riesgo activo switch layer 3 9576. (Continuación)

	I.2	Daños por agua	La concentración del líquido sobrante por parte del aire acondicionado causaría daños en los equipos.	Muy baja	2	10	3	Intolerable
	I.*	Desastres industriales	No hay exposición o vulnerabilidad, por parte de esta amenaza.	Muy baja	2	10	3	Intolerable
	I.3	Contaminación mecánica	No hay exposición o vulnerabilidad, por parte de esta amenaza.	Muy baja	2	10	3	Intolerable
	I.4	Contaminación electromagnética	No hay exposición o vulnerabilidad, por parte de esta amenaza.	Muy baja	2	10	3	Intolerable
	I.5	Avería de origen físico o lógico	La manipulación por parte de cada uno de los componentes encontrados en la dependencia, como también por defectos de los componentes desde fabrica	Muy baja	2	10	3	Intolerable
	I.6	Corte del suministro eléctrico	Amenaza debida a factores externos, a clemencias de tipo naturales como lluvias u otros.	Muy baja	2	10	3	Intolerable
	I.7	Condiciones inadecuadas de temperatura o humedad	No se cuenta con una infraestructura adecuada para soportar los defectos del sistema de refrigeración.	Muy baja	2	10	3	Intolerable

Tabla 19. Estimación del riesgo activo switch layer 3 9576. (Continuación)

	I.11	Emanaciones electromagnéticas	No hay exposición o vulnerabilidad, por parte de esta amenaza.	Muy baja	2	10	3	Intolerable
ERRORES Y FALLOS NO INTENCIONADOS	**E.2**	Errores del administrador	Pérdida total o parcial del tiempo de ejecución de sus actividades, dependiendo de la gravedad del asunto.	Muy baja	2	10	3	Intolerable
	E.23	Errores de mantenimiento / actualización de equipos(hardware)	Perjuicio a la mantenibilidad del sistema de información.	Muy baja	2	10	3	Intolerable
	E.24	Caída del sistema por agotamiento de recursos	Saturación del sistema informático.	Muy baja	2	10	3	Intolerable
	E.25	Perdida de equipos (Robo)	Recuperación de soportes reciclados o desechados.	Muy baja	2	10	3	Intolerable
ATAQUES INTENCIONADOS	**A.6**	Abuso de privilegios de acceso	Abuso de cada uno de los derechos otorgados.	Muy baja	2	10	3	Intolerable
	A.7	Uso no previsto	Implementación de recursos (económicos y de tiempo) en actividades no relacionadas.	Muy baja	2	10	3	Intolerable
	A.11	Acceso no autorizado	Uso ilícito del hardware	Muy baja	2	10	3	Intolerable

Tabla 19. Estimación del riesgo activo switch layer 3 9576. (Continuación)

	A.23	Manipulación de los equipos	Sabotaje del hardware y software conteniente.	Muy baja	2	10	3	Intolerable
	A.24	Denegación de servicio	Saturación del sistema de información.	Muy baja	2	10	3	Intolerable
	A.25	Robo	Robo de porte de la información, puede esta ser física o digital.	Muy baja	2	10	3	Intolerable
	A.26	Ataque destructivo	Destrucción de los contenedores de la información, en recipientes físicos y lógicos.	Muy baja	2	10	3	Intolerable

Fuente: Autoría propia

Tabla 20. Estimación del riesgo activo switch layer 3 9577

ACTIVO TI	**SWITCH LAYER 3 9577**							
ADMINISTRADOR	PIMIENTO CARDENAS WILSON MAURICIO							
DEGRADACIÓN	60%							
IMPACTO	5							
TIPO DE ACTIVO	HARDWARE							
Tipo	**ID**	**Amenaza**	**Exposición/Vulnerabilidad**	**RIESGO ACTUAL**				
							3.04	Intolerable
				Frecuencia (F)		**R**	**NR**	
DESASTRES NATURA	**N.1**	Fuego	No existe sistema de alarma contra incendios. Se posee un solo extintor de solkaflam (clase c) recomendados para incendios en	Muy baja	2	10	3	Intolerable

Tabla 20. Estimación del riesgo activo switch layer 3 9577. (Continuación)

			lugares donde se encuentren equipos eléctricos.					
	N.2	Daños por agua	La infraestructura está expuesta a goteras, cuenta con averías en el techo en donde el agua de las lluvias	Muy baja	2	10	3	Intolerable
	N.*	Desastres naturales	La oficina de la dependencia de sistemas se encuentra en zona baja de riesgo de desastre natural de origen volcánico debido a su cercanía con el volcán nevado del Tolima.	Raro	1	5	2	Tolerable
DE ORIGEN INDUSTRIAL	**I.1**	Fuego	No existe sistema de alarma contra incendios. Se posee un solo extintor de solkaflam (clase c) recomendados para incendios en lugares donde se encuentren equipos eléctricos.	Muy baja	2	10	3	Intolerable
	I.2	Daños por agua	La concentración del líquido sobrante por parte del aire acondicionado causaría daños en los equipos.	Muy baja	2	10	3	Intolerable
	I.*	Desastres industriales	No hay exposición o vulnerabilidad, por parte de esta amenaza.	Muy baja	2	10	3	Intolerable

Tabla 20. Estimación del riesgo activo switch layer 3 9577. (Continuación)

	I.3	Contaminación mecánica	No hay exposición o vulnerabilidad, por parte de esta amenaza.	Muy baja	2	10	3	Intolerable
	I.4	Contaminación electromagnética	No hay exposición o vulnerabilidad, por parte de esta amenaza.	Muy baja	2	10	3	Intolerable
	I.5	Avería de origen físico o lógico	La manipulación por parte de cada uno de los componentes encontrados en la dependencia, como también por defectos de los componentes desde fabrica	Muy baja	2	10	3	Intolerable
	I.6	Corte del suministro eléctrico	Amenaza debida a factores externos, a clemencias de tipo naturales como lluvias u otros.	Muy baja	2	10	3	Intolerable
	I.7	Condiciones inadecuadas de temperatura o humedad	No se cuenta con una infraestructura adecuada para soportar los defectos del sistema de refrigeración.	Muy baja	2	10	3	Intolerable
	I.11	Emanaciones electromagnéticas	No hay exposición o vulnerabilidad, por parte de esta amenaza.	Muy baja	2	10	3	Intolerable
ERRORES Y FALLOS NO	**E.2**	Errores del administrador	Pérdida total o parcial del tiempo de ejecución de sus actividades, dependiendo de la gravedad del asunto.	Muy baja	2	10	3	Intolerable

Tabla 20. Estimación del riesgo activo switch layer 3 9577. (Continuación)

	E.23	Errores de mantenimiento / actualización de equipos(hardware)	Perjuicio a la mantenibilidad del sistema de información.	Muy baja	2	10	3	Intolerable
	E.24	Caída del sistema por agotamiento de recursos	Saturación del sistema informático.	Muy baja	2	10	3	Intolerable
	E.25	Perdida de equipos (Robo)	Recuperación de soportes reciclados o desechados.	Muy baja	2	10	3	Intolerable
ATAQUES INTENCIONADOS	**A.6**	Abuso de privilegios de acceso	Abuso de cada uno de los derechos otorgados.	Muy baja	2	10	3	Intolerable
	A.7	Uso no previsto	Implementación de recursos (económicos y de tiempo) en actividades no relacionadas.	Muy baja	2	10	3	Intolerable
	A.11	Acceso no autorizado	Uso ilícito del hardware	Muy baja	2	10	3	Intolerable
	A.23	Manipulación de los equipos	Sabotaje del hardware y software conteniente.	Muy baja	2	10	3	Intolerable
	A.24	Denegación de servicio	Saturación del sistema de información.	Muy baja	2	10	3	Intolerable

Tabla 20. Estimación del riesgo activo switch layer 3 9577. (Continuación)

	A.25	Robo	Robo de porte de la información, puede esta ser física o digital.	Muy baja	2	10	3	Intolerable
	A.26	Ataque destructivo	Destrucción de los contenedores de la información, en recipientes físicos y lógicos.	Muy baja	2	10	3	Intolerable

Fuente: Autoría propia

Tabla 21. Estimación del riesgo activo switch layer 3 9575

ACTIVO TI	**SWITCH LAYER 3 9575**
ADMINISTRADOR	PIMIENTO CARDENAS WILSON MAURICIO
DEGRADACIÓN	60%
IMPACTO	5
TIPO DE ACTIVO	HARDWARE

