ANÁLISIS Y EVALUACIÓN DE RIESGOS EN EL CENTRO DE DESARROLLO E INNOVACIÓN TECNOLÓGICA – CEDIT DE LA UNIVERSIDAD FRANCISCO DE PAULA SANTANDER OCAÑA

LIBARDO ANDREY QUINTERO GONZÁLEZ

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA

ESCUELA DE CIENCIAS BÁSICAS TECNOLOGIA E INGENIERÍA

ESPECIALIZACION EN SEGURIDAD INFORMÁTICA

OCAÑA

2017

ANÁLISIS Y EVALUACIÓN DE RIESGOS EN EL CENTRO DE DESARROLLO E INNOVACIÓN TECNOLÓGICA - CEDIT DE LA UNIVERSIDAD FRANCISCO DE PAULA SANTANDER OCAÑA

LIBARDO ANDREY QUINTERO GONZÁLEZ

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

DIRECTOR:

SALOMÓN GONZÁLEZ GARCÍA

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA

ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGIA E INGENIERÍA

ESPECIALIZACION EN SEGURIDAD INFORMATICA

OCAÑA

2017

Nota de aceptación.

_____
_____
_____
_____
_____
_____

Firma del director de proyecto

Firma del jurado

CONTENIDO

pág.
INTRODUCCIÓN 9
1. DEFINICION DEL PROBLEMA 11
1.1. DESCRIPCIÓN 11
1.2. FORMULACIÓN DEL PROBLEMA 12
2. JUSTIFICACIÓN 13
3. OBJETIVOS 15
3.1. OBJETIVO GENERAL 15
3.2. OBJETIVOS ESPECÍFICOS 15
5. MARCO REFERENCIAL 17
5.1. ANTECEDENTES 17
5.2. MARCO CONTEXTUAL 20
5.3. MARCO TEÓRICO 22
5.4. MARCO CONCEPTUAL 31
5.5. MARCO LEGAL 34
6. DISEÑO METODOLÓGICO 36
6.1. TIPO DE INVESTIGACIÓN 36
6.2. POBLACIÓN Y MUESTRA 36
6.3. INSTRUMENTOS DE RECOLECCIÓN DE INFORMACIÓN 37
6.4. METODOLOGÍA DE DESARROLLO 37
7. ACTIVOS PRESENTES EN EL CEDIT 39
8. VALORACIÓN DE ACTIVOS 41
9. AMENAZAS 44
9.1. IDENTIFICACIÓN DE AMENAZAS 44
9.2. VALORACIÓN DE AMENAZAS 46
10. PROBABILIDAD E IMPACTO DE LOS ACTIVOS 56
10.1. PROBABILIDAD DE OCURRENCIA 56
10.2. MEDICIÓN DE IMPACTO 56
11. ESCALA DE RIESGOS 66
12. CONTROLES 80
13. LISTA DE CHEQUEO 104

14. CONCLUSIONES.....117
15. INFORME Y RECOMENDACIONES 118
16. DIVULGACIÓN.....121
BIBLIOGRAFIA.....122
ANEXOS.....124

LISTA DE TABLAS

pág.

Tabla 1 Activos de la empresa....39
Tabla 2 Escala de Valoración....41
Tabla 3 Valoración de Activos....41
Tabla 4 Rango de Frecuencia de las amenazas....46
Tabla 5 Impacto en los activos....46
Tabla 6 Resumen Valoración de amenazas....47
Tabla 7 Probabilidad de Ocurrencia....56
Tabla 8 Escala de impacto....56
Tabla 9 Tabla de Probabilidad e Impacto de las amenazas en los activos....57
Tabla 10 Tabla de escala de riesgos....66
Tabla 11 Matriz de Riesgo....67
Tabla 12 Lista de Controles....82
Tabla 13 Lista de Chequeo....104

LISTA DE FIGURAS

pág.

Figura 1: Estructura de MAGERIT ..... **¡Error! Marcador no definido.**

ANEXOS

pág.

Anexo A. Resumen RAE.....124

INTRODUCCIÓN

Antes de que los sistemas informáticos llegaran para mejorar los procesos en las organizaciones, el tratamiento que se daba al principal activo con que cuentan las mismas, es decir la información o datos, era guardada en papel y almacenada en contenedores físicos, los cuales se exponían a ciertos riesgos que iban desde cómo se transportaban, almacenaban y posteriormente como se podía acceder a la información sin generar nuevos riesgos que estaban cada vez menos controlados, dificultando el procesamiento y veracidad de los datos almacenados.

Con la aparición de los sistemas informáticos y la digitalización de la información se mejoró evidentemente escenarios como la utilización de grandes espacios físicos para el almacenamiento de la información, pero más allá de optimizar los espacios de almacenamiento, los sistemas informáticos permitieron optimizar el análisis y el procesamiento de los datos.

Siendo así no se podría desconocer que el riesgo ante el almacenamiento y procesamiento de la información está presente, es más se puede afirmar que ante la facilidad del manejo de la información que brindan los sistemas, el peligro a su falta de integridad o veracidad puede aumentar si no se cuenta con un sistema integral de seguridad informática.

El trabajo colaborativo, los accesos a la internet y el brindar a otros usuarios acceso a los sistemas e información propia de una organización son factores que han hecho que los riesgos ante una vulnerabilidad en el sistema de información aumenten considerablemente, siendo fundamental para una compañía identificar cuáles de sus recursos son los que requieren de una mayor atención en cuanto al control de acceso y los permisos que deben tener los diferentes usuarios a la hora de acceder al sistema.

En este sentido la seguridad informática dirigida a los sistemas automatizados y la seguridad de la información se deben entender como el conjunto de normas establecidas como medidas preventivas y reactivas que una organización debe adoptar con el fin de poder salvaguardar la integridad de la información contenida dentro de su infraestructura tecnológica y su estructura física, buscando siempre poder mantener la confidencialidad, disponibilidad e integridad.

El Centro de Desarrollo e Innovación Tecnológica de la Universidad Francisco de Paula Santander Ocaña (CEDIT), es una dependencia que se encuentra adscrito a la División de Investigación y Extensión (DIE), la cual nace al evidenciarse la necesidad de fortalecer los vínculos de la comunidad ocañera con la extensión e investigación, con el propósito de generar conocimiento, desarrollo e innovación tecnológica en las diferentes áreas de la ciencia más específicamente en las relacionadas con las tecnologías de la Información y las Comunicaciones (TIC), mediante investigación científica y el desarrollo tecnológico de excelencia.[1] Todo esto contribuye en la región promoviendo una cultura de investigación en innovación tecnológica, integrando el conocimiento con las políticas del estado en función del desarrollo socioeconómico del país potenciando los sectores científicos, académicos y tecnológicos para hacer parte del desarrollo y fortalecimiento de la capacidad tecnológica de la industria regional y nacional.

Son cada vez mayores las amenazas a las que se expone una organización, en este caso el CEDIT, dentro de su operatividad produce información confidencial, la cual debe ser compartida entre las tres unidades operativas que conforma el equipo de trabajo, los riesgos del trabajo colaborativo al compartir datos pueden dejar en evidencia las vulnerabilidades que dentro de su estructura organizativa y operacional puede atentar contra la integridad, confidencialidad y veracidad de la información. En este sentido la seguridad informática dentro del CEDIT debe garantizar que el material y los recursos tecnológicos se usen dentro de los parámetros establecidos que permitan conservar la disponibilidad, autenticidad y confidencialidad de la información.

Con el desarrollo del presente proyecto se busca a través del análisis y la evaluación de los riesgos de la seguridad informática del Centro de Desarrollo e Innovación Tecnológica CEDIT, detectar las amenazas y vulnerabilidades de tal manera que se fortalezca la protección de la información clasificada del CEDIT, por tal motivo se espera obtener como resultado un informe detallado en el cual se evidencien los riegos potenciales clasificados en la seguridad informática.

[1] CEDIT – Quiénes somos. [en línea]. 2016. [Citado 06 de Marzo de 2016]. Disponible en: https://cedit.ufpso.edu.co/index-1.html

1. DEFINICION DEL PROBLEMA

1.1. DESCRIPCIÓN

El Centro de Desarrollo de Innovación Tecnológica CEDIT, identificado como una dependencia de la Universidad Francisco de Paula Santander Ocaña, genera desde cada una de sus tres unidades operativas información confidencial y de gran importancia para la generación de proyectos de innovación y emprendimiento dirigidos especialmente al área de la ciencia y la tecnología. Actualmente el CEDIT está organizado en tres unidades.

- Unidad de Investigación y desarrollo de nuevas tecnologías
- Unidad de generación y ejecución de proyectos
- Unidad de relaciones externas, comunicación y trabajo social.

Cada una de ellas maneja desde su operación información de vital importancia para la unidad en sí, para el CEDIT y por ende para la Universidad, ya que desde su integralidad esta información además de permitir la gestión y operación de proyectos tecnológicos, también es utilizada para mostrar los avances en cuanto a la gestión y el trabajo de extensión que la Universidad promueve desde esta dependencia.

Actualmente el CEDIT no cuenta con una política que permita establecer los mecanismos para la salvaguarda de la información y los recursos tecnológicos que tienen a su cargo, así como tampoco se tiene una metodología formalmente establecida a través de la cual sus miembros entiendan y tengan claro los riesgos a los que exponen la información que generan.

Situaciones como pérdida o duplicidad de la información y el acceso de usuarios no autorizados a la información clasificada de los diferentes proyectos que se generan y gestionan dentro del Centro de Desarrollo e Innovación Tecnológica CEDIT, son los problemas que se detectan y se pretenden corregir a través del análisis y evaluación de los riesgos de la seguridad informática de esta dependencia de la Universidad Francisco de Paula Santander Ocaña.

1.2. FORMULACIÓN DEL PROBLEMA

¿Cómo el análisis y la evaluación de los riesgos de la seguridad informática ayudará a disminuir riesgos a los que está expuesta la información confidencial en el Centro de Desarrollo e Innovación Tecnológica CEDIT de la Universidad Francisco de Paula Santander Ocaña?

2. **JUSTIFICACIÓN**

El presente proyecto es importante para la Universidad Francisco de Paula Santander Ocaña, ya que, dentro de su programa de extensión, la Universidad ha liderado proyectos tecnológicos que han permitido a la comunidad de Ocaña y su provincia entrar en el conocimiento de las nuevas tecnologías de la información y las comunicaciones TIC, sin estar vinculados directamente como estudiantes, docentes o administrativos de la Universidad.

Siendo así el Centro de Desarrollo e Innovación Tecnológica CEDIT, ha formulado, gestionado y ejecutado estos proyectos, guardando dentro de su sistema de información todos los datos e información clasificada generada desde la ejecución de ellos. En tal caso para la Universidad es de vital importancia que toda esta información de proyectos este salvaguardada de manera íntegra, de tal manera que se tenga disponible y se garantice que los datos obtenidos a partir de la ejecución de los proyectos sean veraces y estén disponibles en todo momento para la presentación de informes que permiten mostrar los resultados obtenidos y el liderazgo de la Universidad en los temas de tecnología en la región.

El Centro de Desarrollo e Innovación Tecnológica – CEDIT, podrá a partir del resultado del presente proyecto tener mayor conocimiento y por consiguiente control sobre sus activos, brindando mayor protección a los datos, a través de políticas de seguridad informática y de la información las cuáles estén formalmente establecidas, donde se contemplen medidas de protección contra la pérdida y modificación de la información, priorizando su confidencialidad, integridad y su disponibilidad.

Con el desarrollo del presente proyecto se beneficiarán todas y cada una de las demás dependencias de la Universidad, en las cuales no se tenga implementado un sistema de seguridad informática, ya que, a partir del análisis y evaluación de los riesgos de seguridad informática en el CEDIT, se ayudará a proteger la información de esta dependencia, sirviendo como modelo y guía para que en las otras dependencias se evalué la seguridad de la información a partir de sus propias necesidades.

Para cada uno de los trabajadores del CEDIT, será importante ya que les permite conocer los riesgos potenciales para la perdida de información y el control de los

accesos a la información que cada uno de ellos maneja. Si bien es cierto que no se pueden tomar correctivos ante cualquier situación si no se conocen los errores o fallas que se comenten en la salvaguarda de la información, este proyecto les permite identificar dichos factores de riesgo. Para los estudiantes y la comunidad universitaria será un proyecto guía para el desarrollo de otras propuestas dirigidas a mejorar los sistemas de seguridad informática en empresas u organizaciones que requieran garantizar la integridad, confidencialidad y disponibilidad de su información.

Es importante resaltar que si no se conoce al detalle la situación de vulnerabilidad y riesgo a la que se está sometiendo la información producida en el CEDIT, se corre el riesgo que en algún momento se presenten situaciones que pongan en peligro la autenticidad, veracidad y disponibilidad de la información.

3. OBJETIVOS

3.1. OBJETIVO GENERAL

Realizar un análisis y evaluación de los riesgos existentes en el Centro de Desarrollo e Innovación Tecnológica – CEDIT de la Universidad Francisco de Paula Santander Ocaña

3.2. OBJETIVOS ESPECÍFICOS

- Realizar el diagnóstico de los activos de información presentes en el CEDIT.
- Aplicar las herramientas informáticas para determinar las falencias existentes en los activos y determinar los riesgos a los que se está expuesto.
- Identificar mecanismos de control y gestión que permitan minimizar las vulnerabilidades encontradas en el análisis y evaluación de los riesgos del sistema informático del CEDIT.
- Elaborar un informe detallado en el cual se establecen recomendaciones basadas en los hallazgos realizados, de tal manera que a partir de este informe el CEDIT pueda definir a futuro un sistema de seguridad informático ajustado a sus necesidades.

4. ALCANCE Y DELIMITACIÓN

El planteamiento de este proyecto se realiza para poder analizar y evaluar los riesgos de seguridad a los que se expone la información generada en el Centro de Innovación Tecnológica - CEDIT de la Universidad Francisco de Paula Santander Ocaña, dentro de su alcance se incluye la seguridad de la información y de los equipos tecnológicos que le permiten a esta dependencia operar y buscar el cumplimiento de los objetivos planteados. Así mismo el resultado del análisis y la evaluación será la base para la formulación de una política de seguridad informática, que permita optimizar la salvaguarda de los datos y activos físicos.

Teniendo en cuenta que cada organización es diferente y tiene sus procedimientos propios, no es posible utilizar otros estudios de seguridad informática para que sean aplicados al CEDIT, por ello se tomarán solo como referencia otras evaluaciones realizadas, teniendo en cuenta que los requerimientos de seguridad informática del CEDIT son propios y se generan a partir de su operatividad, en la cual se deben establecer las prioridades y necesidades de las tres unidades que conforman esta dependencia de la Universidad Francisco de Paula Santander Ocaña.

El área geográfica seleccionada para el desarrollo del proyecto, está orientada al Centro de Desarrollo de Innovación Tecnológica - CEDIT, adscrito a la División de Investigación y Extensión DIE de la Universidad Francisco de Paula Santander Ocaña.

5. MARCO REFERENCIAL

5.1. ANTECEDENTES

No se tienen antecedentes de que para el Centro de Desarrollo e Innovación Tecnológica – CEDIT, de la Universidad Francisco de Paula Santander Ocaña, se haya desarrollado un proyecto para el análisis y evaluación de los riesgos de la seguridad informática.

Sin embargo, si se tienen antecedentes de este tipo de proyectos como trabajos de grado dirigidos a otras organizaciones, dentro de los cuales se mencionan los siguientes:

- El trabajo realizado por Perafán Ruiz (2014), sobre Análisis de Riesgos de la Seguridad de la Información para la Institución Universitaria Colegio Mayor Del Cauca[2], pone en evidencia cómo al día de hoy los sistemas de información se han convertido en parte fundamental para las organizaciones, y los sistemas, datos e información conllevan una gran responsabilidad en el logro de los objetivos, los cuales pueden mejorarse por medio de una correcta sistematización y documentación. Al referirse de tratamiento de información se habla de aspectos como el manejo de documentos en medios físicos, así como su almacenaje y fácil recuperación, mejor conocido como gestión documental, además, se resaltan aspectos importantes como la forma de almacenamiento de los datos digitales, modelos de respaldo de información, planes de contingencia o de continuidad del negocio, sistemas físicos de protección y accesibilidad a sitios o áreas restringidas. Este trabajo muestra como a través del análisis de los riesgos a de la seguridad informática, se generan controles que permiten mejorar y normalizar los procesos de la Universidad.

- El trabajo realizado por Patiño Alpala (2014), Propuesta de actualización, apropiación y aplicación de Políticas de Seguridad Informática en una empresa corporativa, Propolsinecor[3], éste con la finalidad de realizar una valoración de los activos informáticos, análisis de amenazas, vulnerabilidades y riesgos que pueden existir al tratarse de seguridad informática, lo que puede terminar afectando los recursos, incluso el prestigio de la compañía; para mitigar los riesgos que puedan presentarse

[2] Perafán Ruiz , John Jairo. Caicedo Cuchimba, Mildred. Análisis de Riesgos de la Seguridad de la Información para la Institución Universitaria Colegio Mayor Del Cauca. [en línea]. 20 de Octubre de 2014. [Citado 09 de Marzo de 2016]. Disponible en http://repository.unad.edu.co/bitstream/10596/2655/3/76327474.pdf

[3] Patiño Alpalpa , Luis Olmedo, Mildred. Propuesta de actualización, apropiación y aplicación de políticas de seguridad informática en una empresa corporativa, PROPOLSINECOR. [en línea]. 26 de Marzo de 2014. [Citado 09 de Marzo de 2016]. Disponible en http://repository.unad.edu.co/bitstream/10596/2742/1/12973210.pdf

es necesario actualizar, apropiarse e implementar políticas claras de Seguridad de la Información, que sean acordes a la organización y a las y actividades que desempeña, éstas deben ser conocidas y aprobadas por la alta gerencia, difundidas e implementadas por la organización y todos sus miembros. Con este proyecto se busca una actualización y apropiación de políticas de seguridad de la información, que protejan los activos de información, en base a la infraestructura y últimos procesos de manejo de información implementados en la compañía, se estudió el marco teórico referente al tema, se identificaron los activos de información, vulnerabilidades y amenazas en la seguridad informática y así estructurar una matriz de riesgos que resultó en acciones de solución a corto, mediano y largo plazo, con el propósito de eliminar o mitigar el riesgo informático y salvaguardar activos de información que son el eje principal de toda gestión de seguridad de la información.

- El trabajo realizado por Cruz Rodríguez (2010), titulado Modelo de Seguridad para la Medición de Vulnerabilidades y Reducción de Riesgos en Redes de Datos[4]; en el que la seguridad informática en las redes de comunicación se considera como un tema muy importante de abordar, pues debido a un fallo en ella puede resultar muy costoso en lo relativo a la productividad, eficiencia, pérdida de datos e información valiosa, es recomendable el uso de modelos y prototipos que ayuden a medir la importancia de la información manejada para con esto realizar una detección de vulnerabilidades y riesgos que pueden existir en dicha red y por tanto poder minimizarlos. Se propone crear un modelo de seguridad informática conociendo los problemas de inseguridad existentes, los ataques y amenazas a las que se enfrentan las redes empresariales conectadas o en uso a través de internet y dar soluciones tecnológicas, para garantizar un adecuado nivel de seguridad informática en la trasmisión de datos, medir vulnerabilidades, reducir los riesgos de la redes de datos y facilitar al administrador de red conocer dichas vulnerabilidades, riesgos en donde a su vez puedan minimizarlos para la protección de la información. Basado en la recopilación de información que permite la identificación de activos de la compañía a proteger, así como los factores de riesgos a los cuales se ve expuesta la red de datos de la mencionada compañía , por otra parte, se deduce mediante pruebas y herramientas empleadas en la infraestructura de la red para identificar vulnerabilidades, amenazas y riesgos, que luego son analizadas y valoradas utilizando técnicas debidamente para presentar en el informe final para el administrador de la red de datos en la compañía, todo esto con el fin de implementar procedimientos de gestión de la seguridad de la información de acuerdo al

[4] Cruz Mendoza, Erik Ivan. Rodríguez Duque, Diana Vanessa. Modelo de seguridad para la mediciónde vulnerabilidades y reducción de riesgos en redes de datos. [en línea]. Noviembre de 2010. [Citado 13 de Marzo de 2016]. Disponible en http://docplayer.es/3908802-Instituto-politecnico-nacional-t-e-s-i-s-modelo-de-seguridad-para-la-medicion-de-vulnerabilidades-y-reduccion-de-riesgos-en-redes-de-datos.html

modelo propuesto, que se basa en verificar, probar e intentar vulnerar aquellos agujeros de seguridad informática. Por la similitud en el desarrollo del análisis de riesgos para el CEDIT, este trabajo de investigación puede aportar elementos fundamentales para el desarrollo del proyecto.

- El trabajo realizado por Sánchez Cañadas (2011), dirigido a la Planificación de un Sistema de Gestión de Seguridad en la Información[5], indicando cómo los sistemas de información están expuestos, cada vez más, a un elevado número de amenazas, que provechando las vulnerabilidades que dichos activos tienen, se transforman en riesgos sobre los activos de la información. Resaltando la importancia de asegurar la disponibilidad, la autenticidad y la confidencialidad de la información se ha transformado, a día de hoy, en una necesidad, que se soluciona al realizar un proceso establecido paso a paso, que esté documentado y que sea socializado en toda la empresa, para que así se logre contrarrestar los riesgos a los que se está expuesto. El proceso que se plantea usar es el SGSI (Sistema de Gestión de la Seguridad de la Información). Este trabajo se utilizará como referencia en cuanto a que define las partes para poder establecer el sistema. Como resultado se indican los controles implantados para intentar reducir al mínimo aquellos riesgos detectados en la organización.

- El trabajo desarrollado por Tirado Goyeneche (2012), Análisis de Riesgos en la Universidad Francisco de Paula Santander Cúcuta[6], en el que se menciona cómo las políticas de seguridad informática surgen y se ven como una herramienta organizacional para concienciar toda la organización sobre la importancia y sensibilidad de la información y servicios críticos que permiten a la empresa crecer y mantenerse competitiva, a través del buen uso de los recursos informáticos y la información, manteniéndolos libres de peligros, daños o riesgos. Este documento de referencia pretende describir a partir de la abstracción de los de la Universidad Francisco de Paula Santander; cómo es el funcionamiento de la empresa y el desarrollo de cada uno de los procesos, desde el punto de vista de la Seguridad Informática; enfocándonos principalmente en la participación de los recursos, tanto físicos como tecnológicos, que en conjunto con la infraestructura física, deben proporcionar seguridad de la información, reconociendo a la misma como un activo fundamental para el desarrollo y sostenimiento de la empresa.

[5] Sánchez Cañadas, Raúl. Planificación de un SGSI (Sistema de Gestión de la Seguridad de la Información). [en línea]. 26 de Enero de 2011. [Citado 15 de Marzo de 2016]. Disponible en http://upcommons.upc.edu/handle/2099.1/11415

[6] Tirado Goyeneche. Análisis de Riesgos en la Universidad Francisco de Paula Santander. [en línea]. Marzo de 2012. [Citado 15 de Marzo de 2016]. Disponible en http://seguridadinformaticaufps.wikispaces.com/file/view/AN%C3%81LISIS+DE+RIESGOS+UNIVERSIDAD+FRANCISCO+DE+PAULA+SANTANDER.docx

5.2. MARCO CONTEXTUAL

Nombre de la empresa: Universidad Francisco de Paula Santander Ocaña

Dependencia: Centro de desarrollo e innovación tecnológica – CEDIT

Reseña histórica: En noviembre de 1973 se suscribió un contrato para la realización de un estudio de factibilidad denominado "un centro de educación superior para Ocaña", que fue terminado y sugirió la creación pronta de un programa de educación a nivel de tecnología en énfasis en ciencias sociales, matemáticas y física. En diciembre de ese mismo año, el rector de la Universidad Francisco de Paula Santander, José Luis Acero Jordán, le envió copia de dicho estudio al ICFES, Instituto que conceptuó que el proyecto para abrir el centro de estudios en Ocaña, era recomendable.[7]

Según Acuerdo No. 003 del 18 de Julio de 1974, por parte del Consejo Superior de la Universidad Francisco de Paula Santander Cúcuta, se crea la Universidad Francisco de Paula Santander Ocaña, como máxima expresión cultural y patrimonio de la región; como una entidad de carácter oficial seccional, con AUTONOMÍA administrativa y patrimonio independiente, adscrito al Ministerio de Educación Nacional.

Su primer coordinador, el doctor Aurelio Carvajalino Cabrales, buscó un lugar adecuado para funcionar la sede, en los claustros Franciscanos al costado del templo de la Gran Convención, y con las directivas del colegio José Eusebio Caro, se acordó el uso compartido del laboratorio de física.[8]

En 1975 comenzó la actividad académica en la entonces seccional de la Universidad Francisco de Paula Santander con un total de 105 estudiantes de Tecnología en Matemáticas y Física, y su primera promoción de licenciados en Matemáticas y Física se logró el 15 de diciembre de 1980. La consecución de 27 hectáreas de la Hacienda El Rhin, en las riveras del Río Algodonal, en comodato a la Universidad por 50 años, que la antigua Escuela de Agricultura de Ocaña cedió a la Universidad, permitió la creación del programa de Tecnología en Producción Agropecuaria, aprobado por el Consejo Superior mediante el Acuerdo No. 024 del

[7] Universidad Francisco de Paula Santander Ocaña – ColombiaAcuerdo 085. [en línea]. 2014. [Citado 20 de Febrero de 2017]. Disponible en [7] https://ufpso.edu.co/ftp/pdf/acuerdos/acuerdo_08512diciem2014.pdf

[8] Universidad Francisco de Paula Santander Ocaña – Colombia. Reseña Histórica. [en línea]. 2016. [Citado 26 de Marzo de 2016]. Disponible en https://ufpso.edu.co/Historia

21 de agosto de 1980, y luego el ICFES otorgó la licencia de funcionamiento el 17 de febrero del año siguiente. Luego se crean las Facultades.[9]

Misión

La Universidad Francisco de Paula Santander Ocaña, institución pública de educación superior, es una comunidad de aprendizaje y autoevaluación en mejoramiento continuo, comprometida con la formación de profesionales idóneos en las áreas del conocimiento, a través de estrategias pedagógicas innovadoras y el uso de las tecnologías; contribuyendo al desarrollo nacional e internacional con pertinencia y responsabilidad social.[10]

Visión

La Universidad Francisco de Paula Santander Ocaña para el **2019**, será reconocida por su excelencia académica, cobertura y calidad, a través de la investigación como eje transversal de la formación y el uso permanente de plataformas de aprendizaje; soportada mediante su capacidad de gestión, la sostenibilidad institucional, el bienestar de su comunidad académica, el desarrollo físico y tecnológico, la innovación y la generación de conocimiento, bajo un marco de responsabilidad social y ambiental hacia la proyección nacional e internacional.[11]

Marco legal

El Centro de desarrollo e innovación tecnológica de la Universidad fue creado bajo la resolución 260 del 18 de Diciembre del año 2013.

Objetivos y funciones

Contribuir en la región a la implementación de una cultura de investigación e innovación tecnológica, integrando el conocimiento con las políticas del estado en función del desarrollo socioeconómico del país.

---

[9] Universidad Francisco de Paula Santander Ocaña – Colombia. Reseña Histórica. [en línea]. 2016. [Citado 26 de Marzo de 2016]. Disponible en https://ufpso.edu.co/Historia

[10] Universidad Francisco de Paula Santander Ocaña – Colombia. Misión. [en línea]. 2016. [Citado 26 de Marzo de 2016]. Disponible en http://web.ufpso.edu.co/inseguridad/universidad.html

[11] Universidad Francisco de Paula Santander Ocaña – Colombia. Visión. [en línea]. 2016. [Citado 26 de Marzo de 2016]. Disponible en http://web.ufpso.edu.co/inseguridad/universidad.html

Potenciar los sectores científicos, académicos y tecnológicos para hacer parte del desarrollo y fortalecimiento de la capacidad tecnológica de la industria regional y nacional.

