IMPLEMENTACIÓN DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN – SGSI, EN EL PROCESO DE APOYO "GESTIÓN TECNOLÓGICA Y DE LA INFORMACIÓN" DEL INSTITUTO DISTRITAL PARA LA PROTECCIÓN DE LA NIÑEZ Y LA JUVENTUD – IDIPRON

ORALIA FRANCO GÓEZ

CARLOS ALBERTO CELIS MÉNDEZ

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA UNAD
ESPECIALIZACIÓN EN SEGURIDAD INFORMATICA
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA
BOGOTÁ
2016

IMPLEMENTACIÓN DEL SISTEMA DE GESTIÓN DESEGURIDAD DE LA INFORMACIÓN – SGSI, EN EL PROCESO DE APOYO "GESTIÓN TECNOLÓGICA Y DE LA INFORMACIÓN" DEL INSTITUTO DISTRITAL PARA LA PROTECCIÓN DE LA NIÑEZ Y LA JUVENTUD – IDIPRON

ORALIA FRANCO GÓEZ

CARLOS ALBERTO CELIS MÉNDEZ

Trabajo de grado presentado como requisito para optar al título de Especialista en Seguridad Informática

Director de Curso
Ing. SALOMON GONZALEZ

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA UNAD
ESPECIALIZACIÓN EN SEGURIDAD INFORMATICA
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA
BOGOTÁ
2016

Nota de Aceptación:

_____

_____

_____

_____

_____

_____

_____

Firma del Presidente del Jurado

_____

Firma del Jurado

_____

Firma del Jurado

Bogotá, 3 de Noviembre de 2016

CONTENIDO

pág.

LISTA DE TABLAS

pág.

LISTA DE FIGURAS

pág.

LISTA DE ANEXOS

pág.

1. DESCRIPCIÓN DEL PROBLEMA

1.1 PLANTEAMIENTO DEL PROBLEMA

El Instituto Distrital para la protección de la niñez y la juventud IDIPRON, con la finalidad de prestar de manera efectiva sus servicios sociales a la población más vulnerable del Distrito Capital ha venido incrementando su infraestructura tecnológica, lo que ha originado la necesidad de llevar un control adecuado de los activos tecnológicos que respaldan el procesamiento de la información en la entidad, con el fin de garantizar la disponibilidad, la integridad y la confidencialidad de la información que se procesa a diario.

Actualmente la entidad no cuenta con un análisis de valoración y gestión adecuada de los activos informáticos que llevan a cabo las operaciones diarias de la entidad, lo que origina que este expuesta a sufrir incidentes de seguridad, tales como: accesos no autorizados, pérdidas de información, denegaciones de servicio, problemas de trazabilidad de la información, entre otros.

Este hecho hace indispensable que se defina un Sistema de Gestión de Seguridad de la Información “SGSI” en el Área de Sistemas con el fin de garantizar la seguridad de la información y la preservación de los activos informáticos.

1.2 FORMULACIÓN DEL PROBLEMA

Cómo puede aportar este proyecto de análisis y valoración de riesgos a los activos informáticos del Instituto Distrital para la protección de la niñez y la juventud IDIPRON, para tomar acciones preventivas y correctivas que garanticen la seguridad de la información y permita reducir los riesgos y los tiempo de indisponibilidad de su información?

No existe un análisis y valoración de riesgos de los activos informáticos en el Instituto Distrital para la Protección de la Niñez y la Juventud – IDIPRON, para tomar acciones preventivas y correctivas que garanticen la seguridad de los activos informáticos y permita reducir los riesgos y los tiempo de indisponibilidad de su información.

2. INTRODUCCIÓN

El avance de las tecnologías de información y Comunicaciones (TIC) han favorecido el desarrollo y los procesos de nuevos modelos de gestión de negocios, sin embargo, de manera paralela también se abren posibilidades de amenazas internas y externas sobre los activos de información.

Por lo tanto, las empresas privadas como las públicas deben acoger mecanismos y estándares que permitan organizar de manera sincronizada y eficiente todos los procesos involucrados, cuya finalidad sea salvaguardar sus activos de información.

La seguridad de la información se constituye como un mecanismo que permite a través de estándares y metodologías, determinar las brechas de seguridad existentes, implementando acciones que logren identificar el grado de exposición, las amenazas que puedan afectar la organización y la definición de los controles necesarios para reducir los riesgos.

El éxito del proceso de seguridad de la información depende de una labor permanente, la cual se logra a través de la construcción de planes, estrategias, procedimientos, políticas y revisiones periódicas; cumpliendo con el ciclo PHVA (Planear, Hacer, Verificar y Actuar).[1]

A través del presente documento se desarrollará el diseño del Sistema de Seguridad de la Información - SGSI en el Proceso “Gestión Tecnológica y de la Información”.

Para el Instituto Distrital para la Protección de la Niñez y la Juventud – IDIPRON es necesario desarrollar e implementar el Sistema Integrado de Seguridad de la Información, el cual hace parte del Subsistema que conforma el Sistema Integrado de Gestión Distrital, con el fin de garantizar que los activos de información del Distrito sean íntegros, confiables y estén disponibles solo para el personal autorizado.

[1] Norma Técnica Colombiana NTC-ISO/IEC 27001

3. OBJETIVOS

3.1 GENERAL

Implementar el sistema de Gestión de Seguridad de la Información en el proceso de "Gestión Tecnológica y de la Información" en el Instituto Distrital para la Protección de la Niñez y la Juventud – IDIPRON, basados en la norma técnica colombiana GT-ISO/IEC 27003.

3.2 ESPECIFICOS

- Realizar el levantamiento de los activos de información del proceso de Gestión Tecnológica y de la Información de la entidad.

- Definir la metodología de evaluación, identificación y análisis de riesgos.

- Evaluar, aplicar y documentar los controles de seguridad de la información con la norma NTC-ISO/IEC 27002.

- Definir el plan de tratamiento de riesgos y el sistema de control interno informático.

4. MARCO REFERENCIAL

4.1 ANTECEDENTES

Con la finalidad de realizar el diseño para la implementación del sistema de gestión de seguridad de la información, fueron consultados los siguientes estudios y proyectos:

Consultoría de Infraestructura, Gestión de Tecnología y de la Seguridad de las Tic de lDIPRON. Fue elaborada por la firma "NewNet S.A" se realizó un proceso público por Concurso de Méritos en el año 2009; el trabajo presentado fue la realización del diagnóstico de la situación actual de la infraestructura de TI (red, backup, impresión, servidores, centro de cómputo), y la propuesta de implementación de dicha infraestructura en 22 sedes del IDIPRON, además la propuesta para la realización del centro de cómputo en la entidad.

Se realizó el inventario, análisis y valoración de riesgos de los activos del instituto existentes en dicha fecha, al igual que el análisis de vulnerabilidades de tres servidores y tres servicios existentes, se realizó el test de intrusión con pruebas de éthica hacking interna y externa para dichos servicios, se definió la arquitectura de seguridad de la entidad y el árbol de ITIL de acuerdo a dos áreas de sistemas existentes y los servicios que se realizaban en cada una de ellas.

Proyecto de grado Diseño de un Sistema de Gestión de la Seguridad Informática – SGSI – para empresas del área textil en las ciudades de Itagüí, Medellín y Bogotá D.C. a través de la Auditoria. Presentada en la Escuela de Ciencias Básicas Tecnología e Ingeniera de la Universidad nacional Abierta y a Distancia – UNAD-. Realizado por los ingenieros Alexander Guzmán García y Carlos Alberto Taborda Bedoya, como requisito para optar el título de Especialista en Seguridad Informática.

Este proyecto diseño cada una de las actividades y etapas que deben desarrollarse en el marco de la auditoria de Seguridad Informática de acuerdo a la naturaleza de dichas empresas, en el marco de la norma ISO/IEC 27001:2013.

El proyecto de Grado Análisis y Gestión del Riesgo de la Información en los Sistemas de Información Misionales de una Entidad del Estado, enfocado en un Sistema de Seguridad de la Información. Presentada en la Escuela de Ciencias Básicas Tecnología e Ingeniera de la Universidad nacional Abierta y a Distancia – UNAD-. Realizado por Hina Luz Garavito Robles, como requisito para optar el título de Especialista en Seguridad Informática.

A través de este proyecto se realizó la valoración de activos, se definieron y estudiaron los riesgos, se definieron las amenazas y se propusieron las recomendaciones, medidas y controles a implementarse en el marco del Sistema Misional de la entidad, de acuerdo a la norma ISO/IEC 27001 y la herramienta Pilar basada en la metodología MAGERIT.

4.2 MARCO CONTEXTUAL

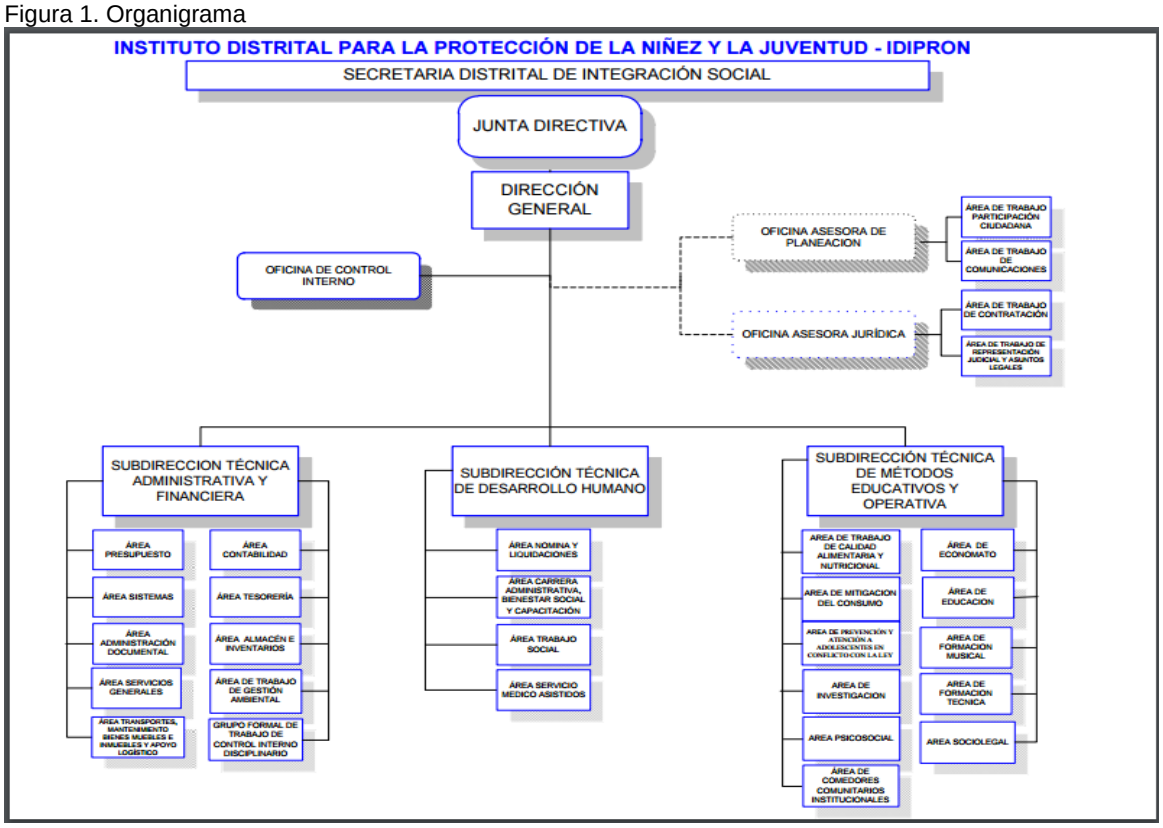
El Instituto Distrital para la Protección de la Niñez y la Juventud, es una Entidad de naturaleza pública descentralizada, con personería jurídica y autonomía administrativa. Creada mediante el Acuerdo No. 80 de 1967 del Concejo de Bogotá y que funciona desde 1970. Con la expedición del Acuerdo 257 de 2006 sobre reforma administrativa, el IDIPRON conforma con la SDIS, el Sector de Integración Social [2] de la alcaldía Mayor de Bogotá.

La misión del IDIPRON busca promover la restitución del goce efectivo de derechos de niños, niñas, adolescentes y jóvenes – NNAJ en edades comprendidas de 8 a 28 años en alto grado de vulnerabilidad social, mediante un proyecto pedagógico.

Dentro de los objetivos estratégicos de la entidad se encuentra el fortalecimiento institucional a través de las Tics con el fin de mejorar de manera integral la gestión de las capacidades administrativa del IDIPRON, para que entre otros aspectos dar cumplimiento a su objeto social.

[2] IDIPRON. ¿Quiénes somos? Disponible en: http://www.idipron.gov.co/index.php/idipron/quienes-somos

Figura 1. Organigrama



Fuente: http://www.idipron.gov.co/images/extras/docs/organigrama2014_2.pdf

El área de sistemas de la Entidad no cuenta con una estructura organizacional aprobada al interior de acuerdo a sus funciones sin embargo esta área soporta en el Sistema Integrado de Gestión de calidad el Proceso de Gestión Tecnológica y de la Información y realiza todas las operaciones tecnológicas de la entidad desarrollando actividades como: Desarrollo de software misional, soporte de sistemas de información, administración e instalación de cableado estructurado, administración de redes (servidores, switches, firewall, administración de red mpls y canal de internet, conexiones con entes distritales), administración de copias y manejo de respaldo, soporte técnico a equipos clientes, administración de mesa de ayuda.

Aunque el Área de Sistemas posee la administración de políticas, servidores y conexiones, la página web institucional es desarrollada y administrada por el Área de Comunicaciones, el portal misional “Académico” es desarrollado y administrado por el componente pedagógico “Colegio del IDIPRON” y el sistema para el registro de la población beneficiaria SIMI es administrado por la Oficina Asesora de Planeación, sin embargo el desarrollo, manejo de base de datos y servidores, conectividad y backup es realizada por el Área de Sistemas.

4.2.1 Funciones del Área de Sistemas

El área de sistemas posee las siguientes funciones aprobadas mediante resoluciones 164 de 2001 y 254 de 2001.

- Desarrollar estudios técnicos y efectuar las diligencias necesarias para la adquisición de nuevas tecnologías en comunicaciones, equipos de cómputo y procesamiento de datos, elementos de informática y sistemas, acordes con las políticas trazadas por el Instituto.
- Desarrollar métodos y procedimientos en coordinación con las dependencias respectivas, sobre la necesidad de información sistematizada y velar por su implementación conforme a las disposiciones legales y políticas del Instituto para el logro de las metas y objetivos propuestos por la entidad.
- Generar y optimizar nuevos productos y/o servicios, para facilitar las actividades y tareas de las diferentes dependencias.
- Diseñar y coordinar con el Instituto los mecanismos de control y seguridad para diferentes tipos de software adquiridos por el IDIPRON.
- Administrar el mantenimiento preventivo y correctivo de hardware y software de propiedad del Instituto.
- Formular e implementar el plan de informática del Instituto.
- Coordinar planes de capacitación para el óptimo funcionamiento de los recursos informáticos de la entidad.
- Brindar soporte técnico a los servidores públicos que prestan sus servicios en las diferentes dependencias y unidades educativas del Instituto.
- Coordinar la entrega de insumos y bienes.

4.2.2 Cargos y funciones del Personal del Área de Sistemas

El Área de Sistemas está conformada por cargos de planta permanente, planta temporal y contratistas, así:

- Profesional Universitario Código 219 Grado 10

Rol: Responsable Área de Sistemas

1. Administrar el desarrollo de cada uno de los macro componentes del Proyecto de inversión 640 en sus líneas
2. Definir las estrategias de acción e intervención que desde los componentes administrativo y social deben acompañar la ejecución de los diferentes convenios interadministrativos, de asociación y cooperación suscritos en el marco del Proyecto de inversión 640.

3. Preparar para la entidad los diferentes informes de gestión y la información de tipo administrativo y financiero que se produzca en desarrollo de los diferentes macro componentes del Proyecto.
4. Ejercer la supervisión o apoyo a la supervisión de los contratos y/o convenios en los que sea designado.
5. Realizar las demás funciones asignadas por la autoridad competente, de acuerdo con el nivel, la naturaleza y el área de desempeño del cargo.[3]

- Profesional Universitario Código 219 Grado 07

Este profesional, actualmente tiene el rol de realizar el estudio previo para las adquisiciones de bienes y servicios del Área de Sistemas, conceptos técnicos y sistema integrado de gestión del proceso.

1. Asesorar y colaborar con las distintas dependencias en la toma de decisiones del área de sistemas relacionadas con las necesidades informáticas de IDIPRON.
2. Aplicar conocimientos, principios y técnicas de su disciplina académica para generar nuevos productos y/o servicios, optimizar los existentes y desarrollar métodos y procedimientos conforme a las disposiciones legales y políticas de IDIPRON para el logro de metas y objetivos propuestos por el Instituto.
3. Estudiar, proponer y dirigir la implantación de nuevas tecnologías para el desarrollo de sistemas de información. 4. Efectuar pruebas de aplicaciones y de los programas correspondientes a fin de comprobar su funcionamiento y aplicabilidad.
5. Estudiar la aplicación de lenguajes apropiados en cada proyecto y determinar su adaptación a las nuevas necesidades o técnicas modernas.
6. Proponer las políticas y controles para llevar a cabo una adecuada auditoria de sistemas.
7. Dirigir el mantenimiento preventivo y correctivo al sistema operacional, bases de datos y redes de información. 8. Analizar y liderar en forma permanente la actualización y orientación tecnológica del Instituto de acuerdo a los últimos avances y nuevos requerimientos en Informática. 9. Colaborar en el análisis de la eficiencia en el diseño de bases de datos y programas.
10. Entregar los informes que le sean requeridos por las diferentes entidades.
11. Colaborar con la Subdirección Administrativa y Financiera en el establecimiento de nuevas políticas para el diseño, pruebas y optimización de programas.
12. Las demás funciones que le sean asignadas por el jefe inmediato de acuerdo a la naturaleza del cargo.[4]

[3] Resolución 013 de 2013 "Instituto distrital para la Protección de la Niñez y la Juventud"
[4] Resolución 038 de 2006

- Profesional Universitario Código 219 Grado 01

Rol: Administrador de servidores físicos y virtualizados (directorio activo, de impresión, dominio principal, dominio misional, redes).

1. Dar concepto de viabilidad sobre la disponibilidad de la infraestructura de hardware y software del IDIPRON (corriente regulada)
2. Realizar actividades de instalación de los sistemas operativos de servidores y estaciones de trabajo
3. Evaluar y poner en funcionamiento servicios de internet.
4. Aplicar políticas de seguridad a los sistema de información del IDIPRON
5. Realizar las demás funciones asignadas por la autoridad competente, de acuerdo con el nivel, la naturaleza y el área de desempeño del cargo.

- Técnico Operativo Código 314 Grado 03

Este profesional tiene el rol de realizar soporte técnico, manejo de la consola de antivirus y políticas y seguimiento del mismo.

1. Realizar actividades de carácter tecnológico y técnico, con base en la aplicación de los fundamentos que sustentan su especialidad.
2. Conocer y manejar correctamente las herramientas básicas de los microcomputadores, tales como el sistema operacional, hojas electrónicas, procesador de palabra y otras utilidades.
3. Procesar programas sistematizados.
4. Responder por el correcto estado de funcionamiento y utilización de los equipos y accesorios asignados para el desarrollo de las funciones.
5. Borrar archivos que no tengan vida útil, previa autorización del Jefe Inmediato.
6. Instalar, reparar y responder por el mantenimiento de los equipos e instrumentos del área respectiva y efectuar los controles periódicos de acuerdo con instrucciones recibidas.
7. Producir el material gráfico tales como libros, plegables, afiches,
8. Las demás funciones asignadas por el Jefe inmediato de acuerdo con la naturaleza de cargo.

- Técnico Operativo Código 314 Grado 03 (2 cargos)

Estos cargos son ocupados por dos funcionarios con roles distintos.

Rol 1: Administrador del servidor y software de mesa de ayuda – Aranda, Monitoreo de antivirus, seguimiento del software de Dataprotector, manejo y tratamiento de copias de respaldo y soporte técnico a computadores.

Rol 2: Administrador del inventario de bienes, seguimiento a software y medios de los mismos, soporte técnico a computadores.

1. Realizar actividades de carácter tecnológico y técnico, con base en la aplicación de los fundamentos que sustentan su especialidad.
2. Conocer y manejar correctamente las herramientas básicas de los microcomputadores, tales como el sistema operacional, hojas electrónicas, procesador de palabra y otras utilidades.
3. Elaborar y apropiar estrategias informáticas para solucionar inconvenientes relacionados con el uso de herramientas tecnológicas.
4. Mantener en óptimas condiciones los recursos informáticos de las Unidades Educativas, contribuyendo al buen desempeño de las mismas.
5. Elaborar y velar por el cumplimiento del Plan de Estudios relacionados con el área de informática en las diferentes Unidades Educativas.
6. Participar en la elaboración del plan de compras, relacionado con los talleres de Sistemas.
7. Evaluar herramientas informáticas que puedan ser aplicados en los diferentes Talleres de las Unidades Educativas.
8. Las demás funciones asignadas por el Jefe inmediato de acuerdo con la naturaleza de cargo.

- Técnico Administrativo Código 367 Grado 01 (2 cargos*)*

Rol 1: Desarrollo y soporte de aplicaciones y sistemas de información, Administrador de base de datos (Oracle, SQL), administrador de firewall, configuración y direccionamiento de canales con entes.

Rol 2: Desarrollo y soporte de aplicaciones, administrador de correo institucional bajo plataforma en software libre.

1. Configurar la red del área local.
2. Realizar diagnóstico sobre la infraestructura de redes concurrencia, acceso para la modelación de las nuevas aplicaciones.
3. Estudiar el prototipo de lenguaje de programación, bases de datos, procedimientos de respaldo y recuperación de la información.
4. Desarrollar nuevas aplicaciones y el mejorar las existentes.
5. Documentar los procedimientos de tecnología de acuerdo con el cambio normativo específico
6. Realizar las demás funciones asignadas por la autoridad competente, de acuerdo con el nivel, la naturaleza y el área de desempeño del cargo. [5]

[5] Resolución 013 de 2013.

- Técnico Operativo Código 314 Grado 01 (2 cargos)

Rol1: Coordinador de soporte técnico de equipos y red de sedes misionales.

Rol2: Coordinador y soporte técnico de impresoras.

1. Realizar mantenimiento preventivo y correctivo de los equipos del IDIPRON
2. Dar soporte a los sistema operativos de las estaciones de trabajo
3. Dar soporte de ofimática a los usuarios del IDIPRON
4. Configurar elementos activos de la red, y conexiones inalámbricas del IDIPRON así como las respectivas estaciones trabajo.
5. Realizar las demás que le sean asignadas en el cumplimiento de los Proyectos y los objetivos del área de desempeño del cargo.[6]

- Auxiliar Administrativo Código 407 Grado 01

1. Realizar actividades de apoyo administrativo o complementario de las tareas propias de los niveles superiores.
2. Recibir, revisar y radicar documentos asignados.
3. Responder ante su superior inmediato por el recibo, radicación y entrega de correspondencia con eficacia y celeridad, así como, de las otras tareas encomendadas.
4. Responder por la actualización y manejo del archivo asignado conforme a las instrucciones recibidas.
5. Llevar y mantener actualizado registros de carácter técnico, administrativo o financiero, verificar la exactitud de los mismos y presentar los informes correspondientes.
6. Realizar las demás que le asigne el Jefe Inmediato, de acuerdo con la naturaleza del cargo.[7]

4.3 MARCO CONCEPTUAL

4.3.1 Amenaza. Es la probabilidad de ocurrencia de un imprevisto que puede ser de origen natural o intencionado; las amenazas representan factores de riesgos externos que pueden explotar una vulnerabilidad existente en la Entidad.

4.3.2 Ciclo PHVA. Es una herramienta que permite implementar y gestionar a través del ciclo de mejora continua (Planear, hacer, verificar y actuar) la implementación de sistemas de gestión de calidad.

[6] Resolución 013 de 2013
[7] Resolución 013 de 2013

4.3.3 Confidencialidad. Propiedad de la seguridad de la información que garantiza que información sea accedida solo por las personas autorizadas.

4.3.4 Disponibilidad. Propiedad de la seguridad de la información que garantiza que la información esté disponible y pueda ser accedida por las personas autorizadas en el momento que ellas lo requieran.

4.3.5 Impacto. Son las consecuencias o pérdidas que pueden ocurrir la materialización de un amenaza o la explotación de una vulnerabilidad; el impacto puede afectar las aspectos financieros, tecnológicos, físicas, de imagen o aspectos legales de la entidad.

4.3.6 Integridad. Propiedad que garantiza que la información no ha sido alterada, modificada por personas no autorizadas para hacerlo.

4.3.7 Riesgo. Es la magnitud de pérdidas proyectadas tras la ocurrencia de explotación de una amenaza o vulnerabilidad.

4.3.8 Seguridad Informática. Consiste en los procedimientos, políticas, técnicas y herramientas de hardware y software implementadas con el fin de proteger los sistemas informáticos y la información.

4.3.9 Valoración de riesgos. Proceso que permite la identificación, análisis y administración de los riesgos que internos y externos que posee una organización.

4.3.10 Vulnerabilidad. Es un factor de riesgo interno que representa las debilidades o el grado de exposición de los activos informáticos de la entidad, lo cual facilita la explotación de una amenaza.

4.4 MARCO TEÓRICO

4.4.1 Activos de Información. Se define como activos de información a todos los elementos de hardware, software, datos, servicios y recurso humano que hacen parte del procesamiento y tratamiento de la información. [8]

4.4.2 Clasificación de activos de información. Es el proceso mediante el cual se determina la criticidad de los activos informáticos los cuales son relevantes para las organizaciones, medición que se realiza con el responsable o dueño del activo.

Un activo de información es aquel elemento que contiene o manipula información. Por ejemplo: Servidores, Bases de datos, personal, software, aplicativos, equipos de cómputo, documentos, etc.

4.4.3 Gestión de Riesgos. Es el mecanismo que permite a las organizaciones analizar, evaluar y planificar los eventos que pueden ocasionar un desastre al interior, eventos que pueden ser externos o internos y cuyos orígenes pueden ser intencionales o no intencionales.

El resultado exitoso del proceso de gestión del riesgo, parte de la utilización de la herramienta que permita de manera sistemática realizar el procedimiento ideal con el fin de determinar el impacto que puede afectar el activo de TI; al mismo tiempo definir el plan de tratamiento de riesgos el cual permita administrar sus riesgos de manera adecuada permitiendo disminuir costos en la aceptación, transferencia, mitigación o reducción de los mismos.

4.4.4 Inventario de activos de información. Son todos los elementos que posee una organización, que se utilizan para el procesamiento de sus datos.

4.4.5 Magerit Versión 3.0. Es una metodología de análisis y gestión de riesgos de los Sistemas de Información elaborada por el Consejo Superior de Administración Electrónica para minimizar los riesgos de la implantación y uso de las Tecnologías de la Información, enfocada a las Administraciones Públicas. [9]

---

[8] Décimo primer lineamiento – Alcaldía Mayor de Bogotá. Disponible en: http://secretariageneralalcaldiamayor.gov.co/sites/default/files/lineamiento_11_inventario_de_activos_de_informacion.pdf

[9] Metodología MAGERIT. Enciclopedia Wikipedia. Disponible en: https://es.wikipedia.org/wiki/MAGERIT_(metodolog%C3%ADa)

La metodología Magerit se constituye como la herramienta que permite administrar de manera eficiente los activos informáticos, iniciando con el levantamiento adecuado de los activos, su valoración y sugiriendo salvaguardas que evaluadas e implementadas puedan garantizar el control adecuado de los riesgos establecidos; lo cual se realizará mediante la concientización a los responsables de los activos, de la definición y valoración sistemática de los riesgos asociados a éstos, siendo partícipes en la definición del plan de mejora y en hacer seguimiento al mismo.

Esta metodología de manera estructurada y organizada permite realizar e implementar el Proceso de Gestión de Riesgos, cuya finalidad es realizar y mantener el plan de tratamiento de riesgos.

4.4.6 Necesidad de la Seguridad de la Información. La seguridad de la información es necesaria de ser implementada en una organización para garantizar o mantener la disponibilidad, la integridad y la confidencialidad de la información.

4.4.7 Norma Técnica Colombiana NTC-ISO/IEC 27001. Esta norma Colombiana, se fundamenta en un estándar internacional que explica la forma de cómo se debe promover la seguridad de la información en una organización, ya que establece una metodología mediante el ciclo PHVA – planear, hacer, verificar y actuar con el fin de implementar y mantener el Sistema de Gestión de Seguridad de la Información.

4.4.8 Guía Técnica Colombiana GTC-ISO/IEC 27002. Es la Guía Técnica Colombiana que establece de manera detallada los controles de seguridad contenidos en la norma NTC-ISO/IEC 27001:2013 que deben aplicarse con el fin de implementar de manera adecuada el Sistema de Gestión de Seguridad de la Información.

La Guía técnica GTC-ISO/IEC 27002:2013, la cual es la última actualización existente se estructura en: 14 dominios, 35 objetivos y 114 controles.

4.4.9 Guía Técnica Colombiana GTC-ISO/IEC 27003. Es la Guía de implementación para llevar a cabo el Sistema de Gestión de la Seguridad de la información, en la cual se establece las fases que deben desarrollarse para definir el proyecto a realizar, el diseño y la implementación del SGSI, de acuerdo y en concordancia con la norma ISO/IEC 27001.

La estructura general para la implementación del SGSI se desarrolla en cinco fases así:

- Obtener la aprobación de la dirección para iniciar el proyecto de SGSI
- Definir el alcance y la política del SGSI

- Realizar el análisis de la organización
- Llevar a cabo la evaluación de riesgos y el plan de tratamiento de riesgos.
- Diseñar el SGSI[10]

4.4.10 Punto de partida para la seguridad de la información. La valoración de los controles de seguridad puede ser considerado como el inicio para la implementación de un sistema de seguridad de la información ya que dichos controles se constituyen sobre una guía que se fundamenta sobre requisitos legales, regulatorios, imprescindibles o de mejores prácticas que deben tenerse en cuenta con el fin de:

a) Proteger los datos y la información
b) Proteger los registros de la organización
c) Cumplir y administrar los derechos de propiedad intelectual. [11]

4.4.11 Seguridad de la Información. Son las medidas correctivas y preventivas que permiten el manejo adecuado de la información con el fin de protegerla cumpliendo con los principios de disponibilidad, integridad, confidencialidad, autenticidad y no repudio.

La Seguridad de la información permite identificar y valorar los riesgos a que puede estar expuestos los activos de información y a definir de manera preventiva el acceso, uso, tratamiento de la misma, al igual que tomar acciones correctivas que van desde la retroalimentación de la propia política o en la evaluación de aspectos y amenazas propias de los acontecimiento ocurridos o de la reglamentación vigente.

La información y los activos de información están expuestos a una gran cantidad de amenazas que pueden ser explotadas por las vulnerabilidades que se presentan al interior de la entidad. Cualquiera que sea la forma en que se presenta, almacena, comparte la información debe tener la protección y tratamiento adecuado.

"La seguridad de la información se logra mediante la implementación de un conjunto adecuado de controles, incluidas las políticas, procesos, procedimientos, estructuras organizacionales y las funciones del software y del hardware. Para esto,

[10] Instituto Colombiano de Normas Técnicas y Certificación – ICONTEC. GTC-ISO/IEC 27003. Técnicas de seguridad. Guía de implementación de un sistema de gestión de seguridad de la información. Bogotá. 2012. p.2

[11] Instituto Colombiano de Normas Técnicas y Certificación – ICONTEC. GTC-ISO/IEC 27002:2013. Código de práctica para Controles de Seguridad de la Información. Bogotá. 2015. p.107

es necesario establecer, implementar, hacer seguimiento, revisar y mejorar estos controles." [12]

4.4.12 Seguridad Informática. Se refiere a la protección de las infraestructuras de las tecnologías de la información y comunicación que soportan una organización.

4.4.13 Sistema de Gestión de la Seguridad de la Información – SGSI. Un SGSI es una metodología de gestión relacionada con la seguridad de la información. Siendo de vital importancia en cualquier organización. "Un SGSI implica crear un plan de diseño, implementación, y mantenimiento de una serie de procesos que permitan gestionar de manera eficiente la información, para asegurar la integridad, confidencialidad y disponibilidad de la información".[13]

Un SGSI comprende: procedimientos, políticas, estructura organizativa, procesos, recursos necesarios documentados y conocidos por toda la empresa, con el fin de proteger la información, que es el recurso más valioso de la organización.

La implementación de un SGSI nos permite conocer, gestionar y minimizar los posibles riesgos que atenten contra la seguridad de la información.

A través de esta metodología se puede: analizar y ordenar la estructura de los sistemas de información, definir procedimientos y controles que permitan mantener su seguridad.

4.4.14 Sistema Integrado de Gestión del Instituto Distrital para la Protección de la Niñez y la Juventud – SIGID. Es la herramienta que permite el mejoramiento de la entidad para realizar las actividades de protección, restitución y promoción del goce efectivo de derechos de Niñas, Niños, Adolescentes y Jóvenes de Bogotá en alto grado de vulnerabilidad social, a través de los subsistemas de Gestión de Calidad, de control interno, de gestión ambiental, de gestión de seguridad de la información, de responsabilidad social, de gestión documental y archivo y de seguridad y salud ocupacional. [14]

---

[12] Guía Técnica Colombiana GTC-ISO/IEC 27002. Código de Práctica para controles de seguridad de la información. Pág. i.

[13] Welivesecurity. La importancia de un SGSI. Recuperado 15 de marzo de 2016. Disponible en: http://www.welivesecurity.com/la-es/2010/09/10/la-importancia-de-un-sgsi/

[14] Manual Sistema Integrado de Gestión. Disponible en: http://www.idipron.gov.co/complementos/intranet/index.php/centro-de-documentacion/category/49-manuales

4.5 MARCO LEGAL

4.5.1 Resolución 305 de 2008. Por la cual se expiden políticas públicas para las entidades, organismos y órganos de control del Distrito Capital, en materia de Tecnologías de la Información y Comunicaciones respecto a la planeación, seguridad, democratización, calidad, racionalización del gasto, conectividad, infraestructura de Datos Espaciales y Software Libre.[15]

4.5.2 Decreto 2573 de 2014. "Por el cual se establecen los lineamientos generales de la Estrategia de Gobierno en línea, se reglamenta parcialmente la Ley 1341 de 2009 y se dictan otras disposiciones".

Define los lineamientos, instrumentos y plazos de la estrategia de Gobierno en Línea para garantizar el máximo aprovechamiento de las Tecnologías de la Información y las Comunicaciones, con el fin de contribuir con la construcción de un Estado abierto, más eficiente, más transparente y más participativo y que preste mejores servicios con la colaboración de toda la sociedad.[16]

4.5.3 Norma Técnica Distrital del Sistema Integrado de Gestión para las entidades y organismos distritales – Sistema Integrado de Gestión Distrital – Decreto 652 del 28 de diciembre de 2011. Por medio del cual se adopta la Norma Técnica Distrital del Sistema Integrado de Gestión para las Entidades y Organismos Distritales.

Determina las generalidades y los requisitos mínimos para establecer, documentar, implementar y mantener un Sistema Integrado de Gestión en las entidades y organismos distritales y agentes obligados.[17]

4.5.4 Ley 1273 de 2009, con la que se modifica el código penal, se crea un nuevo bien jurídico 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. [18]

---

[15] Secretaría General Alcaldía Mayor de Bogotá D.C. - Comisión Distrital de Sistemas – CDS. Recuperado 25 de octubre de 2015. Disponible en: http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=33486

[16] Ministerio de Tecnologías de la Información y las Comunicaciones. Decreto 2573 de 2014. Recuperado 25 de octubre de 2015. Disponible en: http://tic.bogota.gov.co/images/boletines/DECRETO-2573-DEL-12-DE-DICIEMBRE-DE-2014-1.pdf

[17] Alcaldía Mayor de Bogotá. Norma Técnica Distrital del sistema integrado de gestión para las entidades y organismos distritales. Bogotá. 2011. P. 60

[18] Congreso de Colombia. Ley 1273 de 2009. Disponible en: http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=34492

Esta ley la componen dos capítulos, el primero hace referencia a conductas delictivas que quebrantan la confidencialidad, la integridad y la disponibilidad de los datos y de los sistemas informáticos. El segundo capítulo hace referencia a los atentados informáticos y otras infracciones. Cada uno de las conductas delictivas enunciadas en los artículos de esta ley, incurren en pena de prisión y multas económicas. Se destacan todos los artículos de esta norma.

5. MARCO METODOLÓGICO

5.1 METODOLOGÍA DE INVESTIGACIÓN

Este proyecto de investigación se adelantará mediante la fase de la investigación cualitativa y cuantitativa, tomando como base la Norma Técnica Colombiana NTC-ISO/IEC 27001 en concordancia con la Norma NTC-ISO/IEC 27003.

Para realizar el análisis y diseño detallado del SGSI en el IDIPRON se desarrollarán las actividades para su implementación, basándose en el ciclo PHVA (Planear, Hacer, Verificar y Actuar).

5.1.1 Población y Muestra. El análisis será realizado en el IDIPRON, y se tomará como muestra la totalidad de los activos informáticos, cuya responsabilidad y manejo recae dentro del proceso de “Gestión Tecnológica y de la Información” del Instituto Distrital para la Protección de la Niñez y la Juventud.

5.1.2 Recolección y Fuentes de Información. El tipo de información que se recolectará, se basará en aspectos generales, de gestión, de ubicación, de propiedad, de acceso, de clasificación y de criticidad, por cada uno de los activos de información inmersos en el proceso de “Gestión tecnológica y de la información”. Estos pueden ser de diversos tipos: datos o información, servicios, software, hardware, redes de comunicaciones, instalaciones, personal, etc.

Se tendrán en cuenta las siguientes fuentes de información: personal responsable del manejo de cada uno de los activos de información, responsable de área, documentos, procedimientos, observaciones, instalaciones, manuales, material multimedia, etc.

5.1.3 Técnicas e instrumentos para recolección. Las técnicas e instrumentos para recolección de datos son tanto cuantitativos y cualitativos: para llevar a cabo la recolección de datos se emplearán las siguientes técnicas: entrevistas estructurada y no estructurada, observación simple y análisis de documentos.

5.1.4 Procesamiento de la información. El procesamiento de la información para la implementación del SGSI en el IDIPRON, inicia con la recolección de la información para luego ser agrupada y analizada. Posteriormente la información se tabulará, con el fin de organizarla y valorarla, tendiente a obtener datos estadísticos,

tablas dinámicas y gráficas que permitan realizar un adecuado análisis de la información.

5.1.5 Análisis de datos. La información recolectada, se analizará teniendo como ayudas tanto la parte numérica como gráfica, basándonos en las técnicas de recolección tanto cuantitativas como cualitativas, esto nos permitirá de manera más comprensible e inteligible la toma de decisiones. Para realizar dicho análisis, se emplearán hojas de cálculo con celdas formuladas, tablas dinámicas, gráficas, entre otros.

5.2 METODOLOGÍA DE DESARROLLO

Para el desarrollo del presente proyecto se tendrá en cuenta la metodología MAGERIT v.3, que permitirá realizar el análisis y evaluación de riesgo de los activos de información, en concordancia con la norma técnica colombiana NTC-ISO/IEC 27001:2013 utilizando el ciclo PHVA (Planear, hacer, verificar y actuar). El cual consta de las siguientes etapas:

5.2.1 Fase 1 – Planeación. Se realizará el análisis del estado actual del SGSI en la entidad a través del análisis diferencial, esto es, verificando el estado actual de la entidad frente al cumplimiento de la norma ISO 27001 y 27002 lo que permitirá definir el alcance real del proyecto.

5.2.2 Fase 2 – Hacer. En esta etapa se definirán los objetivos, el alcance y el tiempo para implementar el SGSI en la entidad, cuyas actividades y tiempos deberán ser aprobadas por el comité de seguridad de la información.

En esta etapa se desarrollarán las siguientes actividades:

- Obtener aprobación de la dirección para iniciar el proyecto de SGSI
- Definir el alcance, sus límites y la política del SGSI
- Realizar el análisis de requisitos de seguridad de la información.
- Realizar la valoración de riesgo y planificar el tratamiento de riesgo.
- Diseñar el SGSI.

5.2.3 Fase 3 –Verificar. En esta fase se establecerán las revisiones necesarias con el fin que se cumplan los objetivos propuestos de manera correcta a través del seguimiento de cada una de las actividades establecidas.

5.2.4 Fase 4 – Actuar. Mejora continua. Durante esta fase se revisarán y evaluarán las acciones de mejora sobre las actividades y acciones preventivas y correctivas que permitan la implantación del SGSI.

6. RECURSOS NECESARIOS

Tabla 1. Recursos requeridos

RECURSO	Ítem / Actividad	Cantidad	Costo Unitario ($)	Costo Total ($)
HUMANO	1. Personal			
	✓ Investigador	2	3.600.000	7.200.000
TECNOLÓGICO	2. Equipos			
	✓ Computador	2	1.500.000	3.000.000
	✓ Impresora Laser	1	400.000	400.000
	✓ Internet	3 Meses	50.000	150.000
TÉCNICO	3. Desplazamientos			
	✓ Transporte	2	300.000	600.000
	✓ Combustible	3 Meses	100.000	600.000
	4. Materiales			
	✓ Memorias USB	2	30.000	60.000
	✓ Papelería (Lapiceros, CD, etc.)	2	70.000	140.000
	✓ Fotocopias	10	20.000	200.000
	✓ Tóner de impresora	2	100.000	200.000
	5. Servicios Técnicos			
	✓ Transcripción de encuestas	2	80.000	160.000
	6. Otros			
	✓ Imprevistos	2	200.000	400.000
Costo Total del Proyecto				$ 13.110.000

Fuente: el autor

7. CRONOGRAMA DE ACTIVIDADES

Figura 2. Cronograma implementación SGSI

Nombre	Duración	Inicio	Terminado
Planificación del proyecto	55 days?	**22/02/16 08:00 AM**	**6/05/16 05:00 PM**
Fase 1: Obtener la aprobación de la dirección para el inicio del proyecto	21 days?	**22/02/16 08:00 AM**	**21/03/16 05:00 PM**
Aclarar las prioridades de la organización para desarrollar el SGSI	2 days?	22/02/16 08:00 AM	23/02/16 05:00 PM
Definir los objetivos del SGSI	2 days?	24/02/16 08:00 AM	25/02/16 05:00 PM
Documentar las limitaciones pertinentes a la seguridad de la información	2 days?	26/02/16 08:00 AM	29/02/16 05:00 PM
Alineación con los sistemas de gestión existentes	2 days?	1/03/16 08:00 AM	2/03/16 05:00 PM
Definir el alcance preliminar del SGSI	7 days?	**3/03/16 08:00 AM**	**11/03/16 05:00 PM**
Definición del alcance preliminar	2 days?	3/03/16 08:00 AM	4/03/16 05:00 PM
Definición de roles y responsabilidades preliminar del SGSI	5 days?	7/03/16 08:00 AM	11/03/16 05:00 PM
Crear el caso del negocio y el plan del proyecto	7 days?	**11/03/16 08:00 AM**	**21/03/16 05:00 PM**
Crear el caso	2 days?	11/03/16 08:00 AM	14/03/16 05:00 PM
Crear el plan de proyecto	5 days?	15/03/16 08:00 AM	21/03/16 05:00 PM
Fase 2: Definir el alcance y la política del SGSI	7 days?	**22/03/16 08:00 AM**	**30/03/16 05:00 PM**
Establecer el Alcance y limite del SGSI en la organización	5 days?	22/03/16 08:00 AM	28/03/16 05:00 PM
Desarrollar la politica del SGSI	3 days?	28/03/16 08:00 AM	30/03/16 05:00 PM
Fase 3: Realizar análisis de requisitos del SGSI en la Organización	7 days?	**31/03/16 08:00 AM**	**8/04/16 05:00 PM**
Definición de requisitos de la seguridad de la información	2 days?	31/03/16 08:00 AM	1/04/16 05:00 PM
Identificación de activos de la información	3 days?	2/04/16 08:00 AM	6/04/16 05:00 PM
Identificación de las vulnerabilidades, amenazas	2 days?	6/04/16 08:00 AM	7/04/16 05:00 PM
Clasificación de los activos de la información	1 day?	8/04/16 08:00 AM	8/04/16 05:00 PM
Resultado del evaluación de la seguridad de la información (actual)	1 day?	8/04/16 08:00 AM	8/04/16 05:00 PM
Fase 4: Evaluación de riesgos y el plan de tratamiento de riesgos	21 days?	**8/04/16 08:00 AM**	**6/05/16 05:00 PM**
Definición y aprobación de la Metodología para la valoración de riesgo	1 day?	8/04/16 08:00 AM	8/04/16 05:00 PM
Valoración de riesgo	8 days	11/04/16 08:00 AM	20/04/16 05:00 PM
Resultados de evaluación del riesgo	4 days?	21/04/16 08:00 AM	26/04/16 05:00 PM
Seleccionar los objetivos de control y controles	3 days	27/04/16 08:00 AM	29/04/16 05:00 PM
Definir la lista de controles y objetivos de control	2 days?	28/04/16 08:00 AM	29/04/16 05:00 PM
Definir el plan de tratamientos de riesgos	3 days	30/04/16 08:00 AM	4/05/16 05:00 PM
Definición del sistema de control interno informático	2 days?	5/05/16 08:00 AM	6/05/16 05:00 PM

Fuente: el autor

8. ANÁLISIS DEL SISTEMA DE SEGURIDAD DE LA INFORMACIÓN

8.1 DESCRIPCIÓN Y ANÁLISIS DE RIESGOS

El siguiente análisis de riesgos tiene como finalidad, hallar cuáles son los activos de información del IDIPRON que pueden estar expuestos a unos niveles altos de riesgo y cuáles son los activos de información que podrían causar un gran impacto en la entidad, si se llegan a materializar las amenazas que lo puedan afectar.

Para poder establecer cuáles son los activos de mayor riesgo y de gran impacto, se da inicio a unas etapas previas que a continuación se exponen, tomando como base la metodología "MAGERIT".

Según esta metodología se deben seguir los siguientes pasos:

- Identificar los activos relevantes para la organización
- Valorar los activos
- Identificar a qué amenazas están expuestos los activos
- Valorar la influencia de la amenaza en cada uno de los activos, en cuanto a la probabilidad de ocurrencia y el porcentaje de degradación que afectaría al valor del activo.
- Determinar el impacto potencial
- Determinación del riesgo potencial

8.2 IDENTIFICACIÓN DE ACTIVOS

Para dar inicio al análisis de riesgos de los activos de TI, se procede a identificar los activos de información que a continuación se listan en la "tabla 2", organizados según el tipo.

Tabla 2. Identificación de Activos

TIPO	ID	NOMBRE DEL ACTIVO
[IS] SERVICIOS	1	Controlador de dominio UPI La 27 sur
	2	Controlador de dominio misional
	3	Controlador de dominio principal
	4	Controlador de dominio Misión Bogotá
	5	Controlador de dominio UPI La 32
	6	Controlador de dominio UPI La Arcadia

Tabla 3. (Continuación)

TIPO	ID	NOMBRE DEL ACTIVO
[IS] SERVICIOS	7	Controlador de dominio UPI La Florida
	8	Correo electrónico ZIMBRA MTA
	9	Correo exchange
	10	Controlador de dominio UPI La Vega
	11	Controlador de dominio UPI El Perdomo
	12	Controlador de dominio UPI San Francisco
	13	Portal Académico
	14	Portal Institucional
	15	Controlador de dominio secundario
	16	Sistema acceso Biométrico
	17	Canal de internet y red MPLS
[SW] APLICACIONES	18	Software de Aplicaciones (medios)
	19	Software de Sistemas operativos (medios)
	20	Software de Base de Datos (medios)
	21	Medios con claves de licenciamiento
	22	Aplicación SIMI – AP
	23	Servidor aplicativo SPRAI
	24	Consola Vcenter
	25	Aplicación Idocument
	26	Base de datos Oracle 11g
	27	Aplicaciones Aranda Software - Parte Misional
	28	Aplicaciones Aranda Software - Parte Administrativa
	29	SYSMAN
	30	SICAPITAL
	31	Antivirus Kaspersky
[HW] EQUIPOS	32	Antispam Barracuda
	33	Impresora Datacard CP 40 Plus
	34	Servidor UPI El Perdomo
	35	Servidor UPI La 27 Sur
	36	Servidor UPI La 32
	37	Servidor UPI La Florida
	38	Servidor UPI La Vega
	39	Access Point
	40	Servidor UPI La Arcadia

Tabla 4. (Continuación)

TIPO	ID	NOMBRE DEL ACTIVO
[HW] EQUIPOS	41	Equipos de cómputo
	42	Servidor UPI San Francisco
	43	Switch de borde 4210G
	44	Sistema de almacenamiento formato rack
	45	Gabinete de 8 blades
	46	Equipo de Seguridad Perimetral
	47	Servidor formato blade marca Hewlett Packard Modelo proliant BL460C G1
	48	Servidor formato blade marca Hewlett Packard. Modelo proliant BL460C G7
	49	Servidor Proliant 120 G5
	50	Servidor Proyecto Misión Bogotá
	51	Impresora para código de barras
	52	Servidor controlador de dominio principal
	53	Switch de borde 4800
	54	Switch de borde - Referencia 2410 - UPI La Rioja
	55	Switch de borde - Referencia 2920 - Proyecto Misión Bogotá
	56	Switch de borde - Referencia 4250T
	57	Switch de borde - Referencia 4500G UPI La Florida
	58	Switch de borde - Referencia 4800G - UPI La 32
	59	Switch de borde - Referencia 4800G - UPI El Perdomo
	60	Switch de borde - Referencia 4800G - UPI La Florida
	61	Switch de borde - Referencia 4800G - UPI La 27 sur
	62	Switch de borde - Referencia 4800G - UPI San Francisco
	63	Switch de borde - Referencia 4800G - UPI La Rioja
	64	Switch de borde - Referencia 4800G - UPI La Vega
	65	Switch de borde - Referencia 4800G - UPI Santa Lucia
	66	Switch de borde - Referencia 4800G - UPI Servitá
	67	Switch de borde - Referencia E2910 HP - UPI Bosa
	68	Switch de borde - Referencia E2910 HP - Proyecto 968
	69	Switch de borde - Referencia V1910 - Proyecto Misión Bogotá
	70	Switch de borde 4500G - Sede Administrativa
	71	Switch de borde. Referencia 4500G - UPI La Arcadia
	72	Switch de borde. Referencia 4800G - UPI La Arcadia
	73	Switch de core. Referencia 5500G - Sede Administrativa
	74	Copia de Respaldo - Dataprotector

Tabla 5. (Continuación)

TIPO	ID	NOMBRE DEL ACTIVO
[HW] EQUIPOS	75	Sistema de Backups - Dataprotector
	76	Servidor de correo - Proliant DL 380 G5
	77	Servidor Ambiente de pruebas y desarrollo
	78	Servidor de base de datos Nómina
	79	Servidor de Virtualización
	80	Servidor base de datos SQL
	81	Servidor de Archivos
	82	Servidor de impresión
	83	Servidor OAS - SICAPITAL
[AUX] ELEMENTOS AUXILIARES	84	UPS de 15 KVA - UPI La Arcadia
	85	UPS de 15 KVA - UPI La Rioja
	86	Planta eléctrica
	87	UPS de 10 KVA - Sede Misión Bogotá
	88	UPS de 10 KVA - UPI La vega
	89	UPS de 15 KVA - UPI Santa Lucia
	90	UPS de 10 KVA - UPI San Francisco
	91	UPS de 15 KVA - UPI El Perdomo
	92	UPS de 15 KVA - UPI La 27 sur
	93	UPS de 15 KVA - UPI Servitá
	94	UPS de 15 KVA - UPI La Florida
	95	UPS de 20 KVA - Sede proyecto 968
	96	UPS de 10 KVA - UPI Bosa
	97	UPS de 20 KVA - UPI La 32
	98	UPS de 20 KVA - UPI La Florida
	99	UPS de 30 KVA - UPI El Perdomo
	100	Sistema de Aire Acondicionado
[D] DATOS / INFORMACIÓN	101	Documentación Técnica
[P] PERSONAL	102	Administradores de Sistemas

Fuente: el autor

8.3 VALORACIÓN DE ACTIVOS

A continuación se procede a valorar cada uno de los activos de información, tomando las siguientes dimensiones de seguridad:

- [D] Disponibilidad
- [I] Integridad de los datos
- [C] Confidencialidad de la información
- [A] Autenticidad de los usuarios y de la información
- [T] Trazabilidad del servicio y de los datos

Y los siguientes criterios de valoración:

Tabla 6. Rangos valoración Activos

Valor			Criterio
MA	Muy Alto	9 - 10	Daño muy grave
A	Alto	6 – 8	Daño grave
M	Medio	3 – 5	Daño importante
B	Bajo	1 – 2	Daño menor
MB	Despreciable	0	Irrelevante a efectos prácticos

Fuente: el autor

En las siguientes tablas se establecen las valoraciones de cada uno de los activos según su tipo.

Cabe resaltar que la valoración de cada uno de los activos no requiere que sean calificados en sus cinco dimensiones, ésta depende o responde si aplica o no a dicha dimensión.

“La valoración que recibe un activo en una cierta dimensión es la medida del perjuicio para la organización si el activo se ve dañado en dicha dimensión”.[19]

Nota: estas valoraciones fueron tomadas por medio de una entrevista al responsable de cada uno de los activos de información.

[19] Magerit-versión 3.0 Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información, Libro 2-Método, https://www.ccn-cert.cni.es/publico/herramientas/pilar5/magerit/ p. 15

8.3.1 Valoración Activos - Tipo: [IS] SERVICIOS

Tabla 7. Valoración Activos tipo: Servicios

Activo	Dimensiones				
	D	I	C	A	T
Controlador de dominio UPI La 27 sur	[10]	[10]	[10]	[9]	
Controlador de dominio misional	[10]	[10]	[10]	[9]	
Controlador de dominio principal	[10]	[10]	[10]	[9]	
Controlador de dominio Misión Bogotá	[10]	[10]	[10]	[9]	
Controlador de dominio UPI La 32	[10]	[10]	[10]	[9]	
Controlador de dominio UPI La Arcadia	[10]	[10]	[10]	[9]	
Controlador de dominio UPI La Florida	[10]	[10]	[10]	[9]	
Correo electrónico ZIMBRA MTA	[10]	[10]	[10]	[7]	
Correo Exchange	[2]	[2]	[2]	[2]	
Controlador de dominio UPI La Vega	[10]	[10]	[10]	[9]	
Controlador de dominio UPI El Perdomo	[10]	[10]	[10]	[9]	
Controlador de dominio UPI San Francisco	[10]	[10]	[10]	[9]	
Portal Académico	[8]	[8]	[10]	[8]	[5]
Portal Institucional	[10]	[10]	[3]	[5]	
Controlador de dominio secundario	[8]	[10]			
Sistema acceso Biométrico	[10]			[10]	
Canal de internet y red MPLS	[10]		[10]		

Fuente: el autor

8.3.2 Valoración Activos - Tipo: [SW] APLICACIONES

Tabla 8 Valoración Activos tipo: Aplicaciones

Activo	Dimensiones				
	D	I	C	A	T
Software de Aplicaciones (medios)	[9]	[9]			
Software de Sistemas operativos (medios)	[9]	[9]			

Tabla 5. (Continuación)

Activo	Dimensiones				
	D	I	C	A	T
Software de Base de Datos (medios)	[9]	[3]			
Medios con claves de licenciamiento	[10]	[9]	[10]		
Aplicación SIMI – AP	[9]	[10]	[10]	[10]	[10]
Servidor aplicativo SPRAI	[5]	[10]	[10]	[10]	
Consola Vcenter	[10]	[10]			
Aplicación Idocument	[8]	[8]	[6]	[4]	
Base de datos Oracle 11g	[10]	[10]	[10]		
Aplicaciones Aranda Software - Parte Misional	[7]	[7]	[6]	[7]	
Aplicaciones Aranda Software - Parte Administrativa	[7]	[7]	[6]	[7]	
SYSMAN	[9]	[9]	[8]	[9]	
SICAPITAL	[7]	[8]	[7]		
Antivirus Kaspersky	[10]	[10]		[8]	[8]

Fuente: el autor

8.3.3 Valoración Activos - Tipo: [HW] EQUIPOS

Tabla 9. Valoración Activos tipo: Equipos

Activo	Dimensiones				
	D	I	C	A	T
Antispam Barracuda	[6]	[6]		[9]	
Impresora Datacard CP 40 Plus	[10]	[10]			
Servidor UPI El Perdomo	[7]	[7]	[9]	[10]	
Servidor UPI La 27 Sur	[7]	[7]	[9]	[10]	
Servidor UPI La 32	[7]	[7]	[9]	[10]	
Servidor UPI La Florida	[7]	[7]	[9]	[10]	
Servidor UPI La Vega	[7]	[7]	[9]	[10]	
Access Point	[6]		[7]	[7]	
Servidor UPI La Arcadia	[7]	[7]	[9]	[10]	
Equipos de cómputo	[5]	[9]	[10]	[7]	
Servidor UPI San Francisco	[7]	[7]	[9]	[10]	
Switch de borde 4210G	[7]				[7]
Sistema de almacenamiento formato rack	[10]	[10]	[10]		
Gabinete de 8 blades	[10]	[10]	[10]	[8]	
Equipo de Seguridad Perimetral	[10]	[8]	[6]		

Tabla 6. (continuación)

Activo	Dimensiones				
	D	I	C	A	T
Servidor formato blade marca Hewlett Packard Modelo proliant BL460C G1	[8]	[8]	[9]	[10]	
Servidor formato blade marca Hewlett Packard. Modelo proliant BL460C G7	[8]	[8]	[9]	[10]	
Servidor Proliant 120 G5	[8]	[8]	[9]	[10]	
Servidor Proyecto Misión Bogotá	[8]	[8]	[9]	[10]	
Impresora para código de barras	[9]	[9]			[9]
Servidor controlador de dominio principal	[9]	[9]	[9]	[10]	
Switch de borde 4800	[7]				
Switch de borde - Referencia 2410 - UPI La Rioja	[7]				
Switch de borde - Referencia 2920 - Proyecto Misión Bogotá	[7]				
Switch de borde - Referencia 4250T	[7]				
Switch de borde - Referencia 4500G UPI La Florida	[7]				
Switch de borde - Referencia 4800G - UPI La 32	[7]				
Switch de borde - Referencia 4800G - UPI El Perdomo	[7]				
Switch de borde - Referencia 4800G - UPI La Florida	[7]				
Switch de borde - Referencia 4800G - UPI La 27 sur	[7]				
Switch de borde - Referencia 4800G - UPI San Francisco	[7]				
Switch de borde - Referencia 4800G - UPI La Rioja	[7]				
Switch de borde - Referencia 4800G - UPI La Vega	[7]				
Switch de borde - Referencia 4800G - UPI Santa Lucia	[7]				
Switch de borde - Referencia 4800G - UPI Servitá	[7]				
Switch de borde - Referencia E2910 HP - UPI Bosa	[7]				
Switch de borde - Referencia E2910 HP - Proyecto 968	[7]				

Tabla 6. (continuación)

Activo	Dimensiones				
	D	I	C	A	T
Switch de borde - Referencia V1910 - Proyecto Misión Bogotá	[7]				
Switch de borde 4500G - Sede Administrativa	[7]				
Switch de borde. Referencia 4500G - UPI La Arcadia	[7]				
Switch de borde. Referencia 4800G - UPI La Arcadia	[7]				
Switch de core. Referencia 5500G - Sede Administrativa	[7]				
Copia de Respaldo - Dataprotector	[7]		[8]		
Sistema de Backups - Dataprotector	[7]		[8]		
Servidor de correo - Proliant DL 380 G5	[9]	[9]	[9]	[10]	
Servidor Ambiente de pruebas y desarrollo	[5]	[6]			
Servidor de base de datos Nómina	[10]	[10]	[10]		
Servidor de Virtualización	[10]	[10]			
Servidor base de datos SQL	[7]	[7]	[7]		
Servidor de Archivos	[10]	[10]	[10]	[10]	
Servidor de impresión	[9]				[8]
Servidor OAS – SICAPITAL	[8]	[8]	[6]	[6]	

Fuente: el autor

8.3.4 Valoración Activos - Tipo: [AUX] ELEMENTOS AUXILIARES

Tabla 10. Valoración Activos tipo: Elementos Auxiliares

Activo	Dimensiones				
	D	I	C	A	T
UPS de 15 KVA - UPI La Arcadia	[6]				
UPS de 15 KVA - UPI La Rioja	[6]				
Planta eléctrica	[6]				
UPS de 10 KVA - Sede Misión Bogotá	[6]				
UPS de 10 KVA - UPI La vega	[6]				
UPS de 15 KVA - UPI Santa Lucia	[6]				
UPS de 10 KVA - UPI San Francisco	[6]				

Tabla 7. (Continuación)

Activo	Dimensiones				
	D	I	C	A	T
UPS de 15 KVA - UPI El Perdomo	[6]				
UPS de 15 KVA - UPI La 27 sur	[6]				
UPS de 15 KVA - UPI Servitá	[6]				
UPS de 15 KVA - UPI La Florida	[6]				
UPS de 20 KVA - Sede proyecto 968	[6]				
UPS de 10 KVA - UPI Bosa	[6]				
UPS de 20 KVA - UPI La 32	[6]				
UPS de 20 KVA - UPI La Florida	[6]				
UPS de 30 KVA - UPI El Perdomo	[6]				
Sistema de Aire Acondicionado	[10]				

Fuente: el autor

8.3.5 Valoración Activos - Tipo: [D] DATOS / INFORMACIÓN

Tabla 11. Valoración Activos tipo: Datos / Información

Activo	Dimensiones				
	D	I	C	A	T
Documentación Técnica	[8]	[6]	[6]	[9]	

Fuente: el autor

8.3.6 Valoración Activos – Tipo: [P] PERSONAL

Tabla 12. Valoración Activos tipo: Personal

Activo	Dimensiones				
	D	I	C	A	T
Administradores de Sistemas	[7]	[4]	[5]		

Fuente: el autor

8.4 IDENTIFICACIÓN Y VALORACIÓN DE AMENAZAS

Posteriormente de haber valorado los activos de información, se procede a identificar y valorar las amenazas por cada uno de los activos de información.