Tipo	**ID**	**Amenaza**	**Exposición/Vulnerabilidad**	**RIESGO ACTUAL**				
							3.04	Intolerable
				Frecuencia (F)		**R**	**NR**	
DESASTRES NATURALES	**N.1**	Fuego	No existe sistema de alarma contra incendios. Se posee un solo extintor de solkaflam (clase c) recomendados para incendios en lugares donde se encuentren equipos eléctricos.	Muy baja	2	10	3	Intolerable
	N.2	Daños por agua	La infraestructura está expuesta a goteras, cuenta con averías en el techo en donde el agua de las lluvias	Muy baja	2	10	3	Intolerable

Tabla 21. Estimación del riesgo activo switch layer 3 9575. (Continuación)

	N.*	Desastres naturales	La oficina de la dependencia de sistemas se encuentra en zona baja de riesgo de desastre natural de origen volcánico debido a su cercanía con el volcán nevado del Tolima.	Raro	1	5	2	Tolerable
DE ORIGEN INDUSTRIAL	**I.1**	Fuego	No existe sistema de alarma contra incendios. Se posee un solo extintor de solkaflam (clase c) recomendados para incendios en lugares donde se encuentren equipos eléctricos.	Muy baja	2	10	3	Intolerable
	I.2	Daños por agua	La concentración del líquido sobrante por parte del aire acondicionado causaría daños en los equipos.	Muy baja	2	10	3	Intolerable
	I.*	Desastres industriales	No hay exposición o vulnerabilidad, por parte de esta amenaza.	Muy baja	2	10	3	Intolerable
	I.3	Contaminación mecánica	No hay exposición o vulnerabilidad, por parte de esta amenaza.	Muy baja	2	10	3	Intolerable
	I.4	Contaminación electromagnética	No hay exposición o vulnerabilidad, por parte de esta amenaza.	Muy baja	2	10	3	Intolerable

Tabla 21. Estimación del riesgo activo switch layer 3 9575. (Continuación)

	I.5	Avería de origen físico o lógico	La manipulación por parte de cada uno de los componentes encontrados en la dependencia, como también por defectos de los componentes desde fabrica	Muy baja	2	10	3	Intolerable
	I.6	Corte del suministro eléctrico	Amenaza debida a factores externos, a clemencias de tipo naturales como lluvias u otros.	Muy baja	2	10	3	Intolerable
	I.7	Condiciones inadecuadas de temperatura o humedad	No se cuenta con una infraestructura adecuada para soportar los defectos del sistema de refrigeración.	Muy baja	2	10	3	Intolerable
	I.11	Emanaciones electromagnéticas	No hay exposición o vulnerabilidad, por parte de esta amenaza.	Muy baja	2	10	3	Intolerable
ERRORES Y FALLOS NO INTENCIONADOS	**E.2**	Errores del administrador	Pérdida total o parcial del tiempo de ejecución de sus actividades, dependiendo de la gravedad del asunto.	Muy baja	2	10	3	Intolerable
	E.23	Errores de mantenimiento / actualización de equipos(hardware)	Perjuicio a la mantenibilidad del sistema de información.	Muy baja	2	10	3	Intolerable

Tabla 21. Estimación del riesgo activo switch layer 3 9575. (Continuación)

	E.24	Caída del sistema por agotamiento de recursos	Saturación del sistema informático.	Muy baja	2	10	3	Intolerable
	E.25	Perdida de equipos (Robo)	Recuperación de soportes reciclados o desechados.	Muy baja	2	10	3	Intolerable
ATAQUES INTENCIONADOS	**A.6**	Abuso de privilegios de acceso	Abuso de cada uno de los derechos otorgados.	Muy baja	2	10	3	Intolerable
	A.7	Uso no previsto	Implementación de recursos (económicos y de tiempo) en actividades no relacionadas.	Muy baja	2	10	3	Intolerable
	A.11	Acceso no autorizado	Uso ilícito del hardware	Muy baja	2	10	3	Intolerable
	A.23	Manipulación de los equipos	Sabotaje del hardware y software conteniente.	Muy baja	2	10	3	Intolerable
	A.24	Denegación de servicio	Saturación del sistema de información.	Muy baja	2	10	3	Intolerable
	A.25	Robo	Robo de porte de la información, puede esta ser física o digital.	Muy baja	2	10	3	Intolerable
	A.26	Ataque destructivo	Destrucción de los contenedores de la información, en recipientes físicos y lógicos.	Muy baja	2	10	3	Intolerable

Fuente: Autoría propia

Tabla 22. Estimación del riesgo activo router cisco modelo 1800 4781

ACTIVO TI	**ROUTER CISCO MODELO 1800 4781**							
ADMINISTRADOR	PIMIENTO CARDENAS WILSON MAURICIO							
DEGRADACIÓN	70%							
IMPACTO	5							
TIPO DE ACTIVO	HARDWARE							
Tipo	**ID**	**Amenaza**	**Exposición/Vulnerabilidad**	**RIESGO ACTUAL**				
							3.04	Intolerable
				Frecuencia (F)		**R**	**NR**	
DESASTRES NATURALES	**N.1**	Fuego	No existe sistema de alarma contra incendios. Se posee un solo extintor de solkaflam (clase c) recomendados para incendios en lugares donde se encuentren equipos eléctricos.	Muy baja	2	10	3	Intolerable
	N.2	Daños por agua	La infraestructura está expuesta a goteras, cuenta con averías en el techo en donde el agua de las lluvias	Muy baja	2	10	3	Intolerable
	N.*	Desastres naturales	La oficina de la dependencia de sistemas se encuentra en zona baja de riesgo de desastre natural de origen volcánico debido a su cercanía con el volcán nevado del Tolima.	Raro	1	5	2	Tolerable

Tabla 22. Estimación del riesgo activo router cisco modelo 1800 4781. (Continuación)

DE ORIGEN INDUSTRIAL	**I.1**	Fuego	No existe sistema de alarma contra incendios. Se posee un solo extintor de solkaflam (clase c) recomendados para incendios en lugares donde se encuentren equipos eléctricos.	Muy baja	2	10	3	Intolerable
	I.2	Daños por agua	La concentración del líquido sobrante por parte del aire acondicionado causaría daños en los equipos.	Muy baja	2	10	3	Intolerable
	I.*	Desastres industriales	No hay exposición o vulnerabilidad, por parte de esta amenaza.	Muy baja	2	10	3	Intolerable
	I.3	Contaminación mecánica	No hay exposición o vulnerabilidad, por parte de esta amenaza.	Muy baja	2	10	3	Intolerable
	I.4	Contaminación electromagnética	No hay exposición o vulnerabilidad, por parte de esta amenaza.	Muy baja	2	10	3	Intolerable
	I.5	Avería de origen físico o lógico	La manipulación por parte de cada uno de los componentes encontrados en la dependencia, como también por defectos de los componentes desde fabrica	Muy baja	2	10	3	Intolerable

Tabla 22. Estimación del riesgo activo router cisco modelo 1800 4781. (Continuación)

	I.6	Corte del suministro eléctrico	Amenaza debida a factores externos, a clemencias de tipo naturales como lluvias u otros.	Muy baja	2	10	3	Intolerable
	I.7	Condiciones inadecuadas de temperatura o humedad	No se cuenta con una infraestructura adecuada para soportar los defectos del sistema de refrigeración.	Muy baja	2	10	3	Intolerable
	I.11	Emanaciones electromagnéticas	No hay exposición o vulnerabilidad, por parte de esta amenaza.	Muy baja	2	10	3	Intolerable
ERRORES Y FALLOS NO INTENCIONADOS	**E.2**	Errores del administrador	Pérdida total o parcial del tiempo de ejecución de sus actividades, dependiendo de la gravedad del asunto.	Muy baja	2	10	3	Intolerable
	E.23	Errores de mantenimiento / actualización de equipos(hardware)	Perjuicio a la mantenibilidad del sistema de información.	Muy baja	2	10	3	Intolerable
	E.24	Caída del sistema por agotamiento de recursos	Saturación del sistema informático.	Muy baja	2	10	3	Intolerable
	E.25	Perdida de equipos (Robo)	Recuperación de soportes reciclados o desechados.	Muy baja	2	10	3	Intolerable

Tabla 22. Estimación del riesgo activo router cisco modelo 1800 4781. (Continuación)

ATAQUES INTENCIONADOS	**A.6**	Abuso de privilegios de acceso	Abuso de cada uno de los derechos otorgados.	Muy baja	2	10	3	Intolerable
	A.7	Uso no previsto	Implementación de recursos (económicos y de tiempo) en actividades no relacionadas.	Muy baja	2	10	3	Intolerable
	A.11	Acceso no autorizado	Uso ilícito del hardware	Muy baja	2	10	3	Intolerable
	A.23	Manipulación de los equipos	Sabotaje del hardware y software conteniente.	Muy baja	2	10	3	Intolerable
	A.24	Denegación de servicio	Saturación del sistema de información.	Muy baja	2	10	3	Intolerable
	A.25	Robo	Robo de porte de la información, puede esta ser física o digital.	Muy baja	2	10	3	Intolerable
	A.26	Ataque destructivo	Destrucción de los contenedores de la información, en recipientes físicos y lógicos.	Muy baja	2	10	3	Intolerable