Incentivar y aumentar los niveles de uso y aplicación de la innovación tecnológica en la sociedad del común, para que de esa manera sean partícipes de su propio desarrollo.

Fortalecer las competencias del talento humano de la Universidad y en el sector académico de la región, en la búsqueda constante de una visión innovadora de las tecnologías y la aplicación en lo industrial y lo social.

Contribuir a consolidar un sistema de investigación, desarrollo e innovación tecnológica que responda a las necesidades y requerimientos de nuestra región además de seguir las estrategias del estado colombiano.

5.3. MARCO TEÓRICO

Seguridad informática: Se refiere a las características y condiciones de los sistemas de procesamiento de datos y su correspondiente almacenamiento, de tal manera que a través de la forma en que se realice se pueda garantizar su confidencialidad, integridad y disponibilidad.

La seguridad informática requiere que dentro de una organización se deben tener identificados y controlados los posibles riesgos en los que puede incurrir un sistema informático. Para ello toda organización debe conocer el peligro, clasificarlo y protegerse de él, de manera que se pueda minimizar el impacto o los daños en el momento de presentarse un evento indeseado que atente contra la integridad de la información.

Hoy en día las tecnologías de la información han llegado a ser herramientas fundamentales para la óptima operación en las organizaciones, a través de ellas se mejoran los procesos y permite a sus miembros contar con información oportuna y veraz cada vez que se requiera.

La información es el activo más importante con el que cuenta toda organización y por ende es a este activo al que se debe brindar mecanismos de seguridad, así mismo cuando en una organización se tienen implementados sistemas de

seguridad de la información, se deben realizar estudios y análisis que permitan evaluar y medir la eficacia de dicho sistema ante los riesgos a los cuales se enfrenta una organización y sus sistemas de información.

Cuando grandes cantidades de datos están almacenados electrónicamente, son incluso más vulnerables que cuando se tienen en forma manual. Estas vulnerabilidades se pueden originar por diferentes factores, técnicos, institucionales, ambientales, incluso por malas decisiones administrativas. Estos sistemas computarizados son vulnerables por las siguientes razones:

- Complejidad en los sistemas de información: Un sistema de información grande al tratar de ser respaldado no se podrá hacer de forma manual. La información se torna demasiado voluminosa para ser tratada manualmente.
- Registros propios del computador: En general no quedan rastros de los cambios en los sistemas computarizados, porque los registros de computadoras solo pueden ser leídos por la máquina.
- Procedimientos computarizados: Parecen ser invisibles y no son bien entendidos y auditados por el personal.
- Por cambios en el core del sistema: Los cambios en los propios sistemas automatizados son más costosos y con frecuencia más complejos que los cambios en los sistemas manuales.
- El desarrollo y operación de los sistemas: Todos los sistemas a diario se ven expuestos al abuso por parte del personal que puedan tener cierto grado de conocimiento para alterarlos y que busquen otra cosa diferente a acatar las normas y políticas que existan y no tengan miedo de romperlas con tal de conseguir su fin. Estas personas pueden lograr hacer cambios en el sistema sin tener autorización para ellos ya que no conlleva a la actividad principal de la empresa, el modificar ciertos aspectos del sistema o alterar equipos y procesos puede afectar directamente la institución, incluso se está expuestos a que estas personas saquen información sin autorización con el ánimo de usarla para un fin completamente distinto para el cuál fue recopilada.
- Sistemas automatizados: Aunque las posibilidades de desastre en los sistemas automatizados no son mayores que en los sistemas manuales, el efecto puede ser mucho mayor. En algunos casos, todos los registros del sistema pueden quedar destruidos y perdidos para siempre.
- Acceso a los sistemas: Todos los sistemas tienen relaciones de entrada y salida con muchas personas, lo que hace más fácil la recolección de la información, pero a medida que los sistemas crecen se hacen más complejo controlar y proteger la información.
- Procesamiento de datos: En los sistemas, la información se procesa de una manera más extensa y según como se programe, de una manera mejor, comparándola con sistemas manuales, pues incluso en los sistemas

pueden existir errores y fallos en el procesamiento de los datos. Todo el proceso que se lleve a cabo en el procesamiento de la información requiere el uso de controles que permitan hacer más efectiva cada vez la recolección y tratamiento de datos y así lograr unos datos de salidas más confiables.

Antes de definir lo que es el análisis de riesgos, tenemos que considerar lo que es un riesgo, a continuación, se exponen las siguientes definiciones:

- Según Fernando Izquierdo Duarte: "El riesgo es un incidente o situación, que ocurre en un sitio concreto durante un intervalo de tiempo determinado, con consecuencias positivas o negativas que podrían afectar el cumplimiento de los objetivos.[12]
- Según Alberto Cancelado González: El riesgo es una condición del mundo real en el cual hay una exposición a la adversidad, conformada por una combinación de circunstancias del entorno, donde hay posibilidad de pérdidas.[13]
- Según Martín Vilches Troncoso: El riesgo es cualquier variable importante de incertidumbre que interfiera con el logro de los objetivos y estrategias del negocio.

En cualquier momento puede ocurrir un hecho no deseado o puede que no ocurra uno deseado, el proceso de análisis de los riesgos debe ser el proceso más importante en la gestión de la seguridad de la información, se parte de la gestión de los riesgos, con lo que se decide qué hacer con ellos, ya sea eliminarlos, ignorarlos, mitigarlos o controlarlos, pero siempre basados en la criticidad de los activos de información más importantes.

Se han tratado de identificar los tipos de riesgos existentes para así hacer más fácil la aplicación de un análisis de ellos, entre los más comunes que se han identificado se encuentran los riesgos de negocios, inherentes, de auditoría, operativos y de control, profesionales y de tecnología, entre otros. A nivel general se debe tener claro el objetivo que se busca obtener del análisis de riesgo, estableciendo una escala valorativa y priorización los riesgos, con una escala definida y los riesgos catalogados y organizados todo se debe recopilar en una matriz que refleje el nivel de impacto según la escala de valoración que haya sido establecida, y así, determinar al final de todo el proceso el estado actual en materia de seguridad de la información.

[12] Administración de riesgos de tecnología de información de una empresa del sector informático. [en línea]. 2015. [Citado 20 de Febrero de 2017]. Disponible en http://repositorio.espe.edu.ec/handle/21000/10826

[13] Análisis de Riesgos de la Seguridad de la Información. [en línea]. 2015. [Citado 20 de Febrero de 2017]. Disponible en http://www.gestiopolis.com/administracion-de-riesgos-en-tecnologia-informatica/

A la hora de determinar el método a utilizar para poder evaluar la seguridad informática en una organización, se puede pensar que el análisis de los riesgos es el más apropiado ya que permite identificar el grado de importancia de cada uno de los riesgos encontrados y su impacto, pero no es así, ya que tal como se define en un artículo realizado por la Universidad de Pamplona, GUIA PARA LA EVALUACION DE SEGURIDAD EN UN SISTEMA[14], por Luz Marina Santos, se enumeran tres métodos tradicionales.

- Análisis de riego
- Lista de chequeo
- Auditoria

Siendo así la definición del método a utilizar para evaluar la seguridad informática depende del grado de conciencia en el que se encuentren los encargados del sistema. Por ejemplo para el caso específico del Centro de Desarrollo e Innovación Tecnológica – CEDIT, de la Universidad Francisco de Paula Santander Ocaña, se debe utilizar inicialmente la lista de chequeo para verificar los principios y prácticas de seguridad estándares, ya que según el artículo referenciado es el método indicado para situaciones en las cuales las pérdidas de información esperadas y la frecuencia de las amenazas no está clara. Posteriormente se aplicaría el análisis de riesgos, una vez se tengan detectados cuales serían las pérdidas de información esperadas y la frecuencia de las amenazas.

Tal como se menciona en el artículo referenciado en el párrafo anterior, el proceso de identificar, analizar y valorar, mitigar o transferir el riesgo es generalmente caracterizado como manejo del riesgo [KRAU-99]. Hay una serie de preguntas que se hacen en este proceso:

- ¿Que podría ocurrir? (amenaza)
- ¿Sí ocurre, cuánto daño podría causar? (impacto)
- ¿Qué tan a menudo podría ocurrir?
- ¿Qué tan ciertas son las respuestas a las anteriores preguntas?

Una vez respondidas acertadamente las anteriores preguntas, se responden ahora las siguientes:

- ¿Qué puede ser hecho? (mitigación del riesgo)
- ¿Cuál es el costo de la medida? (anual)
- ¿Es la medida efectiva? (análisis costo/beneficio)

[14] GUIA PARA LA EVALUACION DE SEGURIDAD EN UN SISTEMA. [en línea]. 2015. [Citado 20 de Febrero de 2017]. Disponible en http://52.1.175.72/portal/sites/all/themes/argo/assets/img/Pagina/pamplona.doc

El análisis de los riesgos busca hacer una cuantificación del impacto que puede conllevar al materializarse una amenaza, para esto se plantean cuatro etapas, hacer una planeación del análisis de riesgos que se va a implementar, identificar las amenazas y vulnerabilidades que puedan existir, valorar el impacto y la frecuencia de los riesgos y por último plantear un control o tratamiento de los riesgos.

Para sistemas muy grandes se recomienda que se planee por aparte cada subsistema que haga parte del sistema en general, para que de esta manera se facilite la presentación de cada subsistema y los informes los comprendan mejor los miembros de la organización.

Las amenazas a las que se pueda ver expuesto un sistema pueden ser ocasionadas por muchas fuentes, el personal que maneje el sistema, daños físicos en los equipos y sus componentes, caídas de los enlaces, incluso daños naturales, entre muchos más. Realizando el análisis se podría llegar a identificarse el origen de las amenazas que existan y poder reducir los riesgos. Se puede hacer un análisis basado en algunos puntos que ayuden a entender las vulnerabilidades.[15]

- Vulnerabilidades de software: aquí se pueden encontrar actualizaciones no probadas, incompatibilidad entre los programas usados, daños por degradación, errores en las aplicaciones, errores en el procesamiento de los datos, errores en el sistema operativo.

- Vulnerabilidades de hardware: se encuentran los daños en los equipos, fallas eléctricas, fallas en los planes de mantenimiento, errores en la seguridad física de los equipos, desastres naturales, fallas en protección contra incendio, inundación y humedad, cortes de energía.

- Vulnerabilidades de datos: se pueden encontrar modificación de los datos no autorizados, ingreso de datos erróneos, alteración de las operaciones, datos incompletos.

- Vulnerabilidades administrativas: aquí se encuentran errores del personal administrativo, en la creación o aplicación de políticas y procedimientos, falta de seguimiento y control, desinformación, no actualizarse en temas de

[15] GUIA PARA LA EVALUACION DE SEGURIDAD EN UN SISTEMA. [en línea]. 2015. [Citado 20 de Febrero de 2017]. Disponible en 52.1.175.72/portal/sites/all/themes/argo/assets/img/Pagina/pamplona.doc

seguridad, falta de compromiso del personal que hace uso del software, y no preocuparse por hallar fallas y corregirlas.

- Vulnerabilidades de comunicaciones: se encuentran fallos en el cableado estructura, fallas en diagrama de red establecido, errores o fallas en los dispositivos de comunicación, fallas en los canales de intercomunicación, falta de protección a los equipos activos de la red, sobrecarga al flujo de red.

- Vulnerabilidades de personal: en este punto se encuentra falta de concientización del personal, falta de seguimiento a los procesos del personal, no manejar controles de acceso, no tener niveles de acceso, tener la información expuesta, no limitar las modificaciones que se puedan hacer.

A través de entrevistas también se pueden hallar vulnerabilidades del sistema, pero estas entrevistas deben ser basadas en principios y las buenas prácticas seguridad para que sean provechosas y arrojen los resultados que se esperan tener de ellas.

Al momento de querer valorar el impacto y la frecuencia al momento de ocurrir una amenaza se puede recurrir a los métodos cuantitativos o cualitativos. El método cuantitativo consiste en revisar información que previamente se haya recolectado, la frecuencia se determina con base a los registro que haya, como logs, bitácoras y demás, el impacto en cambio, se determina en base al valor del número de operaciones que el sistema de procesar al ocurrir un evento. Para el impacto existe una fórmula que se expresa de la siguiente manera:

*I = valor recurso * factor de exposición*

Por el impacto se ve afectada confidencialidad, integridad y disponibilidad de los recursos del sistema.

Algunos métodos utilizan como elemento para valorar los riesgos la posibilidad de ocurrencia de presentarse una amenaza.

Si se habla de ponderación de los factores de riesgo, esta implica darle un valor de importancia al riesgo en términos de porcentaje basado en el impacto que pueda ocasionar en la organización, en la posibilidad que se pueda convertir en realidad.

También se hace una valoración del riesgo, lo que consiste en medir la pérdida a la que se puede incurrir y la probabilidad de que ocurra esta pérdida, para ellos se basa en el siguiente esquema.

Cuadrante	Valoración del riesgo
Impacto significante y probabilidad Alta	Alto
Impacto significante y probabilidad Baja	Medio-alto
Impacto insignificante y probabilidad Alta	Medio-bajo
Impacto insignificante y probabilidad Baja	Bajo

Para entender mejor la valoración se puede ver de la siguiente manera:

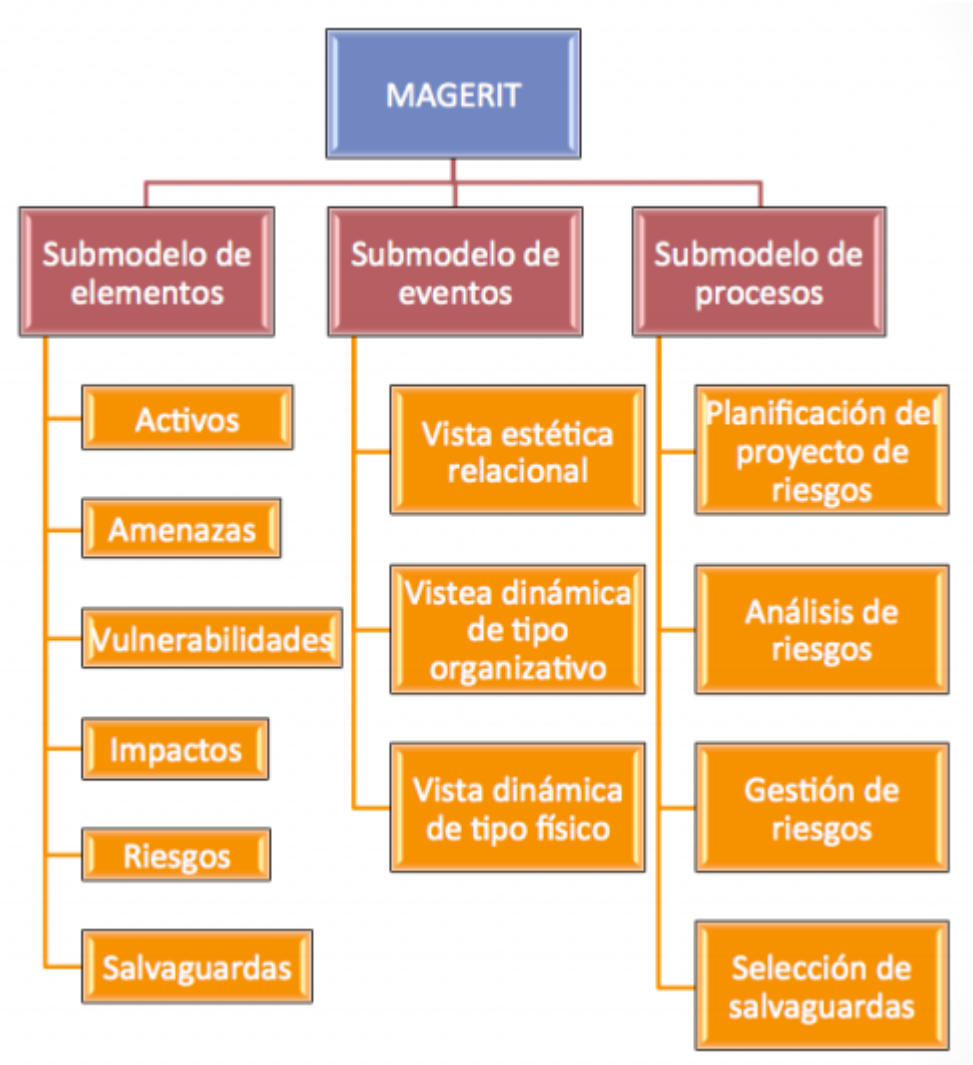
- Riesgo alto: Exponerse a la pérdida total.
- Riesgo medio: No se alcanza una pérdida total, pero, sin embargo, se debe accionar de una manera inminente para asegurar la continuidad y operatividad del negocio.
- Riesgo bajo: Las pérdidas no alcanzan a afectar significativamente la empresa y no generan gran impacto en las operaciones.

- ***ISO 27001:***
  Esta es una norma internacional en la cual se describe la manera como se debe gestionar la seguridad de la información en una empresa. La publicación emitida en el año 2013 es la más reciente y desde entonces se conoce por su nombre completo ISO/IEC 27001:2013. Esta norma se puede implementar en cualquier tipo de organización que se desee, revisada y redactada por los mejores especialistas del mundo en el tema, proporciona una metodología para implementar la gestión de la seguridad de la información. Cualquier empresa puede ser certificada en esta norma, la cual se ha convertido en la más importante para la seguridad de la información a nivel mundial y por ello muchas empresas han certificado su cumplimiento, dando mayor reconocimiento y credibilidad a sus procesos.
  Esta norma vela principalmente por proteger la confidencialidad, integridad y disponibilidad de la información de la empresa que la implemente, realizando una evaluación de los riesgos que permita identificar cuáles son los potenciales problemas que podrían afectar la información y posteriormente definir lo que se debe hacer para evitar la materialización de estos riesgos. Se determinan controles y políticas que son los que permiten mitigar los riesgos que se hayan determinado que se puedan presentar. Por

lo general, las empresas ya tienen todo su hardware y software, pero no hacen un uso seguro de ellos, por lo que la mayor parte de la implementación de ISO 27001 se relacionada con determinar reglas organizacionales necesarias para prevenir violaciones de la seguridad.
En general la ISO 27001 embarca la implementación de múltiples políticas, procedimientos, controles y demás dentro de sistema de gestión de seguridad de la información (SGSI).

- ***Metodología de análisis del riesgo:***
  Son desarrolladas para la identificación de la falta de controles y el establecimiento de un plan de contramedidas. Existen dos tipos: Las cuantitativas y las cualitativas, de las que existen gran cantidad de ambas clases. La metodología que el proyecto adopta es MAGERIT (Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información): El esquema completo de Etapas, Actividades y Tareas del Sub-modelo de Procesos de MAGERIT el cual puede aplicarse o no en su totalidad, dependiendo de la complejidad misma del proyecto es el siguiente:

Figura 1: Estructura de MAGERIT



Fuente: https://goo.gl/images/nbL2Ao

El principal objetivo de la metodología de Análisis y Gestión de Riesgos de los Sistemas de Información, mejor conocida como MAGERIT es el implementar la gestión de riesgos para que así se tomen decisiones por parte de los órganos de gobierno. La metodología Magerit busca centrarse en el análisis de riesgos para conocer lo seguro o inseguros que pueden ser los sistemas. El mayor inconveniente que se presenta es la complejidad del problema al que se puede enfrentar, pues hay muchos elementos qué considerar y si el análisis no es riguroso, las conclusiones a las que se logre llegar podrían no ser confiables. La idea que se busca obtener con Magerit es una aproximación metódica que no deje lugar a la improvisación, ni dependa de la arbitrariedad, sino que sea un proceso paso a paso y bien documentado que permita detectar todas las amenazas que puedan existir y los riesgos en los que se pueda incurrir.

Con la metodología Magerit se busca alcanzar objetivos directos como concienciar al personal que hace parte de las organizaciones de información que existe una serie de riesgos que a su vez existe una gran necesidad de gestionarlos; proporcionar un método con el cuál se logre analizar los riesgos que genera el uso de tecnologías de la información y comunicaciones (TIC); con toda la metodología lograr un tratamiento adecuado y oportuno y así mantener los riesgos bajo control.

Además de estos, existe un objetivo indirecto que es instruir la organización para implementar de una forma adecuada procesos de evaluación, auditoría, certificación o acreditación, dependiendo de las necesidades de cada una.

5.4. MARCO CONCEPTUAL

- ***Sistema informático:*** Un sistema informático está conformado por un conjunto de elementos que funcionan relacionándose entre sí en busca de lograr un objetivo o fin común. En este caso los elementos que conforman el sistema informático son el hardware, el software y las personas que interactúan con ellos. Un sistema Informático puede formar parte de un sistema de información.

- ***Administración de los datos:*** La administración de los datos contribuye al adecuado manejo de los mismos, tomando en cuenta que, según su principio fundamental, son propiedad de la institución como un todo. Por ello, es necesario que la información se considere pilar estratégico de las entidades, como base fundamental de la administración y planeación institucional, y en este sentido debe ser el director (DI) o vicepresidentes de la información los principales defensores de la implementación de estos sistemas. Las acciones deben estar orientadas a administrar la información considerando los datos como recursos institucionales, y en este sentido, definir su accesibilidad tomando en cuenta los diferentes niveles (todo el personal o los directivos) según corresponda. De acuerdo a este criterio, se debe analizar la información que requiere cada área para cumplir su misión, y en función de ello, será el acceso a los datos. Como resultado, los datos pueden pertenecer exclusivamente a un área, sin que el resto pueda disponerla. De manera general, toda entidad debe establecer una política de información que defina claramente las condiciones de acceso y distribución, tomando como base reglas vinculadas a la clasificación, estandarización e inventario de la misma. Además se debe registrar una traza de procedimientos y responsabilidades, especificando criterios como:

unidades que comparten información, puntos donde es posible que se distribuya, responsables de actualizar y mantenerla.[16]

- ***Política de seguridad informática:*** Una política de seguridad informática, es un documento que contiene los procedimientos y planes que salvaguarden los recursos informáticos dentro de los cuales se incluye la información. Son una forma de comunicación con el personal, ya que las mismas constituyen un canal formal de actuación, en relación con los recursos y servicios informáticos de la organización.

  Las políticas de seguridad establecen las reglas y procedimientos que regulan la forma en que una organización previene, protege y maneja los riesgos de diferentes datos, sin importar el origen de estos.

  Como parte integral de un Sistema de Gestión de Seguridad de la Información (SGSI), un manual de normas y políticas de seguridad, trata de definir; qué, por qué, de qué y cómo se debe proteger la información. Estos engloban una serie de objetivos, estableciendo los mecanismos necesarios para lograr un nivel de seguridad adecuado a las necesidades establecidas dentro de la organización.[17]

- ***Riesgos:*** Los riesgos se determinan como la posibilidad de que se produzca un impacto determinado en los activos de una organización.
  Los riesgos son medibles y controlables.

- ***Vulnerabilidad:*** Debilidad de un activo que puede ser explotada por una amenaza para materializar una agresión sobre dicho activo.[18]

- ***Check list:*** La lista de chequeo se considera como el método de evaluación más antiguo que existe, utilizado ampliamente en procesos de auditoría, en seguridad informática se centra en revisar si existen o no controles administrativos, operativos y técnicos, pero sin evaluar la efectividad de los controles que se implanten. Además se identifica que se cumplan los principios de seguridad generalmente aceptados (GSSPs).[19]

---

[16] J. Benavides Abajo; J. M. Olaizola Bartolomé; E. Rivero Cornelio. *SQL: Para usuarios y programadores*. Tercera Edición. Madrid: Paraninfo, 1997. ISBN:84-283-1821-2.

[17] Esquemas de Seguridad Informática. Políticas de Seguridad Definición de Política. [en línea]. 2014. [Citado 05 de Agosto de 2017]. Disponible en: http://redyseguridad.fi-p.unam.mx/proyectos/seguridad/DefinicionPolitica.php

[18] ISO 27001: Vulnerabilidades de la organización. [en línea]. 2015. [Citado 20 de Febrero de 2017]. Disponible en: http://www.pmg-ssi.com/2015/06/iso-27001-vulnerabilidades-de-la-organizacion/

[19] Organización de un centro de cómputo. [en línea]. 2016. [Citado 10 de Julio de 2017]. Disponible en: https://es.slideshare.net/berkcornie/organizacin-de-un-centro-de-cmputos-64599219

- ***Tecnologías de la Información y las comunicaciones TIC:*** El conjunto de tecnologías que permiten la adquisición, producción, almacenamiento, tratamiento, comunicación, registro y presentación de informaciones, en forma de voz, imágenes y datos contenidos en señales de naturaleza acústica, óptica o electromagnética.

  Las TIC incluyen la electrónica como tecnología base que soporta el desarrollo de las telecomunicaciones, la informática y el audiovisual.

- ***Seguridad informática:*** Se refiere a las características y condiciones de los sistemas de procesamiento de datos y su correspondiente almacenamiento, de tal manera que a través de la forma en que se realice se pueda garantizar su confidencialidad, integridad y disponibilidad.

  La seguridad informática requiere que dentro de una organización se deben tener identificados y controlados los posibles riesgos en los que puede incurrir un sistema informático. Para ello toda organización debe conocer el peligro, clasificarlo y protegerse de él, de manera que se pueda minimizar el impacto o los daños en el momento de presentarse un evento indeseado que atente contra la integridad de la información.

- ***Administración de los datos:*** La administración de los datos contribuye al adecuado manejo de los mismos, tomando en cuenta que, según su principio fundamental, son propiedad de la institución como un todo. Por ello, es necesario que la información se considere pilar estratégico de las entidades, como base fundamental de la administración y planeación institucional, y en este sentido debe ser el director (DI) o vicepresidentes de la información los principales defensores de la implementación de estos sistemas. Las acciones deben estar orientadas a administrar la información considerando los datos como recursos institucionales, y en este sentido, definir su accesibilidad tomando en cuenta los diferentes niveles (todo el personal o los directivos) según corresponda. De acuerdo a este criterio, se debe analizar la información que requiere cada área para cumplir su misión, y en función de ello, será el acceso a los datos. Como resultado, los datos pueden pertenecer exclusivamente a un área, sin que el resto pueda disponerla. De manera general, toda entidad debe establecer una política de información que defina claramente las condiciones de acceso y distribución, tomando como base reglas vinculadas a la clasificación, estandarización e inventario de la misma. Además se debe registrar una traza de procedimientos y responsabilidades, especificando criterios como: unidades que comparten información, puntos donde es posible que se distribuya, responsables de actualizar y mantenerla.[20]

[20] J. Benavides Abajo; J. M. Olaizola Bartolomé; E. Rivero Cornelio. *SQL: Para usuarios y programadores*. Tercera Edición. Madrid: Paraninfo, 1997. ISBN:84-283-1821-2.

- ***Activo:*** Recurso del sistema de información necesario para que la organización funcione correctamente y alcance los objetivos propuestos.[21]

- ***Disponibilidad***: o disposición de los servicios a ser usados cuando sea necesario. La carencia de disponibilidad supone una interrupción del servicio. La disponibilidad afecta directamente a la productividad de las organizaciones.[22]

- ***Integridad***: Se trata del mantenimiento de las características de completitud y corrección de los datos. Con esto se previene que la información sea manipulada, corrupta o incompleta.

- ***Confidencialidad***: Se refiere a que la información llegue solamente a las personas autorizadas, a para quien es dirigida en realidad y pueda hacer un uso adecuado de ella.