En cuanto a la identificación de las amenazas, se tomará como base la clasificación establecida en la metodología “MAGERIT”, organizada en cuatro grupos, de la siguiente manera:

- [N] Desastres Naturales
- [I] De Origen Industrial
- [E] Errores y fallos no intencionados
- [A] Ataques intencionados

En cuanto a la probabilidad de ocurrencia de la amenaza, se tomarán los siguientes niveles de probabilidad.

Tabla 13. Niveles probabilidad Amenazas

Nivel	Descripción
MA	Muy Alto
A	Alto
M	Medio
B	Bajo
MB	Muy Bajo

Fuente: el autor

A su vez, por cada amenaza identificada en cada uno de los activos, se debe especificar el porcentaje que el activo puede degradarse de acuerdo a dicha amenaza en las dimensiones que pueda afectar en el activo (Disponibilidad, Integridad, Confidencialidad, Autenticidad y Trazabilidad). En la siguiente tabla se muestran los rangos de degradación.

Tabla 14. Niveles degradación del valor

Valor		Criterio
90% - 100%	MA	Degradación MUY ALTA del activo
70% - 89%	A	Degradación ALTA considerable del activo
50% - 69%	M	Degradación MEDIANA del activo
10% - 49%	B	Degradación BAJA del activo
1% - 9%	MB	Degradación MUY BAJA del activo

Fuente: el autor

Con base en lo anterior, como se muestra en la siguiente tabla, en la segunda columna, el nombre de la amenaza que puede afectar al activo (identificada con un código de acuerdo al catálogo de amenazas establecida en la metodología "MAGERIT"), en la tercera columna se establece el nivel de probabilidad de ocurrencia de la amenaza, y en la siguiente columna se puede establecer el porcentaje de degradación que sufriría el activo en la dimensión que afecte (D = Disponibilidad, I = Integridad, C = Confidencialidad, A = Autenticidad, T = Trazabilidad).

Nota: estas valoraciones fueron tomadas por medio de una entrevista al responsable de cada activo de información.

8.4.1 Identificación y Valoración de Amenazas Tipo: [IS] SERVICIOS

Tabla 15. Identificación y valoración de amenazas en activos tipo: Servicios

ACTIVOS	Amenazas	Probabilidad	Dimensiones				
			[D]	[I]	[C]	[A]	[T]
Controlador de dominio UPI La 27 sur	[E.2] Errores del administrador del sistema / de la seguridad	**B**	**30%**	**30%**	**30%**		
	[E.15] Alteración de la información	**MB**		**100%**	**100%**		
	[E.18] Destrucción de la información	**MB**	**90%**	**90%**	**90%**		
	[E.19] Fugas de información	**B**	**5%**	**90%**	**90%**		
	[E.24] caída del sistema por agotamiento de recursos	**B**	**50%**				
	[A.5] suplantación de la identidad del usuario	**MB**		**50%**	**50%**	**100%**	
	[A.6] Abuso de privilegios de acceso	**M**		**10%**	**10%**		
	[A.7] uso no previsto	**M**	**100%**	**10%**	**10%**		
	[A.11] Acceso no autorizado	**M**		**10%**	**50%**		
	[A.15] Modificación de la información	**A**		**50%**			

Tabla 12. (Continuación)

ACTIVOS	Amenazas	Probabilidad	Dimensiones				
			[D]	[I]	[C]	[A]	[T]
Controlador de dominio UPI La 27 sur	[A.18] Destrucción de la información	**M**	**50%**	**50%**			
	[A.19] revelación de información	**M**			**50%**		
	[A.24] Denegación de servicio	**A**	**50%**				
Controlador de dominio misional	[E.2] Errores del administrador del sistema / de la seguridad	**B**	**30%**	**30%**	**30%**		
	[E.15] Alteración de la información	**MB**		**100%**	**100%**		
	[E.18] Destrucción de la información	**MB**	**90%**	**90%**	**90%**		
	[E.19] Fugas de información	**B**	**5%**	**90%**	**90%**		
	[E.24] caída del sistema por agotamiento de recursos	**B**	**50%**				
	[A.5] suplantación de la identidad del usuario	**MB**		**50%**	**50%**	**100%**	
	[A.6] Abuso de privilegios de acceso	**M**		**10%**	**10%**		
	[A.7] uso no previsto	**M**	**100%**	**10%**	**10%**		
	[A.11] Acceso no autorizado	**M**		**10%**	**50%**		
	[A.15] Modificación de la información	**A**		**50%**			
	[A.18] Destrucción de la información	**M**	**50%**				
	[A.19] revelación de información	**M**			**50%**		
	[A.24] Denegación de servicio	**A**	**50%**				
Controlador de dominio principal	[E.2] Errores del administrador del sistema / de la seguridad	**B**	**30%**	**30%**	**30%**		

Tabla 12. (Continuación)

ACTIVOS	Amenazas	Probabilidad	Dimensiones				
			[D]	[I]	[C]	[A]	[T]
Controlador de dominio principal	[E.15] Alteración de la información	MB		100%	100%		
	[E.18] Destrucción de la información	MB	90%	90%	90%		
	[E.19] Fugas de información	B	5%	90%	90%		
	[E.24] caída del sistema por agotamiento de recursos	B	50%				
	[A.5] suplantación de la identidad del usuario	MB		50%	50%	100%	
	[A.6] Abuso de privilegios de acceso	M		10%	10%		
	[A.7] uso no previsto	M	100%	10%	10%		
	[A.11] Acceso no autorizado	M		10%	50%		
	[A.15] Modificación de la información	A		50%			
	[A.18] Destrucción de la información	M	50%				
	[A.19] revelación de información	M			50%		
	[A.24] Denegación de servicio	A	50%				
Controlador de dominio Misión Bogotá	[E.2] Errores del administrador del sistema / de la seguridad	B	30%	30%	30%		
	[E.15] Alteración de la información	MB		100%	100%		
	[E.18] Destrucción de la información	MB	90%	90%	90%		
	[E.19] Fugas de información	B	5%	90%	90%		
	[E.24] caída del sistema por agotamiento de recursos	B	50%				

Tabla 12. (Continuación)

ACTIVOS	Amenazas	Probabilidad	Dimensiones				
			[D]	[I]	[C]	[A]	[T]
Controlador de dominio Misión Bogotá	[A.5] suplantación de la identidad del usuario	**MB**		**50%**	**50%**	**100%**	
	[A.6] Abuso de privilegios de acceso	**M**		**10%**	**10%**		
	[A.7] uso no previsto	**M**	**100%**	**10%**	**10%**		
	[A.11] Acceso no autorizado	**M**		**10%**	**50%**		
	[A.15] Modificación de la información	**A**		**50%**			
	[A.18] Destrucción de la información	**M**	**50%**				
	[A.19] revelación de información	**M**			**50%**		
	[A.24] Denegación de servicio	**A**	**50%**				
Controlador de dominio UPI La 32	[E.2] Errores del administrador del sistema / de la seguridad	**B**	**30%**	**30%**	**30%**		
	[E.15] Alteración de la información	**MB**		**100%**	**100%**		
	[E.18] Destrucción de la información	**MB**	**90%**	**90%**	**90%**		
	[E.19] Fugas de información	**B**	**5%**	**90%**	**90%**		
	[E.24] caída del sistema por agotamiento de recursos	**B**	**50%**				
	[A.5] suplantación de la identidad del usuario	**MB**		**50%**	**50%**	**100%**	
	[A.6] Abuso de privilegios de acceso	**M**		**10%**	**10%**		
	[A.7] uso no previsto	**M**	**100%**	**10%**	**10%**		
	[A.11] Acceso no autorizado	**M**		**10%**	**50%**		

Tabla 12. (Continuación)

ACTIVOS	Amenazas	Probabilidad	Dimensiones				
			[D]	[I]	[C]	[A]	[T]
Controlador de dominio UPI La 32	[A.15] Modificación de la información	**A**		**50%**			
	[A.18] Destrucción de la información	**M**	**50%**				
	[A.19] revelación de información	**M**			**50%**		
	[A.24] Denegación de servicio	**A**	**50%**				
Controlador de dominio UPI La Arcadia	[E.2] Errores del administrador del sistema / de la seguridad	**B**	**30%**	**30%**	**30%**		
	[E.15] Alteración de la información	**MB**		**100%**	**100%**		
	[E.18] Destrucción de la información	**MB**	**90%**	**90%**	**90%**		
	[E.19] Fugas de información	**B**	**5%**	**90%**	**90%**		
	[E.24] caída del sistema por agotamiento de recursos	**B**	**50%**				
	[A.5] suplantación de la identidad del usuario	**MB**		**50%**	**50%**	**100%**	
	[A.6] Abuso de privilegios de acceso	**M**		**10%**	**10%**		
	[A.7] uso no previsto	**M**	**100%**	**10%**	**10%**		
	[A.11] Acceso no autorizado	**M**		**10%**	**50%**		
	[A.15] Modificación de la información	**A**		**50%**			
	[A.18] Destrucción de la información	**M**	**50%**				
	[A.19] revelación de información	**M**			**50%**		
	[A.24] Denegación de servicio	**A**	**50%**				

Tabla 12. (Continuación)

ACTIVOS	Amenazas	Probabilidad	Dimensiones				
			[D]	[I]	[C]	[A]	[T]
Controlador de dominio UPI La Florida	[E.2] Errores del administrador del sistema / de la seguridad	**B**	**30%**	**30%**	**30%**		
	[E.15] Alteración de la información	**MB**		**100%**	**100%**		
	[E.18] Destrucción de la información	**MB**	**90%**	**90%**	**90%**		
	[E.19] Fugas de información	**B**	**5%**	**90%**	**90%**		
	[E.24] caída del sistema por agotamiento de recursos	**B**	**50%**				
	[A.5] suplantación de la identidad del usuario	**MB**		**50%**	**50%**	**100%**	
	[A.6] Abuso de privilegios de acceso	**M**		**10%**	**10%**		
	[A.7] uso no previsto	**M**	**100%**	**10%**	**10%**		
	[A.11] Acceso no autorizado	**M**		**10%**	**50%**		
	[A.15] Modificación de la información	**A**		**50%**			
	[A.18] Destrucción de la información	**M**	**50%**				
	[A.19] revelación de información	**M**			**50%**		
	[A.24] Denegación de servicio	**A**	**50%**				
Correo electrónico ZIMBRA MTA	[E.1] Errores de los usuarios	**A**	**10%**	**70%**	**70%**		
	[E.2] Errores del administrador del sistema / de la seguridad	**M**	**50%**	**50%**	**50%**		
	[E.15] Alteración de la información	**B**		**40%**			

Tabla 12. (Continuación)

ACTIVOS	Amenazas	Probabilidad	Dimensiones				
			[D]	[I]	[C]	[A]	[T]
Correo electrónico ZIMBRA MTA	[E.18] Destrucción de la información	**A**	**100%**	**100%**			
	[E.19] Fugas de información	**A**			**100%**		
	[E.24] caída del sistema por agotamiento de recursos	**A**	**50%**				
	[A.5] suplantación de la identidad del usuario	**M**		**50%**	**50%**	**100%**	
	[A.6] Abuso de privilegios de acceso	**M**		**80%**	**100%**		
	[A.7] uso no previsto	**M**	**100%**	**10%**	**10%**		
	[A.11] Acceso no autorizado	**M**		**30%**	**50%**		
	[A.13] Repudio (negación de actuaciones)	**M**		**100%**			
	[A.18] Destrucción de la información	**M**	**50%**				
	[A.19] revelación de información	**M**			**50%**		
	[A.24] Denegación de servicio	**A**	**50%**				
Correo Exchange	[E.1] Errores de los usuarios	**MB**	**10%**	**70%**	**70%**		
	[E.2] Errores del administrador del sistema / de la seguridad	**MB**	**50%**	**50%**	**50%**		
	[E.15] Alteración de la información	**MB**		**40%**			
	[E.18] Destrucción de la información	**MB**	**100%**	**100%**			
	[E.19] Fugas de información	**MB**			**100%**		
	[E.24] caída del sistema por agotamiento de recursos	**MB**	**50%**				

Tabla 12. (Continuación)

ACTIVOS	Amenazas	Probabilidad	Dimensiones				
			[D]	[I]	[C]	[A]	[T]
Correo Exchange	[A.5] suplantación de la identidad del usuario	MB		50%	50%	100%	
	[A.6] Abuso de privilegios de acceso	MB		80%	100%		
	[A.7] uso no previsto	MB	100%	10%	10%		
	[A.11] Acceso no autorizado	MB		30%	50%		
	[A.13] Repudio (negación de actuaciones)	MB		100%			
	[A.18] Destrucción de la información	MB	50%				
	[A.19] revelación de información	MB			50%		
	[A.24] Denegación de servicio	MB	50%				
Controlador de dominio UPI La Vega	[E.2] Errores del administrador del sistema / de la seguridad	B	30%	30%	30%		
	[E.15] Alteración de la información	MB		100%	100%		
	[E.18] Destrucción de la información	MB	90%	90%	90%		
	[E.19] Fugas de información	B	5%	90%	90%		
	[E.24] caída del sistema por agotamiento de recursos	B	50%				
	[A.5] suplantación de la identidad del usuario	MB		50%	50%	100%	
	[A.6] Abuso de privilegios de acceso	M		10%	10%		
	[A.7] uso no previsto	M	100%	10%	10%		
	[A.11] Acceso no autorizado	M		10%	50%		

Tabla 12. (Continuación)

ACTIVOS	Amenazas	Probabilidad	Dimensiones				
			[D]	[I]	[C]	[A]	[T]
Controlador de dominio UPI La Vega	[A.15] Modificación de la información	**A**		**50%**			
	[A.18] Destrucción de la información	**M**	**50%**				
	[A.19] revelación de información	**M**			**50%**		
	[A.24] Denegación de servicio	**A**	**50%**				
Controlador de dominio UPI El Perdomo	[E.2] Errores del administrador del sistema / de la seguridad	**B**	**30%**	**30%**	**30%**		
	[E.15] Alteración de la información	**MB**		**100%**	**100%**		
	[E.18] Destrucción de la información	**MB**	**90%**	**90%**	**90%**		
	[E.19] Fugas de información	**B**	**5%**	**90%**	**90%**		
	[E.24] caída del sistema por agotamiento de recursos	**B**	**50%**				
	[A.5] suplantación de la identidad del usuario	**MB**		**50%**	**50%**	**100%**	
	[A.6] Abuso de privilegios de acceso	**M**		**10%**	**10%**		
	[A.7] uso no previsto	**M**	**100%**	**10%**	**10%**		
	[A.11] Acceso no autorizado	**M**		**10%**	**50%**		
	[A.15] Modificación de la información	**A**		**50%**			
	[A.18] Destrucción de la información	**M**	**50%**				
	[A.19] revelación de información	**M**			**50%**		
	[A.24] Denegación de servicio	**A**	**50%**				

Tabla 12. (Continuación)

ACTIVOS	Amenazas	Probabilidad	Dimensiones				
			[D]	[I]	[C]	[A]	[T]
Controlador de dominio UPI San Francisco	[E.2] Errores del administrador del sistema / de la seguridad	**B**	**30%**	**30%**	**30%**		
	[E.15] Alteración de la información	**MB**		**100%**	**100%**		
	[E.18] Destrucción de la información	**MB**	**90%**	**90%**	**90%**		
	[E.19] Fugas de información	**B**	**5%**	**90%**	**90%**		
	[E.24] caída del sistema por agotamiento de recursos	**B**	**50%**				
	[A.5] suplantación de la identidad del usuario	**MB**		**50%**	**50%**	**100%**	
	[A.6] Abuso de privilegios de acceso	**M**		**10%**	**10%**		
	[A.7] uso no previsto	**M**	**100%**	**10%**	**10%**		
	[A.11] Acceso no autorizado	**M**		**10%**	**50%**		
	[A.15] Modificación de la información	**A**		**50%**			
	[A.18] Destrucción de la información	**M**	**50%**				
	[A.19] revelación de información	**M**			**50%**		
	[A.24] Denegación de servicio	**A**	**50%**				
Portal Académico	[E.2] Errores del administrador del sistema / de la seguridad	**M**	**100%**	**100%**			
	[E.3] Errores de monitorización (log)	**M**	**50%**	**50%**			
	[E.4] Errores de configuración	**A**	**100%**	**100%**			
	[E.15] Alteración de la información	**MB**	**30%**	**30%**			

Tabla 12. (Continuación)

ACTIVOS	Amenazas	Probabilidad	Dimensiones				
			[D]	[I]	[C]	[A]	[T]
Portal Académico	[E.18] Destrucción de la información	**MB**	**100%**	**100%**			
	[E.20] vulnerabilidades de los programas (software)	**M**	**30%**	**30%**			
	[E.21] Errores de mantenimiento / actualización de programas (software)	**M**	**20%**	**20%**			
	[E.24] caída del sistema por agotamiento de recursos	**B**	**100%**	**100%**			
	[E.28] Indisponibilidad del personal	**M**	**10%**	**10%**			
	[A.5] suplantación de la identidad del usuario	**B**	**80%**	**80%**	**100%**		
	[A.6] Abuso de privilegios de acceso	**B**	**10%**	**10%**			
	[A.8] Difusión de software dañino	**M**	**100%**	**100%**	**100%**		
	[A.11] Acceso no autorizado	**M**	**80%**	**80%**	**100%**		
	[A.15] Modificación de la información	**B**	**50%**	**50%**			
	[A.18] Destrucción de la información	**MB**	**100%**	**100%**			
	[A.22] Manipulación de programas	**M**	**50%**	**50%**			
	[A.24] Denegación de servicio	**M**	**100%**	**100%**			
Portal Institucional	[E.2] Errores del administrador del sistema / de la seguridad	**MB**	**50%**	**50%**		**20%**	
	[E.3] Errores de monitorización (log)	**B**	**1%**	**1%**			

Tabla 12. (Continuación)

ACTIVOS	Amenazas	Probabilidad	Dimensiones				
			[D]	[I]	[C]	[A]	[T]
Portal Institucional	[E.4] Errores de configuración	**B**	**80%**	**80%**			
	[E.15] Alteración de la información	**B**		**50%**	**50%**	**50%**	
	[E.18] Destrucción de la información	**B**		**80%**		**60%**	
	[E.20] vulnerabilidades de los programas (software)	**M**	**100%**	**100%**			
	[E.21] Errores de mantenimiento / actualización de programas (software)	**M**	**50%**	**50%**			
	[E.24] caída del sistema por agotamiento de recursos	**B**	**100%**	**100%**			
	[E.28] Indisponibilidad del personal	**MB**			**5%**		
	[A.8] Difusión de software dañino	**B**	**50%**	**80%**		**20%**	
	[A.11] Acceso no autorizado	**B**		**70%**	**70%**	**70%**	
	[A.15] Modificación de la información	**MB**		**60%**	**40%**		
	[A.18] Destrucción de la información	**B**	**90%**	**90%**			
	[A.24] Denegación de servicio	**MB**	**100%**				
Controlador de dominio secundario	[E.2] Errores del administrador del sistema / de la seguridad	**B**	**90%**	**90%**			
	[E.4] Errores de configuración	**MB**	**95%**	**95%**			
	[E.21] Errores de mantenimiento / actualización de programas (software)	**B**	**30%**	**30%**			

Tabla 12. (Continuación)

ACTIVOS	Amenazas	Probabilidad	Dimensiones				
			[D]	[I]	[C]	[A]	[T]
Sistema de Acceso Biométrico	[N.*] Desastres naturales	MB	75%			75%	
	[I.1] Fuego	MB	75%			75%	
	[I.2] Daños por agua	MB	80%			80%	
	[I.5] Avería de origen físico o lógico	MB	90%			90%	
	[I.6] Corte del suministro eléctrico	M	60%			60%	
	[A.25] Robo de equipos	MB	100%			100%	
	[A.26] Ataque destructivo	MB	100%			100%	
Canal de internet y red MPLS	[N.1] Fuego	MB	100%				100%
	[N.2] Daños por agua	MB	100%				100%
	[N.*] Desastres naturales	MB	95%				95%
	[I.1] Fuego	MB	90%				90%
	[I.5] Avería de origen físico o lógico	MB	100%				100%
	[I.6] Corte del suministro eléctrico	B	100%				100%
	[I.7] Condiciones inadecuadas de temperatura o humedad	MB	75%				75%
	[I.8.12] Interrupción deliberada por un agente externo	M	100%				100%
	[E.4] Errores de configuración	MB	80%				80%
	[E.23] Errores de mantenimiento / actualización de equipos (hardware)	MB	50%				50%
	[E.24] caída del sistema por agotamiento de recursos	MB	90%				90%
	[A.25] Robo de equipos	M	100%				100%

Fuente: realizado en PILAR 5.2.9

8.4.2 Identificación y Valoración de Amenazas Tipo: [SW] APLICACIONES

Tabla 16. Identificación y valoración de amenazas en activos tipo: Aplicaciones

ACTIVOS	Amenazas	Probabilidad	Dimensiones				
			[D]	[I]	[C]	[A]	[T]
Software de Aplicaciones (medios)	[N.1] Fuego	**MB**	**90%**	**90%**			
	[I.5] Avería de origen físico o lógico	**M**	**50%**	**60%**			
	[A.7] uso no previsto	**B**	**20%**	**20%**			
Software de Sistemas operativos (medios)	[N.1] Fuego	**MB**	**90%**	**90%**			
	[I.5] Avería de origen físico o lógico	**M**	**50%**	**60%**			
	[A.7] uso no previsto	**B**	**20%**	**20%**			
Software de Base de Datos (medios)	[N.1] Fuego	**MB**	**90%**	**90%**			
	[I.5] Avería de origen físico o lógico	**M**	**50%**	**60%**			
	[A.7] uso no previsto	**B**	**20%**	**20%**			
Medios con claves de licenciamiento	[N.1] Fuego	**MB**	**90%**	**90%**			
	[I.5] Avería de origen físico o lógico	**M**	**50%**	**60%**			
	[A.7] uso no previsto	**B**	**20%**	**20%**			
Aplicación SIMI – AP	[E.1] Errores de los usuarios	**M**		**80%**		**80%**	
	[E.2] Errores del administrador del sistema / de la seguridad	**B**	**60%**				
	[E.3] Errores de monitorización (log)	**MB**	**100%**				
	[E.4] Errores de configuración	**MB**	**100%**				
	[E.15] Alteración de la información	**B**		**100%**		**100%**	**100%**

Tabla 13. (Continuación)

ACTIVOS	Amenazas	Probabilidad	Dimensiones				
			[D]	[I]	[C]	[A]	[T]
Aplicación SIMI – AP	[E.19.1] A personal interno que no necesita conocerlo	**MB**			**100%**		
	[E.20.dos] Denegación de Servicio	**M**	**100%**				
	[E.28.4] Personal insuficiente	**M**					**70%**
	[A.5.1] Por personal interno	**B**			**100%**		
	[A.7.1] Por personal interno	**MB**			**100%**		
	[A.15.1] Sin beneficio para nadie	**MB**			**100%**		
Servidor aplicativo SPRAI	[E.2] Errores del administrador del sistema / de la seguridad	**B**	**50%**				
	[E.4] Errores de configuración	**B**	**50%**				
	[E.19.1] A personal interno que no necesita conocerlo	**M**			**100%**		
	[E.20.read] Acceso de LECTURA	**MB**	**50%**				
Consola Vcenter	[N.1] Fuego	**M**	**90%**	**90%**			
	[N.2] Daños por agua	**M**	**90%**	**90%**			
	[I.1] Fuego	**M**	**90%**	**90%**			
	[I.2] Daños por agua	**M**	**90%**	**90%**			
	[E.2] Errores del administrador del sistema / de la seguridad	**MB**	**40%**	**40%**			
	[E.4] Errores de configuración	**MB**	**40%**	**40%**			
	[E.24] caída del sistema por agotamiento de recursos	**B**	**60%**	**60%**			
	[A.8] Difusión de software dañino	**M**	**50%**	**50%**			

Tabla 13. (Continuación)

ACTIVOS	Amenazas	Probabilidad	Dimensiones				
			[D]	[I]	[C]	[A]	[T]
Consola Vcenter	[A.23] Manipulación del hardware	**MB**	**100%**	**100%**			
	[A.24] Denegación de servicio	**MB**	**30%**	**30%**			
	[A.26] Ataque destructivo	**MB**	**100%**	**100%**			
Aplicación Idocument	[E.2] Errores del administrador del sistema / de la seguridad	**M**	**80%**	**80%**	**40%**	**90%**	
	[E.15] Alteración de la información	**B**		**80%**	**90%**		
Base de datos Oracle 11g	[N.1] Fuego	**MB**	**100%**	**100%**	**100%**		
	[N.*] Desastres naturales	**MB**	**100%**	**100%**	**100%**		
	[E.1] Errores de los usuarios	**M**	**10%**	**70%**			
	[E.2] Errores del administrador del sistema / de la seguridad	**M**	**80%**	**30%**	**70%**		
	[E.14] Fugas de información	**M**			**100%**		
	[E.15] Alteración de la información	**M**		**90%**	**90%**		
	[E.18] Destrucción de la información	**B**	**100%**	**100**	**100%**		
	[A.6] Abuso de privilegios de acceso	**M**	**30%**	**100%**	**100%**		
	[A.15] Modificación de la información	**B**		**90%**	**100%**		
Aplicaciones Aranda Software - Parte Misional	[N.*] Desastres naturales	**MB**	**100%**				
	[I.6] Corte del suministro eléctrico	**B**	**70%**				
	[I.7] Condiciones inadecuadas de temperatura o humedad	**MB**	**70%**				
	[E.1] Errores de los usuarios	**B**				**30%**	

Tabla 13. (Continuación)

ACTIVOS	Amenazas	Probabilidad	Dimensiones				
			[D]	[I]	[C]	[A]	[T]
Aplicaciones Aranda Software - Parte Misional	[E.2] Errores del administrador del sistema / de la seguridad	**B**	**10%**				**60%**
	[E.3] Errores de monitorización (log)	**B**					**60%**
	[E.4] Errores de configuración	**B**	**40%**				
	[E.18] Destrucción de la información	**B**		**30%**			
	[E.21] Errores de mantenimiento / actualización de programas (software)	**A**		**50%**			**50%**
	[E.24] caída del sistema por agotamiento de recursos	**MB**	**70%**				**50%**
	[A.8] Difusión de software dañino	**MB**	**80%**	**70%**			
	[A.11] Acceso no autorizado	**M**			**80%**	**80%**	
Aplicaciones Aranda Software - Parte Administrativa	[N.*] Desastres naturales	**MB**	**100%**				
	[I.6] Corte del suministro eléctrico	**B**	**70%**				
	[I.7] Condiciones inadecuadas de temperatura o humedad	**MB**	**70%**				
	[E.1] Errores de los usuarios	**B**				**30%**	
	[E.2] Errores del administrador del sistema / de la seguridad	**B**					**60%**
	[E.3] Errores de monitorización (log)	**B**					**60%**
	[E.4] Errores de configuración	**B**	**40%**				
	[E.18] Destrucción de la información	**B**		**30%**			

Tabla 13. (Continuación)

ACTIVOS	Amenazas	Probabilidad	Dimensiones				
			[D]	[I]	[C]	[A]	[T]
Aplicaciones Aranda Software - Parte Administrativa	[E.21] Errores de mantenimiento / actualización de programas (software)	**A**		**50%**			
	[E.24] caída del sistema por agotamiento de recursos	**MB**	**70%**				
	[A.8] Difusión de software dañino	**MB**	**80%**	**70%**			
	[A.11] Acceso no autorizado	**M**			**80%**	**80%**	
SYSMAN	[I.8] Fallos de servicios de comunicación	**M**	**70%**				
	[E.1] Errores de los usuarios	**M**	**50%**	**60%**	**60%**		
	[E.2] Errores del administrador	**B**	**80%**	**40%**	**70%**		
	[E.4] Errores de configuración	**B**		**80%**			
	[E.14] Escapes de información	**B**			**90%**		
	[E.15] Alteración accidental de la información	**M**		**80%**			
	[E.18] Destrucción de información	**M**	**90%**				
	[E.20] Vulnerabilidad de los programas (software)	**A**	**40%**	**50%**	**30%**		
	[E.21] Errores de mantenimiento / actualización de programas (software)	**A**	**70%**	**60%**			
	[E.24] Caída del sistema por agotamiento de recursos	**M**	**90%**				
	[A.5] Suplantación de la identidad del usuario	**M**		**90%**	**100%**	**100%**	

Tabla 13. (Continuación)

ACTIVOS	Amenazas	Probabilidad	Dimensiones				
			[D]	[I]	[C]	[A]	[T]
SYSMAN	[A.6] Abuso de privilegios de acceso	**M**	**40%**	**80%**	**90%**		
	[A.7] Uso no previsto	**M**	**40%**	**80%**	**90%**		
	[A.11] Acceso no autorizado	**B**		**80%**	**100%**		
	[A.15] Modificación de la información	**A**		**90%**			
	[A.17] Corrupción de la información	**M**		**90%**	**80%**		
	[A.18] Destrucción la información	**B**	**90%**				
	[A.19] Divulgación de información	**M**			**100%**		
SICAPITAL	[E.1] Errores de los usuarios	**A**	**40%**	**60%**	**60%**		
	[E.2] Errores del administrador	**B**	**80%**	**60%**	**70%**		
	[E.4] Errores de configuración	**M**		**80%**			
	[E.7] Deficiencias en la organización	**A**	**70%**				
	[E.15] Alteración accidental de la información	**M**		**90%**			
	[E.18] Destrucción de información	**B**	**90%**				
	[E.20] Vulnerabilidades de los programas (software)	**M**	**70%**	**70%**	**60%**		
	[E.21] Errores de mantenimiento / actualización de programas (software)	**M**	**30%**	**50%**			
	[E.24] Caída del sistema por agotamiento de recursos	**B**	**90%**				
	[E.28] Indisponibilidad del personal	**A**	**80%**				

Tabla 13. (Continuación)

ACTIVOS	Amenazas	Probabilidad	Dimensiones				
			[D]	[I]	[C]	[A]	[T]
Antivirus Kaspersky	[E.1] Errores de los usuarios	**B**	**10%**	**10%**			
	[E.2] Errores del administrador del sistema / de la seguridad	**B**	**5%**	**5%**			
	[E.3] Errores de monitorización (log)	**MB**	**20%**	**20%**			**20%**
	[E.4] Errores de configuración	**MB**	**20%**	**20%**			
	[E.20] vulnerabilidades de los programas (software)	**MB**	**15%**	**15%**			
	[E.21] Errores de mantenimiento / actualización de programas (software)	**MB**	**5%**	**5%**			
	[A.6] Abuso de privilegios de acceso	**MB**	**5%**	**5%**			
	[A.8] Difusión de software dañino	**MB**	**15%**	**15%**			
	[A.11] Acceso no autorizado	**MB**	**5%**	**5%**	**5%**		
	[A.22] Manipulación de programas	**B**	**5%**	**5%**			

Fuente: realizado en PILAR 5.2.9

8.4.3 Identificación y Valoración de Amenazas Tipo: [HW] EQUIPOS

Tabla 17. Identificación y valoración de amenazas en activos tipo: Equipos

ACTIVOS	Amenazas	Probabilidad	Dimensiones				
			[D]	[I]	[C]	[A]	[T]
Antispam Barracuda	[N.1] Fuego	**B**	**100%**				
	[N.2] Daños por agua	**M**	**60%**				
	[N.*] Desastres naturales	**MB**	**70%**				
	[I.1] Fuego	**B**	**100%**				
	[I.2] Daños por agua	**M**	**60%**				

Tabla 14. (Continuación)

ACTIVOS	Amenazas	Probabilidad	Dimensiones				
			[D]	[I]	[C]	[A]	[T]
Antispam Barracuda	[I.*] Desastres industriales	**MB**	**80%**				
	[I.3] Contaminación medioambiental	**M**	**50%**				
	[I.5] Avería de origen físico o lógico	**M**	**50%**				
	[I.6] Corte del suministro eléctrico	**A**	**40%**				
	[I.7] Condiciones inadecuadas de temperatura o humedad	**M**	**40%**				
	[E.2] Errores del administrador del sistema / de la seguridad	**A**	**70%**	**70%**			
	[E.23] Errores de mantenimiento / actualización de equipos (hardware)	**A**	**50%**				
	[E.25] Pérdida de equipos	**B**	**100%**				
	[A.6] Abuso de privilegios de acceso	**B**		**10%**			
	[A.7] uso no previsto	**B**	**10%**				
	[A.11] Acceso no autorizado	**M**		**100%**			
	[A.23] Manipulación del hardware	**B**	**100%**				
	[A.24] Denegación de servicio	**M**	**100%**				
	[A.26] Ataque destructivo	**M**	**100%**				
Impresora Datacard CP 40 Plus	[N.1] Fuego	**MB**	**100%**				
	[N.2] Daños por agua	**MB**	**100%**				
	[N.*] Desastres naturales	**MB**	**100%**				
	[I.1] Fuego	**MB**	**100%**				

Tabla 14. (Continuación)

ACTIVOS	Amenazas	Probabilidad	Dimensiones				
			[D]	[I]	[C]	[A]	[T]
Impresora Datacard CP 40 Plus	[I.2] Daños por agua	**MB**	**100%**				
	[I.*] Desastres industriales	**MB**	**100%**				
	[I.3] Contaminación medioambiental	**MB**	**50%**				
	[I.4] Contaminación electromagnética	**MB**	**50%**				
	[I.5] Avería de origen físico o lógico	**M**	**100%**				
	[I.6] Corte del suministro eléctrico	**B**	**100%**				
	[I.7] Condiciones inadecuadas de temperatura o humedad	**MB**	**10%**				
	[E.2] Errores del administrador del sistema / de la seguridad	**MB**	**10%**				
	[E.23] Errores de mantenimiento / actualización de equipos (hardware)	**B**	**80%**				
	[E.24] caída del sistema por agotamiento de recursos	**MB**	**100%**				
	[E.25] Pérdida de equipos	**MB**	**100%**				
	[A.23] Manipulación del hardware	**B**	**80%**				
	[A.25] Robo de equipos	**MB**	**100%**				
	[A.26] Ataque destructivo	**MB**	**100%**				
Servidor UPI El Perdomo	[N.1] Fuego	**B**	**100%**				
	[N.2] Daños por agua	**B**	**100%**				

Tabla 14. (Continuación)

ACTIVOS	Amenazas	Probabilidad	Dimensiones				
			[D]	[I]	[C]	[A]	[T]
Servidor UPI El Perdomo	[N.*] Desastres naturales	**B**	**100%**				
	[I.5] Avería de origen físico o lógico	**MB**	**50%**				
	[I.6] Corte del suministro eléctrico	**A**	**75%**				
	[I.7] Condiciones inadecuadas de temperatura o humedad	**M**	**75%**				
	[E.2] Errores del administrador del sistema / de la seguridad	**MB**	**20%**	**20%**	**20%**		
	[E.4] Errores de configuración	**MB**	**50%**	**50%**	**50%**		
	[E.8] Difusión de software dañino	**M**	**70%**	**70%**			
	[E.23] Errores de mantenimiento / actualización de equipos (hardware)	**MB**	**10%**				
	[E.25] Pérdida de equipos	**MB**	**100%**				
	[A.6] Abuso de privilegios de acceso	**M**		**50%**	**50%**		
	[A.7] uso no previsto	**MB**	**15%**	**15%**	**15%**		
	[A.11] Acceso no autorizado	**MB**		**10%**	**80%**		
	[A.23] Manipulación del hardware	**M**	**50%**		**50%**		
	[A.24] Denegación de servicio	**B**	**75%**				
	[A.25] Robo de equipos	**MB**	**100%**				
	[A.26] Ataque destructivo	**MB**	**100%**				
Servidor UPI La 27 Sur	[N.1] Fuego	**B**	**100%**				
	[N.2] Daños por agua	**B**	**100%**				

Tabla 14. (Continuación)

ACTIVOS	Amenazas	Probabilidad	Dimensiones				
			[D]	[I]	[C]	[A]	[T]
Servidor UPI La 27 Sur	[N.*] Desastres naturales	**B**	**100%**				
	[I.5] Avería de origen físico o lógico	**MB**	**50%**				
	[I.6] Corte del suministro eléctrico	**A**	**75%**				
	[I.7] Condiciones inadecuadas de temperatura o humedad	**M**	**75%**				
	[E.2] Errores del administrador del sistema / de la seguridad	**MB**	**20%**	**20%**	**20%**		
	[E.4] Errores de configuración	**MB**	**50%**	**50%**	**50%**		
	[E.8] Difusión de software dañino	**M**	**70%**	**70%**			
	[E.23] Errores de mantenimiento / actualización de equipos (hardware)	**MB**	**10%**				
	[E.25] Pérdida de equipos	**MB**	**100%**				
	[A.6] Abuso de privilegios de acceso	**M**		**50%**	**50%**		
	[A.7] uso no previsto	**MB**	**15%**	**15%**	**15%**		
	[A.11] Acceso no autorizado	**MB**		**10%**	**80%**		
	[A.23] Manipulación del hardware	**M**	**50%**				
	[A.24] Denegación de servicio	**B**	**75%**				
	[A.25] Robo de equipos	**MB**	**100%**				
	[A.26] Ataque destructivo	**MB**	**100%**				
Servidor UPI La 32	[N.1] Fuego	**B**	**100%**				
	[N.2] Daños por agua	**B**	**100%**				
	[N.*] Desastres naturales	**B**	**100%**				

Tabla 14. (Continuación)

ACTIVOS	Amenazas	Probabilidad	Dimensiones				
			[D]	[I]	[C]	[A]	[T]
Servidor UPI La 32	[I.5] Avería de origen físico o lógico	**MB**	**50%**				
	[I.6] Corte del suministro eléctrico	**A**	**75%**				
	[I.7] Condiciones inadecuadas de temperatura o humedad	**M**	**75%**				
	[E.2] Errores del administrador del sistema / de la seguridad	**MB**	**20%**	**20%**	**20%**		
	[E.4] Errores de configuración	**MB**	**50%**	**50%**	**50%**		
	[E.8] Difusión de software dañino	**M**	**70%**	**70%**			
	[E.23] Errores de mantenimiento / actualización de equipos (hardware)	**MB**	**10%**				
	[E.25] Pérdida de equipos	**MB**	**100%**				
	[A.6] Abuso de privilegios de acceso	**M**		**50%**	**50%**		
	[A.7] uso no previsto	**MB**	**15%**	**15%**	**15%**		
	[A.11] Acceso no autorizado	**MB**		**10%**	**80%**		
	[A.23] Manipulación del hardware	**M**	**50%**				
	[A.24] Denegación de servicio	**B**	**75%**				
	[A.25] Robo de equipos	**MB**	**100%**				
	[A.26] Ataque destructivo	**MB**	**100%**				
Servidor UPI La Florida	[N.1] Fuego	**B**	**100%**				
	[N.2] Daños por agua	**B**	**100%**				
	[N.*] Desastres naturales	**B**	**100%**				

Tabla 14. (Continuación)

ACTIVOS	Amenazas	Probabilidad	Dimensiones				
			[D]	[I]	[C]	[A]	[T]
Servidor UPI La Florida	[I.5] Avería de origen físico o lógico	**MB**	**50%**				
	[I.6] Corte del suministro eléctrico	**A**	**75%**				
	[I.7] Condiciones inadecuadas de temperatura o humedad	**M**	**75%**				
	[E.2] Errores del administrador del sistema / de la seguridad	**MB**	**20%**	**20%**	**20%**		
	[E.4] Errores de configuración	**MB**	**50%**	**50%**	**50%**		
	[E.8] Difusión de software dañino	**M**	**70%**	**70%**			
	[E.23] Errores de mantenimiento / actualización de equipos (hardware)	**MB**	**10%**				
	[E.25] Pérdida de equipos	**MB**	**100%**				
	[A.6] Abuso de privilegios de acceso	**M**		**50%**	**50%**		
	[A.7] uso no previsto	**MB**	**15%**	**15%**	**15%**		
	[A.11] Acceso no autorizado	**MB**		**10%**	**10%**		
	[A.23] Manipulación del hardware	**M**	**50%**				
	[A.24] Denegación de servicio	**B**	**75%**				
	[A.25] Robo de equipos	**MB**	**100%**				
	[A.26] Ataque destructivo	**MB**	**100%**				
Servidor UPI La Vega	[N.1] Fuego	**B**	**100%**				
	[N.2] Daños por agua	**B**	**100%**				
	[N.*] Desastres naturales	**B**	**100%**				

Tabla 14. (Continuación)

ACTIVOS	Amenazas	Probabilidad	Dimensiones				
			[D]	[I]	[C]	[A]	[T]
Servidor UPI La Vega	[I.5] Avería de origen físico o lógico	**MB**	**50%**				
	[I.6] Corte del suministro eléctrico	**A**	**75%**				
	[I.7] Condiciones inadecuadas de temperatura o humedad	**M**	**75%**				
	[E.2] Errores del administrador del sistema / de la seguridad	**MB**	**20%**	**20%**	**20%**		
	[E.4] Errores de configuración	**MB**	**50%**	**50%**	**50%**		
	[E.8] Difusión de software dañino	**M**	**70%**	**70%**			
	[E.23] Errores de mantenimiento / actualización de equipos (hardware)	**MB**	**10%**				
	[E.25] Pérdida de equipos	**MB**	**100%**				
	[A.6] Abuso de privilegios de acceso	**M**		**50%**	**50%**		
	[A.7] uso no previsto	**MB**	**15%**	**15%**	**15%**		
	[A.11] Acceso no autorizado	**MB**		**10%**	**10%**		
	[A.23] Manipulación del hardware	**M**	**50%**				
	[A.24] Denegación de servicio	**B**	**75%**				
	[A.25] Robo de equipos	**MB**	**100%**				
	[A.26] Ataque destructivo	**MB**	**100%**				
Access Point	[N.1] Fuego	**MB**	**100%**				
	[N.2] Daños por agua	**B**	**100%**				
	[N.*] Desastres naturales	**MB**	**100%**				
	[I.5.3] Equipos de comunicaciones	**M**	**100%**				

Tabla 14. (Continuación)

ACTIVOS	Amenazas	Probabilidad	Dimensiones				
			[D]	[I]	[C]	[A]	[T]
Access Point	[I.7] Condiciones inadecuadas de temperatura o humedad	**MB**	**100%**				
	[I.8] Fallo de servicios de comunicaciones	**M**	**50%**		**50%**		
	[E.2] Errores del administrador del sistema / de la seguridad	**B**	**50%**		**50%**		
	[E.4] Errores de configuración	**B**	**50%**		**50%**		
	[E.19] Fugas de información	**MB**	**50%**		**70%**		
	[E.23] Errores de mantenimiento / actualización de equipos (hardware)	**B**	**50%**		**50%**		
	[E.25] Pérdida de equipos	**M**	**100%**				
	[A.5] suplantación de la identidad del usuario	**MB**	**50%**		**80%**	**100%**	
	[A.11] Acceso no autorizado	**M**	**50%**		**80%**	**100%**	
	[A.23] Manipulación del hardware	**B**	**50%**		**70%**		
	[A.24.1] Saturación de los canales de comunicaciones	**M**	**30%**				
	[A.25] Robo de equipos	**B**	**100%**				
Servidor UPI La Arcadia	[N.1] Fuego	**B**	**100%**				
	[N.2] Daños por agua	**B**	**100%**				
	[N.*] Desastres naturales	**B**	**100%**				
	[I.5] Avería de origen físico o lógico	**MB**	**50%**				
	[I.6] Corte del suministro eléctrico	**A**	**75%**				

Tabla 14. (Continuación)

ACTIVOS	Amenazas	Probabilidad	Dimensiones				
			[D]	[I]	[C]	[A]	[T]
Servidor UPI La Arcadia	[I.7] Condiciones inadecuadas de temperatura o humedad	**M**	**75%**				
	[E.2] Errores del administrador del sistema / de la seguridad	**MB**	**20%**	**20%**	**20%**		
	[E.4] Errores de configuración	**MB**	**50%**	**50%**	**50%**		
	[E.8] Difusión de software dañino	**M**	**70%**	**70%**			
	[E.23] Errores de mantenimiento / actualización de equipos (hardware)	**MB**	**10%**				
	[E.25] Pérdida de equipos	**MB**	**100%**				
	[A.6] Abuso de privilegios de acceso	**M**		**50%**	**50%**		
	[A.7] uso no previsto	**MB**	**15%**	**15%**	**15%**		
	[A.11] Acceso no autorizado	**MB**		**10%**	**10%**		
	[A.23] Manipulación del hardware	**M**	**50%**				
	[A.24] Denegación de servicio	**B**	**75%**				
	[A.25] Robo de equipos	**MB**	**100%**				
	[A.26] Ataque destructivo	**MB**	**100%**				
Equipos de cómputo	[N.1] Fuego	**MB**	**100%**	**90%**	**70%**	**80%**	
	[N.2] Daños por agua	**MB**	**100%**	**90%**	**70%**	**80%**	
	[N.*] Desastres naturales	**MB**	**100%**	**90%**	**70%**	**80%**	
	[I.1] Fuego	**MB**	**100%**	**90%**	**70%**	**80%**	
	[I.2] Daños por agua	**MB**	**100%**	**90%**	**70%**	**80%**	
	[I.*] Desastres industriales	**MB**	**100%**	**90%**	**70%**	**80%**	

Tabla 14. (Continuación)

ACTIVOS	Amenazas	Probabilidad	Dimensiones				
			[D]	[I]	[C]	[A]	[T]
Equipos de cómputo	[I.3] Contaminación medioambiental	**MB**	**90%**	**90%**	**70%**	**70%**	
	[I.5] Avería de origen físico o lógico	**A**	**60%**	**60%**	**70%**	**70%**	
	[I.6] Corte del suministro eléctrico	**A**	**30%**	**70%**	**20%**	**20%**	
	[I.7] Condiciones inadecuadas de temperatura o humedad	**M**	**40%**	**40%**	**30%**	**30%**	
	[E.23] Errores de mantenimiento / actualización de equipos (hardware)	**MA**	**70%**	**70%**	**40%**	**20%**	
	[E.25] Pérdida de equipos	**B**	**100%**	**100%**	**100%**	**100%**	
	[A.6] Abuso de privilegios de acceso	**A**	**10%**	**90%**	**90%**	**10%**	
	[A.7] uso no previsto	**A**	**10%**	**90%**	**90%**	**10%**	
	[A.11] Acceso no autorizado	**M**	**10%**	**90%**	**90%**	**10%**	
	[A.23] Manipulación del hardware	**M**	**90%**	**90%**	**10%**	**10%**	
	[A.25] Robo de equipos	**M**	**100%**	**100%**	**100%**	**100%**	
	[A.26] Ataque destructivo	**MB**	**70%**	**90%**	**70%**	**60%**	
Servidor UPI San Francisco	[N.1] Fuego	**B**	**100%**				
	[N.2] Daños por agua	**B**	**100%**				
	[N.*] Desastres naturales	**B**	**100%**				
	[I.5] Avería de origen físico o lógico	**MB**	**50%**				
	[I.6] Corte del suministro eléctrico	**A**	**75%**				
	[I.7] Condiciones inadecuadas de temperatura o humedad	**M**	**75%**				

Tabla 14. (Continuación)

ACTIVOS	Amenazas	Probabilidad	Dimensiones				
			[D]	[I]	[C]	[A]	[T]
Servidor UPI San Francisco	[E.2] Errores del administrador del sistema / de la seguridad	**MB**	**20%**	**20%**	**20%**		
	[E.4] Errores de configuración	**MB**	**50%**	**50%**	**50%**		
	[E.8] Difusión de software dañino	**M**	**70%**	**70%**			
	[E.23] Errores de mantenimiento / actualización de equipos (hardware)	**MB**	**10%**				
	[E.25] Pérdida de equipos	**MB**	**100%**		**100%**		
	[A.6] Abuso de privilegios de acceso	**M**		**50%**	**50%**		
	[A.7] uso no previsto	**MB**	**15%**	**15%**	**15%**		
	[A.11] Acceso no autorizado	**MB**		**10%**	**80%**		
	[A.23] Manipulación del hardware	**M**	**50%**		**50%**		
	[A.24] Denegación de servicio	**B**	**75%**				
	[A.24.3] Saturación de los recursos hardware	**MB**	**50%**				
	[A.25] Robo de equipos	**MB**	**100%**		**100%**		
	[A.26] Ataque destructivo	**MB**	**100%**				
Switch de borde 4210G	[N.2] Daños por agua	**MB**	**100%**				
	[N.*] Desastres naturales	**MB**	**100%**				
	[I.1] Fuego	**MB**	**100%**				
	[I.3] Contaminación medioambiental	**B**	**70%**				
	[I.6] Corte del suministro eléctrico	**M**	**70%**				

Tabla 14. (Continuación)

ACTIVOS	Amenazas	Probabilidad	Dimensiones				
			[D]	[I]	[C]	[A]	[T]
Switch de borde 4210G	[I.7] Condiciones inadecuadas de temperatura o humedad	**B**	**10%**				
	[E.2] Errores del administrador del sistema / de la seguridad	**MB**	**10%**				
	[E.4] Errores de configuración	**B**	**10%**				
	[E.23] Errores de mantenimiento / actualización de equipos (hardware)	**B**	**10%**				
	[A.7] uso no previsto	**MB**	**5%**				
	[A.11] Acceso no autorizado	**MB**	**10%**				
	[A.23] Manipulación del hardware	**MB**	**10%**				
	[A.25] Robo de equipos	**MB**	**100%**				
Sistema de almacenamiento formato rack	[I.6.12] Interrupción deliberada por un agente externo	**M**	**100%**	**100%**			
Gabinete de 8 blades	[E.23] Errores de mantenimiento / actualización de equipos (hardware)	**MB**	**90%**	**90%**			
	[E.24] caída del sistema por agotamiento de recursos	**B**	**100%**	**100%**			
Equipo de Seguridad Perimetral	[N.1] Fuego	**B**	**100%**	**100%**			
	[N.2] Daños por agua	**B**	**100%**	**100%**			
	[N.*] Desastres naturales	**B**	**100%**	**100%**			
	[E.2] Errores del administrador del sistema / de la seguridad	**M**	**80%**	**100%**	**90%**		
	[E.3] Errores de monitorización (log)	**M**		**70%**	**100%**		**80%**

Tabla 14. (Continuación)

ACTIVOS	Amenazas	Probabilidad	Dimensiones				
			[D]	[I]	[C]	[A]	[T]
Equipo de Seguridad Perimetral	[E.4] Errores de configuración	**M**	**80%**	**80%**	**80%**		**20%**
	[E.21] Errores de mantenimiento / actualización de programas (software)	**M**	**80%**	**80%**	**80%**		**20%**
	[A.3] Manipulación de los registros de actividad (log)	**B**		**60%**	**80%**		**100%**
	[A.11] Acceso no autorizado	**MB**	**80%**	**90%**	**100%**	**90%**	
	[A.12] Análisis de tráfico	**B**		**80%**	**80%**		
	[A.23] Manipulación del hardware	**B**	**90%**	**90%**	**80%**		
	[A.24] Denegación de servicio	**MB**	**100%**	**100%**			
Servidor formato blade marca Hewlett Packard Modelo proliant BL460C G1	[N.1] Fuego	**B**	**100%**				
	[N.2] Daños por agua	**B**	**100%**				
	[N.*] Desastres naturales	**B**	**100%**				
	[I.5] Avería de origen físico o lógico	**MB**	**50%**				
	[I.6] Corte del suministro eléctrico	**A**	**75%**				
	[I.7] Condiciones inadecuadas de temperatura o humedad	**M**	**75%**				
	[E.2] Errores del administrador del sistema / de la seguridad	**MB**	**20%**	**20%**	**20%**		
	[E.4] Errores de configuración	**MB**	**50%**	**50%**	**50%**		
	[E.8] Difusión de software dañino	**M**	**70%**	**70%**			
	[E.23] Errores de mantenimiento / actualización de equipos (hardware)	**MB**	**10%**				

Tabla 14. (Continuación)

ACTIVOS	Amenazas	Probabilidad	Dimensiones				
			[D]	[I]	[C]	[A]	[T]
Servidor formato blade marca Hewlett Packard Modelo proliant BL460C G1	[E.25] Pérdida de equipos	**MB**	**100%**		**100%**		
	[A.6] Abuso de privilegios de acceso	**B**		**50%**	**50%**		
	[A.7] uso no previsto	**MB**	**15%**	**15%**	**15%**		
	[A.11] Acceso no autorizado	**MB**		**10%**	**80%**		
	[A.23] Manipulación del hardware	**M**	**50%**		**50%**		
	[A.24] Denegación de servicio	**B**	**75%**				
	[A.24.3] Saturación de los recursos hardware	**MB**	**50%**				
	[A.25] Robo de equipos	**MB**	**100%**		**100%**		
	[A.26] Ataque destructivo	**MB**	**100%**				
Servidor formato blade marca Hewlett Packard. Modelo proliant BL460C G7	[N.1] Fuego	**B**	**100%**				
	[N.2] Daños por agua	**B**	**100%**				
	[N.*] Desastres naturales	**B**	**100%**				
	[I.5] Avería de origen físico o lógico	**MB**	**50%**				
	[I.6] Corte del suministro eléctrico	**A**	**75%**				
	[I.7] Condiciones inadecuadas de temperatura o humedad	**M**	**75%**				
	[E.2] Errores del administrador del sistema / de la seguridad	**MB**	**20%**	**20%**	**20%**		
	[E.4] Errores de configuración	**MB**	**50%**	**50%**	**50%**		
	[E.8] Difusión de software dañino	**M**	**70%**	**70%**			

Tabla 14. (Continuación)

ACTIVOS	Amenazas	Probabilidad	Dimensiones				
			[D]	[I]	[C]	[A]	[T]
Servidor formato blade marca Hewlett Packard. Modelo proliant BL460C G7	[E.23] Errores de mantenimiento / actualización de equipos (hardware)	**MB**	**10%**				
	[E.25] Pérdida de equipos	**MB**	**100%**		**100%**		
	[A.6] Abuso de privilegios de acceso	**B**		**50%**	**50%**		
	[A.7] uso no previsto	**MB**	**15%**	**15%**	**15%**		
	[A.11] Acceso no autorizado	**MB**		**10%**	**80%**		
	[A.23] Manipulación del hardware	**M**	**50%**		**50%**		
	[A.24] Denegación de servicio	**B**	**75%**				
	[A.24.3] Saturación de los recursos hardware	**MB**	**50%**				
	[A.25] Robo de equipos	**MB**	**100%**		**100%**		
	[A.26] Ataque destructivo	**MB**	**100%**				
Servidor Proliant 120 G5	[N.1] Fuego	**B**	**100%**				
	[N.2] Daños por agua	**B**	**100%**				
	[N.*] Desastres naturales	**B**	**100%**				
	[I.5] Avería de origen físico o lógico	**MB**	**50%**				
	[I.6] Corte del suministro eléctrico	**A**	**75%**				
	[I.7] Condiciones inadecuadas de temperatura o humedad	**M**	**75%**				
	[E.2] Errores del administrador del sistema / de la seguridad	**MB**	**20%**	**20%**	**20%**		
	[E.4] Errores de configuración	**MB**	**50%**	**50%**	**50%**		

Tabla 14. (Continuación)

ACTIVOS	Amenazas	Probabilidad	Dimensiones				
			[D]	[I]	[C]	[A]	[T]
Servidor Proliant 120 G5	[E.8] Difusión de software dañino	**M**	**70%**	**70%**			
	[E.23] Errores de mantenimiento / actualización de equipos (hardware)	**MB**	**10%**				
	[E.25] Pérdida de equipos	**MB**	**100%**		**100%**		
	[A.6] Abuso de privilegios de acceso	**B**		**50%**	**50%**		
	[A.7] uso no previsto	**MB**	**15%**	**15%**	**15%**		
	[A.11] Acceso no autorizado	**MB**		**10%**	**80%**		
	[A.23] Manipulación del hardware	**M**	**50%**		**50%**		
	[A.24] Denegación de servicio	**B**	**75%**				
	[A.24.3] Saturación de los recursos hardware	**MB**	**50%**				
	[A.25] Robo de equipos	**MB**	**100%**		**100%**		
	[A.26] Ataque destructivo	**MB**	**100%**				
Servidor Proyecto Misión Bogotá	[N.1] Fuego	**B**	**100%**				
	[N.2] Daños por agua	**B**	**100%**				
	[N.*] Desastres naturales	**B**	**100%**				
	[I.5] Avería de origen físico o lógico	**MB**	**50%**				
	[I.6] Corte del suministro eléctrico	**A**	**75%**				
	[I.7] Condiciones inadecuadas de temperatura o humedad	**M**	**75%**				
	[E.2] Errores del administrador del sistema / de la seguridad	**MB**	**20%**	**20%**	**20%**		

Tabla 14. (Continuación)

ACTIVOS	Amenazas	Probabilidad	Dimensiones				
			[D]	[I]	[C]	[A]	[T]
Servidor Proyecto Misión Bogotá	[E.4] Errores de configuración	**MB**	**50%**	**50%**	**50%**		
	[E.8] Difusión de software dañino	**M**	**70%**	**70%**			
	[E.23] Errores de mantenimiento / actualización de equipos (hardware)	**MB**	**10%**				
	[E.25] Pérdida de equipos	**MB**	**100%**		**100%**		
	[A.6] Abuso de privilegios de acceso	**B**		**50%**	**50%**		
	[A.7] uso no previsto	**MB**	**15%**	**15%**	**15%**		
	[A.11] Acceso no autorizado	**MB**		**10%**	**80%**		
	[A.23] Manipulación del hardware	**M**	**50%**		**50%**		
	[A.24] Denegación de servicio	**B**	**75%**				
	[A.24.3] Saturación de los recursos hardware	**MB**	**50%**				
	[A.25] Robo de equipos	**MB**	**100%**		**100%**		
	[A.26] Ataque destructivo	**MB**	**100%**				
Impresora para código de barras	[N.1] Fuego	**MB**	**100%**				
	[N.2] Daños por agua	**MB**	**100%**				
	[N.*] Desastres naturales	**MB**	**100%**				
	[I.1] Fuego	**MB**	**100%**				
	[I.2] Daños por agua	**MB**	**100%**				
	[I.*] Desastres industriales	**MB**	**100%**				
	[I.3] Contaminación medioambiental	**MB**	**100%**				
	[I.4] Contaminación electromagnética	**MB**	**50%**				

Tabla 14. (Continuación)

ACTIVOS	Amenazas	Probabilidad	Dimensiones				
			[D]	[I]	[C]	[A]	[T]
Impresora para código de barras	[I.5] Avería de origen físico o lógico	**M**	**50%**				
	[I.6] Corte del suministro eléctrico	**B**	**100%**				
	[I.7] Condiciones inadecuadas de temperatura o humedad	**MB**	**100%**				
	[E.2] Errores del administrador del sistema / de la seguridad	**MB**	**10%**				
	[E.23] Errores de mantenimiento / actualización de equipos (hardware)	**B**	**10%**				
	[E.24] caída del sistema por agotamiento de recursos	**MB**	**80%**				
	[E.25] Pérdida de equipos	**MB**	**100%**				
	[A.23] Manipulación del hardware	**B**	**100%**				
	[A.25] Robo de equipos	**MB**	**80%**				
	[A.26] Ataque destructivo	**MB**	**100%**				
Servidor controlador de dominio principal	[N.1] Fuego	**B**	**100%**				
	[N.2] Daños por agua	**B**	**100%**				
	[N.*] Desastres naturales	**B**	**100%**				
	[I.5] Avería de origen físico o lógico	**MB**	**50%**				
	[I.6] Corte del suministro eléctrico	**A**	**75%**				
	[I.7] Condiciones inadecuadas de temperatura o humedad	**M**	**75%**				