Fuente: Autoría propia

Tabla 23. Estimación del riesgo activo red telefónica

ACTIVO TI	**RED TELEFÓNICA**
ADMINISTRADOR	PIMIENTO CARDENAS WILSON MAURICIO
DEGRADACIÓN	60%
IMPACTO	5

Tabla 23. Estimación del riesgo activo red telefónica. (Continuación)

TIPO DE ACTIVO		REDES DE COMUNICACIÓN							
Tipo	**ID**	**Amenaza**	**Exposición/Vulnerabilidad**	**RIESGO ACTUAL**					
							4	Extremo	
				Frecuencia (F)		**R**	**NR**		
DE ORIGEN INDUSTRIA	**I.8**	Fallo de servicios de comunicaciones	Atentados externos por parte de grupos ha margen de la ley que puedan atentar contra la infraestructura que trasmite cada uno de los servicios.	Media	4	20	4	Extremo	
ERRORES Y FALLOS NO INTENCIONADOS	**E.2**	Errores del administrador	Pérdida total o parcial del tiempo de ejecución de sus actividades, dependiendo de la gravedad del asunto.	Media	4	20	4	Extremo	
	E.9	Errores de [re-] encaminamiento	La dependencia cuenta con sistemas de cifrado y verificación (puerto – puerto) para el manejo de la movilidad de la información.	Media	4	20	4	Extremo	
	E.10	Errores de secuencia	La dependencia cuenta con sistemas de cifrado y verificación (puerto – puerto) para el manejo de la movilidad de la información.	Media	4	20	4	Extremo	
	E.15	Alteración accidental de la información	La dependencia cuenta con sistemas de cifrado y verificación (puerto – puerto) para el manejo de la movilidad de la información.	Media	4	20	4	Extremo	

Tabla 23. Estimación del riesgo activo red telefónica. (Continuación)

	E.18	Destrucción de información	El departamento de sistemas cuenta con copias de seguridad periódicas	Media	4	20	4	Extremo
	E.19	Fugas de información	Las personas contratadas están atadas a cláusulas de confidencialidad.	Media	4	20	4	Extremo
	E.24	Caída del sistema por agotamiento de recursos	Saturación del sistema informático.	Media	4	20	4	Extremo
ATAQUES INTENCIONADOS	**A.5**	Suplantación de la identidad del usuario	Acceso a personas que no cuenten con los permisos necesarios o con las credenciales necesarias.	Media	4	20	4	Extremo
	A.6	Abuso de privilegios de acceso	Abuso de cada uno de los derechos otorgados.	Media	4	20	4	Extremo
	A.7	Uso no previsto	Implementación de recursos (económicos y de tiempo) en actividades no relacionadas.	Media	4	20	4	Extremo
	A.9	[Re-]encaminamiento de mensajes	La dependencia cuenta con sistemas de cifrado y verificación (puerto – puerto) para el manejo de la movilidad de la información.	Media	4	20	4	Extremo
	A.10	Alteración de secuencia	Alteración de datos.	Media	4	20	4	Extremo

Tabla 23. Estimación del riesgo activo red telefónica. (Continuación)

	A.11	Acceso no autorizado	Uso ilícito del hardware	Media	4	20	4	Extremo
	A.12	Análisis de trafico	Análisis de cada uno de los datos transitados por la red interna de la institución.	Media	4	20	4	Extremo
	A.14	Interceptación de información (escucha)	Escucha pasiva.	Media	4	20	4	Extremo
	A.15	Modificación deliberada de la información	Datos erróneos en el momento de la movilización de la información.	Media	4	20	4	Extremo
	A.19	Divulgación de información	Información filtrada abiertamente a personas no correspondientes.	Media	4	20	4	Extremo
	A.24	Denegación de servicio	Saturación del sistema de información.	Media	4	20	4	Extremo

Fuente: Autoría propia

Tabla 24. Estimación de la probabilidad activo internet movistar

ACTIVO TI	**INTERNET MOVISTAR**			
ADMINISTRADOR	PIMIENTO CARDENAS WILSON MAURICIO			
DEGRADACIÓN	90%			
IMPACTO	8			
TIPO DE ACTIVO	REDES DE COMUNICACIÓN			
Tipo	**ID**	**Amenaza**	**Exposición/Vulnerabilidad**	**RIESGO ACTUAL**

Tabla 24. Estimación de la probabilidad activo internet movistar. (Continuación)

							4	Extremo
				Frecuencia (F)		**R**	**NR**	
DE ORIGEN INDUSTRIAL	**I.8**	Fallo de servicios de comunicaciones	Atentados externos por parte de grupos ha margen de la ley que puedan atentar contra la infraestructura que trasmite cada uno de los servicios.	Media	4	20	4	Extremo
ERRORES Y FALLOS NO INTENCIONADOS	**E.2**	Errores del administrador	Pérdida total o parcial del tiempo de ejecución de sus actividades, dependiendo de la gravedad del asunto.	Media	4	20	4	Extremo
	E.9	Errores de [re-] encaminamiento	La dependencia cuenta con sistemas de cifrado y verificación (puerto – puerto) para el manejo de la movilidad de la información.	Media	4	20	4	Extremo
	E.10	Errores de secuencia	La dependencia cuenta con sistemas de cifrado y verificación (puerto – puerto) para el manejo de la movilidad de la información.	Media	4	20	4	Extremo
	E.15	Alteración accidental de la información	La dependencia cuenta con sistemas de cifrado y verificación (puerto – puerto) para el manejo de la movilidad de la información.	Media	4	20	4	Extremo

Tabla 24. Estimación de la probabilidad activo internet movistar. (Continuación)

	E.18	Destrucción de información	El departamento de sistemas cuenta con copias de seguridad periódicas	Media	4	20	4	Extremo
	E.19	Fugas de información	Las personas contratadas están atadas a cláusulas de confidencialidad.	Media	4	20	4	Extremo
	E.24	Caída del sistema por agotamiento de recursos	Saturación del sistema informático.	Media	4	20	4	Extremo
ATAQUES INTENCIONADOS	**A.5**	Suplantación de la identidad del usuario	Acceso a personas que no cuenten con los permisos necesarios o con las credenciales necesarias.	Media	4	20	4	Extremo
	A.6	Abuso de privilegios de acceso	Abuso de cada uno de los derechos otorgados.	Media	4	20	4	Extremo
	A.7	Uso no previsto	Implementación de recursos (económicos y de tiempo) en actividades no relacionadas.	Media	4	20	4	Extremo
	A.9	[Re-]encaminamiento de mensajes	La dependencia cuenta con sistemas de cifrado y verificación (puerto – puerto) para el manejo de la movilidad de la información.	Media	4	20	4	Extremo
	A.10	Alteración de secuencia	Alteración de datos.	Media	4	20	4	Extremo

Tabla 24. Estimación de la probabilidad activo internet movistar. (Continuación)

	A.11	Acceso no autorizado	Uso ilícito del hardware	Media	4	20	4	Extremo
	A.12	Análisis de trafico	Análisis de cada uno de los datos transitados por la red interna de la institución.	Media	4	20	4	Extremo
	A.14	Interceptación de información (escucha)	Escucha pasiva.	Media	4	20	4	Extremo
	A.15	Modificación deliberada de la información	Datos erróneos en el momento de la movilización de la información.	Media	4	20	4	Extremo
	A.19	Divulgación de información	Información filtrada abiertamente a personas no correspondientes.	Media	4	20	4	Extremo
	A.24	Denegación de servicio	Saturación del sistema de información.	Media	4	20	4	Extremo

Fuente: Autoría propia

Tabla 25. Estimación del riesgo activo red LAN

ACTIVO TI	**RED LAN**			
ADMINISTRADOR	PIMIENTO CARDENAS WILSON MAURICIO			
DEGRADACIÓN	90%			
IMPACTO	8			
TIPO DE ACTIVO	REDES DE COMUNICACIÓN			
Tipo	**ID**	**Amenaza**	**Exposición/Vulnerabilidad**	**RIESGO ACTUAL**

Tabla 25. Estimación del riesgo activo red LAN. (Continuación)