- ***Autenticidad:*** Se conoce como la garantía que puede brindar una autoridad de la originalidad y buena procedencia de ciertos datos.

- ***Riesgo:*** Se hace referencia a una estimación del grado de exposición a que una amenaza le ocurra a los activos causando daños a la Organización.

- ***Análisis de riesgos:*** Es el proceso sistemático con el que se determinan a los riesgos que está expuesta una organización y se estima la magnitud de ellos.

- ***Probabilidad:*** posibilidad de ocurrencia de una acción previamente identificada, mide la frecuencia con la cual se obtiene un resultado, se iguala la idea de probabilidad con el concepto de riesgo.

- ***Impacto:*** medir la consecuencia al materializarse una amenaza.

5.5. MARCO LEGAL

En Colombia se tienen vigentes las siguientes leyes dentro del marco de seguridad de la información.

[21] Términos relacionados con la seguridad informática. [en línea]. 2016. [Citado 20 de Febrero de 2017]. Disponible en https://www.ecured.cu/Seguridad_Inform%C3%A1tica

[22] Pilar. Herramientas para el análisis y la gestión de riesgos. [en línea]. 2016. [Citado 20 de Febrero de 2017]. Disponible en: http://administracionelectronica.gob.es/pae_Home/dms/pae_Home/documentos/Estrategias/pae_Tecnimap/pae_TECNIMAP_2004/pae_COM_2004-Perspectivas_de_futuro/6_022.pdf

LEY 603 DE 2000. Esta ley se refiere a la protección de los derechos de autor en Colombia. Recuerde: el software es un activo, además está protegido por el Derecho de Autor y la Ley 603 de 2000 obliga a las empresas a declarar si los problemas de software son o no legales.

LEY ESTATUTARIA 1266 DEL 31 DE DICIEMBRE DE 2008. 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.

LEY 1273 DEL 5 DE ENERO DE 2009. Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - 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.

LEY 1341 DEL 30 DE JULIO DE 2009. Por la cual se definen los principios y conceptos sobre la sociedad de la información y la organización de las Tecnologías de la Información y las Comunicaciones -TIC-, se crea la Agencia Nacional del Espectro y se dictan otras disposiciones.

LEY ESTATUTARIA 1581 DE 2012. Entró en vigencia la Ley 1581 del 17 de octubre 2012 de PROTECCIÓN DE DATOS PERSONALES, sancionada siguiendo los lineamientos establecidos por el Congreso de la República y la Sentencia C-748 de 2011 de la Corte Constitucional.

Como resultado de la sanción de la anunciada ley toda entidad pública o privada, cuenta con un plazo de seis meses para crear sus propias políticas internas de manejo de datos personales, establecer procedimientos adecuados para la atención de peticiones, quejas y reclamos, así como ajustar todos los procesos, contratos y autorizaciones a las disposiciones de la nueva norma.

6. DISEÑO METODOLÓGICO

6.1. TIPO DE INVESTIGACIÓN

Para el presente estudio se utilizará el método basado en una investigación descriptiva con enfoque cualitativo, ya que se pretende identificar los riesgos de seguridad de la información, detectando situaciones en cada una de las unidades bajo las cuales se encuentra dividido el equipo de trabajo del CEDIT, realizando una descripción exacta de las actividades, procesos y personas con el fin de extraer experiencias significativas que contribuyan al conocimiento y evaluación de la seguridad de la información y la protección de los datos.

El enfoque cualitativo para el análisis del riesgo, permitirá obtener un valor a partir de dos elementos fundamentales como son, la probabilidad de que se produzca un evento y el impacto que generaría si se llegara a presentar un evento.

Ahora bien para realizar el análisis de los riesgos en seguridad informática, existen metodologías específicas, que permiten analizar el sistema, identificar las amenazas y las vulnerabilidades asociadas a los procesos y activos de la organización. Dentro de las metodologías más comunes se tienen Magerit, Octave y Mehari, siendo así para el desarrollo del presente proyecto se analizará cuál de estas metodologías se ajusta más, para que sea aplicada en el CEDIT.

6.2. POBLACIÓN Y MUESTRA

La población objeto de estudio en el presente proyecto son los miembros del Centro de desarrollo e innovación tecnológica – CEDIT de la Universidad Francisco de Paula Santander Ocaña. Actualmente el CEDIT cuenta con doce (12) puestos de trabajo, los cuales están discriminados de la siguiente forma.

- Director del CEDIT
- Secretaria
- Unidad de emprendimiento: Tres (4) funcionarios
- Unidad de proyectos: Tres (3) funcionarios
- Unidad de relaciones: Tres (3) funcionarios

6.3. INSTRUMENTOS DE RECOLECCIÓN DE INFORMACIÓN

Los instrumentos a utilizar para la recolección de información son los Check List y entrevistas, así mismo se utilizarán técnicas de monitoreo mencionadas en el párrafo anterior.

Las técnicas de recolección de datos se aplicarán a cada una de las unidades que conforman el CEDIT, en primera instancia se realizará una entrevista la cual será diseñada con el fin de poder conocer de manera libre y espontánea la forma como los miembros del CEDIT llevan a cabo los procedimientos de acceso, modificación y salvaguarda de la información.

Así mismo la entrevista se utilizará para determinar si los miembros del CEDIT reconocen la importancia que tiene la seguridad informática para la salvaguarda de la información manejada en cada uno de los procesos que ellos llevan a cabo.

Para la aplicación de los Check List se hará por unidades monitoreando en cada uno de ellos la existencia de controles para el tratamiento de la información.

Luego de haber recolectado la información, será analizada y tabulada con el fin de poder obtener resultados claros que permitan realizar una evaluación de los posibles riesgos en el Centro de desarrollo e innovación tecnológica de la Universidad.

Dentro de la ejecución del proyecto se aplicarán técnicas como Pentesting en redes LAN y WLAN, Detección de intrusos en Redes, Formulación de redes Seguras, Comportamiento de intrusos en diversas redes informáticas, Análisis de Botnets, Protocolos seguros basados a IPV6, Pentesting páginas web y Pentesting Bases de datos.

6.4. METODOLOGÍA DE DESARROLLO

Objetivo 1

Realizar diagnóstico de los activos de información presentes en el CEDIT.

- Actividad 1: Realizar un levantamiento del inventario de los activos presentes en el CEDIT, tomando de cada uno las características principales

- Actividad 2: Hacer una clasificación e identificación de todos los activos que se encuentren en el levantamiento.

Objetivo 2

Aplicar una metodología de evaluación de riesgos que permita definir las vulnerabilidades y amenazas de seguridad existentes, así mismo evaluar los riesgos de acuerdo con la escala definida en una metodología especifica.

- Actividad 1: Escoger la metodología que más se asemeje según la necesidad y los recursos con que se cuente.
- Actividad 2: Obtener toda la información que requiera del CEDIT la metodología escogida, para ser aplicada correctamente.
- Actividad 3: Hacer uso de toda la información recopilada y aplicar la metodología seleccionada para obtener los resultados.

Objetivo 3

Identificar mecanismos de control y gestión que permitan minimizar las vulnerabilidades encontradas en el análisis y evaluación de los riesgos del sistema informático del CEDIT.

- Actividad 1: Aplicar la metodología y analizar toda la información recopilada para identificar los riesgos y vulnerabilidades existentes.
- Actividad 2: Escoger los controles existentes que se puedan aplicar y más se ajusten a lo manejado y encontrado.

Objetivo 4

Elaborar un informe detallado en el cual se establecen recomendaciones basadas en los hallazgos realizados, de tal manera que a partir de este informe el CEDIT pueda definir a futuro un sistema de seguridad informático ajustado a sus necesidades.

- Actividad 1: Elaborar un informe basado en los hallazgos realizados y mediciones arrojadas según la metodología aplicada.
- Actividad 2: Ajustar el informe para dar solución al problema previamente identificado en el CEDIT.

7. ACTIVOS PRESENTES EN EL CEDIT

Se inició haciendo un levantamiento de los activos primordiales con los que cuenta el CEDIT, esto con el fin de conocer en sitio con lo que se está tratando y lo que se involucra en el avance del proyecto.

Los activos que se encuentran en el CEDIT son los siguientes, de acuerdo a la clasificación que se le da a cada uno de ellos.

Tabla 1 Activos de la empresa

Activos esenciales
Sistemas de Información de los proyectos Histórico personal que ha hecho uso de los recursos de CEDIT Manuales de usuario de lo desarrollado por medio del CEDIT Diccionario de datos
Arquitectura del sistema
Canales dedicados Dispositivos de irradiación de internet
Datos / Información
Sistema de información Copias de seguridad mensuales de la información y archivos importantes
Claves criptográficas
Claves de usuarios de la plataforma tecnológica Claves de servidores Claves de acceso externo Claves de acceso a zonas restringidas
Servicios
Página Web Correo Electrónico Telefonía (conexión de voz, buzón de voz, llamada en espera, menú de bienvenida, grabación de llamadas)
Aplicaciones (software)
Sistema de Información Paquete de ofimática Edición de audio y videos Sistemas operativos Aplicaciones de diseño Herramientas de desarrollo Aplicativos web Sistema de CCTV

Tabla1. (Continuación)

Equipos informáticos (Hardware)
Estaciones de trabajo
Escáner
Fotocopiadoras
Impresoras
Portátiles
Video Beam
Servidores
NAS
Firewalls
Switches
Router
Planta telefónica
Patch panel
Cámaras de seguridad
Soportes de información
NAS
Discos externos
Discos duros
Cintas magnéticas
Replicas ubicadas en otras ciudades
Servicios en la nube
Equipamiento auxiliar
UPS
PDU’s
Fibra óptica
Transceiver
Cableado estructurado
Tableros de operación
Inversores de administración de energía
Instalaciones
Edificaciones
Salas de espera
Cuartos de equipos de comunicación y seguridad
Cuartos de aires
Personal
Administrativos de la empresa
Usuarios
Vigilancia
Personal del área de sistemas

Fuente: El autor.

8. VALORACIÓN DE ACTIVOS

Se emplea la siguiente tabla de valoración:

Tabla 2 Escala de Valoración

Valor		Criterio
10	Extremo	Daño extremadamente grave
9	Muy alto	Daño muy grave
6-8	Alto	Daño grave
3-5	Medio	Daño importante
1-2	Bajo	Daño menor
0	Despreciable	Irrelevante a efectos prácticos

Fuente: El Autor.

Nomenclatura utilizada:
I (Integridad), C (Confiabilidad), D (Disponibilidad), A (Autenticidad), T (Trazabilidad)

Tabla 3 Valoración de Activos

Activo	I	C	D	A	T
Activos esenciales					
Sistemas de Información de los proyectos	10	10	10	10	10
Histórico personal que ha hecho uso de los recursos de CEDIT	10	10	10	10	10
Manuales de usuario de la plataforma	10	7	10	10	10
Diccionario de datos	9	9	9	9	9
Arquitectura del sistema					
Canales dedicados	10	10	10	10	10
Dispositivos de irradiación de internet	10	10	10	10	10
Datos / Información					
Sistema de información	10	10	10	10	8
Copias de seguridad mensuales de la información y archivos importantes	7	10	9	10	6
Claves criptográficas					
Claves de usuarios de la plataforma tecnológica	8	10	10	10	7
Claves de servidores	10	10	10	10	10
Claves de acceso externo	8	10	8	8	7
Claves de acceso a zonas restringidas	10	10	10	10	10

Tabla3. (Continuación)

Activo	I	C	D	A	T
Servicios					
Página Web	10	8	10	10	7
Correo Electrónico	8	8	8	8	8
Telefonía (conexión de voz, buzón de voz, llamada en espera, menú de bienvenida, grabación de llamadas)	8	7	10	8	7
Aplicaciones (software)					
Sistema de Información	10	10	10	10	10
Paquete de ofimática	8	8	9	8	8
Edición de audio y videos	8	8	8	8	8
Sistemas operativos	8	8	9	8	8
Aplicaciones de diseño	8	8	8	8	8
Herramientas de desarrollo	8	9	8	8	8
Aplicativos web	7	8	7	7	7
Sistema de CCTV	10	9	9	8	8
Equipos informáticos (Hardware)					
Estaciones de trabajo	8	8	9	9	8
Escáner	7	7	7	7	7
Fotocopiadoras	7	7	7	7	7
Impresoras	7	7	9	8	7
Portátiles	7	7	7	7	7
Video Beam	7	7	7	7	7
Servidores	10	10	10	10	10
NAS	8	9	9	9	9
Firewalls	8	10	10	10	10
Switches	8	10	10	8	8
Router	7	10	10	9	8
Planta telefónica	7	8	10	7	7
Patch panel	7	7	7	7	7
Cámaras de seguridad	8	9	10	8	8
Soportes de información					
NAS	7	9	9	9	7
Discos externos	7	9	9	9	7
Discos duros	7	8	9	9	7
Cintas magnéticas	10	10	9	9	9
Replicas ubicadas en otras ciudades	10	10	10	9	9
Servicios en la nube	9	10	10	9	9

Tabla 3. (Continuación)

Activo	I	C	D	A	T
Equipamiento auxiliar					
UPS	7	8	10	8	8
PDU's	7	8	10	8	7
Fibra óptica	9	8	10	8	8
Transceiver	9	8	10	8	8
Cableado estructurado	9	8	10	8	9
Tableros de operación	7	8	8	8	9
Inversores de administración de energía	7	8	8	8	7
Instalaciones					
Edificaciones	10	8	10	8	8
Salas de espera	10	8	8	9	7
Cuartos de equipos de comunicación y seguridad	8	10	10	8	7
Cuartos de aires	7	9	9	8	7
Personal					
Administrativos de la empresa	10	10	8	10	9
Usuarios	7	7	8	7	10
Vigilancia	10	10	10	10	9
Personal del área de sistemas	10	10	10	10	10

Fuente: El Autor.

9. AMENAZAS

9.1. IDENTIFICACIÓN DE AMENAZAS

Según el catálogo de amenazas presentes en el Libro II de MAGERIT, las amenazas posibles son:

[N] Desastres naturales

[N.1] Fuego
[N.2] Daños por agua
[N.*] Desastres naturales

[I] De origen industrial

[I.1] Fuego
[I.2] Daños por agua
[I.*] Desastres industriales
[I.3] Contaminación mecánica
[I.4] Contaminación electromagnética
[I.5] Avería de origen físico o lógico
[I.6] Corte del suministro eléctrico
[I.7] Condiciones inadecuadas de temperatura o humedad
[I.8] Fallo de servicios de comunicaciones
[I.9] Interrupción de otros servicios o suministros esenciales
[I.10] Degradación de los soportes de almacenamiento de la información
[I.11] Emanaciones electromagnéticas
[E] Errores y fallos no intencionados

[E.1] Errores de los usuarios

[E.2] Errores del administrador
[E.3] Errores de monitorización (log)
[E.4] Errores de configuración
[E.7] Deficiencias en la organización
[E.8] Difusión de software dañino
[E.9] Errores de [re-]encaminamiento
[E.10] Errores de secuencia
[E.14] Fugas de información
[E.15] Alteración de la información
[E.16] Introducción de falsa información
[E.17] Degradación de la información
[E.18] Destrucción de la información
[E.19] Divulgación de información
[E.20] Vulnerabilidades de los programas (software)
[E.21] Errores de mantenimiento / actualización de programas (software)

[E.23] Errores de mantenimiento / actualización de equipos (hardware)
[E.24] Caída del sistema por agotamiento de recursos
[E.25] Pérdida de equipos
[E.28] Indisponibilidad del personal

[A] Ataques deliberados

[A.4] Manipulación de la configuración
[A.5] Suplantación de la identidad del usuario
[A.6] Abuso de privilegios de acceso
[A.7] Uso no previsto
[A.8] Difusión de software dañino
[A.9] Reencaminamiento de mensajes
[A.10] Alteración de secuencia
[A.11] Acceso no autorizado
[A.12] Análisis de tráfico
[A.13] Repudio
[A.14] Interceptación de información (escucha)
[A.15] Modificación de información
[A.16] Introducción de falsa información
[A.17] Corrupción de la información
[A.18] Destrucción de la información
[A.19] Divulgación de información
[A.22] Manipulación de programas
[A.24] Denegación de servicio
[A.25] Robo de equipos
[A.26] Ataque destructivo
[A.27] Ocupación enemiga
[A.28] Indisponibilidad del personal
[A.29] Extorsión
[A.30] Ingeniería social

9.2. VALORACIÓN DE AMENAZAS

Tabla 4 Rango de Frecuencia de las amenazas

Amenaza	**Rango**	**Valor**
Frecuencia Muy Alta	1 vez al día	100
Frecuencia Alta	1 vez a la semana	70
Frecuencia Media	1 vez al trimestre	50
Frecuencia Baja	1 vez al semestre	10
Frecuencia muy Baja	1 vez al año	0

Fuente. El autor.

Tabla 5 Impacto en los activos

Impacto	**Valor**
Muy Alto	100
Alto	75
Medio	50
Bajo	20
Muy Bajo	5

Fuente. El Autor.

Tabla 6 Resumen Valoración de amenazas

Activos esenciales	Amenaza	Frecuencia	I	C	D	A	T
Sistemas de Información de los proyectos	[E.1] Errores de los usuarios	10	75%	-	-	75%	100
	[E.2] Errores del administrador	10	75%	-	75%	20%	%
	[E.3] Errores de monitorización (log)	5	15%	-	-	-	-
	[E.4] Errores de configuración	5	75%	-	15%	-	75%
	[E.14] Fugas de información	10	100%	100%	-	-	-
	[E.15] Alteración de la información	10	75%	100%	-	75%	-
	[E.16] Introducción de falsa información	50	-	75%	-	75%	50%
	[E.19] Divulgación de información	50	15%	100%	-	-	75%
	[E.24] Caída del sistema por agotamiento de	5	75%	20%	100%	-	-
	recursos	5	50%	50%	75%	-	-
	[A.4] Manipulación de la configuración	10	75%	75%	-	75%	-
	[A.5] Suplantación de la identidad del usuario	10	100%	100%	75%	-	-
	[A.6] Abuso de privilegios de acceso						-
	[A.24] Denegación de servicio						50%
Histórico personal que ha hecho uso de los recursos de CEDIT	[E.14] Fugas de información	5	50%	100%	-	-	-
	[E.15] Alteración de la información	5	-	75%	-	100	50%
	[E.16] Introducción de falsa información	5	75%	15%	-	%	50%
	[E.19] Divulgación de información	5	75%	100%	-	75%	-
						15%	
Manuales de usuario de lo desarrollado por medio del CEDIT	[E.1] Errores de los usuarios	10	50%	-	-	15%	75%
	[E.14] Fugas de información	5	20%	75%	-	-	-
Diccionario de datos	[E.14] Fugas de información	5	20%	75%	-	-	-
	[E.15] Alteración de la información	5	15%	-	-	15%	75%
	[E.19] Divulgación de información	10	-	100%	-	-	-

Tabla 6. (Continuación)

Arquitectura del sistema	Amenaza	Frecuencia	I	C	D	A	T
Canales dedicados	[I.8] Fallo de servicios de comunicaciones	5	75%	-	100%	-	75%
	[A.9] Reencaminamiento de mensajes	5	75%	75%	15%	-	-
	[A.12] Análisis de tráfico	5	15%	20%	-	-	-
	[A.14] Interceptación de información (escucha)	10	15%	75%	-	-	-
	[A.24] Denegación de servicio	5	100%	-	100%	-	50%
Dispositivos de irradiación de internet	[I.8] Fallo de servicios de comunicaciones	10	75%	-	100%	-	50%
	[E.1] Errores de los usuarios	5	-	-	15%	20%	75%
	[A.9] Reencaminamiento de mensajes	5	50%	50%	-	-	-
	[A.12] Análisis de tráfico	50	-	20%	-	-	-
	[A.14] Interceptación de información (escucha)	10	-	75%	-	-	-
Datos / Información	Amenaza	Frecuencia	I	C	D	A	T
Sistema de información	[E.2] Errores del administrador	10	-	-	-	50%	15%
	[E.14] Fugas de información	5	-	100%	-	-	-
	[E.15] Alteración de la información	5	75%	-	-	75%	100
	[E.24] Caída del sistema por agotamiento de	5	-	-	100%	-	%
	recursos	5	-	-	-	15%	75%
	[A.11] Acceso no autorizado	5	75%	-	100%	-	15%
	[A.24] Denegación de servicio						75%
Copias de seguridad mensuales de la información y archivos importantes	[N.1] Fuego	5	100%	-	15%	-	15%
	[N.2] Daños por agua	5	100%	-	15%	-	15%
	[I.10] Degradación de los soportes de almacenamiento de la información	5	75%	-	15%	15%	15%
	[E.14] Fugas de información	5	-	100%	-	-	-

Tabla 6. (Continuación)

Claves criptográficas	Amenaza	Frecuencia	I	C	D	A	T
Claves de usuarios de la plataforma tecnológica	[E.2] Errores del administrador [E.14] Fugas de información	5 5	- -	- 75%	- -	- -	50% -
Claves de servidores	[E.2] Errores del administrador [E.14] Fugas de información	5 5	- -	- 100%	- -	- -	50% -
Claves de acceso externo	[E.14] Fugas de información	5	-	15%	-	-	-
Claves de acceso a zonas restringidas	[E.14] Fugas de información	5	-	100%	-	-	-
Servicios	Amenaza	Frecuencia	I	C	D	A	T
Página Web	[I.8] Fallo de servicios de comunicaciones [E.24] Caída del sistema por agotamiento de recursos [A.24] Denegación de servicio	5 5 5	75% 100% 100%	- - -	100% 100% 100%	- - -	50% 20% 50%
Correo Electrónico	[E.2] Errores del administrador [A.9] Reencaminamiento de mensajes [A.11] Acceso no autorizado	5 5 10	- 75% -	- 75% 75%	- - 15%	15% 15% 15%	15% - 15%
Telefonía (conexión de voz, buzón de voz, llamada en espera, menú de bienvenida, grabación de llamadas)	[N.1] Fuego [N.2] Daños por agua [E.24] Caída del sistema por agotamiento de recursos [A.4] Manipulación de la configuración	5 5 5 5	- - - -	- - - -	15% 15% 75% -	- - - 15%	- - 15% 15%

Tabla 6. (Continuación)

Aplicaciones (software)	Amenaza	Frecuencia	I	C	D	A	T
Sistema de Información	[E.1] Errores de los usuarios	10	15%	-	-	15%	50%
	[E.14] Fugas de información	50	-	75%	-	-	-
	[E.15] Alteración de la información	10	75%	75%	-	20%	75%
	[E.24] Caída del sistema por agotamiento de recursos	5	-	-	100%	-	15%
	[A.4] Manipulación de la configuración	5	-	-	-	15%	15%
	[A.11] Acceso no autorizado	5	-	100%	50%	15%	-
	[A.24] Denegación de servicio	5	-	-	100%	-	15%
Paquete de ofimática	[E.1] Errores de los usuarios	10	-	-	-	15%	15%
	[E.20] Vulnerabilidades de los programas	10	-	15%	15%	-	-
	[E.21] Errores de mantenimiento / actualización de programas (software)	10	-	-	15%	15%	15%
Edición de audio y videos	[E.1] Errores de los usuarios	5	-	-	-	15%	15%
	[E.20] Vulnerabilidades de los programas (software)	5	-	15%	-	-	-
	[E.21] Errores de mantenimiento / actualización de programas (software)	10	-	-	-	15%	15%
Sistemas operativos	[E.1] Errores de los usuarios	50	-	-	-	15%	15%
	[E.8] Difusión de software dañino	5	-	15%	15%	15%	-
	[E.21] Errores de mantenimiento / actualización de programas (software)	10	-	-	-	15%	15%
	[A.4] Manipulación de la configuración	5	-	-	-	15%	-
Aplicaciones de diseño	[E.1] Errores de los usuarios	5	-	-	-	15%	15%
	[E.20] Vulnerabilidades de los programas (software)	5	-	15%	-	-	-
	[E.21] Errores de mantenimiento / actualización de programas (software)	10	-	-	-	15%	15%
Herramientas de desarrollo	[E.1] Errores de los usuarios	10	-	-	-	15%	15%
	[E.21] Errores de mantenimiento / actualización de programas (software)	10	-	-	15%	-	15%
Aplicativos web	[I.8] Fallo de servicios de comunicaciones	5	75%	-	100%	-	15%

Tabla 6. (Continuación)

Sistema de CCTV	[I.8] Fallo de servicios de comunicaciones	5	75%	-	100%	-	15%
	[E.14] Fugas de información	10	-	75%	-	-	-
	[A.4] Manipulación de la configuración	5	-	-	15%	15%	-
	[A.24] Denegación de servicio	5	-	-	100%	-	15%
Equipos informáticos (Hardware)	Amenaza	Frecuencia	I	C	D	A	T
Estaciones de trabajo	[N.2] Daños por agua	10	-	-	100%	-	15%
	[E.8] Difusión de software dañino	50	-	50%	50%	15%	-
	[E.23] Errores de mantenimiento / actualización de equipos (hardware)	10	-	-	15%	15%	15%
	[A.4] Manipulación de la configuración	50	-	15%	-	50%	15%
	[A.8] Difusión de software dañino	50	-	-	15%	15%	-
	[A.22] Manipulación de programas	50	-	-	-	15%	-
Escáner	[E.1] Errores de los usuarios	50	-	-	15%	15%	15%
Fotocopiadoras	[E.1] Errores de los usuarios	10	-	-	15%	15%	15%
	[E.23] Errores de mantenimiento / actualización de equipos (hardware)	10	-	-	-	15%	-
Impresoras	[E.1] Errores de los usuarios	10	-	-	15%	15%	15%
Portátiles	[N.2] Daños por agua	5	-	-	100%	-	15%
	[E.23] Errores de mantenimiento / actualización de equipos (hardware)	10	-	-	15%	15%	-
	[E.25] Pérdida de equipos	10	-	100%	100%	-	-
	[A.8] Difusión de software dañino	50	-	15%	15%	15%	-
	[A.22] Manipulación de programas	50	-	-	-	15%	-
	[A.25] Robo de equipos	5	-	75%	100%	-	15%
Video Beam	[E.1] Errores de los usuarios	5	-	-	15%	15%	-
	[E.25] Pérdida de equipos	5	-	-	100%	-	-
	[A.25] Robo de equipos	5	-	-	100%	-	-

Tabla 6. (Continuación)

Servidores	[E.3] Errores de monitorización (log)	5	-	-	-	-	50%
	[E.4] Errores de configuración	5	-	-	50%	15%	15%
	[E.8] Difusión de software dañino	5	50%	15%	15%	15%	15%
	[E.14] Fugas de información	5	-	75%	-	-	-
	[E.23] Errores de mantenimiento / actualización de equipos (hardware)	5	15%	-	15%	15%	15%
	[A.4] Manipulación de la configuración	5	-	-	15%	15%	15%
	[A.11] Acceso no autorizado	5	-	75%	20%	15%	-
NAS	[I.10] Degradación de los soportes de almacenamiento de la información	5	50%	-	15%	15%	15%
Firewalls	[E.3] Errores de monitorización (log)	5	-	-	-	-	75%
	[E.4] Errores de configuración	5	-	-	15%	15%	-
	[E.14] Fugas de información	5	-	75%	-	-	-
	[A.4] Manipulación de la configuración	5	50%	-	15%	15%	20%
	[A.11] Acceso no autorizado	5	-	75%	15%	15%	15%
Switches	[E.1] Errores de los usuarios	5	-	-	15%	15%	20%
	[A.4] Manipulación de la configuración	10	-	-	15%	15%	-
Router	[E.4] Errores de configuración	5	15%	-	15%	15%	15%
	[A.4] Manipulación de la configuración	10	-	-	15%	15%	-
	[A.12] Análisis de tráfico	5	-	50%	-	-	-
	[A.14] Interceptación de información (escucha)	5	-	75%	-	-	-
Planta telefónica	[E.1] Errores de los usuarios	10	-	-	15%	15%	20%
Patch panel	[E.1] Errores de los usuarios	5	-	-	15%	15%	20%
Cámaras de seguridad	[N.2] Daños por agua	5	-	-	100%	-	75%
	[A.14] Interceptación de información (escucha)	5	-	50%	-	-	-