Tabla 14. (Continuación)

ACTIVOS	Amenazas	Probabilidad	Dimensiones				
			[D]	[I]	[C]	[A]	[T]
Servidor controlador de dominio principal	[E.2] Errores del administrador del sistema / de la seguridad	**MB**	**20%**	**20%**	**20%**		
	[E.4] Errores de configuración	**MB**	**50%**	**50%**	**50%**		
	[E.8] Difusión de software dañino	**M**	**70%**	**70%**			
	[E.23] Errores de mantenimiento / actualización de equipos (hardware)	**MB**	**10%**				
	[E.25] Pérdida de equipos	**MB**	**100%**		**100%**		
	[A.6] Abuso de privilegios de acceso	**B**		**50%**	**50%**		
	[A.7] uso no previsto	**MB**	**15%**	**15%**	**15%**		
	[A.11] Acceso no autorizado	**MB**		**10%**	**80%**		
	[A.23] Manipulación del hardware	**M**	**50%**		**50%**		
	[A.24] Denegación de servicio	**B**	**75%**				
	[A.24.3] Saturación de los recursos hardware	**MB**	**50%**				
	[A.25] Robo de equipos	**MB**	**100%**		**100%**		
	[A.26] Ataque destructivo	**MB**	**100%**				
Switch de borde 4800	[N.2] Daños por agua	**MB**	**100%**				
	[N.*] Desastres naturales	**MB**	**100%**				
	[I.1] Fuego	**MB**	**100%**				
	[I.3] Contaminación medioambiental	**B**	**70%**				
	[I.6] Corte del suministro eléctrico	**M**	**70%**				

Tabla 14. (Continuación)

ACTIVOS	Amenazas	Probabilidad	Dimensiones				
			[D]	[I]	[C]	[A]	[T]
Switch de borde 4800	[I.7] Condiciones inadecuadas de temperatura o humedad	**B**	**10%**				
	[E.2] Errores del administrador del sistema / de la seguridad	**MB**	**10%**				
	[E.4] Errores de configuración	**B**	**10%**				
	[E.23] Errores de mantenimiento / actualización de equipos (hardware)	**B**	**10%**				
	[A.7] uso no previsto	**MB**	**5%**				
	[A.11] Acceso no autorizado	**MB**	**10%**				
	[A.23] Manipulación del hardware	**MB**	**10%**				
	[A.25] Robo de equipos	**MB**	**100%**				
Switch de borde - Referencia 2410 - UPI La Rioja	[N.2] Daños por agua	**MB**	**100%**				
	[N.*] Desastres naturales	**MB**	**100%**				
	[I.1] Fuego	**MB**	**100%**				
	[I.3] Contaminación medioambiental	**B**	**70%**				
	[I.6] Corte del suministro eléctrico	**M**	**70%**				
	[I.7] Condiciones inadecuadas de temperatura o humedad	**B**	**10%**				
	[E.2] Errores del administrador del sistema / de la seguridad	**MB**	**10%**				
	[E.4] Errores de configuración	**B**	**10%**				
	[E.23] Errores de mantenimiento / actualización de equipos (hardware)	**B**	**10%**				

Tabla 14. (Continuación)

ACTIVOS	Amenazas	Probabilidad	Dimensiones				
			[D]	[I]	[C]	[A]	[T]
Switch de borde - Referencia 2410 - UPI La Rioja	[A.7] uso no previsto	**MB**	**5%**				
	[A.11] Acceso no autorizado	**MB**	**10%**				
	[A.23] Manipulación del hardware	**MB**	**10%**				
	[A.25] Robo de equipos	**MB**	**100%**				
Switch de borde - Referencia 2920 - Proyecto Misión Bogotá	[N.2] Daños por agua	**MB**	**100%**				
	[N.*] Desastres naturales	**MB**	**100%**				
	[I.1] Fuego	**MB**	**100%**				
	[I.3] Contaminación medioambiental	**B**	**70%**				
	[I.6] Corte del suministro eléctrico	**M**	**70%**				
	[I.7] Condiciones inadecuadas de temperatura o humedad	**B**	**10%**				
	[E.2] Errores del administrador del sistema / de la seguridad	**MB**	**10%**				
	[E.4] Errores de configuración	**B**	**10%**				
	[E.23] Errores de mantenimiento / actualización de equipos (hardware)	**B**	**10%**				
	[A.7] uso no previsto	**MB**	**5%**				
	[A.11] Acceso no autorizado	**MB**	**10%**				
	[A.23] Manipulación del hardware	**MB**	**10%**				
	[A.25] Robo de equipos	**MB**	**100%**				
Switch de borde - Referencia 4250T	[N.2] Daños por agua	**MB**	**100%**				

Tabla 14. (Continuación)

ACTIVOS	Amenazas	Probabilidad	Dimensiones				
			[D]	[I]	[C]	[A]	[T]
Switch de borde - Referencia 4250T	[N.*] Desastres naturales	**MB**	**100%**				
	[I.1] Fuego	**MB**	**100%**				
	[I.3] Contaminación medioambiental	**B**	**70%**				
	[I.6] Corte del suministro eléctrico	**M**	**70%**				
	[I.7] Condiciones inadecuadas de temperatura o humedad	**B**	**10%**				
	[E.2] Errores del administrador del sistema / de la seguridad	**MB**	**10%**				
	[E.4] Errores de configuración	**B**	**10%**				
	[E.23] Errores de mantenimiento / actualización de equipos (hardware)	**B**	**10%**				
	[A.7] uso no previsto	**MB**	**5%**				
	[A.11] Acceso no autorizado	**MB**	**10%**				
	[A.23] Manipulación del hardware	**MB**	**10%**				
	[A.25] Robo de equipos	**MB**	**100%**				
Switch de borde - Referencia 4500G UPI La Florida	[N.2] Daños por agua	**MB**	**100%**				
	[N.*] Desastres naturales	**MB**	**100%**				
	[I.1] Fuego	**MB**	**100%**				
	[I.3] Contaminación medioambiental	**B**	**70%**				
	[I.6] Corte del suministro eléctrico	**M**	**70%**				
	[I.7] Condiciones inadecuadas de temperatura o humedad	**B**	**10%**				

Tabla 14. (Continuación)

ACTIVOS	Amenazas	Probabilidad	Dimensiones				
			[D]	[I]	[C]	[A]	[T]
Switch de borde - Referencia 4500G UPI La Florida	[E.2] Errores del administrador del sistema / de la seguridad	**MB**	**10%**				
	[E.4] Errores de configuración	**B**	**10%**				
	[E.23] Errores de mantenimiento / actualización de equipos (hardware)	**B**	**10%**				
	[A.7] uso no previsto	**MB**	**5%**				
	[A.11] Acceso no autorizado	**MB**	**10%**				
	[A.23] Manipulación del hardware	**MB**	**10%**				
	[A.25] Robo de equipos	**MB**	**100%**				
Switch de borde - Referencia 4800G - UPI La 32	[N.2] Daños por agua	**MB**	**100%**				
	[N.*] Desastres naturales	**MB**	**100%**				
	[I.1] Fuego	**MB**	**100%**				
	[I.3] Contaminación medioambiental	**B**	**70%**				
	[I.6] Corte del suministro eléctrico	**M**	**70%**				
	[I.7] Condiciones inadecuadas de temperatura o humedad	**B**	**10%**				
	[E.2] Errores del administrador del sistema / de la seguridad	**MB**	**10%**				
	[E.4] Errores de configuración	**B**	**10%**				
	[E.23] Errores de mantenimiento / actualización de equipos (hardware)	**B**	**10%**				
	[A.7] uso no previsto	**MB**	**5%**				

Tabla 14. (Continuación)

ACTIVOS	Amenazas	Probabilidad	Dimensiones				
			[D]	[I]	[C]	[A]	[T]
Switch de borde - Referencia 4800G - UPI La 32	[A.11] Acceso no autorizado	**MB**	**10%**				
	[A.23] Manipulación del hardware	**MB**	**10%**				
	[A.25] Robo de equipos	**MB**	**100%**				
Switch de borde - Referencia 4800G - UPI El Perdomo	[N.2] Daños por agua	**MB**	**100%**				
	[N.*] Desastres naturales	**MB**	**100%**				
	[I.1] Fuego	**MB**	**100%**				
	[I.3] Contaminación medioambiental	**B**	**70%**				
	[I.6] Corte del suministro eléctrico	**M**	**70%**				
	[I.7] Condiciones inadecuadas de temperatura o humedad	**B**	**10%**				
	[E.2] Errores del administrador del sistema / de la seguridad	**MB**	**10%**				
	[E.4] Errores de configuración	**B**	**10%**				
	[E.23] Errores de mantenimiento / actualización de equipos (hardware)	**B**	**10%**				
	[A.7] uso no previsto	**MB**	**5%**				
	[A.11] Acceso no autorizado	**MB**	**10%**				
	[A.23] Manipulación del hardware	**MB**	**10%**				
	[A.25] Robo de equipos	**MB**	**100%**				
Switch de borde - Referencia 4800G - UPI La Florida	[N.2] Daños por agua	**MB**	**100%**				
	[N.*] Desastres naturales	**MB**	**100%**				

Tabla 14. (Continuación)

ACTIVOS	Amenazas	Probabilidad	Dimensiones				
			[D]	[I]	[C]	[A]	[T]
Switch de borde - Referencia 4800G - UPI La Florida	[I.1] Fuego	**MB**	**100%**				
	[I.3] Contaminación medioambiental	**B**	**70%**				
	[I.6] Corte del suministro eléctrico	**M**	**70%**				
	[I.7] Condiciones inadecuadas de temperatura o humedad	**B**	**10%**				
	[E.2] Errores del administrador del sistema / de la seguridad	**MB**	**10%**				
	[E.4] Errores de configuración	**B**	**10%**				
	[E.23] Errores de mantenimiento / actualización de equipos (hardware)	**B**	**10%**				
	[A.7] uso no previsto	**MB**	**5%**				
	[A.11] Acceso no autorizado	**MB**	**10%**				
	[A.23] Manipulación del hardware	**MB**	**10%**				
	[A.25] Robo de equipos	**MB**	**100%**				
Switch de borde - Referencia 4800G - UPI La 27 sur	[N.2] Daños por agua	**MB**	**100%**				
	[N.*] Desastres naturales	**MB**	**100%**				
	[I.1] Fuego	**MB**	**100%**				
	[I.3] Contaminación medioambiental	**B**	**70%**				
	[I.6] Corte del suministro eléctrico	**M**	**70%**				
	[I.7] Condiciones inadecuadas de temperatura o humedad	**B**	**10%**				

Tabla 14. (Continuación)

ACTIVOS	Amenazas	Probabilidad	Dimensiones				
			[D]	[I]	[C]	[A]	[T]
Switch de borde - Referencia 4800G - UPI La 27 sur	[E.2] Errores del administrador del sistema / de la seguridad	**MB**	**10%**				
	[E.4] Errores de configuración	**B**	**10%**				
	[E.23] Errores de mantenimiento / actualización de equipos (hardware)	**B**	**10%**				
	[A.7] uso no previsto	**MB**	**5%**				
	[A.11] Acceso no autorizado	**MB**	**10%**				
	[A.23] Manipulación del hardware	**MB**	**10%**				
	[A.25] Robo de equipos	**MB**	**100%**				
Switch de borde - Referencia 4800G - UPI San Francisco	[N.2] Daños por agua	**MB**	**100%**				
	[N.*] Desastres naturales	**MB**	**100%**				
	[I.1] Fuego	**MB**	**100%**				
	[I.3] Contaminación medioambiental	**B**	**70%**				
	[I.6] Corte del suministro eléctrico	**M**	**70%**				
	[I.7] Condiciones inadecuadas de temperatura o humedad	**B**	**10%**				
	[E.2] Errores del administrador del sistema / de la seguridad	**MB**	**10%**				
	[E.4] Errores de configuración	**B**	**10%**				
	[E.23] Errores de mantenimiento / actualización de equipos (hardware)	**B**	**10%**				
	[A.7] uso no previsto	**MB**	**5%**				

Tabla 14. (Continuación)

ACTIVOS	Amenazas	Probabilidad	Dimensiones				
			[D]	[I]	[C]	[A]	[T]
Switch de borde - Referencia 4800G - UPI San Francisco	[A.11] Acceso no autorizado	**MB**	**10%**				
	[A.23] Manipulación del hardware	**MB**	**10%**				
	[A.25] Robo de equipos	**MB**	**100%**				
Switch de borde - Referencia 4800G - UPI La Rioja	[N.2] Daños por agua	**MB**	**100%**				
	[N.*] Desastres naturales	**MB**	**100%**				
	[I.1] Fuego	**MB**	**100%**				
	[I.3] Contaminación medioambiental	**B**	**70%**				
	[I.6] Corte del suministro eléctrico	**M**	**70%**				
	[I.7] Condiciones inadecuadas de temperatura o humedad	**B**	**10%**				
	[E.2] Errores del administrador del sistema / de la seguridad	**MB**	**10%**				
	[E.4] Errores de configuración	**B**	**10%**				
	[E.23] Errores de mantenimiento / actualización de equipos (hardware)	**B**	**10%**				
	[A.7] uso no previsto	**MB**	**5%**				
	[A.11] Acceso no autorizado	**MB**	**10%**				
	[A.23] Manipulación del hardware	**MB**	**10%**				
	[A.25] Robo de equipos	**MB**	**100%**				
Switch de borde - Referencia 4800G - UPI La Vega	[N.2] Daños por agua	**MB**	**100%**				
	[N.*] Desastres naturales	**MB**	**100%**				

Tabla 14. (Continuación)

ACTIVOS	Amenazas	Probabilidad	Dimensiones				
			[D]	[I]	[C]	[A]	[T]
Switch de borde - Referencia 4800G - UPI La Vega	[I.1] Fuego	**MB**	**100%**				
	[I.3] Contaminación medioambiental	**B**	**70%**				
	[I.6] Corte del suministro eléctrico	**M**	**70%**				
	[I.7] Condiciones inadecuadas de temperatura o humedad	**B**	**10%**				
	[E.2] Errores del administrador del sistema / de la seguridad	**MB**	**10%**				
	[E.4] Errores de configuración	**B**	**10%**				
	[E.23] Errores de mantenimiento / actualización de equipos (hardware)	**B**	**10%**				
	[A.7] uso no previsto	**MB**	**5%**				
	[A.11] Acceso no autorizado	**MB**	**10%**				
	[A.23] Manipulación del hardware	**MB**	**10%**				
	[A.25] Robo de equipos	**MB**	**100%**				
Switch de borde - Referencia 4800G - UPI Santa Lucia	[N.2] Daños por agua	**MB**	**100%**				
	[N.*] Desastres naturales	**MB**	**100%**				
	[I.1] Fuego	**MB**	**100%**				
	[I.3] Contaminación medioambiental	**B**	**70%**				
	[I.6] Corte del suministro eléctrico	**M**	**70%**				
	[I.7] Condiciones inadecuadas de temperatura o humedad	**B**	**10%**				

Tabla 14. (Continuación)

ACTIVOS	Amenazas	Probabilidad	Dimensiones				
			[D]	[I]	[C]	[A]	[T]
Switch de borde - Referencia 4800G - UPI Santa Lucia	[E.2] Errores del administrador del sistema / de la seguridad	**MB**	**10%**				
	[E.4] Errores de configuración	**B**	**10%**				
	[E.23] Errores de mantenimiento / actualización de equipos (hardware)	**B**	**10%**				
	[A.7] uso no previsto	**MB**	**5%**				
	[A.11] Acceso no autorizado	**MB**	**10%**				
	[A.23] Manipulación del hardware	**MB**	**10%**				
	[A.25] Robo de equipos	**MB**	**100%**				
Switch de borde - Referencia 4800G - UPI Servitá	[N.2] Daños por agua	**MB**	**100%**				
	[N.*] Desastres naturales	**MB**	**100%**				
	[I.1] Fuego	**MB**	**100%**				
	[I.3] Contaminación medioambiental	**B**	**70%**				
	[I.6] Corte del suministro eléctrico	**M**	**70%**				
	[I.7] Condiciones inadecuadas de temperatura o humedad	**B**	**10%**				
	[E.2] Errores del administrador del sistema / de la seguridad	**MB**	**10%**				
	[E.4] Errores de configuración	**B**	**10%**				
	[E.23] Errores de mantenimiento / actualización de equipos (hardware)	**B**	**10%**				
	[A.7] uso no previsto	**MB**	**5%**				

Tabla 14. (Continuación)

ACTIVOS	Amenazas	Probabilidad	Dimensiones				
			[D]	[I]	[C]	[A]	[T]
Switch de borde - Referencia 4800G - UPI Servitá	[A.11] Acceso no autorizado	**MB**	**10%**				
	[A.23] Manipulación del hardware	**MB**	**10%**				
	[A.25] Robo de equipos	**MB**	**100%**				
Switch de borde - Referencia E2910 HP - UPI Bosa	[N.2] Daños por agua	**MB**	**100%**				
	[N.*] Desastres naturales	**MB**	**100%**				
	[I.1] Fuego	**MB**	**100%**				
	[I.3] Contaminación medioambiental	**B**	**70%**				
	[I.6] Corte del suministro eléctrico	**M**	**70%**				
	[I.7] Condiciones inadecuadas de temperatura o humedad	**B**	**10%**				
	[E.2] Errores del administrador del sistema / de la seguridad	**MB**	**10%**				
	[E.4] Errores de configuración	**B**	**10%**				
	[E.23] Errores de mantenimiento / actualización de equipos (hardware)	**B**	**10%**				
	[A.7] uso no previsto	**MB**	**5%**				
	[A.11] Acceso no autorizado	**MB**	**10%**				
	[A.23] Manipulación del hardware	**MB**	**10%**				
	[A.25] Robo de equipos	**MB**	**100%**				
Switch de borde - Referencia E2910 HP - Proyecto 968	[N.2] Daños por agua	**MB**	**100%**				
	[N.*] Desastres naturales	**MB**	**100%**				

Tabla 14. (Continuación)

ACTIVOS	Amenazas	Probabilidad	Dimensiones				
			[D]	[I]	[C]	[A]	[T]
Switch de borde - Referencia E2910 HP - Proyecto 968	[I.1] Fuego	**MB**	**100%**				
	[I.3] Contaminación medioambiental	**B**	**70%**				
	[I.6] Corte del suministro eléctrico	**M**	**70%**				
	[I.7] Condiciones inadecuadas de temperatura o humedad	**B**	**10%**				
	[E.2] Errores del administrador del sistema / de la seguridad	**MB**	**10%**				
	[E.4] Errores de configuración	**B**	**10%**				
	[E.23] Errores de mantenimiento / actualización de equipos (hardware)	**B**	**10%**				
	[A.7] uso no previsto	**MB**	**5%**				
	[A.11] Acceso no autorizado	**MB**	**10%**				
	[A.23] Manipulación del hardware	**MB**	**10%**				
	[A.25] Robo de equipos	**MB**	**100%**				
Switch de borde - Referencia V1910 - Proyecto Misión Bogotá	[N.2] Daños por agua	**MB**	**100%**				
	[N.*] Desastres naturales	**MB**	**100%**				
	[I.1] Fuego	**MB**	**100%**				
	[I.3] Contaminación medioambiental	**B**	**70%**				
	[I.6] Corte del suministro eléctrico	**M**	**70%**				
	[I.7] Condiciones inadecuadas de temperatura o humedad	**B**	**10%**				

Tabla 14. (Continuación)

ACTIVOS	Amenazas	Probabilidad	Dimensiones				
			[D]	[I]	[C]	[A]	[T]
Switch de borde - Referencia V1910 - Proyecto Misión Bogotá	[E.2] Errores del administrador del sistema / de la seguridad	**MB**	**10%**				
	[E.4] Errores de configuración	**B**	**10%**				
	[E.23] Errores de mantenimiento / actualización de equipos (hardware)	**B**	**10%**				
	[A.7] uso no previsto	**MB**	**5%**				
	[A.11] Acceso no autorizado	**MB**	**10%**				
	[A.23] Manipulación del hardware	**MB**	**10%**				
	[A.25] Robo de equipos	**MB**	**100%**				
Switch de borde 4500G - Sede Administrativa	[N.2] Daños por agua	**MB**	**100%**				
	[N.*] Desastres naturales	**MB**	**100%**				
	[I.1] Fuego	**MB**	**100%**				
	[I.3] Contaminación medioambiental	**B**	**70%**				
	[I.6] Corte del suministro eléctrico	**M**	**70%**				
	[I.7] Condiciones inadecuadas de temperatura o humedad	**B**	**10%**				
	[E.2] Errores del administrador del sistema / de la seguridad	**MB**	**10%**				
	[E.4] Errores de configuración	**B**	**10%**				
	[E.23] Errores de mantenimiento / actualización de equipos (hardware)	**B**	**10%**				
	[A.7] uso no previsto	**MB**	**5%**				

Tabla 14. (Continuación)

ACTIVOS	Amenazas	Probabilidad	Dimensiones				
			[D]	[I]	[C]	[A]	[T]
Switch de borde 4500G - Sede Administrativa	[A.11] Acceso no autorizado	**MB**	**10%**				
	[A.23] Manipulación del hardware	**MB**	**10%**				
	[A.25] Robo de equipos	**MB**	**100%**				
Switch de borde. Referencia 4500G - UPI La Arcadia	[N.2] Daños por agua	**MB**	**100%**				
	[N.*] Desastres naturales	**MB**	**100%**				
	[I.1] Fuego	**MB**	**100%**				
	[I.3] Contaminación medioambiental	**B**	**70%**				
	[I.6] Corte del suministro eléctrico	**M**	**70%**				
	[I.7] Condiciones inadecuadas de temperatura o humedad	**B**	**10%**				
	[E.2] Errores del administrador del sistema / de la seguridad	**MB**	**10%**				
	[E.4] Errores de configuración	**B**	**10%**				
	[E.23] Errores de mantenimiento / actualización de equipos (hardware)	**B**	**10%**				
	[A.7] uso no previsto	**MB**	**5%**				
	[A.11] Acceso no autorizado	**MB**	**10%**				
	[A.23] Manipulación del hardware	**MB**	**10%**				
	[A.25] Robo de equipos	**MB**	**100%**				
Switch de borde. Referencia 4800G - UPI La Arcadia	[N.2] Daños por agua	**MB**	**100%**				

Tabla 14. (Continuación)

ACTIVOS	Amenazas	Probabilidad	Dimensiones				
			[D]	[I]	[C]	[A]	[T]
Switch de borde. Referencia 4800G - UPI La Arcadia	[N.*] Desastres naturales	**MB**	**100%**				
	[I.1] Fuego	**MB**	**100%**				
	[I.3] Contaminación medioambiental	**B**	**70%**				
	[I.6] Corte del suministro eléctrico	**M**	**70%**				
	[I.7] Condiciones inadecuadas de temperatura o humedad	**B**	**10%**				
	[E.2] Errores del administrador del sistema / de la seguridad	**MB**	**10%**				
	[E.4] Errores de configuración	**B**	**10%**				
	[E.23] Errores de mantenimiento / actualización de equipos (hardware)	**B**	**10%**				
	[A.7] uso no previsto	**MB**	**5%**				
	[A.11] Acceso no autorizado	**MB**	**10%**				
	[A.23] Manipulación del hardware	**MB**	**10%**				
	[A.25] Robo de equipos	**MB**	**100%**				
Switch de core. Referencia 5500G - Sede Administrativa	[N.2] Daños por agua	**MB**	**100%**				
	[N.*] Desastres naturales	**MB**	**100%**				
	[I.1] Fuego	**MB**	**100%**				
	[I.3] Contaminación medioambiental	**B**	**70%**				
	[I.6] Corte del suministro eléctrico	**M**	**70%**				
	[I.7] Condiciones inadecuadas de temperatura o humedad	**B**	**10%**				

Tabla 14. (Continuación)

ACTIVOS	Amenazas	Probabilidad	Dimensiones				
			[D]	[I]	[C]	[A]	[T]
Switch de core. Referencia 5500G - Sede Administrativa	[E.2] Errores del administrador del sistema / de la seguridad	**MB**	**10%**				
	[E.4] Errores de configuración	**B**	**10%**				
	[E.23] Errores de mantenimiento / actualización de equipos (hardware)	**B**	**10%**				
	[A.7] uso no previsto	**MB**	**5%**				
	[A.11] Acceso no autorizado	**MB**	**10%**				
	[A.23] Manipulación del hardware	**MB**	**10%**				
	[A.25] Robo de equipos	**MB**	**100%**				
Copia de Respaldo - Dataprotector	[N.2] Daños por agua	**MB**	**100%**				
	[N.*] Desastres naturales	**MB**	**100%**				
	[I.6] Corte del suministro eléctrico	**B**	**70%**				
	[I.7] Condiciones inadecuadas de temperatura o humedad	**B**	**10%**				
	[I.8] Fallo de servicios de comunicaciones	**B**	**50%**				
	[I.9] Interrupción de otros servicios o suministros esenciales	**B**	**70%**				
	[E.2] Errores del administrador del sistema / de la seguridad	**MB**	**30%**				
	[E.4] Errores de configuración	**B**	**70%**				
	[E.18] Destrucción de la información	**B**		**80%**	**70%**		

Tabla 14. (Continuación)

ACTIVOS	Amenazas	Probabilidad	Dimensiones				
			[D]	[I]	[C]	[A]	[T]
Copia de Respaldo - Dataprotector	[E.21] Errores de mantenimiento / actualización de programas (software)	**A**					**70%**
	[E.24] caída del sistema por agotamiento de recursos	**B**	**60%**				
	[A.23] Manipulación del hardware	**MB**	**100%**				**100%**
Sistema de Backups - Dataprotector	[N.2] Daños por agua	**MB**	**100%**				
	[N.*] Desastres naturales	**MB**	**100%**				
	[I.6] Corte del suministro eléctrico	**B**	**70%**				
	[I.7] Condiciones inadecuadas de temperatura o humedad	**B**	**10%**				
	[I.8] Fallo de servicios de comunicaciones	**B**	**50%**				
	[I.9] Interrupción de otros servicios o suministros esenciales	**B**	**70%**				
	[E.2] Errores del administrador del sistema / de la seguridad	**MB**	**30%**				
	[E.4] Errores de configuración	**B**	**70%**				
	[E.18] Destrucción de la información	**B**		**80%**	**70%**		
	[E.21] Errores de mantenimiento / actualización de programas (software)	**A**					**70%**
	[E.24] caída del sistema por agotamiento de recursos	**B**	**60%**				

Tabla 14. (Continuación)

ACTIVOS	Amenazas	Probabilidad	Dimensiones				
			[D]	[I]	[C]	[A]	[T]
Sistema de Backups - Dataprotector	[A.23] Manipulación del hardware	**MB**	**100%**				**100%**
Servidor de correo - Proliant DL 380 G5	[N.1] Fuego	**MB**	**100%**				
	[N.2] Daños por agua	**MB**	**100%**				
	[N.*] Desastres naturales	**MB**	**100%**				
	[I.5] Avería de origen físico o lógico	**MB**	**50%**				
	[I.6] Corte del suministro eléctrico	**M**	**70%**				
	[I.7] Condiciones inadecuadas de temperatura o humedad	**B**	**50%**				
	[E.2] Errores del administrador del sistema / de la seguridad	**MB**	**10%**	**10%**	**10%**		
	[E.4] Errores de configuración	**MB**	**30%**	**30%**	**30%**		
	[E.8] Difusión de software dañino	**B**	**70%**				
	[E.23] Errores de mantenimiento / actualización de equipos (hardware)	**MB**	**10%**				
	[E.25] Pérdida de equipos	**MB**	**100%**				
	[A.6] Abuso de privilegios de acceso	**MB**		**50%**	**50%**		
	[A.7] uso no previsto	**MB**	**15%**	**15%**	**15%**		
	[A.11] Acceso no autorizado	**MB**		**10%**	**80%**		
	[A.23] Manipulación del hardware	**B**	**50%**		**50%**		
	[A.24] Denegación de servicio	**B**	**70%**				
	[A.25] Robo de equipos	**MB**	**100%**				

Tabla 14. (Continuación)

ACTIVOS	Amenazas	Probabilidad	Dimensiones				
			[D]	[I]	[C]	[A]	[T]
Servidor de correo - Proliant DL 380 G5	[A.26] Ataque destructivo	**MB**	**100%**				
Servidor Ambiente de pruebas y desarrollo	[N.1] Fuego	**B**	**100%**	**100%**			
	[N.2] Daños por agua	**B**	**100%**	**100%**			
	[N.*] Desastres naturales	**B**	**100%**	**100%**			
	[E.1] Errores de los usuarios	**MB**	**30%**				
	[E.2] Errores del administrador del sistema / de la seguridad	**B**	**50%**	**50%**	**50%**		
	[E.4] Errores de configuración	**MB**	**50%**	**50%**	**50%**		
	[E.19] Fugas de información	**M**		**40%**	**80%**		
Servidor de base de datos Nómina	[N.1] Fuego	**MB**	**100%**	**100%**	**100%**		
	[N.2] Daños por agua	**MB**	**100%**	**100%**	**100%**		
	[N.*] Desastres naturales	**MB**	**100%**	**100%**	**100%**		
	[E.1] Errores de los usuarios	**M**	**10%**	**70%**			
	[E.2] Errores del administrador del sistema / de la seguridad	**M**	**80%**	**30%**	**70%**		
	[E.14] Fugas de información	**M**			**100%**		
	[E.15] Alteración de la información	**M**		**90%**	**90%**		
	[E.18] Destrucción de la información	**B**	**100%**	**100%**	**100%**		
	[A.6] Abuso de privilegios de acceso	**M**	**30%**	**100%**	**100%**	**80%**	
	[A.15] Modificación de la información	**B**		**90%**	**100%**		
Servidor de Virtualización	[N.1] Fuego	**M**	**90%**	**90%**			
	[N.2] Daños por agua	**M**	**90%**	**90%**			

Tabla 14. (Continuación)

ACTIVOS	Amenazas	Probabilidad	Dimensiones				
			[D]	[I]	[C]	[A]	[T]
Servidor de Virtualización	[I.1] Fuego	**M**	**90%**	**90%**			
	[I.2] Daños por agua	**M**	**90%**	**90%**			
	[E.2] Errores del administrador del sistema / de la seguridad	**MB**	**40%**	**40%**			
	[E.4] Errores de configuración	**MB**	**40%**	**40%**			
	[E.24] caída del sistema por agotamiento de recursos	**B**	**60%**	**60%**			
	[A.8] Difusión de software dañino	**M**	**50%**	**50%**			
	[A.23] Manipulación del hardware	**MB**	**100%**	**100%**			
	[A.24] Denegación de servicio	**MB**	**30%**	**30%**			
	[A.26] Ataque destructivo	**MB**	**100%**	**100%**			
Servidor base de datos SQL	[N.*] Desastres naturales	**MB**	**100%**	**100%**			
	[E.2] Errores del administrador del sistema / de la seguridad	**MB**	**10%**	**50%**			
	[E.4] Errores de configuración	**MB**	**10%**	**50%**			
	[E.15] Alteración de la información	**MB**	**15%**	**60%**			
	[E.21] Errores de mantenimiento / actualización de programas (software)	**M**	**5%**				**70%**
	[A.6] Abuso de privilegios de acceso	**MB**			**60%**		
	[A.8] Difusión de software dañino	**B**	**70%**	**70%**			
	[A.11] Acceso no autorizado	**B**			**70%**		
	[A.15] Modificación de la información	**B**		**70%**	**70%**	**70%**	
Servidor de Archivos	[N.2] Daños por agua	**MB**	**100%**	**100%**			

Tabla 14. (Continuación)

ACTIVOS	Amenazas	Probabilidad	Dimensiones				
			[D]	[I]	[C]	[A]	[T]
Servidor de Archivos	[N.*] Desastres naturales	**MB**	**100%**	**100%**			
	[I.3] Contaminación medioambiental	**B**	**70%**				
	[I.6] Corte del suministro eléctrico	**B**	**70%**				
	[I.7] Condiciones inadecuadas de temperatura o humedad	**MB**	**40%**				
	[E.1] Errores de los usuarios	**M**		**80%**			
	[E.2] Errores del administrador del sistema / de la seguridad	**MB**	**5%**				**50%**
	[E.4] Errores de configuración	**MB**	**5%**				**60%**
	[E.15] Alteración de la información	**M**		**80%**			
	[E.18] Destrucción de la información	**A**		**80%**			
	[E.24] caída del sistema por agotamiento de recursos	**M**	**50%**				**50%**
	[A.6] Abuso de privilegios de acceso	**MB**		**80%**	**80%**	**80%**	
	[A.8] Difusión de software dañino	**MB**	**25%**	**60%**			
	[A.11] Acceso no autorizado	**MB**		**80%**	**80%**		
	[A.15] Modificación de la información	**B**		**80%**	**80%**		
	[A.18] Destrucción de la información	**B**		**80%**	**80%**		
Servidor de impresión	[N.1] Fuego	**MB**	**100%**				**100%**
	[N.2] Daños por agua	**MB**	**100%**				**100%**
	[N.*] Desastres naturales	**B**	**100%**				**100%**
	[I.5] Avería de origen físico o lógico	**MB**	**100%**				**100%**

Tabla 14. (Continuación)

ACTIVOS	Amenazas	Probabilidad	Dimensiones				
			[D]	[I]	[C]	[A]	[T]
Servidor de impresión	[I.6] Corte del suministro eléctrico	**MB**	**100%**				**100%**
	[I.7] Condiciones inadecuadas de temperatura o humedad	**MB**	**70%**				**70%**
	[I.8.11] Interrupción accidental	**MB**	**70%**				**70%**
	[E.2] Errores del administrador del sistema / de la seguridad	**MB**	**60%**				**60%**
	[E.4] Errores de configuración	**MB**	**60%**				**60%**
	[E.21] Errores de mantenimiento / actualización de programas (software)	**MB**	**60%**				**60%**
	[E.24] caída del sistema por agotamiento de recursos	**B**	**90%**				**90%**
	[A.5] suplantación de la identidad del usuario	**MB**	**100%**				**100%**
	[A.6] Abuso de privilegios de acceso	**MB**	**80%**				**80%**
	[A.8] Difusión de software dañino	**B**	**100%**				**100%**
	[A.11] Acceso no autorizado	**MB**	**100%**				**100%**
	[A.24] Denegación de servicio	**B**	**100%**				**100%**
Servidor OAS – SICAPITAL	[N.1] Fuego	**MB**	**100%**				
	[N.2] Daños por agua	**MB**	**100%**				
	[N.*] Desastres naturales	**MB**	**100%**				
	[I.5] Avería de origen físico o lógico	**B**	**10%**	**10%**			
	[I.6] Corte del suministro eléctrico	**M**	**80%**	**10%**			

Tabla 14. (Continuación)

ACTIVOS	Amenazas	Probabilidad	Dimensiones				
			[D]	[I]	[C]	[A]	[T]
Servidor OAS – SICAPITAL	[I.7] Condiciones inadecuadas de temperatura o humedad	**M**	**80%**	**10%**			
	[I.8.11] Interrupción accidental	**MB**	**60%**				
	[E.2] Errores del administrador del sistema / de la seguridad	**B**	**60%**				
	[E.4] Errores de configuración	**B**	**100%**				
	[E.21] Errores de mantenimiento / actualización de programas (software)	**B**	**60%**				
	[E.23] Errores de mantenimiento / actualización de equipos (hardware)	**B**	**60%**				
	[E.24] caída del sistema por agotamiento de recursos	**MB**	**70%**				
	[A.4] Manipulación de los ficheros de configuración	**MB**	**100%**				
	[A.5] suplantación de la identidad del usuario	**M**		**60%**	**90%**	**100%**	
	[A.6] Abuso de privilegios de acceso	**B**		**60%**	**90%**	**80%**	
	[A.18] Destrucción de la información	**MB**		**100%**	**100%**	**100%**	**60%**
	[A.24] Denegación de servicio	**M**	**90%**				

Fuente: realizado en PILAR 5.2.9

8.4.4 Identificación y Valoración de Amenazas Tipo: [AUX] ELEMENTOS AUXILIARES

Tabla 18. Identificación y valoración de amenazas en activos tipo: Elementos Auxiliares

ACTIVOS	Amenazas	Probabilidad	Dimensiones				
			[D]	[I]	[C]	[A]	[T]
UPS de 15 KVA - UPI La Arcadia	[N.2] Daños por agua	**MB**	**20%**				
	[N.*] Desastres naturales	**MB**	**80%**				
	[I.1] Fuego	**MB**	**80%**				
	[I.5] Avería de origen físico o lógico	**MB**	**20%**				
	[I.6] Corte del suministro eléctrico	**B**	**20%**				
	[I.7] Condiciones inadecuadas de temperatura o humedad	**B**	**10%**				
	[I.9] Interrupción de otros servicios o suministros esenciales	**B**	**10%**				
	[E.23] Errores de mantenimiento / actualización de equipos (hardware)	**MB**	**10%**				
	[A.7] uso no previsto	**MB**	**10%**				
	[A.23] Manipulación del hardware	**MB**	**10%**				
UPS de 15 KVA - UPI La Rioja	[N.2] Daños por agua	**MB**	**20%**				
	[N.*] Desastres naturales	**MB**	**80%**				
	[I.1] Fuego	**MB**	**80%**				
	[I.5] Avería de origen físico o lógico	**MB**	**20%**				
	[I.6] Corte del suministro eléctrico	**B**	**20%**				

Tabla 15. (Continuación)

ACTIVOS	Amenazas	Probabilidad	Dimensiones				
			[D]	[I]	[C]	[A]	[T]
UPS de 15 KVA - UPI La Rioja	[I.7] Condiciones inadecuadas de temperatura o humedad	**B**	**10%**				
	[I.9] Interrupción de otros servicios o suministros esenciales	**B**	**10%**				
	[E.23] Errores de mantenimiento / actualización de equipos (hardware)	**MB**	**10%**				
	[A.7] uso no previsto	**MB**	**10%**				
	[A.23] Manipulación del hardware	**MB**	**10%**				
Planta eléctrica	[N.*] Desastres naturales	**MB**	**80%**				
	[I.1] Fuego	**MB**	**80%**				
	[I.3] Contaminación medioambiental	**B**	**30%**				
	[I.5] Avería de origen físico o lógico	**B**	**30%**				
	[I.6] Corte del suministro eléctrico	**MB**	**20%**				
	[I.7] Condiciones inadecuadas de temperatura o humedad	**MB**	**10%**				
	[I.9] Interrupción de otros servicios o suministros esenciales	**B**	**10%**				
	[E.23] Errores de mantenimiento / actualización de equipos (hardware)	**MB**	**10%**				
	[A.26] Ataque destructivo	**MB**	**80%**				
UPS de 10 KVA - Sede Misión Bogotá	[N.2] Daños por agua	**MB**	**20%**				

Tabla 15. (Continuación)

ACTIVOS	Amenazas	Probabilidad	Dimensiones				
			[D]	[I]	[C]	[A]	[T]
UPS de 10 KVA - Sede Misión Bogotá	[N.*] Desastres naturales	**MB**	**80%**				
	[I.1] Fuego	**MB**	**80%**				
	[I.5] Avería de origen físico o lógico	**MB**	**20%**				
	[I.6] Corte del suministro eléctrico	**B**	**20%**				
	[I.7] Condiciones inadecuadas de temperatura o humedad	**B**	**10%**				
	[I.9] Interrupción de otros servicios o suministros esenciales	**B**	**10%**				
	[E.23] Errores de mantenimiento / actualización de equipos (hardware)	**MB**	**10%**				
	[A.7] uso no previsto	**MB**	**10%**				
	[A.23] Manipulación del hardware	**MB**	**10%**				
UPS de 10 KVA - UPI La vega	[N.2] Daños por agua	**MB**	**20%**				
	[N.*] Desastres naturales	**MB**	**80%**				
	[I.1] Fuego	**MB**	**80%**				
	[I.5] Avería de origen físico o lógico	**MB**	**20%**				
	[I.6] Corte del suministro eléctrico	**B**	**20%**				
	[I.7] Condiciones inadecuadas de temperatura o humedad	**B**	**10%**				
	[I.9] Interrupción de otros servicios o suministros esenciales	**B**	**10%**				

Tabla 15. (Continuación)

ACTIVOS	Amenazas	Probabilidad	Dimensiones				
			[D]	[I]	[C]	[A]	[T]
UPS de 10 KVA - UPI La vega	[E.23] Errores de mantenimiento / actualización de equipos (hardware)	**MB**	**10%**				
	[A.7] uso no previsto	**MB**	**10%**				
	[A.23] Manipulación del hardware	**MB**	**10%**				
UPS de 15 KVA - UPI Santa Lucia	[N.2] Daños por agua	**MB**	**20%**				
	[N.*] Desastres naturales	**MB**	**80%**				
	[I.1] Fuego	**MB**	**80%**				
	[I.5] Avería de origen físico o lógico	**MB**	**20%**				
	[I.6] Corte del suministro eléctrico	**B**	**20%**				
	[I.7] Condiciones inadecuadas de temperatura o humedad	**B**	**10%**				
	[I.9] Interrupción de otros servicios o suministros esenciales	**B**	**10%**				
	[E.23] Errores de mantenimiento / actualización de equipos (hardware)	**MB**	**10%**				
	[A.7] uso no previsto	**MB**	**10%**				
	[A.23] Manipulación del hardware	**MB**	**10%**				
UPS de 10 KVA - UPI San Francisco	[N.2] Daños por agua	**MB**	**20%**				
	[N.*] Desastres naturales	**MB**	**80%**				
	[I.1] Fuego	**MB**	**80%**				
	[I.5] Avería de origen físico o lógico	**MB**	**20%**				

Tabla 15. (Continuación)

ACTIVOS	Amenazas	Probabilidad	Dimensiones				
			[D]	[I]	[C]	[A]	[T]
UPS de 10 KVA - UPI San Francisco	[I.6] Corte del suministro eléctrico	**B**	**20%**				
	[I.7] Condiciones inadecuadas de temperatura o humedad	**B**	**10%**				
	[I.9] Interrupción de otros servicios o suministros esenciales	**B**	**10%**				
	[E.23] Errores de mantenimiento / actualización de equipos (hardware)	**MB**	**10%**				
	[A.7] uso no previsto	**MB**	**10%**				
	[A.23] Manipulación del hardware	**MB**	**10%**				
UPS de 15 KVA - UPI El Perdomo	[N.2] Daños por agua	**MB**	**20%**				
	[N.*] Desastres naturales	**MB**	**80%**				
	[I.1] Fuego	**MB**	**80%**				
	[I.5] Avería de origen físico o lógico	**MB**	**20%**				
	[I.6] Corte del suministro eléctrico	**B**	**20%**				
	[I.7] Condiciones inadecuadas de temperatura o humedad	**B**	**10%**				
	[I.9] Interrupción de otros servicios o suministros esenciales	**B**	**10%**				
	[E.23] Errores de mantenimiento / actualización de equipos (hardware)	**MB**	**10%**				
	[A.7] uso no previsto	**MB**	**10%**				

Tabla 15. (Continuación)

ACTIVOS	Amenazas	Probabilidad	Dimensiones				
			[D]	[I]	[C]	[A]	[T]
UPS de 15 KVA - UPI El Perdomo	[A.23] Manipulación del hardware	**MB**	**10%**				
UPS de 15 KVA - UPI La 27 sur	[N.2] Daños por agua	**MB**	**20%**				
	[N.*] Desastres naturales	**MB**	**80%**				
	[I.1] Fuego	**MB**	**80%**				
	[I.5] Avería de origen físico o lógico	**MB**	**20%**				
	[I.6] Corte del suministro eléctrico	**B**	**20%**				
	[I.7] Condiciones inadecuadas de temperatura o humedad	**B**	**10%**				
	[I.9] Interrupción de otros servicios o suministros esenciales	**B**	**10%**				
	[E.23] Errores de mantenimiento / actualización de equipos (hardware)	**MB**	**10%**				
	[A.7] uso no previsto	**MB**	**10%**				
	[A.23] Manipulación del hardware	**MB**	**10%**				
UPS de 15 KVA - UPI Servitá	[N.2] Daños por agua	**MB**	**20%**				
	[N.*] Desastres naturales	**MB**	**80%**				
	[I.1] Fuego	**MB**	**80%**				
	[I.5] Avería de origen físico o lógico	**MB**	**20%**				
	[I.6] Corte del suministro eléctrico	**B**	**20%**				
	[I.7] Condiciones inadecuadas de temperatura o humedad	**B**	**10%**				

Tabla 15. (Continuación)

ACTIVOS	Amenazas	Probabilidad	Dimensiones				
			[D]	[I]	[C]	[A]	[T]
UPS de 15 KVA - UPI Servitá	[I.9] Interrupción de otros servicios o suministros esenciales	**B**	**10%**				
	[E.23] Errores de mantenimiento / actualización de equipos (hardware)	**MB**	**10%**				
	[A.7] uso no previsto	**MB**	**10%**				
	[A.23] Manipulación del hardware	**MB**	**10%**				
UPS de 15 KVA - UPI La Florida	[N.2] Daños por agua	**MB**	**20%**				
	[N.*] Desastres naturales	**MB**	**80%**				
	[I.1] Fuego	**MB**	**80%**				
	[I.5] Avería de origen físico o lógico	**MB**	**20%**				
	[I.6] Corte del suministro eléctrico	**B**	**20%**				
	[I.7] Condiciones inadecuadas de temperatura o humedad	**B**	**10%**				
	[I.9] Interrupción de otros servicios o suministros esenciales	**B**	**10%**				
	[E.23] Errores de mantenimiento / actualización de equipos (hardware)	**MB**	**10%**				
	[A.7] uso no previsto	**MB**	**10%**				
	[A.23] Manipulación del hardware	**MB**	**10%**				
UPS de 20 KVA - Sede proyecto 968	[N.2] Daños por agua	**MB**	**20%**				
	[N.*] Desastres naturales	**MB**	**80%**				

Tabla 15. (Continuación)

ACTIVOS	Amenazas	Probabilidad	Dimensiones				
			[D]	[I]	[C]	[A]	[T]
UPS de 20 KVA - Sede proyecto 968	[I.1] Fuego	**MB**	**80%**				
	[I.5] Avería de origen físico o lógico	**MB**	**20%**				
	[I.6] Corte del suministro eléctrico	**B**	**20%**				
	[I.7] Condiciones inadecuadas de temperatura o humedad	**B**	**10%**				
	[I.9] Interrupción de otros servicios o suministros esenciales	**B**	**10%**				
	[E.23] Errores de mantenimiento / actualización de equipos (hardware)	**MB**	**10%**				
	[A.7] uso no previsto	**MB**	**10%**				
	[A.23] Manipulación del hardware	**MB**	**10%**				
UPS de 10 KVA - UPI Bosa	[N.2] Daños por agua	**MB**	**20%**				
	[N.*] Desastres naturales	**MB**	**80%**				
	[I.1] Fuego	**MB**	**80%**				
	[I.5] Avería de origen físico o lógico	**MB**	**20%**				
	[I.6] Corte del suministro eléctrico	**B**	**20%**				
	[I.7] Condiciones inadecuadas de temperatura o humedad	**B**	**10%**				
	[I.9] Interrupción de otros servicios o suministros esenciales	**B**	**10%**				

Tabla 15. (Continuación)

ACTIVOS	Amenazas	Probabilidad	Dimensiones				
			[D]	[I]	[C]	[A]	[T]
UPS de 10 KVA - UPI Bosa	[E.23] Errores de mantenimiento / actualización de equipos (hardware)	**MB**	**10%**				
	[A.7] uso no previsto	**MB**	**10%**				
	[A.23] Manipulación del hardware	**MB**	**10%**				
UPS de 20 KVA - UPI La 32	[N.2] Daños por agua	**MB**	**20%**				
	[N.*] Desastres naturales	**MB**	**80%**				
	[I.1] Fuego	**MB**	**80%**				
	[I.5] Avería de origen físico o lógico	**MB**	**20%**				
	[I.6] Corte del suministro eléctrico	**B**	**20%**				
	[I.7] Condiciones inadecuadas de temperatura o humedad	**B**	**10%**				
	[I.9] Interrupción de otros servicios o suministros esenciales	**B**	**10%**				
	[E.23] Errores de mantenimiento / actualización de equipos (hardware)	**MB**	**10%**				
	[A.7] uso no previsto	**MB**	**10%**				
	[A.23] Manipulación del hardware	**MB**	**10%**				
UPS de 20 KVA - UPI La Florida	[N.2] Daños por agua	**MB**	**20%**				
	[N.*] Desastres naturales	**MB**	**80%**				
	[I.1] Fuego	**MB**	**80%**				
	[I.5] Avería de origen físico o lógico	**MB**	**20%**				

Tabla 15. (Continuación)

ACTIVOS	Amenazas	Probabilidad	Dimensiones				
			[D]	[I]	[C]	[A]	[T]
UPS de 20 KVA - UPI La Florida	[I.6] Corte del suministro eléctrico	**B**	**20%**				
	[I.7] Condiciones inadecuadas de temperatura o humedad	**B**	**10%**				
	[I.9] Interrupción de otros servicios o suministros esenciales	**B**	**10%**				
	[E.23] Errores de mantenimiento / actualización de equipos (hardware)	**MB**	**10%**				
	[A.7] uso no previsto	**MB**	**10%**				
	[A.23] Manipulación del hardware	**MB**	**10%**				
UPS de 30 KVA - UPI El Perdomo	[N.2] Daños por agua	**MB**	**20%**				
	[N.*] Desastres naturales	**MB**	**80%**				
	[I.1] Fuego	**MB**	**80%**				
	[I.5] Avería de origen físico o lógico	**MB**	**20%**				
	[I.6] Corte del suministro eléctrico	**B**	**20%**				
	[I.7] Condiciones inadecuadas de temperatura o humedad	**B**	**10%**				
	[I.9] Interrupción de otros servicios o suministros esenciales	**B**	**10%**				
	[E.23] Errores de mantenimiento / actualización de equipos (hardware)	**MB**	**10%**				
	[A.7] uso no previsto	**MB**	**10%**				

Tabla 15. (Continuación)

ACTIVOS	Amenazas	Probabilidad	Dimensiones				
			[D]	[I]	[C]	[A]	[T]
UPS de 30 KVA - UPI El Perdomo	[A.23] Manipulación del hardware	**MB**	**10%**				
Sistema de aire acondicionado	[N.*] Desastres naturales	**MB**	**70%**				
	[I.5] Avería de origen físico o lógico	**MB**	**70%**				
	[I.6] Corte del suministro eléctrico	**MB**	**50%**				

Fuente: realizado en PILAR 5.2.9

8.4.5 Identificación y Valoración de Amenazas Tipo: [D] DATOS / INFORMACIÓN

Tabla 19. Identificación y valoración de amenazas en activos tipo: Datos / Información

ACTIVOS	Amenazas	Probabilidad	Dimensiones				
			[D]	[I]	[C]	[A]	[T]
Documentación Técnica	[N.2] Daños por agua	**MB**	**90%**	**90%**			
	[N.*] Desastres naturales	**MB**	**100%**	**100%**			
	[I.1] Fuego	**MB**	**100%**	**100%**			
	[I.7] Condiciones inadecuadas de temperatura o humedad	**M**	**30%**	**30%**			
	[E.18] Destrucción de la información	**B**	**50%**	**50%**			

Fuente: realizado en PILAR 5.2.9

8.4.6 Identificación y Valoración de Amenazas Tipo: [P] PERSONAL

Tabla 20. Identificación y valoración de amenazas en activos tipo: Personal

ACTIVOS	Amenazas	Probabilidad	Dimensiones				
			[D]	[I]	[C]	[A]	[T]
Administradores de Sistemas	[E.7] Deficiencias en la organización	**M**	**20%**				

Tabla 17. (Continuación)

ACTIVOS	Amenazas	Probabilidad	Dimensiones				
			[D]	[I]	[C]	[A]	[T]
Administradores de Sistemas	[E.28] Indisponibilidad del personal	M	70%				
	[A.29] Extorsión	MB	30%	60%	70%		
	[A.30] Ingeniería Social	MB	30%	70%	80%		

Fuente: realizado en PILAR 5.2.9

8.5 ESTIMACIÓN DEL ESTADO DEL RIESGO

En esta tarea se procesa e interpreta los resultados obtenidos de las actividades anteriores, y consta de dos partes:

- Estimación del impacto
- Estimación del Riesgo

8.5.1. Impacto Potencial

"Se denomina impacto a la medida del daño sobre el activo derivado de la materialización de una amenaza. Conociendo el valor de los activos (en varias dimensiones) y la degradación que causan las amenazas, es directo el impacto que estas tendrían sobre el sistema". [20] Como a continuación se establece en la "Tabla 16".

Tabla 21. Valoración estimada del Impacto

IMPACTO			Degradación				
			1% - 9%	10%-49%	50%-69%	70%-89%	90%-100%
Valor	9-10	MA	M	A	A	MA	MA
	7-8	A	B	M	M	A	A
	4-6	M	MB	B	B	M	M
	1-3	B	MB	MB	MB	B	B
	0	MB	MB	MB	MB	MB	MB

Fuente: Magerit V.3 – Libro II – Catálogo de elementos

En las siguientes tablas se muestran los resultados obtenidos en cuanto al impacto potencial por cada uno de los activos según la dimensión que haya sido afectado.