							4	Extremo
				Frecuencia (F)		**R**	**NR**	
DE ORIGEN INDUSTRIAL	**I.8**	Fallo de servicios de comunicaciones	Atentados externos por parte de grupos ha margen de la ley que puedan atentar contra la infraestructura que trasmite cada uno de los servicios.	Media	4	20	4	Extremo
ERRORES Y FALLOS NO INTENCIONADOS	**E.2**	Errores del administrador	Pérdida total o parcial del tiempo de ejecución de sus actividades, dependiendo de la gravedad del asunto.	Media	4	20	4	Extremo
	E.9	Errores de [re-] encaminamiento	La dependencia cuenta con sistemas de cifrado y verificación (puerto – puerto) para el manejo de la movilidad de la información.	Media	4	20	4	Extremo
	E.10	Errores de secuencia	La dependencia cuenta con sistemas de cifrado y verificación (puerto – puerto) para el manejo de la movilidad de la información.	Media	4	20	4	Extremo
	E.15	Alteración accidental de la información	La dependencia cuenta con sistemas de cifrado y verificación (puerto – puerto) para el manejo de la movilidad de la información.	Media	4	20	4	Extremo

Tabla 25. Estimación del riesgo activo red LAN. (Continuación)

	E.18	Destrucción de información	El departamento de sistemas cuenta con copias de seguridad periódicas	Media	4	20	4	Extremo
	E.19	Fugas de información	Las personas contratadas están atadas a cláusulas de confidencialidad.	Media	4	20	4	Extremo
	E.24	Caída del sistema por agotamiento de recursos	Saturación del sistema informático.	Media	4	20	4	Extremo
ATAQUES INTENCIONADOS	**A.5**	Suplantación de la identidad del usuario	Acceso a personas que no cuenten con los permisos necesarios o con las credenciales necesarias.	Media	4	20	4	Extremo
	A.6	Abuso de privilegios de acceso	Abuso de cada uno de los derechos otorgados.	Media	4	20	4	Extremo
	A.7	Uso no previsto	Implementación de recursos (económicos y de tiempo) en actividades no relacionadas.	Media	4	20	4	Extremo
	A.9	[Re-]encaminamiento de mensajes	La dependencia cuenta con sistemas de cifrado y verificación (puerto – puerto) para el manejo de la movilidad de la información.	Media	4	20	4	Extremo
	A.10	Alteración de secuencia	Alteración de datos.	Media	4	20	4	Extremo

Tabla 25. Estimación del riesgo activo red LAN. (Continuación)

	A.11	Acceso no autorizado	Uso ilícito del hardware	Media	4	20	4	Extremo
	A.12	Análisis de trafico	Análisis de cada uno de los datos transitados por la red interna de la institución.	Media	4	20	4	Extremo
	A.14	Interceptación de información (escucha)	Escucha pasiva.	Media	4	20	4	Extremo
	A.15	Modificación deliberada de la información	Datos erróneos en el momento de la movilización de la información.	Media	4	20	4	Extremo
	A.19	Divulgación de información	Información filtrada abiertamente a personas no correspondientes.	Media	4	20	4	Extremo
	A.24	Denegación de servicio	Saturación del sistema de información.	Media	4	20	4	Extremo

Fuente: Autoría propia

Tabla 26. Estimación de la probabilidad activo red WIFI

ACTIVO TI	**RED WIFI**			
ADMINISTRADOR	PIMIENTO CARDENAS WILSON MAURICIO			
DEGRADACIÓN	70%			
IMPACTO	5			
TIPO DE ACTIVO	REDES DE COMUNICACIÓN			
Tipo	**ID**	**Amenaza**	**Exposición/Vulnerabilidad**	**RIESGO ACTUAL**

Tabla 26. Estimación de la probabilidad activo red WIFI. (Continuación)

							4	Extremo
				Frecuencia (F)		**R**	**NR**	
DE ORIGEN INDUSTRIAL	**I.8**	Fallo de servicios de comunicaciones	Atentados externos por parte de grupos ha margen de la ley que puedan atentar contra la infraestructura que trasmite cada uno de los servicios.	Media	4	20	4	Extremo
ERRORES Y FALLOS NO INTENCIONADOS	**E.2**	Errores del administrador	Pérdida total o parcial del tiempo de ejecución de sus actividades, dependiendo de la gravedad del asunto.	Media	4	20	4	Extremo
	E.9	Errores de [re-] encaminamiento	La dependencia cuenta con sistemas de cifrado y verificación (puerto – puerto) para el manejo de la movilidad de la información.	Media	4	20	4	Extremo
	E.10	Errores de secuencia	La dependencia cuenta con sistemas de cifrado y verificación (puerto – puerto) para el manejo de la movilidad de la información.	Media	4	20	4	Extremo
	E.15	Alteración accidental de la información	La dependencia cuenta con sistemas de cifrado y verificación (puerto – puerto) para el manejo de la movilidad de la información.	Media	4	20	4	Extremo

Tabla 26. Estimación de la probabilidad activo red WIFI. (Continuación)

	E.18	Destrucción de información	El departamento de sistemas cuenta con copias de seguridad periódicas	Media	4	20	4	Extremo
	E.19	Fugas de información	Las personas contratadas están atadas a cláusulas de confidencialidad.	Media	4	20	4	Extremo
	E.24	Caída del sistema por agotamiento de recursos	Saturación del sistema informático.	Media	4	20	4	Extremo
ATAQUES INTENCIONADOS	**A.5**	Suplantación de la identidad del usuario	Acceso a personas que no cuenten con los permisos necesarios o con las credenciales necesarias.	Media	4	20	4	Extremo
	A.6	Abuso de privilegios de acceso	Abuso de cada uno de los derechos otorgados.	Media	4	20	4	Extremo
	A.7	Uso no previsto	Implementación de recursos (económicos y de tiempo) en actividades no relacionadas.	Media	4	20	4	Extremo
	A.9	[Re-]encaminamiento de mensajes	La dependencia cuenta con sistemas de cifrado y verificación (puerto – puerto) para el manejo de la movilidad de la información.	Media	4	20	4	Extremo
	A.10	Alteración de secuencia	Alteración de datos.	Media	4	20	4	Extremo

Tabla 26. Estimación de la probabilidad activo red WIFI. (Continuación)

	A.11	Acceso no autorizado	Uso ilícito del hardware	Media	4	20	4	Extremo
	A.12	Análisis de trafico	Análisis de cada uno de los datos transitados por la red interna de la institución.	Media	4	20	4	Extremo
	A.14	Interceptación de información (escucha)	Escucha pasiva.	Media	4	20	4	Extremo
	A.15	Modificación deliberada de la información	Datos erróneos en el momento de la movilización de la información.	Media	4	20	4	Extremo
	A.19	Divulgación de información	Información filtrada abiertamente a personas no correspondientes.	Media	4	20	4	Extremo
	A.24	Denegación de servicio	Saturación del sistema de información.	Media	4	20	4	Extremo

Fuente: Autoría propia

Tabla 27. Estimación del riesgo activo red de datos

ACTIVO TI	**RED DE DATOS**			
ADMINISTRADOR	PIMIENTO CARDENAS WILSON MAURICIO			
DEGRADACIÓN	70%			
IMPACTO	5			
TIPO DE ACTIVO	REDES DE COMUNICACIÓN			
Tipo	**ID**	**Amenaza**	**Exposición/Vulnerabilidad**	**RIESGO ACTUAL**

Tabla 27. Estimación del riesgo activo red de datos. (Continuación)

							4	Extremo
				Frecuencia (F)		**R**	**NR**	
DE ORIGEN INDUSTRIAL	**I.8**	Fallo de servicios de comunicaciones	Atentados externos por parte de grupos ha margen de la ley que puedan atentar contra la infraestructura que trasmite cada uno de los servicios.	Media	4	20	4	Extremo
ERRORES Y FALLOS NO INTENCIONADOS	**E.2**	Errores del administrador	Pérdida total o parcial del tiempo de ejecución de sus actividades, dependiendo de la gravedad del asunto.	Media	4	20	4	Extremo
	E.9	Errores de [re-] encaminamiento	La dependencia cuenta con sistemas de cifrado y verificación (puerto – puerto) para el manejo de la movilidad de la información.	Media	4	20	4	Extremo
	E.10	Errores de secuencia	La dependencia cuenta con sistemas de cifrado y verificación (puerto – puerto) para el manejo de la movilidad de la información.	Media	4	20	4	Extremo
	E.15	Alteración accidental de la información	La dependencia cuenta con sistemas de cifrado y verificación (puerto – puerto) para el manejo de la movilidad de la información.	Media	4	20	4	Extremo

Tabla 27. Estimación del riesgo activo red de datos. (Continuación)