Tabla 6. (Continuación)

Soportes de información	Amenaza	Frecuencia	I	C	D	A	T
NAS	[I.10] Degradación de los soportes de almacenamiento de la información	5	75%	-	15%	15%	15%
	[A.17] Corrupción de la información	5	20%	-	15%	50%	-
Discos externos	[I.4] Contaminación electromagnética	5	-	-	15%	15%	-
	[E.14] Fugas de información	5	-	75%	-	-	-
	[E.25] Pérdida de equipos	10	-	-	100%	-	15%
Discos duros	[I.4] Contaminación electromagnética	5	-	-	15%	15%	-
	[E.14] Fugas de información	5	-	100%	100%	-	-
Cintas magnéticas	[I.4] Contaminación electromagnética	5	-	-	15%	15%	-
	[I.10] Degradación de los soportes de almacenamiento de la información	5	75%	-	15%	15%	15%
	[A.17] Corrupción de la información	5	75%	-	15%	50%	-
Replicas ubicadas en otras ciudades	[I.7] Condiciones inadecuadas de temperatura o humedad	5	20%	-	15%	-	-
	[I.8] Fallo de servicios de comunicaciones	10	-	-	100%	-	20%
	[I.10] Degradación de los soportes de almacenamiento de la información	5	15%	-	15%	15%	-
	[E.3] Errores de monitorización (log)	50	-	-	-	-	75%
	[E.4] Errores de configuración	5	-	-	15%	15%	15%
	[A.17] Corrupción de la información	5	75%	-	-	50%	-
	[A.19] Divulgación de información	5	-	100%	-	-	-
Servicios en la nube	[I.8] Fallo de servicios de comunicaciones	5	-	-	100%	-	50%
	[E.14] Fugas de información	5	-	100%	-	-	-
	[A.17] Corrupción de la información	5	75%	-	-	20%	15%
	[A.19] Divulgación de información	5	-	75%	-	15%	-
Equipamiento auxiliar	Amenaza	Frecuencia	I	C	D	A	T
UPS	[N.1] Fuego	5	-	-	100%	-	15%
	[N.2] Daños por agua	5	-	-	100%	-	15%
	[I.6] Corte del suministro eléctrico	10	-	-	50%	-	15%
PDU’s	[I.6] Corte del suministro eléctrico	10	-	-	100%	-	15%

Tabla 6. (Continuación)

Fibra óptica	[N.*] Desastres naturales	10	-	-	100%	-	20%
Transceiver	[I.8] Fallo de servicios de comunicaciones	10	-	-	100%	-	20%
Cableado estructurado	[I.4] Contaminación electromagnética	5	-	-	15%	15%	15%
Tableros de operación	[I.4] Contaminación electromagnética	5	-	-	15%	15%	15%
	[I.6] Corte del suministro eléctrico	10	-	-	100%	-	15%
Inversores de administración de energía	[I.4] Contaminación electromagnética	5	-	-	15%	15%	15%
	[I.6] Corte del suministro eléctrico	10	-	-	100%	-	15%
Instalaciones	Amenaza	Frecuencia	I	C	D	A	T
Edificaciones	[N.1] Fuego	5	-	-	50%	-	-
	[N.*] Desastres naturales	5	-	-	100%	-	-
	[I.6] Corte del suministro eléctrico	10	-	-	50%	-	15%
	[A.11] Acceso no autorizado	5	-	15%	15%	15%	-
	[A.26] Ataque destructivo	5	-	-	20%	-	-
Salas de espera	[N.1] Fuego	5	-	-	50%	-	-
	[A.26] Ataque destructivo	5	-	-	20%	-	-
	[A.27] Ocupación enemiga	5	-	-	100%	-	-
Cuartos de equipos de comunicación y seguridad	[I.7] Condiciones inadecuadas de temperatura o humedad	5	-	-	15%	-	-
	[A.11] Acceso no autorizado	5	-	15%	15%	15%	-
	[A.25] Robo de equipos	5	-	75%	100%	50%	-
	[A.26] Ataque destructivo	5	-	-	50%	-	-
Cuartos de aires	[N.2] Daños por agua	5	-	-	100%	-	-
	[I.7] Condiciones inadecuadas de temperatura o humedad	5	-	-	15%	15%	-

Tabla 6. (Continuación)

Personal	Amenaza	Frecuencia	I	C	D	A	T
Administrativos de la empresa	[E.1] Errores de los usuarios	10	-	-	15%	15%	50%
	[E.14] Fugas de información	50	75%	75%	-	-	-
	[E.28] Indisponibilidad del personal	50	-	-	100%	-	-
	[A.5] Suplantación de la identidad del usuario	5	-	100%	15%	50%	15%
	[A.6] Abuso de privilegios de acceso	50	-	-	15%	-	15%
	[A.28] Indisponibilidad del personal	5	-	-	100%	-	-
	[A.29] Extorsión	5	-	-	15%	50%	-
	[A.30] Ingeniería social	10	-	50%	15%	15%	-
Usuarios	[E.1] Errores de los usuarios	5	-	-	-	15%	15%
	[E.14] Fugas de información	50	20%	-	-	-	-
	[A.30] Ingeniería social	10	-	-	15%	15%	-
Vigilancia	[E.14] Fugas de información	10	-	75%	-	-	-
	[E.28] Indisponibilidad del personal	5	-	-	100%	-	15%
	[A.5] Suplantación de la identidad del usuario	5	-	75%	50%	50%	-
	[A.6] Abuso de privilegios de acceso	5	-	-	15%	15%	-
	[A.28] Indisponibilidad del personal	5	-	-	100%	-	15%
	[A.29] Extorsión	5	-	15%	15%	15%	-
	[A.30] Ingeniería social	10	-	15%	15%	50%	-
Personal del área de sistemas	[E.1] Errores de los usuarios	5	-	-	-	15%	15%
	[E.14] Fugas de información	10	-	100%	-	-	-
	[E.28] Indisponibilidad del personal	5	-	-	100%	-	20%
	[A.5] Suplantación de la identidad del usuario	5	-	100%	15%	50%	20%
	[A.6] Abuso de privilegios de acceso	50	-	-	15%	15%	15%
	[A.28] Indisponibilidad del personal	5	-	-	100%	-	15%
	[A.29] Extorsión	5	-	15%	15%	50%	-
	[A.30] Ingeniería social	10	-	75%	15%	75%	-

Fuente: El Autor.

10. PROBABILIDAD E IMPACTO DE LOS ACTIVOS

10.1. PROBABILIDAD DE OCURRENCIA

Tabla 7 Probabilidad de Ocurrencia.

Valor		Descripción
3	Alto	Muy frecuente
2	Medio	Frecuente
1	Bajo	Poco frecuente
0	Nulo	Nulo

Fuente: El Autor.

10.2. MEDICIÓN DE IMPACTO

Tabla 8 Escala de impacto

Valor		Descripción
3	Alto	Catastrófico
2	Medio	Moderado
1	Bajo	Menor
0	Nulo	Insignificante

Fuente: El Autor.

Tabla 9 Tabla de Probabilidad e Impacto de las amenazas en los activos

Activos esenciales	Amenaza	Probabilidad	Impacto				
			I	C	D	A	T
Sistemas de Información de los proyectos	[E.1] Errores de los usuarios	1	0	2	1	2	2
	[E.2] Errores del administrador	1	0	0	1	1	1
	[E.3] Errores de monitorización (log)	1	0	0	0	0	3
	[E.4] Errores de configuración	1	0	0	1	1	1
	[E.14] Fugas de información	1	1	3	0	0	0
	[E.15] Alteración de la información	1	1	2	0	3	1
	[E.16] Introducción de falsa información	1	0	2	0	2	1
	[E.19] Divulgación de información	1	0	1	0	0	0
	[E.24] Caída del sistema por agotamiento de recursos	1	1	0	3	0	2
	[A.4] Manipulación de la configuración	1	1	1	2	1	2
	[A.5] Suplantación de la identidad del usuario	1	1	2	2	2	1
	[A.6] Abuso de privilegios de acceso	1	0	1	1	1	1
	[A.24] Denegación de servicio	1	0	1	3	0	2
Histórico personal que ha hecho uso de los recursos de CEDIT	[E.14] Fugas de información	1	0	3	0	0	0
	[E.15] Alteración de la información	1	1	2	0	1	1
	[E.16] Introducción de falsa información	1	1	2	0	1	1
	[E.19] Divulgación de información	1	0	3	0	0	0
Manuales de usuario de lo desarrollado por medio del CEDIT	[E.1] Errores de los usuarios	1	0	0	0	1	1
	[E.14] Fugas de información	1	0	3	0	0	0
Diccionario de datos	[E.14] Fugas de información	1	0	3	0	0	0
	[E.15] Alteración de la información	1	1	2	0	1	2
	[E.19] Divulgación de información	1	0	3	0	0	0

Tabla 9. (Continuación)

Arquitectura del sistema	Amenaza	Probabilidad	Impacto				
			I	C	D	A	T
Canales dedicados	[I.8] Fallo de servicios de comunicaciones	1	1	1	3	1	2
	[A.9] Reencaminamiento de mensajes	1	1	2	0	2	1
	[A.12] Análisis de tráfico	1	0	2	0	1	0
	[A.14] Interceptación de información (escucha)	1	1	3	0	0	0
	[A.24] Denegación de servicio	1	1	2	3	1	1
Dispositivos de irradiación de internet	[I.8] Fallo de servicios de comunicaciones	1	1	2	3	1	1
	[E.1] Errores de los usuarios	1	0	0	0	1	2
	[A.9] Reencaminamiento de mensajes	1	0	3	0	1	1
	[A.12] Análisis de tráfico	1	0	2	0	1	0
	[A.14] Interceptación de información (escucha)	1	0	3	0	1	0
Datos / Información	Amenaza	Probabilidad	Impacto				
			I	C	D	A	T
Sistema de información	[E.2] Errores del administrador	1	0	0	0	1	1
	[E.14] Fugas de información	1	0	3	0	0	0
	[E.15] Alteración de la información	1	1	2	0	1	3
	[E.24] Caída del sistema por agotamiento de recursos	1	1	1	3	1	1
	[A.11] Acceso no autorizado	1	1	2	2	2	2
	[A.24] Denegación de servicio		0	2	3	1	1
Copias de seguridad mensuales de la información y archivos importantes	[N.1] Fuego	1	1	0	3	0	0
	[N.2] Daños por agua	1	1	0	3	0	0
	[I.10] Degradación de los soportes de almacenamiento de la información	1	1	0	2	1	1
	[E.14] Fugas de información	1	0	3	0	0	0

Tabla 9. (Continuación)

Claves criptográficas	Amenaza	Probabilidad	Impacto				
			I	C	D	A	T
Claves de usuarios de la plataforma tecnológica	[E.2] Errores del administrador [E.14] Fugas de información	1 1	0 0	0 3	0 0	1 2	1 0
Claves de servidores	[E.2] Errores del administrador [E.14] Fugas de información	1 1	0 0	0 3	0 0	1 2	1 0
Claves de acceso externo	[E.14] Fugas de información	1	0	3	0	2	0
Claves de acceso a zonas restringidas	[E.14] Fugas de información	1	0	3	0	2	0
Servicios	Amenaza	Probabilidad	Impacto				
			I	C	D	A	T
Página Web	[I.8] Fallo de servicios de comunicaciones [E.24] Caída del sistema por agotamiento de recursos [A.24] Denegación de servicio	1 1 1	1 1 1	1 1 1	3 3 3	0 0 0	2 2 3
Correo Electrónico	[E.2] Errores del administrador [A.9] Reencaminamiento de mensajes [A.11] Acceso no autorizado	1 1 1	0 0 1	0 2 2	0 0 2	1 2 1	1 2 2
Telefonía (conexión de voz, buzón de voz, llamada en espera, menú de bienvenida, grabación de llamadas)	[N.1] Fuego [N.2] Daños por agua [E.24] Caída del sistema por agotamiento de recursos [A.4] Manipulación de la configuración	1 1 1 1	1 1 1 1	0 0 1 2	3 3 2 1	0 0 0 2	0 0 3 1

Tabla 9. (Continuación)

Aplicaciones (software)	Amenaza	Probabilidad	Impacto				
			I	C	D	A	T
Sistema de Información	[E.1] Errores de los usuarios	1	0	1	0	1	2
	[E.14] Fugas de información	1	0	3	0	1	0
	[E.15] Alteración de la información	1	1	2	0	2	2
	[E.24] Caída del sistema por agotamiento de recursos	1	1	1	3	0	1
	[A.4] Manipulación de la configuración	1	1	2	2	1	2
	[A.11] Acceso no autorizado	1	1	2	2	2	2
	[A.24] Denegación de servicio	1	0	1	3	0	1
Paquete de ofimática	[E.1] Errores de los usuarios	1	0	1	0	1	1
	[E.20] Vulnerabilidades de los programas	1	1	1	2	1	0
	[E.21] Errores de mantenimiento / actualización de programas (software)	1	1	1	1	1	0
Edición de audio y videos	[E.1] Errores de los usuarios	1	0	1	0	1	0
	[E.20] Vulnerabilidades de los programas	1	1	1	2	1	0
	[E.21] Errores de mantenimiento / actualización de programas (software)	1	1	1	1	1	0
Sistemas operativos	[E.1] Errores de los usuarios	1	0	1	0	1	0
	[E.8] Difusión de software dañino	1	1	2	2	1	0
	[E.21] Errores de mantenimiento / actualización de programas (software)	1	1	1	1	1	0
	[A.4] Manipulación de la configuración	1	1	1	2	1	0
Aplicaciones de diseño	[E.1] Errores de los usuarios	1	0	0	0	1	0
	[E.20] Vulnerabilidades de los programas (software)	1	1	0	1	1	0
	[E.21] Errores de mantenimiento / actualización de programas (software)	1	1	1	1	1	0
Herramientas de desarrollo	[E.1] Errores de los usuarios	1	0	0	0	1	0
	[E.21] Errores de mantenimiento / actualización de programas (software)	1	1	0	1	1	0
Aplicativos web	[I.8] Fallo de servicios de comunicaciones	1	1	1	3	0	2

Tabla 9. (Continuación)

Sistema de CCTV	[I.8] Fallo de servicios de comunicaciones	1	1	1	3	0	2
	[E.14] Fugas de información	1	0	3	0	1	0
	[A.4] Manipulación de la configuración	1	1	1	2	1	2
	[A.24] Denegación de servicio	1	1	1	3	0	1
Equipos informáticos (Hardware)	Amenaza	Probabilidad	Impacto				
			I	C	D	A	T
Estaciones de trabajo	[N.2] Daños por agua	1	3	0	3	0	0
	[E.8] Difusión de software dañino	2	2	1	2	1	1
	[E.23] Errores de mantenimiento / actualización de equipos (hardware)	1	1	1	1	1	1
	[A.4] Manipulación de la configuración	2	2	2	1	1	1
	[A.8] Difusión de software dañino	2	2	2	1	1	1
	[A.22] Manipulación de programas	2	1	1	1	1	1
Escáner	[E.1] Errores de los usuarios	2	1	1	2	0	1
Fotocopiadoras	[E.1] Errores de los usuarios	1	1	1	1	0	1
	[E.23] Errores de mantenimiento / actualización de equipos (hardware)	1	1	1	1	1	1
Impresoras	[E.1] Errores de los usuarios	1	1	1	1	0	1
Portátiles	[N.2] Daños por agua	1	3	0	3	0	0
	[E.23] Errores de mantenimiento / actualización de equipos (hardware)	1	2	1	1	1	1
	[E.25] Pérdida de equipos	1	2	2	3	0	3
	[A.8] Difusión de software dañino	1	2	2	2	1	2
	[A.22] Manipulación de programas	2	2	2	1	1	1
	[A.25] Robo de equipos	1	3	2	3	0	3
Video Beam	[E.1] Errores de los usuarios	1	1	0	1	1	1
	[E.25] Pérdida de equipos	1	3	0	3	0	3
	[A.25] Robo de equipos	1	2	0	3	0	3

Tabla 9. (Continuación)

Servidores	[E.3] Errores de monitorización (log)	1	0	0	0	0	3
	[E.4] Errores de configuración	1	1	1	2	1	1
	[E.8] Difusión de software dañino	1	2	1	2	1	1
	[E.14] Fugas de información	1	0	3	0	0	0
	[E.23] Errores de mantenimiento / actualización de equipos (hardware)	1	1	2	1	1	1
	[A.4] Manipulación de la configuración	1	2	2	2	1	1
	[A.11] Acceso no autorizado	1	2	2	2	2	1
NAS	[I.10] Degradación de los soportes de almacenamiento de la información	1	1	1	1	1	1
Firewalls	[E.3] Errores de monitorización (log)	1	0	0	0	0	3
	[E.4] Errores de configuración	1	1	2	1	1	1
	[E.14] Fugas de información	1	0	3	1	1	1
	[A.4] Manipulación de la configuración	1	2	2	2	1	2
	[A.11] Acceso no autorizado	1	2	3	2	2	2
Switches	[E.1] Errores de los usuarios	1	0	1	1	1	1
	[A.4] Manipulación de la configuración	1	1	1	1	1	1
Router	[E.4] Errores de configuración	1	0	1	1	1	1
	[A.4] Manipulación de la configuración	1	1	1	1	1	1
	[A.12] Análisis de tráfico	1	0	3	0	1	0
	[A.14] Interceptación de información (escucha)	1	0	3	0	1	0
Planta telefónica	[E.1] Errores de los usuarios	1	1	1	1	1	1
Patch panel	[E.1] Errores de los usuarios	1	1	1	1	1	1
Cámaras de seguridad	[N.2] Daños por agua	1	1	0	3	0	0
	[A.14] Interceptación de información (escucha)	1	0	3	0	1	0
Soportes de información	Amenaza	Probabilidad	Impacto				
			I	C	D	A	T
NAS	[I.10] Degradación de los soportes de almacenamiento de la información	1	1	1	1	1	1
	[A.17] Corrupción de la información	1	2	0	1	1	0

Tabla 9. (Continuación)

Discos externos	[I.4] Contaminación electromagnética	1	1	0	1	1	0
	[E.14] Fugas de información	1	1	3	0	1	0
	[E.25] Pérdida de equipos	1	0	1	3	0	3
Discos duros	[I.4] Contaminación electromagnética	1	1	0	1	1	0
	[E.14] Fugas de información	1	0	3	0	1	0
Cintas magnéticas	[I.4] Contaminación electromagnética	1	1	0	1	1	0
	[I.10] Degradación de los soportes de almacenamiento de la información	1	1	1	1	1	1
	[A.17] Corrupción de la información	1	1	2	0	2	0
Replicas ubicadas en otras ciudades	[I.7] Condiciones inadecuadas de temperatura o humedad	1	1	0	1	0	0
	[I.8] Fallo de servicios de comunicaciones	1	1	1	3	1	2
	[I.10] Degradación de los soportes de almacenamiento de la información	1	1	1	0	1	0
	[E.3] Errores de monitorización (log)	2	0	0	1	0	3
	[E.4] Errores de configuración	1	1	1	0	1	1
	[A.17] Corrupción de la información	1	1	1	0	2	0
	[A.19] Divulgación de información	1	0	3	0	0	0
Servicios en la nube	[I.8] Fallo de servicios de comunicaciones	1	1	1	3	1	3
	[E.14] Fugas de información	1	0	3	0	0	0
	[A.17] Corrupción de la información	1	1	1	0	3	0
	[A.19] Divulgación de información	1	0	3	0	1	0
Equipamiento auxiliar	Amenaza	Probabilidad	Impacto				
			I	C	D	A	T
UPS	[N.1] Fuego	1	3	0	3	0	0
	[N.2] Daños por agua	1	3	0	3	0	0
	[I.6] Corte del suministro eléctrico	1	1	0	3	1	1
PDU’s	[I.6] Corte del suministro eléctrico	1	1	0	3	1	1
Fibra óptica	[N.*] Desastres naturales	1	3	0	3	0	2
Transceiver	[I.8] Fallo de servicios de comunicaciones	1	1	1	3	1	1
Cableado estructurado	[I.4] Contaminación electromagnética	1	1	0	1	1	0

Tabla 9. (Continuación)

Tableros de operación	[I.4] Contaminación electromagnética [I.6] Corte del suministro eléctrico	1 1	1 1	0 0	1 3	1 0	0 1
Inversores de administración de energía	[I.4] Contaminación electromagnética [I.6] Corte del suministro eléctrico	1 1	1 1	0 0	1 3	1 0	0 1
Instalaciones	Amenaza	Probabilidad	Impacto				
			I	C	D	A	T
Edificaciones	[N.1] Fuego [N.*] Desastres naturales [I.6] Corte del suministro eléctrico [A.11] Acceso no autorizado [A.26] Ataque destructivo	1 1 1 1 1	2 2 1 0 2	0 0 0 2 0	2 3 1 1 1	0 0 0 2 0	2 2 2 1 1
Salas de espera	[N.1] Fuego [A.26] Ataque destructivo [A.27] Ocupación enemiga	1 1 1	2 2 1	0 0 0	2 2 2	0 0 1	1 1 1
Cuartos de equipos de comunicación y seguridad	[I.7] Condiciones inadecuadas de temperatura o humedad [A.11] Acceso no autorizado [A.25] Robo de equipos [A.26] Ataque destructivo	1 1 1 1	1 1 0 1	0 2 2 0	2 1 1 2	0 2 0 0	0 0 2 1
Cuartos de aires	[N.2] Daños por agua [I.7] Condiciones inadecuadas de temperatura o humedad	1 1	1 1	0 0	3 1	0 1	0 0

Tabla 9. (Continuación)

Personal	Amenaza	Probabilidad	Impacto				
			I	C	D	A	T
Administrativos de la empresa	[E.1] Errores de los usuarios	1	0	0	0	1	2
	[E.14] Fugas de información	2	0	3	0	1	0
	[E.28] Indisponibilidad del personal	2	1	0	3	0	3
	[A.5] Suplantación de la identidad del usuario	1	2	2	2	3	2
	[A.6] Abuso de privilegios de acceso	2	0	1	1	2	1
	[A.28] Indisponibilidad del personal	2	2	0	3	0	3
	[A.29] Extorsión	1	1	2	1	1	1
	[A.30] Ingeniería social	1	1	2	1	1	1
Usuarios	[E.1] Errores de los usuarios	1	0	0	0	1	1
	[E.14] Fugas de información	1	0	3	0	0	0
	[A.30] Ingeniería social	1	1	2	1	1	1
Vigilancia	[E.14] Fugas de información	1	0	3	1	1	0
	[E.28] Indisponibilidad del personal	1	1	0	3	0	2
	[A.5] Suplantación de la identidad del usuario	1	2	2	2	2	2
	[A.6] Abuso de privilegios de acceso	1	0	2	1	1	1
	[A.28] Indisponibilidad del personal	1	1	0	3	0	3
	[A.29] Extorsión	1	1	2	1	1	1
	[A.30] Ingeniería social	1	1	2	1	1	1
Personal del área de sistemas	[E.1] Errores de los usuarios	1	0	0	0	1	1
	[E.14] Fugas de información	1	0	3	0	1	0
	[E.28] Indisponibilidad del personal	1	1	0	3	0	3
	[A.5] Suplantación de la identidad del usuario	1	1	3	2	3	2
	[A.6] Abuso de privilegios de acceso	1	1	2	1	2	1
	[A.28] Indisponibilidad del personal	1	1	0	3	0	3
	[A.29] Extorsión	1	1	2	1	1	1
	[A.30] Ingeniería social	1	2	3	1	1	1

Fuente: El Autor.

11. ESCALA DE RIESGOS

Tabla 10 Tabla de escala de riesgos

Probabilidad		Impacto			
		Nulo (N)	Bajo (B)	Medio (M)	Alto (A)
		0	1	2	3
0	Nulo (N)	0	0	0	0
1	Bajo (B)	0	1	2	3
2	Medio (M)	0	2	4	6
3	Alto (A)	0	3	6	9

Fuente: El Autor.

Riesgo Alto (A): 6 - 9 (**Rojo**), Se necesitan planes correctivos.

Riego Medio (M): 3 - 5 (**Amarillo**), Se necesitan planes preventivos.

Riesgo Bajo (B): 1 - 2 (**Naranja**), Se necesitan planes detectivos.

Riesgo Nulo (N): 0 (**Verde**), No se necesitan planes.