[20] Magerit-versión 3.0 Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información, Libro 1-Método, https://www.ccn-cert.cni.es/publico/herramientas/pilar5/magerit/ p. 28

8.5.1.1 Impacto: [IS] SERVICIOS

Tabla 22. Impacto potencial activos de tipo: Servicios

ACTIVOS	Amenazas	Dimensiones				
		[D]	[I]	[C]	[A]	[T]
Controlador de dominio UPI La 27 sur	[E.2] Errores del administrador del sistema / de la seguridad	A	A	A		
	[E.15] Alteración de la información		MA	MA		
	[E.18] Destrucción de la información	MA	MA	MA		
	[E.19] Fugas de información	M	MA	MA		
	[E.24] caída del sistema por agotamiento de recursos	A				
	[A.5] suplantación de la identidad del usuario		A	A	MA	
	[A.6] Abuso de privilegios de acceso		A	A		
	[A.7] uso no previsto	MA	A	A		
	[A.11] Acceso no autorizado		A	A		
	[A.15] Modificación de la información		A			
	[A.18] Destrucción de la información	A	A			
	[A.19] revelación de información			A		
	[A.24] Denegación de servicio	A				
Controlador de dominio misional	[E.2] Errores del administrador del sistema / de la seguridad	A	A	A		
	[E.15] Alteración de la información		MA	MA		

Tabla 19. (Continuación)

ACTIVOS	Amenazas	Dimensiones				
		[D]	[I]	[C]	[A]	[T]
Controlador de dominio misional	[E.18] Destrucción de la información	MA	MA	MA		
	[E.19] Fugas de información	M	MA	MA		
	[E.24] caída del sistema por agotamiento de recursos	A				
	[A.5] suplantación de la identidad del usuario		A	A	MA	
	[A.6] Abuso de privilegios de acceso		A	A		
	[A.7] uso no previsto	MA	A	A		
	[A.11] Acceso no autorizado		A	A		
	[A.15] Modificación de la información		A			
	[A.18] Destrucción de la información	A	A			
	[A.19] revelación de información			A		
	[A.24] Denegación de servicio	A				
Controlador de dominio principal	[E.2] Errores del administrador del sistema / de la seguridad	A	A	A		
	[E.15] Alteración de la información		MA	MA		
	[E.18] Destrucción de la información	MA	MA	MA		
	[E.19] Fugas de información	M	MA	MA		
	[E.24] caída del sistema por agotamiento de recursos	A				

Tabla 19. (Continuación)

ACTIVOS	Amenazas	Dimensiones				
		[D]	[I]	[C]	[A]	[T]
Controlador de dominio principal	[A.5] suplantación de la identidad del usuario		A	A	MA	
	[A.6] Abuso de privilegios de acceso		A	A		
	[A.7] uso no previsto	MA	A	A		
	[A.11] Acceso no autorizado		A	A		
	[A.15] Modificación de la información		A			
	[A.18] Destrucción de la información	A	A			
	[A.19] revelación de información			A		
	[A.24] Denegación de servicio	A				
Controlador de dominio Misión Bogotá	[E.2] Errores del administrador del sistema / de la seguridad	A	A	A		
	[E.15] Alteración de la información		MA	MA		
	[E.18] Destrucción de la información	MA	MA	MA		
	[E.19] Fugas de información	M	MA	MA		
	[E.24] caída del sistema por agotamiento de recursos	A				
	[A.5] suplantación de la identidad del usuario		A	A	MA	
	[A.6] Abuso de privilegios de acceso		A	A		
	[A.7] uso no previsto	MA	A	A		
	[A.11] Acceso no autorizado		A	A		

Tabla 19. (Continuación)

ACTIVOS	Amenazas	Dimensiones				
		[D]	[I]	[C]	[A]	[T]
Controlador de dominio Misión Bogotá	[A.15] Modificación de la información		A			
	[A.18] Destrucción de la información	A	A			
	[A.19] revelación de información			A		
	[A.24] Denegación de servicio	A				
Controlador de dominio UPI La 32	[E.2] Errores del administrador del sistema / de la seguridad	A	A	A		
	[E.15] Alteración de la información		MA	MA		
	[E.18] Destrucción de la información	MA	MA	MA		
	[E.19] Fugas de información	M	MA	MA		
	[E.24] caída del sistema por agotamiento de recursos	A				
	[A.5] suplantación de la identidad del usuario		A	A	MA	
	[A.6] Abuso de privilegios de acceso		A	A		
	[A.7] uso no previsto	MA	A	A		
	[A.11] Acceso no autorizado		A	A		
	[A.15] Modificación de la información		A			
	[A.18] Destrucción de la información	A	A			
	[A.19] revelación de información			A		

Tabla 19. (Continuación)

ACTIVOS	Amenazas	Dimensiones				
		[D]	[I]	[C]	[A]	[T]
Controlador de dominio UPI La 32	[A.24] Denegación de servicio	A				
Controlador de dominio UPI La Arcadia	[E.2] Errores del administrador del sistema / de la seguridad	A	A	A		
	[E.15] Alteración de la información		MA	MA		
	[E.18] Destrucción de la información	MA	MA	MA		
	[E.19] Fugas de información	M	MA	MA		
	[E.24] caída del sistema por agotamiento de recursos	A				
	[A.5] suplantación de la identidad del usuario		A	A	MA	
	[A.6] Abuso de privilegios de acceso		A	A		
	[A.7] uso no previsto	MA	A	A		
	[A.11] Acceso no autorizado		A	A		
	[A.15] Modificación de la información		A			
	[A.18] Destrucción de la información	A	A			
	[A.19] revelación de información			A		
	[A.24] Denegación de servicio	A				
Controlador de dominio UPI La Florida	[E.2] Errores del administrador del sistema / de la seguridad	A	A	A		
	[E.15] Alteración de la información		MA	MA		

Tabla 19. (Continuación)

ACTIVOS	Amenazas	Dimensiones				
		[D]	[I]	[C]	[A]	[T]
Controlador de dominio UPI La Florida	[E.18] Destrucción de la información	MA	MA	MA		
	[E.19] Fugas de información	M	MA	MA		
	[E.24] caída del sistema por agotamiento de recursos	A				
	[A.5] suplantación de la identidad del usuario		A	A	MA	
	[A.6] Abuso de privilegios de acceso		A	A		
	[A.7] uso no previsto	MA	A	A		
	[A.11] Acceso no autorizado		A	A		
	[A.15] Modificación de la información		A			
	[A.18] Destrucción de la información	A	A			
	[A.19] revelación de información			A		
	[A.24] Denegación de servicio	A				
Correo electrónico ZIMBRA MTA	[E.1] Errores de los usuarios	A	MA	MA		
	[E.2] Errores del administrador del sistema / de la seguridad	A	A	A		
	[E.15] Alteración de la información		A			
	[E.18] Destrucción de la información	MA	MA			
	[E.19] Fugas de información			MA		

Tabla 19. (Continuación)

ACTIVOS	Amenazas	Dimensiones				
		[D]	[I]	[C]	[A]	[T]
Correo electrónico ZIMBRA MTA	[E.24] caída del sistema por agotamiento de recursos	A				
	[A.5] suplantación de la identidad del usuario		A	A	A	
	[A.6] Abuso de privilegios de acceso		MA	MA		
	[A.7] uso no previsto	MA	A	A		
	[A.11] Acceso no autorizado		A	A		
	[A.13] Repudio (negación de actuaciones)		MA			
	[A.18] Destrucción de la información	A				
	[A.19] revelación de información			A		
	[A.24] Denegación de servicio	A				
Correo Exchange	[E.1] Errores de los usuarios	MB	B	B		
	[E.2] Errores del administrador del sistema / de la seguridad	MB	MB	MB		
	[E.15] Alteración de la información		MB			
	[E.18] Destrucción de la información	B	B			
	[E.19] Fugas de información			B		
	[E.24] caída del sistema por agotamiento de recursos	MB				
	[A.5] suplantación de la identidad del usuario		MB	MB	B	

Tabla 19. (Continuación)

ACTIVOS	Amenazas	Dimensiones				
		[D]	[I]	[C]	[A]	[T]
Correo Exchange	[A.6] Abuso de privilegios de acceso		B	B		
	[A.7] uso no previsto	B	MB	MB		
	[A.11] Acceso no autorizado		MB	MB		
	[A.13] Repudio (negación de actuaciones)		B			
	[A.18] Destrucción de la información	MB				
	[A.19] revelación de información			MB		
	[A.24] Denegación de servicio	MB				
Controlador de dominio UPI La Vega	[E.2] Errores del administrador del sistema / de la seguridad	A	A	A		
	[E.15] Alteración de la información		MA	MA		
	[E.18] Destrucción de la información	MA	MA	MA		
	[E.19] Fugas de información	M	MA	MA		
	[E.24] caída del sistema por agotamiento de recursos	A				
	[A.5] suplantación de la identidad del usuario		A	A	MA	
	[A.6] Abuso de privilegios de acceso		A	A		
	[A.7] uso no previsto	MA	A	A		
	[A.11] Acceso no autorizado		A	A		
	[A.15] Modificación de la información		A			

Tabla 19. (Continuación)

ACTIVOS	Amenazas	Dimensiones				
		[D]	[I]	[C]	[A]	[T]
Controlador de dominio UPI La Vega	[A.18] Destrucción de la información	A	A			
	[A.19] revelación de información			A		
	[A.24] Denegación de servicio	A				
Controlador de dominio UPI El Perdomo	[E.2] Errores del administrador del sistema / de la seguridad	A	A	A		
	[E.15] Alteración de la información		MA	MA		
	[E.18] Destrucción de la información	MA	MA	MA		
	[E.19] Fugas de información	M	MA	MA		
	[E.24] caída del sistema por agotamiento de recursos	A				
	[A.5] suplantación de la identidad del usuario		A	A	MA	
	[A.6] Abuso de privilegios de acceso		A	A		
	[A.7] uso no previsto	MA	A	A		
	[A.11] Acceso no autorizado		A	A		
	[A.15] Modificación de la información		A			
	[A.18] Destrucción de la información	A				
	[A.19] revelación de información			A		
	[A.24] Denegación de servicio	A				

Tabla 19. (Continuación)

ACTIVOS	Amenazas	Dimensiones				
		[D]	[I]	[C]	[A]	[T]
Controlador de dominio UPI San Francisco	[E.2] Errores del administrador del sistema / de la seguridad	A	A	A		
	[E.15] Alteración de la información		MA	MA		
	[E.18] Destrucción de la información	MA	MA	MA		
	[E.19] Fugas de información	M	MA	MA		
	[E.24] caída del sistema por agotamiento de recursos	A				
	[A.5] suplantación de la identidad del usuario		A	A	MA	
	[A.6] Abuso de privilegios de acceso		A	A		
	[A.7] uso no previsto	MA	A	A		
	[A.11] Acceso no autorizado		A	A		
	[A.15] Modificación de la información		A			
	[A.18] Destrucción de la información	A	A			
	[A.19] revelación de información			A		
	[A.24] Denegación de servicio	A				
Portal Académico	[E.2] Errores del administrador del sistema / de la seguridad	A	A			
	[E.3] Errores de monitorización (log)	M	M			
	[E.4] Errores de configuración	A	A			

Tabla 19. (Continuación)

ACTIVOS	Amenazas	Dimensiones				
		[D]	[I]	[C]	[A]	[T]
Portal Académico	[E.15] Alteración de la información	M	M			
	[E.18] Destrucción de la información	A	A			
	[E.20] vulnerabilidades de los programas (software)	M	M			
	[E.21] Errores de mantenimiento / actualización de programas (software)	M	M			
	[E.24] caída del sistema por agotamiento de recursos	A	A			
	[E.28] Indisponibilidad del personal	M	M			
	[A.5] suplantación de la identidad del usuario	A	A	MA		
	[A.6] Abuso de privilegios de acceso	M	M			
	[A.8] Difusión de software dañino	A	A	MA		
	[A.11] Acceso no autorizado	A	A	MA		
	[A.15] Modificación de la información	M	M			
	[A.18] Destrucción de la información	A	A			
	[A.22] Manipulación de programas	M	M			
	[A.24] Denegación de servicio	A	A			

Tabla 19. (Continuación)

ACTIVOS	Amenazas	Dimensiones				
		[D]	[I]	[C]	[A]	[T]
Portal Institucional	[E.2] Errores del administrador del sistema / de la seguridad	A	A		B	
	[E.3] Errores de monitorización (log)	MB	MB			
	[E.4] Errores de configuración	MA	MA			
	[E.15] Alteración de la información		A	MB	B	
	[E.18] Destrucción de la información		MA		B	
	[E.20] vulnerabilidades de los programas (software)	MA	MA			
	[E.21] Errores de mantenimiento / actualización de programas (software)	A	A			
	[E.24] caída del sistema por agotamiento de recursos	MA	MA			
	[E.28] Indisponibilidad del personal			MB		
	[A.8] Difusión de software dañino	A	MA		B	
	[A.11] Acceso no autorizado		MA	B	M	
	[A.15] Modificación de la información		A	MB		
	[A.18] Destrucción de la información	MA	MA			
	[A.24] Denegación de servicio	MA				

Tabla 19. (Continuación)

ACTIVOS	Amenazas	Dimensiones				
		[D]	[I]	[C]	[A]	[T]
Controlador de dominio secundario	[E.2] Errores del administrador del sistema / de la seguridad	A	MA			
	[E.4] Errores de configuración	A	MA			
	[E.21] Errores de mantenimiento / actualización de programas (software)	M	A			
Sistema de Acceso Biométrico	[N.*] Desastres naturales	MA			MA	
	[I.1] Fuego	MA			MA	
	[I.2] Daños por agua	MA			MA	
	[I.5] Avería de origen físico o lógico	MA			MA	
	[I.6] Corte del suministro eléctrico	A			A	
	[A.25] Robo de equipos	MA			MA	
	[A.26] Ataque destructivo	MA			MA	
Canal de internet y red MPLS	[N.1] Fuego	MA				
	[N.2] Daños por agua	MA				
	[N.*] Desastres naturales	MA				
	[I.1] Fuego	MA				
	[I.5] Avería de origen físico o lógico	MA				
	[I.6] Corte del suministro eléctrico	MA				
	[I.7] Condiciones inadecuadas de temperatura o humedad	MA				

Tabla 19. (Continuación)

ACTIVOS	Amenazas	Dimensiones				
		[D]	[I]	[C]	[A]	[T]
Canal de internet y red MPLS	[I.8.12] Interrupción deliberada por un agente externo	MA				
	[E.4] Errores de configuración	MA				
	[E.23] Errores de mantenimiento / actualización de equipos (hardware)	A				
	[E.24] caída del sistema por agotamiento de recursos	MA				
	[A.25] Robo de equipos	MA				

Fuente: Autor

8.5.1.2 Impacto: [SW] APLICACIONES

Tabla 23. Impacto potencial activos de tipo: Aplicaciones

ACTIVOS	Amenazas	Dimensiones				
		[D]	[I]	[C]	[A]	[T]
Software de Aplicaciones (medios)	[N.1] Fuego	MA	MA			
	[I.5] Avería de origen físico o lógico	A	A			
	[A.7] uso no previsto	A	A			
Software de Sistemas operativos (medios)	[N.1] Fuego	MA	MA			
	[I.5] Avería de origen físico o lógico	A	A			
	[A.7] uso no previsto	A	A			
Software de Base de Datos (medios)	[N.1] Fuego	MA	B			

Tabla 20. (Continuación)

ACTIVOS	Amenazas	Dimensiones				
		[D]	[I]	[C]	[A]	[T]
Software de Base de Datos (medios)	[I.5] Avería de origen físico o lógico	A	MB			
	[A.7] uso no previsto	A	MB			
Medios con claves de licenciamiento	[N.1] Fuego	MA	MA			
	[I.5] Avería de origen físico o lógico	A	A			
	[A.7] uso no previsto	A	A			
Aplicación SIMI – AP	[E.1] Errores de los usuarios		MA		MA	
	[E.2] Errores del administrador del sistema / de la seguridad	A				
	[E.3] Errores de monitorización (log)	MA				
	[E.4] Errores de configuración	MA				
	[E.15] Alteración de la información		MA		MA	MA
	[E.19.1] A personal interno que no necesita conocerlo			MA		
	[E.20.dos] Denegación de Servicio	MA				
	[E.28.4] Personal insuficiente					MA
	[A.5.1] Por personal interno			MA		
	[A.7.1] Por personal interno			MA		
	[A.15.1] Sin beneficio para nadie			MA		
Servidor aplicativo SPRAI	[E.2] Errores del administrador del sistema / de la seguridad	B				

Tabla 20. (Continuación)

ACTIVOS	Amenazas	Dimensiones				
		[D]	[I]	[C]	[A]	[T]
Servidor aplicativo SPRAI	[E.4] Errores de configuración	B				
	[E.19.1] A personal interno que no necesita conocerlo			MA		
	[E.20.read] Acceso de LECTURA	B				
Consola Vcenter	[N.1] Fuego	MA	MA			
	[N.2] Daños por agua	MA	MA			
	[I.1] Fuego	MA	MA			
	[I.2] Daños por agua	MA	MA			
	[E.2] Errores del administrador del sistema / de la seguridad	A	A			
	[E.4] Errores de configuración	A	A			
	[E.24] caída del sistema por agotamiento de recursos	A	A			
	[A.8] Difusión de software dañino	A	A			
	[A.23] Manipulación del hardware	MA	MA			
	[A.24] Denegación de servicio	A	A			
	[A.26] Ataque destructivo	MA	MA			
Aplicación Idocument	[E.2] Errores del administrador del sistema / de la seguridad	A	A	B	M	
	[E.15] Alteración de la información		A	M		
Base de datos Oracle 11g	[N.1] Fuego	A	A	M		
	[N.*] Desastres naturales	A	A	M		

Tabla 20. (Continuación)

ACTIVOS	Amenazas	Dimensiones				
		[D]	[I]	[C]	[A]	[T]
Base de datos Oracle 11g	[E.1] Errores de los usuarios	M	A			
	[E.2] Errores del administrador del sistema / de la seguridad	A	M	M		
	[E.14] Fugas de información			M		
	[E.15] Alteración de la información		A	M		
	[E.18] Destrucción de la información	A	A	M		
	[A.6] Abuso de privilegios de acceso	M	A	M		
	[A.15] Modificación de la información		A	M		
	[A.30] Ingeniería social (picaresca)		M	B		
Aplicaciones Aranda Software - Parte Misional	[N.*] Desastres naturales	A				
	[I.6] Corte del suministro eléctrico	A				
	[I.7] Condiciones inadecuadas de temperatura o humedad	A				
	[E.1] Errores de los usuarios				M	
	[E.2] Errores del administrador del sistema / de la seguridad	M				
	[E.4] Errores de configuración	M				
	[E.18] Destrucción de la información		M			

Tabla 20. (Continuación)

ACTIVOS	Amenazas	Dimensiones				
		[D]	[I]	[C]	[A]	[T]
Aplicaciones Aranda Software - Parte Misional	[E.21] Errores de mantenimiento / actualización de programas (software)		M			
	[E.24] caída del sistema por agotamiento de recursos	A				
	[A.8] Difusión de software dañino	A	A			
	[A.11] Acceso no autorizado			M	A	
Aplicaciones Aranda Software - Parte Administrativa	[N.*] Desastres naturales	A				
	[I.6] Corte del suministro eléctrico	A				
	[I.7] Condiciones inadecuadas de temperatura o humedad	A				
	[E.1] Errores de los usuarios				M	
	[E.2] Errores del administrador del sistema / de la seguridad	M				
	[E.4] Errores de configuración	M				
	[E.18] Destrucción de la información		M			
	[E.21] Errores de mantenimiento / actualización de programas (software)		M			
	[E.24] caída del sistema por agotamiento de recursos	A				
	[A.8] Difusión de software dañino	A	A			

Tabla 20. (Continuación)

ACTIVOS	Amenazas	Dimensiones				
		[D]	[I]	[C]	[A]	[T]
	[A.11] Acceso no autorizado			M	A	
SYSMAN	[I.8] Fallos de servicios de comunicación	MA				
	[E.1] Errores de los usuarios	A	A	M		
	[E.2] Errores del administrador	MA	A	A		
	[E.4] Errores de configuración		MA			
	[E.14] Escapes de información			A		
	[E.15] Alteración accidental de la información		MA			
	[E.18] Destrucción de información	MA				
	[E.20] Vulnerabilidades de los programas (software)	A	A	M		
	[E.21] Errores de mantenimiento / actualización de programas (software)	MA	A			
	[E.24] Caída del sistema por agotamiento de recursos	MA				
	[A.5] Suplantación de la identidad del usuario		MA	A	MA	
	[A.6] Abuso de privilegios de acceso	A	MA	A		
	[A.7] Uso no previsto	A	MA	A		
	[A.11] Acceso no autorizado		MA	A		
	[A.15] Modificación de la información		MA			

Tabla 20. (Continuación)

ACTIVOS	Amenazas	Dimensiones				
		[D]	[I]	[C]	[A]	[T]
SYSMAN	[A.17] Corrupción de la información		MA	A		
	[A.18] Destrucción la información	MA				
	[A.19] Divulgación de información			A		
SICAPITAL	[E.1] Errores de los usuarios	M	M	M		
	[E.2] Errores del administrador	A	M	A		
	[E.4] Errores de configuración		A			
	[E.7] Deficiencias en la organización	A				
	[E.15] Alteración accidental de la información		A			
	[E.18] Destrucción de información	A				
	[E.20] Vulnerabilidades de los programas (software)	A	A	M		
	[E.21] Errores de mantenimiento / actualización de programas (software)	M	M			
	[E.24] Caída del sistema por agotamiento de recursos	A				
	[E.28] Indisponibilidad del personal	A				
Antivirus Kaspersky	[E.1] Errores de los usuarios	A	A			
	[E.2] Errores del administrador del sistema / de la seguridad	M	M			

Tabla 20. (Continuación)

ACTIVOS	Amenazas	Dimensiones				
		[D]	[I]	[C]	[A]	[T]
Antivirus Kaspersky	[E.3] Errores de monitorización (log)	A	A			M
	[E.4] Errores de configuración	A	A			
	[E.20] vulnerabilidades de los programas (software)	A	A			
	[E.21] Errores de mantenimiento / actualización de programas (software)	M	M			
	[A.6] Abuso de privilegios de acceso	M	M			
	[A.8] Difusión de software dañino	A	A			
	[A.11] Acceso no autorizado	M	M			
	[A.22] Manipulación de programas	M	M			

Fuente: Autor

8.5.1.3 Impacto: [HW] EQUIPOS

Tabla 24. Impacto potencial activos de tipo: Equipos

ACTIVOS	Amenazas	Impacto Acumulado				
		[D]	[I]	[C]	[A]	[T]
Antispam Barracuda	[N.1] Fuego	M				
	[N.2] Daños por agua	B				
	[N.*] Desastres naturales	M				
	[I.1] Fuego	M				
	[I.2] Daños por agua	B				
	[I.*] Desastres industriales	M				
	[I.3] Contaminación medioambiental	B				

Tabla 21. (Continuación)

ACTIVOS	Amenazas	Dimensiones				
		[D]	[I]	[C]	[A]	[T]
Antispam Barracuda	[I.5] Avería de origen físico o lógico	B				
	[I.6] Corte del suministro eléctrico	B				
	[I.7] Condiciones inadecuadas de temperatura o humedad	B				
	[E.2] Errores del administrador del sistema / de la seguridad	M	M			
	[E.23] Errores de mantenimiento / actualización de equipos (hardware)	B				
	[E.25] Pérdida de equipos	M				
	[A.6] Abuso de privilegios de acceso		B			
	[A.7] uso no previsto	B				
	[A.11] Acceso no autorizado		M			
	[A.23] Manipulación del hardware	M				
	[A.24] Denegación de servicio	M				
	[A.26] Ataque destructivo	M				
Impresora Datacard CP 40 Plus	[N.1] Fuego	MA				
	[N.2] Daños por agua	MA				
	[N.*] Desastres naturales	MA				
	[I.1] Fuego	MA				
	[I.2] Daños por agua	MA				
	[I.*] Desastres industriales	MA				

Tabla 21. (Continuación)

ACTIVOS	Amenazas	Dimensiones				
		[D]	[I]	[C]	[A]	[T]
Impresora Datacard CP 40 Plus	[I.3] Contaminación medioambiental	A				
	[I.4] Contaminación electromagnética	A				
	[I.5] Avería de origen físico o lógico	MA				
	[I.6] Corte del suministro eléctrico	MA				
	[I.7] Condiciones inadecuadas de temperatura o humedad	A				
	[E.2] Errores del administrador del sistema / de la seguridad	A				
	[E.23] Errores de mantenimiento / actualización de equipos (hardware)	MA				
	[E.24] caída del sistema por agotamiento de recursos	MA				
	[E.25] Pérdida de equipos	MA				
	[A.23] Manipulación del hardware	MA				
	[A.25] Robo de equipos	MA				
	[A.26] Ataque destructivo	MA				
Servidor UPI El Perdomo	[N.1] Fuego	A				
	[N.2] Daños por agua	A				
	[N.*] Desastres naturales	A				
	[I.5] Avería de origen físico o lógico	M				

Tabla 21. (Continuación)

ACTIVOS	Amenazas	Dimensiones				
		[D]	[I]	[C]	[A]	[T]
Servidor UPI El Perdomo	[I.6] Corte del suministro eléctrico	A				
	[I.7] Condiciones inadecuadas de temperatura o humedad	A				
	[E.2] Errores del administrador del sistema / de la seguridad	M	M	A		
	[E.4] Errores de configuración	M	M	M		
	[E.8] Difusión de software dañino	A	A			
	[E.23] Errores de mantenimiento / actualización de equipos (hardware)	B				
	[E.25] Pérdida de equipos	A				
	[A.6] Abuso de privilegios de acceso		M	M		
	[A.7] uso no previsto	M	M	M		
	[A.11] Acceso no autorizado		M	MA		
	[A.23] Manipulación del hardware	M		A		
	[A.24] Denegación de servicio	A				
	[A.25] Robo de equipos	A				
	[A.26] Ataque destructivo	A				
Servidor UPI La 27 Sur	[N.1] Fuego	A				
	[N.2] Daños por agua	A				
	[N.*] Desastres naturales	A				
	[I.5] Avería de origen físico o lógico	M				

Tabla 21. (Continuación)

ACTIVOS	Amenazas	Dimensiones				
		[D]	[I]	[C]	[A]	[T]
Servidor UPI La 27 Sur	[I.6] Corte del suministro eléctrico	A				
	[I.7] Condiciones inadecuadas de temperatura o humedad	A				
	[E.2] Errores del administrador del sistema / de la seguridad	M	M	A		
	[E.4] Errores de configuración	M	M	M		
	[E.8] Difusión de software dañino	A	A			
	[E.23] Errores de mantenimiento / actualización de equipos (hardware)	B				
	[E.25] Pérdida de equipos	A				
	[A.6] Abuso de privilegios de acceso		M	M		
	[A.7] uso no previsto	M	M	M		
	[A.11] Acceso no autorizado		M	MA		
	[A.23] Manipulación del hardware	M		A		
	[A.24] Denegación de servicio	A				
	[A.25] Robo de equipos	A				
	[A.26] Ataque destructivo	A				
Servidor UPI La 32	[N.1] Fuego	A				
	[N.2] Daños por agua	A				
	[N.*] Desastres naturales	A				
	[I.5] Avería de origen físico o lógico	M				

Tabla 21. (Continuación)

ACTIVOS	Amenazas	Dimensiones				
		[D]	[I]	[C]	[A]	[T]
Servidor UPI La 32	[I.6] Corte del suministro eléctrico	A				
	[I.7] Condiciones inadecuadas de temperatura o humedad	A				
	[E.2] Errores del administrador del sistema / de la seguridad	M	M	A		
	[E.4] Errores de configuración	M	M	M		
	[E.8] Difusión de software dañino	A	A			
	[E.23] Errores de mantenimiento / actualización de equipos (hardware)	B				
	[E.25] Pérdida de equipos	A				
	[A.6] Abuso de privilegios de acceso		M	M		
	[A.7] uso no previsto	M	M	M		
	[A.11] Acceso no autorizado		M	MA		
	[A.23] Manipulación del hardware	M		A		
	[A.24] Denegación de servicio	A				
	[A.25] Robo de equipos	A				
	[A.26] Ataque destructivo	A				
Servidor UPI La Florida	[N.1] Fuego	A				
	[N.2] Daños por agua	A				
	[N.*] Desastres naturales	A				
	[I.5] Avería de origen físico o lógico	M				

Tabla 21. (Continuación)

ACTIVOS	Amenazas	Dimensiones				
		[D]	[I]	[C]	[A]	[T]
Servidor UPI La Florida	[I.6] Corte del suministro eléctrico	A				
	[I.7] Condiciones inadecuadas de temperatura o humedad	A				
	[E.2] Errores del administrador del sistema / de la seguridad	M	M	A		
	[E.4] Errores de configuración	M	M	M		
	[E.8] Difusión de software dañino	A	A			
	[E.23] Errores de mantenimiento / actualización de equipos (hardware)	B				
	[E.25] Pérdida de equipos	A				
	[A.6] Abuso de privilegios de acceso		M	M		
	[A.7] uso no previsto	M	M	M		
	[A.11] Acceso no autorizado		M	MA		
	[A.23] Manipulación del hardware	M		A		
	[A.24] Denegación de servicio	A				
	[A.25] Robo de equipos	A				
	[A.26] Ataque destructivo	A				
Servidor UPI La Vega	[N.1] Fuego	A				
	[N.2] Daños por agua	A				
	[N.*] Desastres naturales	A				
	[I.5] Avería de origen físico o lógico	M				

Tabla 21. (Continuación)

ACTIVOS	Amenazas	Dimensiones				
		[D]	[I]	[C]	[A]	[T]
Servidor UPI La Vega	[I.6] Corte del suministro eléctrico	A				
	[I.7] Condiciones inadecuadas de temperatura o humedad	A				
	[E.2] Errores del administrador del sistema / de la seguridad	M	M	A		
	[E.4] Errores de configuración	M	M	M		
	[E.8] Difusión de software dañino	A	A			
	[E.23] Errores de mantenimiento / actualización de equipos (hardware)	B				
	[E.25] Pérdida de equipos	A				
	[A.6] Abuso de privilegios de acceso		M	M		
	[A.7] uso no previsto	M	M	M		
	[A.11] Acceso no autorizado		M	MA		
	[A.23] Manipulación del hardware	M		A		
	[A.24] Denegación de servicio	A				
	[A.25] Robo de equipos	A				
	[A.26] Ataque destructivo	A				
Access Point	[N.1] Fuego	M				
	[N.2] Daños por agua	M				
	[N.*] Desastres naturales	M				
	[I.5.3] Equipos de comunicaciones	M				

Tabla 21. (Continuación)

ACTIVOS	Amenazas	Dimensiones				
		[D]	[I]	[C]	[A]	[T]
Access Point	[I.7] Condiciones inadecuadas de temperatura o humedad	M				
	[I.8] Fallo de servicios de comunicaciones	B		M		
	[E.2] Errores del administrador del sistema / de la seguridad	B		M		
	[E.4] Errores de configuración	B		M		
	[E.19] Fugas de información	B		A		
	[E.23] Errores de mantenimiento / actualización de equipos (hardware)	B		M		
	[E.25] Pérdida de equipos	M				
	[A.5] suplantación de la identidad del usuario	B		A	A	
	[A.11] Acceso no autorizado	B		A	A	
	[A.23] Manipulación del hardware	B		A		
	[A.24.1] Saturación de los canales de comunicaciones	B				
	[A.25] Robo de equipos	M				
Servidor UPI La Arcadia	[N.1] Fuego	A				
	[N.2] Daños por agua	A				
	[N.*] Desastres naturales	A				
	[I.5] Avería de origen físico o lógico	M				
	[I.6] Corte del suministro eléctrico	A				

Tabla 21. (Continuación)

ACTIVOS	Amenazas	Dimensiones				
		[D]	[I]	[C]	[A]	[T]
Servidor UPI La Arcadia	[I.7] Condiciones inadecuadas de temperatura o humedad	A				
	[E.2] Errores del administrador del sistema / de la seguridad	M	M	A		
	[E.4] Errores de configuración	M	M	M		
	[E.8] Difusión de software dañino	A	A			
	[E.23] Errores de mantenimiento / actualización de equipos (hardware)	B				
	[E.25] Pérdida de equipos	A				
	[A.6] Abuso de privilegios de acceso		M	M		
	[A.7] uso no previsto	M	M	M		
	[A.11] Acceso no autorizado		M	MA		
	[A.23] Manipulación del hardware	M		A		
	[A.24] Denegación de servicio	A				
	[A.25] Robo de equipos	A				
	[A.26] Ataque destructivo	A				
Equipos de cómputo	[N.1] Fuego	M	MA	MA	A	
	[N.2] Daños por agua	M	MA	MA	A	
	[N.*] Desastres naturales	M	MA	MA	A	
	[I.1] Fuego	M	MA	MA	A	
	[I.2] Daños por agua	M	MA	MA	A	
	[I.*] Desastres industriales	M	MA	MA	A	
	[I.3] Contaminación medioambiental	M	MA	MA	A	

Tabla 21. (Continuación)

ACTIVOS	Amenazas	Dimensiones				
		[D]	[I]	[C]	[A]	[T]
Equipos de cómputo	[I.5] Avería de origen físico o lógico	B	A	MA	A	
	[I.6] Corte del suministro eléctrico	B	MA	A	M	
	[I.7] Condiciones inadecuadas de temperatura o humedad	B	A	A	M	
	[E.23] Errores de mantenimiento / actualización de equipos (hardware)	M	MA	A	M	
	[E.25] Pérdida de equipos	M	MA	MA	A	
	[A.6] Abuso de privilegios de acceso	B	MA	MA	M	
	[A.7] uso no previsto	B	MA	MA	M	
	[A.11] Acceso no autorizado	B	MA	MA	M	
	[A.23] Manipulación del hardware	B	MA	A	M	
	[A.25] Robo de equipos	M	MA	MA	A	
	[A.26] Ataque destructivo	M	MA	MA	M	
Servidor UPI San Francisco	[N.1] Fuego	A				
	[N.2] Daños por agua	A				
	[N.*] Desastres naturales	A				
	[I.5] Avería de origen físico o lógico	M				
	[I.6] Corte del suministro eléctrico	A				
	[I.7] Condiciones inadecuadas de temperatura o humedad	A				

Tabla 21. (Continuación)

ACTIVOS	Amenazas	Dimensiones				
		[D]	[I]	[C]	[A]	[T]
Servidor UPI San Francisco	[E.2] Errores del administrador del sistema / de la seguridad	M	M	A		
	[E.4] Errores de configuración	M	M	A		
	[E.8] Difusión de software dañino	A	A			
	[E.23] Errores de mantenimiento / actualización de equipos (hardware)	M				
	[E.25] Pérdida de equipos	A		MA		
	[A.6] Abuso de privilegios de acceso		M	A		
	[A.7] uso no previsto	M	M	A		
	[A.11] Acceso no autorizado		M	MA		
	[A.23] Manipulación del hardware	M		A		
	[A.24] Denegación de servicio	A				
	[A.24.3] Saturación de los recursos hardware	M				
	[A.25] Robo de equipos	A		MA		
	[A.26] Ataque destructivo	A				
Switch de borde 4210G	[N.2] Daños por agua	A				
	[N.*] Desastres naturales	A				
	[I.1] Fuego	A				
	[I.3] Contaminación medioambiental	A				
	[I.6] Corte del suministro eléctrico	A				

Tabla 21. (Continuación)

ACTIVOS	Amenazas	Dimensiones				
		[D]	[I]	[C]	[A]	[T]
Switch de borde 4210G	[I.7] Condiciones inadecuadas de temperatura o humedad	M				
	[E.2] Errores del administrador del sistema / de la seguridad	M				
	[E.4] Errores de configuración	M				
	[E.23] Errores de mantenimiento / actualización de equipos (hardware)	M				
	[A.7] uso no previsto	B				
	[A.11] Acceso no autorizado	M				
	[A.23] Manipulación del hardware	M				
	[A.25] Robo de equipos	A				
Sistema de almacenamiento formato rack	[I.6.12] Interrupción deliberada por un agente externo	MA	MA			
Gabinete de 8 blades	[E.23] Errores de mantenimiento / actualización de equipos (hardware)	MA	MA			
	[E.24] caída del sistema por agotamiento de recursos	MA	MA			
Equipo de Seguridad Perimetral	[N.1] Fuego	MA	A			
	[N.2] Daños por agua	MA	A			
	[N.*] Desastres naturales	MA	A			
	[E.2] Errores del administrador del sistema / de la seguridad	MA	A	M		

Tabla 21. (Continuación)

ACTIVOS	Amenazas	Dimensiones				
		[D]	[I]	[C]	[A]	[T]
Equipo de Seguridad Perimetral	[E.3] Errores de monitorización (log)		A	M		
	[E.4] Errores de configuración	MA	A	M		
	[E.21] Errores de mantenimiento / actualización de programas (software)	MA	A	M		
	[A.3] Manipulación de los registros de actividad (log)		M	M		
	[A.11] Acceso no autorizado	MA	A	M		
	[A.12] Análisis de tráfico		A	M		
	[A.23] Manipulación del hardware	MA	A	M		
	[A.24] Denegación de servicio	MA	A			
Servidor formato blade marca Hewlett Packard Modelo proliant BL460C G1	[N.1] Fuego	A				
	[N.2] Daños por agua	A				
	[N.*] Desastres naturales	A				
	[I.5] Avería de origen físico o lógico	M				
	[I.6] Corte del suministro eléctrico	A				
	[I.7] Condiciones inadecuadas de temperatura o humedad	A				
	[E.2] Errores del administrador del sistema / de la seguridad	M	M	A		
	[E.4] Errores de configuración	M	M	A		

Tabla 21. (Continuación)

ACTIVOS	Amenazas	Dimensiones				
		[D]	[I]	[C]	[A]	[T]
Servidor formato blade marca Hewlett Packard Modelo proliant BL460C G1	[E.8] Difusión de software dañino	A	A			
	[E.23] Errores de mantenimiento / actualización de equipos (hardware)	M				
	[E.25] Pérdida de equipos	A		MA		
	[A.6] Abuso de privilegios de acceso		M	A		
	[A.7] uso no previsto	M	M	A		
	[A.11] Acceso no autorizado		M	MA		
	[A.23] Manipulación del hardware	M		A		
	[A.24] Denegación de servicio	A				
	[A.24.3] Saturación de los recursos hardware	M				
	[A.25] Robo de equipos	A		MA		
	[A.26] Ataque destructivo	A				
Servidor formato blade marca Hewlett Packard. Modelo proliant BL460C G7	[N.1] Fuego	A				
	[N.2] Daños por agua	A				
	[N.*] Desastres naturales	A				
	[I.5] Avería de origen físico o lógico	M				
	[I.6] Corte del suministro eléctrico	A				
	[I.7] Condiciones inadecuadas de temperatura o humedad	A				

Tabla 21. (Continuación)

ACTIVOS	Amenazas	Dimensiones				
		[D]	[I]	[C]	[A]	[T]
Servidor formato blade marca Hewlett Packard. Modelo proliant BL460C G7	[E.2] Errores del administrador del sistema / de la seguridad	M	M	A		
	[E.4] Errores de configuración	M	M	A		
	[E.8] Difusión de software dañino	A	A			
	[E.23] Errores de mantenimiento / actualización de equipos (hardware)	M				
	[E.25] Pérdida de equipos	A		MA		
	[A.6] Abuso de privilegios de acceso		M	A		
	[A.7] uso no previsto	M	M	A		
	[A.11] Acceso no autorizado		M	MA		
	[A.23] Manipulación del hardware	M		A		
	[A.24] Denegación de servicio	A				
	[A.24.3] Saturación de los recursos hardware	M				
	[A.25] Robo de equipos	A		MA		
	[A.26] Ataque destructivo	A				
Servidor Proliant 120 G5	[N.1] Fuego	A				
	[N.2] Daños por agua	A				
	[N.*] Desastres naturales	A				
	[I.5] Avería de origen físico o lógico	M				
	[I.6] Corte del suministro eléctrico	A				

Tabla 21. (Continuación)

ACTIVOS	Amenazas	Dimensiones				
		[D]	[I]	[C]	[A]	[T]
Servidor Proliant 120 G5	[I.7] Condiciones inadecuadas de temperatura o humedad	A				
	[E.2] Errores del administrador del sistema / de la seguridad	M	M	A		
	[E.4] Errores de configuración	M	M	A		
	[E.8] Difusión de software dañino	A	A			
	[E.23] Errores de mantenimiento / actualización de equipos (hardware)	M				
	[E.25] Pérdida de equipos	A		MA		
	[A.6] Abuso de privilegios de acceso		M	A		
	[A.7] uso no previsto	M	M	A		
	[A.11] Acceso no autorizado		M	MA		
	[A.23] Manipulación del hardware	M		A		
	[A.24] Denegación de servicio	A				
	[A.24.3] Saturación de los recursos hardware	M				
	[A.25] Robo de equipos	A		MA		
	[A.26] Ataque destructivo	A				
Servidor Proyecto Misión Bogotá	[N.1] Fuego	A				
	[N.2] Daños por agua	A				
	[N.*] Desastres naturales	A				
	[I.5] Avería de origen físico o lógico	M				

Tabla 21. (Continuación)

ACTIVOS	Amenazas	Dimensiones				
		[D]	[I]	[C]	[A]	[T]
Servidor Proyecto Misión Bogotá	[I.6] Corte del suministro eléctrico	A				
	[I.7] Condiciones inadecuadas de temperatura o humedad	A				
	[E.2] Errores del administrador del sistema / de la seguridad	M	M	A		
	[E.4] Errores de configuración	M	M	A		
	[E.8] Difusión de software dañino	A	A			
	[E.23] Errores de mantenimiento / actualización de equipos (hardware)	M				
	[E.25] Pérdida de equipos	A		MA		
	[A.6] Abuso de privilegios de acceso		M	A		
	[A.7] uso no previsto	M	M	A		
	[A.11] Acceso no autorizado		M	MA		
	[A.23] Manipulación del hardware	M		A		
	[A.24] Denegación de servicio	A				
	[A.24.3] Saturación de los recursos hardware	M				
	[A.25] Robo de equipos	A		MA		
	[A.26] Ataque destructivo	A				
Impresora para código de barras	[N.1] Fuego	MA				
	[N.2] Daños por agua	MA				
	[N.*] Desastres naturales	MA				

Tabla 21. (Continuación)

ACTIVOS	Amenazas	Dimensiones				
		[D]	[I]	[C]	[A]	[T]
Impresora para código de barras	[I.1] Fuego	MA				
	[I.2] Daños por agua	MA				
	[I.*] Desastres industriales	MA				
	[I.3] Contaminación medioambiental	MA				
	[I.4] Contaminación electromagnética	A				
	[I.5] Avería de origen físico o lógico	A				
	[I.6] Corte del suministro eléctrico	MA				
	[I.7] Condiciones inadecuadas de temperatura o humedad	MA				
	[E.2] Errores del administrador del sistema / de la seguridad	A				
	[E.23] Errores de mantenimiento / actualización de equipos (hardware)	A				
	[E.24] caída del sistema por agotamiento de recursos	MA				
	[E.25] Pérdida de equipos	MA				
	[A.23] Manipulación del hardware	MA				
	[A.25] Robo de equipos	MA				
	[A.26] Ataque destructivo	MA				
Servidor controlador de dominio principal	[N.1] Fuego	MA				
	[N.2] Daños por agua	MA				

Tabla 21. (Continuación)

ACTIVOS	Amenazas	Dimensiones				
		[D]	[I]	[C]	[A]	[T]
Servidor controlador de dominio principal	[N.*] Desastres naturales	MA				
	[I.5] Avería de origen físico o lógico	A				
	[I.6] Corte del suministro eléctrico	MA				
	[I.7] Condiciones inadecuadas de temperatura o humedad	MA				
	[E.2] Errores del administrador del sistema / de la seguridad	A	A	A		
	[E.4] Errores de configuración	A	A	A		
	[E.8] Difusión de software dañino	MA	MA			
	[E.23] Errores de mantenimiento / actualización de equipos (hardware)	A				
	[E.25] Pérdida de equipos	MA		MA		
	[A.6] Abuso de privilegios de acceso		A	A		
	[A.7] uso no previsto	A	A	A		
	[A.11] Acceso no autorizado		A	MA		
	[A.23] Manipulación del hardware	A		A		
	[A.24] Denegación de servicio	MA				
	[A.24.3] Saturación de los recursos hardware	A				
	[A.25] Robo de equipos	MA		MA		
	[A.26] Ataque destructivo	MA				
Switch de borde 4800	[N.2] Daños por agua	A				

Tabla 21. (Continuación)

ACTIVOS	Amenazas	Dimensiones				
		[D]	[I]	[C]	[A]	[T]
Switch de borde 4800	[N.*] Desastres naturales	A				
	[I.1] Fuego	A				
	[I.3] Contaminación medioambiental	A				
	[I.6] Corte del suministro eléctrico	A				
	[I.7] Condiciones inadecuadas de temperatura o humedad	M				
	[E.2] Errores del administrador del sistema / de la seguridad	M				
	[E.4] Errores de configuración	M				
	[E.23] Errores de mantenimiento / actualización de equipos (hardware)	M				
	[A.7] uso no previsto	B				
	[A.11] Acceso no autorizado	M				
	[A.23] Manipulación del hardware	M				
	[A.25] Robo de equipos	A				
Switch de borde - Referencia 2410 - UPI La Rioja	[N.2] Daños por agua	A				
	[N.*] Desastres naturales	A				
	[I.1] Fuego	A				
	[I.3] Contaminación medioambiental	A				
	[I.6] Corte del suministro eléctrico	A				
	[I.7] Condiciones inadecuadas de temperatura o humedad	M				

Tabla 21. (Continuación)

ACTIVOS	Amenazas	Dimensiones				
		[D]	[I]	[C]	[A]	[T]
Switch de borde - Referencia 2410 - UPI La Rioja	[E.2] Errores del administrador del sistema / de la seguridad	M				
	[E.4] Errores de configuración	M				
	[E.23] Errores de mantenimiento / actualización de equipos (hardware)	M				
	[A.7] uso no previsto	B				
	[A.11] Acceso no autorizado	M				
	[A.23] Manipulación del hardware	M				
	[A.25] Robo de equipos	A				
Switch de borde - Referencia 2920 - Proyecto Misión Bogotá	[N.2] Daños por agua	A				
	[N.*] Desastres naturales	A				
	[I.1] Fuego	A				
	[I.3] Contaminación medioambiental	A				
	[I.6] Corte del suministro eléctrico	A				
	[I.7] Condiciones inadecuadas de temperatura o humedad	M				
	[E.2] Errores del administrador del sistema / de la seguridad	M				
	[E.4] Errores de configuración	M				
	[E.23] Errores de mantenimiento / actualización de equipos (hardware)	M				
	[A.7] uso no previsto	B				

Tabla 21. (Continuación)

ACTIVOS	Amenazas	Dimensiones				
		[D]	[I]	[C]	[A]	[T]
Switch de borde - Referencia 2920 - Proyecto Misión Bogotá	[A.11] Acceso no autorizado	M				
	[A.23] Manipulación del hardware	M				
	[A.25] Robo de equipos	A				
Switch de borde - Referencia 4250T	[N.2] Daños por agua	A				
	[N.*] Desastres naturales	A				
	[I.1] Fuego	A				
	[I.3] Contaminación medioambiental	A				
	[I.6] Corte del suministro eléctrico	A				
	[I.7] Condiciones inadecuadas de temperatura o humedad	M				
	[E.2] Errores del administrador del sistema / de la seguridad	M				
	[E.4] Errores de configuración	M				
	[E.23] Errores de mantenimiento / actualización de equipos (hardware)	M				
	[A.7] uso no previsto	B				
	[A.11] Acceso no autorizado	M				
	[A.23] Manipulación del hardware	M				
	[A.25] Robo de equipos	A				
Switch de borde - Referencia 4500G UPI La Florida	[N.2] Daños por agua	A				
	[N.*] Desastres naturales	A				
	[I.1] Fuego	A				

Tabla 21. (Continuación)

ACTIVOS	Amenazas	Dimensiones				
		[D]	[I]	[C]	[A]	[T]
Switch de borde - Referencia 4500G UPI La Florida	[I.3] Contaminación medioambiental	A				
	[I.6] Corte del suministro eléctrico	A				
	[I.7] Condiciones inadecuadas de temperatura o humedad	M				
	[E.2] Errores del administrador del sistema / de la seguridad	M				
	[E.4] Errores de configuración	M				
	[E.23] Errores de mantenimiento / actualización de equipos (hardware)	M				
	[A.7] uso no previsto	B				
	[A.11] Acceso no autorizado	M				
	[A.23] Manipulación del hardware	M				
	[A.25] Robo de equipos	A				
Switch de borde - Referencia 4800G - UPI La 32	[N.2] Daños por agua	A				
	[N.*] Desastres naturales	A				
	[I.1] Fuego	A				
	[I.3] Contaminación medioambiental	A				
	[I.6] Corte del suministro eléctrico	A				
	[I.7] Condiciones inadecuadas de temperatura o humedad	M				

Tabla 21. (Continuación)

ACTIVOS	Amenazas	Dimensiones				
		[D]	[I]	[C]	[A]	[T]
Switch de borde - Referencia 4800G - UPI La 32	[E.2] Errores del administrador del sistema / de la seguridad	M				
	[E.4] Errores de configuración	M				
	[E.23] Errores de mantenimiento / actualización de equipos (hardware)	M				
	[A.7] uso no previsto	B				
	[A.11] Acceso no autorizado	M				
	[A.23] Manipulación del hardware	M				
	[A.25] Robo de equipos	A				
Switch de borde - Referencia 4800G - UPI El Perdomo	[N.2] Daños por agua	A				
	[N.*] Desastres naturales	A				
	[I.1] Fuego	A				
	[I.3] Contaminación medioambiental	A				
	[I.6] Corte del suministro eléctrico	A				
	[I.7] Condiciones inadecuadas de temperatura o humedad	M				
	[E.2] Errores del administrador del sistema / de la seguridad	M				
	[E.4] Errores de configuración	M				
	[E.23] Errores de mantenimiento / actualización de equipos (hardware)	M				
	[A.7] uso no previsto	B				

Tabla 21. (Continuación)

ACTIVOS	Amenazas	Dimensiones				
		[D]	[I]	[C]	[A]	[T]
Switch de borde - Referencia 4800G - UPI El Perdomo	[A.11] Acceso no autorizado	M				
	[A.23] Manipulación del hardware	M				
	[A.25] Robo de equipos	A				
Switch de borde - Referencia 4800G - UPI La Florida	[N.2] Daños por agua	A				
	[N.*] Desastres naturales	A				
	[I.1] Fuego	A				
	[I.3] Contaminación medioambiental	A				
	[I.6] Corte del suministro eléctrico	A				
	[I.7] Condiciones inadecuadas de temperatura o humedad	M				
	[E.2] Errores del administrador del sistema / de la seguridad	M				
	[E.4] Errores de configuración	M				
	[E.23] Errores de mantenimiento / actualización de equipos (hardware)	M				
	[A.7] uso no previsto	B				
	[A.11] Acceso no autorizado	M				
	[A.23] Manipulación del hardware	M				
	[A.25] Robo de equipos	A				
Switch de borde - Referencia 4800G - UPI La 27 sur	[N.2] Daños por agua	A				
	[N.*] Desastres naturales	A				

Tabla 21. (Continuación)

ACTIVOS	Amenazas	Dimensiones				
		[D]	[I]	[C]	[A]	[T]
Switch de borde - Referencia 4800G - UPI La 27 sur	[I.1] Fuego	A				
	[I.3] Contaminación medioambiental	A				
	[I.6] Corte del suministro eléctrico	A				
	[I.7] Condiciones inadecuadas de temperatura o humedad	M				
	[E.2] Errores del administrador del sistema / de la seguridad	M				
	[E.4] Errores de configuración	M				
	[E.23] Errores de mantenimiento / actualización de equipos (hardware)	M				
	[A.7] uso no previsto	B				
	[A.11] Acceso no autorizado	M				
	[A.23] Manipulación del hardware	M				
	[A.25] Robo de equipos	A				
Switch de borde - Referencia 4800G - UPI San Francisco	[N.2] Daños por agua	A				
	[N.*] Desastres naturales	A				
	[I.1] Fuego	A				
	[I.3] Contaminación medioambiental	A				
	[I.6] Corte del suministro eléctrico	A				
	[I.7] Condiciones inadecuadas de temperatura o humedad	M				

Tabla 21. (Continuación)

ACTIVOS	Amenazas	Dimensiones				
		[D]	[I]	[C]	[A]	[T]
Switch de borde - Referencia 4800G - UPI San Francisco	[E.2] Errores del administrador del sistema / de la seguridad	M				
	[E.4] Errores de configuración	M				
	[E.23] Errores de mantenimiento / actualización de equipos (hardware)	M				
	[A.7] uso no previsto	B				
	[A.11] Acceso no autorizado	M				
	[A.23] Manipulación del hardware	M				
	[A.25] Robo de equipos	A				
Switch de borde - Referencia 4800G - UPI La Rioja	[N.2] Daños por agua	A				
	[N.*] Desastres naturales	A				
	[I.1] Fuego	A				
	[I.3] Contaminación medioambiental	A				
	[I.6] Corte del suministro eléctrico	A				
	[I.7] Condiciones inadecuadas de temperatura o humedad	M				
	[E.2] Errores del administrador del sistema / de la seguridad	M				
	[E.4] Errores de configuración	M				
	[E.23] Errores de mantenimiento / actualización de equipos (hardware)	M				
	[A.7] uso no previsto	B				

Tabla 21. (Continuación)

ACTIVOS	Amenazas	Dimensiones				
		[D]	[I]	[C]	[A]	[T]
Switch de borde - Referencia 4800G - UPI La Rioja	[A.11] Acceso no autorizado	M				
	[A.23] Manipulación del hardware	M				
	[A.25] Robo de equipos	A				
Switch de borde - Referencia 4800G - UPI La Vega	[N.2] Daños por agua	A				
	[N.*] Desastres naturales	A				
	[I.1] Fuego	A				
	[I.3] Contaminación medioambiental	A				
	[I.6] Corte del suministro eléctrico	A				
	[I.7] Condiciones inadecuadas de temperatura o humedad	M				
	[E.2] Errores del administrador del sistema / de la seguridad	M				
	[E.4] Errores de configuración	M				
	[E.23] Errores de mantenimiento / actualización de equipos (hardware)	M				
	[A.7] uso no previsto	B				
	[A.11] Acceso no autorizado	M				
	[A.23] Manipulación del hardware	M				
	[A.25] Robo de equipos	A				
Switch de borde - Referencia 4800G - UPI Santa Lucia	[N.2] Daños por agua	A				
	[N.*] Desastres naturales	A				

Tabla 21. (Continuación)

ACTIVOS	Amenazas	Dimensiones				
		[D]	[I]	[C]	[A]	[T]
Switch de borde - Referencia 4800G - UPI Santa Lucia	[I.1] Fuego	A				
	[I.3] Contaminación medioambiental	A				
	[I.6] Corte del suministro eléctrico	A				
	[I.7] Condiciones inadecuadas de temperatura o humedad	M				
	[E.2] Errores del administrador del sistema / de la seguridad	M				
	[E.4] Errores de configuración	M				
	[E.23] Errores de mantenimiento / actualización de equipos (hardware)	M				
	[A.7] uso no previsto	B				
	[A.11] Acceso no autorizado	M				
	[A.23] Manipulación del hardware	M				
	[A.25] Robo de equipos	A				
Switch de borde - Referencia 4800G - UPI Servitá	[N.2] Daños por agua	A				
	[N.*] Desastres naturales	A				
	[I.1] Fuego	A				
	[I.3] Contaminación medioambiental	A				
	[I.6] Corte del suministro eléctrico	A				
	[I.7] Condiciones inadecuadas de temperatura o humedad	M				

Tabla 21. (Continuación)

ACTIVOS	Amenazas	Dimensiones				
		[D]	[I]	[C]	[A]	[T]
Switch de borde - Referencia 4800G - UPI Servitá	[E.2] Errores del administrador del sistema / de la seguridad	M				
	[E.4] Errores de configuración	M				
	[E.23] Errores de mantenimiento / actualización de equipos (hardware)	M				
	[A.7] uso no previsto	B				
	[A.11] Acceso no autorizado	M				
	[A.23] Manipulación del hardware	M				
	[A.25] Robo de equipos	A				
Switch de borde - Referencia E2910 HP - UPI Bosa	[N.2] Daños por agua	A				
	[N.*] Desastres naturales	A				
	[I.1] Fuego	A				
	[I.3] Contaminación medioambiental	A				
	[I.6] Corte del suministro eléctrico	A				
	[I.7] Condiciones inadecuadas de temperatura o humedad	M				
	[E.2] Errores del administrador del sistema / de la seguridad	M				
	[E.4] Errores de configuración	M				
	[E.23] Errores de mantenimiento / actualización de equipos (hardware)	M				
	[A.7] uso no previsto	B				

Tabla 21. (Continuación)

ACTIVOS	Amenazas	Dimensiones				
		[D]	[I]	[C]	[A]	[T]
Switch de borde - Referencia E2910 HP - UPI Bosa	[A.11] Acceso no autorizado	M				
	[A.23] Manipulación del hardware	M				
	[A.25] Robo de equipos	A				
Switch de borde - Referencia E2910 HP - Proyecto 968	[N.2] Daños por agua	A				
	[N.*] Desastres naturales	A				
	[I.1] Fuego	A				
	[I.3] Contaminación medioambiental	A				
	[I.6] Corte del suministro eléctrico	A				
	[I.7] Condiciones inadecuadas de temperatura o humedad	M				
	[E.2] Errores del administrador del sistema / de la seguridad	M				
	[E.4] Errores de configuración	M				
	[E.23] Errores de mantenimiento / actualización de equipos (hardware)	M				
	[A.7] uso no previsto	B				
	[A.11] Acceso no autorizado	M				
	[A.23] Manipulación del hardware	M				
	[A.25] Robo de equipos	A				
Switch de borde - Referencia V1910 - Proyecto Misión Bogotá	[N.2] Daños por agua	A				

Tabla 21. (Continuación)

ACTIVOS	Amenazas	Dimensiones				
		[D]	[I]	[C]	[A]	[T]
Switch de borde - Referencia V1910 - Proyecto Misión Bogotá	[N.*] Desastres naturales	A				
	[I.1] Fuego	A				
	[I.3] Contaminación medioambiental	A				
	[I.6] Corte del suministro eléctrico	A				
	[I.7] Condiciones inadecuadas de temperatura o humedad	M				
	[E.2] Errores del administrador del sistema / de la seguridad	M				
	[E.4] Errores de configuración	M				
	[E.23] Errores de mantenimiento / actualización de equipos (hardware)	M				
	[A.7] uso no previsto	B				
	[A.11] Acceso no autorizado	M				
	[A.23] Manipulación del hardware	M				
	[A.25] Robo de equipos	A				
Switch de borde 4500G - Sede Administrativa	[N.2] Daños por agua	A				
	[N.*] Desastres naturales	A				
	[I.1] Fuego	A				
	[I.3] Contaminación medioambiental	A				
	[I.6] Corte del suministro eléctrico	A				
	[I.7] Condiciones inadecuadas de temperatura o humedad	M				

Tabla 21. (Continuación)

ACTIVOS	Amenazas	Dimensiones				
		[D]	[I]	[C]	[A]	[T]
Switch de borde 4500G - Sede Administrativa	[E.2] Errores del administrador del sistema / de la seguridad	M				
	[E.4] Errores de configuración	M				
	[E.23] Errores de mantenimiento / actualización de equipos (hardware)	M				
	[A.7] uso no previsto	B				
	[A.11] Acceso no autorizado	M				
	[A.23] Manipulación del hardware	M				
	[A.25] Robo de equipos	A				
Switch de borde. Referencia 4500G - UPI La Arcadia	[N.2] Daños por agua	A				
	[N.*] Desastres naturales	A				
	[I.1] Fuego	A				
	[I.3] Contaminación medioambiental	A				
	[I.6] Corte del suministro eléctrico	A				
	[I.7] Condiciones inadecuadas de temperatura o humedad	M				
	[E.2] Errores del administrador del sistema / de la seguridad	M				
	[E.4] Errores de configuración	M				
	[E.23] Errores de mantenimiento / actualización de equipos (hardware)	M				

Tabla 21. (Continuación)

ACTIVOS	Amenazas	Dimensiones				
		[D]	[I]	[C]	[A]	[T]
Switch de borde. Referencia 4500G - UPI La Arcadia	[A.7] uso no previsto	B				
	[A.11] Acceso no autorizado	M				
	[A.23] Manipulación del hardware	M				
	[A.25] Robo de equipos	A				
Switch de borde. Referencia 4800G - UPI La Arcadia	[N.2] Daños por agua	A				
	[N.*] Desastres naturales	A				
	[I.1] Fuego	A				
	[I.3] Contaminación medioambiental	A				
	[I.6] Corte del suministro eléctrico	A				
	[I.7] Condiciones inadecuadas de temperatura o humedad	M				
	[E.2] Errores del administrador del sistema / de la seguridad	M				
	[E.4] Errores de configuración	M				
	[E.23] Errores de mantenimiento / actualización de equipos (hardware)	M				
	[A.7] uso no previsto	B				
	[A.11] Acceso no autorizado	M				
	[A.23] Manipulación del hardware	M				
	[A.25] Robo de equipos	A				
Switch de core. Referencia	[N.2] Daños por agua	A				

Tabla 21. (Continuación)

ACTIVOS	Amenazas	Dimensiones				
		[D]	[I]	[C]	[A]	[T]
Switch de core. Referencia 5500G - Sede Administrativa	[N.*] Desastres naturales	A				
	[I.1] Fuego	A				
	[I.3] Contaminación medioambiental	A				
	[I.6] Corte del suministro eléctrico	A				
	[I.7] Condiciones inadecuadas de temperatura o humedad	M				
	[E.2] Errores del administrador del sistema / de la seguridad	M				
	[E.4] Errores de configuración	M				
	[E.23] Errores de mantenimiento / actualización de equipos (hardware)	M				
	[A.7] uso no previsto	B				
	[A.11] Acceso no autorizado	M				
	[A.23] Manipulación del hardware	M				
	[A.25] Robo de equipos	A				
Copia de Respaldo - Dataprotector	[N.2] Daños por agua	A				
	[N.*] Desastres naturales	A				
	[I.6] Corte del suministro eléctrico	A				
	[I.7] Condiciones inadecuadas de temperatura o humedad	M				
	[I.8] Fallo de servicios de comunicaciones	M				

Tabla 21. (Continuación)

ACTIVOS	Amenazas	Dimensiones				
		[D]	[I]	[C]	[A]	[T]
Copia de Respaldo - Dataprotector	[I.9] Interrupción de otros servicios o suministros esenciales	A				
	[E.2] Errores del administrador del sistema / de la seguridad	M				
	[E.4] Errores de configuración	A				
	[E.18] Destrucción de la información			A		
	[E.21] Errores de mantenimiento / actualización de programas (software)					
	[E.24] caída del sistema por agotamiento de recursos	M				
	[A.23] Manipulación del hardware	A				
Sistema de Backups - Dataprotector	[N.2] Daños por agua	A				
	[N.*] Desastres naturales	A				
	[I.6] Corte del suministro eléctrico	A				
	[I.7] Condiciones inadecuadas de temperatura o humedad	M				
	[I.8] Fallo de servicios de comunicaciones	M				
	[I.9] Interrupción de otros servicios o suministros esenciales	A				
	[E.2] Errores del administrador del sistema / de la seguridad	M				

Tabla 21. (Continuación)

ACTIVOS	Amenazas	Dimensiones				
		[D]	[I]	[C]	[A]	[T]
Sistema de Backups - Dataprotector	[E.4] Errores de configuración	A				
	[E.18] Destrucción de la información			A		
	[E.21] Errores de mantenimiento / actualización de programas (software)					
	[E.24] caída del sistema por agotamiento de recursos	M				
	[A.23] Manipulación del hardware	A				
Servidor de correo - Proliant DL 380 G5	[N.1] Fuego	MA				
	[N.2] Daños por agua	MA				
	[N.*] Desastres naturales	MA				
	[I.5] Avería de origen físico o lógico	A				
	[I.6] Corte del suministro eléctrico	MA				
	[I.7] Condiciones inadecuadas de temperatura o humedad	A				
	[E.2] Errores del administrador del sistema / de la seguridad	A	A	A		
	[E.4] Errores de configuración	A	A	A		
	[E.8] Difusión de software dañino	MA				
	[E.23] Errores de mantenimiento / actualización de equipos (hardware)	A				
	[E.25] Pérdida de equipos	MA				

Tabla 21. (Continuación)

ACTIVOS	Amenazas	Dimensiones				
		[D]	[I]	[C]	[A]	[T]
Servidor de correo - Proliant DL 380 G5	[A.6] Abuso de privilegios de acceso		A	A		
	[A.7] uso no previsto	A	A	A		
	[A.11] Acceso no autorizado		A	MA		
	[A.23] Manipulación del hardware	A		A		
	[A.24] Denegación de servicio	MA				
	[A.25] Robo de equipos	MA				
	[A.26] Ataque destructivo	MA				
Servidor Ambiente de pruebas y desarrollo	[N.1] Fuego	M	M			
	[N.2] Daños por agua	M	M			
	[N.*] Desastres naturales	M	M			
	[E.1] Errores de los usuarios	B				
	[E.2] Errores del administrador del sistema / de la seguridad	B	B			
	[E.4] Errores de configuración	B	B			
	[E.19] Fugas de información		B			
Servidor de base de datos Nómina	[N.1] Fuego	MA	MA	MA		
	[N.2] Daños por agua	MA	MA	MA		
	[N.*] Desastres naturales	MA	MA	MA		
	[E.1] Errores de los usuarios	A	MA			
	[E.2] Errores del administrador del sistema / de la seguridad	MA	A	MA		
	[E.14] Fugas de información			MA		

Tabla 21. (Continuación)

ACTIVOS	Amenazas	Dimensiones				
		[D]	[I]	[C]	[A]	[T]
Servidor de base de datos Nómina	[E.15] Alteración de la información		MA	MA		
	[E.18] Destrucción de la información	MA	MA	MA		
	[A.6] Abuso de privilegios de acceso	A	MA	MA		
	[A.15] Modificación de la información		MA	MA		
Servidor de Virtualización	[N.1] Fuego	MA	MA			
	[N.2] Daños por agua	MA	MA			
	[I.1] Fuego	MA	MA			
	[I.2] Daños por agua	MA	MA			
	[E.2] Errores del administrador del sistema / de la seguridad	A	A			
	[E.4] Errores de configuración	A	A			
	[E.24] caída del sistema por agotamiento de recursos	A	A			
	[A.8] Difusión de software dañino	A	A			
	[A.23] Manipulación del hardware	MA	MA			
	[A.24] Denegación de servicio	A	A			
	[A.26] Ataque destructivo	MA	MA			
Servidor base de datos SQL	[N.*] Desastres naturales	A	A			
	[E.2] Errores del administrador del sistema / de la seguridad	M	M			
	[E.4] Errores de configuración	M	M			
	[E.15] Alteración de la información	M	M			

Tabla 21. (Continuación)