	E.18	Destrucción de información	El departamento de sistemas cuenta con copias de seguridad periódicas	Media	4	20	4	Extremo
	E.19	Fugas de información	Las personas contratadas están atadas a cláusulas de confidencialidad.	Media	4	20	4	Extremo
	E.24	Caída del sistema por agotamiento de recursos	Saturación del sistema informático.	Media	4	20	4	Extremo
ATAQUES INTENCIONADOS	**A.5**	Suplantación de la identidad del usuario	Acceso a personas que no cuenten con los permisos necesarios o con las credenciales necesarias.	Media	4	20	4	Extremo
	A.6	Abuso de privilegios de acceso	Abuso de cada uno de los derechos otorgados.	Media	4	20	4	Extremo
	A.7	Uso no previsto	Implementación de recursos (económicos y de tiempo) en actividades no relacionadas.	Media	4	20	4	Extremo
	A.9	[Re-]encaminamiento de mensajes	La dependencia cuenta con sistemas de cifrado y verificación (puerto – puerto) para el manejo de la movilidad de la información.	Media	4	20	4	Extremo
	A.10	Alteración de secuencia	Alteración de datos.	Media	4	20	4	Extremo

Tabla 27. Estimación del riesgo activo red de datos. (Continuación)

	A.11	Acceso no autorizado	Uso ilícito del hardware	Media	4	20	4	Extremo
	A.12	Análisis de trafico	Análisis de cada uno de los datos transitados por la red interna de la institución.	Media	4	20	4	Extremo
	A.14	Interceptación de información (escucha)	Escucha pasiva.	Media	4	20	4	Extremo
	A.15	Modificación deliberada de la información	Datos erróneos en el momento de la movilización de la información.	Media	4	20	4	Extremo
	A.19	Divulgación de información	Información filtrada abiertamente a personas no correspondientes.	Media	4	20	4	Extremo
	A.24	Denegación de servicio	Saturación del sistema de información.	Media	4	20	4	Extremo

Fuente: Autoría propia

Tabla 28. Estimación del riesgo activo DDS 1TB

ACTIVO TI	**DDS 1TB**			
ADMINISTRADOR	PIMIENTO CARDENAS WILSON MAURICIO			
DEGRADACIÓN	35%			
IMPACTO	3			
TIPO DE ACTIVO	SOPORTES DE INFORMACIÓN			
Tipo	**ID**	**Amenaza**	**Exposición/Vulnerabilidad**	**RIESGO ACTUAL**

Tabla 28. Estimación del riesgo activo DDS 1TB. (Continuación)

							4	Extremo
				Frecuencia (F)		**R**	**NR**	
DESASTRES NATURALES	**N.1**	Fuego	No existe sistema de alarma contra incendios. Se posee un solo extintor de solkaflam (clase c) recomendados para incendios en lugares donde se encuentren equipos eléctricos.	Baja	3	15	4	Extremo
	N.2	Daños por agua	La infraestructura está expuesta a goteras, cuenta con averías en el techo en donde el agua de las lluvias	Baja	3	15	4	Extremo
	N.*	Desastres naturales	La oficina de la dependencia de sistemas se encuentra en zona baja de riesgo de desastre natural de origen volcánico debido a su cercanía con el volcán nevado del Tolima.	Baja	3	15	4	Extremo
DE ORIGEN INDUSTRIAL	**I.1**	Fuego	No existe sistema de alarma contra incendios. Se posee un solo extintor de solkaflam (clase c) recomendados para incendios en lugares donde se encuentren equipos eléctricos.	Baja	3	15	4	Extremo
	I.2	Daños por agua	La concentración del líquido sobrante por parte del aire acondicionado causaría daños en los equipos.	Baja	3	15	4	Extremo

Tabla 28. Estimación del riesgo activo DDS 1TB. (Continuación)

	I.*	Desastres industriales	No hay exposición o vulnerabilidad, por parte de esta amenaza.	Baja	3	15	4	Extremo
	I.3	Contaminación mecánica	No hay exposición o vulnerabilidad, por parte de esta amenaza.	Baja	3	15	4	Extremo
	I.4	Contaminación electromagnética	No hay exposición o vulnerabilidad, por parte de esta amenaza.	Baja	3	15	4	Extremo
	I.5	Avería de origen físico o lógico	La manipulación por parte de cada uno de los componentes encontrados en la dependencia, como también por defectos de los componentes desde fabrica	Baja	3	15	4	Extremo
	I.6	Corte del suministro eléctrico	Amenaza debida a factores externos, a clemencias de tipo naturales como lluvias u otros.	Baja	3	15	4	Extremo
	I.7	Condiciones inadecuadas de temperatura o humedad	No se cuenta con una infraestructura adecuada para soportar los defectos del sistema de refrigeración.	Baja	3	15	4	Extremo
	I.10	Degradación de los soportes de almacén amiento de la información	Pérdida gradual de cada uno de los registros históricos de la dependencia.	Baja	3	15	4	Extremo

Tabla 28. Estimación del riesgo activo DDS 1TB. (Continuación)

	I.11	Emanaciones electromagnéticas	No hay exposición o vulnerabilidad, por parte de esta amenaza.	Baja	3	15	4	Extremo
ERRORES Y FALLOS NO INTENCIONADOS	**E.1**	Errores de los usuarios	Pérdida total o parcial del tiempo de ejecución de sus actividades, dependiendo de la gravedad del asunto.	Baja	3	15	4	Extremo
	E.2	Errores del administrador	Pérdida total o parcial del tiempo de ejecución de sus actividades, dependiendo de la gravedad del asunto.	Baja	3	15	4	Extremo
	E.15	Alteración accidental de la información	La dependencia cuenta con sistemas de cifrado y verificación (puerto – puerto) para el manejo de la movilidad de la información.	Baja	3	15	4	Extremo
	E.18	Destrucción de información	El departamento de sistemas cuenta con copias de seguridad periódicas	Baja	3	15	4	Extremo
	E.19	Fugas de información	Las personas contratadas están atadas a cláusulas de confidencialidad.	Baja	3	15	4	Extremo
	E.23	Errores de mantenimiento / actualización de equipos(hardware)	Perjuicio a la mantenibilidad del sistema de información.	Baja	3	15	4	Extremo

Tabla 28. Estimación del riesgo activo DDS 1TB. (Continuación)

	E.25	Perdida de equipos (Robo)	Recuperación de soportes reciclados o desechados.	Baja	3	15	4	Extremo
ATAQUES INTENCIONADOS	**A.7**	Uso no previsto	Implementación de recursos (económicos y de tiempo) en actividades no relacionadas.	Baja	3	15	4	Extremo
	A.11	Acceso no autorizado	Uso ilícito del hardware	Baja	3	15	4	Extremo
	A.15	Modificación deliberada de la información	Datos erróneos en el momento de la movilización de la información.	Baja	3	15	4	Extremo
	A.18	Destrucción de información	Perdida de la información.	Baja	3	15	4	Extremo
	A.19	Divulgación de información	Información filtrada abiertamente a personas no correspondientes.	Baja	3	15	4	Extremo
	A.23	Manipulación de los equipos	Sabotaje del hardware y software conteniente.	Baja	3	15	4	Extremo
	A.25	Robo	Robo de porte de la información, puede esta ser física o digital.	Baja	3	15	4	Extremo
	A.26	Ataque destructivo	Destrucción de los contenedores de la información, en recipientes físicos y lógicos.	Baja	3	15	4	Extremo

Fuente: Autoría propia

Tabla 29. Estimación del riesgo activo materiales físicos

ACTIVO TI	**MATERIALES FÍSICOS**
ADMINISTRADOR	PIMIENTO CARDENAS WILSON MAURICIO
DEGRACIÓN	25%
IMPACTO	2
TIPO DE ACTIVO	SOPORTES DE INFORMACIÓN

Tipo	ID	Amenaza	Exposición/Vulnerabilidad	RIESGO ACTUAL				
							2	Tolerable
				Frecuencia (F)		R	NR	
DESASTRES NATURALES	**N.1**	Fuego	No existe sistema de alarma contra incendios. Se posee un solo extintor de solkaflam (clase c) recomendados para incendios en lugares donde se encuentren equipos eléctricos.	Baja	3	6	2	Tolerable
	N.2	Daños por agua	La infraestructura está expuesta a goteras, cuenta con averías en el techo en donde el agua de las lluvias	Baja	3	6	2	Tolerable
	N.*	Desastres naturales	La oficina de la dependencia de sistemas se encuentra en zona baja de riesgo de desastre natural de origen volcánico debido a su cercanía con el volcán nevado del Tolima.	Baja	3	6	2	Tolerable