Tabla 11 Matriz de Riesgo

Activos esenciales	Amenaza	Probabilidad	Impacto					Riesgo Total				
			I	C	D	A	T	I	C	D	A	T
Sistemas de Información de los proyectos	[E.1] Errores de los usuarios	1	0	2	1	2	2	0	2	1	2	2
	[E.2] Errores del administrador	1	0	0	1	1	1	0	0	1	1	1
	[E.3] Errores de monitorización (log)	1	0	0	0	0	3	0	0	0	0	3
	[E.4] Errores de configuración	1	0	0	1	1	1	0	0	1	1	1
	[E.14] Fugas de información	1	1	3	0	0	0	1	3	0	0	0
	[E.15] Alteración de la información	1	1	2	0	3	1	1	2	0	3	1
	[E.16] Introducción de falsa información	1	0	2	0	2	1	0	2	0	2	1
	[E.19] Divulgación de información	1	0	1	0	0	0	0	1	0	0	0
	[E.24] Caída del sistema por agotamiento de recursos	1	1	0	3	0	2	1	0	3	0	2
	[A.4] Manipulación de la configuración	1	1	1	2	1	2	1	1	2	1	2
	[A.5] Suplantación de la identidad del usuario	1	1	2	2	2	1	1	2	2	2	1
	[A.6] Abuso de privilegios de acceso	1	0	1	1	1	1	0	1	1	1	1
	[A.24] Denegación de servicio	1	0	1	3	0	2	0	1	3	0	2
Histórico personal que ha hecho uso de los recursos de CEDIT	[E.14] Fugas de información	1	0	3	0	0	0	0	3	0	0	0
	[E.15] Alteración de la información	1	1	2	0	1	1	1	2	0	1	1
	[E.16] Introducción de falsa información	1	1	2	0	1	1	1	2	0	1	1
	[E.19] Divulgación de información	1	0	3	0	0	0	0	3	0	0	0
Manuales de usuario de lo desarrollado por medio del CEDIT	[E.1] Errores de los usuarios	1	0	0	0	1	1	0	0	0	1	1
	[E.14] Fugas de información	1	0	3	0	0	0	0	3	0	0	0

Tabla 11. (Continuación)

Activos esenciales	Amenaza	Probabilidad	Impacto					Riesgo Total				
			I	C	D	A	T	I	C	D	A	T
Diccionario de datos	[E.14] Fugas de información	1	0	3	0	0	0	0	3	0	0	0
	[E.15] Alteración de la información	1	1	2	0	1	2	1	2	0	1	2
	[E.19] Divulgación de información	1	0	3	0	0	0	0	3	0	0	0
Arquitectura del sistema	Amenaza	Probabilidad	Impacto					Riesgo Total				
			I	C	D	A	T	I	C	D	A	T
Canales dedicados	[I.8] Fallo de servicios de comunicaciones	1	1	1	3	1	2	1	1	3	1	2
	[A.9] Reencaminamiento de mensajes	1	1	2	0	2	1	1	2	0	2	1
	[A.12] Análisis de tráfico	1	0	2	0	1	0	0	2	0	1	0
	[A.14] Interceptación de información (escucha)	1	1	3	0	0	0	1	3	0	0	0
	[A.24] Denegación de servicio	1	1	2	3	1	1	1	2	3	1	1
Dispositivos de irradiación de internet	[I.8] Fallo de servicios de comunicaciones	1	1	2	3	1	1	1	2	3	1	1
	[E.1] Errores de los usuarios	1	0	0	0	1	2	0	0	0	1	2
	[A.9] Reencaminamiento de mensajes	1	0	3	0	1	1	0	3	0	1	1
	[A.12] Análisis de tráfico	1	0	2	0	1	0	0	2	0	1	0
	[A.14] Interceptación de información (escucha)	1	0	3	0	1	0	0	3	0	1	0

Tabla 11. (Continuación)

Datos / Información	Amenaza	Probabilidad	Impacto					Riesgo Total				
			I	C	D	A	T	I	C	D	A	T
Sistema de información	[E.2] Errores del administrador	1	0	0	0	1	1	0	0	0	1	1
	[E.14] Fugas de información	1	0	3	0	0	0	0	3	0	0	0
	[E.15] Alteración de la información	1	1	2	0	1	3	1	2	0	1	3
	[E.24] Caída del sistema por agotamiento de recursos	1	1	1	3	1	1	1	1	3	1	1
	[A.11] Acceso no autorizado	1	1	2	2	2	2	1	2	2	2	2
	[A.24] Denegación de servicio	1	0	2	3	1	1	0	2	3	1	1
Copias de seguridad mensuales de la información y archivos importantes	[N.1] Fuego	1	1	0	3	0	0	1	0	3	0	0
	[N.2] Daños por agua	1	1	0	3	0	0	1	0	3	0	0
	[I.10] Degradación de los soportes de almacenamiento de la información	1	1	0	2	1	1	1	0	2	1	1
	[E.14] Fugas de información	1	0	3	0	0	0	0	3	0	0	0
Claves criptográficas	Amenaza	Probabilidad	Impacto					Riesgo Total				
			I	C	D	A	T	I	C	D	A	T
Claves de usuarios de la plataforma tecnológica	[E.2] Errores del administrador	1	0	0	0	1	1	0	0	0	1	1
	[E.14] Fugas de información	1	0	3	0	2	0	0	3	0	2	0
Claves de servidores	[E.2] Errores del administrador	1	0	0	0	1	1	0	0	0	1	1
	[E.14] Fugas de información	1	0	3	0	2	0	0	3	0	2	0
Claves de acceso externo	[E.14] Fugas de información	1	0	3	0	2	0	0	3	0	2	0
Claves de acceso a zonas restringidas	[E.14] Fugas de información	1	0	3	0	2	0	0	3	0	2	0

Tabla 11. (Continuación)

Servicios	Amenaza	Probabilidad	Impacto					Riesgo Total				
			I	C	D	A	T	I	C	D	A	T
Página Web	[I.8] Fallo de servicios de comunicaciones	1	1	1	3	0	2	1	1	3	0	2
	[E.24] Caída del sistema por agotamiento de recursos	1	1	1	3	0	2	1	1	3	0	2
	[A.24] Denegación de servicio	1	1	1	3	0	3	1	1	3	0	3
Correo Electrónico	[E.2] Errores del administrador	1	0	0	0	1	1	0	0	0	1	1
	[A.9] Reencaminamiento de mensajes	1	0	2	0	2	2	0	2	0	2	2
	[A.11] Acceso no autorizado	1	1	2	2	1	2	1	2	2	1	2
Telefonía (conexión de voz, buzón de voz, llamada en espera, menú de bienvenida, grabación de llamadas)	[N.1] Fuego	1	1	0	3	0	0	1	0	3	0	0
	[N.2] Daños por agua	1	1	0	3	0	0	1	0	3	0	0
	[E.24] Caída del sistema por agotamiento de recursos	1	1	1	2	0	3	1	1	2	0	3
	[A.4] Manipulación de la configuración	1	1	2	1	2	1	1	2	1	2	1

Tabla 11. (Continuación)

Aplicaciones (software)	Amenaza	Probabilidad	Impacto					Riesgo Total				
			I	C	D	A	T	I	C	D	A	T
Sistema de Información	[E.1] Errores de los usuarios	1	0	1	0	1	2	0	1	0	1	2
	[E.14] Fugas de información	1	0	3	0	1	0	0	3	0	1	0
	[E.15] Alteración de la información	1	1	2	0	2	2	1	2	0	2	2
	[E.24] Caída del sistema por agotamiento de recursos	1	1	1	3	0	1	1	1	3	0	1
	[A.4] Manipulación de la configuración	1	1	2	2	1	2	1	2	2	1	2
	[A.11] Acceso no autorizado	1	1	2	2	2	2	1	2	2	2	2
	[A.24] Denegación de servicio	1	0	1	3	0	1	0	1	3	0	1
Paquete de ofimática	[E.1] Errores de los usuarios	1	0	1	0	1	1	0	1	0	1	1
	[E.20] Vulnerabilidades de los programas (software)	1	1	1	2	1	0	1	1	2	1	0
	[E.21] Errores de mantenimiento / actualización de programas (software)	1	1	1	1	1	0	1	1	1	1	0
Edición de audio y videos	[E.1] Errores de los usuarios	1	0	1	0	1	0	0	1	0	1	0
	[E.20] Vulnerabilidades de los programas (software)	1	1	1	2	1	0	1	1	2	1	0
	[E.21] Errores de mantenimiento / actualización de programas (software)	1	1	1	1	1	0	1	1	1	1	0

Tabla 11. (Continuación)

Aplicaciones (software)	Amenaza	Probabilidad	Impacto					Riesgo Total				
			I	C	D	A	T	I	C	D	A	T
Sistemas operativos	[E.1] Errores de los usuarios	1	0	1	0	1	0	0	1	0	1	0
	[E.8] Difusión de software dañino	1	1	2	2	1	0	1	2	2	1	0
	[E.21] Errores de mantenimiento / actualización de programas (software)	1	1	1	1	1	0	1	1	1	1	0
	[A.4] Manipulación de la configuración	1	1	1	2	1	0	1	1	2	1	0
Aplicaciones de diseño	[E.1] Errores de los usuarios	1	0	0	0	1	0	0	0	0	1	0
	[E.20] Vulnerabilidades de los programas (software)	1	1	0	1	1	0	1	0	1	1	0
	[E.21] Errores de mantenimiento / actualización de programas (software)	1	1	1	1	1	0	1	1	1	1	0
Herramientas de desarrollo	[E.1] Errores de los usuarios	1	0	0	0	1	0	0	0	0	1	0
	[E.21] Errores de mantenimiento / actualización de programas (software)	1	1	0	1	1	0	1	0	1	1	0
Aplicativos web	[I.8] Fallo de servicios de comunicaciones	1	1	1	3	0	2	1	1	3	0	2
Sistema de CCTV	[I.8] Fallo de servicios de comunicaciones	1	1	1	3	0	2	1	1	3	0	2
	[E.14] Fugas de información	1	0	3	0	1	0	0	3	0	1	0
	[A.4] Manipulación de la configuración	1	1	1	2	1	2	1	1	2	1	2
	[A.24] Denegación de servicio	1	1	1	3	0	1	1	1	3	0	1

Tabla 11. (Continuación)

Equipos informáticos (Hardware)	Amenaza	Probabilidad	Impacto					Riesgo Total				
			I	C	D	A	T	I	C	D	A	T
Estaciones de trabajo	[N.2] Daños por agua	1	3	0	3	0	0	3	0	3	0	0
	[E.8] Difusión de software dañino	2	2	1	2	1	1	4	2	4	2	2
	[E.23] Errores de mantenimiento / actualización de equipos (hardware)	1	1	1	1	1	1	1	1	1	1	1
	[A.4] Manipulación de la configuración	2	2	2	1	1	1	4	4	2	2	2
	[A.8] Difusión de software dañino	2	2	2	1	1	1	4	4	2	2	2
	[A.22] Manipulación de programas	2	1	1	1	1	1	2	2	2	2	2
Escáner	[E.1] Errores de los usuarios	2	1	1	2	0	1	2	2	4	0	2
Fotocopiadoras	[E.1] Errores de los usuarios	1	1	1	1	0	1	1	1	1	0	1
	[E.23] Errores de mantenimiento / actualización de equipos (hardware)	1	1	1	1	1	1	1	1	1	1	1
Impresoras	[E.1] Errores de los usuarios	1	1	1	1	0	1	1	1	1	0	1
Portátiles	[N.2] Daños por agua	1	3	0	3	0	0	3	0	3	0	0
	[E.23] Errores de mantenimiento / actualización de equipos (hardware)	1	2	1	1	1	1	2	1	1	1	1
	[E.25] Pérdida de equipos	1	2	2	3	0	3	2	2	3	0	3
	[A.8] Difusión de software dañino	1	2	2	2	1	2	2	2	2	1	2
	[A.22] Manipulación de programas	2	2	2	1	1	1	4	4	2	2	2
	[A.25] Robo de equipos	1	3	2	3	0	3	3	2	3	0	3

Tabla 11. (Continuación)

Equipos informáticos (Hardware)	Amenaza	Probabilidad	Impacto					Riesgo Total				
			I	C	D	A	T	I	C	D	A	T
Video Beam	[E.1] Errores de los usuarios	1	1	0	1	1	1	1	0	1	1	1
	[E.25] Pérdida de equipos	1	3	0	3	0	3	3	0	3	0	3
	[A.25] Robo de equipos	1	2	0	3	0	3	2	0	3	0	3
Servidores	[E.3] Errores de monitorización (log)	1	0	0	0	0	3	0	0	0	0	3
	[E.4] Errores de configuración	1	1	1	2	1	1	1	1	2	1	1
	[E.8] Difusión de software dañino	1	2	1	2	1	1	2	1	2	1	1
	[E.14] Fugas de información	1	0	3	0	0	0	0	3	0	0	0
	[E.23] Errores de mantenimiento / actualización de equipos (hardware)	1	1	2	1	1	1	1	2	1	1	1
	[A.4] Manipulación de la configuración	1	2	2	2	1	1	2	2	2	1	1
	[A.11] Acceso no autorizado	1	2	2	2	2	1	2	2	2	2	1
NAS	[I.10] Degradación de los soportes de almacenamiento de la información	1	1	1	1	1	1	1	1	1	1	1
Firewalls	[E.3] Errores de monitorización (log)	1	0	0	0	0	3	0	0	0	0	3
	[E.4] Errores de configuración	1	1	2	1	1	1	1	2	1	1	1
	[E.14] Fugas de información	1	0	3	1	1	1	0	3	1	1	1
	[A.4] Manipulación de la configuración	1	2	2	2	1	2	2	2	2	1	2
	[A.11] Acceso no autorizado	1	2	3	2	2	2	2	3	2	2	2
Switches	[E.1] Errores de los usuarios	1	0	1	1	1	1	0	1	1	1	1
	[A.4] Manipulación de la configuración	1	1	1	1	1	1	1	1	1	1	1

Tabla 11. (Continuación)

Equipos informáticos (Hardware)	Amenaza	Probabilidad	Impacto					Riesgo Total				
			I	C	D	A	T	I	C	D	A	T
Router	[E.4] Errores de configuración	1	0	1	1	1	1	0	1	1	1	1
	[A.4] Manipulación de la configuración	1	1	1	1	1	1	1	1	1	1	1
	[A.12] Análisis de tráfico	1	0	3	0	1	0	0	3	0	1	0
	[A.14] Interceptación de información (escucha)	1	0	3	0	1	0	0	3	0	1	0
Planta telefónica	[E.1] Errores de los usuarios	1	1	1	1	1	1	1	1	1	1	1
Patch panel	[E.1] Errores de los usuarios	1	1	1	1	1	1	1	1	1	1	1
Cámaras de seguridad	[N.2] Daños por agua	1	1	0	3	0	0	1	0	3	0	0
	[A.14] Interceptación de información (escucha)	1	0	3	0	1	0	0	3	0	1	0
Soportes de información	Amenaza	Probabilidad	Impacto					Riesgo Total				
			I	C	D	A	T	I	C	D	A	T
NAS	[I.10] Degradación de los soportes de almacenamiento de la información	1	1	1	1	1	1	1	1	1	1	1
	[A.17] Corrupción de la información	1	2	0	1	1	0	2	0	1	1	0
Discos externos	[I.4] Contaminación electromagnética	1	1	0	1	1	0	1	0	1	1	0
	[E.14] Fugas de información	1	1	3	0	1	0	1	3	0	1	0
	[E.25] Pérdida de equipos	1	0	1	3	0	3	0	1	3	0	3
Discos duros	[I.4] Contaminación electromagnética	1	1	0	1	1	0	1	0	1	1	0
	[E.14] Fugas de información	1	0	3	0	1	0	0	3	0	1	0

Tabla 11. (Continuación)

Soportes de información	Amenaza	Probabilidad	Impacto					Riesgo Total				
			I	C	D	A	T	I	C	D	A	T
Cintas magnéticas	[I.4] Contaminación electromagnética	1	1	0	1	1	0	1	0	1	1	0
	[I.10] Degradación de los soportes de almacenamiento de la información	1	1	1	1	1	1	1	1	1	1	1
	[A.17] Corrupción de la información	1	1	2	0	2	0	1	2	0	2	0
Replicas ubicadas en otras ciudades	[I.7] Condiciones inadecuadas de temperatura o humedad	1	1	0	1	0	0	1	0	1	0	0
	[I.8] Fallo de servicios de comunicaciones	1	1	1	3	1	2	1	1	3	1	2
	[I.10] Degradación de los soportes de almacenamiento de la información	1	1	1	0	1	0	1	1	0	1	0
	[E.3] Errores de monitorización (log)	2	0	0	1	0	3	0	0	2	0	6
	[E.4] Errores de configuración	1	1	1	0	1	1	1	1	0	1	1
	[A.17] Corrupción de la información	1	1	1	0	2	0	1	1	0	2	0
	[A.19] Divulgación de información	1	0	3	0	0	0	0	3	0	0	0
Servicios en la nube	[I.8] Fallo de servicios de comunicaciones	1	1	1	3	1	3	1	1	3	1	3
	[E.14] Fugas de información	1	0	3	0	0	0	0	3	0	0	0
	[A.17] Corrupción de la información	1	1	1	0	3	0	1	1	0	3	0
	[A.19] Divulgación de información	1	0	3	0	1	0	0	3	0	1	0
Equipamiento auxiliar	Amenaza	Probabilidad	Impacto					Riesgo Total				
			I	C	D	A	T	I	C	D	A	T
UPS	[N.1] Fuego	1	3	0	3	0	0	3	0	3	0	0
	[N.2] Daños por agua	1	3	0	3	0	0	3	0	3	0	0
	[I.6] Corte del suministro eléctrico	1	1	0	3	1	1	1	0	3	1	1

Tabla 11. (Continuación)

Equipamiento auxiliar	Amenaza	Probabilidad	Impacto					Riesgo Total				
			I	C	D	A	T	I	C	D	A	T
PDU's	[I.6] Corte del suministro eléctrico	1	1	0	3	1	1	1	0	3	1	1
Fibra óptica	[N.*] Desastres naturales	1	3	0	3	0	2	3	0	3	0	2
Transceiver	[I.8] Fallo de servicios de comunicaciones	1	1	1	3	1	1	1	1	3	1	1
Cableado estructurado	[I.4] Contaminación electromagnética	1	1	0	1	1	0	1	0	1	1	0
Tableros de operación	[I.4] Contaminación electromagnética	1	1	0	1	1	0	1	0	1	1	0
	[I.6] Corte del suministro eléctrico	1	1	0	3	0	1	1	0	3	0	1
Inversores de administración de energía	[I.4] Contaminación electromagnética	1	1	0	1	1	0	1	0	1	1	0
	[I.6] Corte del suministro eléctrico	1	1	0	3	0	1	1	0	3	0	1
Instalaciones	Amenaza	Probabilidad	Impacto					Riesgo Total				
			I	C	D	A	T	I	C	D	A	T
Edificaciones	[N.1] Fuego	1	2	0	2	0	2	2	0	2	0	2
	[N.*] Desastres naturales	1	2	0	3	0	2	2	0	3	0	2
	[I.6] Corte del suministro eléctrico	1	1	0	1	0	2	1	0	1	0	2
	[A.11] Acceso no autorizado	1	0	2	1	2	1	0	2	1	2	1
	[A.26] Ataque destructivo	1	2	0	1	0	1	2	0	1	0	1
Salas de espera	[N.1] Fuego	1	2	0	2	0	1	2	0	2	0	1
	[A.26] Ataque destructivo	1	2	0	2	0	1	2	0	2	0	1
	[A.27] Ocupación enemiga	1	1	0	2	1	1	1	0	2	1	1

Tabla 11. (Continuación)

Instalaciones	Amenaza	Probabilidad	Impacto					Riesgo Total				
			I	C	D	A	T	I	C	D	A	T
Cuartos de equipos de comunicación y seguridad	[I.7] Condiciones inadecuadas de temperatura o humedad	1	1	0	2	0	0	1	0	2	0	0
	[A.11] Acceso no autorizado	1	1	2	1	2	0	1	2	1	2	0
	[A.25] Robo de equipos	1	0	2	1	0	2	0	2	1	0	2
	[A.26] Ataque destructivo	1	1	0	2	0	1	1	0	2	0	1
Cuartos de aires	[N.2] Daños por agua	1	1	0	3	0	0	1	0	3	0	0
	[I.7] Condiciones inadecuadas de temperatura o humedad	1	1	0	1	1	0	1	0	1	1	0
Personal	Amenaza	Probabilidad	Impacto					Riesgo Total				
			I	C	D	A	T	I	C	D	A	T
Administrativos de la empresa	[E.1] Errores de los usuarios	1	0	0	0	1	2	0	0	0	1	2
	[E.14] Fugas de información	2	0	3	0	1	0	0	6	0	2	0
	[E.28] Indisponibilidad del personal	2	1	0	3	0	3	2	0	6	0	6
	[A.5] Suplantación de la identidad del usuario	1	2	2	2	3	2	2	2	2	3	2
	[A.6] Abuso de privilegios de acceso	2	0	1	1	2	1	0	2	2	4	2
	[A.28] Indisponibilidad del personal	2	2	0	3	0	3	4	0	6	0	6
	[A.29] Extorsión	1	1	2	1	1	1	1	2	1	1	1
	[A.30] Ingeniería social	1	1	2	1	1	1	1	2	1	1	1
Usuarios	[E.1] Errores de los usuarios	1	0	0	0	1	1	0	0	0	1	1
	[E.14] Fugas de información	1	0	3	0	0	0	0	3	0	0	0
	[A.30] Ingeniería social	1	1	2	1	1	1	1	2	1	1	1

Tabla 11. (Continuación)

Personal	Amenaza	Probabilidad	Impacto					Riesgo Total				
			I	C	D	A	T	I	C	D	A	T
Vigilancia	[E.14] Fugas de información	1	0	3	1	1	0	0	3	1	1	0
	[E.28] Indisponibilidad del personal	1	1	0	3	0	2	1	0	3	0	2
	[A.5] Suplantación de la identidad del usuario	1	2	2	2	2	2	2	2	2	2	2
	[A.6] Abuso de privilegios de acceso	1	0	2	1	1	1	0	2	1	1	1
	[A.28] Indisponibilidad del personal	1	1	0	3	0	3	1	0	3	0	3
	[A.29] Extorsión	1	1	2	1	1	1	1	2	1	1	1
	[A.30] Ingeniería social	1	1	2	1	1	1	1	2	1	1	1
Personal del área de sistemas	[E.1] Errores de los usuarios	1	0	0	0	1	1	0	0	0	1	1
	[E.14] Fugas de información	1	0	3	0	1	0	0	3	0	1	0
	[E.28] Indisponibilidad del personal	1	1	0	3	0	3	1	0	3	0	3
	[A.5] Suplantación de la identidad del usuario	1	1	3	2	3	2	1	3	2	3	2
	[A.6] Abuso de privilegios de acceso	1	1	2	1	2	1	1	2	1	2	1
	[A.28] Indisponibilidad del personal	1	1	0	3	0	3	1	0	3	0	3
	[A.29] Extorsión	1	1	2	1	1	1	1	2	1	1	1
	[A.30] Ingeniería social	1	2	3	1	1	1	2	3	1	1	1

Fuente. El Autor.

12. CONTROLES

Un control interno informático pretende que con su implementación diariamente se pueda supervisar que todas las actividades de los sistemas de información se ejecuten dando cumplimiento a los procedimientos, estándares y normas que hayan sido fijados por la alta gerencia de la organización y la dirección informática, y como los requerimientos legales lo dispongan, además busca asegurarse que las medidas que se obtienen de los mecanismos que se apliquen sean fructuosas y ayuden a mejorar el proceso de auditoría en general, así como también de las auditorías externas al grupo. Este plan se propone de la siguiente manera.

- Administración de sistemas: Administrar las redes por medio del uso de vlan aplicando seguridad por puertos sobre los switches, monitoreo por medio de cámaras de seguridad en los centros de datos, separar los dispositivos de comunicación con los dispositivos internos de interconexión, mantener los servidores y unidades externos separados y bajo llave, control de acceso por huella a los centros de datos y registro de la actividad a realizar, continuo monitoreo y mantenimiento de las ups, tableros de manejo independientes de circuitos regulados y comunes, conexiones eléctricas de los servidores por medio de pdu, sistema centralizado de aire para mantener la temperatura en los centros de datos con equipos de respaldos y sensores en diferentes sitios, manejo de piso falso y encerramiento del centro de datos en vidrio para la continua monitorización, implementación de alta disponibilidad en servidores y dispositivos activos de red.
- Seguridad:
    - Controles preventivos: Implantación, ejecución y continuo monitoreo de una DMZ y a la vez un IDS, software de seguridad que impida los accesos no autorizados al sistema, bloqueo de medios extraíbles, implantación de un sistema de antivirus y una DLP, montaje de un firewall entre la empresa y el exterior, implementación de un proxy con políticas y controles de seguridad entre los equipos de cómputo y la web, un analizador de tráfico, implementación de VPN´s para interconexiones entre sucursales separadas geográficamente, aplicación de políticas de seguridad a los equipos de cómputo que impidan la ejecución de programas como administrador, además que frenen el cambio de las configuraciones de los sistemas, aplicación de seguridad en los equipos de interconexión internos, sistema centralizado de alertas y fallos en los equipos de cómputo.
    - Controles detectivos: Sistema VIGIA para registro de todos los errores (Operativos, por error del sistema, o por fallas de los equipos de cómputo y sus periféricos), registro de intentos de acceso no autorizados, LOG´s de la ejecución de los aplicativos en los

servidores, sistema de registro de la actividad diaria para detectar errores u omisiones.
    - Controles correctivos: Realización de copias de seguridad de los archivos, configuraciones y las bases de datos (antes de eventos de cambio al sistema, diarias, mensuales, anuales), réplicas en equipos locales, réplicas y copias de seguridad en equipos ubicados fuera de la sede y la ciudad, aplicación de un plan de continuidad de negocio, contar con equipos servidores espejo y con equipos de backups.
- Gestión del cambio: contar con equipos y servidores aislados a la red de producción en los que se hagan las pruebas funcionales de software, instruir continuamente y mantener actualizados al personal de pruebas en cuanto a metodologías ágiles para la rápida aplicación de cambios, hacer uso del manejo y trazabilidad de requerimientos hechos por usuarios que hacen uso del sistema.

De acuerdo a los estándares de control de la norma ISO 27002 se implementan los siguientes controles:

Tabla 12 Lista de Controles

Nombre Control ISO 27002	Ctrl. ISO	Ctrl. NIST	Nombre Control. NIST	Control
Documentación de la Política de Seguridad de Información	5.1.1	AT-1	Políticas y Procedimientos de Concientización y Capacitación en Seguridad	Se realizará una definición clara de todas las responsabilidades en cuando a seguridad de la información.
		CP-1	Políticas y Procedimientos de Planificación de Contingencias	
Revisión de la Política de Seguridad de la Información	5.1.2	N/A	Revisión y evaluación	La política de seguridad será revisada en intervalos planificados o en caso que ocurran cambios significantes para propender asegurar su uso continuo, adecuación y efectividad.
Compromiso Gerencial a la seguridad de la información	6.1.1	PL-1	Políticas y Procedimientos de Planificación de Seguridad	La Gerencia se compromete a apoyar activamente en la seguridad dentro de la organización a través de direcciones claras demostrando compromisos, asignaciones explícitas y reconocimiento de las responsabilidades de la seguridad de la información.
		PL-2	Plan de Seguridad del Sistema	
		PL-3	Actualización del Plan de Seguridad del Sistema	
Coordinación en seguridad de la información	6.1.2	PL-1	Políticas y Procedimientos de Planificación de Seguridad	La información de las actividades de seguridad será coordinada por representantes de las diferentes partes de la organización.
		PL-2	Plan de Seguridad del Sistema	
		PL-3	Actualización del Plan de Seguridad del Sistema	
Asignación de Responsabilidades de seguridad de la información	6.1.3	PL-1	Políticas y Procedimientos de Planificación de Seguridad	Se definirá claramente todas las responsabilidades en cuanto a seguridad de la información. Y estas quedarán plasmadas en las políticas y planes que se documenten.
		PL-2	Plan de Seguridad del Sistema	
		PL-3	Actualización del Plan de Seguridad del Sistema	

Tabla 12. (Continuación)

Nombre Control ISO 27002	Ctrl. ISO	Ctrl. NIST	Nombre Control. NIST	Control
Proceso de autorización para las facilidades de Procesamiento de la Información	6.1.4	AC-20	Sistemas de información de propiedad personal	Se establece un proceso de autorización por parte del personal de recurso humano para la gestión de cada nuevo recurso del tratamiento de la información.
		CA-1	Políticas y Procedimientos de Certificación, Acreditación y Valuación de Seguridad	
		PL-1	Políticas y procedimientos de Planificación	
		PL-2	Plan de Seguridad del Sistema	
		PL-3	Actualización del Plan de Seguridad del Sistema	
Acuerdos de confidencialidad	6.1.5	PL-1	Políticas y Procedimientos de Planificación	Se incluye en los contratos acuerdos de confidencialidad y de no divulgación de la información a la que se tenga acceso.
		PL-2	Plan de Seguridad del Sistema	
		PL-3	Actualización del Plan de Seguridad del Sistema	
		PS-6	Acuerdos de Acceso	
Contactos con autoridades	6.1.6	IR-4	Manejo de Incidentes	Se mantendrán los contactos apropiados con autoridades locales y nacionales.
		IR-6	Monitoreo de Incidentes	
		PL-1	Políticas y Procedimientos de Planificación	
		PL-2	Plan de Seguridad del Sistema	
		PL-3	Actualización del Plan de Seguridad del Sistema	
Contactos con grupos de intereses especiales	6.1.7	AT-5	Contactos con Grupos y Asociaciones de Seguridad	Se mantendrán los contactos apropiados con grupos de interés especiales, foros especializados en seguridad informática, asociaciones de profesionales, y empresas de actualización de conocimientos.
		PL-1	Políticas y Procedimientos de Planificación de Seguridad	
		PL-2	Plan de Seguridad del Sistema	
		PL-3	Actualización del Plan de Seguridad del Sistema	
		SI-5	Alertas y avisos de seguridad	

Tabla 12. (Continuación)

Nombre Control ISO 27002	Ctrl. ISO	Ctrl. NIST	Nombre Control. NIST	Control
Revisión independiente de la seguridad de la información	6.1.8	CA-2	Valuaciones de Seguridad	Serán revisados independientemente el alcance de la organización para la gestión de la seguridad de la información y su implementación en intervalos planificados o cuando ocurran cambios significativos.
		PL-1	Políticas y Procedimientos de Planificación	
		PL-2	Plan de Seguridad del Sistema	
		PL-3	Actualización del Plan de Seguridad del Sistema	
Identificación del riesgo relacionado con terceros	6.2.1	PS-7	Seguridad del Personal de Terceros	Se identificarán los riesgos para la información y los servicios de procesamiento de información de la organización de los procesos que involucren partes externas.
		RA-3	Valuación de Riesgos	
		SA-9	Servicios Externos del Sistema de Información	
Atención a la seguridad en el trato con los clientes	6.2.2	AC-2	Gestión de Cuentas	Los requisitos identificados de seguridad serán anexados antes de dar acceso a los clientes a la información o activos.
		IR-6	Monitoreo de Incidentes	
Atención a la seguridad en los acuerdos con terceros o outsourcing	6.2.3	AC-2	Gestión de Cuentas	Los acuerdos con terceras partes que impliquen acceso, proceso, comunicación o gestión de la información cubrirán todos los requisitos de seguridad relevantes.
		AT-2	Concientización en Seguridad	
		IR-6	Monitoreo de Incidentes	
		MA-5	Personal de Mantenimiento	
		PS-7	Seguridad del Personal de Terceros	
Inventario de Activos	7.1.1	CM-2	Configuraciones Básicas de los sistemas de información e Inventario de los componentes	Se realizará una identificación de todos los activos y se mantendrá actualizado el inventario de activos.
Propiedad de los activos	7.1.2	N/A	N/A	Todos los activos se rotularán en el inventario con información alusiva a la empresa.
Uso aceptable de los activos	7.1.3	PL-4	Reglas de Comportamiento	Se identificarán, documentarán e implementarán las reglas para un uso aceptable de la información.
Pautas de clasificación	7.2.1	RA-2	Categorización de la Seguridad	La información será clasificada en función de su valor, requisitos legales, sensibilidad y criticidad.