ACTIVOS	Amenazas	Dimensiones				
		[D]	[I]	[C]	[A]	[T]
Servidor base de datos SQL	[E.21] Errores de mantenimiento / actualización de programas (software)	B				
	[A.6] Abuso de privilegios de acceso			M		
	[A.8] Difusión de software dañino	A	A			
	[A.11] Acceso no autorizado			A		
	[A.15] Modificación de la información		A	A		
Servidor de Archivos	[N.2] Daños por agua	MA	MA			
	[N.*] Desastres naturales	MA	MA			
	[I.3] Contaminación medioambiental	MA				
	[I.6] Corte del suministro eléctrico	MA				
	[I.7] Condiciones inadecuadas de temperatura o humedad	A				
	[E.1] Errores de los usuarios		MA			
	[E.2] Errores del administrador del sistema / de la seguridad	M				
	[E.4] Errores de configuración	M				
	[E.15] Alteración de la información		MA			
	[E.18] Destrucción de la información		MA			
	[E.24] caída del sistema por agotamiento de recursos	A				
	[A.6] Abuso de privilegios de acceso		MA	MA	MA	

Tabla 21. (Continuación)

ACTIVOS	Amenazas	Dimensiones				
		[D]	[I]	[C]	[A]	[T]
Servidor de Archivos	[A.8] Difusión de software dañino	A	A			
	[A.11] Acceso no autorizado		MA	MA		
	[A.15] Modificación de la información		MA	MA		
	[A.18] Destrucción de la información		MA	MA		
Servidor de impresión	[N.1] Fuego	MA				A
	[N.2] Daños por agua	MA				A
	[N.*] Desastres naturales	MA				A
	[I.5] Avería de origen físico o lógico	MA				A
	[I.6] Corte del suministro eléctrico	MA				A
	[I.7] Condiciones inadecuadas de temperatura o humedad	MA				A
	[I.8.11] Interrupción accidental	MA				A
	[E.2] Errores del administrador del sistema / de la seguridad	A				M
	[E.4] Errores de configuración	A				M
	[E.21] Errores de mantenimiento / actualización de programas (software)	A				M
	[E.24] caída del sistema por agotamiento de recursos	MA				A
	[A.5] suplantación de la identidad del usuario	MA				A

Tabla 21. (Continuación)

ACTIVOS	Amenazas	Dimensiones				
		[D]	[I]	[C]	[A]	[T]
Servidor de impresión	[A.6] Abuso de privilegios de acceso	MA				A
	[A.8] Difusión de software dañino	MA				A
	[A.11] Acceso no autorizado	MA				A
	[A.24] Denegación de servicio	MA				A
Servidor OAS – SICAPITAL	[N.1] Fuego	A				
	[N.2] Daños por agua	A				
	[N.*] Desastres naturales	A				
	[I.5] Avería de origen físico o lógico	M	M			
	[I.6] Corte del suministro eléctrico	A	M			
	[I.7] Condiciones inadecuadas de temperatura o humedad	A	M			
	[I.8.11] Interrupción accidental	M				
	[E.2] Errores del administrador del sistema / de la seguridad	M				
	[E.4] Errores de configuración	A				
	[E.21] Errores de mantenimiento / actualización de programas (software)	M				
	[E.23] Errores de mantenimiento / actualización de equipos (hardware)	M				
	[E.24] caída del sistema por agotamiento de recursos	A				

Tabla 21. (Continuación)

ACTIVOS	Amenazas	Dimensiones				
		[D]	[I]	[C]	[A]	[T]
Servidor OAS – SICAPITAL	[A.4] Manipulación de los ficheros de configuración	A				
	[A.5] suplantación de la identidad del usuario		M	M	M	
	[A.6] Abuso de privilegios de acceso		M	M	M	
	[A.18] Destrucción de la información		A	M	M	
	[A.24] Denegación de servicio	A				

Fuente: Autor

8.5.1.4 Impacto: [AUX] ELEMENTOS AUXILIARES

Tabla 25. Impacto potencial activos de tipo: Elementos Auxiliares

ACTIVOS	Amenazas	Dimensiones				
		[D]	[I]	[C]	[A]	[T]
UPS de 15 KVA - UPI La Arcadia	[N.2] Daños por agua	B				
	[N.*] Desastres naturales	M				
	[I.1] Fuego	M				
	[I.5] Avería de origen físico o lógico	B				
	[I.6] Corte del suministro eléctrico	B				
	[I.7] Condiciones inadecuadas de temperatura o humedad	MB				
	[I.9] Interrupción de otros servicios o suministros esenciales	B				

Tabla 22. (Continuación)

ACTIVOS	Amenazas	Dimensiones				
		[D]	[I]	[C]	[A]	[T]
UPS de 15 KVA - UPI La Arcadia	[E.23] Errores de mantenimiento / actualización de equipos (hardware)	B				
	[A.7] uso no previsto	B				
	[A.23] Manipulación del hardware	B				
UPS de 15 KVA - UPI La Rioja	[N.2] Daños por agua	B				
	[N.*] Desastres naturales	M				
	[I.1] Fuego	M				
	[I.5] Avería de origen físico o lógico	B				
	[I.6] Corte del suministro eléctrico	B				
	[I.7] Condiciones inadecuadas de temperatura o humedad	MB				
	[I.9] Interrupción de otros servicios o suministros esenciales	B				
	[E.23] Errores de mantenimiento / actualización de equipos (hardware)	B				
	[A.7] uso no previsto	B				
	[A.23] Manipulación del hardware	B				
Planta eléctrica	[N.*] Desastres naturales	M				
	[I.1] Fuego	M				
	[I.3] Contaminación medioambiental	B				

Tabla 22. (Continuación)

ACTIVOS	Amenazas	Dimensiones				
		[D]	[I]	[C]	[A]	[T]
Planta eléctrica	[I.5] Avería de origen físico o lógico	B				
	[I.6] Corte del suministro eléctrico	B				
	[I.7] Condiciones inadecuadas de temperatura o humedad	B				
	[I.9] Interrupción de otros servicios o suministros esenciales	B				
	[E.23] Errores de mantenimiento / actualización de equipos (hardware)	B				
	[A.26] Ataque destructivo	M				
UPS de 10 KVA - Sede Misión Bogotá	[N.2] Daños por agua	B				
	[N.*] Desastres naturales	M				
	[I.1] Fuego	M				
	[I.5] Avería de origen físico o lógico	B				
	[I.6] Corte del suministro eléctrico	B				
	[I.7] Condiciones inadecuadas de temperatura o humedad	MB				
	[I.9] Interrupción de otros servicios o suministros esenciales	B				

Tabla 22. (Continuación)

ACTIVOS	Amenazas	Dimensiones				
		[D]	[I]	[C]	[A]	[T]
UPS de 10 KVA - Sede Misión Bogotá	[E.23] Errores de mantenimiento / actualización de equipos (hardware)	B				
	[A.7] uso no previsto	B				
	[A.23] Manipulación del hardware	B				
UPS de 10 KVA - UPI La vega	[N.2] Daños por agua	B				
	[N.*] Desastres naturales	M				
	[I.1] Fuego	M				
	[I.5] Avería de origen físico o lógico	B				
	[I.6] Corte del suministro eléctrico	B				
	[I.7] Condiciones inadecuadas de temperatura o humedad	MB				
	[I.9] Interrupción de otros servicios o suministros esenciales	B				
	[E.23] Errores de mantenimiento / actualización de equipos (hardware)	B				
	[A.7] uso no previsto	B				
	[A.23] Manipulación del hardware	B				
UPS de 15 KVA - UPI Santa Lucia	[N.2] Daños por agua	B				
	[N.*] Desastres naturales	M				
	[I.1] Fuego	M				

Tabla 22. (Continuación)

ACTIVOS	Amenazas	Dimensiones				
		[D]	[I]	[C]	[A]	[T]
UPS de 15 KVA - UPI Santa Lucia	[I.5] Avería de origen físico o lógico	B				
	[I.6] Corte del suministro eléctrico	B				
	[I.7] Condiciones inadecuadas de temperatura o humedad	MB				
	[I.9] Interrupción de otros servicios o suministros esenciales	B				
	[E.23] Errores de mantenimiento / actualización de equipos (hardware)	B				
	[A.7] uso no previsto	B				
	[A.23] Manipulación del hardware	B				
UPS de 10 KVA - UPI San Francisco	[N.2] Daños por agua	B				
	[N.*] Desastres naturales	M				
	[I.1] Fuego	M				
	[I.5] Avería de origen físico o lógico	B				
	[I.6] Corte del suministro eléctrico	B				
	[I.7] Condiciones inadecuadas de temperatura o humedad	MB				
	[I.9] Interrupción de otros servicios o suministros esenciales	B				

Tabla 22. (Continuación)

ACTIVOS	Amenazas	Dimensiones				
		[D]	[I]	[C]	[A]	[T]
UPS de 10 KVA - UPI San Francisco	[E.23] Errores de mantenimiento / actualización de equipos (hardware)	B				
	[A.7] uso no previsto	B				
	[A.23] Manipulación del hardware	B				
UPS de 15 KVA - UPI El Perdomo	[N.2] Daños por agua	B				
	[N.*] Desastres naturales	M				
	[I.1] Fuego	M				
	[I.5] Avería de origen físico o lógico	B				
	[I.6] Corte del suministro eléctrico	B				
	[I.7] Condiciones inadecuadas de temperatura o humedad	MB				
	[I.9] Interrupción de otros servicios o suministros esenciales	B				
	[E.23] Errores de mantenimiento / actualización de equipos (hardware)	B				
	[A.7] uso no previsto	B				
	[A.23] Manipulación del hardware	B				
UPS de 15 KVA - UPI La 27 sur	[N.2] Daños por agua	B				
	[N.*] Desastres naturales	M				
	[I.1] Fuego	M				

Tabla 22. (Continuación)

ACTIVOS	Amenazas	Dimensiones				
		[D]	[I]	[C]	[A]	[T]
UPS de 15 KVA - UPI La 27 sur	[I.5] Avería de origen físico o lógico	B				
	[I.6] Corte del suministro eléctrico	B				
	[I.7] Condiciones inadecuadas de temperatura o humedad	MB				
	[I.9] Interrupción de otros servicios o suministros esenciales	B				
	[E.23] Errores de mantenimiento / actualización de equipos (hardware)	B				
	[A.7] uso no previsto	B				
	[A.23] Manipulación del hardware	B				
UPS de 15 KVA - UPI Servitá	[N.2] Daños por agua	B				
	[N.*] Desastres naturales	M				
	[I.1] Fuego	M				
	[I.5] Avería de origen físico o lógico	B				
	[I.6] Corte del suministro eléctrico	B				
	[I.7] Condiciones inadecuadas de temperatura o humedad	MB				
	[I.9] Interrupción de otros servicios o suministros esenciales	B				

Tabla 22. (Continuación)

ACTIVOS	Amenazas	Dimensiones				
		[D]	[I]	[C]	[A]	[T]
UPS de 15 KVA - UPI Servitá	[E.23] Errores de mantenimiento / actualización de equipos (hardware)	B				
	[A.7] uso no previsto	B				
	[A.23] Manipulación del hardware	B				
UPS de 15 KVA - UPI La Florida	[N.2] Daños por agua	B				
	[N.*] Desastres naturales	M				
	[I.1] Fuego	M				
	[I.5] Avería de origen físico o lógico	B				
	[I.6] Corte del suministro eléctrico	B				
	[I.7] Condiciones inadecuadas de temperatura o humedad	MB				
	[I.9] Interrupción de otros servicios o suministros esenciales	B				
	[E.23] Errores de mantenimiento / actualización de equipos (hardware)	B				
	[A.7] uso no previsto	B				
	[A.23] Manipulación del hardware	B				
UPS de 20 KVA - Sede proyecto 968	[N.2] Daños por agua	B				

Tabla 22. (Continuación)

ACTIVOS	Amenazas	Dimensiones				
		[D]	[I]	[C]	[A]	[T]
UPS de 20 KVA - Sede proyecto 968	[N.*] Desastres naturales	M				
	[I.1] Fuego	M				
	[I.5] Avería de origen físico o lógico	B				
	[I.6] Corte del suministro eléctrico	B				
	[I.7] Condiciones inadecuadas de temperatura o humedad	MB				
	[I.9] Interrupción de otros servicios o suministros esenciales	B				
	[E.23] Errores de mantenimiento / actualización de equipos (hardware)	B				
	[A.7] uso no previsto	B				
	[A.23] Manipulación del hardware	B				
UPS de 10 KVA - UPI Bosa	[N.2] Daños por agua	B				
	[N.*] Desastres naturales	M				
	[I.1] Fuego	M				
	[I.5] Avería de origen físico o lógico	B				
	[I.6] Corte del suministro eléctrico	B				
	[I.7] Condiciones inadecuadas de temperatura o humedad	MB				

Tabla 22. (Continuación)

ACTIVOS	Amenazas	Dimensiones				
		[D]	[I]	[C]	[A]	[T]
UPS de 10 KVA - UPI Bosa	[I.9] Interrupción de otros servicios o suministros esenciales	B				
	[E.23] Errores de mantenimiento / actualización de equipos (hardware)	B				
	[A.7] uso no previsto	B				
	[A.23] Manipulación del hardware	B				
UPS de 20 KVA - UPI La 32	[N.2] Daños por agua	B				
	[N.*] Desastres naturales	M				
	[I.1] Fuego	M				
	[I.5] Avería de origen físico o lógico	B				
	[I.6] Corte del suministro eléctrico	B				
	[I.7] Condiciones inadecuadas de temperatura o humedad	MB				
	[I.9] Interrupción de otros servicios o suministros esenciales	B				
	[E.23] Errores de mantenimiento / actualización de equipos (hardware)	B				
	[A.7] uso no previsto	B				
	[A.23] Manipulación del hardware	B				

Tabla 22. (Continuación)

ACTIVOS	Amenazas	Dimensiones				
		[D]	[I]	[C]	[A]	[T]
UPS de 20 KVA - UPI La Florida	[N.2] Daños por agua	B				
	[N.*] Desastres naturales	M				
	[I.1] Fuego	M				
	[I.5] Avería de origen físico o lógico	B				
	[I.6] Corte del suministro eléctrico	B				
	[I.7] Condiciones inadecuadas de temperatura o humedad	MB				
	[I.9] Interrupción de otros servicios o suministros esenciales	B				
	[E.23] Errores de mantenimiento / actualización de equipos (hardware)	B				
	[A.7] uso no previsto	B				
	[A.23] Manipulación del hardware	B				
UPS de 30 KVA - UPI El Perdomo	[N.2] Daños por agua	B				
	[N.*] Desastres naturales	M				
	[I.1] Fuego	M				
	[I.5] Avería de origen físico o lógico	B				
	[I.6] Corte del suministro eléctrico	B				
	[I.7] Condiciones inadecuadas de temperatura o humedad	MB				

Tabla 22. (Continuación)

ACTIVOS	Amenazas	Dimensiones				
		[D]	[I]	[C]	[A]	[T]
UPS de 30 KVA - UPI El Perdomo	[I.9] Interrupción de otros servicios o suministros esenciales	B				
	[E.23] Errores de mantenimiento / actualización de equipos (hardware)	B				
	[A.7] uso no previsto	B				
	[A.23] Manipulación del hardware	B				
Sistema de aire acondicionado	[N.*] Desastres naturales	MA				
	[I.5] Avería de origen físico o lógico	MA				
	[I.6] Corte del suministro eléctrico	A				

Fuente: Autor

8.5.1.5 Impacto: [D] DATOS / INFORMACIÓN

Tabla 26. Impacto potencial activos de tipo: Datos / Información

ACTIVOS	Amenazas	Impacto				
		[D]	[I]	[C]	[A]	[T]
Documentación Técnica	[N.2] Daños por agua	A	A			
	[N.*] Desastres naturales	A	A			
	[I.1] Fuego	A	A			
	[I.7] Condiciones inadecuadas de temperatura o humedad	M	M			
	[E.18] Destrucción de la información	M	M			

Fuente: Autor

8.5.1.6 Impacto: [P] PERSONAL

Tabla 27. Impacto potencial activos de tipo: Personal

ACTIVOS	Amenazas	Impacto				
		[D]	[I]	[C]	[A]	[T]
Administradores de Sistemas	[E.7] Deficiencias en la organización	M				
	[E.28] Indisponibilidad del personal	A				
	[A.29] Extorsión	M	B	M		
	[A.30] Ingeniería Social	M	M	M		

Fuente: Autor

8.5.2 Riesgo Potencial

En este apartado el objetivo es determinar el riesgo potencial al que está sometido el sistema, conociendo el impacto de las amenazas sobre los activos.
Entendiéndose como riesgo a la medida del daño probable sobre un sistema.

Para la estimación del riesgo se toman los valores de la probabilidad de ocurrencia de cada amenaza frente a los activos y el impacto acumulado, con base a la siguiente tabla de valoraciones para la estimación del riesgo (tabla 25).

Tabla 28. Criterios de valoración para estimación de riesgo

RIESGO		Probabilidad				
		MB	B	M	A	MA
Impacto	MA	A	MA	MA	MA	MA
	A	M	A	A	MA	MA
	M	B	M	M	A	A
	B	MB	B	B	M	M
	MB	MB	MB	MB	B	B

Fuente: MAGERIT v.3 – Libro II – Catálogo de elementos

8.5.2.1 Riesgo Potencial: [IS] SERVICIOS

Tabla 29. Riesgo potencial activos de tipo: Servicios

ACTIVOS	Amenazas	Impacto					P	RIESGO				
		[D]	[I]	[C]	[A]	[T]		[D]	[I]	[C]	[A]	[T]
Controlador de dominio UPI La 27 sur	[E.2] Errores del administrador del sistema / de la seguridad	A	A	A			B	A	A	A		
	[E.15] Alteración de la información		MA	MA			MB		A	A		
	[E.18] Destrucción de la información	MA	MA	MA			MB	A	A	A		
	[E.19] Fugas de información	M	MA	MA			B	M	MA	MA		
	[E.24] caída del sistema por agotamiento de recursos	A					B	A				
	[A.5] suplantación de la identidad del usuario		A	A	MA		MB		M	M	A	
	[A.6] Abuso de privilegios de acceso		A	A			M		A	A		
	[A.7] uso no previsto	MA	A	A			M	MA	A	A		
	[A.11] Acceso no autorizado		A	A			M		A	A		
	[A.15] Modificación de la información		A				A		MA			
	[A.18] Destrucción de la información	A	A				M	A	A			
	[A.19] revelación de información			A			M			A		
	[A.24] Denegación de servicio	A					A	MA				
Controlador de dominio misional	[E.2] Errores del administrador del sistema / de la seguridad	A	A	A			B	A	A	A		
	[E.15] Alteración de la información		MA	MA			MB		A	A		
	[E.18] Destrucción de la información	MA	MA	MA			MB	A	A	A		
	[E.19] Fugas de información	M	MA	MA			B	M	MA	MA		
	[E.24] caída del sistema por agotamiento de recursos	A					B	A				
	[A.5] suplantación de la identidad del usuario		A	A	MA		MB		M	M	A	
	[A.6] Abuso de privilegios de acceso		A	A			M		A	A		
	[A.7] uso no previsto	MA	A	A			M	MA	A	A		
	[A.11] Acceso no autorizado		A	A			M		A	A		

Tabla 26. (Continuación)

ACTIVOS	Amenazas	Impacto					P	RIESGO				
		[D]	[I]	[C]	[A]	[T]		[D]	[I]	[C]	[A]	[T]
Controlador de dominio misional	[A.15] Modificación de la información		A				A		MA			
	[A.18] Destrucción de la información	A	A				M	A	A			
	[A.19] revelación de información			A			M			A		
	[A.24] Denegación de servicio	A					A	MA				
Controlador de dominio principal	[E.2] Errores del administrador del sistema / de la seguridad	A	A	A			B	A	A	A		
	[E.15] Alteración de la información		MA	MA			MB		A	A		
	[E.18] Destrucción de la información	MA	MA	MA			MB	A	A	A		
	[E.19] Fugas de información	M	MA	MA			B	M	MA	MA		
	[E.24] caída del sistema por agotamiento de recursos	A					B	A				
	[A.5] suplantación de la identidad del usuario		A	A	MA		MB		M	M	A	
	[A.6] Abuso de privilegios de acceso		A	A			M		A	A		
	[A.7] uso no previsto	MA	A	A			M	MA	A	A		
	[A.11] Acceso no autorizado		A	A			M		A	A		
	[A.15] Modificación de la información		A				A		MA			
	[A.18] Destrucción de la información	A	A				M	A	A			
	[A.19] revelación de información			A			M			A		
	[A.24] Denegación de servicio	A					A	MA				
Controlador de dominio Misión Bogotá	[E.2] Errores del administrador del sistema / de la seguridad	A	A	A			B	A	A	A		
	[E.15] Alteración de la información		MA	MA			MB		A	A		
	[E.18] Destrucción de la información	MA	MA	MA			MB	A	A	A		
	[E.19] Fugas de información	M	MA	MA			B	M	MA	MA		
	[E.24] caída del sistema por agotamiento de recursos	A					B	A				
	[A.5] suplantación de la identidad del usuario		A	A	MA		MB		M	M	A	

Tabla 26. (Continuación)

ACTIVOS	Amenazas	Impacto					P	RIESGO				
		[D]	[I]	[C]	[A]	[T]		[D]	[I]	[C]	[A]	[T]
Controlador de dominio Misión Bogotá	[A.6] Abuso de privilegios de acceso		A	A			M		A	A		
	[A.7] uso no previsto	MA	A	A			M	MA	A	A		
	[A.11] Acceso no autorizado		A	A			M		A	A		
	[A.15] Modificación de la información		A				A		MA			
	[A.18] Destrucción de la información	A	A				M	A	A			
	[A.19] revelación de información			A			M			A		
	[A.24] Denegación de servicio	A					A	MA				
Controlador de dominio UPI La 32	[E.2] Errores del administrador del sistema / de la seguridad	A	A	A			B	A	A	A		
	[E.15] Alteración de la información		MA	MA			MB		A	A		
	[E.18] Destrucción de la información	MA	MA	MA			MB	A	A	A		
	[E.19] Fugas de información	M	MA	MA			B	M	MA	MA		
	[E.24] caída del sistema por agotamiento de recursos	A					B	A				
	[A.5] suplantación de la identidad del usuario		A	A	MA		MB		M	M	A	
	[A.6] Abuso de privilegios de acceso		A	A			M		A	A		
	[A.7] uso no previsto	MA	A	A			M	MA	A	A		
	[A.11] Acceso no autorizado		A	A			M		A	A		
	[A.15] Modificación de la información		A				A		MA			
	[A.18] Destrucción de la información	A	A				M	A	A			
	[A.19] revelación de información			A			M			A		
	[A.24] Denegación de servicio	A					A	MA				
Controlador de dominio UPI La Arcadia	[E.2] Errores del administrador del sistema / de la seguridad	A	A	A			B	A	A	A		
	[E.15] Alteración de la información		MA	MA			MB		A	A		
	[E.18] Destrucción de la información	MA	MA	MA			MB	A	A	A		
	[E.19] Fugas de información	M	MA	MA			B	M	MA	MA		

Tabla 26. (Continuación)

ACTIVOS	Amenazas	Impacto					P	RIESGO				
		[D]	[I]	[C]	[A]	[T]		[D]	[I]	[C]	[A]	[T]
Controlador de dominio UPI La Arcadia	[E.24] caída del sistema por agotamiento de recursos	A					B	A				
	[A.5] suplantación de la identidad del usuario		A	A	MA		MB		M	M	A	
	[A.6] Abuso de privilegios de acceso		A	A			M		A	A		
	[A.7] uso no previsto	MA	A	A			M	MA	A	A		
	[A.11] Acceso no autorizado		A	A			M		A	A		
	[A.15] Modificación de la información		A				A		MA			
	[A.18] Destrucción de la información	A	A				M	A	A			
	[A.19] revelación de información			A			M			A		
	[A.24] Denegación de servicio	A					A	MA				
Controlador de dominio UPI La Florida	[E.2] Errores del administrador del sistema / de la seguridad	A	A	A			B	A	A	A		
	[E.15] Alteración de la información		MA	MA			MB		A	A		
	[E.18] Destrucción de la información	MA	MA	MA			MB	A	A	A		
	[E.19] Fugas de información	M	MA	MA			B	M	MA	MA		
	[E.24] caída del sistema por agotamiento de recursos	A					B	A				
	[A.5] suplantación de la identidad del usuario		A	A	MA		MB		M	M	A	
	[A.6] Abuso de privilegios de acceso		A	A			M		A	A		
	[A.7] uso no previsto	MA	A	A			M	MA	A	A		
	[A.11] Acceso no autorizado		A	A			M		A	A		
	[A.15] Modificación de la información		A				A		MA			
	[A.18] Destrucción de la información	A	A				M	A	A			
	[A.19] revelación de información			A			M			A		
	[A.24] Denegación de servicio	A					A	MA				
Correo electrónico ZIMBRA MTA	[E.1] Errores de los usuarios	A	MA	MA			A	MA	MA	MA		

Tabla 26. (Continuación)

ACTIVOS	Amenazas	Impacto					P	RIESGO				
		[D]	[I]	[C]	[A]	[T]		[D]	[I]	[C]	[A]	[T]
Correo electrónico ZIMBRA MTA	[E.2] Errores del administrador del sistema / de la seguridad	A	A	A			M	A	A	A		
	[E.15] Alteración de la información		A				B		A			
	[E.18] Destrucción de la información	MA	MA				A	MA	MA			
	[E.19] Fugas de información			MA			A			MA		
	[E.24] caída del sistema por agotamiento de recursos	A					A	MA				
	[A.5] suplantación de la identidad del usuario		A	A	A		M		A	A	A	
	[A.6] Abuso de privilegios de acceso		MA	MA			M		MA	MA		
	[A.7] uso no previsto	MA	A	A			M	MA	A	A		
	[A.11] Acceso no autorizado		A	A			M		A	A		
	[A.13] Repudio (negación de actuaciones)		MA				M		MA			
	[A.18] Destrucción de la información	A					M	A				
	[A.19] revelación de información			A			M			A		
	[A.24] Denegación de servicio	A					A	MA				
Correo Exchange	[E.1] Errores de los usuarios	MB	B	B			MB	MB	MB	MB		
	[E.2] Errores del administrador del sistema / de la seguridad	MB	MB	MB			MB	MB	MB	MB		
	[E.15] Alteración de la información		MB				MB		MB			
	[E.18] Destrucción de la información	B	B				MB	MB	MB			
	[E.19] Fugas de información			B			MB			MB		
	[E.24] caída del sistema por agotamiento de recursos	MB					MB	MB				
	[A.5] suplantación de la identidad del usuario		MB	MB	B		MB		MB	MB	MB	
	[A.6] Abuso de privilegios de acceso		B	B			MB		MB	MB		
	[A.7] uso no previsto	B	MB	MB			MB	MB	MB	MB		
	[A.11] Acceso no autorizado		MB	MB			MB		MB	MB		
	[A.13] Repudio (negación de actuaciones)		B				MB		MB			

Tabla 26. (Continuación)

ACTIVOS	Amenazas	Impacto					P	RIESGO				
		[D]	[I]	[C]	[A]	[T]		[D]	[I]	[C]	[A]	[T]
Correo Exchange	[A.18] Destrucción de la información	MB					MB	MB				
	[A.19] revelación de información			MB			MB			MB		
	[A.24] Denegación de servicio	MB					MB	MB				
Controlador de dominio UPI La Vega	[E.2] Errores del administrador del sistema / de la seguridad	A	A	A			B	A	A	A		
	[E.15] Alteración de la información		MA	MA			MB		A	A		
	[E.18] Destrucción de la información	MA	MA	MA			MB	A	A	A		
	[E.19] Fugas de información	M	MA	MA			B	M	MA	MA		
	[E.24] caída del sistema por agotamiento de recursos	A					B	A				
	[A.5] suplantación de la identidad del usuario		A	A	MA		MB		M	M	A	
	[A.6] Abuso de privilegios de acceso		A	A			M		A	A		
	[A.7] uso no previsto	MA	A	A			M	MA	A	A		
	[A.11] Acceso no autorizado		A	A			M		A	A		
	[A.15] Modificación de la información		A				A		MA			
	[A.18] Destrucción de la información	A	A				M	A	A			
	[A.19] revelación de información			A			M			A		
	[A.24] Denegación de servicio	A					A	MA				
Controlador de dominio UPI El Perdomo	[E.2] Errores del administrador del sistema / de la seguridad	A	A	A			B	A	A	A		
	[E.15] Alteración de la información		MA	MA			MB		A	A		
	[E.18] Destrucción de la información	MA	MA	MA			MB	A	A	A		
	[E.19] Fugas de información	M	MA	MA			B	M	MA	MA		
	[E.24] caída del sistema por agotamiento de recursos	A					B	A				
	[A.5] suplantación de la identidad del usuario		A	A	MA		MB		M	M	A	
	[A.6] Abuso de privilegios de acceso		A	A			M		A	A		

Tabla 26. (Continuación)

ACTIVOS	Amenazas	Impacto					P	RIESGO				
		[D]	[I]	[C]	[A]	[T]		[D]	[I]	[C]	[A]	[T]
Controlador de dominio UPI El Perdomo	[A.7] uso no previsto	MA	A	A			M	MA	A	A		
	[A.11] Acceso no autorizado		A	A			M		A	A		
	[A.15] Modificación de la información		A				A		MA			
	[A.18] Destrucción de la información	A					M	A				
	[A.19] revelación de información			A			M			A		
	[A.24] Denegación de servicio	A					A	MA				
Controlador de dominio UPI San Francisco	[E.2] Errores del administrador del sistema / de la seguridad	A	A	A			B	A	A	A		
	[E.15] Alteración de la información		MA	MA			MB		A	A		
	[E.18] Destrucción de la información	MA	MA	MA			MB	A	A	A		
	[E.19] Fugas de información	M	MA	MA			B	M	MA	MA		
	[E.24] caída del sistema por agotamiento de recursos	A					B	A				
	[A.5] suplantación de la identidad del usuario		A	A	MA		MB		M	M	A	
	[A.6] Abuso de privilegios de acceso		A	A			M		A	A		
	[A.7] uso no previsto	MA	A	A			M	MA	A	A		
	[A.11] Acceso no autorizado		A	A			M		A	A		
	[A.15] Modificación de la información		A				A		MA			
	[A.18] Destrucción de la información	A	A				M	A	A			
	[A.19] revelación de información			A			M			A		
	[A.24] Denegación de servicio	A					A	MA				
Portal Académico	[E.2] Errores del administrador del sistema / de la seguridad	A	A				M	A	A			
	[E.3] Errores de monitorización (log)	M	M				M	M	M			
	[E.4] Errores de configuración	A	A				A	MA	MA			
	[E.15] Alteración de la información	M	M				MB	B	B			
	[E.18] Destrucción de la información	A	A				MB	M	M			

Tabla 26. (Continuación)

ACTIVOS	Amenazas	Impacto					P	RIESGO				
		[D]	[I]	[C]	[A]	[T]		[D]	[I]	[C]	[A]	[T]
Portal Académico	[E.20] vulnerabilidades de los programas (software)	M	M				M	M	M			
	[E.21] Errores de mantenimiento / actualización de programas (software)	M	M				M	M	M			
	[E.24] caída del sistema por agotamiento de recursos	A	A				B	A	A			
	[E.28] Indisponibilidad del personal	M	M				M	M	M			
	[A.5] suplantación de la identidad del usuario	A	A	MA			B	A	A	MA		
	[A.6] Abuso de privilegios de acceso	M	M				B	M	M			
	[A.8] Difusión de software dañino	A	A	MA			M	A	A	MA		
	[A.11] Acceso no autorizado	A	A	MA			M	A	A	MA		
	[A.15] Modificación de la información	M	M				B	M	M			
	[A.18] Destrucción de la información	A	A				MB	M	M			
	[A.22] Manipulación de programas	M	M				M	M	M			
	[A.24] Denegación de servicio	A	A				M	A	A			
Portal Institucional	[E.2] Errores del administrador del sistema / de la seguridad	A	A		B		MB	M	M		MB	
	[E.3] Errores de monitorización (log)	MB	MB				B	MB	MB			
	[E.4] Errores de configuración	MA	MA				B	MA	MA			
	[E.15] Alteración de la información		A	MB	B		B		A	MB	B	
	[E.18] Destrucción de la información		MA		B		B		MA		B	
	[E.20] vulnerabilidades de los programas (software)	MA	MA				M	MA	MA			
	[E.21] Errores de mantenimiento / actualización de programas (software)	A	A				M	A	A			
	[E.24] caída del sistema por agotamiento de recursos	MA	MA				B	MA	MA			

Tabla 26. (Continuación)

ACTIVOS	Amenazas	Impacto					P	RIESGO				
		[D]	[I]	[C]	[A]	[T]		[D]	[I]	[C]	[A]	[T]
Portal Institucional	[E.28] Indisponibilidad del personal			MB			MB			MB		
	[A.8] Difusión de software dañino	A	MA		B		B	A	MA		B	
	[A.11] Acceso no autorizado		MA	B	M		B		MA	B	M	
	[A.15] Modificación de la información		A	MB			MB		M	MB		
	[A.18] Destrucción de la información	MA	MA				B	MA	MA			
	[A.24] Denegación de servicio	MA					MB	A				
Controlador de dominio secundario	[E.2] Errores del administrador del sistema / de la seguridad	A	MA				B	A	MA			
	[E.4] Errores de configuración	A	MA				MB	M	A			
	[E.21] Errores de mantenimiento / actualización de programas (software)	M	A				B	M	A			
Sistema de Acceso Biométrico	[N.*] Desastres naturales	MA			MA		MB	A			A	
	[I.1] Fuego	MA			MA		MB	A			A	
	[I.2] Daños por agua	MA			MA		MB	A			A	
	[I.5] Avería de origen físico o lógico	MA			MA		MB	A			A	
	[I.6] Corte del suministro eléctrico	A			A		M	A			A	
	[A.25] Robo de equipos	MA			MA		MB	A			A	
	[A.26] Ataque destructivo	MA			MA		MB	A			A	
Canal de internet y red MPLS	[N.1] Fuego	MA					MB	A				
	[N.2] Daños por agua	MA					MB	A				
	[N.*] Desastres naturales	MA					MB	A				
	[I.1] Fuego	MA					MB	A				
	[I.5] Avería de origen físico o lógico	MA					MB	A				
	[I.6] Corte del suministro eléctrico	MA					B	MA				
	[I.7] Condiciones inadecuadas de temperatura o humedad	MA					MB	A				
	[I.8.12] Interrupción deliberada por un agente externo	MA					M	MA				

Tabla 26. (Continuación)

ACTIVOS	Amenazas	Impacto					P	RIESGO				
		[D]	[I]	[C]	[A]	[T]		[D]	[I]	[C]	[A]	[T]
Canal de internet y red MPLS	[E.4] Errores de configuración	MA					MB	A				
	[E.23] Errores de mantenimiento / actualización de equipos (hardware)	A					MB	M				
	[E.24] caída del sistema por agotamiento de recursos	MA					MB	A				
	[A.25] Robo de equipos	MA					M	MA				

Fuente: Autor

8.5.2.2 Riesgo Potencial: [SW] APLICACIONES

Tabla 30. Riesgo potencial activos de tipo: Aplicaciones

ACTIVOS	Amenazas	Impacto					P	Riesgo				
		[D]	[I]	[C]	[A]	[T]		[D]	[I]	[C]	[A]	[T]
Software de Aplicaciones (medios)	[N.1] Fuego	MA	MA				MB	A	A			
	[I.5] Avería de origen físico o lógico	A	A				M	A	A			
	[A.7] uso no previsto	A	A				B	A	A			
Software de Sistemas operativos (medios)	[N.1] Fuego	MA	MA				MB	A	A			
	[I.5] Avería de origen físico o lógico	A	A				M	A	A			
	[A.7] uso no previsto	A	A				B	A	A			
Software de Base de Datos (medios)	[N.1] Fuego	MA	B				MB	A	MB			
	[I.5] Avería de origen físico o lógico	A	MB				M	A	MB			
	[A.7] uso no previsto	A	MB				B	A	MB			
Medios con claves de licenciamiento	[N.1] Fuego	MA	MA				MB	A	A			
	[I.5] Avería de origen físico o lógico	A	A				M	A	A			
	[A.7] uso no previsto	A	A				B	A	A			
Aplicación SIMI – AP	[E.1] Errores de los usuarios		MA		MA		M		MA		MA	

Tabla 27. (Continuación)

ACTIVOS	Amenazas	Impacto					P	RIESGO				
		[D]	[I]	[C]	[A]	[T]		[D]	[I]	[C]	[A]	[T]
Aplicación SIMI – AP	[E.2] Errores del administrador del sistema / de la seguridad	A					B	A				
	[E.3] Errores de monitorización (log)	MA					MB	A				
	[E.4] Errores de configuración	MA					MB	A				
	[E.15] Alteración de la información		MA		MA	MA	B		MA		MA	MA
	[E.19.1] A personal interno que no necesita conocerlo			MA			MB			A		
	[E.20.dos] Denegación de Servicio	MA					M	MA				
	[E.28.4] Personal insuficiente					MA	M					MA
	[A.5.1] Por personal interno			MA			B			MA		
	[A.7.1] Por personal interno			MA			MB			A		
	[A.15.1] Sin beneficio para nadie			MA			MB			A		
Servidor aplicativo SPRAI	[E.2] Errores del administrador del sistema / de la seguridad	B					B	B				
	[E.4] Errores de configuración	B					B	B				
	[E.19.1] A personal interno que no necesita conocerlo			MA			M			MA		
Servidor aplicativo SPRAI SPRAI	[E.20.read] Acceso de LECTURA	B					MB	MB				
Consola Vcenter	[N.1] Fuego	MA	MA				M	MA	MA			
	[N.2] Daños por agua	MA	MA				M	MA	MA			
	[I.1] Fuego	MA	MA				M	MA	MA			
	[I.2] Daños por agua	MA	MA				M	MA	MA			
	[E.2] Errores del administrador del sistema / de la seguridad	A	A				MB	M	M			
	[E.4] Errores de configuración	A	A				MB	M	M			
	[E.24] caída del sistema por agotamiento de recursos	A	A				B	A	A			
	[A.8] Difusión de software dañino	A	A				M	A	A			
	[A.23] Manipulación del hardware	MA	MA				MB	A	A			
	[A.24] Denegación de servicio	A	A				MB	M	M			

Tabla 27. (Continuación)

ACTIVOS	Amenazas	Impacto					P	RIESGO				
		[D]	[I]	[C]	[A]	[T]		[D]	[I]	[C]	[A]	[T]
Consola Vcenter	[A.26] Ataque destructivo	MA	MA				MB	A	A			
Aplicación Idocument	[E.2] Errores del administrador del sistema / de la seguridad	A	A	B	M		M	A	A	B	M	
	[E.15] Alteración de la información		A	M			B		A	M		
Base de datos Oracle 11g	[N.1] Fuego	A	A	M			MB	M	M	B		
	[N.*] Desastres naturales	A	A	M			MB	M	M	B		
	[E.1] Errores de los usuarios	M	A				M	M	A			
	[E.2] Errores del administrador del sistema / de la seguridad	A	M	M			M	A	M	M		
	[E.14] Fugas de información			M			M			M		
	[E.15] Alteración de la información		A	M			M		A	M		
	[E.18] Destrucción de la información	A	A	M			B	A	A	M		
	[A.6] Abuso de privilegios de acceso	M	A	M			M	M	A	M		
	[A.15] Modificación de la información		A	M			B		A	M		
	[A.30] Ingeniería social (picaresca)		M	B			MB		B	MB		
Aplicaciones Aranda Software - Parte Misional	[N.*] Desastres naturales	A					MB	M				
Aplicaciones Aranda Software - Parte Misional	[I.6] Corte del suministro eléctrico	A					B	A				
	[I.7] Condiciones inadecuadas de temperatura o humedad	A					MB	M				
	[E.1] Errores de los usuarios				M		B				M	
	[E.2] Errores del administrador del sistema / de la seguridad	M					B	M				
	[E.4] Errores de configuración	M					B	M				
	[E.18] Destrucción de la información		M				B		M			
	[E.21] Errores de mantenimiento / actualización de programas (software)		M				A		A			

Tabla 27. (Continuación)

ACTIVOS	Amenazas	Impacto					P	RIESGO				
		[D]	[I]	[C]	[A]	[T]		[D]	[I]	[C]	[A]	[T]
Aplicaciones Aranda Software - Parte Misional	[E.24] caída del sistema por agotamiento de recursos	A					MB	M				
	[A.8] Difusión de software dañino	A	A				MB	M	M			
	[A.11] Acceso no autorizado			M	A		M			M	A	
Aplicaciones Aranda Software - Parte Administrativa	[N.*] Desastres naturales	A					MB	M				
	[I.6] Corte del suministro eléctrico	A					B	A				
	[I.7] Condiciones inadecuadas de temperatura o humedad	A					MB	M				
	[E.1] Errores de los usuarios				M		B				M	
	[E.2] Errores del administrador del sistema / de la seguridad	M					B	M				
	[E.4] Errores de configuración	M					B	M				
	[E.18] Destrucción de la información		M				B		M			
	[E.21] Errores de mantenimiento / actualización de programas (software)		M				A		A			
	[E.24] caída del sistema por agotamiento de recursos	A					MB	M				
	[A.8] Difusión de software dañino	A	A				MB	M	M			
	[A.11] Acceso no autorizado			M	A		M			M		
SYSMAN	[I.8] Fallos de servicios de comunicación	MA					M	MA				
	[E.1] Errores de los usuarios	A	A	M			M	A	A	M		
	[E.2] Errores del administrador	MA	A	A			B	MA	A	A		
	[E.4] Errores de configuración		MA				B		MA			
	[E.14] Escapes de información			A			B			A		
	[E.15] Alteración accidental de la información		MA				M		MA			
	[E.18] Destrucción de información	MA					M	MA				
	[E.20] Vulnerabilidades de los programas (software)	A	A	M			A	MA	MA	A		

Tabla 27. (Continuación)

ACTIVOS	Amenazas	Impacto					P	RIESGO				
		[D]	[I]	[C]	[A]	[T]		[D]	[I]	[C]	[A]	[T]
SYSMAN	[E.21] Errores de mantenimiento / actualización de programas (software)	MA	A				A	MA	MA			
	[E.24] Caída del sistema por agotamiento de recursos	MA					M	MA				
	[A.5] Suplantación de la identidad del usuario		MA	A	MA		M		MA	A	MA	
	[A.6] Abuso de privilegios de acceso	A	MA	A			M	A	MA	A		
	[A.7] Uso no previsto	A	MA	A			M	A	MA	A		
	[A.11] Acceso no autorizado		MA	A			B		MA	A		
	[A.15] Modificación de la información		MA				A		MA			
	[A.17] Corrupción de la información		MA	A			M		MA	A		
	[A.18] Destrucción la información	MA					B	MA				
	[A.19] Divulgación de información			A			M			A		
SICAPITAL	[E.1] Errores de los usuarios	M	M	M			A	A	A	A		
	[E.2] Errores del administrador	A	M	A			B	A	M	A		
	[E.4] Errores de configuración		A				M		A			
	[E.7] Deficiencias en la organización	A					A	MA				
	[E.15] Alteración accidental de la información		A				M		A			
	[E.18] Destrucción de información	A					B	A				
	[E.20] Vulnerabilidades de los programas (software)	A	A	M			M	A	A	M		
	[E.21] Errores de mantenimiento / actualización de	M	M				M	M	M			
	programas (software)											
	[E.24] Caída del sistema por agotamiento de recursos	A					B	A				
	[E.28] Indisponibilidad del personal	A					A	MA				
Antivirus Kaspersky	[E.1] Errores de los usuarios	A	A				B	A	A			
	[E.2] Errores del administrador del sistema / de la seguridad	M	M				B	M	M			

Tabla 27. (Continuación)

ACTIVOS	Amenazas	Impacto					P	RIESGO				
		[D]	[I]	[C]	[A]	[T]		[D]	[I]	[C]	[A]	[T]
Antivirus Kaspersky	[E.3] Errores de monitorización (log)	A	A			M	MB	M	M			B
	[E.4] Errores de configuración	A	A				MB	M	M			
	[E.20] vulnerabilidades de los programas (software)	A	A				MB	M	M			
	[E.21] Errores de mantenimiento / actualización de programas (software)	M	M				MB	B	B			
	[A.6] Abuso de privilegios de acceso	M	M				MB	B	B			
	[A.8] Difusión de software dañino	A	A				MB	M	M			
	[A.11] Acceso no autorizado	M	M				MB	B	B			
	[A.22] Manipulación de programas	M	M				B	M	M			

Fuente: Autor

8.5.2.3 Riesgo Potencial: [HW] EQUIPOS

Tabla 31. Riesgo potencial activos de tipo: Equipos

ACTIVOS	Amenazas	Impacto Acumulado					P	Riesgo				
		[D]	[I]	[C]	[A]	[T]		[D]	[I]	[C]	[A]	T
Antispam Barracuda	[N.1] Fuego	M					B	M				
	[N.2] Daños por agua	B					M	B				
	[N.*] Desastres naturales	M					MB	B				
	[I.1] Fuego	M					B	M				
	[I.2] Daños por agua	B					M	B				
	[I.*] Desastres industriales	M					MB	B				
	[I.3] Contaminación medioambiental	B					M	B				
	[I.5] Avería de origen físico o lógico	B					M	B				
Antispam Barracuda	[I.6] Corte del suministro eléctrico	B					A	M				
	[I.7] Condiciones inadecuadas de temperatura o humedad	B					M	B				
	[E.2] Errores del administrador del sistema / de la seguridad	M	M				A	A	A			

Tabla 28. (Continuación)

ACTIVOS	Amenazas	Impacto Acumulado					P	Riesgo				
		[D]	[I]	[C]	[A]	[T]		[D]	[I]	[C]	[A]	T
Antispam Barracuda	[E.23] Errores de mantenimiento / actualización de equipos (hardware)	B					A	M				
	[E.25] Pérdida de equipos	M					B	M				
	[A.6] Abuso de privilegios de acceso		B				B		B			
	[A.7] uso no previsto	B					B	B				
	[A.11] Acceso no autorizado		M				M		M			
	[A.23] Manipulación del hardware	M					B	M				
	[A.24] Denegación de servicio	M					M	M				
	[A.26] Ataque destructivo	M					M	M				
Impresora Datacard CP 40 Plus	[N.1] Fuego	MA					MB	A				
	[N.2] Daños por agua	MA					MB	A				
	[N.*] Desastres naturales	MA					MB	A				
	[I.1] Fuego	MA					MB	A				
	[I.2] Daños por agua	MA					MB	A				
	[I.*] Desastres industriales	MA					MB	A				
	[I.3] Contaminación medioambiental	A					MB	M				
	[I.4] Contaminación electromagnética	A					MB	M				
	[I.5] Avería de origen físico o lógico	MA					M	MA				
	[I.6] Corte del suministro eléctrico	MA					B	MA				
	[I.7] Condiciones inadecuadas de temperatura o humedad	A					MB	M				
	[E.2] Errores del administrador del sistema / de la seguridad	A					MB	M				
	[E.23] Errores de mantenimiento / actualización de equipos (hardware)	MA					B	MA				
	[E.24] caída del sistema por agotamiento de recursos	MA					MB	A				
Impresora Datacard CP 40 Plus	[E.25] Pérdida de equipos	MA					MB	A				

Tabla 28. (Continuación)

ACTIVOS	Amenazas	Impacto Acumulado					P	Riesgo				
		[D]	[I]	[C]	[A]	[T]		[D]	[I]	[C]	[A]	T
Impresora Datacard CP 40 Plus	[A.23] Manipulación del hardware	MA					B	MA				
	[A.25] Robo de equipos	MA					MB	A				
	[A.26] Ataque destructivo	MA					MB	A				
Servidor UPI El Perdomo	[N.1] Fuego	A					B	A				
	[N.2] Daños por agua	A					B	A				
	[N.*] Desastres naturales	A					B	A				
	[I.5] Avería de origen físico o lógico	M					MB	B				
	[I.6] Corte del suministro eléctrico	A					A	MA				
	[I.7] Condiciones inadecuadas de temperatura o humedad	A					M	A				
	[E.2] Errores del administrador del sistema / de la seguridad	M	M	A			MB	B	B	M		
	[E.4] Errores de configuración	M	M	M			MB	B	B	B		
	[E.8] Difusión de software dañino	A	A				M	A	A			
	[E.23] Errores de mantenimiento / actualización de equipos (hardware)	B					MB	MB				
	[E.25] Pérdida de equipos	A					MB	M				
	[A.6] Abuso de privilegios de acceso		M	M			M		M	M		
	[A.7] uso no previsto	M	M	M			MB	B	B	B		
	[A.11] Acceso no autorizado		M	MA			MB		B	A		
	[A.23] Manipulación del hardware	M		A			M	M		A		
	[A.24] Denegación de servicio	A					B	A				
	[A.25] Robo de equipos	A					MB	M				
	[A.26] Ataque destructivo	A					MB	M				
Servidor UPI La 27 Sur	[N.1] Fuego	A					B	A				
	[N.2] Daños por agua	A					B	A				
	[N.*] Desastres naturales	A					B	A				
	[I.5] Avería de origen físico o lógico	M					MB	B				

Tabla 28. (Continuación)

ACTIVOS	Amenazas	Impacto Acumulado					P	Riesgo				
		[D]	[I]	[C]	[A]	[T]		[D]	[I]	[C]	[A]	T
Servidor UPI La 27 Sur	[I.6] Corte del suministro eléctrico	A					A	MA				
	[I.7] Condiciones inadecuadas de temperatura o humedad	A					M	A				
	[E.2] Errores del administrador del sistema / de la seguridad	M	M	A			MB	B	B	M		
	[E.4] Errores de configuración	M	M	M			MB	B	B	B		
	[E.8] Difusión de software dañino	A	A				M	A	A			
	[E.23] Errores de mantenimiento / actualización de equipos (hardware)	B					MB	MB				
	[E.25] Pérdida de equipos	A					MB	M				
	[A.6] Abuso de privilegios de acceso		M	M			M		M	M		
	[A.7] uso no previsto	M	M	M			MB	B	B	B		
	[A.11] Acceso no autorizado		M	MA			MB		B	A		
	[A.23] Manipulación del hardware	M		A			M	M		A		
	[A.24] Denegación de servicio	A					B	A				
	[A.25] Robo de equipos	A					MB	M				
	[A.26] Ataque destructivo	A					MB	M				
Servidor UPI La 32	[N.1] Fuego	A					B	A				
	[N.2] Daños por agua	A					B	A				
	[N.*] Desastres naturales	A					B	A				
	[I.5] Avería de origen físico o lógico	M					MB	B				
	[I.6] Corte del suministro eléctrico	A					A	MA				
	[I.7] Condiciones inadecuadas de temperatura o humedad	A					M	A				
	[E.2] Errores del administrador del sistema / de la seguridad	M	M	A			MB	B	B	M		
	[E.4] Errores de configuración	M	M	M			MB	B	B	B		
	[E.8] Difusión de software dañino	A	A				M	A	A			
	[E.23] Errores de mantenimiento / actualización de equipos (hardware)	B					MB	MB				
	[E.25] Pérdida de equipos	A					MB	M				

Tabla 28. (Continuación)

ACTIVOS	Amenazas	Impacto Acumulado					P	Riesgo				
		[D]	[I]	[C]	[A]	[T]		[D]	[I]	[C]	[A]	T
Servidor UPI La 32	[A.6] Abuso de privilegios de acceso		M	M			M		M	M		
	[A.7] uso no previsto	M	M	M			MB	B	B	B		
	[A.11] Acceso no autorizado		M	MA			MB		B	A		
	[A.23] Manipulación del hardware	M		A			M	M		A		
	[A.24] Denegación de servicio	A					B	A				
	[A.25] Robo de equipos	A					MB	M				
	[A.26] Ataque destructivo	A					MB	M				
Servidor UPI La Florida	[N.1] Fuego	A					B	A				
	[N.2] Daños por agua	A					B	A				
	[N.*] Desastres naturales	A					B	A				
	[I.5] Avería de origen físico o lógico	M					MB	B				
	[I.6] Corte del suministro eléctrico	A					A	MA				
	[I.7] Condiciones inadecuadas de temperatura o humedad	A					M	A				
	[E.2] Errores del administrador del sistema / de la seguridad	M	M	A			MB	B	B	M		
	[E.4] Errores de configuración	M	M	M			MB	B	B	B		
	[E.8] Difusión de software dañino	A	A				M	A	A			
	[E.23] Errores de mantenimiento / actualización de equipos (hardware)	B					MB	MB				
	[E.25] Pérdida de equipos	A					MB	M				
	[A.6] Abuso de privilegios de acceso		M	M			M		M	M		
	[A.7] uso no previsto	M	M	M			MB	B	B	B		
	[A.11] Acceso no autorizado		M	MA			MB		B	A		
	[A.23] Manipulación del hardware	M		A			M	M		A		
	[A.24] Denegación de servicio	A					B	A				
	[A.25] Robo de equipos	A					MB	M				
	[A.26] Ataque destructivo	A					MB	M				

Tabla 28. (Continuación)

ACTIVOS	Amenazas	Impacto Acumulado					P	Riesgo				
		[D]	[I]	[C]	[A]	[T]		[D]	[I]	[C]	[A]	T
Servidor UPI La Vega	[N.1] Fuego	A					B	A				
	[N.2] Daños por agua	A					B	A				
	[N.*] Desastres naturales	A					B	A				
	[I.5] Avería de origen físico o lógico	M					MB	B				
	[I.6] Corte del suministro eléctrico	A					A	MA				
	[I.7] Condiciones inadecuadas de temperatura o humedad	A					M	A				
	[E.2] Errores del administrador del sistema / de la seguridad	M	M	A			MB	B	B	M		
	[E.4] Errores de configuración	M	M	M			MB	B	B	B		
	[E.8] Difusión de software dañino	A	A				M	A	A			
	[E.23] Errores de mantenimiento / actualización de equipos (hardware)	B					MB	MB				
	[E.25] Pérdida de equipos	A					MB	M				
	[A.6] Abuso de privilegios de acceso		M	M			M		M	M		
	[A.7] uso no previsto	M	M	M			MB	B	B	B		
	[A.11] Acceso no autorizado		M	MA			MB		B	A		
	[A.23] Manipulación del hardware	M		A			M	M		A		
	[A.24] Denegación de servicio	A					B	A				
	[A.25] Robo de equipos	A					MB	M				
	[A.26] Ataque destructivo	A					MB	M				
Access Point	[N.1] Fuego	M					MB	B				
	[N.2] Daños por agua	M					B	M				
	[N.*] Desastres naturales	M					MB	B				
	[I.5.3] Equipos de comunicaciones	M					M	M				
	[I.7] Condiciones inadecuadas de temperatura o humedad	M					MB	B				
	[I.8] Fallo de servicios de comunicaciones	B		M			M	B		M		
	[E.2] Errores del administrador del sistema / de la seguridad	B		M			B	B		M		

Tabla 28. (Continuación)

ACTIVOS	Amenazas	Impacto Acumulado					P	Riesgo				
		[D]	[I]	[C]	[A]	[T]		[D]	[I]	[C]	[A]	T
Access Point	[E.4] Errores de configuración	B		M			B	B		M		
	[E.19] Fugas de información	B		A			MB	MB		M		
	[E.23] Errores de mantenimiento / actualización de equipos (hardware)	B		M			B	B		M		
	[E.25] Pérdida de equipos	M					M	M				
	[A.5] suplantación de la identidad del usuario	B		A	A		MB	MB		M	M	
	[A.11] Acceso no autorizado	B		A	A		M	B		A	A	
	[A.23] Manipulación del hardware	B		A			B	B		A		
	[A.24.1] Saturación de los canales de comunicaciones	B					M	B				
	[A.25] Robo de equipos	M					B	M				
Servidor UPI La Arcadia	[N.1] Fuego	A					B	A				
	[N.2] Daños por agua	A					B	A				
	[N.*] Desastres naturales	A					B	A				
	[I.5] Avería de origen físico o lógico	M					MB	B				
	[I.6] Corte del suministro eléctrico	A					A	MA				
	[I.7] Condiciones inadecuadas de temperatura o humedad	A					M	A				
	[E.2] Errores del administrador del sistema / de la seguridad	M	M	A			MB	B	B	M		
	[E.4] Errores de configuración	M	M	M			MB	B	B	B		
	[E.8] Difusión de software dañino	A	A				M	A	A			
	[E.23] Errores de mantenimiento / actualización de equipos (hardware)	B					MB	MB				
	[E.25] Pérdida de equipos	A					MB	M				
	[A.6] Abuso de privilegios de acceso		M	M			M		M	M		
	[A.7] uso no previsto	M	M	M			MB	B	B	B		
	[A.11] Acceso no autorizado		M	MA			MB		B	A		
	[A.23] Manipulación del hardware	M		A			M	M		A		

Tabla 28. (Continuación)

ACTIVOS	Amenazas	Impacto Acumulado					P	Riesgo				
		[D]	[I]	[C]	[A]	[T]		[D]	[I]	[C]	[A]	T
Servidor UPI La Arcadia	[A.24] Denegación de servicio	A					B	A				
	[A.25] Robo de equipos	A					MB	M				
	[A.26] Ataque destructivo	A					MB	M				
Equipos de cómputo	[N.1] Fuego	M	MA	MA	A		MB	B	A	A	M	
	[N.2] Daños por agua	M	MA	MA	A		MB	B	A	A	M	
	[N.*] Desastres naturales	M	MA	MA	A		MB	B	A	A	M	
	[I.1] Fuego	M	MA	MA	A		MB	B	A	A	M	
	[I.2] Daños por agua	M	MA	MA	A		MB	B	A	A	M	
	[I.*] Desastres industriales	M	MA	MA	A		MB	B	A	A	M	
	[I.3] Contaminación medioambiental	M	MA	MA	A		MB	B	A	A	M	
	[I.5] Avería de origen físico o lógico	B	A	MA	A		A	M	MA	MA	MA	
	[I.6] Corte del suministro eléctrico	B	MA	A	M		A	M	MA	MA	A	
	[I.7] Condiciones inadecuadas de temperatura o humedad	B	A	A	M		M	B	A	A	M	
	[E.23] Errores de mantenimiento / actualización de equipos (hardware)	M	MA	A	M		MA	A	MA	MA	A	
	[E.25] Pérdida de equipos	M	MA	MA	A		B	M	MA	MA	A	
	[A.6] Abuso de privilegios de acceso	B	MA	MA	M		A	M	MA	MA	A	
	[A.7] uso no previsto	B	MA	MA	M		A	M	MA	MA	A	
	[A.11] Acceso no autorizado	B	MA	MA	M		M	B	MA	MA	M	
	[A.23] Manipulación del hardware	B	MA	A	M		M	B	MA	A	M	
	[A.25] Robo de equipos	M	MA	MA	A		M	M	MA	MA	A	
	[A.26] Ataque destructivo	M	MA	MA	M		MB	B	A	A	B	
Servidor UPI San Francisco	[N.1] Fuego	A					B	A				
	[N.2] Daños por agua	A					B	A				
	[N.*] Desastres naturales	A					B	A				
	[I.5] Avería de origen físico o lógico	M					MB	B				
	[I.6] Corte del suministro eléctrico	A					A	MA				
	[I.7] Condiciones inadecuadas de temperatura o humedad	A					M	A				

Tabla 28. (Continuación)

ACTIVOS	Amenazas	Impacto Acumulado					P	Riesgo				
		[D]	[I]	[C]	[A]	[T]		[D]	[I]	[C]	[A]	T
Servidor UPI San Francisco	[E.2] Errores del administrador del sistema / de la seguridad	M	M	A			MB	B	B	M		
	[E.4] Errores de configuración	M	M	A			MB	B	B	M		
	[E.8] Difusión de software dañino	A	A				M	A	A			
	[E.23] Errores de mantenimiento / actualización de equipos (hardware)	M					MB	B				
	[E.25] Pérdida de equipos	A		MA			MB	M		A		
	[A.6] Abuso de privilegios de acceso		M	A			M		M	A		
	[A.7] uso no previsto	M	M	A			MB	B	B	M		
	[A.11] Acceso no autorizado		M	MA			MB		B	A		
	[A.23] Manipulación del hardware	M		A			M	M		A		
	[A.24] Denegación de servicio	A					B	A				
	[A.24.3] Saturación de los recursos hardware	M					MB	B				
	[A.25] Robo de equipos	A		MA			MB	M		A		
	[A.26] Ataque destructivo	A					MB	M				
Switch de borde 4210G	[N.2] Daños por agua	A					MB	M				
	[N.*] Desastres naturales	A					MB	M				
	[I.1] Fuego	A					MB	M				
	[I.3] Contaminación medioambiental	A					B	A				
	[I.6] Corte del suministro eléctrico	A					M	A				
	[I.7] Condiciones inadecuadas de temperatura o humedad	M					B	M				
	[E.2] Errores del administrador del sistema / de la seguridad	M					MB	B				
	[E.4] Errores de configuración	M					B	M				
	[E.23] Errores de mantenimiento / actualización de equipos (hardware)	M					B	M				
	[A.7] uso no previsto	B					MB	MB				
	[A.11] Acceso no autorizado	M					MB	B				
	[A.23] Manipulación del hardware	M					MB	B				