Tabla 29. Estimación del riesgo activo materiales físicos. (Continuación)

DE ORIGEN INDUSTRIAL	**I.1**	Fuego	No existe sistema de alarma contra incendios. Se posee un solo extintor de solkaflam (clase c) recomendados para incendios en lugares donde se encuentren equipos eléctricos.	Baja	3	6	2	Tolerable
	I.2	Daños por agua	La concentración del líquido sobrante por parte del aire acondicionado causaría daños en los equipos.	Baja	3	6	2	Tolerable
	I.*	Desastres industriales	No hay exposición o vulnerabilidad, por parte de esta amenaza.	Baja	3	6	2	Tolerable
	I.3	Contaminación mecánica	No hay exposición o vulnerabilidad, por parte de esta amenaza.	Baja	3	6	2	Tolerable
	I.4	Contaminación electromagnética	No hay exposición o vulnerabilidad, por parte de esta amenaza.	Baja	3	6	2	Tolerable
	I.5	Avería de origen físico o lógico	La manipulación por parte de cada uno de los componentes encontrados en la dependencia, como también por defectos de los componentes desde fabrica	Baja	3	6	2	Tolerable
	I.6	Corte del suministro eléctrico	Amenaza debida a factores externos, a clemencias de tipo naturales como lluvias u otros.	Baja	3	6	2	Tolerable

Tabla 29. Estimación del riesgo activo materiales físicos. (Continuación)

	I.7	Condiciones inadecuadas de temperatura o humedad	No se cuenta con una infraestructura adecuada para soportar los defectos del sistema de refrigeración.	Baja	3	6	2	Tolerable
	I.10	Degradación de los soportes de almacén amiento de la información	Pérdida gradual de cada uno de los registros históricos de la dependencia.	Baja	3	6	2	Tolerable
	I.11	Emanaciones electromagnéticas	No hay exposición o vulnerabilidad, por parte de esta amenaza.	Baja	3	6	2	Tolerable
ERRORES Y FALLOS NO INTENCIONADOS	**E.1**	Errores de los usuarios	Pérdida total o parcial del tiempo de ejecución de sus actividades, dependiendo de la gravedad del asunto.	Baja	3	6	2	Tolerable
	E.2	Errores del administrador	Pérdida total o parcial del tiempo de ejecución de sus actividades, dependiendo de la gravedad del asunto.	Baja	3	6	2	Tolerable
	E.15	Alteración accidental de la información	La dependencia cuenta con sistemas de cifrado y verificación (puerto – puerto) para el manejo de la movilidad de la información.	Baja	3	6	2	Tolerable

Tabla 29. Estimación del riesgo activo materiales físicos. (Continuación)

	E.18	Destrucción de información	El departamento de sistemas cuenta con copias de seguridad periódicas	Baja	3	6	2	Tolerable
	E.19	Fugas de información	Las personas contratadas están atadas a cláusulas de confidencialidad.	Baja	3	6	2	Tolerable
	E.23	Errores de mantenimiento / actualización de equipos(hardware)	Perjuicio a la mantenibilidad del sistema de información.	Baja	3	6	2	Tolerable
	E.25	Perdida de equipos (Robo)	Recuperación de soportes reciclados o desechados.	Baja	3	6	2	Tolerable
ATAQUES INTENCIONADOS	**A.7**	Uso no previsto	Implementación de recursos (económicos y de tiempo) en actividades no relacionadas.	Baja	3	6	2	Tolerable
	A.11	Acceso no autorizado	Uso ilícito del hardware	Baja	3	6	2	Tolerable
	A.15	Modificación deliberada de la información	Datos erróneos en el momento de la movilización de la información.	Baja	3	6	2	Tolerable
	A.18	Destrucción de información	Perdida de la información.	Baja	3	6	2	Tolerable
	A.19	Divulgación de información	Información filtrada abiertamente a personas no correspondientes.	Baja	3	6	2	Tolerable

Tabla 29. Estimación del riesgo activo materiales físicos. (Continuación)

	A.23	Manipulación de los equipos	Sabotaje del hardware y software conteniente.	Baja	3	6	2	Tolerable
	A.25	Robo	Robo de porte de la información, puede esta ser física o digital.	Baja	3	6	2	Tolerable
	A.26	Ataque destructivo	Destrucción de los contenedores de la información, en recipientes físicos y lógicos.	Baja	3	6	2	Tolerable

Fuente: Autoría propia

Tabla 30. Estimación del riesgo activo UPS 10 KVA 9578

ACTIVO TI	**UPS 10 KVA 9578**
ADMINISTRADOR	PIMIENTO CARDENAS WILSON MAURICIO
DEGRADACIÓN	70%
IMPACTO	5
TIPO DE ACTIVO	EQUIPAMIENTO AUXILIAR

Tipo	**ID**	**Amenaza**	**Exposición/Vulnerabilidad**	**RIESGO ACTUAL**				
							3.36	Intolerable
				Frecuencia (F)		**R**	**NR**	
DESASTRES NATURALES	**N.1**	Fuego	No existe sistema de alarma contra incendios. Se posee un solo extintor de solkaflam (clase c) recomendados para incendios en lugares donde se encuentren equipos eléctricos.	Muy baja	2	10	3	Intolerable

Tabla 30. Estimación del riesgo activo UPS 10 KVA 9578. (Continuación)

	N.2	Daños por agua	La infraestructura está expuesta a goteras, cuenta con averías en el techo en donde el agua de las lluvias	Muy baja	2	10	3	Intolerable
	N.*	Desastres naturales	La oficina de la dependencia de sistemas se encuentra en zona baja de riesgo de desastre natural de origen volcánico debido a su cercanía con el volcán nevado del Tolima.	Muy baja	2	10	3	Intolerable
DE ORIGEN INDUSTRIAL	**I.1**	Fuego	No existe sistema de alarma contra incendios. Se posee un solo extintor de solkaflam (clase c) recomendados para incendios en lugares donde se encuentren equipos eléctricos.	Muy baja	2	10	3	Intolerable
	I.2	Daños por agua	La concentración del líquido sobrante por parte del aire acondicionado causaría daños en los equipos.	Muy baja	2	10	3	Intolerable
	I.*	Desastres industriales	No hay exposición o vulnerabilidad, por parte de esta amenaza.	Muy baja	2	10	3	Intolerable
	I.3	Contaminación mecánica	No hay exposición o vulnerabilidad, por parte de esta amenaza.	Muy baja	2	10	3	Intolerable

Tabla 30. Estimación del riesgo activo UPS 10 KVA 9578. (Continuación)

	I.4	Contaminación electromagnética	No hay exposición o vulnerabilidad, por parte de esta amenaza.	Muy baja	2	10	3	Intolerable
	I.5	Avería de origen físico o lógico	La manipulación por parte de cada uno de los componentes encontrados en la dependencia, como también por defectos de los componentes desde fabrica	Muy baja	2	10	3	Intolerable
	I.6	Corte del suministro eléctrico	Amenaza debida a factores externos, a clemencias de tipo naturales como lluvias u otros.	Muy baja	2	10	3	Intolerable
	I.7	Condiciones inadecuadas de temperatura o humedad	No se cuenta con una infraestructura adecuada para soportar los defectos del sistema de refrigeración.	Muy baja	2	10	3	Intolerable
	I.9	Interrupción de otros servicios y suministros esenciales	No hay exposición o vulnerabilidad, por parte de esta amenaza.	Muy baja	2	10	3	Intolerable
	I.11	Emanaciones electromagnéticas	No hay exposición o vulnerabilidad, por parte de esta amenaza.	Muy baja	2	10	3	Intolerable
ERRORES Y	**E.23**	Errores de mantenimiento /	Perjuicio a la mantenibilidad del sistema de información.	Baja	3	15	4	Extremo

Tabla 30. Estimación del riesgo activo UPS 10 KVA 9578. (Continuación)

		actualización de equipos(hardware)						
	E.25	Perdida de equipos (Robo)	Recuperación de soportes reciclados o desechados.	Baja	3	15	4	Extremo
ATAQUES INTENCIONADOS	**A.7**	Uso no previsto	Implementación de recursos (económicos y de tiempo) en actividades no relacionadas.	Baja	3	15	4	Extremo
	A.11	Acceso no autorizado	Uso ilícito del hardware	Baja	3	15	4	Extremo
	A.23	Manipulación de los equipos	Sabotaje del hardware y software conteniente.	Baja	3	15	4	Extremo
	A.25	Robo	Robo de porte de la información, puede esta ser física o digital.	Baja	3	15	4	Extremo
	A.26	Ataque destructivo	Destrucción de los contenedores de la información, en recipientes físicos y lógicos.	Baja	3	15	4	Extremo