Tabla 12. (Continuación)

Nombre Control ISO 27002	Ctrl. ISO	Ctrl. NIST	Nombre Control. NIST	Control
Etiquetado y manejo de la Información	7.2.2	AC-15	Marcado automatizado	Se define un conjunto adecuado de procedimientos para marcar y tratar la información de acuerdo con el esquema adoptado.
		AC-16	Etiquetado automatizado	
		MP-3	Etiquetado de Medios	
		SC-16	Transmisión de Parámetros Seguridad	
Roles y Responsabilidades	8.1.1	PS-1	Políticas y Procedimientos de Seguridad del Personal	Las funciones y responsabilidades de los empleados, contratistas y terceros serán definidas y documentadas según la política.
		PS-7	Seguridad del Personal de Terceros	
Selección	8.1.2	PS-2	Categorización de Posiciones	Se llevarán listas de verificación de todos los candidatos para empleo, contratistas y terceros.
		PS-3	Filtrado del Personal	
		PS-7	Seguridad del Personal de Terceros	
Términos y condiciones de empleo	8.1.3	PL-4	Reglas de Comportamiento	Los empleados, contratistas y terceros deberán aceptar y firmar los términos y condiciones del contrato de empleo, donde se establece sus obligaciones para la seguridad
		PS-4	Terminación de la relación laboral	
		PS-6	Acuerdos de Acceso	
		PS-7	Seguridad del Personal de Terceros	
Responsabilidad Gerencial	8.2.1	PS-7	Seguridad del Personal de Terceros	El gerente deberá requerir empleados, contratistas y usuarios de terceros para aplicar la seguridad en concordancia con las políticas y los procedimientos implantados.
Concientización, formación y entrenamiento en seguridad de la información	8.2.2	AT-1	Políticas y Procedimientos de Concientización y Capacitación en Seguridad	Todos los empleados, contratistas y usuarios de terceros recibirán formación apropiada del conocimiento y actualizaciones regulares en políticas y procedimientos para sus funciones.
		AT-2	Concientización en Seguridad	
		AT-3	Entrenamiento en Seguridad	
Proceso disciplinario	8.2.3	PS-8	Sanciones al Personal	Se abrirá un proceso formal para empleados que han cometido una apertura en la seguridad.
Responsabilidades en la terminación de la relación laboral	8.3.1	PS-4	Terminación de la relación laboral	Serán definidas y aplicadas las responsabilidades para realizar la finalización o cambio de un empleo.
		PS-5	Transferencia de Personal	

Tabla 12. (Continuación)

Nombre Control ISO 27002	Ctrl. ISO	Ctrl. NIST	Nombre Control. NIST	Control
Devolución de activos	8.3.2	PS-4	Terminación de la relación laboral	Todos los empleados, contratistas y terceros deberán retornar todos los activos de la organización que estén en su posesión, al momento de culminar su labor.
Remoción de derechos de acceso	8.3.3	AC-2	Gestión de Cuentas	Todos los derechos de acceso serán removidos a todos los empleados, contratistas o usuarios de terceros a la información e instalaciones de procesamiento.
		PS-4	Terminación de la relación laboral	
		PS-5	Transferencia de Personal	
Perímetro de seguridad física	9.1.1	PE-3	Control de Acceso Físico	Se usarán controles de acceso con huella para proteger áreas que contengan información y recursos de alto cuidado.
Controles de acceso físico	9.1.2	PE-2	Autorizaciones de Acceso Físico	Las áreas de seguridad se protegerán por controles de entrada adecuados asegurando el permiso sólo a personal autorizado.
		PE-3	Control de Acceso Físico	
		PE-5	Control de Acceso para Medios de Presentación	
		PE-6	Monitoreo de Accesos Físicos	
		PE-8	Registros de Acceso	
Seguridad en oficinas, recintos e instalaciones	9.1.3	N/A	N/A	Se implementará controles de acceso con huella a estas instalaciones.
Protección contra amenazas externas y del ambiente	9.1.4	PE-13	Protección contra Incendios	Se designará y aplicará protección física del fuego, inundación, terremoto, explosión, malestar civil y otras formas de desastres natural o humana.
		PE-15	Protección contra Daños de Inundaciones	
Trabajo en áreas seguras	9.1.5	PE-3	Control de Acceso Físico	Será diseñado y aplicado el plan de protección física y pautas para trabajar en áreas seguras.
Áreas de acceso público, entrega y carga	9.1.6	PE-2	Autorizaciones de Acceso Físico	Las áreas de carga y descarga serán controladas y monitoreadas, de ser posible se aislarán de los recursos de tratamiento de información para evitar acceso no autorizado.
		PE-3	Control de Acceso Físico	
		PE-16	Entrega y Remoción	

Tabla 12. (Continuación)

Nombre Control ISO 27002	Ctrl. ISO	Ctrl. NIST	Nombre Control. NIST	Control
Ubicación y protección del equipamiento	9.2.1	PE-13	Protección contra Incendios	Los equipos serán situados de una mejor forma y serán protegidos para reducir el riesgo de amenazas del entorno, así como las oportunidades de accesos no autorizados.
		PE-14	Controles de Temperatura y Humedad	
		PE-15	Protección contra Daños de Inundaciones	
		PE-18	Localización de Componentes del Sistema de Información	
Suministro de energía	9.2.2	PE-9	Equipamiento e Instalación de Alimentación Eléctrica	Se protegerán los equipos contra fallos de energía u otras anomalías eléctricas con PDU's y UPS's.
		PE-10	Apagado de Emergencia	
		PE-11	Alimentación de Emergencia	
		PE-12	Alumbrado de Emergencia	
Seguridad del cableado	9.2.3	PE-4	Control de Acceso para Medios de Transmisión	Se protegerá el cableado en tubería para prevenir interceptación o daño del cableado de energía y telecomunicaciones que transporten datos o soporten servicios de información.
		PE-9	Equipamiento e Instalación de Alimentación Eléctrica	
Mantenimiento de equipos	9.2.4	MA-2	Mantenimiento Periódico	Se regirá un plan de mantenimientos trimestral para asegurar la continua disponibilidad e integridad de los equipos.
		MA-5	Personal de Mantenimiento	
Seguridad del equipamiento propio fuera de la empresa	9.2.5	AC-20	Sistemas de información de propiedad personal	Los equipos que se encuentren fuera de las instalaciones de la empresa serán protegidos con carcazas más resistentes y su información será cifrada.
Descarte o reúso seguros del equipamiento	9.2.6	MP-6	Sanitización y Eliminación de Medios	Todos los elementos del equipo que contengan dispositivos de almacenamiento serán cifrados.
Retiro de bienes	9.2.7	PE-16	Entrega y Remoción	El equipo, información o software no podrá ser sacado fuera de las instalaciones sin autorización.

Tabla 12. (Continuación)

Nombre Control ISO 27002	Ctrl. ISO	Ctrl. NIST	Nombre Control. NIST	Control
Documentación de los procedimientos operativos	10.1.1	MA-1	Políticas y Procedimientos de Mantenimiento del Sistema	Se documentarán y mantendrán los procedimientos de operación y serán puestos a disposición de todos los usuarios que lo requieran.
		MP-1	Políticas y Procedimientos de Protección de Medios	
Gestión de Cambios	10.1.2	CM-3	Control de Cambios de Configuraciones	Se llevará un control de los cambios en los sistemas y recursos de tratamiento de la información.
		CM-4	Monitoreo de Cambios de Configuración	
Separación de funciones	10.1.3	AC-5	Separación de Funciones	Las tareas y responsabilidades serán segregadas para reducir oportunidades de modificación no autorizada.
Separación de las facilidades de desarrollo y operación	10.1.4	N/A	N/A	Los recursos serán separados para desarrollo, prueba y producción.
Entrega de Servicios	10.2.1	SA-9	Servicios Externos del Sistema de Información	Se diseñará un procedimiento que especifique cómo debe tratarse los servicios externos.
Monitoreo y revisión de servicios de terceros	10.2.2	SA-9	Servicios Externos del Sistema de Información	Los servicios, reportes y registros provistos por terceros serán monitoreados regularmente.
Gestión de cambios en servicios de terceros	10.2.3	CM-3	Control de Cambios de Configuraciones	Los cambios en la provisión del servicio serán gestionados teniendo en cuenta su importancia.
Administración de la Capacidad	10.3.1	SA-2	Asignación de Recursos	El uso de recursos y proyecciones hechas de requisitos de capacidades serán monitoreados.
Aceptación de sistemas	10.3.2	AT-3	Entrenamiento en Seguridad	Se establecerán criterios de aceptación para nuevos sistemas de información y versiones nuevas o mejoras, y con ellos desarrollar pruebas adecuadas antes de su aceptación.
		CA-1	Políticas y Procedimientos de Certificación, Acreditación y Valuación de Seguridad	
		CA-4	Certificación de Seguridad	
		CA-6	Acreditación de Seguridad	
		CP-2	Plan de Contingencia	

Tabla 12. (Continuación)

Nombre Control ISO 27002	Ctrl. ISO	Ctrl. NIST	Nombre Control. NIST	Control
Controles contra código malicioso	10.4.1	AT-2	Concientización en Seguridad	Se implementarán controles para detectar el software malicioso y prevenirse contra él, juntos a los procedimientos adecuados para concientizar los usuarios.
		CP-1	Políticas y Procedimientos de Planificación de Contingencias	
		CP-2	Plan de Contingencia	
		IR-1	Políticas y procedimientos de Respuesta a Incidentes	
		SC-18	Código móvil	
		SI-3	Protección contra código malicioso	
		SI-5	Alertas y avisos de seguridad	
Controles contra código Móvil	10.4.2	SC-18	Código móvil	Se confirmará que el código móvil usado opera de acuerdo a una política de seguridad.
Respaldo de la Información	10.5.1	CP-4	Pruebas del Plan de Contingencias	Se realizarán copias de respaldo de la información y del software.
		CP-6	Sitios Alternativos de Almacenamiento	
		CP-9	Respaldo del Sistema de Información	
		PE-3	Control de Acceso Físico	
		PE-14	Controles de Temperatura y Humedad	
Controles de Red	10.6.1	AC-5	Separación de Obligaciones	Las redes se manejarán y controlarán adecuadamente para protegerla de amenazas y mantener la seguridad de los sistemas y aplicaciones que las usan.
		SC-8	Integridad de las Transmisiones	
		SC-9	Confidencialidad de las Transmisiones	
Seguridad de los servicios de Red	10.6.2	AC-4	Forzado de Flujo de Información	Las características de seguridad, niveles de servicio y los requisitos de gestión de todos los servicios de red serán identificadas e incluidas en acuerdos de servicio de red.
		CA-3	Conexiones del Sistema de Información	
		SA-9	Servicios Externos del Sistema de Información	
		SI-4	Herramientas y Técnicas de Monitoreo del Sistema de Información	

Tabla 12. (Continuación)

Nombre Control ISO 27002	Ctrl. ISO	Ctrl. NIST	Nombre Control. NIST	Control
Administración de medios informáticos removibles	10.7.1	MP-1	Políticas y Procedimientos de Protección de Medios	Se definirán procedimientos para la gestión de los medios informáticos removibles.
		MP-4	Almacenamiento de Medios	
		MP-6	Sanitización y Eliminación de Medios	
		PE-14	Controles de Temperatura y Humedad	
		PE-16	Entrega y Remoción	
Descarte de medios de almacenamiento	10.7.2	MP-1	Políticas y Procedimientos de Protección de Medios	Los medios serán eliminados de forma segura y sin peligro cuando no se necesiten más, utilizando procedimientos formales.
		MP-4	Almacenamiento de Medios	
		MP-6	Sanitización y Eliminación de Medios	
Procedimientos para el manejo de la información	10.7.3	MP-1	Políticas y Procedimientos de Protección de Medios	Será definida una política que contemple el mecanismo a seguir para el uso de la información, y especificar la información que se puede usar.
		MP-2	Acceso a Medios	
		MP-3	Etiquetado de Medios	
		MP-4	Almacenamiento de Medios	
		SI-10	Exactitud, Totalidad, Validez y Autenticidad de la Información	
		SI-12	Manejo y Retención de la Salida de Información	
Seguridad de la documentación del sistema	10.7.4	MP-1	Políticas y Procedimientos de Protección de Medios	La documentación será protegida con claves de acceso y registro de apertura para protegerla contra accesos no autorizados.
		MP-4	Almacenamiento de Medios	
		SA-5	Documentación del Sistema de Información	
Políticas y procedimientos de intercambio de información	10.8.1	SC-1	Políticas y Procedimientos de Protección del Sistema y Comunicaciones	Se establecerán políticas, procedimientos y controles en el uso de VPN's en la transmisión de los datos.
		SC-4	Remanentes de Información	
		SC-8	Integridad de las Transmisiones	
		SC-9	Confidencialidad de las Transmisiones	

Tabla 12. (Continuación)

Nombre Control ISO 27002	Ctrl. ISO	Ctrl. NIST	Nombre Control. NIST	Control
Acuerdos de intercambio	10.8.2	AU-10	No Repudio	Se definirán acuerdos para el intercambio de información y software entre la organización y terceros.
		MP-3	Etiquetado de Medios	
		SC-16	Transmisión de Parámetros de Seguridad	
Medios físicos en tránsito	10.8.3	MP-5	Transporte de Medios	Los medios que contengan información serán encriptados y protegidos con contraseña para protegerlos durante el transporte fuera de los límites físicos.
Mensajería Electrónica	10.8.4	SC-5	Protección contra Negación de Servicios	Se tendrá un servidor de mensajería de respaldo.
Sistemas de Información de Negocios	10.8.5	CP-2	Plan de Contingencia	Se desarrollarán e implementarán políticas y procedimientos de continuidad del negocio, con el fin de establecer cómo recuperarse tras una falla y el negocio continúe en operación.
Comercio Electrónico	10.9.1	AU-10	No Repudio	El comercio electrónico será implementado bajo un servicio que garantice la confidencialidad e integridad de la información, además de garantía de autenticidad al recipiente de la información.
		CA-3	Conexiones del Sistema de Información	
		SC-8	Integridad de las Transmisiones	
		SC-9	Confidencialidad de las Transmisiones	
Transacciones en línea	10.9.2	SC-11	Trayectorias Confiables	Se utilizará una entidad certificadora para darle una mayor confianza a lo que se transmite.
		SC-16	Transmisión de Parámetros de Seguridad	
Información disponible públicamente	10.9.3	SC-14	Protecciones de Acceso Público	Toda la información será publicada sólo por los medios oficiales de la empresa, que contengan certificados por entidades reconocidas.

Tabla 12. (Continuación)

Nombre Control ISO 27002	Ctrl. ISO	Ctrl. NIST	Nombre Control. NIST	Control
Registro de Auditoría	10.10.1	AC-5	Separación de Obligaciones	Los registros de auditoria grabando actividades de los usuarios, excepciones y eventos de la seguridad de información serán respaldados en un servidor de réplica y resguardados en una ubicación distinta, con el fin de que asistan investigaciones futuras y en el monitoreo de los controles de acceso.
		AU-1	Políticas Procedimientos de Auditoria y Responsabilidades	
		AU-2	Eventos auditables	
		AU-3	Contenido de los Registros de Auditoria	
		AU-11	Retención de la Auditoria	
		SI-4	Herramientas y Técnicas de Monitoreo del Sistema de Información	
Monitoreo del uso del sistema	10.10.2	AC-13	Supervisión y revisión del Control de Acceso	Se usarán auditorias de uso en todos los servicios, que almacenen todo lo que cada usuario realice y las operaciones que ejecute.
		AU-1	Políticas Procedimientos de Auditoria y Responsabilidades	
		AU-6	Monitoreo, Análisis e Informes de Auditoria	
		RA-3	Valuación de Riesgos	
		SI-4	Herramientas y Técnicas de Monitoreo del Sistema de Información	

Tabla 12. (Continuación)

Nombre Control ISO 27002	Ctrl. ISO	Ctrl. NIST	Nombre Control. NIST	Control
Protección de la información de registros (logs)	10.10.3	AU-1	Políticas Procedimientos de Auditoria y Responsabilidades	Se activarán los logs de todos los servicios que se ofrezcan y estos serán respaldados en caso de manipulación.
		AU-4	Capacidad de Almacenamiento de Auditorias	
		AU-5	Procesamiento de Auditoria	
		AU-7	Reducción de Auditoria y Generación de Informes	
		AU-9	Protección de la Información de Auditoria	
Registros (logs) de administradores y operadores	10.10.4	AU-1	Políticas Procedimientos de Auditoria y Responsabilidades	Las actividades del administrador y de los operadores del sistema serán registradas.
		AU-3	Contenido de los Registros de Auditoria	
		AU-6	Monitoreo, Análisis e Informes de Auditoria	
		SI-4	Herramientas y Técnicas de Monitoreo del Sistema de Información	
Registro de Fallas	10.10.5	AU-1	Políticas Procedimientos de Auditoria y Responsabilidades	Se llevará una bitácora en la que se registre las fallas que se presenten, por qué se originó y la acción correctiva que se aplicó
		RA-3	Valuación de Riesgos	
		SI-2	Remediación de agujeros de seguridad	
Sincronización de relojes	10.10.6	AU-1	Políticas Procedimientos de Auditoria y Responsabilidades	Los relojes de todos los sistemas dentro de la organización serán sincronizados con la fuente de http://horalegal.inm.gov.co/
		AU-8	Estampado de fecha y hora	
Política de Control de Acceso	11.1.1	AC-1	Políticas y Procedimientos de Control de Acceso	Será establecida una política de control de acceso, documentada y revisada, estará basada en los requisitos de seguridad y del negocio.

Tabla 12. (Continuación)

Nombre Control ISO 27002	Ctrl. ISO	Ctrl. NIST	Nombre Control. NIST	Control
Registración de usuarios	11.2.1	AC-2	Gestión de Cuentas	La creación de los nuevos usuarios y los permisos asignados serán solicitados por su jefe y visado por el superior que avale lo solicitado, además se guardará un histórico de los permisos asignados.
		PS-4	Terminación de la relación laboral	
		PS-5	Transferencia de Personal	
		PS-7	Seguridad del Personal de Terceros	
		PS-8	Sanciones al Personal	
Medida de los Privilegios	11.2.2	AC-2	Gestión de Cuentas	Se define una matriz de perfiles para controlar los privilegios que se otorgan.
		AC-6	Privilegios mínimos	
Gestión de contraseñas de usuarios	11.2.3	IA-2	Identificación y Autenticación de Usuarios	Se controlará la asignación de contraseñas por medio de un proceso de gestión formal.
		IA-4	Gestión de Identificadores	
Revisión de derechos de acceso de usuarios	11.2.4	AC-2	Gestión de Cuentas	Cada tres meses se revisarán los usuarios y los derechos de acceso con los que cuente, para verificar que concuerde con las funciones que tenga asignadas.
		AC-3	Imposición de acceso	
		AC-13	Supervisión y revisión del Control de Acceso	
Uso de Contraseñas	11.3.1	N/A	N/A	Se seguirán buenas políticas de seguridad para la selección y uso de contraseñas.
Equipamiento no atendido de usuarios	11.3.2	AC-11	Bloqueo de sesione	Los usuarios se asegurarán que los equipos informáticos desatendidos estén protegidos.
		AC-12	Terminación de sesiones	
Políticas de escritorio y pantalla limpias	11.3.3	PE-5	Control de Acceso para Medios de Presentación	Se adoptará una política de escritorio limpio.
Política sobre el uso de servicios de red	11.4.1	AC-1	Políticas y Procedimientos de Control de Acceso	Los usuarios solo tendrán acceso directo a los servicios para los que están autorizados.
Autenticación de usuarios para conexiones externas	11.4.2	AC-17	Acceso remoto	Se solicitarán los accesos externos y estos serán visados por el jefe de infraestructura tecnológica y aplicado y monitoreado por el administrador de la red.
		AC-18	Restricciones de acceso inalámbrico	
		IA-2	Identificación y Autenticación de Usuarios	
		IA-3	Identificación y Autenticación de Dispositivos	

Tabla 12. (Continuación)

Nombre Control ISO 27002	Ctrl. ISO	Ctrl. NIST	Nombre Control. NIST	Control
Identificación del equipamiento en redes	11.4.3	AC-17	Acceso remoto	Se implementa una estructura de nombres de los equipos que sea único en la red con IP estáticas.
		IA-3	Identificación y Autenticación de Dispositivos	
Diagnóstico remoto y protección del puerto de configuración	11.4.4	AC-17	Acceso remoto	Se dará soporte remoto solo por el personal autorizado y se cerrarán los puertos que no se autoricen.
		MA-4	Mantenimiento Remoto	
Subdivisión de redes	11.4.5	AC-3	Forzado de Acceso	Los grupos de servicios de información, usuarios y sistemas de información serán segregados de la red, por medio de vlan que serán configuradas en los switches y los permisos serán gestionados a través del firewall lógico
		AC-4	Forzado de Flujo de Información	
		CA-3	Conexiones del Sistema de Información	
		SC-2	Particionamiento de las Aplicaciones	
		SC-3	Aislado de la Función de Seguridad	
Control de conexiones de red	11.4.6	AC-4	Forzado de Flujo de Información	Sólo serán permitidas las conexiones a los servicios que cada equipo requiera, y se llevará un log del tráfico que se genere.
		CA-3	Conexiones del Sistema de Información	
		SC-7	Protección de Fronteras	
Control de enrutados en la red	11.4.7	AC-4	Forzado de Flujo de Información	Con el uso de vlan en la red todo el tráfico se enruta a través del firewall lógico el cual controlará los acceso y registrará toda la actividad.
		CA-3	Conexiones del Sistema de Información	
Procedimientos de registro seguro	11.5.1	AC-7	Intentos de logueo fallados	Será controlado el acceso a los sistemas operativos mediante un procedimiento de registro de inicio seguro que solo conocerá el usuario de cada equipo.
		AC-8	Notificación de Uso de los Sistemas	
		AC-9	Notificación de Logueos previos	
		IA-6	Realimentación del autenticador	
Identificación y autenticación de usuarios	11.5.2	IA-2	Identificación y Autenticación de Usuarios	Se dispondrá de un identificador único para el uso personal de todos los usuarios y se implementará el acceso con huella para verificar la identidad a los equipos con información crítica.
		IA-4	Gestión de Identificadores	
		IA-5	Realimentación del Autenticador	

Tabla 12. (Continuación)

Nombre Control ISO 27002	Ctrl. ISO	Ctrl. NIST	Nombre Control. NIST	Control
Sistema de Administración de Contraseñas	11.5.3	IA-5	Realimentación del autenticador	Se proporcionará un medio eficaz e interactivo para asegurar la calidad de contraseñas.
Uso de utilitarios del sistema	11.5.4	N/A	N/A	Se mantendrán actualizados los sistemas operativos y se desactivará el software que no sea necesario para la labor de la empresa.
Time-out de sesiones	11.5.5	AC-12	Terminación de sesiones	Las sesiones expirarán tras un periodo de inactividad de 10 minutos.
Limitación del tiempo de conexión	11.5.6	SC-10	Desconexión de la Red	El tiempo de conexión será otorgado y monitoreado por el administrador de la red.
Restricciones al acceso a la Información	11.6.1	CM-5	Restricciones de Acceso para Cambios	Se dará acceso solo a los usuarios autorizados.
Aislamiento de sistemas sensibles	11.6.2	N/A	N/A	Se proporcionarán entornos informáticos dedicados aislados a los sistemas sensibles.
Computación y comunicaciones móviles	11.7.1	AC-18	Restricciones de acceso inalámbrico	Será adoptada una política y medidas de seguridad apropiadas con el fin de proteger contra los riesgos cuando se usan dispositivos de informática.
		AC-19	Control de acceso para sistemas portátiles y móviles	
		AC-20	Sistemas de información de propiedad personal	
		AT-2	Concientización en Seguridad	
		AT-3	Entrenamiento en Seguridad	
		CP-9	Respaldo del Sistema de Información	
		IA-3	Identificación y Autenticación de Dispositivos	
Teletrabajo	11.7.2	AC-2	Gestión de Cuentas	Se implementará una VPN para la conexión a los servicios de los usuarios que requieran y se les autorice hacer teletrabajo.
		AC-18	Restricciones de acceso inalámbrico	
		PE-17	Sitio Alternativo de Trabajo	

Tabla 12. (Continuación)

Nombre Control ISO 27002	Ctrl. ISO	Ctrl. NIST	Nombre Control. NIST	Control
Análisis y especificaciones de requerimientos de Seguridad	12.1.1	SA-1	Políticas y Procedimientos del Sistema y Servicios	Se especificarán los requisitos de control en los enunciados de los requisitos de negocio para sistemas nuevos o mejoras a sistemas existentes.
		SA-4	Adquisiciones	
		SA-8	Principios de Diseño de Seguridad	
		SI-9	Restricciones para entrada de Información	
Validación de datos de entrada	12.2.1	SI-7	Integridad del Software y la Información	Los datos de entrada a las aplicaciones del sistema serán revisados y aprobados por el administrador de casa sistema que se esté alimentando o director del proyecto en ejecución.
		SI-9	Restricciones para entrada de Información	
		SI-10	Exactitud, Totalidad, Validez y Autenticidad de la Información	
		SI-11	Manejo de Errores	
Control del procesamiento interno	12.2.2	SI-7	Integridad del Software y la Información	Será incorporado comprobaciones de validación a los sistemas para detectar cualquier tipo de corrupción de información a través de errores del proceso o por actos deliberados.
		SI-9	Restricciones para entrada de Información	
		SI-10	Exactitud, Totalidad, Validez y Autenticidad de la Información	
		SI-11	Manejo de Errores	
Integridad de Mensajes	12.2.3	SI-11	Manejo de Errores	La información será transmitida sólo a través de los aplicativos de la empresa.
Validación de datos de salida	12.2.4	SI-7	Integridad del Software y la Información	Se validarán los datos de salida de un sistema de aplicación para garantizar que el proceso de la información ha sido correcto y apropiado a las circunstancias.
		SI-11	Manejo de Errores	
		SI-12	Manejo y Retención de la Salida de Información	
Política sobre el uso de controles criptográficos	12.3.1	AU-10	No Repudio	Será desarrollada e implementada una política de uso de las medidas criptográficas para proteger la información.
		SC-12	Establecimiento y Gestión de Claves Criptográficas	
		SC-17	Certificadores de Infraestructura de Clave Pública	