Tabla 28. (Continuación)

ACTIVOS	Amenazas	Impacto Acumulado					P	Riesgo				
		[D]	[I]	[C]	[A]	[T]		[D]	[I]	[C]	[A]	T
Sistema de almacenamiento formato rack	[I.6.12] Interrupción deliberada por un agente externo	MA	MA				M	MA	MA			
Gabinete de 8 blades	[E.23] Errores de mantenimiento / actualización de equipos (hardware)	MA	MA				MB	A	A			
	[E.24] caída del sistema por agotamiento de recursos	MA	MA				B	MA	MA			
Equipo de Seguridad Perimetral	[N.1] Fuego	MA	A				B	MA	A			
	[N.2] Daños por agua	MA	A				B	MA	A			
	[N.*] Desastres naturales	MA	A				B	MA	A			
	[E.2] Errores del administrador del sistema / de la seguridad	MA	A	M			M	MA	A	M		
	[E.3] Errores de monitorización (log)		A	M			M		A	M		
	[E.4] Errores de configuración	MA	A	M			M	MA	A	M		
	[E.21] Errores de mantenimiento / actualización de programas (software)	MA	A	M			M	MA	A	M		
	[A.3] Manipulación de los registros de actividad (log)		M	M			B		M	M		
	[A.11] Acceso no autorizado	MA	A	M			MB	A	M	B		
	[A.12] Análisis de tráfico		A	M			B		A	M		
	[A.23] Manipulación del hardware	MA	A	M			B	MA	A	M		
	[A.24] Denegación de servicio	MA	A				MB	A	M			
Servidor formato blade marca Hewlett Packard Modelo proliant BL460C G1	[N.1] Fuego	A					B	A				
	[N.2] Daños por agua	A					B	A				
	[N.*] Desastres naturales	A					B	A				
	[I.5] Avería de origen físico o lógico	M					MB	B				
	[I.6] Corte del suministro eléctrico	A					A	MA				
	[I.7] Condiciones inadecuadas de temperatura o humedad	A					M	A				
	[E.2] Errores del administrador del sistema / de la seguridad	M	M	A			MB	B	B	M		
	[E.4] Errores de configuración	M	M	A			MB	B	B	M		

Tabla 28. (Continuación)

ACTIVOS	Amenazas	Impacto Acumulado					P	Riesgo				
		[D]	[I]	[C]	[A]	[T]		[D]	[I]	[C]	[A]	T
Servidor formato blade marca Hewlett Packard Modelo proliant BL460C G1	[E.8] Difusión de software dañino	A	A				M	A	A			
	[E.23] Errores de mantenimiento / actualización de equipos (hardware)	M					MB	B				
	[E.25] Pérdida de equipos	A		MA			MB	M		A		
	[A.6] Abuso de privilegios de acceso		M	A			B		M	A		
	[A.7] uso no previsto	M	M	A			MB	B	B	M		
	[A.11] Acceso no autorizado		M	MA			MB		B	A		
	[A.23] Manipulación del hardware	M		A			M	M		A		
	[A.24] Denegación de servicio	A					B	A				
	[A.24.3] Saturación de los recursos hardware	M					MB	B				
	[A.25] Robo de equipos	A		MA			MB	M		A		
	[A.26] Ataque destructivo	A					MB	M				
Servidor formato blade marca Hewlett Packard. Modelo proliant BL460C G7	[N.1] Fuego	A					B	A				
	[N.2] Daños por agua	A					B	A				
	[N.*] Desastres naturales	A					B	A				
	[I.5] Avería de origen físico o lógico	M					MB	B				
	[I.6] Corte del suministro eléctrico	A					A	MA				
	[I.7] Condiciones inadecuadas de temperatura o humedad	A					M	A				
	[E.2] Errores del administrador del sistema / de la seguridad	M	M	A			MB	B	B	M		
	[E.4] Errores de configuración	M	M	A			MB	B	B	M		
	[E.8] Difusión de software dañino	A	A				M	A	A			
	[E.23] Errores de mantenimiento / actualización de equipos (hardware)	M					MB	B				
	[E.25] Pérdida de equipos	A		MA			MB	M		A		

Tabla 28. (Continuación)

ACTIVOS	Amenazas	Impacto Acumulado					P	Riesgo				
		[D]	[I]	[C]	[A]	[T]		[D]	[I]	[C]	[A]	T
Servidor formato blade marca Hewlett Packard. Modelo proliant BL460C G7	[A.6] Abuso de privilegios de acceso		M	A			B		M	A		
	[A.7] uso no previsto	M	M	A			MB	B	B	M		
	[A.11] Acceso no autorizado		M	MA			MB		B	A		
	[A.23] Manipulación del hardware	M		A			M	M		A		
	[A.24] Denegación de servicio	A					B	A				
	[A.24.3] Saturación de los recursos hardware	M					MB	B				
	[A.25] Robo de equipos	A		MA			MB	M		A		
	[A.26] Ataque destructivo	A					MB	M				
Servidor Proliant 120 G5	[N.1] Fuego	A					B	A				
	[N.2] Daños por agua	A					B	A				
	[N.*] Desastres naturales	A					B	A				
	[I.5] Avería de origen físico o lógico	M					MB	B				
	[I.6] Corte del suministro eléctrico	A					A	MA				
	[I.7] Condiciones inadecuadas de temperatura o humedad	A					M	A				
	[E.2] Errores del administrador del sistema / de la seguridad	M	M	A			MB	B	B	M		
	[E.4] Errores de configuración	M	M	A			MB	B	B	M		
	[E.8] Difusión de software dañino	A	A				M	A	A			
	[E.23] Errores de mantenimiento / actualización de equipos (hardware)	M					MB	B				
	[E.25] Pérdida de equipos	A		MA			MB	M		A		
	[A.6] Abuso de privilegios de acceso		M	A			B		M	A		
	[A.7] uso no previsto	M	M	A			MB	B	B	M		
	[A.11] Acceso no autorizado		M	MA			MB		B	A		
	[A.23] Manipulación del hardware	M		A			M	M		A		
	[A.24] Denegación de servicio	A					B	A				
	[A.24.3] Saturación de los recursos hardware	M					MB	B				
	[A.25] Robo de equipos	A		MA			MB	M		A		

Tabla 28. (Continuación)

ACTIVOS	Amenazas	Impacto Acumulado					P	Riesgo				
		[D]	[I]	[C]	[A]	[T]		[D]	[I]	[C]	[A]	T
	[A.26] Ataque destructivo	A					MB	M				
Servidor Proyecto Misión Bogotá	[N.1] Fuego	A					B	A				
	[N.2] Daños por agua	A					B	A				
	[N.*] Desastres naturales	A					B	A				
	[I.5] Avería de origen físico o lógico	M					MB	B				
	[I.6] Corte del suministro eléctrico	A					A	MA				
	[I.7] Condiciones inadecuadas de temperatura o humedad	A					M	A				
	[E.2] Errores del administrador del sistema / de la seguridad	M	M	A			MB	B	B	M		
	[E.4] Errores de configuración	M	M	A			MB	B	B	M		
	[E.8] Difusión de software dañino	A	A				M	A	A			
	[E.23] Errores de mantenimiento / actualización de equipos (hardware)	M					MB	B				
	[E.25] Pérdida de equipos	A		MA			MB	M		A		
	[A.6] Abuso de privilegios de acceso		M	A			B		M	A		
	[A.7] uso no previsto	M	M	A			MB	B	B	M		
	[A.11] Acceso no autorizado		M	MA			MB		B	A		
	[A.23] Manipulación del hardware	M		A			M	M		A		
	[A.24] Denegación de servicio	A					B	A				
	[A.24.3] Saturación de los recursos hardware	M					MB	B				
	[A.25] Robo de equipos	A		MA			MB	M		A		
	[A.26] Ataque destructivo	A					MB	M				
Impresora para código de barras	[N.1] Fuego	MA					MB	A				
	[N.2] Daños por agua	MA					MB	A				
	[N.*] Desastres naturales	MA					MB	A				
	[I.1] Fuego	MA					MB	A				

Tabla 28. (Continuación)

ACTIVOS	Amenazas	Impacto Acumulado					P	Riesgo				
		[D]	[I]	[C]	[A]	[T]		[D]	[I]	[C]	[A]	T
Impresora para código de barras	[I.3] Contaminación medioambiental	MA					MB	A				
	[I.4] Contaminación electromagnética	A					MB	M				
	[I.5] Avería de origen físico o lógico	A					M	A				
	[I.6] Corte del suministro eléctrico	MA					B	MA				
	[I.7] Condiciones inadecuadas de temperatura o humedad	MA					MB	A				
	[E.2] Errores del administrador del sistema / de la seguridad	A					MB	M				
	[E.23] Errores de mantenimiento / actualización de equipos (hardware)	A					B	A				
	[E.24] caída del sistema por agotamiento de recursos	MA					MB	A				
	[E.25] Pérdida de equipos	MA					MB	A				
	[A.23] Manipulación del hardware	MA					B	MA				
	[A.25] Robo de equipos	MA					MB	A				
	[A.26] Ataque destructivo	MA					MB	A				
Servidor controlador de dominio principal	[N.1] Fuego	MA					B	MA				
	[N.2] Daños por agua	MA					B	MA				
	[N.*] Desastres naturales	MA					B	MA				
	[I.5] Avería de origen físico o lógico	A					MB	M				
	[I.6] Corte del suministro eléctrico	MA					A	MA				
	[I.7] Condiciones inadecuadas de temperatura o humedad	MA					M	MA				
	[E.2] Errores del administrador del sistema / de la seguridad	A	A	A			MB	M	M	M		
	[E.4] Errores de configuración	A	A	A			MB	M	M	M		
	[E.8] Difusión de software dañino	MA	MA				M	MA	MA			
	[E.23] Errores de mantenimiento / actualización de equipos (hardware)	A					MB	M				

Tabla 28. (Continuación)

ACTIVOS	Amenazas	Impacto Acumulado					P	Riesgo				
		[D]	[I]	[C]	[A]	[T]		[D]	[I]	[C]	[A]	T
Servidor controlador de dominio principal	[E.25] Pérdida de equipos	MA		MA			MB	A		A		
	[A.6] Abuso de privilegios de acceso		A	A			B		A	A		
	[A.7] uso no previsto	A	A	A			MB	M	M	M		
	[A.11] Acceso no autorizado		A	MA			MB		M	A		
	[A.23] Manipulación del hardware	A		A			M	A		A		
	[A.24] Denegación de servicio	MA					B	MA				
	[A.24.3] Saturación de los recursos hardware	A					MB	M				
	[A.25] Robo de equipos	MA		MA			MB	A		A		
	[A.26] Ataque destructivo	MA					MB	A				
Switch de borde 4800	[N.2] Daños por agua	A					MB	M				
	[N.*] Desastres naturales	A					MB	M				
	[I.1] Fuego	A					MB	M				
	[I.3] Contaminación medioambiental	A					B	A				
	[I.6] Corte del suministro eléctrico	A					M	A				
	[I.7] Condiciones inadecuadas de temperatura o humedad	M					B	M				
	[E.2] Errores del administrador del sistema / de la seguridad	M					MB	B				
	[E.4] Errores de configuración	M					B	M				
	[E.23] Errores de mantenimiento / actualización de equipos (hardware)	M					B	M				
	[A.7] uso no previsto	B					MB	MB				
	[A.11] Acceso no autorizado	M					MB	B				
	[A.23] Manipulación del hardware	M					MB	B				
	[A.25] Robo de equipos	A					MB	M				
Switch de borde - Referencia 2410 - UPI La Rioja	[N.2] Daños por agua	A					MB	M				
	[N.*] Desastres naturales	A					MB	M				
	[I.1] Fuego	A					MB	M				

Tabla 28. (Continuación)

ACTIVOS	Amenazas	Impacto Acumulado					P	Riesgo				
		[D]	[I]	[C]	[A]	[T]		[D]	[I]	[C]	[A]	T
Switch de borde - Referencia 2410 - UPI La Rioja	[I.3] Contaminación medioambiental	A					B	A				
	[I.6] Corte del suministro eléctrico	A					M	A				
	[I.7] Condiciones inadecuadas de temperatura o humedad	M					B	M				
	[E.2] Errores del administrador del sistema / de la seguridad	M					MB	B				
	[E.4] Errores de configuración	M					B	M				
	[E.23] Errores de mantenimiento / actualización de equipos (hardware)	M					B	M				
	[A.7] uso no previsto	B					MB	MB				
	[A.11] Acceso no autorizado	M					MB	B				
	[A.23] Manipulación del hardware	M					MB	B				
	[A.25] Robo de equipos	A					MB	M				
Switch de borde - Referencia 2920 - Proyecto Misión Bogotá	[N.2] Daños por agua	A					MB	M				
	[N.*] Desastres naturales	A					MB	M				
	[I.1] Fuego	A					MB	M				
	[I.3] Contaminación medioambiental	A					B	A				
	[I.6] Corte del suministro eléctrico	A					M	A				
	[I.7] Condiciones inadecuadas de temperatura o humedad	M					B	M				
	[E.2] Errores del administrador del sistema / de la seguridad	M					MB	B				
	[E.4] Errores de configuración	M					B	M				
	[E.23] Errores de mantenimiento / actualización de equipos (hardware)	M					B	M				
	[A.7] uso no previsto	B					MB	MB				
	[A.11] Acceso no autorizado	M					MB	B				
	[A.23] Manipulación del hardware	M					MB	B				
	[A.25] Robo de equipos	A					MB	M				
	[N.2] Daños por agua	A					MB	M				

Tabla 28. (Continuación)

ACTIVOS	Amenazas	Impacto Acumulado					P	Riesgo				
		[D]	[I]	[C]	[A]	[T]		[D]	[I]	[C]	[A]	T
Switch de borde - Referencia 4250T	[N.*] Desastres naturales	A					MB	M				
	[I.1] Fuego	A					MB	M				
	[I.3] Contaminación medioambiental	A					B	A				
	[I.6] Corte del suministro eléctrico	A					M	A				
	[I.7] Condiciones inadecuadas de temperatura o humedad	M					B	M				
	[E.2] Errores del administrador del sistema / de la seguridad	M					MB	B				
	[E.4] Errores de configuración	M					B	M				
	[E.23] Errores de mantenimiento / actualización de equipos (hardware)	M					B	M				
	[A.7] uso no previsto	B					MB	MB				
	[A.11] Acceso no autorizado	M					MB	B				
	[A.23] Manipulación del hardware	M					MB	B				
	[A.25] Robo de equipos	A					MB	M				
	[N.2] Daños por agua	A					MB	M				
Switch de borde - Referencia 4500G UPI La Florida	[N.*] Desastres naturales	A					MB	M				
	[I.1] Fuego	A					MB	M				
	[I.3] Contaminación medioambiental	A					B	A				
	[I.6] Corte del suministro eléctrico	A					M	A				
	[I.7] Condiciones inadecuadas de temperatura o humedad	M					B	M				
	[E.2] Errores del administrador del sistema / de la seguridad	M					MB	B				
	[E.4] Errores de configuración	M					B	M				
	[E.23] Errores de mantenimiento / actualización de equipos (hardware)	M					B	M				
	[A.7] uso no previsto	B					MB	MB				

Tabla 28. (Continuación)

ACTIVOS	Amenazas	Impacto Acumulado					P	Riesgo				
		[D]	[I]	[C]	[A]	[T]		[D]	[I]	[C]	[A]	T
Switch de borde - Referencia 4500G UPI La Florida	[A.11] Acceso no autorizado	M					MB	B				
	[A.23] Manipulación del hardware	M					MB	B				
	[A.25] Robo de equipos	A					MB	M				
Switch de borde - Referencia 4800G - UPI La 32	[N.2] Daños por agua	A					MB	M				
	[N.*] Desastres naturales	A					MB	M				
	[I.1] Fuego	A					MB	M				
	[I.3] Contaminación medioambiental	A					B	A				
	[I.6] Corte del suministro eléctrico	A					M	A				
	[I.7] Condiciones inadecuadas de temperatura o humedad	M					B	M				
	[E.2] Errores del administrador del sistema / de la seguridad	M					MB	B				
	[E.4] Errores de configuración	M					B	M				
	[E.23] Errores de mantenimiento / actualización de equipos (hardware)	M					B	M				
	[A.7] uso no previsto	B					MB	MB				
	[A.11] Acceso no autorizado	M					MB	B				
	[A.23] Manipulación del hardware	M					MB	B				
	[A.25] Robo de equipos	A					MB	M				
Switch de borde - Referencia 4800G - UPI El Perdomo	[N.2] Daños por agua	A					MB	M				
	[N.*] Desastres naturales	A					MB	M				
	[I.1] Fuego	A					MB	M				
	[I.3] Contaminación medioambiental	A					B	A				
	[I.6] Corte del suministro eléctrico	A					M	A				
	[I.7] Condiciones inadecuadas de temperatura o humedad	M					B	M				
	[E.2] Errores del administrador del sistema / de la seguridad	M					MB	B				
	[E.4] Errores de configuración	M					B	M				

Tabla 28. (Continuación)

ACTIVOS	Amenazas	Impacto Acumulado					P	Riesgo				
		[D]	[I]	[C]	[A]	[T]		[D]	[I]	[C]	[A]	T
Switch de borde - Referencia 4800G - UPI El Perdomo	[E.23] Errores de mantenimiento / actualización de equipos (hardware)	M					B	M				
	[A.7] uso no previsto	B					MB	MB				
	[A.11] Acceso no autorizado	M					MB	B				
	[A.25] Robo de equipos	A					MB	M				
Switch de borde - Referencia 4800G - UPI La Florida	[N.2] Daños por agua	A					MB	M				
	[N.*] Desastres naturales	A					MB	M				
	[I.1] Fuego	A					MB	M				
	[I.3] Contaminación medioambiental	A					B	A				
	[I.6] Corte del suministro eléctrico	A					M	A				
	[I.7] Condiciones inadecuadas de temperatura o humedad	M					B	M				
	[E.2] Errores del administrador del sistema / de la seguridad	M					MB	B				
	[E.4] Errores de configuración	M					B	M				
	[E.23] Errores de mantenimiento / actualización de equipos (hardware)	M					B	M				
	[A.7] uso no previsto	B					MB	MB				
	[A.11] Acceso no autorizado	M					MB	B				
	[A.23] Manipulación del hardware	M					MB	B				
	[A.25] Robo de equipos	A					MB	M				
Switch de borde - Referencia 4800G - UPI La 27 sur	[N.2] Daños por agua	A					MB	M				
	[N.*] Desastres naturales	A					MB	M				
	[I.1] Fuego	A					MB	M				
	[I.3] Contaminación medioambiental	A					B	A				
	[I.6] Corte del suministro eléctrico	A					M	A				
	[I.7] Condiciones inadecuadas de temperatura o humedad	M					B	M				
	[E.2] Errores del administrador del sistema / de la seguridad	M					MB	B				

Tabla 28. (Continuación)

ACTIVOS	Amenazas	Impacto Acumulado					P	Riesgo				
		[D]	[I]	[C]	[A]	[T]		[D]	[I]	[C]	[A]	T
Switch de borde - Referencia 4800G - UPI La 27 sur	[E.4] Errores de configuración	M					B	M				
	[E.23] Errores de mantenimiento / actualización de equipos (hardware)	M					B	M				
	[A.7] uso no previsto	B					MB	MB				
	[A.11] Acceso no autorizado	M					MB	B				
	[A.25] Robo de equipos	A					MB	M				
Switch de borde - Referencia 4800G - UPI San Francisco	[N.2] Daños por agua	A					MB	M				
	[N.*] Desastres naturales	A					MB	M				
	[I.1] Fuego	A					MB	M				
	[I.3] Contaminación medioambiental	A					B	A				
	[I.6] Corte del suministro eléctrico	A					M	A				
	[I.7] Condiciones inadecuadas de temperatura o humedad	M					B	M				
	[E.2] Errores del administrador del sistema / de la seguridad	M					MB	B				
	[E.4] Errores de configuración	M					B	M				
	[E.23] Errores de mantenimiento / actualización de equipos (hardware)	M					B	M				
	[A.7] uso no previsto	B					MB	MB				
	[A.11] Acceso no autorizado	M					MB	B				
	[A.23] Manipulación del hardware	M					MB	B				
	[A.25] Robo de equipos	A					MB	M				
Switch de borde - Referencia 4800G - UPI La Rioja	[N.2] Daños por agua	A					MB	M				
	[N.*] Desastres naturales	A					MB	M				
	[I.1] Fuego	A					MB	M				
	[I.3] Contaminación medioambiental	A					B	A				
	[I.6] Corte del suministro eléctrico	A					M	A				
	[I.7] Condiciones inadecuadas de temperatura o humedad	M					B	M				
	[E.2] Errores del administrador del sistema / de la seguridad	M					MB	B				
	[E.4] Errores de configuración	M					B	M				

Tabla 28. (Continuación)

ACTIVOS	Amenazas	Impacto Acumulado					P	Riesgo				
		[D]	[I]	[C]	[A]	[T]		[D]	[I]	[C]	[A]	T
Switch de borde - Referencia 4800G - UPI La Rioja	[E.23] Errores de mantenimiento / actualización de equipos (hardware)	M					B	M				
	[A.7] uso no previsto	B					MB	MB				
	[A.11] Acceso no autorizado	M					MB	B				
	[A.25] Robo de equipos	A					MB	M				
Switch de borde - Referencia 4800G - UPI La Vega	[N.2] Daños por agua	A					MB	M				
	[N.*] Desastres naturales	A					MB	M				
	[I.1] Fuego	A					MB	M				
	[I.3] Contaminación medioambiental	A					B	A				
	[I.6] Corte del suministro eléctrico	A					M	A				
	[I.7] Condiciones inadecuadas de temperatura o humedad	M					B	M				
	[E.2] Errores del administrador del sistema / de la seguridad	M					MB	B				
	[E.4] Errores de configuración	M					B	M				
	[E.23] Errores de mantenimiento / actualización de equipos (hardware)	M					B	M				
	[A.7] uso no previsto	B					MB	MB				
	[A.11] Acceso no autorizado	M					MB	B				
	[A.23] Manipulación del hardware	M					MB	B				
	[A.25] Robo de equipos	A					MB	M				
Switch de borde - Referencia 4800G - UPI Santa Lucia	[N.2] Daños por agua	A					MB	M				
	[N.*] Desastres naturales	A					MB	M				
	[I.1] Fuego	A					MB	M				
	[I.3] Contaminación medioambiental	A					B	A				
	[I.6] Corte del suministro eléctrico	A					M	A				
	[I.7] Condiciones inadecuadas de temperatura o humedad	M					B	M				
	[E.2] Errores del administrador del sistema / de la seguridad	M					MB	B				

Tabla 28. (Continuación)

ACTIVOS	Amenazas	Impacto Acumulado					P	Riesgo				
		[D]	[I]	[C]	[A]	[T]		[D]	[I]	[C]	[A]	T
Switch de borde - Referencia 4800G - UPI Santa Lucia	[E.4] Errores de configuración	M					B	M				
	[E.23] Errores de mantenimiento / actualización de equipos (hardware)	M					B	M				
	[A.7] uso no previsto	B					MB	MB				
	[A.11] Acceso no autorizado	M					MB	B				
	[A.25] Robo de equipos	A					MB	M				
Switch de borde - Referencia 4800G - UPI Servitá	[N.2] Daños por agua	A					MB	M				
	[N.*] Desastres naturales	A					MB	M				
	[I.1] Fuego	A					MB	M				
	[I.3] Contaminación medioambiental	A					B	A				
	[I.6] Corte del suministro eléctrico	A					M	A				
	[I.7] Condiciones inadecuadas de temperatura o humedad	M					B	M				
	[E.2] Errores del administrador del sistema / de la seguridad	M					MB	B				
	[E.4] Errores de configuración	M					B	M				
	[E.23] Errores de mantenimiento / actualización de equipos (hardware)	M					B	M				
	[A.7] uso no previsto	B					MB	MB				
	[A.11] Acceso no autorizado	M					MB	B				
	[A.23] Manipulación del hardware	M					MB	B				
	[A.25] Robo de equipos	A					MB	M				
Switch de borde - Referencia E2910 HP - UPI Bosa	[N.2] Daños por agua	A					MB	M				
	[N.*] Desastres naturales	A					MB	M				
	[I.1] Fuego	A					MB	M				
	[I.3] Contaminación medioambiental	A					B	A				
	[I.6] Corte del suministro eléctrico	A					M	A				
	[I.7] Condiciones inadecuadas de temperatura o humedad	M					B	M				
	[E.2] Errores del administrador del sistema / de la seguridad	M					MB	B				
	[E.4] Errores de configuración	M					B	M				

Tabla 28. (Continuación)

ACTIVOS	Amenazas	Impacto Acumulado					P	Riesgo				
		[D]	[I]	[C]	[A]	[T]		[D]	[I]	[C]	[A]	T
Switch de borde - Referencia E2910 HP - UPI Bosa	[E.23] Errores de mantenimiento / actualización de equipos (hardware)	M					B	M				
	[A.7] uso no previsto	B					MB	MB				
	[A.11] Acceso no autorizado	M					MB	B				
	[A.25] Robo de equipos	A					MB	M				
Switch de borde - Referencia E2910 HP - Proyecto 968	[N.2] Daños por agua	A					MB	M				
	[N.*] Desastres naturales	A					MB	M				
	[I.1] Fuego	A					MB	M				
	[I.3] Contaminación medioambiental	A					B	A				
	[I.6] Corte del suministro eléctrico	A					M	A				
	[I.7] Condiciones inadecuadas de temperatura o humedad	M					B	M				
	[E.2] Errores del administrador del sistema / de la seguridad	M					MB	B				
	[E.4] Errores de configuración	M					B	M				
	[E.23] Errores de mantenimiento / actualización de equipos (hardware)	M					B	M				
	[A.7] uso no previsto	B					MB	MB				
	[A.11] Acceso no autorizado	M					MB	B				
	[A.23] Manipulación del hardware	M					MB	B				
	[A.25] Robo de equipos	A					MB	M				
Switch de borde - Referencia V1910 - Proyecto Misión Bogotá	[N.2] Daños por agua	A					MB	M				
	[N.*] Desastres naturales	A					MB	M				
	[I.1] Fuego	A					MB	M				
	[I.3] Contaminación medioambiental	A					B	A				
	[I.6] Corte del suministro eléctrico	A					M	A				
	[I.7] Condiciones inadecuadas de temperatura o humedad	M					B	M				
	[E.2] Errores del administrador del sistema / de la seguridad	M					MB	B				
	[E.4] Errores de configuración	M					B	M				

Tabla 28. (Continuación)

ACTIVOS	Amenazas	Impacto Acumulado					P	Riesgo				
		[D]	[I]	[C]	[A]	[T]		[D]	[I]	[C]	[A]	T
Switch de borde - Referencia V1910 - Proyecto Misión Bogotá	[E.23] Errores de mantenimiento / actualización de equipos (hardware)	M					B	M				
	[A.7] uso no previsto	B					MB	MB				
	[A.11] Acceso no autorizado	M					MB	B				
	[A.25] Robo de equipos	A					MB	M				
Switch de borde 4500G - Sede Administrativa	[N.2] Daños por agua	A					MB	M				
	[N.*] Desastres naturales	A					MB	M				
	[I.1] Fuego	A					MB	M				
	[I.3] Contaminación medioambiental	A					B	A				
	[I.6] Corte del suministro eléctrico	A					M	A				
	[I.7] Condiciones inadecuadas de temperatura o humedad	M					B	M				
	[E.2] Errores del administrador del sistema / de la seguridad	M					MB	B				
	[E.4] Errores de configuración	M					B	M				
	[E.23] Errores de mantenimiento / actualización de equipos (hardware)	M					B	M				
	[A.7] uso no previsto	B					MB	MB				
	[A.11] Acceso no autorizado	M					MB	B				
	[A.23] Manipulación del hardware	M					MB	B				
	[A.25] Robo de equipos	A					MB	M				
Switch de borde. Referencia 4500G - UPI La Arcadia	[N.2] Daños por agua	A					MB	M				
	[N.*] Desastres naturales	A					MB	M				
	[I.1] Fuego	A					MB	M				
	[I.3] Contaminación medioambiental	A					B	A				
	[I.6] Corte del suministro eléctrico	A					M	A				
	[I.7] Condiciones inadecuadas de temperatura o humedad	M					B	M				
	[E.2] Errores del administrador del sistema / de la seguridad	M					MB	B				

Tabla 28. (Continuación)

ACTIVOS	Amenazas	Impacto Acumulado					P	Riesgo				
		[D]	[I]	[C]	[A]	[T]		[D]	[I]	[C]	[A]	T
Switch de borde. Referencia 4500G - UPI La Arcadia	[E.4] Errores de configuración	M					B	M				
	[E.23] Errores de mantenimiento / actualización de equipos (hardware)	M					B	M				
	[A.7] uso no previsto	B					MB	MB				
	[A.11] Acceso no autorizado	M					MB	B				
	[A.23] Manipulación del hardware	M					MB	B				
	[A.25] Robo de equipos	A					MB	M				
Switch de borde. Referencia 4800G - UPI La Arcadia	[N.2] Daños por agua	A					MB	M				
	[N.*] Desastres naturales	A					MB	M				
	[I.1] Fuego	A					MB	M				
	[I.3] Contaminación medioambiental	A					B	A				
	[I.6] Corte del suministro eléctrico	A					M	A				
	[I.7] Condiciones inadecuadas de temperatura o humedad	M					B	M				
	[E.2] Errores del administrador del sistema / de la seguridad	M					MB	B				
	[E.4] Errores de configuración	M					B	M				
	[E.23] Errores de mantenimiento / actualización de equipos (hardware)	M					B	M				
	[A.7] uso no previsto	B					MB	MB				
	[A.11] Acceso no autorizado	M					MB	B				
	[A.23] Manipulación del hardware	M					MB	B				
	[A.25] Robo de equipos	A					MB	M				
Switch de core. Referencia 5500G - Sede Administrativa	[N.2] Daños por agua	A					MB	M				
	[N.*] Desastres naturales	A					MB	M				
	[I.1] Fuego	A					MB	M				

Tabla 28. (Continuación)

ACTIVOS	Amenazas	Impacto Acumulado					P	Riesgo				
		[D]	[I]	[C]	[A]	[T]		[D]	[I]	[C]	[A]	T
Switch de core. Referencia 5500G - Sede Administrativa	[I.3] Contaminación medioambiental	A					B	A				
	[I.6] Corte del suministro eléctrico	A					M	A				
	[I.7] Condiciones inadecuadas de temperatura o humedad	M					B	M				
	[E.2] Errores del administrador del sistema / de la seguridad	M					MB	B				
	[E.4] Errores de configuración	M					B	M				
	[E.23] Errores de mantenimiento / actualización de equipos (hardware)	M					B	M				
	[A.7] uso no previsto	B					MB	MB				
	[A.11] Acceso no autorizado	M					MB	B				
	[A.23] Manipulación del hardware	M					MB	B				
	[A.25] Robo de equipos	A					MB	M				
Copia de Respaldo - Dataprotector	[N.2] Daños por agua	A					MB	M				
	[N.*] Desastres naturales	A					MB	M				
	[I.6] Corte del suministro eléctrico	A					B	A				
	[I.7] Condiciones inadecuadas de temperatura o humedad	M					B	M				
	[I.8] Fallo de servicios de comunicaciones	M					B	M				
	[I.9] Interrupción de otros servicios o suministros esenciales	A					B	A				
	[E.2] Errores del administrador del sistema / de la seguridad	M					MB	B				
	[E.4] Errores de configuración	A					B	A				

Tabla 28. (Continuación)

ACTIVOS	Amenazas	Impacto Acumulado					P	Riesgo				
		[D]	[I]	[C]	[A]	[T]		[D]	[I]	[C]	[A]	T
Copia de Respaldo - Dataprotector	[E.18] Destrucción de la información			A			B			A		
	[E.21] Errores de mantenimiento / actualización de programas (software)						A					
	[E.24] caída del sistema por agotamiento de recursos	M					B	M				
	[A.23] Manipulación del hardware	A					MB	M				
Sistema de Backups - Dataprotector	[N.2] Daños por agua	A					MB	M				
	[N.*] Desastres naturales	A					MB	M				
	[I.6] Corte del suministro eléctrico	A					B	A				
	[I.7] Condiciones inadecuadas de temperatura o humedad	M					B	M				
	[I.8] Fallo de servicios de comunicaciones	M					B	M				
	[I.9] Interrupción de otros servicios o suministros esenciales	A					B	A				
	[E.2] Errores del administrador del sistema / de la seguridad	M					MB	B				
	[E.4] Errores de configuración	A					B	A				
	[E.18] Destrucción de la información			A			B			A		
	[E.21] Errores de mantenimiento / actualización de programas (software)						A					
	[E.24] caída del sistema por agotamiento de recursos	M					B	M				
	[A.23] Manipulación del hardware	A					MB	M				
Servidor de correo - Proliant DL 380 G5	[N.1] Fuego	MA					MB	A				
	[N.2] Daños por agua	MA					MB	A				

Tabla 28. (Continuación)

ACTIVOS	Amenazas	Impacto Acumulado					P	Riesgo				
		[D]	[I]	[C]	[A]	[T]		[D]	[I]	[C]	[A]	T
Servidor de correo - Proliant DL 380 G5	[N.*] Desastres naturales	MA					MB	A				
	[I.5] Avería de origen físico o lógico	A					MB	M				
	[I.6] Corte del suministro eléctrico	MA					M	MA				
	[I.7] Condiciones inadecuadas de temperatura o humedad	A					B	A				
	[E.2] Errores del administrador del sistema / de la seguridad	A	A	A			MB	M	M	M		
	[E.4] Errores de configuración	A	A	A			MB	M	M	M		
	[E.8] Difusión de software dañino	MA					B	MA				
	[E.23] Errores de mantenimiento / actualización de equipos (hardware)	A					MB	M				
	[E.25] Pérdida de equipos	MA					MB	A				
	[A.6] Abuso de privilegios de acceso		A	A			MB		M	M		
	[A.7] uso no previsto	A	A	A			MB	M	M	M		
	[A.11] Acceso no autorizado		A	MA			MB		M	A		
	[A.23] Manipulación del hardware	A		A			B	A		A		
	[A.24] Denegación de servicio	MA					B	MA				
	[A.25] Robo de equipos	MA					MB	A				
	[A.26] Ataque destructivo	MA					MB	A				
Servidor Ambiente de pruebas y desarrollo	[N.1] Fuego	M	M				B	M	M			
	[N.2] Daños por agua	M	M				B	M	M			
	[N.*] Desastres naturales	M	M				B	M	M			
	[E.1] Errores de los usuarios	B					MB	MB				
	[E.2] Errores del administrador del sistema / de la seguridad	B	B				B	B	B			
	[E.4] Errores de configuración	B	B				MB	MB	MB			
	[E.19] Fugas de información		B				M		B			
	[N.1] Fuego	MA	MA	MA			MB	A	A	A		
	[N.2] Daños por agua	MA	MA	MA			MB	A	A	A		

Tabla 28. (Continuación)

ACTIVOS	Amenazas	Impacto Acumulado					P	Riesgo				
		[D]	[I]	[C]	[A]	[T]		[D]	[I]	[C]	[A]	T
Servidor de base de datos Nómina	[N.*] Desastres naturales	MA	MA	MA			MB	A	A	A		
	[E.1] Errores de los usuarios	A	MA				M	A	MA			
	[E.2] Errores del administrador del sistema / de la seguridad	MA	A	MA			M	MA	A	MA		
	[E.14] Fugas de información			MA			M			MA		
	[E.15] Alteración de la información		MA	MA			M		MA	MA		
	[E.18] Destrucción de la información	MA	MA	MA			B	MA	MA	MA		
	[A.6] Abuso de privilegios de acceso	A	MA	MA			M	A	MA	MA		
	[A.15] Modificación de la información		MA	MA			B		MA	MA		
Servidor de Virtualización	[N.1] Fuego	MA	MA				M	MA	MA			
	[N.2] Daños por agua	MA	MA				M	MA	MA			
	[I.1] Fuego	MA	MA				M	MA	MA			
	[I.2] Daños por agua	MA	MA				M	MA	MA			
	[E.2] Errores del administrador del sistema / de la seguridad	A	A				MB	M	M			
	[E.4] Errores de configuración	A	A				MB	M	M			
	[E.24] caída del sistema por agotamiento de recursos	A	A				B	A	A			
	[A.8] Difusión de software dañino	A	A				M	A	A			
	[A.23] Manipulación del hardware	MA	MA				MB	A	A			
	[A.24] Denegación de servicio	A	A				MB	M	M			
	[A.26] Ataque destructivo	MA	MA				MB	A	A			
Servidor base de datos SQL	[N.*] Desastres naturales	A	A				MB	M	M			
	[E.2] Errores del administrador del sistema / de la seguridad	M	M				MB	B	B			
	[E.4] Errores de configuración	M	M				MB	B	B			
	[E.15] Alteración de la información	M	M				MB	B	B			

Tabla 28. (Continuación)

ACTIVOS	Amenazas	Impacto Acumulado					P	Riesgo				
		[D]	[I]	[C]	[A]	[T]		[D]	[I]	[C]	[A]	T
Servidor base de datos SQL	[E.21] Errores de mantenimiento / actualización de MBprogramas (software)	B					M	B				
	[A.6] Abuso de privilegios de acceso			M			MB			B		
	[A.8] Difusión de software dañino	A	A				B	A	A			
	[A.11] Acceso no autorizado			A			B			A		
	[A.15] Modificación de la información		A	A			B		A	A		
Servidor de Archivos	[N.2] Daños por agua	MA	MA				MB	A	A			
	[N.*] Desastres naturales	MA	MA				MB	A	A			
	[I.3] Contaminación medioambiental	MA					B	MA				
	[I.6] Corte del suministro eléctrico	MA					B	MA				
	[I.7] Condiciones inadecuadas de temperatura o humedad	A					MB	M				
	[E.1] Errores de los usuarios		MA				M		MA			
	[E.2] Errores del administrador del sistema / de la seguridad	M					MB	B				
	[E.4] Errores de configuración	M					MB	B				
	[E.15] Alteración de la información		MA				M		MA			
	[E.18] Destrucción de la información		MA				A		MA			
	[E.24] caída del sistema por agotamiento de recursos	A					M	A				
	[A.6] Abuso de privilegios de acceso		MA	MA	MA		MB		A	A	A	
	[A.8] Difusión de software dañino	A	A				MB	M	M			
	[A.11] Acceso no autorizado		MA	MA			MB		A	A		
	[A.15] Modificación de la información		MA	MA			B		MA	MA		
	[A.18] Destrucción de la información		MA	MA			B		MA	MA		
Servidor de impresión	[N.1] Fuego	MA				A	MB	A				M
	[N.2] Daños por agua	MA				A	MB	A				M
	[N.*] Desastres naturales	MA				A	B	MA				A

Tabla 28. (Continuación)

ACTIVOS	Amenazas	Impacto Acumulado					P	Riesgo				
		[D]	[I]	[C]	[A]	[T]		[D]	[I]	[C]	[A]	T
Servidor de impresión	[I.5] Avería de origen físico o lógico	MA				A	MB	A				M
	[I.6] Corte del suministro eléctrico	MA				A	MB	A				M
	[I.7] Condiciones inadecuadas de temperatura o humedad	MA				A	MB	A				M
	[I.8.11] Interrupción accidental	MA				A	MB	A				M
	[E.2] Errores del administrador del sistema / de la seguridad	A				M	MB	M				B
	[E.4] Errores de configuración	A				M	MB	M				B
	[E.21] Errores de mantenimiento / actualización de programas (software)	A				M	MB	M				B
	[E.24] caída del sistema por agotamiento de recursos	MA				A	B	MA				A
	[A.5] suplantación de la identidad del usuario	MA				A	MB	A				M
	[A.6] Abuso de privilegios de acceso	MA				A	MB	A				M
	[A.8] Difusión de software dañino	MA				A	B	MA				A
	[A.11] Acceso no autorizado	MA				A	MB	A				M
	[A.24] Denegación de servicio	MA				A	B	MA				A
Servidor OAS – SICAPITAL	[N.1] Fuego	A					MB	M				
	[N.2] Daños por agua	A					MB	M				
	[N.*] Desastres naturales	A					MB	M				
	[I.5] Avería de origen físico o lógico	M	M				B	M	M			
	[I.6] Corte del suministro eléctrico	A	M				M	A	M			
	[I.7] Condiciones inadecuadas de temperatura o humedad	A	M				M	A	M			
	[I.8.11] Interrupción accidental	M					MB	B				
	[E.2] Errores del administrador del sistema / de la seguridad	M					B	M				

Tabla 28. (Continuación)

ACTIVOS	Amenazas	Impacto Acumulado					P	Riesgo				
		[D]	[I]	[C]	[A]	[T]		[D]	[I]	[C]	[A]	T
	[E.4] Errores de configuración	A					B	A				
Servidor OAS – SICAPITAL	[E.21] Errores de mantenimiento / actualización de programas (software)	M					B	M				
	[E.23] Errores de mantenimiento / actualización de equipos (hardware)	M					B	M				
	[E.24] caída del sistema por agotamiento de recursos	A					MB	M				
	[A.4] Manipulación de los ficheros de configuración	A					MB	M				
	[A.5] suplantación de la identidad del usuario		M	M	M		M		M	M	M	
	[A.6] Abuso de privilegios de acceso		M	M	M		B		M	M	M	
	[A.18] Destrucción de la información		A	M	M		MB		M	B	B	
	[A.24] Denegación de servicio	A					M	A				

Fuente: Autor

8.5.2.4 Riesgo Potencial: [AUX] ELEMENTOS AUXILIARES

Tabla 32. Riesgo potencial activos de tipo: Elementos Auxiliares

ACTIVOS	Amenazas	Impacto					P	Riesgo				
		[D]	[I]	[C]	[A]	[T]		[D]	[I]	[C]	[A]	[T]
UPS de 15 KVA - UPI La Arcadia	[N.2] Daños por agua	B					MB	MB				
	[N.*] Desastres naturales	M					MB	B				
	[I.1] Fuego	M					MB	B				
	[I.5] Avería de origen físico o lógico	B					MB	MB				
	[I.6] Corte del suministro eléctrico	B					B	B				
	[I.7] Condiciones inadecuadas de temperatura o humedad	MB					B	MB				
	[I.9] Interrupción de otros servicios o suministros esenciales	B					B	B				

Tabla 29. (Continuación)

ACTIVOS	Amenazas	Impacto					P	Riesgo				
		[D]	[I]	[C]	[A]	[T]		[D]	[I]	[C]	[A]	[T]
UPS de 15 KVA - UPI La Arcadia	[E.23] Errores de mantenimiento / actualización de equipos (hardware)	B					MB	MB				
	[A.7] uso no previsto	B					MB	MB				
	[A.23] Manipulación del hardware	B					MB	MB				
UPS de 15 KVA - UPI La Rioja	[N.2] Daños por agua	B					MB	MB				
	[N.*] Desastres naturales	M					MB	B				
	[I.1] Fuego	M					MB	B				
	[I.5] Avería de origen físico o lógico	B					MB	MB				
	[I.6] Corte del suministro eléctrico	B					B	B				
	[I.7] Condiciones inadecuadas de temperatura o humedad	MB					B	MB				
	[I.9] Interrupción de otros servicios o suministros esenciales	B					B	B				
	[E.23] Errores de mantenimiento / actualización de equipos (hardware)	B					MB	MB				
	[A.7] uso no previsto	B					MB	MB				
	[A.23] Manipulación del hardware	B					MB	MB				
Planta eléctrica	[N.*] Desastres naturales	M					MB	B				
	[I.1] Fuego	M					MB	B				
	[I.3] Contaminación medioambiental	B					B	B				
	[I.5] Avería de origen físico o lógico	B					B	B				
	[I.6] Corte del suministro eléctrico	B					MB	MB				
	[I.7] Condiciones inadecuadas de temperatura o humedad	B					MB	MB				
	[I.9] Interrupción de otros servicios o suministros esenciales	B					B	B				
	[E.23] Errores de mantenimiento / actualización de equipos (hardware)	B					MB	MB				
	[A.26] Ataque destructivo	M					MB	B				

Tabla 29. (Continuación)

ACTIVOS	Amenazas	Impacto					P	Riesgo				
		[D]	[I]	[C]	[A]	[T]		[D]	[I]	[C]	[A]	[T]
UPS de 10 KVA - Sede Misión Bogotá	[N.2] Daños por agua	B					MB	MB				
	[N.*] Desastres naturales	M					MB	B				
	[I.1] Fuego	M					MB	B				
	[I.5] Avería de origen físico o lógico	B					MB	MB				
	[I.6] Corte del suministro eléctrico	B					B	B				
	[I.7] Condiciones inadecuadas de temperatura o humedad	MB					B	MB				
	[I.9] Interrupción de otros servicios o suministros esenciales	B					B	B				
	[E.23] Errores de mantenimiento / actualización de equipos (hardware)	B					MB	MB				
	[A.7] uso no previsto	B					MB	MB				
	[A.23] Manipulación del hardware	B					MB	MB				
UPS de 10 KVA - UPI La vega	[N.2] Daños por agua	B					MB	MB				
	[N.*] Desastres naturales	M					MB	B				
	[I.1] Fuego	M					MB	B				
	[I.5] Avería de origen físico o lógico	B					MB	MB				
	[I.6] Corte del suministro eléctrico	B					B	B				
	[I.7] Condiciones inadecuadas de temperatura o humedad	MB					B	MB				
	[I.9] Interrupción de otros servicios o suministros esenciales	B					B	B				
	[E.23] Errores de mantenimiento / actualización de equipos (hardware)	B					MB	MB				
	[A.7] uso no previsto	B					MB	MB				
	[A.23] Manipulación del hardware	B					MB	MB				
UPS de 15 KVA - UPI Santa Lucia	[N.2] Daños por agua	B					MB	MB				

Tabla 29. (Continuación)

ACTIVOS	Amenazas	Impacto					P	Riesgo				
		[D]	[I]	[C]	[A]	[T]		[D]	[I]	[C]	[A]	[T]
UPS de 15 KVA - UPI Santa Lucia	[N.*] Desastres naturales	M					MB	B				
	[I.1] Fuego	M					MB	B				
	[I.5] Avería de origen físico o lógico	B					MB	MB				
	[I.6] Corte del suministro eléctrico	B					B	B				
	[I.7] Condiciones inadecuadas de temperatura o humedad	MB					B	MB				
	[I.9] Interrupción de otros servicios o suministros esenciales	B					B	B				
	[E.23] Errores de mantenimiento / actualización de equipos (hardware)	B					MB	MB				
	[A.7] uso no previsto	B					MB	MB				
	[A.23] Manipulación del hardware	B					MB	MB				
UPS de 10 KVA - UPI San Francisco	[N.2] Daños por agua	B					MB	MB				
	[N.*] Desastres naturales	M					MB	B				
	[I.1] Fuego	M					MB	B				
	[I.5] Avería de origen físico o lógico	B					MB	MB				
	[I.6] Corte del suministro eléctrico	B					B	B				
	[I.7] Condiciones inadecuadas de temperatura o humedad	MB					B	MB				
	[I.9] Interrupción de otros servicios o suministros esenciales	B					B	B				
	[E.23] Errores de mantenimiento / actualización de equipos (hardware)	B					MB	MB				
	[A.7] uso no previsto	B					MB	MB				
	[A.23] Manipulación del hardware	B					MB	MB				
UPS de 15 KVA - UPI El Perdomo	[N.2] Daños por agua	B					MB	MB				
	[N.*] Desastres naturales	M					MB	B				
	[I.1] Fuego	M					MB	B				

Tabla 29. (Continuación)

ACTIVOS	Amenazas	Impacto					P	Riesgo				
		[D]	[I]	[C]	[A]	[T]		[D]	[I]	[C]	[A]	[T]
UPS de 15 KVA - UPI El Perdomo	[I.5] Avería de origen físico o lógico	B					MB	MB				
	[I.6] Corte del suministro eléctrico	B					B	B				
	[I.7] Condiciones inadecuadas de temperatura o humedad	MB					B	MB				
	[I.9] Interrupción de otros servicios o suministros esenciales	B					B	B				
	[E.23] Errores de mantenimiento / actualización de equipos (hardware)	B					MB	MB				
	[A.7] uso no previsto	B					MB	MB				
	[A.23] Manipulación del hardware	B					MB	MB				
UPS de 15 KVA - UPI La 27 sur	[N.2] Daños por agua	B					MB	MB				
	[N.*] Desastres naturales	M					MB	B				
	[I.1] Fuego	M					MB	B				
	[I.5] Avería de origen físico o lógico	B					MB	MB				
	[I.6] Corte del suministro eléctrico	B					B	B				
	[I.7] Condiciones inadecuadas de temperatura o humedad	MB					B	MB				
	[I.9] Interrupción de otros servicios o suministros esenciales	B					B	B				
	[E.23] Errores de mantenimiento / actualización de equipos (hardware)	B					MB	MB				
	[A.7] uso no previsto	B					MB	MB				
	[A.23] Manipulación del hardware	B					MB	MB				
UPS de 15 KVA - UPI Servitá	[N.2] Daños por agua	B					MB	MB				
	[N.*] Desastres naturales	M					MB	B				
	[I.1] Fuego	M					MB	B				
	[I.5] Avería de origen físico o lógico	B					MB	MB				
	[I.6] Corte del suministro eléctrico	B					B	B				

Tabla 29. (Continuación)

ACTIVOS	Amenazas	Impacto					P	Riesgo				
		[D]	[I]	[C]	[A]	[T]		[D]	[I]	[C]	[A]	[T]
UPS de 15 KVA - UPI Servitá	[I.7] Condiciones inadecuadas de temperatura o humedad	MB					B	MB				
	[I.9] Interrupción de otros servicios o suministros esenciales	B					B	B				
	[E.23] Errores de mantenimiento / actualización de equipos (hardware)	B					MB	MB				
	[A.7] uso no previsto	B					MB	MB				
	[A.23] Manipulación del hardware	B					MB	MB				
UPS de 15 KVA - UPI La Florida	[N.2] Daños por agua	B					MB	MB				
	[N.*] Desastres naturales	M					MB	B				
	[I.1] Fuego	M					MB	B				
	[I.5] Avería de origen físico o lógico	B					MB	MB				
	[I.6] Corte del suministro eléctrico	B					B	B				
	[I.7] Condiciones inadecuadas de temperatura o humedad	MB					B	MB				
	[I.9] Interrupción de otros servicios o suministros esenciales	B					B	B				
	[E.23] Errores de mantenimiento / actualización de equipos (hardware)	B					MB	MB				
	[A.7] uso no previsto	B					MB	MB				
	[A.23] Manipulación del hardware	B					MB	MB				
UPS de 20 KVA - Sede proyecto 968	[N.2] Daños por agua	B					MB	MB				
	[N.*] Desastres naturales	M					MB	B				
	[I.1] Fuego	M					MB	B				
	[I.5] Avería de origen físico o lógico	B					MB	MB				
	[I.6] Corte del suministro eléctrico	B					B	B				
	[I.7] Condiciones inadecuadas de temperatura o humedad	MB					B	MB				
	[I.9] Interrupción de otros servicios o suministros esenciales	B					B	B				

Tabla 29. (Continuación)

ACTIVOS	Amenazas	Impacto					P	Riesgo				
		[D]	[I]	[C]	[A]	[T]		[D]	[I]	[C]	[A]	[T]
UPS de 20 KVA - Sede proyecto 968	[E.23] Errores de mantenimiento / actualización de equipos (hardware)	B					MB	MB				
	[A.7] uso no previsto	B					MB	MB				
	[A.23] Manipulación del hardware	B					MB	MB				
UPS de 10 KVA - UPI Bosa	[N.2] Daños por agua	B					MB	MB				
	[N.*] Desastres naturales	M					MB	B				
	[I.1] Fuego	M					MB	B				
	[I.5] Avería de origen físico o lógico	B					MB	MB				
	[I.6] Corte del suministro eléctrico	B					B	B				
	[I.7] Condiciones inadecuadas de temperatura o humedad	MB					B	MB				
	[I.9] Interrupción de otros servicios o suministros esenciales	B					B	B				
	[E.23] Errores de mantenimiento / actualización de equipos (hardware)	B					MB	MB				
	[A.7] uso no previsto	B					MB	MB				
	[A.23] Manipulación del hardware	B					MB	MB				
UPS de 20 KVA - UPI La 32	[N.2] Daños por agua	B					MB	MB				
	[N.*] Desastres naturales	M					MB	B				
	[I.1] Fuego	M					MB	B				
	[I.5] Avería de origen físico o lógico	B					MB	MB				
	[I.6] Corte del suministro eléctrico	B					B	B				
	[I.7] Condiciones inadecuadas de temperatura o humedad	MB					B	MB				
	[I.9] Interrupción de otros servicios o suministros esenciales	B					B	B				
	[E.23] Errores de mantenimiento / actualización de equipos (hardware)	B					MB	MB				

Tabla 29. (Continuación)

ACTIVOS	Amenazas	Impacto					P	Riesgo				
		[D]	[I]	[C]	[A]	[T]		[D]	[I]	[C]	[A]	[T]
UPS de 20 KVA - UPI La 32	[A.7] uso no previsto	B					MB	MB				
	[A.23] Manipulación del hardware	B					MB	MB				
UPS de 20 KVA - UPI La Florida	[N.2] Daños por agua	B					MB	MB				
	[N.*] Desastres naturales	M					MB	B				
	[I.1] Fuego	M					MB	B				
	[I.5] Avería de origen físico o lógico	B					MB	MB				
	[I.6] Corte del suministro eléctrico	B					B	B				
	[I.7] Condiciones inadecuadas de temperatura o humedad	MB					B	MB				
	[I.9] Interrupción de otros servicios o suministros esenciales	B					B	B				
	[E.23] Errores de mantenimiento / actualización de equipos (hardware)	B					MB	MB				
	[A.7] uso no previsto	B					MB	MB				
	[A.23] Manipulación del hardware	B					MB	MB				
UPS de 30 KVA - UPI El Perdomo	[N.2] Daños por agua	B					MB	MB				
	[N.*] Desastres naturales	M					MB	B				
	[I.1] Fuego	M					MB	B				
	[I.5] Avería de origen físico o lógico	B					MB	MB				
	[I.6] Corte del suministro eléctrico	B					B	B				
	[I.7] Condiciones inadecuadas de temperatura o humedad	MB					B	MB				
	[I.9] Interrupción de otros servicios o suministros esenciales	B					B	B				
	[E.23] Errores de mantenimiento / actualización de equipos (hardware)	B					MB	MB				
	[A.7] uso no previsto	B					MB	MB				
	[A.23] Manipulación del hardware	B					MB	MB				

Tabla 29. (Continuación)

ACTIVOS	Amenazas	Impacto					P	Riesgo				
		[D]	[I]	[C]	[A]	[T]		[D]	[I]	[C]	[A]	[T]
Sistema de aire acondicionado	[N.*] Desastres naturales	MA					MB	A				
	[I.5] Avería de origen físico o lógico	MA					MB	A				
	[I.6] Corte del suministro eléctrico	A					MB	M				

Fuente: Autor

8.5.2.5 Riesgo Potencial: [D] DATOS / INFORMACIÓN

Tabla 33. Riesgo potencial activos de tipo: Datos / Información

ACTIVOS	Amenazas	Impacto					P	Riesgo				
		[D]	[I]	[C]	[A]	[T]		[D]	[I]	[C]	[A]	[T]
Documentación Técnica	[N.2] Daños por agua	A	A				MB	M	M			
	[N.*] Desastres naturales	A	A				MB	M	M			
	[I.1] Fuego	A	A				MB	M	M			
	[I.7] Condiciones inadecuadas de temperatura o humedad	M	M				M	M	M			
	[E.18] Destrucción de la información	M	M				B	M	M			

Fuente: Autor

8.5.2.6 Riesgo Potencial: [P] PERSONAL

Tabla 34. Riesgo potencial activos de tipo: Personal

ACTIVOS	Amenazas	Impacto					P	Riesgo				
		[D]	[I]	[C]	[A]	[T]		[D]	[I]	[C]	[A]	[T]
Administradores de Sistemas	[E.7] Deficiencias en la organización	M					M	M				
	[E.28] Indisponibilidad del personal	A					M	A				
	[A.29] Extorsión	M	B	M			MB	B	MB	B		
	[A.30] Ingeniería Social	M	M	M			MB	B	B	B		

Fuente: Autor

8.5.2.7 Interpretación de los resultados

Una vez evaluado los activos y conocido el riesgo a los que están expuestos los mismos, se seleccionan los activos que poseen una valoración alta.

Esto con el fin de implementar posteriormente los controles para evitar que las amenazas se materialicen.

Dentro de este grupo de activos los que mayor riesgo tienen, son: el correo electrónico Zimbra y los equipos de cómputo.

En el activo del correo zimbra, el riesgo puede ocurrir puesto que tiene una probabilidad alta en cuanto a errores de los usuarios y en el manejo y respaldo de la información. Así mismo en las caídas del sistema bien sea por agotamiento de recursos y denegaciones del servicio.

En el activo de equipos de cómputo, el riesgo puede ocurrir puesto que tiene una probabilidad alta, a causa de averías de origen físico o lógico, abusos de privilegios de acceso y usos no previstos.

En el activo de tipo servicio “controladores de dominio”, el riesgo puede ocurrir ya que tiene una probabilidad alta en abusos de privilegios de acceso, usos no previstos, denegaciones de servicio y modificaciones de la información.

En el activo servidor de virtualización, el riesgo puede ocurrir puesto que tiene una probabilidad alta en cuanto a difusión de software dañino.

En el activo “Aplicación SIMI”, el riesgo puede ocurrir puesto que tiene una probabilidad alta por motivo a errores de los usuarios, denegaciones de servicio y de personal insuficiente.

En el activo “Antispam Barracuda”, el riesgo puede ocurrir puesto que tiene una probabilidad alta en errores del administrador del sistema, errores de mantenimiento, denegaciones de servicio y ataques destructivos.

9. CONTROLES DE SEGURIDAD DE LA INFORMACIÓN

Tabla 35. Controles de Seguridad de la Información

Dominio de Control	Objetivo de Control	Referencia del control	Título del control	Descripción del control	Controles seleccionados y de los fundamentos de la selección				Aplicado? (Si/No)	Estado actual del control	Justificación para la exclusión o documento de referencia
					Requerimiento Legal	Obligatorio	Requerimiento del negocio	Análisis de riesgos			
POLITICAS DE SEGURIDAD DE LA INFORMACION	Directrices establecidas por la dirección para la seguridad de la información	5.1.1	Políticas para la seguridad de la Información	Control: Se debería definir un conjunto de políticas para la seguridad de la información, aprobada por la dirección, publicada y comunicada a los empleados y a las partes externas pertinentes.	X	X		X	SI	El control se encuentra implementado y actualizado	Manual de política de seguridad y controles básicos y específicos para el manejo de la información - Código A-TIC-MA-001
		5.1.2	Revisión de las políticas para la seguridad de la información	Control: Las políticas para la seguridad de la información se deberían revisar a intervalos planificados o si ocurren cambios significativos, para para asegurar su conveniencia, adecuación y eficacia continuas.	X	X			SI	El control se revisa técnicamente por el Área de sistemas y administrativamente por los miembros del Comité de Sistemas y Tecnologías de la Información.	Manual de política de seguridad y controles básicos y específicos para el manejo de la información - Código A-TIC-MA-001 "numeral 5 Control de cambios", Resolución 282 del 07 de mayo de 2015.
ORGANIZACION DE LA SEGURIDAD DE LA INFORMACION	Organización Interna	A6.1.1	Roles y responsabilidades para la seguridad de la información	Control: Se deberían definir y asignar todas las responsabilidades de la seguridad de la información.	X	X	X	X	SI	Están definidas las responsabilidades para la implementación de la política de seguridad, sin embargo no están aprobadas las responsabilidades a nivel de responsable de los activos informáticos a nivel de Entidad.	Manual de política de seguridad y controles básicos y específicos para el manejo de la información - Código A-TIC-MA-001, acta de sistemas fecha 04 de noviembre de 2015.
		A6.1.2	Segregación de funciones	Control: Las funciones y áreas de responsabilidad en conflicto se deberían separar para reducir las posibilidades de modificación no autorizada o no intencional, o el uso indebido de los activos de la organización	X	X	X	X	NO	El control no se encuentra implementado	Sin embargo a través de la capacitación de la política de seguridad divulga las implicaciones sobre el manejo de accesos indebidos contemplados por la ley 1273 de 2009.