Fuente: Autoría propia

Tabla 31. Estimación de la probabilidad activo UPS 10 KVA 9579

ACTIVO TI	**UPS 10 KVA 9579**
ADMINISTRADOR	PIMIENTO CARDENAS WILSON MAURICIO
DEGRADACIÓN	70%
IMPACTO	5

Tabla 31. Estimación de la probabilidad activo UPS 10 KVA 9579. (Continuación)

TIPO DE ACTIVO		EQUIPAMIENTO AUXILIAR						
Tipo	**ID**	**Amenaza**	**Exposición/Vulnerabilidad**	**RIESGO ACTUAL**				
							3.36	Intolerable
				Frecuencia (F)		**R**	**NR**	
DESASTRES NATURALES	**N.1**	Fuego	No existe sistema de alarma contra incendios. Se posee un solo extintor de solkaflam (clase c) recomendados para incendios en lugares donde se encuentren equipos eléctricos.	Muy baja	2	10	3	Intolerable
	N.2	Daños por agua	La infraestructura está expuesta a goteras, cuenta con averías en el techo en donde el agua de las lluvias	Muy baja	2	10	3	Intolerable
	N.*	Desastres naturales	La oficina de la dependencia de sistemas se encuentra en zona baja de riesgo de desastre natural de origen volcánico debido a su cercanía con el volcán nevado del Tolima.	Muy baja	2	10	3	Intolerable
DE ORIGEN INDUSTRIAL	**I.1**	Fuego	No existe sistema de alarma contra incendios. Se posee un solo extintor de solkaflam (clase c) recomendados para incendios en lugares donde se encuentren equipos eléctricos.	Muy baja	2	10	3	Intolerable

Tabla 31. Estimación de la probabilidad activo UPS 10 KVA 9579. (Continuación)

	I.2	Daños por agua	La concentración del líquido sobrante por parte del aire acondicionado causaría daños en los equipos.	Muy baja	2	10	3	Intolerable
	I.*	Desastres industriales	No hay exposición o vulnerabilidad, por parte de esta amenaza.	Muy baja	2	10	3	Intolerable
	I.3	Contaminación mecánica	No hay exposición o vulnerabilidad, por parte de esta amenaza.	Muy baja	2	10	3	Intolerable
	I.4	Contaminación electromagnética	No hay exposición o vulnerabilidad, por parte de esta amenaza.	Muy baja	2	10	3	Intolerable
	I.5	Avería de origen físico o lógico	La manipulación por parte de cada uno de los componentes encontrados en la dependencia, como también por defectos de los componentes desde fabrica	Muy baja	2	10	3	Intolerable
	I.6	Corte del suministro eléctrico	Amenaza debida a factores externos, a clemencias de tipo naturales como lluvias u otros.	Muy baja	2	10	3	Intolerable
	I.7	Condiciones inadecuadas de temperatura o humedad	No se cuenta con una infraestructura adecuada para soportar los defectos del sistema de refrigeración.	Muy baja	2	10	3	Intolerable

Tabla 31. Estimación de la probabilidad activo UPS 10 KVA 9579. (Continuación)

	I.9	Interrupción de otros servicios y suministros esenciales	No hay exposición o vulnerabilidad, por parte de esta amenaza.	Muy baja	2	10	3	Intolerable
	I.11	Emanaciones electromagnéticas	No hay exposición o vulnerabilidad, por parte de esta amenaza.	Muy baja	2	10	3	Intolerable
ERRORES Y FALLOS NO INTENCIONADOS	**E.23**	Errores de mantenimiento / actualización de equipos(hardware)	Perjuicio a la mantenibilidad del sistema de información.	Baja	3	15	4	Extremo
	E.25	Perdida de equipos (Robo)	Recuperación de soportes reciclados o desechados.	Baja	3	15	4	Extremo
ATAQUES INTENCIONADOS	**A.7**	Uso no previsto	Implementación de recursos (económicos y de tiempo) en actividades no relacionadas.	Baja	3	15	4	Extremo
	A.11	Acceso no autorizado	Uso ilícito del hardware	Baja	3	15	4	Extremo
	A.23	Manipulación de los equipos	Sabotaje del hardware y software conteniente.	Baja	3	15	4	Extremo
	A.25	Robo	Robo de porte de la información, puede esta ser física o digital.	Baja	3	15	4	Extremo

Tabla 31. Estimación de la probabilidad activo UPS 10 KVA 9579. (Continuación)

	A.26	Ataque destructivo	Destrucción de los contenedores de la información, en recipientes físicos y lógicos.	Baja	3	15	4	Extremo

Fuente: Autoría propia

Tabla 32. Estimación del riesgo activo UPS 10 KVA 9580

ACTIVO TI			**UPS 10 KVA 9580**					
ADMINISTRADOR			PIMIENTO CARDENAS WILSON MAURICIO					
DEGRADACIÓN			70%					
IMPACTO			5					
TIPO DE ACTIVO			EQUIPAMIENTO AUXILIAR					
Tipo	**ID**	**Amenaza**	**Exposición/Vulnerabilidad**	**RIESGO ACTUAL**				
							3.36	Intolerable
				Frecuencia (F)		**R**	**NR**	
DESASTRES NATURALES	**N.1**	Fuego	No existe sistema de alarma contra incendios. Se posee un solo extintor de solkaflam (clase c) recomendados para incendios en lugares donde se encuentren equipos eléctricos.	Muy baja	2	10	3	Intolerable
	N.2	Daños por agua	La infraestructura está expuesta a goteras, cuenta con averías en el techo en donde el agua de las lluvias	Muy baja	2	10	3	Intolerable

Tabla 32. Estimación del riesgo activo UPS 10 KVA 9580. (Continuación)

	N.*	Desastres naturales	La oficina de la dependencia de sistemas se encuentra en zona baja de riesgo de desastre natural de origen volcánico debido a su cercanía con el volcán nevado del Tolima.	Muy baja	2	10	3	Intolerable
DE ORIGEN INDUSTRIAL	**I.1**	Fuego	No existe sistema de alarma contra incendios. Se posee un solo extintor de solkaflam (clase c) recomendados para incendios en lugares donde se encuentren equipos eléctricos.	Muy baja	2	10	3	Intolerable
	I.2	Daños por agua	La concentración del líquido sobrante por parte del aire acondicionado causaría daños en los equipos.	Muy baja	2	10	3	Intolerable
	I.*	Desastres industriales	No hay exposición o vulnerabilidad, por parte de esta amenaza.	Muy baja	2	10	3	Intolerable
	I.3	Contaminación mecánica	No hay exposición o vulnerabilidad, por parte de esta amenaza.	Muy baja	2	10	3	Intolerable
	I.4	Contaminación electromagnética	No hay exposición o vulnerabilidad, por parte de esta amenaza.	Muy baja	2	10	3	Intolerable

Tabla 32. Estimación del riesgo activo UPS 10 KVA 9580. (Continuación)

	I.5	Avería de origen físico o lógico	La manipulación por parte de cada uno de los componentes encontrados en la dependencia, como también por defectos de los componentes desde fabrica	Muy baja	2	10	3	Intolerable
	I.6	Corte del suministro eléctrico	Amenaza debida a factores externos, a clemencias de tipo naturales como lluvias u otros.	Muy baja	2	10	3	Intolerable
	I.7	Condiciones inadecuadas de temperatura o humedad	No se cuenta con una infraestructura adecuada para soportar los defectos del sistema de refrigeración.	Muy baja	2	10	3	Intolerable
	I.9	Interrupción de otros servicios y suministros esenciales	No hay exposición o vulnerabilidad, por parte de esta amenaza.	Muy baja	2	10	3	Intolerable
	I.11	Emanaciones electromagnéticas	No hay exposición o vulnerabilidad, por parte de esta amenaza.	Muy baja	2	10	3	Intolerable
ERRORES Y FALLOS NO	**E.23**	Errores de mantenimiento / actualización de equipos(hardware)	Perjuicio a la mantenibilidad del sistema de información.	Baja	3	15	4	Extremo

Tabla 32. Estimación del riesgo activo UPS 10 KVA 9580. (Continuación)

	E.25	Perdida de equipos (Robo)	Recuperación de soportes reciclados o desechados.	Baja	3	15	4	Extremo
ATAQUES INTENCIONADOS	**A.7**	Uso no previsto	Implementación de recursos (económicos y de tiempo) en actividades no relacionadas.	Baja	3	15	4	Extremo
	A.11	Acceso no autorizado	Uso ilícito del hardware	Baja	3	15	4	Extremo
	A.23	Manipulación de los equipos	Sabotaje del hardware y software conteniente.	Baja	3	15	4	Extremo
	A.25	Robo	Robo de porte de la información, puede esta ser física o digital.	Baja	3	15	4	Extremo
	A.26	Ataque destructivo	Destrucción de los contenedores de la información, en recipientes físicos y lógicos.	Baja	3	15	4	Extremo