Tabla 12. (Continuación)

Nombre Control ISO 27002	Ctrl. ISO	Ctrl. NIST	Nombre Control. NIST	Control
Administración de Claves	12.3.2	SC-12	Establecimiento y Gestión de Claves Criptográficas	Se utilizarán claves criptográficas para apoyar el uso de las técnicas criptográficas.
		SC-17	Certificadores de Infraestructura de Clave Pública	
Control del Software Operacional	12.4.1	CM-1	Políticas y Procedimientos de Gestión de Configuraciones	Serán establecidos procedimientos para controlar la instalación del software en sistemas operacionales.
		CM-3	Control de Cambios de Configuraciones	
		SI-2	Remediación de agujeros de seguridad	
Protección de los datos de prueba de sistemas	12.4.2	N/A	N/A	Los datos que se manejen en pruebas serán copia de una base de datos real pero que con anterioridad haya sido ofuscada y se cambie cada mes.
Control de Acceso a las biblioteca de los fuentes de programas	12.4.3	N/A	N/A	Solo el DBA tendrá acceso al código fuentes o compilado y donde se almacenen.
Procedimientos de Control de Cambios	12.5.1	CM-1	Políticas y Procedimientos de Gestión de Configuraciones	La implementación de cambios se controlará usando procedimientos formales de cambio.
		CM-3	Control de Cambios de Configuraciones	
		RA-3	Valuación de Riesgos	
		SA-10	Gestión de Configuración de Desarrolladores	
		SA-11	Pruebas de Seguridad de Desarrolladores	
		SI-2	Remediación de agujeros de seguridad	

Tabla 12. (Continuación)

Nombre Control ISO 27002	Ctrl. ISO	Ctrl. NIST	Nombre Control. NIST	Control
Revisión técnica de las aplicaciones luego de cambios en el Sistema Operativo	12.5.2	CM-3	Control de Cambios de Configuraciones	Las aplicaciones del sistema serán revisadas y probadas para verificar que el sistema continúe trabajando de la mejor manera y todos los periféricos sigan en funcionamiento.
		SA-10	Gestión de Configuración de Desarrolladores	
		SA-11	Pruebas de Seguridad de Desarrolladores	
Restricciones en los cambios en paquetes de software	12.5.3	CM-3	Control de Cambios de Configuraciones	Se limitará a cambios necesarios estrictamente controlados.
Desarrollo de software por parte de terceros	12.5.5	N/A	N/A	El código, las operaciones y resultados de las aplicaciones externas serán verificados por el DBA.
Control de vulnerabilidades técnicas	12.6.1	RA-3	Valuación de Riesgos	Se tratará de obtener a tiempo la información sobre las vulnerabilidades técnicas de los sistemas de información utilizadas.
		RA-5	Escaneo de Vulnerabilidades	
		SI-2	Remediación de agujeros de seguridad	
Reportes de eventos de seguridad de la información	13.1.1	AT-2	Concientización en Seguridad	Se reportará lo más rápido posible los eventos de seguridad de información a través de una gestión de canales apropiada.
		AT-3	Entrenamiento en Seguridad	
		IR-1	Políticas y procedimientos de Respuesta a Incidentes	
		IR-2	Entrenamiento en Respuesta a Incidentes	
Reportes de debilidades de seguridad	13.1.2	IR-1	Políticas y procedimientos de Respuesta a Incidentes	Se anotarán y reportarán las debilidades o sospechas de seguridad encontradas por todos los usuarios.
		IR-6	Monitoreo de Incidentes	
Responsabilidades y Procedimientos	13.2.1	AU-6	Monitoreo, Análisis e Informes de Auditoria	Serán establecidos manuales de funciones para todos los cargos, especificando las funciones, el alcance y las responsabilidades de cada uno.
		IR-1	Políticas y procedimientos de Respuesta a Incidentes	
		IR-4	Manejo de Incidentes	
		SC-5	Protección contra Negación de Servicios	
Aprendizaje a partir de incidentes de seguridad de la Información	13.2.2	IR-4	Manejo de Incidentes	Será establecido un mecanismo para que los tipos, volúmenes y costos de los incidentes en la seguridad sean cuantificados y monitoreados.

Tabla 12. (Continuación)

Nombre Control ISO 27002	Ctrl. ISO	Ctrl. NIST	Nombre Control. NIST	Control
Recolección de evidencia	13.2.3	N/A	N/A	Cada vez que ocurra un incidente de seguridad será recogida toda la evidencia posible para soportar el procedimiento que se infringió y esta quedará documentada y almacenada.
Inclusión de la Seguridad de la Información en el proceso de gestión de continuidad de negocios	14.1.1	CP-1	Políticas y Procedimientos de Planificación de Contingencias	En toda la organización se instalará un proceso de gestión para el desarrollo y mantenimiento de la empresa.
		RA-3	Valuación de Riesgos	
Continuidad de Negocios y Valuación de Riesgos	14.1.2	RA-3	Valuación de Riesgos	Se identificarán las interrupciones causadas, y consecuencias para la seguridad de la información.
Desarrollo e implementación de planes de continuidad que incluyan seguridad de la información	14.1.3	CP-1	Políticas y Procedimientos de Planificación de Contingencias	Serán desarrollados planes de mantenimiento y recuperación de las operaciones del negocio, que aseguren la disponibilidad de información al nivel y en escalas de tiempo requeridas tras la interrupción o falla de sus procesos críticos.
		CP-2	Plan de Contingencia	
		CP-3	Entrenamiento en Contingencias	
		CP-5	Actualización del Plan de Contingencias	
		IR-7	Asistencia para la Respuesta a Incidentes	
Marcos de trabajo para la planificación de continuidad de los negocios	14.1.4	AT-2	Concientización en Seguridad	Se mantendrá un esquema único de planes de continuidad del negocio para asegurar que dichos planes sean consistentes.
		AT-3	Entrenamiento en Seguridad	
		CP-2	Plan de Contingencia	
		CP-3	Entrenamiento en Contingencias	
		CP-5	Actualización del Plan de Contingencias	
		CP-7	Asistencia para la Respuesta a Incidentes	
		CP-8	Servicios de Telecomunicaciones	
		CP-10	Recuperación y Reconstitución del Sistema de Información	
Prueba, mantenimiento y revaluación de planes de continuidad de negocios	14.1.5	CP-4	Pruebas del Plan de Contingencias	Se probarán regularmente los planes de continuidad del negocio.
		CP-5	Actualización del Plan de Contingencias	

Tabla 12. (Continuación)

Nombre Control ISO 27002	Ctrl. ISO	Ctrl. NIST	Nombre Control. NIST	Control
Identificación de legislaciones aplicables	15.1.1	AC-1	Políticas y Procedimientos de Control de Acceso	Serán definidas las leyes que se pueden infringir y se establecerán los mecanismos aplicados con las sanciones correspondientes.
		AT-1	Políticas y Procedimientos de Concientización y Capacitación en Seguridad	
		AU-1	Políticas Procedimientos de Auditoria y Responsabilidades	
		CA-1	Políticas y Procedimientos de Certificación, Acreditación y Valuación de Seguridad	
		CM-1	Políticas y Procedimientos de Gestión de Configuraciones	
		CP-1	Políticas y Procedimientos de Planificación de Contingencias	
		IA-1	Políticas y Procedimientos de Identificación y Autenticación	
		IR-1	Políticas y procedimientos de Respuesta a Incidentes	
		MA-1	Políticas y Procedimientos de Mantenimiento del Sistema	
		MP-1	Políticas y Procedimientos de Protección de Medios	
		PE-1	Políticas y Procedimientos de Protección Física y Ambiental	
		PL-1	Políticas y Procedimientos de Planificación de Seguridad	
		PS-1	Políticas y Procedimientos de Seguridad del Personal	

Tabla 12. (Continuación)

Nombre Control ISO 27002	Ctrl. ISO	Ctrl. NIST	Nombre Control. NIST	Control
Identificación de legislaciones aplicables		RA-1	Políticas y Procedimientos de Valuación de Riesgos	
		SA-1	Políticas y Procedimientos del Sistema y Servicios	
		SC-1	Políticas y Procedimientos de Protección del Sistema y Comunicaciones	
		SI-1	Políticas y Procedimientos del Sistema y Servicios	
Derechos de Propiedad Intelectual	15.1.2	CM-2	Configuraciones Básicas de los sistemas de información e Inventario de los componentes	Se registrará el software producido internamente y sólo se utilizará software del que se tenga licencia de uso.
		SA-6	Restricción del Uso de Software	
		SA-7	Software instalado por Usuarios	
Protección de registros de la organización	15.1.3	AU-9	Protección de la Información de Auditoria	Los registros importantes de la organización se respaldarán en una ubicación y locación diferente para protegerse frente a su pérdida, destrucción y falsificación.
		AU-11	Retención de la Auditoria	
		MP-1	Políticas y Procedimientos de Protección de Medios	
		MP-3	Etiquetado de Medios	
		MP-4	Almacenamiento de Medios	
Protección de datos y privacidad de la información personal	15.1.4	AT-2	Concientización en Seguridad	Se asegurará la información con validaciones de huella para acceder a ella.
		PL-5	Valuación de Impactos a la Privacidad	
Prevención del mal uso de las facilidades de procesamiento de la información	15.1.5	AC-8	Notificación de Uso de los Sistemas	Se capacitará periódicamente al personal para utilizar los recursos y la información solo para propósitos autorizados.
		PL-4	Reglas de Comportamiento	
Regulación de controles criptográficos	15.1.6	N/A	N/A	Se usarán controles criptográficos en conformidad con los acuerdos, leyes y regulaciones.

Tabla 12. (Continuación)

Nombre Control ISO 27002	Ctrl. ISO	Ctrl. NIST	Nombre Control. NIST	Control
Conformidad con la política de seguridad	15.2.1	CA-2	Valuaciones de Seguridad	Se hará una verificación trimestral por parte de auditoría con el fin de verificar que se cumpla lo que se ha estipulado.
		CA-5	Plan de Acción e Hitos	
		CA-7	Monitoreo Continuo	
Chequeos de conformidad Técnica	15.2.2	CA-2	Valuaciones de Seguridad	Se realizará un monitoreo continuo de las normas de implantación de la seguridad en los sistemas.
		CA-7	Monitoreo Continuo	
Controles de Auditoría de Sistemas de Información	15.3.1	PL-6	Planificación de Actividades relacionadas con la Seguridad	Se hará una lista de las actividades que incluye la auditoría y los tiempos de cada una de ellas.
Protección de herramientas de auditoría de sistemas de información	15.3.2	AU-9	Protección de la Información de Auditoria	Solo el personal autorizado tendrá acceso a las herramientas de auditoria, por medio de controles de red y claves de acceso.

Fuente. El Autor.

13. LISTA DE CHEQUEO

Tabla 13 Lista de Chequeo

Lista de chequeo basado en Iso 27002				
Empresa: CEDIT – Universidad Francisco de Paula Santander Ocaña				
Responsable: Libardo Andrey Quintero González			Fecha: 27/10/2016	
Elemento auditado	CheckList	Cumple		Observaciones
		Si	No	
Documentación de la Política de Seguridad de Información	Existen roles y responsabilidades para todos los cargos concernientes a Seguridad de la Información		X	
Revisión de la Política de Seguridad de la Información	Se cuentan con intervalos definidos de tiempo para revisiones de la política		X	
Compromiso Gerencial a la seguridad de la información	La gerencia tiene identificadas las metas de seguridad de la información y provee los recursos necesarios para la seguridad de la información		X	
Coordinación en seguridad de la información	Las actividades de seguridad son ejecutadas en cumplimiento con la política de seguridad de la información.		X	
Asignación de Responsabilidades de seguridad de la información	Se revisa en los manuales de políticas y procedimientos que no existan inconsistencias, en cuanto a la asignación de responsabilidades concernientes a seguridad de la información		X	
Proceso de autorización para las facilidades de Procesamiento de la Información	Se realizan evaluaciones del uso de medios informáticos personales para el tratamiento de la información de la empresa		X	
Acuerdos de confidencialidad	Existen acuerdos de confidencialidad que sean aplicados a personal interno y externo.		X	
Contactos con autoridades	Existe una comunicación directa y periódica con las autoridades locales inmediatas		X	

Tabla 13. (Continuación)

Lista de chequeo basado en Iso 27002				
Empresa: CEDIT – Universidad Francisco de Paula Santander Ocaña				
Responsable: Libardo Andrey Quintero González				Fecha: 27/10/2016
Elemento auditado	CheckList	Cumple		Observaciones
		Si	No	
Contactos con grupos de intereses especiales	Existen subscripciones con grupos a nivel local y nacional sobre temas de seguridad	X		Parcialmente Implementado. Falta contactos apropiados con grupos de interés en seguridad informática
Revisión independiente de la seguridad de la información	Existen intervalos de planificación para la implementación de nuevos proyectos para salvaguardar la información.	X		Parcialmente Implementado. Falta hacer una revisión por separado y a fondo de la seguridad de la información, así como establecer intervalos para esto
Identificación del riesgo relacionado con terceros	Existe una política especificando controles para acceso a recursos por parte de terceros		X	
Atención a la seguridad en el trato con los clientes	Se documente si existen términos contractuales antes de otorgar el acceso.		X	
Atención a la seguridad en los acuerdos con terceros o outsourcing	En los acuerdos con terceras partes exista la política de seguridad de la información		X	
Inventario de Activos	Existe la política de inventarios de activos de la información.	X		Parcialmente Implementado. No existe una correcta nomenclatura que identifique los activos, no todos los activos están inventariados
Propiedad de los activos	Esta especificado en los manuales los controles y responsabilidades que el propietario de los activos presta		X	
Uso aceptable de los activos	En los contratos con terceros existen cláusulas que responsabilicen en uso adecuado de los activos		X	
Pautas de clasificación	Existe la clasificación de activos en los manuales	X		Implementado

Tabla 13. (Continuación)

Lista de chequeo basado en Iso 27002				
Empresa: CEDIT – Universidad Francisco de Paula Santander Ocaña				
Responsable: Libardo Andrey Quintero González				Fecha: 27/10/2016
Elemento auditado	CheckList	Cumple		Observaciones
		Si	No	
Etiquetado y manejo de la Información	Existe un procedimiento de tratamiento de la información según su clasificación	X		Parcialmente Implementado. No toda la información está etiquetada
Roles y Responsabilidades	Está especificado en los manuales las responsabilidades de cada una de las partes	X		Parcialmente Implementado. Falta agregarle responsabilidades a algunos puestos
Selección	Existen listas de verificación para los procesos de selección de personal	X		Parcialmente Implementado. Falta hacer un checklist independiente para cada cargo
Términos y condiciones de empleo	Existe un ítem claro en los contratos donde se evidencie que el empleado aceptado las condiciones que se establecen	X		Implementado
Responsabilidad Gerencial	La gerencia está implicada en el proceso de selección de la empresa	X		Implementado
Proceso disciplinario	Existen rutas de acción para las fallas de seguridad cometidas		X	
Responsabilidades en la terminación de la relación laboral	Existe un procedimiento claro de terminación laboral	X		Implementado
Devolución de activos	Se cuenta con un proceso para cuando haya una terminación laboral	X		Parcialmente Implementado. Falta el registro de devolución de activos
Remoción de derechos de acceso	En la política existe un ítem de remoción de accesos y activos al terminar un contrato laboral		X	
Perímetro de seguridad física	Existe un control de ingreso de personal a las instalaciones restringidas		X	
Controles de acceso físico	Hay restricción de ingreso a áreas sensibles de la empresa		X	
Seguridad en oficinas, recintos e instalaciones	Existen políticas de seguridad física		X	
Protección contra amenazas externas y del ambiente	Se cuenta con un plan de simulacros controlados con el personal		X	
Trabajo en áreas seguras	Existen cámaras y monitoreo en las áreas sensibles de la empresa	X		Implementado

Tabla 13. (Continuación)

Lista de chequeo basado en Iso 27002				
Empresa: CEDIT – Universidad Francisco de Paula Santander Ocaña				
Responsable: Libardo Andrey Quintero González			Fecha: 27/10/2016	
Elemento auditado	CheckList	Cumple		Observaciones
		Si	No	
Áreas de acceso público, entrega y carga	Existe una identificación para las áreas públicas de la empresa	X		Parcialmente Implementado. Faltan algunas áreas por identificar
Ubicación y protección del equipamiento	Existen políticas de seguridad industrial	X		Parcialmente Implementado. Falta hacer una mejora en la ubicación del equipo
Suministro de energía	Se cuenta con UPS y respaldo de energía	X		Implementado
Seguridad del cableado	El cableado estructurado se encuentra correctamente protegido basado en un estándar	X		Implementado
Mantenimiento de equipos	Existe un plan de mantenimientos preventivos a los equipos que lo requieran	X		Parcialmente Implementado. Hay que organizar mejor el plan de mantenimiento y los periodos para ejecutarse
Seguridad del equipamiento propio fuera de la empresa	Existen seguros y pólizas sobre equipos de préstamo y traslado	X		Parcialmente Implementado. Falta hacer un registro y control de los equipos que cuentan con la pólizas y su vigencia
Descarte o reúso seguros del equipamiento	Existe una hoja de vida de equipos que permite evidenciar su uso y tiempo en la empresa	X		Parcialmente Implementado. Falta definir el tiempo de vida útil para cada tipo de equipo
Retiro de bienes	Existe la política de retiro de equipos y programas instalados	X		Parcialmente Implementado. Hay que mejorar las exigencias de cada equipo para así saber lo que se debe retirar
Documentación de los procedimientos operativos	Hay una política para la elaboración de manuales, políticas y procedimientos		X	

Tabla 13. (Continuación)

Lista de chequeo basado en Iso 27002				
Empresa: CEDIT – Universidad Francisco de Paula Santander Ocaña				
Responsable: Libardo Andrey Quintero González			Fecha: 27/10/2016	
Elemento auditado	CheckList	Cumple		Observaciones
		Si	No	
Gestión de Cambios	Se deja rastro de modificaciones hechas	X		Parcialmente Implementado. Se debe mejorar la trazabilidad de cambios hechos
Separación de funciones	Existe una política de segregación de funciones		X	
Separación de las facilidades de desarrollo y operación	Existen ambientes diferentes para desarrollo y producción		X	
Entrega de Servicios	Se implementan los controles de seguridad según un acuerdo de entrega		X	
Monitoreo y revisión de servicios de terceros	Existe un monitoreo y acompañamiento de personal externo		X	
Gestión de cambios en servicios de terceros	Se lleva control sobre cambios en servicios		X	
Administración de la Capacidad	Se monitorean las proyecciones hechas		X	
Aceptación de sistemas	Existe un procedimiento de atención de errores posterior al pase a producción		X	
Controles contra código malicioso	Existe una política de requerimiento de licencias de software	X		Parcialmente Implementado. Faltan controles preventivos
Controles contra código Móvil	Existe una política de requerimiento de licencias de software	X		Parcialmente Implementado. Faltan controles preventivos
Respaldo de la Información	Existe un esquema de respaldo de la información	X		Parcialmente Implementado. Hay que mejorar los tiempos y archivos a respaldar y la ubicación donde se almacenan.
Controles de Red	Se cuenta con controles especiales a los datos transmitidos a través de la LAN y WAN		X	

Tabla 13. (Continuación)

Lista de chequeo basado en Iso 27002				
Empresa: CEDIT – Universidad Francisco de Paula Santander Ocaña				
Responsable: Libardo Andrey Quintero González			Fecha: 27/10/2016	
Elemento auditado	CheckList	Cumple		Observaciones
		Si	No	
Seguridad de los servicios de Red	Se hacen cumplir las clausulas para gestionar la red de forma segura	X		Parcialmente Implementado. Faltan mecanismos de fortalecimiento de la seguridad
Administración de medios informáticos removibles	Existe un proceso de ejecución seguro de medios removibles		X	
Descarte de medios de almacenamiento	Se cuenta con un proceso de destrucción de la información		X	
Procedimientos para el manejo de la información	Se cuenta con un proceso de manipulación de la información		X	
Seguridad de la documentación del sistema	Se cuenta con un procedimiento de no publicación de información sensible	X		Parcialmente Implementado. Falta definir qué se puede publicar
Políticas y procedimientos de intercambio de información	Se cuenta con un ítem de intercambio de información en la política de seguridad		X	
Acuerdos de intercambio	Existen cláusulas de confidencialidad previo a la otorgación de información		X	
Medios físicos en tránsito	Se cuenta con un ítem de intercambio de información en la política de seguridad		X	
Mensajería Electrónica	Existe control sobre información envida y recibida a través de correo electrónico		X	
Sistemas de Información de Negocios	Hay una política de protección de la información		X	
Comercio Electrónico	Existe una política que especifique la información que puede ser publicada	X		Parcialmente Implementado. Falta definir lo que se puede publicar
Transacciones en línea	Existe una política que especifique la información que puede ser publicada	X		Parcialmente Implementado. Falta definir lo que se puede publicar
Información disponible públicamente	Existe una política que especifique la información que puede ser publicada	X		Parcialmente Implementado. Falta definir lo que se puede publicar

Tabla 13. (Continuación)

Lista de chequeo basado en Iso 27002				
Empresa: CEDIT – Universidad Francisco de Paula Santander Ocaña				
Responsable: Libardo Andrey Quintero González			Fecha: 27/10/2016	
Elemento auditado	CheckList	Cumple		Observaciones
		Si	No	
Registro de Auditoría	Existe registro de logueo y acceso en los activos		X	
Monitoreo del uso del sistema	Existe monitoreo de acceso a la red	X		Parcialmente Implementado. Falta registros de auditoría y demás controles
Protección de la información de registros (logs)	Existe un registro de eventos	X		Parcialmente Implementado. Falta establecer logs de auditoría
Registros (logs) de administradores y operadores	Existe registro de logueo y acceso en los activos	X		Parcialmente Implementado. Falta establecer logs de auditoría
Registro de Fallas	Existe un registro de averías con el procesamiento o comunicación de la información.		X	
Sincronización de relojes	Se cuenta con un equipo confiable con el cual sincronizarse las máquinas	X		Implementado
Política de Control de Acceso	Existen perfiles de acceso a los usuarios	X		Parcialmente Implementado. Falta establecer niveles de acceso para definir mejor los controles de acceso a los usuarios
Registración de usuarios	Comprobar la existencia de documentos de compromiso antes de otorgar acceso a los diferentes entornos		X	
Medida de los Privilegios	Comprobar la existencia de documentos de compromiso antes de otorgar acceso a los diferentes entornos		X	

Tabla 13. (Continuación)

Lista de chequeo basado en Iso 27002				
Empresa: CEDIT – Universidad Francisco de Paula Santander Ocaña				
Responsable: Libardo Andrey Quintero González			Fecha: 27/10/2016	
Elemento auditado	CheckList	Cumple		Observaciones
		Si	No	
Gestión de contraseñas de usuarios	Existe una política que especifique el formato de la contraseña y cada cuanto debe expirar		X	
Revisión de derechos de acceso de usuarios	Existe un intervalo de tiempo de revisión de los permisos a los entornos		X	
Uso de Contraseñas	Están detalladas las políticas de la seguridad que deberá tener las contraseñas por parte de los usuarios		X	
Equipamiento no atendido de usuarios	Existen políticas que detallen la protección de los equipos en la ausencia de los usuarios		X	
Políticas de escritorio y pantalla limpias	Existe una política detallada sobre pantallas y escritorios limpios		X	
Política sobre el uso de servicios de red	Existe una política especificando quien puede autorizar el acceso a qué red o que servicio de red.		X	
Autenticación de usuarios para conexiones externas	Se tiene una lista de control para especificar qué usuarios se pueden conectar remotamente		X	
Identificación del equipamiento en redes	Existe un control de red que identifique equipos que no son confiables conectarse a la red y no permita acceso a ningún tipo de recursos basándose en registro de estaciones		X	
Diagnóstico remoto y protección del puerto de configuración	Se cuenta con diagnósticos remotos y configuración de puertos		X	
Subdivisión de redes	Existe segmentación o separación de la red y controles	X		Implementado
Control de conexiones de red	Existen una lista de requisitos de las aplicaciones que requieren conexiones	X		Parcialmente Implementado. Falta establecer requisitos de las aplicaciones

Tabla 13. (Continuación)

Lista de chequeo basado en Iso 27002				
Empresa: CEDIT – Universidad Francisco de Paula Santander Ocaña				
Responsable: Libardo Andrey Quintero González			Fecha: 27/10/2016	
Elemento auditado	CheckList	Cumple		Observaciones
		Si	No	
Control de enrutados en la red	Existen políticas de enrutamiento de información	X		Parcialmente Implementado. Falta establecer requisitos de las aplicaciones
Procedimientos de registro seguro	Existen políticas de dominio del Directorio Activo	X		Parcialmente Implementado. Hay que mejorar las políticas de directorio activo
Identificación y autenticación de usuarios	Existen políticas de dominio del Directorio Activo	X		Parcialmente Implementado. Hay que mejorar las políticas de directorio activo
Sistema de Administración de Contraseñas	Se cuenta con normas para cambio periódico de contraseñas		X	
Uso de utilitarios del sistema	Se tiene control sobre las aplicaciones instaladas en las estaciones de trabajo		X	
Time-out de sesiones	Se tiene política sobre el bloqueo de estaciones ya aplicaciones después de cierto periodo de inactividad		X	
Limitación del tiempo de conexión	Se tiene política sobre el bloqueo de estaciones y aplicaciones después de cierto periodo de inactividad		X	
Restricciones al acceso a la Información	Se cuenta con privilegios de acceso a las carpetas que contiene información valiosa	X		Implementado
Aislamiento de sistemas sensibles	Se controla con autenticación y reglas de acceso a las carpetas con información sensible	X		Parcialmente Implementado. Falta definir perfiles de acceso a los usuarios
Computación y comunicaciones móviles	Existen políticas internas para computación y uso del móvil		X	
Teletrabajo	Existe controles y políticas que se tiene para evitar que utilizando la VPN se pueda contagiar de virus la red		X	

Tabla 13. (Continuación)

Lista de chequeo basado en Iso 27002				
Empresa: CEDIT – Universidad Francisco de Paula Santander Ocaña				
Responsable: Libardo Andrey Quintero González			Fecha: 27/10/2016	
Elemento auditado	CheckList	Cumple		Observaciones
		Si	No	
Análisis y especificaciones de requerimientos de Seguridad	Existen políticas de la adquisición o desarrollo de software según las necesidades		X	
Validación de datos de entrada	Existen políticas de registro de actividad en los aplicativos		X	
Control del procesamiento interno	Existen políticas de registro de actividad en los aplicativos		X	
Integridad de Mensajes	Existen mecanismos para controlar la integridad de los mensajes		X	
Validación de datos de salida	Existe una política para el desarrollo de aplicaciones y verificación de los datos de salida	X		Parcialmente Implementado. Hay que mejorar los procedimientos de desarrollo de aplicaciones
Política sobre el uso de controles criptográficos	Existe una política especificando controles criptográficos para información sensible		X	
Administración de Claves	Se usan técnicas criptográficas para la creación de claves		X	
Control del Software Operacional	Existe la política de restringir la instalación de software no autorizado y la desinstalación de aplicaciones		X	
Protección de los datos de prueba de sistemas	Existe la política para evitar el uso de datos reales para las pruebas del sistema	X		Parcialmente Implementado. Falta la política para ofuscar las bases de datos de se utilizan en pruebas
Control de Acceso a las biblioteca de los fuentes de programas	Existe una política de transporte y manipulación de código fuente		X	
Procedimientos de Control de Cambios	Existe control e historial de cambio a las aplicaciones	X		Parcialmente Implementado. Hay que mejorar el historial de cambios