Tabla 32. (Continuación)

Dominio de Control	Objetivo de Control	Referencia del control	Título del control	Descripción del control	Controles seleccionados y de los fundamentos de la selección				Aplicado? (Si/No)	Estado actual del control	Justificación para la exclusión o documento de referencia
					Requerimiento Legal	Obligatorio	Requerimiento del negocio	Análisis de riesgos			
ORGANIZACION DE LA SEGURIDAD DE LA INFORMACION	Organización Interna	A6.1.3	Contacto con las autoridades	Control: Se deberían mantener contactos apropiados con las autoridades pertinentes.	X	X	X		NO	El control no se encuentra implementado	A pesar de que existen mecanismos a través de los profesionales de representación judicial de la Oficina Asesora Jurídica no existe un procedimiento divulgado y documentado del manejo de este control
		A6.1.4	Contacto con los grupos de interés especial	Control: Se deberían mantener contactos apropiados con grupos de interés especial u otros foros y asociaciones profesionales especializadas en seguridad			X		NO	El control no se encuentra implementado	No existen evidencias de relaciones con grupos que permitan estar atentos a las alertas, vulnerabilidades y amenazas sobre seguridad de la información.
		A6.1.5	Seguridad de la información en la gestión de proyectos	Control: La seguridad de la información se debería tratar en la gestión de proyectos, independientemente del tipo de proyecto.			X	X	NO	El control no se encuentra implementado	No existen procedimientos, documentación o metodología en la formulación de proyectos donde se aplique este control.
	Dispositivos Móviles y de Teletrabajo	A6.2.1	Política para dispositivos móviles	Control: Se deberían adoptar una política y unas medidas de seguridad de soporte, para gestionar los riesgos introducidos por el uso de dispositivos móviles.	X			X	NO	El control no se encuentra implementado adecuadamente	La entidad cuenta con conexiones para dispositivos móviles a través de las políticas de GPO y Vlans en el firewall para brindar dicho servicios a los usuarios que lo requieren sin embargo no se evidencia los registros de dichos usuarios, conexiones, copias sobre los accesos.
		A6.2.2	Teletrabajo	Control: Se deberían implementar una política y unas medidas de seguridad de soporte, para proteger la información a la que se tiene acceso, que es procesada o almacenada en los lugares en los que se realiza teletrabajo.	X				NO	El control no se encuentra implementado	La entidad no ha definido los procedimientos técnicos para facilitar el acceso a los usuarios.

Tabla 32. (Continuación)

Dominio de Control	Objetivo de Control	Referencia del control	Título del control	Descripción del control	Controles seleccionados y de los fundamentos de la selección				Aplicado? (Si/No)	Estado actual del control	Justificación para la exclusión o documento de referencia
					Requerimiento Legal	Obligatorio	Requerimiento del negocio	Análisis de riesgos			
SEGURIDAD DE LOS RECURSOS HUMANOS	Antes de asumir el empleo	A7.1.1	Selección	Control: Las verificaciones de los antecedentes de todos los candidatos a un empleo se deberían llevar a cabo de acuerdo con las leyes, reglamentaciones y ética pertinentes y deben ser proporcionales a los requisitos de negocio, a la clasificación de la información a que se va a tener acceso y a los riesgos percibidos.	X	X			NO	El control no se encuentra implementado	
		A7.1.2	Términos y Condiciones del empleo	Control: Los acuerdos contractuales con empleados y contratistas deberían establecer sus responsabilidades y las de la organización en cuanto a la seguridad de la información.	X				NO	El control no se encuentra implementado	La política de seguridad incluye la responsabilidad sobre el cumplimiento de la seguridad de la información para todos los usuarios, sin embargo no existen directrices dentro de los contratos o nombramientos en donde se especifiquen dichas responsabilidades.
	Durante la ejecución del empleo	A7.2.1	Responsabilidades de la dirección	Control: La dirección debería exigir a todos los empleados y contratista la aplicación de la seguridad de la información de acuerdo con las políticas y procedimientos establecidos por la organización.	X				SI	El control se encuentra implementado parcialmente	El área de Sistemas capacita y divulga a los funcionarios y contratistas sobre la toma de conciencia en la seguridad de la información
		A7.2.2	Toma de conciencia, educación y formación en la seguridad de la Información.	Control: Todos los empleados de la organización, y en donde sea pertinente, los contratistas, deberían recibir la educación y la formación en toma de conciencia apropiada, y actualizaciones regulares sobre las políticas y procedimientos de la organización pertinentes para su cargo.	X	X	X		SI	El control se encuentra implementado	El área de Sistemas capacita y divulga a los funcionarios y contratistas sobre la toma de conciencia en la seguridad de la información. Actas y formatos de asistencia comité, junta, reunión y/o capacitación con código g A-GDH-FT-010 años 2013 a 2015

Tabla 32. (Continuación)

Dominio de Control	Objetivo de Control	Referencia del control	Título del control	Descripción del control	Controles seleccionados y de los fundamentos de la selección				Aplicado? (Si/No)	Estado actual del control	Justificación para la exclusión o documento de referencia
					Requerimiento Legal	Obligatorio	Requerimiento del negocio	Análisis de riesgos			
SEGURIDAD DE LOS RECURSOS HUMANOS	Durante la ejecución del empleo	A7.2.3	Proceso disciplinario.	Control: Se debería contar con un proceso formal, el cual debe ser comunicado, para emprender acciones contra empleados que hayan cometido una violación a la seguridad de la información.	X	X			SI	El control se encuentra implementado	Las acciones pertinentes son realizadas por el grupo de trabajo de control interno disciplinario el cual depende de la Subdirección Técnica Administrativa y Financiera
	Terminación y cambio de empleo	A7.3.1	Responsabilidades en la terminación o cambio del empleo	Control: Las responsabilidades y los deberes de seguridad de la información que permanecen validos después de la terminación o cambio de empleo de deberían definir, comunicar al empleado o contratista y se deberían hacer cumplir.	X	X	X		SI	El control se encuentra implementado	Este control es realizado por la subdirección Técnica de Desarrollo Humano, quien informa a través de memorando a cada una de las áreas con el fin de que cada una de ellas entregue la certificación de paz y salvo correspondiente.
GESTIÓN DE ACTIVOS	Responsabilidad por los activos	A8.1.1	Inventario de activos	Control: Se deberían identificar la información, otros activos asociados con información y las instalaciones de procesamiento de información, y se deberían elaborar y mantener un inventario de estos activos.	X	X	X	X	SI	El control esta implementado	Este control esta implementado a nivel de los activos que gestiona el proceso de Gestión Tecnológica y de la información, el cual está avalado y aprobado por el grupo de funcionarios y contratistas del Área de Sistemas.
		A8.1.2	Propiedad de los Activos	Control: Los activos mantenidos en el inventario deberían tener un propietario.	X	X	X	X	SI	El control esta implementado	Este control esta implementado a nivel de los activos que gestiona el proceso de Gestión Tecnológica y de la información, el cual está avalado y aprobado por el grupo de funcionarios y contratistas del Área de Sistemas; de igual manera el área e almacén tiene establecido los propietarios de los activos de acuerdo al Manual de procedimientos administrativos y contables para el manejo y control de bienes en los Entes públicos del Distrito Capital

Tabla 32. (Continuación)

Dominio de Control	Objetivo de Control	Referencia del control	Título del control	Descripción del control	Controles seleccionados y de los fundamentos de la selección				Aplicado? (Si/No)	Estado actual del control	Justificación para la exclusión o documento de referencia
					Requerimiento Legal	Obligatorio	Requerimiento del negocio	Análisis de riesgos			
GESTIÓN DE ACTIVOS	Responsabilidad por los activos	A8.1.3	Uso aceptable de los activos	Control: Se deberían identificar, documentar e implementar reglas para el uso aceptable de información y de activos asociados con información e instalaciones de procesamiento de información.		X	X	X	NO	El control no está implementado	No existe un procedimiento establecido ni obligaciones contractuales que den alcance y permitan el manejo de los activos de información, solo existe la generación de una certificación a nivel de paz y salvo para la finalización de relaciones contractuales.
		A8.1.4	Devolución de Activos	Control: Todos los empleados y usuarios de partes externas deberían devolver todos los activos de la organización que se encuentren a su cargo, al terminar su empleo, contrato o acuerdo.	X	X	X	X	SI	El control se encuentra implementado	Se realiza a través de paz y salvos que tienen que ser emitidas por diferentes áreas, sin embargo se debe fortalecer el procedimiento ya que debe ser controlado la copia de la información institucional en cualquier formato, ya que esto debe ser autorizado de manera oficial.
	Clasificación de la información	A8.2.1	Clasificación de la información	Control: La información se debería clasificar en función de los requisitos legales, valor, criticidad y susceptibilidad a divulgación o a modificación no autorizada.	X	X	X	X	NO	El control no se encuentra implementado	No se encuentra clasificada la información
		A8.2.2	Etiquetado de la información	Control: Se debería desarrollar e implementar un conjunto adecuado de procedimientos para el etiquetado de la información, de acuerdo con el esquema de clasificación de información adoptado por la organización.	X	X	X	X	NO	El control no se encuentra implementado	No existe documentación sobre avances de implementación de este control.
		A8.2.3	Manejo de activos	Control: Se deberían desarrollar e implementar procedimientos para el manejo de activos, de acuerdo con el esquema de clasificación de información adoptado por la organización.	X	X	X	X	NO	El control no se encuentra implementado	No se ha definido el procedimiento para manejo de activos de acuerdo al esquema de clasificación de los mismos, sin embargo a nivel de los activos de TI existe acta de fecha 04 de noviembre de 2015 que define los responsable de dichos activos.

Tabla 32. (Continuación)

Dominio de Control	Objetivo de Control	Referencia del control	Título del control	Descripción del control	Controles seleccionados y de los fundamentos de la selección				Aplicado? (Si/No)	Estado actual del control	Justificación para la exclusión o documento de referencia
					Requerimiento Legal	Obligatorio	Requerimiento del negocio	Análisis de riesgos			
GESTIÓN DE ACTIVOS	Manejo de medios	A8.3.1	Gestión de medios removibles	Control: Se deberían implementar procedimientos para la gestión de medio removibles, de acuerdo con el esquema de clasificación adoptado por la organización.		X	X		NO	El control no se encuentra implementado	No existen procedimientos claros para el manejo de medios removibles, ni evidencias para mitigar la degradación de los mismos.
		A8.3.2	Disposición de los medios	Control: Se debería disponer en forma segura de los medios cuando ya no se requieran, utilizando procedimientos formales.		X	X	X	NO	El control no se encuentra implementado	No existen procedimientos documentados que permitan y reflejen la destrucción de datos en medios obsoletos, tampoco existe evidencia de confidencialidad a través de los acuerdos con terceros con quien se realiza la disposición final de los medios.
		A8.3.3	Transferencia de medios físicos	Control: Los medios que contienen información de deberían proteger contra acceso no autorizado, uso indebido o corrupción durante el transporte.	X	X			NO	El control no se encuentra implementado	En lo concerniente a los activos de TI, no se maneja esta procedimiento, se debe valorar también por la parte de Gestión documental en el manejo de correspondencia física.
CONTROL DE ACCESO	Requisitos del negocio para el control de acceso	A9.1.1	Política de control de acceso	Control: Se debería establecer, documentar y revisar una política de control de acceso con base en los requisitos del negocio y de seguridad de la información.	X	X	X		SI	El control se encuentra implementado	Se encuentra implementado en cuanto a permisos de accesos físicos a las áreas de procesamiento de la información, acceso a los servicios de respaldo, aplicaciones o archivos, sin embargo se debe realizar el procedimiento pendiente. Las políticas están creadas dentro del Manual de política de seguridad y controles básicos y específicos para el manejo de la información - Código A-TIC-MA-001 y los formatos CONTROL DE ACCESO AL CENTRO DE COMPUTO Y CUARTOS DE COMUNICACIONES A-TIC-FT-009

Tabla 32. (Continuación)

Dominio de Control	Objetivo de Control	Referencia del control	Título del control	Descripción del control	Controles seleccionados y de los fundamentos de la selección				Aplicado? (Si/No)	Estado actual del control	Justificación para la exclusión o documento de referencia
					Requerimiento Legal	Obligatorio	Requerimiento del negocio	Análisis de riesgos			
CONTROL DE ACCESO	Requisitos del negocio para el control de acceso	A9.1.2	Acceso a redes y a Servicios de red	Control: Solo se debería permitir acceso de los usuarios a la red y a los servicios de red para los que hayan sido autorizados específicamente.			X		NO	No esta implementado el control	No existen documentos ni procedimientos asociados a definición de acceso de usuarios a redes y servicios, se asignan de acuerdo a lo solicitado por el Responsable de la dependencia o supervisor del contrato del usuario.
	Gestión de acceso de usuarios	A9.2.1	Registro y cancelación del registro de usuarios	Control: Se debería implementar un proceso formal de registro y de cancelación de registro de usuarios, para posibilitar la asignación de los derechos de acceso.	X	X	X		SI	El control se encuentra implementado parcialmente	Se realiza la asignación de registro de usuarios en la base de datos de los Sistemas de información, existen diferentes servicios que se sincronizan por medio del LDAP del directorio activo, sin embargo no existe procedimiento ni registros documentados sobre cancelación de usuarios.
		A9.2.2	Suministro de acceso de usuarios	Control: Se debería implementar un proceso de suministro de acceso formal de usuarios para asignar o revocar los derechos de acceso para todo tipo de usuarios para todos los sistemas y servicios.	X	X	X		SI	El control se encuentra implementado parcialmente	Dentro del Manual de política de seguridad y controles básicos y específicos para el manejo de la información - Código A-TIC-MA-001, está indicado de manera general los permisos y horarios para el manejo de la red, adicional los permisos son permitidos de acuerdo a los requerimientos solicitados por los responsables de las Áreas o supervisores de los contratos de dichos usuarios. Sin embargo no existe un procedimiento establecido ni documentación de los registros de estas actividades.
		A9.2.3	Gestión de derechos de acceso privilegiado	Control: Se debería restringir y controlar la asignación y uso de derechos de acceso privilegiado	X	X	X		NO	El control no se encuentra implementado	Los permisos son permitidos de acuerdo a los requerimientos solicitados por los responsables de las Áreas o supervisores de los contratos de dichos usuarios. Sin embargo no existe un procedimiento establecido ni documentación sobre los derechos de accesos.

Tabla 32. (Continuación)

Dominio de Control	Objetivo de Control	Referencia del control	Título del control	Descripción del control	Controles seleccionados y de los fundamentos de la selección				Aplicado? (Si/No)	Estado actual del control	Justificación para la exclusión o documento de referencia
					Requerimiento Legal	Obligatorio	Requerimiento del negocio	Análisis de riesgos			
CONTROL DE ACCESO	Gestión de acceso de usuarios	A9.2.4	Gestión de información de autentica-ción secreta de usuarios	Control: La asignación de información de autenticación secreta se debería controlar por medio de un proceso de gestión formal.	X	X	X		SI	El control se encuentra implementado	Existe dentro de la política de GPO, LDAP y sistemas de información mecanismos de cifrado, proceso de parametrización para el manejo de contraseñas; las cuales también se encuentran establecidos en la política de seguridad de la información a través del documento Manual de política de seguridad y controles básicos y específicos para el manejo de la información - Código A-TIC-MA-001
		A9.2.5	Revisión de los derechos de acceso de usuarios	Control: Los propietarios de los activos deberían revisar los derechos de acceso de los usuarios, a intervalos regulares.	X	X	X		NO	El control no está implementado	No existe documentación que evidencie la implementación o seguimiento al control
		A9.2.6	Retiro o ajuste de los derechos de usuario	Control: Los derechos de acceso de todos los empleados y de usuarios externos a la información y a las instalaciones de procesamiento de información se deberían retirar al terminar su empleo, contrato o acuerdo, o se deberían ajustar cuando se hagan cambios.	X	X	X		SI	El control se encuentra implementado	Una vez se informa al área de sistemas la novedad de retiro, vacaciones o reasignación del lugar de trabajo los usuarios, se procede a bloquear la cuenta o reorganizar a la unidad organizacional pertinente.
	Responsabilidades del usuario	A9.3.1	Uso de información de información secreta para la autenticación	Control: Se debería exigir a los usuarios que cumplan las prácticas de la organización para el uso de información secreta para la autenticación.	X	X	X		SI	El control se encuentra implementado	Existe dentro de la política de GPO, LDAP y sistemas de información mecanismos de cifrado, proceso de parametrización para el manejo de contraseñas; las cuales se refuerzan con la política de seguridad, en cuanto al manejo a los usuarios. Política establecida en el Manual de política de seguridad y controles básicos y específicos para el manejo de la información - Código A-TIC-MA-001

Tabla 32. (Continuación)

Dominio de Control	Objetivo de Control	Referencia del control	Título del control	Descripción del control	Controles seleccionados y de los fundamentos de la selección				Aplicado? (Si/No)	Estado actual del control	Justificación para la exclusión o documento de referencia
					Requerimiento Legal	Obligatorio	Requerimiento del negocio	Análisis de riesgos			
CONTROL DE ACCESO	Control de acceso a sistemas y aplicaciones	A9.4.1	Restricción de acceso a la información	Control: El acceso a la información y a la funcionalidad de las aplicaciones se debería restringir de acuerdo con la política de control de acceso.		X	X		SI	El control se encuentra implementado	Se da acceso a los usuarios dependiendo del rol solicitado por el responsable del Área o supervisor del contrato.
		A9.4.2	Procedimiento de ingreso seguro	Control: Cuando lo requiere la política de control de acceso, el acceso a sistemas y aplicaciones se debería controlar mediante un proceso de ingreso seguro.	X	X	X		SI	El control se encuentra implementado	Existe la política creada dentro del Manual de política de seguridad y controles básicos y específicos para el manejo de la información - Código A-TIC-MA-001, las contraseñas se crean dentro de los esquemas de contraseña de cada aplicación.
		A9.4.3	Sistema de gestión de contraseñas	Control: Los sistemas de gestión de contraseñas deberían ser interactivos y deberían asegurar la calidad de las contraseñas.	X	X	X		SI	El control se encuentra implementado	Existe la política creada dentro del Manual de política de seguridad y controles básicos y específicos para el manejo de la información - Código A-TIC-MA-001, las contraseñas se crean de acuerdo a la autoridad de cada aplicación, en la gestión de contraseñas para el ingreso a la red y sobre las políticas del LDAP estas deben ser cambiada cada 30 días, en cuanto a las aplicaciones el cambio de contraseñas se gestionan dependiendo de cada la aplicación.
		A9.4.4	Uso de programas utilitarios privilegiados	Control: Se debería restringir y controlar estrictamente el usos de programas utilitarios que podrían tener capacidad de anular el sistema y los controles de las aplicaciones.			X		NO	El control no se encuentra implementado	No esta implementado un programa utilitario en el proceso de TI.
		A9.4.5	Control de acceso a códigos fuente de programas	Control: Se debería restringir el acceso a los códigos fuente de los programas.			X		NO	El control no se encuentra implementado	No existe un procedimiento establecido.

Tabla 32. (Continuación)

Dominio de Control	Objetivo de Control	Referencia del control	Título del control	Descripción del control	Controles seleccionados y de los fundamentos de la selección				Aplicado? (Si/No)	Estado actual del control	Justificación para la exclusión o documento de referencia
					Requerimiento Legal	Obligatorio	Requerimiento del negocio	Análisis de riesgos			
CRIPTOGRAFIA	Controles criptográficos	A10.1.1	Política sobre el uso de controles criptográficos	Control: Se debería desarrollar e implementar una política sobre el uso de controles criptográficos para la protección de la información.			X		NO	El control no se encuentra implementado	No existe un procedimiento en la entidad o un requerimiento por un área específica sobre este control.
		A10.1.2	Gestión de llaves	Control: Se debería desarrollar e implementar una política sobre el uso, protección y tiempo de vida de las llaves criptográficas, durante todo su ciclo de vida.	X	X	X	X	NO	El control no se encuentra implementado	No existe evidencias de procedimientos para el manejo de generación, resguardo, custodia, almacenamiento y bajas de llaves criptográficas; las llaves existentes se les da tratamiento de acuerdo al ente que lo requiere y es responsabilidad del funcionario dueño de la firma.
SEGURIDAD FISICA Y DEL ENTORNO	Áreas seguras	A11.1.1	Perímetro de seguridad física	Control: Se deberían definir y usar perímetros de seguridad, y usarlos para proteger áreas que contengan información confidencial o critica, e instalaciones de manejo de información.	X	X	X		SI	El control se encuentra implementado	Están definidos los perímetros de seguridad física para el resguardo adecuado de los activos de información, los cuales se encuentran documentados en los planos existentes.
		A11.1.2	Controles de acceso físicos	Control: Las áreas seguras se deberían proteger mediante controles de acceso apropiados para asegurar que sólo se permite el ingreso a personal autorizado.	X	X	X		SI	El control se encuentra implementado	Existen obligaciones contractuales y procedimientos para la empresa que presta el servicio de vigilancia para el manejo y control de registros de funcionaros, visitantes, monitoreo de accesos, en cuanto a la seguridad del centro de cómputo y área de comunicaciones el área de sistemas posee control biométrico para el acceso al centro de cómputo y formato para el CONTROL DE ACCESO AL CENTRO DE COMPUTO Y CUARTOS DE COMUNICACIONES con código A-TIC-FT-009, actualmente se está realizando el procedimiento de seguridad de la información.

Tabla 32. (Continuación)

Dominio de Control	Objetivo de Control	Referencia del control	Título del control	Descripción del control	Controles seleccionados y de los fundamentos de la selección				Aplicado? (Si/No)	Estado actual del control	Justificación para la exclusión o documento de referencia
					Requerimiento Legal	Obligatorio	Requerimiento del negocio	Análisis de riesgos			
SEGURIDAD FISICA Y DEL ENTORNO	Áreas seguras	A11.1.3	Seguridad de oficinas, recinto e instalaciones	Control: Se debería diseñar y aplicar la seguridad física a oficinas, recintos e instalaciones.	X	X	X		SI	El control se encuentra implementado mediadamente, sin embrago debe documentarse y actualizarse.	Actualmente existen seguridad a nivel de acceso a las instalaciones a nivel general y en algunas áreas específicas, sin embrago debe fortalecerse este control.
		A11.1.4	Protección contra amenazas externas y ambientales	Control: Se deberían diseñar y aplicar protección física contra desastres naturales, ataques maliciosos o accidentes.	X	X	X		SI	El control se encuentra medianamente implementado	En cuanto al proceso de Ti existen los elementos para protección contra incendio en el centro de cómputo.
		A11.1.5	Trabajo en áreas seguras	Control: Se debería diseñar y aplicar procedimientos para trabajo en áreas seguras.	X	X	X		SI	El control se encuentra medianamente implementado	Se debe revisar y documentar las políticas existentes; este control solo se ve aplicado en el Área de Tesorería
		A11.1.6	Áreas de despacho y carga	Control: Se debería controlar los puntos de acceso tales como las áreas de despacho y de carga y otros puntos en donde pueden entrar personas no autorizadas y, si es posible, aislarlos de las instalaciones de procesamiento de información para evitar el acceso no autorizado.	X	X	X		NO	El control no se encuentra implementado	Se deben crear políticas y formatos aprobados donde se evidencien las actividades realizadas de implementación de este control
	Equipos	A11.2.1	ubicación y protección de los equipos	Control: Los equipos deberían estar ubicados y protegidos para reducir los riesgos de amenazas y peligros del entorno, y las posibilidades de acceso no autorizado.	X	X	X		SI	El control se encuentra implementado	Existe la política aprobada sobre la seguridad y protección de los equipos de TI, sin embargo hay que fortalecer las actividades sobre este control
		A11.2.2	Servicios de suministro	Control: Los equipos se deberían proteger contra fallas de energía y otras interrupciones causadas por fallas en los servicios de suministro.	X	X	X		SI	El control se encuentra implementado	Aunque se encuentra implementado se requiere revisión y documentación actualizada.

Tabla 32. (Continuación)

Dominio de Control	Objetivo de Control	Referencia del control	Título del control	Descripción del control	Controles seleccionados y de los fundamentos de la selección				Aplicado? (Si/No)	Estado actual del control	Justificación para la exclusión o documento de referencia
					Requerimiento Legal	Obligatorio	Requerimiento del negocio	Análisis de riesgos			
SEGURIDAD FISICA Y DEL ENTORNO	Equipos	A11.2.3	Seguridad del cableado	Control: El cableado de energía eléctrica y de telecomunicaciones que porta datos o brinda soporte a los servicios de información debería estar protegido contra interceptación, interferencia o daño.	X	X	X		SI	El control se encuentra implementado	Aunque se encuentra implementado se requiere revisión y documentación actualizada; se debe contar con la documentación de acceso a los paneles de red de telecomunicaciones, de energía eléctrica normal y regulada.
		A11.2.4	Mantenimiento de equipos	Control: Los equipos se deberían mantener correctamente para asegurar su disponibilidad e integridad continuas.	X	X	X	X	SI	El control se encuentra implementado	Se realiza el mantenimiento de todos los equipos del proceso de TI, existe la política y la documentación pertinente la cual se refleja a través de los formatos 013 CONOGRAMA DE MANTENIMIENTO PREVENTIVO A-TIC-FT-013 y 005 REGISTRO DE SOPORTE TÉCNICO DE HARDWARE Y SOFTWARE POR EQUIPO A-TIC-FT-005
		A11.2.5	Retiro de activos	Control: Los equipos, información o software no se deberían retirar de su sitio sin autorización previa	X	X	X	X	SI	El control se encuentra implementado	Este control se encuentra documentado y se realiza a los funcionarios y contratistas según los procedimientos y políticas existentes.
		A11.2.6	Seguridad de equipos y activos fuera de las instalaciones	Control: Se deberían aplicar medidas de seguridad a los activos que se encuentran fuera de las instalaciones de la organización, teniendo en cuenta los diferentes riesgos de trabajar fuera de dichas instalaciones.	X	X	X	X	NO	El control no se encuentra implementado	Debe realizarse el procedimiento apropiado para el manejo de este control.
		A11.2.7	Disposición segura o reutilización de equipos	Control: Se deberían verificar todos los elementos de equipos que contengan medios de almacenamiento para asegurar que cualquier dato sensible o software licenciado haya sido retirado o sobrescrito en forma segura antes de su disposición o reúso.	X	X	X	X	SI	El control se encuentra implementado medianamente	Se realiza formateo de los equipos para reúso, se hace borrado de la información de dispositivos para darlos de baja, sin embargo hay que fortalecer los procedimientos y realizar la documentación pertinente.

Tabla 32. (Continuación)

Dominio de Control	Objetivo de Control	Referencia del control	Título del control	Descripción del control	Controles seleccionados y de los fundamentos de la selección				Aplicado? (Si/No)	Estado actual del control	Justificación para la exclusión o documento de referencia
					Requerimiento Legal	Obligatorio	Requerimiento del negocio	Análisis de riesgos			
SEGURIDAD FISICA Y DEL ENTORNO	Equipos	A11.2.8	Equipos de usuario desatendido	Control: Los usuarios deberían asegurarse de que a los equipos desatendidos se les da protección apropiada.	X	X	X	X	SI	El control se encuentra implementado	Bloqueo automático de sesión, a través de política de GPO. Política existente en el Manual de política de seguridad y controles básicos y específicos para el manejo de la información - Código A-TIC-MA-001
		A11.2.9	Política de escritorio limpio y pantalla limpia	Control: Se debería adoptar una política de escritorio limpio para los papeles y medios de almacenamiento removibles, y una política de pantalla limpia en las instalaciones de procesamiento de información.	X	X			SI	El control se encuentra implementado	Existe la política de seguridad sobre este control, en la parte de política en cuanto a papeles físicos en el escritorio el proceso de Gestión Ambiental capacita y divulga sobre estas actividades de acuerdo con su área específica.
SEGURIDAD DE LAS OPERACIONES	Procedimientos operacionales y responsabilidades	A12.1.1	Procedimientos de operación documentados	Control: Los procedimientos de operación se deberían documentar y poner a disposición de todos los usuarios que los necesitan.	X	X	X		SI	Control implementado parcialmente	Se debe documentar todos los procedimientos de operación de las actividades de instalación, configuración y su de los sistemas computacionales; actualmente se cuenta con la información actualizada y aprobada en: MANUAL DE USUARIO DEL SPRAI A-TIC-MA-003, MANUAL DE ADMINISTRADOR DEL SPRAI A-TIC-MA-004, MANUAL PARA EL MANEJO DE LA APLICACION DE RESPALDOS DATA PROTECTOR Y POLITICAS DE RESGUARDO A-TIC-MA-005, MANUAL DE USUARIO SIMI A-TIC-MA-006 e instructivo ARANDA SERVICE DESK- MESA DE AYUDA SISTEMAS SEDE ADMINISTRATIVA A-TIC-IN-001

Tabla 32. (Continuación)

Dominio de Control	Objetivo de Control	Referencia del control	Título del control	Descripción del control	Controles seleccionados y de los fundamentos de la selección				Aplicado? (Si/No)	Estado actual del control	Justificación para la exclusión o documento de referencia
					Requerimiento Legal	Obligatorio	Requerimiento del negocio	Análisis de riesgos			
SEGURIDAD DE LAS OPERACIONES	Procedimientos operacionales y responsabilidades	A12.1.2	Gestión de cambios	Control: Se deberían controlar los cambios en la organización, en los procesos de negocio, en las instalaciones y en los sistemas de procesamiento de información que afectan la seguridad de la información.	X	X			NO	El control no se encuentra implementado	No existen procedimientos y políticas donde se implemente este control.
		A12.1.3	Gestión de capacidad	Control: Se debe hacer seguimiento al uso de recursos, hacer los ajustes, y hacer proyecciones de los requisitos de capacidad futura, para asegurar el desempeño requerido del sistema.	X	X			NO	El control no se encuentra implementado	No existe documentación ni procedimientos sobre control en la entidad.
		A12.1.4	Separación de los ambientes de desarrollo, prueba y operación	Control: Se deberían separar los ambientes de desarrollo, pruebas y producción, para reducir los riesgos de acceso o cambios no autorizados al ambiente de operación.	X	X			NO	En control se encuentra implementado parcialmente	Aunque existe la política y los ambientes de pruebas y desarrollo están separados, no existe ninguna documentación al respecto por lo tanto es indispensable realizar los formatos y procedimientos pertinentes.
	Protección contra los códigos maliciosos	A12.2.1	Controles contra códigos maliciosos	Control: Se debería implementar controles de detección, de prevención y de recuperación, combinados con la toma de conciencia apropiada de los usuarios, para proteger contra códigos maliciosos.		X	X		SI	El control se encuentra implementado adecuadamente	El control se encuentra implementado a través de la política de seguridad y la existencia de los contratos de soporte del software de antivirus, las políticas aplicadas y el monitoreo permanente que se hace a políticas y equipos y el respaldo de políticas a través del equipo de seguridad perimetral.
	Copias de respaldo	A12.3.1	Respaldo de la información	Control: Se deberían hacer copias de respaldo de la información, software e imágenes de los sistemas, y ponerlas a prueba regularmente de acuerdo con una política de copias de respaldo acordadas.	X	X	X		SI	El control se encuentra implementado adecuadamente	El control se encuentra implementado aunque debe reforzarse los procedimientos y realizar pruebas de restauración eventualmente. Formato de seguimiento de realización de backups: BITACORA DE BACKUP A-TIC-FT-012

Tabla 32. (Continuación)

Dominio de Control	Objetivo de Control	Referencia del control	Título del control	Descripción del control	Controles seleccionados y de los fundamentos de la selección				Aplicado? (Si/No)	Estado actual del control	Justificación para la exclusión o documento de referencia
					Requerimiento Legal	Obligatorio	Requerimiento del negocio	Análisis de riesgos			
SEGURIDAD DE LAS OPERACIONES	Registro y seguimiento	A12.4.1	Registro de eventos	Control: Se deberían elaborar, conservar y revisar regularmente los registros acerca de actividades del usuario, excepciones, fallas y eventos de seguridad de la información.	X	X			NO	El control no se encuentra implementado	No hay políticas aplicadas ni documentación acerca de actividades sobre este control, se debería implementar un sistema de gestión y monitoreo de la red; sin embargo las soluciones de directorio activo, firewall, correo tiene sus propias soluciones.
		A12.4.2	Protección de la información de registro	Control: Los sistemas de gestión de registro y la información de registro se deberían proteger contra alteración y acceso no autorizado.	X	X			NO	El control no se encuentra implementado	No hay políticas aplicadas ni documentación acerca de actividades sobre este control
		A12.4.3	Registros del administrador y del operador	Control: Las actividades del administrador y del operador del sistema se deberían registrar, y los registros se deben proteger y revisar con regularidad.		X	X		NO	El control no se encuentra implementado	No hay políticas aplicadas ni documentación acerca de actividades sobre este control
		A12.4.4	Sincronización de relojes	Control: Los relojes de todos los sistemas de procesamiento de información pertinentes dentro de una organización o ámbito de seguridad se deberían sincronizar con una única fuente de referencia de tiempo.	X	X	X		SI	El control se encuentra implementado adecuadamente	Se realiza a través del protocolo W32Time
	Control de software operacional	A12.5.1	Instalación de software en sistemas operativos	Control: Se deberían implementar procedimientos para controlar la instalación de software en sistemas operativos.	X	X	X		NO	El control no se encuentra implementado	No hay registros de las configuraciones y actividades que evidencien el desarrollo de este control.
	Gestión de la vulnerabilidad técnica	A12.6.1	Gestión de las vulnerabilidades técnicas	Control: Se debería obtener oportunamente información acerca de las vulnerabilidades técnicas de los sistemas de información que se usen; evaluar la exposición de la organización a estas vulnerabilidades, y tomar las medidas apropiadas para tratar el riesgo asociado.	X	X	X		NO	El control no se encuentra implementado	No existe evidencia ni procedimientos para la implementación de este control.

Tabla 32. (Continuación)

Dominio de Control	Objetivo de Control	Referencia del control	Título del control	Descripción del control	Controles seleccionados y de los fundamentos de la selección				Aplicado? (Si/No)	Estado actual del control	Justificación para la exclusión o documento de referencia
					Requerimiento Legal	Obligatorio	Requerimiento del negocio	Análisis de riesgos			
SEGURIDAD DE LAS OPERACIONES	Gestión de la vulnerabilidad técnica	A12.6.2	Restricciones sobre la instalación de software	Control: Se deberían establecer e implementar las reglas para la instalación de software por parte de los usuarios.	X	X	X		SI	El control se encuentra implementado	Esta aprobada la política dentro del documento Manual de política de seguridad y controles básicos y específicos para el manejo de la información - Código A-TIC-MA-001, desde los permisos de usuarios de GPO del directorio activo están contemplados los permisos y las restricciones de los mismos a los usuarios.
	Consideraciones sobre auditorias de sistemas de información	A12.7.1	Controles de auditorías de sistemas de información	Control: Los requisitos y actividades de auditoria que involucran la verificación de los sistemas operativos se deberían planificar y acordar cuidadosamente para minimizar las interrupciones en los procesos del negocio.	X	X	X		NO	El control no se encuentra implementado	No existen actividades sobre pruebas técnicas, acceso a software y procedimientos concernientes a pruebas de auditoría
SEGURIDAD DE LAS COMUNICACIONES	Gestión de la seguridad de las redes	A13.1.1	Controles de redes	Control: Las redes se deberían Gestionar y controlar para proteger la información en sistemas y aplicaciones.	X	X	X		**SI**	El control se encuentra implementado parcialmente	El control se encuentra implementado a través del Firewall sin embargo no existe documentación sobre esta implementación.
		A13.1.2	Seguridad de los servicios de red	Control: Se deberían identificar los mecanismos de seguridad, los niveles de servicio y los requisitos de gestión de todos los servicios de red, e incluirlos en los acuerdos de servicio de red, ya sea que los servicios se presten internamente o se contraten externamente.	X	X	X		SI	El control se encuentra implementado parcialmente	El control se encuentra implementado a través del Firewall y los switch sin embargo no existe documentación sobre esta implementación.
		A13.1.3	Separación en las redes	Control: Los grupos de servicios de información, usuarios y sistemas de información se deberían separar en las redes.	X	X	X		SI	El control se encuentra implementado parcialmente	El control se encuentra implementado a través del Firewall y los switch sin embargo no existe documentación sobre esta implementación.

Tabla 32. (Continuación)

Dominio de Control	Objetivo de Control	Referencia del control	Título del control	Descripción del control	Controles seleccionados y de los fundamentos de la selección				Aplicado? (Si/No)	Estado actual del control	Justificación para la exclusión o documento de referencia
					Requerimiento Legal	Obligatorio	Requerimiento del negocio	Análisis de riesgos			
SEGURIDAD DE LAS COMUNICACIONES	Transferencia de información	A13.2.1	Políticas y procedimientos de transferencia de información	Control: Se debería contar con políticas, procedimientos y controles de transferencia información formales para proteger la transferencia de información mediante el uso de todo tipo de instalaciones de comunicaciones.			X		SI	El control no se encuentra implementado	No hay evidencia de implementación de este control
		A13.2.2	Acuerdos sobre transferencia de información	Control: Los acuerdos deberían tratar la transferencia segura de información de la información negocio entre la organización y las partes externas.			X		SI	El control no se encuentra implementado	No hay evidencia de implementación de este control
		A13.2.3	Mensajería electrónica	Control: Se debería proteger adecuadamente la información incluida en la mensajería electrónica.	X	X			SI	El control se encuentra implementado	El control se encuentra implementado a través del servicio de correo electrónico, las políticas están definidas dentro Manual de política de seguridad y controles básicos y específicos para el manejo de la información - Código A-TIC-MA-001, la configuración de la plataforma de correo y la divulgación de las políticas.
		A13.2.4	Acuerdos de confidencialidad o de no divulgación	Control: Se debería identificar, revisar regularmente y documentar los requisitos para los acuerdos de confidencialidad o no divulgación que reflejen las necesidades de la organización.	X	X	X		SI	El control no se encuentra implementado	No hay evidencia de la implementación de este control
ADQUISICION, DESARROLLO Y MANTENIMIENTO DE LOS SISTEMAS	Requisitos de seguridad de los sistemas de información	A14.1.1	Análisis y especificación de los requisitos de seguridad de la información	Control: Los requisitos relacionados con seguridad de la información se debería incluir en los requisitos para nuevos sistemas de información o para mejoras a los sistemas de información existentes.	X	X	X		SI	El control se encuentra implementado parcialmente	Aunque se llevan a cabo actividades sobre este control debe revisarse y documentarse de manera adecuada.

Tabla 32. (Continuación)

Dominio de Control	Objetivo de Control	Referencia del control	Título del control	Descripción del control	Controles seleccionados y de los fundamentos de la selección				Aplicado? (Si/No)	Estado actual del control	Justificación para la exclusión o documento de referencia
					Requerimiento Legal	Obligatorio	Requerimiento del negocio	Análisis de riesgos			
ADQUISICION, DESARROLLO Y MANTENIMIENTO DE LOS SISTEMAS	Requisitos de seguridad de los sistemas de información	A14.1.2	Seguridad de los servicios de las aplicaciones en redes publicas	Control: La información involucrada en los servicios de las aplicaciones que pasan sobre redes públicas se debería proteger de actividades fraudulentas, disputas contractuales y divulgación y modificación no autorizadas.	X	X	X		SI	El control se encuentra implementado parcialmente	Se debe revisar y fortalecer los procedimientos y actividades de este control al mismo tiempo tener documentado todo tipo de políticas y accesos, actualmente este control se realizar a través del Firewall - Configuración de DMZ para los servicios aplicados.
		A14.1.3	Protección de transacciones de los servicios de las aplicaciones	Control: La información involucrada en las transacciones de los servicios de las aplicaciones se debería proteger para evitar la transmisión incompleta, el enrutamiento errado, la alteración no autorizada de mensajes, la divulgación no autorizada, y la duplicación o producción de mensajes no autorizada.	X	X			SI	El control se encuentra implementado parcialmente	El control se encuentra implementado a través del código desarrollado, sin embargo no se encuentra la documentación respectiva donde se evidencie adecuadamente este manejo.
	Seguridad en los procesos de desarrollo y soporte	A14.2.1	Política de desarrollo seguro	Control: Se deberían establecer y aplicar reglas para el desarrollo de software y de sistemas, a los desarrollos dentro de la organización.		X			SI	El control no se encuentra implementado	Se debe revisar y documentar este control ya que se realizan actividades en los desarrollos pero no están documentados.
		A14.2.2	Procedimientos de control de cambio en sistemas	Control: Los cambios a los sistemas dentro del ciclo de vida de desarrollo se deberían controlar mediante el uso de procedimientos formales de control de cambios.		X			SI	El control se encuentra implementado parcialmente.	Las actividades de desarrollo de software se documentan en los formatos de SOLICITUD DESARROLLO Y/O ACTUALIZACIÓN DE SOFTWARE A-TIC-FT-010 y LEVANTAMIENTO DE REQUERIMIENTOS A-TIC-FT-011, sin embargos este control debe revisarse
		A14.2.3	Revisión técnica de las aplicaciones después de cambios en la plataforma de operación.	Control: Cuando se cambian las plataformas de operación, se deberían revisar las aplicaciones críticas del negocio, y someter a prueba para asegurar que no haya impacto adverso en las operaciones o seguridad de la organización.		X			SI	El control no se encuentra implementado	No existe evidencia de la implementación de este control

Tabla 32. (Continuación)

Dominio de Control	Objetivo de Control	Referencia del control	Título del control	Descripción del control	Controles seleccionados y de los fundamentos de la selección				Aplicado? (Si/No)	Estado actual del control	Justificación para la exclusión o documento de referencia
					Requerimiento Legal	Obligatorio	Requerimiento del negocio	Análisis de riesgos			
ADQUISICION, DESARROLLO Y MANTENIMIENTO DE LOS SISTEMAS	Seguridad en los procesos de desarrollo y soporte	A14.2.4	Restricciones en los cambios o los paquetes de software	Control: Se deberían desalentar las modificaciones a los paquetes de software, los cuales se deben limitar a los cambios necesarios, y todos los cambios se deberían controlar estrictamente.		X			SI	El control no se encuentra implementado	Se realizan actividades sobre pruebas de versiones específicamente en el sistema de información SYSMAN, sin embargo no existe documentación ni procedimientos internos al respecto.
		A14.2.5	Principios de construcción de los sistemas seguros	Control: Se deberían establecer, documentar y mantener principios para la construcción de sistemas seguros, y aplicarlos a cualquier actividad de implementación de sistemas de información.		X			SI	El control no se encuentra implementado	No se evidencia documentación sobre la aplicación de este control
		A14.2.6	Ambiente de desarrollo seguro	Control: Las organizaciones deberían establecer y proteger adecuadamente los ambientes de desarrollo seguros para las actividades de desarrollo e integración de sistemas que comprendan todo el ciclo de vida de desarrollo de sistemas.		X			SI	El control se encuentra parcialmente implementado	Se realizan actividades sobre sobre este control dentro del instituto, sin embargo se debe revisar la aplicación del control y la documentación respectiva.
		A14.2.7	Desarrollo contratado externamente	Control: La organización debería supervisar y hacer seguimiento de la actividad de desarrollo de sistemas contratados externamente.		X			SI	El control se encuentra implementado parcialmente	Se deben fortalecer las obligaciones contractuales, el seguimiento de compromisos, sin embargo este control se aplica parcialmente.
		A14.2.8	Pruebas de seguridad de sistemas	Control: Durante el desarrollo se deberían llevar a cabo pruebas de funcionalidad de la seguridad.		X			SI	El control no se encuentra implementado	No se encuentra documentación que evidencie la implementación de este control, por lo tanto debe revisarse y documentarse este control ya que si debe ser aplicado en el instituto.

Tabla 32. (Continuación)

Dominio de Control	Objetivo de Control	Referencia del control	Título del control	Descripción del control	Controles seleccionados y de los fundamentos de la selección				Aplicado? (Si/No)	Estado actual del control	Justificación para la exclusión o documento de referencia
					Requerimiento Legal	Obligatorio	Requerimiento del negocio	Análisis de riesgos			
ADQUISICION, DESARROLLO Y MANTENIMIENTO DE LOS SISTEMAS	Seguridad en los procesos de desarrollo y soporte	A14.2.9	Prueba de aceptación de sistemas	Control: Para los sistemas de información nuevos, actualizaciones y nuevas versiones, se debería establecer programas de prueba para aceptación y criterios de aceptación relacionados.		X			SI	El control se encuentra implementado parcialmente	En el formato SOLICITUD DESARROLLO Y/O ACTUALIZACIÓN DE SOFTWARE A-TIC-FT-010, se documenta las pruebas pilotos realizadas por los desarrolladores y los usuarios funcionales y se documentan las actividades en dicho formato, sin embargo hay que actualizar la implementación del control.
	Datos de prueba	A14.3.1	Protección de datos de prueba	Control: Los datos de prueba se deben seleccionar, proteger y controlar cuidadosamente.		X			SI	El control no se encuentra implementado	No se evidencia documentación sobre este control, por lo tanto se debe revisar y documentar estas actividades.
RELACIONES CON LOS PORVEEDORES	Seguridad de la información en las relaciones con los proveedores	A15.1.1	Política de seguridad de la información para las relaciones con proveedores	Control: Los requisitos de seguridad de la información para mitigar los riesgos asociados con el acceso de proveedores a los activos de la organización se deberían acordar con estos y se deberían documentar.	X	X			SI	El control no se encuentra implementado	No existe documentación respectiva sobre políticas de seguridad de la información con proveedores
		A15.1.2	Tratamiento de la seguridad dentro de los acuerdos con proveedores.	Control: Se deberían establecer y acordar todos los requisitos de seguridad de la información pertinentes con cada proveedor que pueda tener acceso, procesar, almacenar, comunicar o suministrar componentes de infraestructura de TI para la información de la organización.	X	X	X		SI	El control no se encuentra implementado parcialmente	Este control se encuentra implementado parcialmente en cuanto a que existen unas obligaciones contractuales pactadas y de acuerdo a la naturaleza de la contratación se fijan los aspectos que debe tener el personal técnico para proveer el servicio; también se manejan políticas de seguridad desde los accesos que se le asignan a los proveedores dependiendo del servicio que se realizará y la información requerida, sin embargo este control debe revisarse y fortalecerse.

Tabla 32. (Continuación)

Dominio de Control	Objetivo de Control	Referencia del control	Título del control	Descripción del control	Controles seleccionados y de los fundamentos de la selección				Aplicado? (Si/No)	Estado actual del control	Justificación para la exclusión o documento de referencia
					Requerimiento Legal	Obligatorio	Requerimiento del negocio	Análisis de riesgos			
RELACIONES CON LOS PORVEEDORES	Seguridad de la información en las relaciones con los proveedores	A15.1.3	Cadena de suministro de tecnología de información y comunicación	Control: Los acuerdos con proveedores deberían incluir requisitos para tratar los riesgos de seguridad de la información asociados con la cadena de suministro de productos y servicios de tecnología de información y comunicación.		X	X		SI	El control no se encuentra implementado	No existe evidencia de la implementación de este control.
	Gestión de la prestación de servicios de proveedores	A15.2.1	Seguimiento y revisión de los servicios de los proveedores	Control: Las organizaciones deberían hacer seguimiento, revisar y auditar con regularidad la prestación de servicios de los proveedores.		X	X		SI	El control esta implementado parcialmente	Los funcionarios del Área de Sistemas a través del monitoreo, obligaciones contractuales e informes hacen seguimiento de los aspectos de seguridad y niveles de desempeño del servicio que prestan los proveedores.
		A15.2.2	Gestión de cambios en los servicios de los proveedores	Control: Se deberían gestionar los cambios en el suministro de servicios por parte de los proveedores incluido el mantenimiento y mejora de las políticas, procedimientos y controles de seguridad de la información existentes, teniendo en cuenta la criticidad de la información, sistemas y procesos del negocio involucrados, y la valoración de los riesgos.		X	X		SI	El control no se encuentra implementado	No se realizan actividades para el cumplimiento de este control
GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACION	Gestión de incidentes y mejoras en la seguridad de la información.	A16.1.1	Responsabilidades y procedimientos	Control: Se deberían establecer las responsabilidades y procedimientos de gestión para asegurar una respuesta rápida, eficaz y ordenada a los incidentes de seguridad de la información.	X	X			SI	El control no se encuentra implementado	No hay procedimientos establecidos sobre el registro de incidentes y procedimientos para el manejo de evidencia forense, sin embargo se realizan actividades a través del grupo de control interno disciplinario.
		A16.1.2	Reporte de eventos de seguridad de la información	Control: Los eventos de seguridad de la información se deberían informar a través de los canales de gestión apropiados, tan pronto como sea posible.	X	X			SI	El control no se encuentra implementado	No existe procedimientos específicos y documentados sobre el manejo de reportes de seguridad de la información; el control debe revisarse y documentarse

Tabla 32. (Continuación)

Dominio de Control	Objetivo de Control	Referencia del control	Título del control	Descripción del control	Controles seleccionados y de los fundamentos de la selección				Aplicado? (Si/No)	Estado actual del control	Justificación para la exclusión o documento de referencia
					Requerimiento Legal	Obligatorio	Requerimiento del negocio	Análisis de riesgos			
GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACION	Gestión de incidentes y mejoras en la seguridad de la información.	A16.1.3	Reporte de debilidades de seguridad de seguridad de la información	Control: Se debería exigir a todos los empleados y contratistas que usan los servicios y sistemas de información de la organización, que observen y reporten cualquier debilidad de seguridad de la información observada o sospechada en los sistemas o servicios.	X	X	X		SI	El control no se encuentra implementado	No existen políticas ni procedimientos para que los empleados y contratistas reporten debilidades observadas que afectan la seguridad de la información.
		A16.1.4	Evaluación de eventos de seguridad de la información y decisiones sobre ellos	Control: Los eventos de seguridad de la información se deberían evaluar y se debería decidir si se van clasificar como incidentes de seguridad de la información.	X	X	X		SI	El control no se encuentra implementado	No hay actividades ni documentación sobre la implementación de este control
		A16.1.5	Respuesta a incidentes de seguridad de la información	Control: Se debería dar respuesta a los incidentes de seguridad de la información de acuerdo con procedimientos documentados.	X	X			SI	El control no se encuentra implementado	No existen procedimientos para dar respuestas a incidentes de seguridad.
		A16.1.6	Aprendizaje obtenido de los incidentes de seguridad de la información.	Control: El conocimiento adquirido al analizar y resolver incidentes de seguridad de la información se debería usar para reducir la posibilidad o impacto de incidentes futuros.		X			SI	El control no se encuentra implementado	Aunque se realizan actividades sobre las lecciones aprendidas de incidentes de seguridad de la información, no hay documentación donde se evidencie la implementación de dicho control.
		A16.1.7	Recolección de evidencia	Control: La organización debería definir y aplicar procedimientos para la identificación, recolección, adquisición y preservación de información que pueda servir como evidencia.		X			SI	El control no se encuentra implementado	No hay procedimiento establecido para identificar recolectar, adquirir y preservar la información que sirva como evidencia dentro de incidentes de seguridad.
ASPECTOS DE SEGURIDAD DE LA INFORMACION DE LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO	Continuidad de la seguridad de la información	A17.1.1	Planificación de la continuidad de la seguridad de la información	Control: La organización debería determinar sus requisitos para la seguridad de la información y la continuidad de la gestión de la seguridad de la información en situaciones adversas, por ejemplo, durante una crisis o desastre.		X	X		SI	El control no se encuentra implementado	No existe un plan de continuidad de seguridad de la información ni actividades asociadas

Tabla 32. (Continuación)

Dominio de Control	Objetivo de Control	Referencia del control	Título del control	Descripción del control	Controles seleccionados y de los fundamentos de la selección				Aplicado? (Si/No)	Estado actual del control	Justificación para la exclusión o documento de referencia
					Requerimiento Legal	Obligatorio	Requerimiento del negocio	Análisis de riesgos			
ASPECTOS DE SEGURIDAD DE LA INFORMACION DE LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO	Continuidad de la seguridad de la información	A17.1.2	Implementación de la continuidad de la seguridad de la información	Control: La organización debería establecer, documentar, implementar y mantener procesos, procedimientos y controles para asegurar el nivel de continuidad requerido para la seguridad de la información durante una situación adversa.		X	X		SI	El control no se encuentra implementado	No hay evidencias de implementación de continuidad de seguridad de la información, el control se debe revisar y documentar
		A17.1.3	Verificación, revisión y evaluación de la continuidad de la seguridad de la información	Control: La organización debería verificar a intervalos regulares los controles de continuidad de la seguridad de la información establecidos e implementados, con el fin de asegurar que son válidos y eficaces durante situaciones adversas.		X	X		SI	El control no se encuentra implementado	No hay evidencias de implementación de este control.
	Redundancias	A17.2.1	Disponibilidad de las instalaciones de procesamiento de información.	Control: Las instalaciones de procesamiento de información se deberían implementar con redundancia suficiente para cumplir los requisitos de disponibilidad.		X	X		SI	El control no se encuentra implementado	Se debe realizar la valoración de activos y costos asociados con el fin de definir el plan alterno, por tanto este control debe implementarse y documentarse.
CUMPLIMIENTO	Cumplimiento de los requisitos legales y contractuales	A18.1.1	Identificación de la legislación aplicable y de los requisitos contractuales	Control: Todos los requisitos estatutarios, reglamentarios y contractuales pertinentes y el enfoque de la organización para cumplirlos, se deberían identificar y documentar explícitamente y mantenerlos actualizados para cada sistema de información y para la organización.	X	X			SI	El control se encuentra implementado	Se encuentra definida la normatividad dentro del normograma de la entidad y el PETIC.

Tabla 32. (Continuación)

Dominio de Control	Objetivo de Control	Referencia del control	Título del control	Descripción del control	Controles seleccionados y de los fundamentos de la selección				Aplicado? (Si/No)	Estado actual del control	Justificación para la exclusión o documento de referencia
					Requerimiento Legal	Obligatorio	Requerimiento del negocio	Análisis de riesgos			
CUMPLIMIENTO	Cumplimiento de los requisitos legales y contractuales	A18.1.2	Derechos de propiedad intelectual (DPI)	Control: Se debería implementar procedimientos apropiados para asegurar el cumplimiento de los requisitos legislativos, de reglamentación y contractuales relacionados con los derechos de propiedad intelectual y el uso de productos de software patentados.	X	X			SI	El control se encuentra implementado	Existe la política aprobada en Manual de política de seguridad y controles básicos y específicos para el manejo de la información - Código A-TIC-MA-001 y están establecidas las actividades de utilización de software legal en la entidad.
		A18.1.3	Protección de registros	Control: Los registros se deberían proteger contra perdida, destrucción, falsificación, acceso no autorizado y liberación no autorizada, de acuerdo con los requisitos legislativos, de reglamentación, contractuales y de negocio.	X	X			SI	El control se encuentra parcialmente implementado	Este control se maneja a través de las mismas políticas y procedimientos de toma de copias de seguridad
		A18.1.4	Privacidad y protección de la información de datos personales	Control: Se deberían asegurar la privacidad y la protección de la información de datos personales, como se exige e la legislación y la reglamentación pertinentes, cuando sea aplicable.	X	X			SI	El control no se encuentra implementado	Se realizan actividades dentro de la seguridad específica de los sistemas de información, sin embargo no existe una política aprobada para el manejo de este control.
		A18.1.5	Reglamentación de controles criptográficos	Control: Se deberían usar controles criptográficos, en cumplimiento de todos los acuerdos, legislación y reglamentación pertinentes.	X				SI	El control no se encuentra implementado	No existe manejo de controles criptográficos en la entidad.
	Revisiones de seguridad de la información	A18.2.1	Revisión independiente de la seguridad de la información	Control: El enfoque de la organización para la gestión de la seguridad de la información y su implementación (es decir los objetivos de control, los controles, las políticas, los procesos y los procedimientos para seguridad de la información), se deberían revisar independientemente a intervalos planificados o cuando ocurran cambios significativos.	X	X	X		SI	El control se encuentra implementado	La oficina de control interno realiza las actividades de control sobre el proceso de Gestión Tecnológica y de la información

Tabla 32. (Continuación)

Dominio de Control	Objetivo de Control	Referencia del control	Título del control	Descripción del control	Controles seleccionados y de los fundamentos de la selección				Aplicado? (Si/No)	Estado actual del control	Justificación para la exclusión o documento de referencia
					Requerimiento Legal	Obligatorio	Requerimiento del negocio	Análisis de riesgos			
CUMPLIMIENTO	Revisiones de seguridad de la información	A18.2.2	Cumplimiento de las políticas y normas de seguridad	Control: Los Gerentes deberían revisar con regularidad el cumplimiento del procesamiento y procedimientos de información dentro de su área de responsabilidad, con las políticas y normas de seguridad apropiadas, y cualquier otro requisito de seguridad.	X	X	X		SI	El control se encuentra implementado parcialmente	La entidad periódicamente revisa la política de seguridad aprobada, sin embargo aún no existe un compromiso y seguimiento formal por cada uno de los responsables de las áreas y dependencias.
		A18.2.3	Revisión del cumplimiento técnico	Control: Los sistemas de información se deben revisar periódicamente para determinar el cumplimiento con las políticas y normas de seguridad de la información.	X	X	X		SI	El control no se encuentra implementado	No se realizan actividades de monitoreo periódico de los sistemas de información en cuanto a pruebas pertinentes de seguridad como son las pruebas de penetración.

Fuente: el autor

10. PLAN DE TRATAMIENTO DE RIESGOS

El Plan de tratamiento de riesgos se realiza a los activos que tuvieron como resultado en el Riesgo Potencial unos niveles medios, altos y muy altos.

Los criterios para realizar el Plan de tratamiento de riesgos se realiza teniendo en cuenta la directriz y los recursos de la Entidad con respecto a la administración y gestión de los activos de información y al lineamiento de la Entidad para tercerizar los servicios de TI.