Fuente: Autoría propia

Tabla 33. Estimación del riesgo activo cuarto o recinto (oficina)

ACTIVO TI	**CUARTO O RECINTO (OFICINA)**						
ADMINISTRADOR	PIMIENTO CARDENAS WILSON MAURICIO						
DEGRADACIÓN	90%						
IMPACTO	8						
TIPO DE ACTIVO	INSTALACIONES						
Tipo	**ID**	**Amenaza**	**Exposición/Vulnerabilidad**	**RIESGO ACTUAL**			
						3.58	Intolerable

Tabla 33. Estimación del riesgo activo cuarto o recinto (oficina). (Continuación)

				Frecuencia (F)		R	NR	
DESASTRES NATURALES	**N.1**	Fuego	No existe sistema de alarma contra incendios. Se posee un solo extintor de solkaflam (clase c) recomendados para incendios en lugares donde se encuentren equipos eléctricos.	Raro	1	8	3	Intolerable
	N.2	Daños por agua	La infraestructura está expuesta a goteras, cuenta con averías en el techo en donde el agua de las lluvias	Raro	1	8	3	Intolerable
	N.*	Desastres naturales	La oficina de la dependencia de sistemas se encuentra en zona baja de riesgo de desastre natural de origen volcánico debido a su cercanía con el volcán nevado del Tolima.	Raro	1	8	3	Intolerable
DE ORIGEN INDUSTRIAL	**I.1**	Fuego	No existe sistema de alarma contra incendios. Se posee un solo extintor de solkaflam (clase c) recomendados para incendios en lugares donde se encuentren equipos eléctricos.	Raro	1	8	3	Intolerable
	I.2	Daños por agua	La concentración del líquido sobrante por parte del aire acondicionado causaría daños en los equipos.	Raro	1	8	3	Intolerable

Tabla 33. Estimación del riesgo activo cuarto o recinto (oficina). (Continuación)

	I.*	Desastres industriales	No hay exposición o vulnerabilidad, por parte de esta amenaza.	Raro	1	8	3	Intolerable
	I.11	Emanaciones electromagnéticas	No hay exposición o vulnerabilidad, por parte de esta amenaza.	Raro	1	8	3	Intolerable
ERRORES Y FALLOS NO INTENCIONADOS	**E.15**	Alteración accidental de la información	La dependencia cuenta con sistemas de cifrado y verificación (puerto – puerto) para el manejo de la movilidad de la información.	Muy bajo	2	16	4	Extremo
	E.18	Destrucción de información	El departamento de sistemas cuenta con copias de seguridad periódicas	Muy bajo	2	16	4	Extremo
	E.19	Fugas de información	Las personas contratadas están atadas a cláusulas de confidencialidad.	Muy bajo	2	16	4	Extremo
ATAQUES INTENCIONADOS	**A.7**	Uso no previsto	Implementación de recursos (económicos y de tiempo) en actividades no relacionadas.	Muy bajo	2	16	4	Extremo
	A.11	Acceso no autorizado	Uso ilícito del hardware	Muy bajo	2	16	4	Extremo
	A.15	Modificación deliberada de la información	Datos erróneos en el momento de la movilización de la información.	Muy bajo	2	16	4	Extremo

Tabla 33. Estimación del riesgo activo cuarto o recinto (oficina). (Continuación)

	A.18	Destrucción de información	Perdida de la información.	Muy bajo	2	16	4	Extremo
	A.19	Divulgación de información	Información filtrada abiertamente a personas no correspondientes.	Muy bajo	2	16	4	Extremo
	A.26	Ataque destructivo	Destrucción de los contenedores de la información, en recipientes físicos y lógicos.	Muy bajo	2	16	4	Extremo
	A.27	Ocupación enemiga	Divulgación de información no consentida.	Muy bajo	2	16	4	Extremo

Fuente: Autoría propia

Tabla 34. Estimación del riesgo activo coordinador de sistemas

ACTIVO TI	**COORDINADOR DE SISTEMAS**
ADMINISTRADOR	PIMIENTO CARDENAS WILSON MAURICIO
DEGRADACIÓN	70%
IMPACTO	5
TIPO DE ACTIVO	PERSONAL

Tipo	**ID**	**Amenaza**	**Exposición/Vulnerabilidad**	**RIESGO ACTUAL**				
							4	Extremo
				Frecuencia (F)		**R**	**NR**	
ERRORES Y	**E.7**	Deficiencias en la organización	No hay exposición o vulnerabilidad, por parte de esta amenaza.	Baja	3	15	4	Extremo

Tabla 34. Estimación del riesgo activo coordinador de sistemas. (Continuación)

	E.19	Fugas de información	Las personas contratadas están atadas a cláusulas de confidencialidad.	Baja	3	15	4	Extremo
	E.28	Indisponibilidad del personal	Daño a la disponibilidad de cada una de las personas influyentes en la dependencia.	Baja	3	15	4	Extremo
ATAQUES INTENCIONADOS	**A.28**	Indisponibilidad del personal	Daño a la disponibilidad de la información.	Baja	3	15	4	Extremo
	A.29	Extorsión	Influenciarían al personal capacitado.	Baja	3	15	4	Extremo
	A.30	Ingeniería social (picaresca)	Intervención de personas con fines no éticas.	Baja	3	15	4	Extremo

Fuente: Autoría propia

Tabla 35. Estimación de la probabilidad activo programador

ACTIVO TI	**PROGRAMADOR**							
ADMINISTRADOR	PIMIENTO CARDENAS WILSON MAURICIO							
DEGRADACIÓN	70%							
IMPACTO	5							
TIPO DE ACTIVO	PERSONAL							
Tipo	**ID**	**Amenaza**	**Exposición/Vulnerabilidad**	**RIESGO ACTUAL**				
							4	Extremo
				Frecuencia (F)		**R**	**NR**	
ERRORES Y	**E.7**	Deficiencias en la organización	No hay exposición o vulnerabilidad, por parte de esta amenaza.	Baja	3	15	4	Extremo

Tabla 35. Estimación de la probabilidad activo programador. (Continuación)

	E.19	Fugas de información	Las personas contratadas están atadas a cláusulas de confidencialidad.	Baja	3	15	4	Extremo
	E.28	Indisponibilidad del personal	Daño a la disponibilidad de cada una de las personas influyentes en la dependencia.	Baja	3	15	4	Extremo
ATAQUES INTENCIONADOS	**A.28**	Indisponibilidad del personal	Daño a la disponibilidad de la información.	Baja	3	15	4	Extremo
	A.29	Extorsión	Influenciarían al personal capacitado.	Baja	3	15	4	Extremo
	A.30	Ingeniería social (picaresca)	Intervención de personas con fines no éticas.	Baja	3	15	4	Extremo

Fuente: Autoría propia

Tabla 36. Estimación de la probabilidad activo ingeniero auxiliar/ soporte técnico

ACTIVO TI	**INGENIERO AUXILIAR/ SOPORTE TÉCNICO**
ADMINISTRADOR	PIMIENTO CARDENAS WILSON MAURICIO
DEGRADACIÓN	40%
IMPACTO	3
TIPO DE ACTIVO	PERSONAL

Tipo	**ID**	**Amenaza**	**Exposición/Vulnerabilidad**	**RIESGO ACTUAL**				
							2	Intolerable
				Frecuencia (F)		**R**	**NR**	
ERRORES Y	**E.7**	Deficiencias en la organización	No hay exposición o vulnerabilidad, por parte de esta amenaza.	Baja	3	9	2	Intolerable

Tabla 36. Estimación de la probabilidad activo ingeniero auxiliar/ soporte técnico. (Continuación)

	E.19	Fugas de información	Las personas contratadas están atadas a cláusulas de confidencialidad.	Baja	3	9	2	Intolerable
	E.28	Indisponibilidad del personal	Daño a la disponibilidad de cada una de las personas influyentes en la dependencia.	Baja	3	9	2	Intolerable
ATAQUES INTENCIONADOS	**A.28**	Indisponibilidad del personal	Daño a la disponibilidad de la información.	Baja	3	9	2	Intolerable
	A.29	Extorsión	Influenciarían al personal capacitado.	Baja	3	9	2	Intolerable
	A.30	Ingeniería social (picaresca)	Intervención de personas con fines no éticas.	Baja	3	9	2	Intolerable

Fuente: Autoría propio

2.