Tabla 13. (Continuación)

Lista de chequeo basado en Iso 27002				
Empresa: CEDIT – Universidad Francisco de Paula Santander Ocaña				
Responsable: Libardo Andrey Quintero González			Fecha: 27/10/2016	
Elemento auditado	CheckList	Cumple		Observaciones
		Si	No	
Revisión técnica de las aplicaciones luego de cambios en el Sistema Operativo	Se prueban las aplicaciones luego de realizarle cambios	X		Implementado
Restricciones en los cambios en paquetes de software	Existe una cláusula que permita hacer cambios a los paquetes	X		Parcialmente Implementado. Falta definir las aplicaciones que requieran cambios o ajustes
Fuga de Información	Existe una política sobre el uso no autorizado de la información		X	
Desarrollo de software por parte de terceros	Se tiene control sobre el desarrollo externo de software		X	
Control de vulnerabilidades técnicas	Existe un proceso de parcheo a las aplicaciones		X	
Reportes de eventos de seguridad de la información	Existen reportes automáticos de incidentes de seguridad		X	
Reportes de debilidades de seguridad	Se controlan y corrigen las debilidades encontradas	X		Parcialmente Implementado. Falta hacer registros de debilidades y mejoras aplicadas
Responsabilidades y Procedimientos	Existe un procedimiento formal en el cual debe de estar establecido las responsabilidades ante un incidente de seguridad de la información		X	
Aprendizaje a partir de incidentes de seguridad de la Información	Existen registros de incidentes de seguridad, con su respectivo informe.		X	
Recolección de evidencia	Esta especificada la custodia y el tratamiento de las evidencias de los incidentes de seguridad de la información		X	
Inclusión de la Seguridad de la Información en el proceso de gestión de continuidad de negocios	Existe una gestión para el desarrollo y el mantenimiento de la continuidad del negocio		X	
Continuidad de Negocios y Valuación de Riesgos	Existe un estudio de impacto y probabilidad para prevenirlo y asegurar la continuidad del negocio		X	

Tabla 13. (Continuación)

Lista de chequeo basado en Iso 27002				
Empresa: CEDIT – Universidad Francisco de Paula Santander Ocaña				
Responsable: Libardo Andrey Quintero González				Fecha: 27/10/2016
Elemento auditado	CheckList	Cumple		Observaciones
		Si	No	
Desarrollo e implementación de planes de continuidad que incluyan seguridad de la información	Existe un plan de mantenimiento y recuperación del negocio		X	
Marcos de trabajo para la planificación de continuidad de los negocios	Se cuenta con un esquema único de plan de continuidad		X	
Prueba, mantenimiento y revaluación de planes de continuidad de negocios	Se hace simulacro de los planes de continuidad del negocio		X	
Identificación de legislaciones aplicables	Se mantiene actualizada la empresa sobre las normas y leyes modificadas y existentes	X		Implementado
Derechos de Propiedad Intelectual	Se asegura el cumplimiento de las restricciones legales, reguladoras y contractuales sobre el uso del material protegido		X	
Protección de registros de la organización	Se protegen los registros importantes de la empresa		X	
Protección de datos y privacidad de la información personal	Se asegura los datos y la privacidad como lo requiere la legislación		X	
Prevención del mal uso de las facilidades de procesamiento de la información	Se controla sobre el mal uso de la información		X	
Regulación de controles criptográficos	Se hace uso de los controles criptográficos		X	
Conformidad con la política de seguridad	Se cumple correctamente los procedimientos de seguridad		X	
Chequeos de conformidad Técnica	Se comprueba regularmente la conformidad con las normas		X	
Controles de Auditoría de Sistemas de Información	Se planifican controles de auditoria		X	

Tabla 13. (Continuación)

Lista de chequeo basado en Iso 27002				
Empresa: CEDIT – Universidad Francisco de Paula Santander Ocaña				
Responsable: Libardo Andrey Quintero González			Fecha: 27/10/2016	
Elemento auditado	CheckList	Cumple		Observaciones
		Si	No	
Protección de herramientas de auditoría de sistemas de información	Se protege las herramientas de auditoria contra accesos no autorizados		X	

Fuente. El Autor.

14. CONCLUSIONES

Una vez culminada la etapa de análisis y evaluación de riesgos basado en la metodología planteada y siguiendo los métodos para construir un SGSI, se concluye que el CEDIT se encuentra en un riesgo Medio-Alto, pues aparte de todas las fortalezas que se encuentran en esta empresa y sus esfuerzos por tratar de organizar y asegurar la información que manejan y producen, no se tienen establecidas políticas, controles y mecanismos definidos, y con los que se cuenta actualmente no están bien planteados ni del todo completos, esto hace más difícil el proteger su activo más importante que es la información.

Se sugiere la contratación de personal especializado en seguridad informática que ayude a establecer mecanismos de control y gestión de la información, tales como manuales de usuario, políticas para salvaguardar la información y seguridad informática entre otras, basados en el inventario de activos hecho con su respectivo diagnóstico.

Por medio de la metodología aplicada de evaluación de riesgos, se logra proveer al CEDIT de un completo resumen de todo lo encontrado en el proceso realizado, en el cuál se evidencia y se define todas las vulnerabilidades y amenazas presentes en el momento, las cuales están indicadas y especificadas en el cuadro de amenazas.

Se plantearon los controles que se pueden aplicar en el CEDIT con el fin de minimizar las vulnerabilidades encontradas en el análisis y evaluación de los riesgos del sistema informático actual, estos controles deben ser puestos a consideración de la gerencia y directivos con el fin de determinar cuáles pueden ser implementados y establecidos de acuerdo a su opinión y presupuesto con el que se cuente.

15. INFORME Y RECOMENDACIONES

Luego de culminar con todas las etapas del presente proyecto se ve evidenciado que no se tiene un sistema establecido con el que se logre hacer un seguimiento a las actividades que se realizan a diario, a su vez un tratamiento de una incidencia que se pueda presentar, tampoco se tiene contemplado un plan de continuidad del negocio que permita la recuperación de la información y del negocio en caso de un grave incidente de seguridad y así poder continuar trabajando, el cual debe ser redactado y puesto en marcha para garantizar el buen funcionamiento en caso de una falla.

De igual manera en la red de datos no se aplican procesos para protegerla, cualquier persona puede conectarse a un punto de red y obtiene acceso a ella, esto se puede prevenir utilizando bloqueo por puerto en los switches, una opción de seguridad propia de los switches Cisco con los que se trabajan, así el puerto se bloquea al momento de detectar una MAC diferente a la que se tiene habitualmente conectada, en cuanto a los puntos de red que no se usan se deben apagar por medio de la configuración del Switch o desconectarlo físicamente. La red inalámbrica también es de fácil acceso, se debe implementar una mayor robustez a la clave para conectarse e implementar filtrado por MAC para garantizar que sólo los equipos permitidos se registren, el direccionamiento por DHCP no lo debe hacer los dispositivos que irradian sino un servidor DHCP instalado en el firewall que se maneje en la oficina; los dispositivos activos de red se encuentran a la vista y sus condiciones no son las más óptimas, estos deben estar protegidos en un cuarto de comunicaciones y con control de acceso.

No se tiene el control apropiado sobre los activos intangibles que se producen, a pesar que el material se genera y se publica en el CEDIT y allí queda toda la trazabilidad de cada proyecto y el producido final, cualquier persona puede llevarse esa información de manera abusiva o compartirla a través de la web, y este es uno de los puntos en los que más se falla, pues la inexistencias de muchos controles y mecanismos permiten que esto suceda, por ende se debe hacer uso del copyright e incluir un contrato donde se especifique que el CEDIT es el dueño del producido, que se firme en el momento en que se empiece a desarrollar cada proyecto.

Como opciones de mejora se propone definir controles de acceso y aseguramiento a la planta física, ya que en el momento la entrada es abierta a toda la comunidad y no se cuenta con registro de acceso del personal que concurre allí. Se puede implementar un sistema de registro de entrada con huella, donde sólo el personal autorizado tenga acceso a las partes de estricto control y donde se tenga cierto nivel de acceso, al hall de espera si pueden acceder todas las personas donde son atendidas por la secretaria general y ella controle el acceso a la sala donde se encuentran los equipos, registrando a cada una de las personas que ingresen, indicando el motivo y el tiempo que demore, en cada uno de estos puntos de control de acceso debe contar con vigilancia y monitoreo.

En temas de contratación de personal se debe ser más exhaustivo en las capacidades a nivel informático de las personas que ingresan a la empresa, pues hay poco personal especializado en las instalaciones, que actualmente no cuentan con personal de respaldo y en ausencia de ellos algunos procesos de detienen, incluyendo la resolución de algún problema que pueda surgir.

Las políticas de uso de los dispositivos de cómputo no están establecidas, el personal que accede y usa los equipos tiene completo control sobre ellos, permitiéndoles instalar y desinstalar software y manipular la configuración de los mismos, por lo que se debe evaluar y establecer la política de uso, mantenimiento y prevención de instalación de software, cambio de configuraciones y acceso al hardware de los equipos.

A nivel de políticas de seguridad no se cuentan con procedimientos de manejo de niveles de acceso que se otorgan a los usuarios y empleados, se evidenció que todos los equipos de cómputo poseen un usuario administrador en el que cualquiera puede entrar y hacer uso completo de las máquinas, ni un manejo adecuado de contraseñas, a los usuarios externos ni a los mismos empleados se les instruye en el uso de contraseñas adecuadas. Se propone implementar varios usuarios en los equipos donde se diferencie si es un usuario que puede tener acceso completo al equipo, como los empleados del CEDIT o si es un usuario que va a hacer uso limitado del equipo, al cual se le deben brindar solos los accesos que se necesiten sin alterar el buen funcionamiento del equipo o afectar el uso para otras personas.

En este documento se reflejó todo el listado de activos de la empresa, con sus respectivas valoraciones, se determinan todas las amenazas y las probabilidades de que estas se materialicen y el impacto que dicha materialización provocaría,

además se realiza la lista de controle que pueden ser aplicados de acuerdo a la norma ISO 27001.

Finalmente, aunque se cuenta con una red sólida y regida por estándares, el nivel de aseguramiento de los servidores y demás equipos importantes, no es la mejor a nivel físico y lógico, pues no se cuentan con controles y mecanismos sólidos y bien establecidos que aseguren y protejan estos equipos de accesos no autorizados, incluso de ataques informáticos, la información se encuentra expuesta, con un mínimo de conocimiento básica en seguridad informática se puede llegar a ella, vulnerando fácilmente algunos controles con los que se cuenta actualmente.

16. DIVULGACIÓN

Una vez concluidas las actividades planteadas en el presente proyecto se organizó una reunión ejecutiva con la alta dirección de la Universidad Francisco de Paula Santander Ocaña, donde se contó con el acompañamiento del director de la División de Investigación y Extensión y del director del Centro de Desarrollo e Innovación Tecnológica, en donde se presentaron los hallazgos encontrados como resultado del análisis y evaluación de riesgos en el CEDIT y se plantearon las correspondientes opciones de mejora.

Para empezar, se hizo una socialización en temas de auditoría donde se tocaron temas propios de dicha auditoría y se dio a conocer la falencia, que no se cuenta con un sistema establecido para el tratamiento de las incidencias presentadas y seguimiento de las actividades diarias, así mismo se dieron a conocer los resultados donde se evidencia que no se tiene el control apropiado sobre los activos intangibles que se producen.

Todos estos resultados obtenidos y presentados fueron expuestos a todas las personas que intervienen en el manejo del CEDIT, de esta manera se logró una concientización acerca de las amenazas y riesgos a los que se está expuesto en la actualidad y la necesidad de mejorar las falencias encontradas.

Con el fin de que todos los resultados y recomendaciones en el presente documento sean tenidos en cuenta, se les entregó una copia de todo el proceso hecho, se documentó y almacenó en el CEDIT, para que así, las directivas puedan tener base para solicitar a la alta gerencia la inversión y desarrollo del proyecto de mejora.

El presente proyecto será publicado en el repositorio para consulta de toda la comunidad educativa.

BIBLIOGRAFIA

- AGUILERA LÓPEZ, Purificación. Seguridad Informática. Primera Edición. Madrid - España: Editex S.A, 2010
- ARIAS, F. El proyecto de investigación; introducción a la metodología científica. 5ta Edición. Caracas: Editorial Espíteme, 2006
- ARIAS RUIZ DE SOMAVIA, RAMÓN; Análisis de Riesgos del Sistema de Información clasificado de Isdefe. Informe interno de la empresa, 2005.
- ÁVILA ARZUZA, M. (2012). Implantación de un SGSI. (Trabajo Final de Máster). Universidad Oberta de Catalunya. [Citado el 03 de Abril de 2016] Disponible en < http://openaccess.uoc.edu/webapps/o2/handle/10609/14743 Trabajo de grado para la implantación de un Sistema de Gestión de Seguridad de la Información en entorno real.
- BORGHELLO, C., (2001), Seguridad informática: sus implicancias e implementación. Trabajo de grado. Universidad tecnológica nacional de Argentina. [Citado el 07 de Abril de 2016] Disponible en < http://www.htmlweb.net/seguridad/tesis/tesis.html
- CRUZ MENDOZA, Erik Iván. RODRIGUEZ DUQUE, Diana Vanessa. Modelo de Seguridad para la Medición de Vulnerabilidades y reducción de Riesgos en Redes de Datos. México : Intitulo Politécnico Nacional UNIICSA, 2010
- DALTABUIT GODÁS, Enrique. HERNÁNDEZ AGUDELO, Leobardo. MALLÉN FULLERTON, Guillermo. VÁZQUEZ GÓMEZ, José de Jesús. La seguridad de la información. México: Limusa, 2007
- GONZÁLEZ BARROSO, J. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Libro I de la metodología Magerit ofrece los lineamientos necesarios en el Proceso de Gestión de Riesgos dentro de un marco de trabajo para administrar los riesgos derivados del uso de tecnologías de la información. Madrid: Ministerio de Hacienda y Administraciones Públicas, Libro I de la metodología Magerit ofrece los lineamientos necesarios en el Proceso de Gestión de Riesgos dentro de un marco de trabajo para administrar los riesgos derivados del uso de tecnologías de la información, 2010
- BENAVIDES ABAJO; J. M. OLAIZOLA BARTOLOMÉ; E. Rivero Cornelio. SQL: Para usuarios y programadores. Tercera Edición. Madrid: Paraninfo, 1997. ISBN:84-283-1821-2.
- RAMÍREZ, G. M. & Constain, G. E. Modelos y estándares de la seguridad Informática. Módulo de estudio de la Universidad Nacional Abierta y a

Distancia, hace referencia a los modelos y estándares aplicables dentro de la seguridad informática, 2012

- SABOGAL R., E. A. (2013) Proyecto de seguridad informática I. Módulo de estudio que presenta los lineamientos y recomendaciones para elaboración del anteproyecto y proyecto de grado requisito para optar por el título de especialistas en seguridad informático ofrecido por la UNAD, 2013
- Seguridad de la información en Colombia. Recurso digital en línea. [Citado el 07 de Abril de 2016] Disponible en < http://seguridadinformacioncolombia.blogspot.com.co/2010/02/marco-legal-de-seguridad-de-la.html
- STALLINGS William, Fundamentos de seguridad en redes aplicaciones y estándares, 2012
- SUMMERS, Rita C. Seguridad informática: Amenazas y Salvaguardias. México: McGraw-Hill Companies, 1996

ANEXOS

Anexo A. Resumen RAE

Título de Documento.	ANÁLISIS Y EVALUACIÓN DE RIESGOS EN EL CENTRO DE DESARROLLO E INNOVACIÓN TECNOLÓGICA – CEDIT DE LA UNIVERSIDAD FRANCISCO DE PAULA SANTANDER OCAÑA
Autor	QUINTERO GONZÁLEZ, Libardo Andrey
Palabras Claves	CEDIT, UFPSO, vulnerabilidad, amenaza, impacto, riesgo, Magerit, gestión, claves, servicios, checklist, activos, disponibilidad, ataque, personal, infraestructura, backup, supervisión, seguridad, control, ISO, funciones, red, teletrabajo, políticas, estándar, análisis, salvaguarda.
Descripción Este documento corresponde a un proyecto aplicado al CEDIT, una empresa local de la ciudad de Ocaña donde su principal fin fue realizar un análisis y evaluación de los riesgos existentes en dicha empresa, para ello se realizó el diagnóstico de los activos de información presentes en el CEDIT, se aplicaron las herramientas informáticas para así determinar las falencias existentes en los activos y determinar los riesgos a los que se estaba expuesto, se identificaron mecanismos de control y gestión que permitieron minimizar las vulnerabilidades encontradas en el análisis y evaluación de los riesgos del sistema informático del CEDIT y por último se elaboró un informe detallado en el cual se establecieron recomendaciones basadas en los hallazgos realizados, de tal manera que a partir de este se pueda definir un sistema de seguridad informático ajustado a las necesidades del CEDIT.	
Fuentes Bibliográficas	AGUILERA LÓPEZ, Purificación. Seguridad Informática. Primera Edición. Madrid - España: Editex S.A, 2010 ARIAS, F. El proyecto de investigación; introducción a la metodología científica. 5ta Edición. Caracas: Editorial Espíteme, 2006 ARIAS RUIZ DE SOMAVIA, RAMÓN; Análisis de Riesgos del

Sistema de Información clasificado de Isdefe. Informe interno de la empresa, 2005.

ÁVILA ARZUZA, M. (2012). Implantación de un SGSI. (Trabajo Final de Máster). Universidad Oberta de Catalunya. [Citado el 03 de Abril de 2016] Disponible en < http://openaccess.uoc.edu/webapps/o2/handle/10609/14743 Trabajo de grado para la implantación de un Sistema de Gestión de Seguridad de la Información en entorno real.

BORGHELLO, C., (2001), Seguridad informática: sus implicancias e implementación. Trabajo de grado. Universidad tecnológica nacional de Argentina. [Citado el 07 de Abril de 2016] Disponible en < http://www.htmlweb.net/seguridad/tesis/tesis.html

CRUZ MENDOZA, Erik Iván. RODRIGUEZ DUQUE, Diana Vanessa. Modelo de Seguridad para la Medición de Vulnerabilidades y reducción de Riesgos en Redes de Datos. México : Intitulo Politécnico Nacional UNIICSA, 2010

DALTABUIT GODÁS, Enrique. HERNÁNDEZ AGUDELO, Leobardo. MALLÉN FULLERTON, Guillermo. VÁZQUEZ GÓMEZ, José de Jesús. La seguridad de la información. México: Limusa, 2007

GONZÁLEZ BARROSO, J. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Libro I de la metodología Magerit ofrece los lineamientos necesarios en el Proceso de Gestión de Riesgos dentro de un marco de trabajo para administrar los riesgos derivados del uso de tecnologías de la información. Madrid: Ministerio de Hacienda y Administraciones Públicas, Libro I de la metodología Magerit ofrece los lineamientos necesarios en el Proceso de Gestión de Riesgos dentro de un marco de trabajo para administrar los riesgos derivados del uso de tecnologías de la información, 2010

BENAVIDES ABAJO; J. M. OLAIZOLA BARTOLOMÉ; E. Rivero Cornelio. SQL: Para usuarios y programadores. Tercera Edición. Madrid: Paraninfo, 1997. ISBN:84-283-1821-2.

RAMÍREZ, G. M. & Constain, G. E. Modelos y estándares de la seguridad Informática. Módulo de estudio de la Universidad Nacional Abierta y a Distancia, hace referencia a los modelos y estándares aplicables dentro de la seguridad informática, 2012

	SABOGAL R., E. A. (2013) Proyecto de seguridad informática I. Módulo de estudio que presenta los lineamientos y recomendaciones para elaboración del anteproyecto y proyecto de grado requisito para optar por el título de especialistas en seguridad informático ofrecido por la UNAD, 2013 Seguridad de la información en Colombia. Recurso digital en línea. [Citado el 07 de Abril de 2016] Disponible en <http://seguridadinformacioncolombia.blogspot.com.co/2010/02/marco-legal-de-seguridad-de-la.html STALLINGS William, Fundamentos de seguridad en redes aplicaciones y estándares, 2012

Contenido: El CEDIT no cuenta con una política que le permita establecer los mecanismos para salvaguardar la información y los recursos tecnológicos que tienen a su cargo, tampoco se cuenta con una metodología formalmente establecida con la que sus miembros entiendan y tengan claro los riesgos a los que exponen la información que generan. La pérdida o duplicidad de la información y el acceso de usuarios no autorizados a la información clasificada de los diferentes proyectos que se generan y gestionan dentro de la institución, son los problemas que se detectan y se pretenden corregir al realizar un análisis y evaluación de los riesgos existentes en el Centro de Desarrollo e Innovación Tecnológica – CEDIT, dependencia de la Universidad Francisco de Paula Santander Ocaña.

Se logra hacer un levantamiento del inventario de los activos presentes en el CEDIT y de acuerdo a la clasificación que se le da a cada uno, se identifican 58 activos principales, estos son: físicos, lógicos, de personal, de infraestructura e intangibles, correspondientes a activos esenciales, arquitectura del sistema, datos e información, claves criptográficas, servicios, aplicaciones, equipos informáticos, soportes de información, equipamiento auxiliar, instalaciones y personal, valorándolos de tal manera que cada uno puede ocasionar una falla grave de acuerdo a su importancia dentro de los procesos que se ejecutan a diario en el CEDIT, la ausencia de alguno de ellos puede convertirse en un fallo o interrupción del servicio, por lo cual se afirma la importancia de este proyecto.

Basándose en la metodología Magerit que a pesar de ser más extensa, ayuda a adaptar mejor las actividades a desarrollar en la empresa para lograr el fin deseado, a través de la aplicación de dicha metodología se logra recopilar la información necesaria y obtener resultados que permitieron identificar los riesgos y vulnerabilidades existentes, dentro de las que se destacan: indisponibilidad del personal, fugas de información, errores de monitorización, fallo de servicios de comunicaciones, pérdida de equipos, difusión de software dañino, manipulación de

la configuración de las estaciones de trabajo, caída del sistema por agotamiento de recursos, entre otros; con esta información se procede a definir los mecanismos de control y gestión que ayuden a la minimización de dichas amenazas, para ello se aplicó una lista de chequeo con el fin de identificar los controles existentes para posteriormente hacer un diagnóstico que permitiera definir el grado de cumplimiento de la política y de esa manera determinar nuevos controles.

Concluido todo el proceso descrito se celebra una reunión ejecutiva con la alta dirección de la Universidad Francisco de Paula Santander Ocaña, contando con la presencia de los directamente implicados en la dirección y supervisión del CEDIT, a los que se les presentan los hallazgos determinado con el análisis y evaluación de riesgos a ellos se les exponen y plantean las correspondientes opciones de mejora. Primeramente se les socializan temas de auditoria mostrándoles que no se tiene un sistema establecido para hacer seguimiento a la actividad diaria ni al momento de presentarse un incidente, tampoco se cuenta con un plan de continuidad del negocio que permita la recuperación en caso de un grave incidente de seguridad. Se les evidencia que en la red de datos no se aplican procesos para protegerla, cualquier persona puede conectarse a un punto de red y obtiene acceso a ella, la red inalámbrica también es de fácil acceso y los dispositivos activos de red se encuentran a la vista y sus condiciones no son las más óptimas. Así mismo se da a conocer los resultados donde se evidencia que no se tiene el control apropiado sobre los activos intangibles que se producen, a pesar que el material se genera y se publica en el CEDIT y allí queda toda la trazabilidad de cada proyecto y el producido final, cualquier persona puede llevarse esa información de manera abusiva o compartirla a través de la web, y este es uno de los puntos en los que más se falla, pues la falta de controles y mecanismos de protección permiten que esto suceda. Se encuentra también que no están establecidas las políticas de uso de los dispositivos de cómputo, el personal que hace uso de ellos puede hacer e instalar prácticamente lo que desee, por lo que se les recomienda establecer la política de uso, mantenimiento y prevención de instalación de software, cambio de configuraciones y acceso al hardware de los equipos. Al tratarse de políticas de seguridad se evidencia que no se cuenta con procedimientos de manejo de niveles de acceso que se otorgan a los usuarios y empleados, se evidenció que todos los equipos de cómputo poseen un usuario administrador en el que cualquiera puede entrar y hacer uso completo de las máquinas, no se da un manejo adecuado de contraseñas, ni a los usuarios externos ni a los mismos empleados se les instruye en el uso de contraseñas seguras.

Aunque se cuenta con una red sólida y regida por algunos estándares, el nivel de aseguramiento de los servidores y demás equipos importantes no es la mejor a nivel físico y lógico, pues no existen mecanismos solidos que ayuden a proteger estos equipos contra accesos no autorizados e incluso ataques informáticos, la información se encuentra expuesta, con un mínimo de conocimiento básico en seguridad informática se puede llegar a ella, vulnerando fácilmente algunos

controles con los que se cuenta actualmente.

Metodología

La metodología fue basada en una investigación descriptiva con enfoque cualitativo, se identificaron los riesgos de seguridad de la información, detectando situaciones en cada una de las unidades bajo las cuales se encuentra dividido el equipo de trabajo del CEDIT, se realizó una descripción exacta de las actividades, procesos y personas, extrayendo experiencias significativas que contribuyeron al conocimiento y evaluación de la seguridad de la información y la protección de los datos. El enfoque cualitativo para el análisis del riesgo permitió obtener un valor a partir de dos elementos fundamentales como la probabilidad de que se produzca un evento y el impacto que generaría si se llegara a presentar un evento.
Para el análisis de los riesgos en seguridad informática, se utilizó una metodología basada en Magerit que permitió analizar el sistema, identificar las amenazas y las vulnerabilidades asociadas a los procesos y activos de la organización.

Conclusiones

Se evidencia que en el momento el CEDIT es una empresa que ha dedicado tiempo y recurso de todo índole para fortalecerse y convertirse en una empresa sólida que aporta muchos beneficios a la comunidad en la que se encuentra, cuentan con una infraestructura tecnológica y física acorde a su carácter de Institución Pública de Educación Superior, brindan soluciones a nivel de tecnología que la comunidad no encuentra fácilmente e instruyen para que a través de estas herramientas se generen espacios de estudio y generación de productos informáticos. Se concluye que se encuentran en un riesgo Bajo debido a que no se tienen establecidas políticas, controles y mecanismos definidos para proteger su activo más importante.

Recomendaciones.

Se sugiere la contratación de personal especializado en seguridad informática que ayude a establecer mecanismos de control y gestión de la información, tales como manuales de usuario, políticas para salvaguardar la información y seguridad informática entre otras, a la vez se propone definir controles de acceso y aseguramiento a la planta física, ya que en el momento la entrada es abierta a toda la comunidad y no se cuenta con registro de acceso del personal que concurre allí. Supervisar y controlar de una mejor manera el acceso a los computadores, además de las áreas administrativas y de cuartos de sistemas que alojan los servidores. Ser más exhaustivo en las capacidades a nivel informático de las personas que ingresan a la empresa, pues hay poco personal especializado en las instalaciones, que actualmente no cuentan con personal de respaldo y en

ausencia de ellos algunos procesos de detienen, incluyendo la resolución de algún problema que pueda surgir.