10.1 Plan Tratamiento de Riesgos: [IS] SERVICIOS

Tabla 36. Plan de Tratamiento de Riesgos: servicios

ACTIVOS	RIESGO	AMENAZAS	VALOR	TRATAMIENTO DE RIESGO	CONTROLES IMPLEMENTADOS	PROYECTOS DEFINIDOS
Controlador de dominio UPI La 27 sur	Pérdida de Disponibilidad del activo de información	[A.7] uso no previsto	Muy Alto	Se mitiga el riesgo con la implementación de los controles 5.1.1 – 5.1.2 – 6.1.1 -6.1.2 – 6.1.3 – 6.1.4 – 6.1.5 – 8.1.1 - 8.1.2 – 8.1.3 – 8.1.4 – 9.1.1 -9.1.2 – 10.1.2 - 16.1.1 – 16.1.2 – 16.1.3 – 16.1.4 – 16.1.5 – 16.1.6 – 16.1.7	Manual de política de seguridad y controles básicos y específicos para el manejo de la información. Planificación de la continuidad de la seguridad de la información.	**Proyecto 6-** Seguimiento y cumplimiento de la Política y Seguridad de la Información de la Entidad. Ver numeral 11.1 **Proyecto 7-** Gestión de incidentes de Seguridad de la Información. Ver numeral 11.1
		[E.2] Errores del administrador del sistema / de la seguridad	Alto	Se mitiga el riesgo con la implementación de los controles 5.1.1 – 5.1.2 – 6.1.1 -6.1.2 – 6.1.3 – 6.1.4 – 6.1.5 – 8.1.1 - 8.1.2 – 8.1.3 – 8.1.4 – 9.1.1 -9.1.2 – 9.2.1 - 9.2.2 - 9.2.3 - 9.2.4 - 9.2.5 - 9.2.6 - 9.3.1 - 9.4.1 - 9.4.2 - 9.4.3 -9.4.4 - 9.4.5 10.1.2 - 12.1.1 - 12.1.2 - 12.1.3 - 12.1.4 - 12.2.1 - 12.3.1 -12.4.1 - 12.4.2 - 12.4.3 - 12.4.4 - 12.5.1 - 12.6.1 - 12.6.2 - 12.7.1- 16.1.1 – 16.1.2 – 16.1.3 – 16.1.4 – 16.1.5 – 16.1.6 – 16.1.7	Manual de política de seguridad y controles básicos y específicos para el manejo de la información.	**Proyecto 2-** Responsabilidades y proyectos de operación. Ver numeral 11.1.
					Registro y gestión de eventos de seguridad.	**Proyecto 3-** Implementación y seguimiento de registros de actividad. Ver numeral 11.1
					Copias de seguridad de la información.	**Proyecto 4–** Control de acceso y responsabilidades de los usuarios a los sistemas y aplicaciones. Ver numeral 11.1

Tabla 33. (Continuación)

ACTIVOS	RIESGO	AMENAZAS	VALOR	TRATAMIENTO DE RIESGO	CONTROLES IMPLEMENTADOS	PROYECTOS DEFINIDOS
Controlador de dominio UPI La 27 sur	Pérdida de Disponibilidad del activo de información	E.18] Destrucción de la información	Alto	Se mitiga el riesgo con la implementación de los controles 5.1.1 – 5.1.2 – 6.1.1 -6.1.2 – 6.1.3 – 6.1.4 – 6.1.5 – 8.1.1 - 8.1.2 – 8.1.3 – 8.1.4 – 9.1.1 -9.1.2 – 9.2.1 - 9.2.2 - 9.2.3 - 9.2.4 - 9.2.5 - 9.2.6 - 9.3.1 - 9.4.1 - 9.4.2 - 9.4.3 -9.4.4 - 9.4.5 10.1.2 - 12.1.1 - 12.1.2 - 12.1.3 - 12.1.4 - 12.2.1 - 12.3.1 -12.4.1 - 12.4.2 - 12.4.3 - 12.4.4 - 12.5.1 - 12.6.1 - 12.6.2 - 12.7.1- 16.1.1 – 16.1.2 – 16.1.3 – 16.1.4 – 16.1.5 – 16.1.6 – 16.1.7	Copias de seguridad de la información.	**Proyecto 6–** Seguimiento y cumplimiento de la política de Seguridad de la información de la entidad. Ver numeral 11.1
		[E.24] caída del sistema por agotamiento de recursos				**Proyecto 7-** Gestión de incidentes de Seguridad de la información. Ver numeral 11.1
		[E.19] Fugas de información	Medio	Se mitiga el riesgo con la implementación de los controles 5.1.1 – 5.1.2 – 6.1.1 -6.1.2 – 6.1.3 – 6.1.4 – 6.1.5 – 8.1.1 - 8.1.2 – 8.1.3 – 8.1.4 – 9.1.1 -9.1.2 – 10.1.2 -11.1.1 - 11.1.2 - 11.1.3 - 11.1.4. -11.1.5 - 11.1.6 - 11.2.2 11.2.3	Manual de política de seguridad y controles básicos y específicos para el manejo de la información. Gestión de derechos de acceso con privilegios especiales.	**Proyecto 1-** Control de acceso físico y protección de la información (Áreas seguras y seguridad de equipos).Ver numeral 11.1. **Proyecto 6–** Seguimiento y cumplimiento de la política de Seguridad de la información de la entidad. Ver numeral 11.1
	Pérdida de la Integridad de la información, lo que implica el acceso indebido o fraudulento al activo de información	[E.19] Fugas de información [A.15] Modificación de la información	Muy Alto	Se mitiga el riesgo con la implementación de los controles 5.1.1 – 5.1.2 – 6.1.1 -6.1.2 – 6.1.3 – 6.1.4 – 6.1.5 – 8.1.1 - 8.1.2 – 8.1.3 – 8.1.4 – 9.1.1 -9.1.2 – 10.1.2 -11.1.1 - 11.1.2 - 11.1.3 - 11.1.4. -11.1.5 - 11.1.6 - 11.2.2 11.2.3	Manual de política de seguridad y controles básicos y específicos para el manejo de la información. Gestión de derechos de acceso con privilegios especiales. Gestión de derechos de acceso con privilegios especiales.	**Proyecto 1**- Control de acceso físico y protección de la información (Áreas seguras y seguridad de equipos).Ver numeral 11.1. **Proyecto 6–** Seguimiento y cumplimiento de la política de Seguridad de la información de la entidad. Ver numeral 11.1
		[A.5] suplantación de la identidad del usuario	Medio	Se mitiga el riesgo con la implementación de los controles 9.1.1 - 9.1.2 - 9.2.4 - 9.2.5 -11.1.1 - 11.1.2 - 11.1.3 - 11.1.4. -11.1.5 - 11.1.6 - 11.2.2 11.2.3	Política de control de acceso. Política de derechos de acceso asignados a usuarios.	**Proyecto 3-** Implementación y seguimiento de registros de actividad. Ver numeral 11.1 **Proyecto 4–** Control de acceso y responsabilidades de los usuarios a los sistemas y aplicaciones. Ver numeral 11.1
		[E.2] Errores del administrador del sistema / de la seguridad [E.15] Alteración de la información [E.18] Destrucción de la información [A.6] Abuso de privilegios de acceso [A.7] uso no previsto [A.11] Acceso no autorizado	Alto	Se mitiga el riesgo con la implementación de los controles 9.1.1 -9.1.2 – 9.2.1 - 9.2.2 - 9.2.3 - 9.2.4 - 9.2.5 - 9.2.6 - 9.3.1 - 9.4.1 - 9.4.2 - 9.4.3 -9.4.4 - 9.4.5	Gestión de acceso a usuarios.	**Proyecto 4–** Control de acceso y responsabilidades de los usuarios a los sistemas y aplicaciones. Ver numeral 11.1

Tabla 33. (Continuación)

ACTIVOS	RIESGO	AMENAZAS	VALOR	TRATAMIENTO DE RIESGO	CONTROLES IMPLEMENTADOS	PROYECTOS DEFINIDOS
Controlador de dominio UPI La 27 sur	Pérdida de la Confidencialidad, acceso no autorizado que permite la utilización indebida o no autorizada del activo de información	[E.19] Fugas de información	Muy Alto	Se mitiga el riesgo con la implementación de los controles 5.1.1 – 5.1.2 – 6.1.1 -6.1.2 – 6.1.3 – 6.1.4 – 6.1.5 – 8.1.1 - 8.1.2 – 8.1.3 – 8.1.4 – 9.1.1 -9.1.2 – 10.1.2 -11.1.1 - 11.1.2 - 11.1.3 - 11.1.4. -11.1.5 - 11.1.6 - 11.2.2 11.2.3	Manual de política de seguridad y controles básicos y específicos para el manejo de la información. Política de control de acceso.	**Proyecto 1**- Control de acceso físico y protección de la información (Áreas seguras y seguridad de equipos).Ver numeral 11.1. **Proyecto 6–** Seguimiento y cumplimiento de la política de Seguridad de la información de la entidad. Ver numeral 11.1
		[E.2] Errores del administrador del sistema / de la seguridad [E.15] Alteración de la información [E.18] Destrucción de la información [A.6] Abuso de privilegios de acceso [A.7] uso no previsto [A.11] Acceso no autorizado [A.19] revelación de información	Alto	Se mitiga el riesgo con la implementación de los controles 5.1.1 – 5.1.2 – 6.1.1 -6.1.2 9.1.1 -9.1.2 – -11.1.1 - 11.1.2	Conjunto de políticas para la seguridad de la información. Política de control de acceso.	**Proyecto 1**- Control de acceso físico y protección de la información (Áreas seguras y seguridad de equipos).Ver numeral 11.1. **Proyecto 6–** Seguimiento y cumplimiento de la política de Seguridad de la información de la entidad. Ver numeral 11.1
		[A.5] suplantación de la identidad del usuario	Medio	Se mitiga el riesgo con la implementación de los controles 9.1.1 - 9.1.2 - 9.2.4 - 9.2.5 -11.1.1 - 11.1.2 - 11.1.3 - 11.1.4. -11.1.5 - 11.1.6 - 11.2.2 11.2.3	Proceso disciplinario. Política de control de acceso a las redes y servicios asociados.	**Proyecto 3-** Implementación y seguimiento de registros de actividad. Ver numeral 11.1 Proyecto 4– Control de acceso y responsabilidades de los usuarios a los sistemas y aplicaciones. Ver numeral 11.1
	Pérdida de Autenticidad, en el comportamiento, resultado o uso del activo de información	[A.5] suplantación de la identidad del usuario	Alto	Se mitiga el riesgo con la implementación de los controles 9.1.1 - 9.1.2 - 9.2.4 - 9.2.5 -11.1.1 - 11.1.2 - 11.1.3 - 11.1.4. -11.1.5 - 11.1.6 - 11.2.2 11.2.3	Política de control de acceso. Política de derechos de acceso asignados a usuarios.	**Proyecto 3-** Implementación y seguimiento de registros de actividad. Ver numeral 11.1 **Proyecto 4–** Control de acceso y responsabilidades de los usuarios a los sistemas y aplicaciones. Ver numeral 11.1

Tabla 33. (Continuación)

ACTIVOS	RIESGO	AMENAZAS	VALOR	TRATAMIENTO DE RIESGO	CONTROLES IMPLEMENTADOS	PROYECTOS DEFINIDOS
Controlador de dominio misional	Pérdida de Disponibilidad del activo de información	[A.7] uso no previsto	Muy Alto	Se mitiga el riesgo con la implementación de loc controles 5.1.1 – 5.1.2 – 6.1.1 -6.1.2 – 6.1.3 – 6.1.4 – 6.1.5 – 8.1.1 - 8.1.2 – 8.1.3 – 8.1.4 – 9.1.1 -9.1.2 – 10.1.2 - 16.1.1 – 16.1.2 – 16.1.3 – 16.1.4 – 16.1.5 – 16.1.6 – 16.1.7	Manual de política de seguridad y controles básicos y específicos para el manejo de la información. Planificación de la continuidad de la seguridad de la información.	**Proyecto 6-** Seguimiento y cumplimiento de la Política y Seguridad de la Información de la Entidad. Ver numeral 11.1 **Proyecto 7-** Gestión de incidentes de Seguridad de la Información. Ver numeral 11.1
		[E.2] Errores del administrador del sistema / de la seguridad E.18] Destrucción de la información [E.24] caída del sistema por agotamiento de recursos	Alto	Se mitiga el riesgo con la implementación de los controles 5.1.1 – 5.1.2 – 6.1.1 -6.1.2 – 6.1.3 – 6.1.4 – 6.1.5 – 8.1.1 - 8.1.2 – 8.1.3 – 8.1.4 – 9.1.1 -9.1.2 – 9.2.1 - 9.2.2 - 9.2.3 - 9.2.4 - 9.2.5 - 9.2.6 - 9.3.1 - 9.4.1 - 9.4.2 - 9.4.3 -9.4.4 - 9.4.5 10.1.2 - 12.1.1 - 12.1.2 - 12.1.3 - 12.1.4 - 12.2.1 - 12.3.1 -12.4.1 - 12.4.2 - 12.4.3 - 12.4.4 - 12.5.1 - 12.6.1 - 12.6.2 - 12.7.1- 16.1.1 – 16.1.2 – 16.1.3 – 16.1.4 – 16.1.5 – 16.1.6 – 16.1.7	Gestión de derechos de acceso asignados a usuarios. Restricción de acceso a la información. Cadena de suministro de tecnologías de la información y comunicaciones. Copias de seguridad de la información.	**Proyecto 2-** Responsabilidades y proyectos de operación. Ver numeral 11.1. **Proyecto 3-** Implementación y seguimiento de registros de actividad. Ver numeral 11.1 **Proyecto 4–** Control de acceso y responsabilidades de los usuarios a los sistemas y aplicaciones. Ver numeral 11.1 **Proyecto 6–** Seguimiento y cumplimiento de la política de Seguridad de la información de la entidad. Ver numeral 11.1 **Proyecto 7-** Gestión de incidentes de Seguridad de la información. Ver numeral 11.1
		[E.19] Fugas de información	Medio	Se mitiga el riesgo1 con la implementación de los controles 5.1.1 – 5.1.2 – 6.1.1 -6.1.2 – 6.1.3 – 6.1.4 – 6.1.5 – 8.1.1 - 8.1.2 – 8.1.3 – 8.1.4 – 9.1.1 -9.1.2 – 10.1.2 -11.1.1 - 11.1.2 - 11.1.3 - 11.1.4. -11.1.5 - 11.1.6 - 11.2.2 11.2.3	Manual de política de seguridad y controles básicos y específicos para el manejo de la información. Gestión de derechos de acceso con privilegios especiales.	**Proyecto 1-** Control de acceso físico y protección de la información (Áreas seguras y seguridad de equipos).Ver numeral 11.1. **Proyecto 6–** Seguimiento y cumplimiento de la política de Seguridad de la información de la Entidad. Ver numeral 11.1
	Pérdida de la Integridad de la información, lo que implica el acceso indebido o fraudulento al activo de información	[E.19] Fugas de información [A.15] Modificación de la información	Muy Alto	Se mitiga el riesgo con la implementación de los controles 5.1.1 – 5.1.2 – 6.1.1 -6.1.2 – 6.1.3 – 6.1.4 – 6.1.5 – 8.1.1 - 8.1.2 – 8.1.3 – 8.1.4 – 9.1.1 -9.1.2 – 10.1.2 -11.1.1 - 11.1.2 - 11.1.3 - 11.1.4. -11.1.5 - 11.1.6 - 11.2.2 11.2.3	Manual de política de seguridad y controles básicos y específicos para el manejo de la información. Gestión de derechos de acceso con privilegios especiales. Gestión de derechos de acceso con privilegios especiales.	**Proyecto 1-** Control de acceso físico y protección de la información (Áreas seguras y seguridad de equipos).Ver numeral 11.1. **Proyecto 6–** Seguimiento y cumplimiento de la política de Seguridad de la información de la entidad. Ver numeral 11.1

Tabla 33. (Continuación)

ACTIVOS	RIESGO	AMENAZAS	VALOR	TRATAMIENTO DE RIESGO	CONTROLES IMPLEMENTADOS	PROYECTOS DEFINIDOS
Controlador de dominio misional	Pérdida de la Integridad de la información, lo que implica el acceso indebido o fraudulento al activo de información	[A.5] suplantación de la identidad del usuario	Medio	Se mitiga el riesgo con la implementación de los controles 9.1.1 - 9.1.2 - 9.2.4 - 9.2.5 -11.1.1 - 11.1.2 - 11.1.3 - 11.1.4. -11.1.5 - 11.1.6 - 11.2.2 11.2.3	Política de control de acceso. Política de derechos de acceso asignados a usuarios.	**Proyecto 3-** Implementación y seguimiento de registros de actividad. Ver numeral 11.1 **Proyecto 4–** Control de acceso y responsabilidades de los usuarios a los sistemas y aplicaciones. Ver numeral 11.1
		[E.2] Errores del administrador del sistema / de la seguridad [E.15] Alteración de la información [E.18] Destrucción de la información [A.6] Abuso de privilegios de acceso [A.7] uso no previsto [A.11] Acceso no autorizado	Alto	Se mitiga el riesgo con la implementación de los controles 9.1.1 -9.1.2 – 9.2.1 - 9.2.2 - 9.2.3 - 9.2.4 - 9.2.5 - 9.2.6 - 9.3.1 - 9.4.1 - 9.4.2 - 9.4.3 -9.4.4 - 9.4.5	Control de acceso a las redes y servicios asociados.	**Proyecto 4–** Control de acceso y responsabilidades de los usuarios a los sistemas y aplicaciones. Ver numeral 11.1
	Pérdida de la Confidencialidad, acceso no autorizado que permite la utilización indebida o no autorizada del activo de información	[E.19] Fugas de información	Muy Alto	Se mitiga el riesgo con la implementación de los controles 5.1.1 – 5.1.2 – 6.1.1 -6.1.2 – 6.1.3 – 6.1.4 – 6.1.5 – 8.1.1 - 8.1.2 – 8.1.3 – 8.1.4 – 9.1.1 -9.1.2 – 10.1.2 -11.1.1 - 11.1.2 - 11.1.3 - 11.1.4. -11.1.5 - 11.1.6 - 11.2.2 11.2.3	Manual de política de seguridad y controles básicos y específicos para el manejo de la información. Gestión de derechos de acceso con privilegios especiales.	**Proyecto 1**- Control de acceso físico y protección de la información (Áreas seguras y seguridad de equipos).Ver numeral 11.1. **Proyecto 6–** Seguimiento y cumplimiento de la política de Seguridad de la información de la Entidad. Ver numeral 11.1
		[E.2] Errores del administrador del sistema / de la seguridad [E.15] Alteración de la información	Alto	Se mitiga el riesgo con la implementación de los controles 5.1.1 – 5.1.2 – 6.1.1 -6.1.2 9.1.1 -9.1.2 – -11.1.1 - 11.1.2	Conjunto de políticas para la seguridad de la información. Política de control de acceso.	**Proyecto 1**- Control de acceso físico y protección de la información (Áreas seguras y seguridad de equipos).Ver numeral 11.1. **Proyecto 6–** Seguimiento y cumplimiento de la política de Seguridad de la información de la Entidad. Ver numeral 11.1

Tabla 33. (Continuación)

ACTIVOS	RIESGO	AMENAZAS	VALOR	TRATAMIENTO DE RIESGO	CONTROLES IMPLEMENTADOS	PROYECTOS DEFINIDOS
Controlador de dominio misional	Pérdida de la Confidencialidad, acceso no autorizado que permite la utilización indebida o no autorizada del activo de información	[E.18] Destrucción de la información [A.6] Abuso de privilegios de acceso [A.7] uso no previsto [A.11] Acceso no autorizado [A.19] revelación de información	Alto	Se mitiga el riesgo con la implementación de los controles 5.1.1 – 5.1.2 – 6.1.1 -6.1.2 9.1.1 -9.1.2 – -11.1.1 - 11.1.2	Conjunto de políticas para la seguridad de la información. Política de control de acceso.	**Proyecto 1**- Control de acceso físico y protección de la información (Áreas seguras y seguridad de equipos).Ver numeral 11.1. **Proyecto 6–** Seguimiento y cumplimiento de la política de Seguridad de la información de la Entidad. Ver numeral 11.1
		[A.5] suplantación de la identidad del usuario	Medio	Se mitiga el riesgo con la implementación de los controles 9.1.1 - 9.1.2 - 9.2.4 - 9.2.5 -11.1.1 - 11.1.2 - 11.1.3 - 11.1.4. -11.1.5 - 11.1.6 - 11.2.2 11.2.3	Política de control de acceso. Política de derechos de acceso asignados a usuarios.	**Proyecto 3-** Implementación y seguimiento de registros de actividad. Ver numeral 11.1 **Proyecto 4–** Control de acceso y responsabilidades de los usuarios a los sistemas y aplicaciones. Ver numeral 11.1
	Pérdida de Autenticidad, en el comportamiento, resultado o uso del activo de información	[A.5] suplantación de la identidad del usuario	Alto	Se mitiga el riesgo con la implementación de los controles 9.1.1 - 9.1.2 - 9.2.4 - 9.2.5 -11.1.1 - 11.1.2 - 11.1.3 - 11.1.4. -11.1.5 - 11.1.6 - 11.2.2 11.2.3	Política de control de acceso. Política de derechos de acceso asignados a usuarios.	**Proyecto 3-** Implementación y seguimiento de registros de actividad. Ver numeral 11.1 **Proyecto 4–** Control de acceso y responsabilidades de los usuarios a los sistemas y aplicaciones. Ver numeral 11.1
Controlador de dominio principal	Pérdida de Disponibilidad del activo de información	[A.7] uso no previsto	Muy Alto	Se mitiga el riesgo con la implementación de los controles 5.1.1 – 5.1.2 – 6.1.1 -6.1.2 – 6.1.3 – 6.1.4 – 6.1.5 – 8.1.1 - 8.1.2 – 8.1.3 – 8.1.4 – 9.1.1 -9.1.2 – 10.1.2 - 16.1.1 – 16.1.2 – 16.1.3 – 16.1.4 – 16.1.5 – 16.1.6 – 16.1.7	Manual de política de seguridad y controles básicos y específicos para el manejo de la información. Planificación de la continuidad de la seguridad de la información.	**Proyecto 6-** Seguimiento y cumplimiento de la Política y Seguridad de la Información de la Entidad. Ver numeral 11.1 **Proyecto 7-** Gestión de incidentes de Seguridad de la Información. Ver numeral 11.1
		[E.2] Errores del administrador del sistema / de la seguridad E.18] Destrucción de la información	Alto	Se mitiga el riesgo con la implementación de los controles 5.1.1 – 5.1.2 – 6.1.1 -6.1.2 – 6.1.3 – 6.1.4 – 6.1.5 – 8.1.1 - 8.1.2 – 8.1.3 – 8.1.4 – 9.1.1 -9.1.2 – 9.2.1 - 9.2.2 - 9.2.3 - 9.2.4 - 9.2.5 - 9.2.6 - 9.3.1 - 9.4.1 - 9.4.2 - 9.4.3 -9.4.4 - 9.4.5 10.1.2 - 12.1.1 - 12.1.2 - 12.1.3 - 12.1.4 - 12.2.1 - 12.3.1 -12.4.1 - 12.4.2 - 12.4.3 - 12.4.4 - 12.5.1 - 12.6.1 - 12.6.2 - 12.7.1- 16.1.1 – 16.1.2 – 16.1.3 – 16.1.4 – 16.1.5 – 16.1.6 – 16.1.7	Política de control de acceso. Copias de seguridad de la información. Manual de política de seguridad y controles básicos y específicos para el manejo de la información. Planificación de la continuidad de la seguridad de la información.	**Proyecto 2-** Responsabilidades y proyectos de operación. Ver numeral 11.1. **Proyecto 3-** Implementación y seguimiento de registros de actividad. Ver numeral 11.1 **Proyecto 4–** Control de acceso y responsabilidades de los usuarios a los sistemas y aplicaciones. Ver numeral 11.1 **Proyecto 6–** Seguimiento y cumplimiento de la política de Seguridad de la información de la Entidad. Ver numeral 11.1

Tabla 33. (Continuación)

ACTIVOS	RIESGO	AMENAZAS	VALOR	TRATAMIENTO DE RIESGO	CONTROLES IMPLEMENTADOS	PROYECTOS DEFINIDOS
Controlador de dominio principal	Pérdida de Disponibilidad del activo de información	[E.24] caída del sistema por agotamiento de recursos	Alto	Se mitiga el riesgo con la implementación de los controles 5.1.1 – 5.1.2 – 6.1.1 -6.1.2 – 6.1.3 – 6.1.4 – 6.1.5 – 8.1.1 - 8.1.2 – 8.1.3 – 8.1.4 – 9.1.1 -9.1.2 – 9.2.1 - 9.2.2 - 9.2.3 - 9.2.4 - 9.2.5 - 9.2.6 - 9.3.1 - 9.4.1 - 9.4.2 - 9.4.3 -9.4.4 - 9.4.5 10.1.2 - 12.1.1 - 12.1.2	Política de control de acceso. Copias de seguridad de la información. Manual de política de seguridad y controles básicos y específicos para el manejo de la información. Planificación de la continuidad de la seguridad de la información.	**Proyecto 6–** Seguimiento y cumplimiento de la política de Seguridad de la información de la Entidad. Ver numeral 11.1 7- Gestión de incidentes de Seguridad de la información. Ver numeral 11.1
		[A.18] Destrucción de la información				
		[E.19] Fugas de información	Medio	Se mitiga el riesgo con la implementación de los controles 5.1.1 – 5.1.2 – 6.1.1 -6.1.2 – 6.1.3 – 6.1.4 – 6.1.5 – 8.1.1 - 8.1.2 – 8.1.3 – 8.1.4 – 9.1.1 -9.1.2 – 10.1.2 -11.1.1 - 11.1.2 - 11.1.3 - 11.1.4. -11.1.5 - 11.1.6 - 11.2.2 11.2.3	Manual de política de seguridad y controles básicos y específicos para el manejo de la información. Gestión de derechos de acceso con privilegios especiales.	**Proyecto 1-** Control de acceso físico y protección de la información (Áreas seguras y seguridad de equipos).Ver numeral 11.1. **Proyecto 6–** Seguimiento y cumplimiento de la política de Seguridad de la información de la Entidad. Ver numeral 11.1
	Pérdida de la Integridad de la información, lo que implica el acceso indebido o fraudulento al activo de información	[E.19] Fugas de información	Muy Alto	Se mitiga el riesgo con la implementación de los controles 5.1.1 – 5.1.2 – 6.1.1 -6.1.2 – 6.1.3 – 6.1.4 – 6.1.5 – 8.1.1 - 8.1.2 – 8.1.3 – 8.1.4 – 9.1.1 -9.1.2 – 10.1.2 -11.1.1 - 11.1.2 - 11.1.3 - 11.1.4. -11.1.5 - 11.1.6 - 11.2.2 11.2.3	Manual de política de seguridad y controles básicos y específicos para el manejo de la información. Política de control de acceso.	**Proyecto 1-** Control de acceso físico y protección de la información (Áreas seguras y seguridad de equipos).Ver numeral 11.1. **Proyecto 6–** Seguimiento y cumplimiento de la política de Seguridad de la información de la Entidad. Ver numeral 11.1
		[A.15] Modificación de la información			Gestión de contraseñas.	
		[A.5] suplantación de la identidad del usuario	Medio	Se mitiga el riesgo con la implementación de los controles 9.1.1 - 9.1.2 - 9.2.4 - 9.2.5 -11.1.1 - 11.1.2 - 11.1.3 - 11.1.4. -11.1.5 - 11.1.6 - 11.2.2 11.2.3	Proceso disciplinario. Política de control de acceso a las redes y servicios asociados.	**Proyecto 3-** Implementación y seguimiento de registros de actividad. Ver numeral 11.1 **Proyecto 4–** Control de acceso y responsabilidades de los usuarios a los sistemas y aplicaciones. Ver numeral 11.1
		[E.2] Errores del administrador del sistema / de la seguridad	Alto	Se mitiga el riesgo con la implementación de los controles 9.1.1 -9.1.2 – 9.2.1 - 9.2.2 - 9.2.3 - 9.2.4 - 9.2.5 - 9.2.6 - 9.3.1 - 9.4.1 - 9.4.2 - 9.4.3 -9.4.4 - 9.4.5	Gestión de acceso a usuarios. Gestión de derechos de acceso asignados a usuarios. Gestión de contraseñas de usuarios.	**Proyecto 4–** Control de acceso y responsabilidades de los usuarios a los sistemas y aplicaciones. Ver numeral 11.1
		[E.15] Alteración de la información				
		[E.18] Destrucción de la información				
		[A.6] Abuso de privilegios de acceso				

Tabla 33. (Continuación)

ACTIVOS	RIESGO	AMENAZAS	VALOR	TRATAMIENTO DE RIESGO	CONTROLES IMPLEMENTADOS	PROYECTOS DEFINIDOS
Controlador de dominio principal		[A.7] uso no previsto				
		[A.11] Acceso no autorizado				
	Pérdida de la Confidencialidad, acceso no autorizado que permite la utilización indebida o no autorizada del activo de información	[E.19] Fugas de información	Muy Alto	Se mitiga el riesgo con la implementación de los controles 5.1.1 – 5.1.2 – 6.1.1 -6.1.2 – 6.1.3 – 6.1.4 – 6.1.5 – 8.1.1 - 8.1.2 – 8.1.3 – 8.1.4 – 9.1.1 -9.1.2 – 10.1.2 -11.1.1 - 11.1.2 - 11.1.3 - 11.1.4. -11.1.5 - 11.1.6 - 11.2.2 11.2.3	Manual de política de seguridad y controles básicos y específicos para el manejo de la información. Gestión de derechos de acceso con privilegios especiales.	**Proyecto 1**- Control de acceso físico y protección de la información (Áreas seguras y seguridad de equipos).Ver numeral 11.1. **Proyecto 6–** Seguimiento y cumplimiento de la política de Seguridad de la información de la Entidad. Ver numeral 11.1
		[E.2] Errores del administrador del sistema / de la seguridad	Alto	Se mitiga el riesgo con la implementación de los controles 5.1.1 – 5.1.2 – 6.1.1 -6.1.2 9.1.1 -9.1.2 – - 11.1.1 - 11.1.2	Conjunto de políticas para la seguridad de la información. Política de control de acceso. Gestión de contraseñas de usuarios.	**Proyecto 1**- Control de acceso físico y protección de la información (Áreas seguras y seguridad de equipos).Ver numeral 11.1. **Proyecto 6–** Seguimiento y cumplimiento de la política de Seguridad de la información de la Entidad. Ver numeral 11.1
		[E.15] Alteración de la información				
		[E.18] Destrucción de la información				
		[A.6] Abuso de privilegios de acceso				
		[A.7] uso no previsto				
		[A.11] Acceso no autorizado				
		[A.19] revelación de información				
		[A.5] suplantación de la identidad del usuario	Medio	Se mitiga el riesgo con la implementación de los controles 9.1.1 - 9.1.2 - 9.2.4 - 9.2.5 -11.1.1 - 11.1.2 - 11.1.3 - 11.1.4. -11.1.5 - 11.1.6 - 11.2.2 11.2.3	Proceso disciplinario. Política de control de acceso a las redes y servicios asociados.	**Proyecto 3-** Implementación y seguimiento de registros de actividad. Ver numeral 11.1 **Proyecto 4–** Control de acceso y responsabilidades de los usuarios a los sistemas y aplicaciones. Ver numeral 11.1

Tabla 33. (Continuación)

ACTIVOS	RIESGO	AMENAZAS	VALOR	TRATAMIENTO DE RIESGO	CONTROLES IMPLEMENTADOS	PROYECTOS DEFINIDOS
Controlador de dominio principal	Pérdida de Autenticidad, en el comportamiento, resultado o uso del activo de información	[A.5] suplantación de la identidad del usuario	Alto	Se mitiga el riesgo con la implementación de los controles 9.1.1 - 9.1.2 - 9.2.4 - 9.2.5 -11.1.1 - 11.1.2 - 11.1.3 - 11.1.4. -11.1.5 - 11.1.6 - 11.2.2 11.2.3	Proceso disciplinario. Política de control de acceso a las redes y servicios asociados.	**Proyecto 3-** Implementación y seguimiento de registros de actividad. Ver numeral 11.1 **Proyecto 4–** Control de acceso y responsabilidades de los usuarios a los sistemas y aplicaciones. Ver numeral 11.1
Controlador de dominio Misión Bogotá	Pérdida de Disponibilidad del activo de información	[A.7] uso no previsto	Muy Alto	Se mitiga el riesgo con la implementación de los controles 5.1.1 – 5.1.2 – 6.1.1 -6.1.2 – 6.1.3 – 6.1.4 – 6.1.5 – 8.1.1 - 8.1.2 – 8.1.3 – 8.1.4 – 9.1.1 -9.1.2 – 10.1.2 - 16.1.1 – 16.1.2 – 16.1.3 – 16.1.4 – 16.1.5 – 16.1.6 – 16.1.7	Conjunto de políticas para la seguridad de la información. Planificación de la continuidad de la seguridad de la información.	**Proyecto 6-** Seguimiento y cumplimiento de la Política y Seguridad de la Información de la Entidad. Ver numeral 11.1 **Proyecto 7-** Gestión de incidentes de Seguridad de la Información. Ver numeral 11.1
		[E.2] Errores del administrador del sistema / de la seguridad E.18] Destrucción de la información [E.24] caída del sistema por agotamiento de recursos	Alto	Se mitiga el riesgo con la implementación de los controles 5.1.1 – 5.1.2 – 6.1.1 -6.1.2 – 6.1.3 – 6.1.4 – 6.1.5 – 8.1.1 - 8.1.2 – 8.1.3 – 8.1.4 – 9.1.1 -9.1.2 – 9.2.1 - 9.2.2 - 9.2.3 - 9.2.4 - 9.2.5 - 9.2.6 - 9.3.1 - 9.4.1 - 9.4.2 - 9.4.3 -9.4.4 - 9.4.5 10.1.2 - 12.1.1 - 12.1.2 - 12.1.3 - 12.1.4 - 12.2.1 - 12.3.1 -12.4.1 - 12.4.2 - 12.4.3 - 12.4.4 - 12.5.1 - 12.6.1 - 12.6.2 - 12.7.1- 16.1.1 – 16.1.2 – 16.1.3 – 16.1.4 – 16.1.5 – 16.1.6 – 16.1.7	Gestión de acceso a usuarios. Manual de política de seguridad y controles básicos y específicos para el manejo de la información. Planificación de la continuidad de la seguridad de la información. Copias de seguridad de la información. Registro y gestión de eventos de seguridad.	**Proyecto 2-** Responsabilidades y proyectos de operación. Ver numeral 11.1. **Proyecto 3-** Implementación y seguimiento de registros de actividad. Ver numeral 11.1 **Proyecto 4–** Control de acceso y responsabilidades de los usuarios a los sistemas y aplicaciones. Ver numeral 11.1 **Proyecto 6–** Seguimiento y cumplimiento de la política de Seguridad de la información de la Entidad. Ver numeral 11.1 7- Gestión de incidentes de Seguridad de la información. Ver numeral 11.1
		[E.19] Fugas de información	Medio	Se mitiga el riesgo con la implementación de los controles 5.1.1 – 5.1.2 – 6.1.1 -6.1.2 – 6.1.3 – 6.1.4 – 6.1.5 – 8.1.1 - 8.1.2 – 8.1.3 – 8.1.4 – 9.1.1 -9.1.2 – 10.1.2 -11.1.1 - 11.1.2 - 11.1.3 - 11.1.4. -11.1.5 - 11.1.6 - 11.2.2 11.2.3	Manual de política de seguridad y controles básicos y específicos para el manejo de la información.	**Proyecto 1-** Control de acceso físico y protección de la información (Áreas seguras y seguridad de equipos).Ver numeral 11.1. **Proyecto 6–** Seguimiento y cumplimiento de la política de Seguridad de la información de la Entidad. Ver numeral 11.1
	Pérdida de la Integridad de la información, lo que implica el acceso indebido o fraudulento al activo de información	[E.19] Fugas de información [A.15] Modificación de la información	Muy Alto	Se mitiga el riesgo con la implementación de los controles 5.1.1 – 5.1.2 – 6.1.1 -6.1.2 – 6.1.3 – 6.1.4 – 6.1.5 – 8.1.1 - 8.1.2 – 8.1.3 – 8.1.4 – 9.1.1 -9.1.2 – 10.1.2 -11.1.1 - 11.1.2 - 11.1.3 - 11.1.4. -11.1.5 - 11.1.6 - 11.2.2 11.2.3	Manual de política de seguridad y controles básicos y específicos para el manejo de la información. Política de control de acceso. Gestión de contraseñas. Gestión de derechos de acceso con privilegios especiales.	**Proyecto 1-** Control de acceso físico y protección de la información (Áreas seguras y seguridad de equipos).Ver numeral 11.1. **Proyecto 6–** Seguimiento y cumplimiento de la política de Seguridad de la información de la Entidad. Ver numeral 11.1

Tabla 33. (Continuación)

ACTIVOS	RIESGO	AMENAZAS	VALOR	TRATAMIENTO DE RIESGO	CONTROLES IMPLEMENTADOS	PROYECTOS DEFINIDOS
Controlador de dominio Misión Bogotá	Pérdida de la Integridad de la información, lo que implica el acceso indebido o fraudulento al activo de información	[A.5] suplantación de la identidad del usuario	Medio	Se mitiga el riesgo con la implementación de los controles 9.1.1 - 9.1.2 - 9.2.4 - 9.2.5 -11.1.1 - 11.1.2 - 11.1.3 - 11.1.4. -11.1.5 - 11.1.6 - 11.2.2 11.2.3	Política de control de acceso. Política de derechos de acceso asignados a usuarios.	**Proyecto 3-** Implementación y seguimiento de registros de actividad. Ver numeral 11.1 **Proyecto 4–** Control de acceso y responsabilidades de los usuarios a los sistemas y aplicaciones. Ver numeral 11.1
		[E.2] Errores del administrador del sistema / de la seguridad	Alto	Se mitiga el riesgo con la implementación de los controles 9.1.1 -9.1.2 – 9.2.1 - 9.2.2 - 9.2.3 - 9.2.4 - 9.2.5 - 9.2.6 - 9.3.1 - 9.4.1 - 9.4.2 - 9.4.3 -9.4.4 - 9.4.5	Gestión de acceso a usuarios. Gestión de derechos de acceso asignados a usuarios. Gestión de contraseñas de usuarios.	**Proyecto 4–** Control de acceso y responsabilidades de los usuarios a los sistemas y aplicaciones. Ver numeral 11.1
		[E.15] Alteración de la información				
		[E.18] Destrucción de la información				
		[A.6] Abuso de privilegios de acceso				
		[A.7] uso no previsto				
		[A.11] Acceso no autorizado				
	Pérdida de la Confidencialidad, acceso no autorizado que permite la utilización indebida o no autorizada del activo de información	[E.19] Fugas de información	Muy Alto	Se mitiga el riesgo con la implementación de los controles 5.1.1 – 5.1.2 – 6.1.1 -6.1.2 – 6.1.3 – 6.1.4 – 6.1.5 – 8.1.1 - 8.1.2 – 8.1.3 – 8.1.4 – 9.1.1 -9.1.2 – 10.1.2 -11.1.1 - 11.1.2 - 11.1.3 - 11.1.4. -11.1.5 - 11.1.6 - 11.2.2 11.2.3	Manual de política de seguridad y controles básicos y específicos para el manejo de la información. Gestión de derechos de acceso con privilegios especiales.	**Proyecto 1-** Control de acceso físico y protección de la información (Áreas seguras y seguridad de equipos).Ver numeral 11.1. **Proyecto 6–** Seguimiento y cumplimiento de la política de Seguridad de la información de la Entidad. Ver numeral 11.1
		[E.2] Errores del administrador del sistema / de la seguridad	Alto	Se mitiga el riesgo con la implementación de los controles 5.1.1 – 5.1.2 – 6.1.1 -6.1.2 9.1.1 -9.1.2 – - 11.1.1 - 11.1.2	Conjunto de políticas para la seguridad de la información. Política de control de acceso. Gestión de contraseñas de usuarios.	**Proyecto 1-** Control de acceso físico y protección de la información (Áreas seguras y seguridad de equipos).Ver numeral 11.1. **Proyecto 6–** Seguimiento y cumplimiento de la política de Seguridad de la información de la Entidad. Ver numeral 11.1
		[E.15] Alteración de la información				
		[E.18] Destrucción de la información				
		[A.6] Abuso de privilegios de acceso				

Tabla 33. (Continuación)

ACTIVOS	RIESGO	AMENAZAS	VALOR	TRATAMIENTO DE RIESGO	CONTROLES IMPLEMENTADOS	PROYECTOS DEFINIDOS
Controlador de dominio Misión Bogotá	Pérdida de la Confidencialidad, acceso no autorizado que permite la utilización indebida o no autorizada del activo de información	[A.7] uso no previsto [A.11] Acceso no autorizado [A.19] revelación de información	Alto	Se mitiga el riesgo con la implementación de los controles 5.1.1 – 5.1.2 – 6.1.1 -6.1.2 9.1.1 -9.1.2 – -11.1.1 - 11.1.2	Conjunto de políticas para la seguridad de la información. Política de control de acceso. Gestión de contraseñas de usuarios.	**Proyecto 1-** Control de acceso físico y protección de la información (Áreas seguras y seguridad de equipos).Ver numeral
		[A.5] suplantación de la identidad del usuario	Medio	Se mitiga el riesgo con la implementación de los controles 9.1.1 - 9.1.2 - 9.2.4 - 9.2.5 -11.1.1 - 11.1.2 - 11.1.3 - 11.1.4. -11.1.5 - 11.1.6 - 11.2.2 11.2.3	Política de control de acceso. Política de derechos de acceso asignados a usuarios.	**Proyecto 3-** Implementación y seguimiento de registros de actividad. Ver numeral 11.1 **Proyecto 4–** Control de acceso y responsabilidades de los usuarios a los sistemas y aplicaciones. Ver numeral 11.1
	Pérdida de Autenticidad, en el comportamiento, resultado o uso del activo de información	[A.5] suplantación de la identidad del usuario	Alto	Se mitiga el riesgo con la implementación de los controles 9.1.1 - 9.1.2 - 9.2.4 - 9.2.5 -11.1.1 - 11.1.2 - 11.1.3 - 11.1.4. -11.1.5 - 11.1.6 - 11.2.2 11.2.3	Política de control de acceso. Política de derechos de acceso asignados a usuarios.	**Proyecto 3-** Implementación y seguimiento de registros de actividad. Ver numeral 11.1 **Proyecto 4–** Control de acceso y responsabilidades de los usuarios a los sistemas y aplicaciones. Ver numeral 11.1
Controlador de dominio UPI La 32	Pérdida de Disponibilidad del activo de información	[A.7] uso no previsto	Muy Alto	Se mitiga el riesgo con la implementación de los controles 5.1.1 – 5.1.2 – 6.1.1 -6.1.2 – 6.1.3 – 6.1.4 – 6.1.5 – 8.1.1 - 8.1.2 – 8.1.3 – 8.1.4 – 9.1.1 -9.1.2 – 10.1.2 - 16.1.1 – 16.1.2 – 16.1.3 – 16.1.4 – 16.1.5 – 16.1.6 – 16.1.7	Conjunto de políticas para la seguridad de la información. Planificación de la continuidad de la seguridad de la información.	**Proyecto 6-** Seguimiento y cumplimiento de la Política y Seguridad de la Información de la Entidad. Ver numeral 11.1 **Proyecto 7-** Gestión de incidentes de Seguridad de la Información. Ver numeral 11.1
		[E.2] Errores del administrador del sistema / de la seguridad E.18] Destrucción de la información	Alto	Se mitiga el riesgo con la implementación de los controles 5.1.1 – 5.1.2 – 6.1.1 -6.1.2 – 6.1.3 – 6.1.4 – 6.1.5 – 8.1.1 - 8.1.2 – 8.1.3 – 8.1.4 – 9.1.1 -9.1.2 – 9.2.1 - 9.2.2 - 9.2.3 - 9.2.4 - 9.2.5 - 9.2.6 - 9.3.1 - 9.4.1 - 9.4.2 - 9.4.3 -9.4.4 - 9.4.5 10.1.2 - 12.1.1 - 12.1.2 - 12.1.3 - 12.1.4 - 12.2.1 - 12.3.1 -12.4.1 - 12.4.2 - 12.4.3 - 12.4.4 - 12.5.1 - 12.6.1 - 12.6.2 - 12.7.1- 16.1.1 – 16.1.2 – 16.1.3 – 16.1.4 – 16.1.5 – 16.1.6 – 16.1.7	Gestión de acceso a usuarios. Manual de política de seguridad y controles básicos y específicos para el manejo de la información. Planificación de la continuidad de la seguridad de la información. Copias de seguridad de la información. Registro y gestión de eventos de seguridad.	**Proyecto 2-** Responsabilidades y proyectos de operación. Ver numeral 11.1. **Proyecto 3-** Implementación y seguimiento de registros de actividad. Ver numeral 11.1 **Proyecto 4–** Control de acceso y responsabilidades de los usuarios a los sistemas y aplicaciones. Ver numeral 11.1 **Proyecto 6–** Seguimiento y cumplimiento de la política de Seguridad de la información de la Entidad. Ver numeral 11.1 7- Gestión de incidentes de Seguridad de la información. Ver numeral 11.1

Tabla 33. (Continuación)

ACTIVOS	RIESGO	AMENAZAS	VALOR	TRATAMIENTO DE RIESGO	CONTROLES IMPLEMENTADOS	PROYECTOS DEFINIDOS
Controlador de dominio UPI La 32	Pérdida de Disponibilidad del activo de información	[E.24] caída del sistema por agotamiento de recursos				
		[E.19] Fugas de información	Medio	Se mitiga el riesgo con la implementación de los controles 5.1.1 – 5.1.2 – 6.1.1 -6.1.2 – 6.1.3 – 6.1.4 – 6.1.5 – 8.1.1 - 8.1.2 – 8.1.3 – 8.1.4 – 9.1.1 -9.1.2 – 10.1.2 -11.1.1 - 11.1.2 - 11.1.3 - 11.1.4. -11.1.5 - 11.1.6 - 11.2.2 11.2.3	Manual de política de seguridad y controles básicos y específicos para el manejo de la información.	**Proyecto 1-** Control de acceso físico y protección de la información (Áreas seguras y seguridad de equipos).Ver numeral 11.1. **Proyecto 6–** Seguimiento y cumplimiento de la política de Seguridad de la información de la Entidad. Ver numeral 11.1
	Pérdida de la Integridad de la información, lo que implica el acceso indebido o fraudulento al activo de información	[E.19] Fugas de información [A.15] Modificación de la información	Muy Alto	Se mitiga el riesgo con la implementación de los controles 5.1.1 – 5.1.2 – 6.1.1 -6.1.2 – 6.1.3 – 6.1.4 – 6.1.5 – 8.1.1 - 8.1.2 – 8.1.3 – 8.1.4 – 9.1.1 -9.1.2 – 10.1.2 -11.1.1 - 11.1.2 - 11.1.3 - 11.1.4. -11.1.5 - 11.1.6 - 11.2.2 11.2.3	Manual de política de seguridad y controles básicos y específicos para el manejo de la información. Política de control de acceso. Gestión de contraseñas. Gestión de derechos de acceso con privilegios especiales.	**Proyecto 1-** Control de acceso físico y protección de la información (Áreas seguras y seguridad de equipos).Ver numeral 11.1. **Proyecto 6–** Seguimiento y cumplimiento de la política de Seguridad de la información de la Entidad. Ver numeral 11.1
		[A.5] suplantación de la identidad del usuario	Medio	Se mitiga el riesgo con la implementación de los controles 9.1.1 - 9.1.2 - 9.2.4 - 9.2.5 -11.1.1 - 11.1.2 - 11.1.3 - 11.1.4. -11.1.5 - 11.1.6 - 11.2.2 11.2.3	Política de control de acceso. Política de derechos de acceso asignados a usuarios.	**Proyecto 3-** Implementación y seguimiento de registros de actividad. Ver numeral 11.1 **Proyecto 4–** Control de acceso y responsabilidades de los usuarios a los sistemas y aplicaciones. Ver numeral 11.1
		[E.2] Errores del administrador del sistema / de la seguridad	Alto	Se mitiga el riesgo con la implementación de los controles 9.1.1 -9.1.2 – 9.2.1 - 9.2.2 - 9.2.3 - 9.2.4 - 9.2.5 - 9.2.6 - 9.3.1 - 9.4.1 - 9.4.2 - 9.4.3 -9.4.4 - 9.4.5	Gestión de acceso a usuarios. Gestión de derechos de acceso asignados a usuarios. Gestión de contraseñas de usuarios.	**Proyecto 4–** Control de acceso y responsabilidades de los usuarios a los sistemas y aplicaciones. Ver numeral 11.1
		[E.15] Alteración de la información				
		[E.18] Destrucción de la información				
		[A.6] Abuso de privilegios de acceso				
		[A.7] uso no previsto				
		[A.11] Acceso no autorizado				

Tabla 33. (Continuación)

ACTIVOS	RIESGO	AMENAZAS	VALOR	TRATAMIENTO DE RIESGO	CONTROLES IMPLEMENTADOS	PROYECTOS DEFINIDOS
Controlador de dominio UPI La 32	Pérdida de la Confidencialidad, acceso no autorizado que permite la utilización indebida o no autorizada del activo de información	[E.19] Fugas de información	Muy Alto	Se mitiga el riesgo con la implementación de los controles 5.1.1 – 5.1.2 – 6.1.1 -6.1.2 – 6.1.3 – 6.1.4 – 6.1.5 – 8.1.1 - 8.1.2 – 8.1.3 – 8.1.4 – 9.1.1 -9.1.2 – 10.1.2 -11.1.1 - 11.1.2 - 11.1.3 - 11.1.4. -11.1.5 - 11.1.6 - 11.2.2 11.2.3	Manual de política de seguridad y controles básicos y específicos para el manejo de la información. Gestión de derechos de acceso con privilegios especiales.	**Proyecto 1-** Control de acceso físico y protección de la información (Áreas seguras y seguridad de equipos).Ver numeral 11.1. **Proyecto 6–** Seguimiento y cumplimiento de la política de Seguridad de la información de la Entidad. Ver numeral 11.1
		[E.2] Errores del administrador del sistema / de la seguridad [E.15] Alteración de la información [E.18] Destrucción de la información [A.6] Abuso de privilegios de acceso [A.7] uso no previsto [A.11] Acceso no autorizado [A.19] revelación de información	Alto	Se mitiga el riesgo con la implementación de los controles 5.1.1 – 5.1.2 – 6.1.1 -6.1.2 9.1.1 -9.1.2 – - 11.1.1 - 11.1.2	Conjunto de políticas para la seguridad de la información. Gestión de acceso a usuarios. Gestión de derechos de acceso asignados a usuarios. Gestión de contraseñas de usuarios. Planificación de la continuidad de la seguridad de la información. Verificación, revisión y evaluación de la continuidad de la seguridad de la información.	**Proyecto 1**- Control de acceso físico y protección de la información (Áreas seguras y seguridad de equipos).Ver numeral 11.1. **Proyecto 6–** Seguimiento y cumplimiento de la política de Seguridad de la información de la Entidad. Ver numeral 11.1
		[A.5] suplantación de la identidad del usuario	Medio	Se mitiga el riesgo con la implementación de los controles 9.1.1 - 9.1.2 - 9.2.4 - 9.2.5 -11.1.1 - 11.1.2 - 11.1.3 - 11.1.4. -11.1.5 - 11.1.6 - 11.2.2 11.2.3	Política de control de acceso. Política de derechos de acceso asignados a usuarios.	**Proyecto 3-** Implementación y seguimiento de registros de actividad. Ver numeral 11.1 **Proyecto 4–** Control de acceso y responsabilidades de los usuarios a los sistemas y aplicaciones. Ver numeral 11.1
	Pérdida de Autenticidad, en el comportamiento, resultado o uso del activo de información	[A.5] suplantación de la identidad del usuario	Alto	Se mitiga el riesgo con la implementación de los controles 9.1.1 - 9.1.2 - 9.2.4 - 9.2.5 -11.1.1 - 11.1.2 - 11.1.3 - 11.1.4. -11.1.5 - 11.1.6 - 11.2.2 11.2.3	Política de control de acceso. Política de derechos de acceso asignados a usuarios.	**Proyecto 3-** Implementación y seguimiento de registros de actividad. Ver numeral 11.1 **Proyecto 4–** Control de acceso y responsabilidades de los usuarios a los sistemas y aplicaciones. Ver numeral 11.1

Tabla 33. (Continuación)

ACTIVOS	RIESGO	AMENAZAS	VALOR	TRATAMIENTO DE RIESGO	CONTROLES IMPLEMENTADOS	PROYECTOS DEFINIDOS
Controlador de dominio UPI La Arcadia	Pérdida de Disponibilidad del activo de información	[A.7] uso no previsto	Muy Alto	Se mitiga el riesgo con la implementación de los controles 5.1.1 – 5.1.2 – 6.1.1 -6.1.2 – 6.1.3 – 6.1.4 – 6.1.5 – 8.1.1 - 8.1.2 – 8.1.3 – 8.1.4 – 9.1.1 -9.1.2 – 10.1.2 - 16.1.1 – 16.1.2 – 16.1.3 – 16.1.4 – 16.1.5 – 16.1.6 – 16.1.7	Conjunto de políticas para la seguridad de la información. Planificación de la continuidad de la seguridad de la información.	**Proyecto 6-** Seguimiento y cumplimiento de la Política y Seguridad de la Información de la Entidad. Ver numeral 11.1 **Proyecto 7-** Gestión de incidentes de Seguridad de la Información. Ver numeral 11.1
		[E.2] Errores del administrador del sistema / de la seguridad E.18] Destrucción de la información [E.24] caída del sistema por agotamiento de recursos [A.18] Destrucción de la información	Alto	Se mitiga el riesgo con la implementación de los controles 5.1.1 – 5.1.2 – 6.1.1 -6.1.2 – 6.1.3 – 6.1.4 – 6.1.5 – 8.1.1 - 8.1.2 – 8.1.3 – 8.1.4 – 9.1.1 -9.1.2 – 9.2.1 - 9.2.2 - 9.2.3 - 9.2.4 - 9.2.5 - 9.2.6 - 9.3.1 - 9.4.1 - 9.4.2 - 9.4.3 -9.4.4 - 9.4.5 10.1.2 - 12.1.1 - 12.1.2 - 12.1.3 - 12.1.4 - 12.2.1 - 12.3.1 -12.4.1 - 12.4.2 - 12.4.3 - 12.4.4 - 12.5.1 - 12.6.1 - 12.6.2 - 12.7.1- 16.1.1 – 16.1.2 – 16.1.3 – 16.1.4 – 16.1.5 – 16.1.6 – 16.1.7	Gestión de acceso a usuarios. Manual de política de seguridad y controles básicos y específicos para el manejo de la información. Planificación de la continuidad de la seguridad de la información. Copias de seguridad de la información. Registro y gestión de eventos de seguridad.	**Proyecto 2-** Responsabilidades y proyectos de operación. Ver numeral 11.1. **Proyecto 3-** Implementación y seguimiento de registros de actividad. Ver numeral 11.1 **Proyecto 4–** Control de acceso y responsabilidades de los usuarios a los sistemas y aplicaciones. Ver numeral 11.1 **Proyecto 6–** Seguimiento y cumplimiento de la política de Seguridad de la información de la Entidad. Ver numeral 11.1 **Proyecto 7-** Gestión de incidentes de Seguridad de la información. Ver numeral 11.1
		[E.19] Fugas de información	Medio	Se mitiga el riesgo con la implementación de los controles 5.1.1 – 5.1.2 – 6.1.1 -6.1.2 – 6.1.3 – 6.1.4 – 6.1.5 – 8.1.1 - 8.1.2 – 8.1.3 – 8.1.4 – 9.1.1 -9.1.2 – 10.1.2 -11.1.1 - 11.1.2 - 11.1.3 - 11.1.4. -11.1.5 - 11.1.6 - 11.2.2 11.2.3	Manual de política de seguridad y controles básicos y específicos para el manejo de la información. Gestión de derechos de acceso con privilegios especiales.	**Proyecto 1-** Control de acceso físico y protección de la información (Áreas seguras y seguridad de equipos).Ver numeral 11.1. **Proyecto 6–** Seguimiento y cumplimiento de la política de Seguridad de la información de la Entidad. Ver numeral 11.1
	Pérdida de la Integridad de la información, lo que implica el acceso indebido o fraudulento al activo de información	[E.19] Fugas de información [A.15] Modificación de la información	Muy Alto	Se mitiga el riesgo con la implementación de los controles 5.1.1 – 5.1.2 – 6.1.1 -6.1.2 – 6.1.3 – 6.1.4 – 6.1.5 – 8.1.1 - 8.1.2 – 8.1.3 – 8.1.4 – 9.1.1 -9.1.2 – 10.1.2 -11.1.1 - 11.1.2 - 11.1.3 - 11.1.4. -11.1.5 - 11.1.6 - 11.2.2 11.2.3	Manual de política de seguridad y controles básicos y específicos para el manejo de la información. Política de control de acceso. Gestión de contraseñas.	**Proyecto 1-** Control de acceso físico y protección de la información (Áreas seguras y seguridad de equipos).Ver numeral 11.1. **Proyecto 6–** Seguimiento y cumplimiento de la política de Seguridad de la información de la Entidad. Ver numeral 11.1
		[A.5] suplantación de la identidad del usuario	Medio	Se mitiga el riesgo con la implementación de los controles 9.1.1 - 9.1.2 - 9.2.4 - 9.2.5 -11.1.1 - 11.1.2 - 11.1.3 - 11.1.4. -11.1.5 - 11.1.6 - 11.2.2 11.2.3	Política de control de acceso. Política de derechos de acceso asignados a usuarios.	**Proyecto 4–** Control de acceso y responsabilidades de los usuarios a los sistemas y aplicaciones. Ver numeral 11.1 **Proyecto 3-** Implementación y seguimiento de registros de actividad. **Proyecto 6–** Seguimiento y cumplimiento de la política de Seguridad de la información de la Entidad.

Tabla 33. (Continuación)

ACTIVOS	RIESGO	AMENAZAS	VALOR	TRATAMIENTO DE RIESGO	CONTROLES IMPLEMENTADOS	PROYECTOS DEFINIDOS
Controlador de dominio UPI La Arcadia	Pérdida de la Integridad de la información, lo que implica el acceso indebido o fraudulento al activo de información	[E.2] Errores del administrador del sistema / de la seguridad	Alto	Se mitiga el riesgo con la implementación de los controles 9.1.1 -9.1.2 – 9.2.1 - 9.2.2 - 9.2.3 - 9.2.4 - 9.2.5 - 9.2.6 - 9.3.1 - 9.4.1 - 9.4.2 - 9.4.3 -9.4.4 - 9.4.5	Gestión de acceso a usuarios. Gestión de derechos de acceso asignados a usuarios. Gestión de contraseñas de usuarios.	**Proyecto 4–** Control de acceso y responsabilidades de los usuarios a los sistemas y aplicaciones. Ver numeral 11.1
		[E.15] Alteración de la información				
		[E.18] Destrucción de la información				
		[A.6] Abuso de privilegios de acceso				
		[A.7] uso no previsto				
		[A.11] Acceso no autorizado				
	Pérdida de la Confidencialidad, acceso no autorizado que permite la utilización indebida o no autorizada del activo de información	[E.19] Fugas de información	Muy Alto	Se mitiga el riesgo con la implementación de los controles 5.1.1 – 5.1.2 – 6.1.1 -6.1.2 – 6.1.3 – 6.1.4 – 6.1.5 – 8.1.1 - 8.1.2 – 8.1.3 – 8.1.4 – 9.1.1 -9.1.2 – 10.1.2 -11.1.1 - 11.1.2 - 11.1.3 - 11.1.4. -11.1.5 - 11.1.6 - 11.2.2 11.2.3	Manual de política de seguridad y controles básicos y específicos para el manejo de la información. Gestión de derechos de acceso con privilegios especiales.	**Proyecto 1-** Control de acceso físico y protección de la información (Áreas seguras y seguridad de equipos).Ver numeral 11.1. **Proyecto 6–** Seguimiento y cumplimiento de la política de Seguridad de la información de la Entidad. Ver numeral 11.1
		[E.2] Errores del administrador del sistema / de la seguridad	Alto	Se mitiga el riesgo con la implementación de los controles 5.1.1 – 5.1.2 – 6.1.1 -6.1.2 9.1.1 -9.1.2 – - 11.1.1 - 11.1.2	Conjunto de políticas para la seguridad de la información. Gestión de acceso a usuarios. Gestión de derechos de acceso asignados a usuarios. Gestión de contraseñas de usuarios. Proceso disciplinario.	**Proyecto 1**- Control de acceso físico y protección de la información (Áreas seguras y seguridad de equipos).Ver numeral 11.1. **Proyecto 6–** Seguimiento y cumplimiento de la política de Seguridad de la información de la Entidad. Ver numeral 11.1
		[E.15] Alteración de la información				
		[E.18] Destrucción de la información				
		[A.6] Abuso de privilegios de acceso				
		[A.7] uso no previsto				

Tabla 33. (Continuación)

ACTIVOS	RIESGO	AMENAZAS	VALOR	TRATAMIENTO DE RIESGO	CONTROLES IMPLEMENTADOS	PROYECTOS DEFINIDOS
Controlador de dominio UPI La Arcadia	Pérdida de la Confidencialidad, acceso no autorizado que permite la utilización indebida o no autorizada del activo de información	[A.11] Acceso no autorizado [A.19] revelación de información	Alto	Se mitiga el riesgo con la implementación de los controles 5.1.1 – 5.1.2 – 6.1.1 -6.1.2 9.1.1 -9.1.2 – - 11.1.1 - 11.1.2	Gestión de derechos de acceso asignados a usuarios. Gestión de contraseñas de usuarios. Proceso disciplinario.	**Proyecto 6–** Seguimiento y cumplimiento de la política de Seguridad de la información de la Entidad. Ver numeral 11.1
		[A.5] suplantación de la identidad del usuario	Medio	Se mitiga el riesgo con la implementación de los controles 9.1.1 - 9.1.2 - 9.2.4 - 9.2.5 -11.1.1 - 11.1.2 - 11.1.3 - 11.1.4. -11.1.5 - 11.1.6 - 11.2.2 11.2.3	Política de control de acceso. Política de derechos de acceso asignados a usuarios.	**Proyecto 3-** Implementación y seguimiento de registros de actividad. Ver numeral 11.1 **Proyecto 4–** Control de acceso y responsabilidades de los usuarios a los sistemas y aplicaciones. Ver numeral 11.1
	Pérdida de Autenticidad, en el comportamiento, resultado o uso del activo de información	[A.5] suplantación de la identidad del usuario	Alto	Se mitiga el riesgo con la implementación de los controles 9.1.1 - 9.1.2 - 9.2.4 - 9.2.5 -11.1.1 - 11.1.2 - 11.1.3 - 11.1.4. -11.1.5 - 11.1.6 - 11.2.2 11.2.3	Política de control de acceso. Política de derechos de acceso asignados a usuarios.	**Proyecto 3-** Implementación y seguimiento de registros de actividad. Ver numeral 11.1 **Proyecto 4–** Control de acceso y responsabilidades de los usuarios a los sistemas y aplicaciones. Ver numeral 11.1
Controlador de dominio UPI La Florida	Pérdida de Disponibilidad del activo de información	[A.7] uso no previsto	Muy Alto	Se mitiga el riesgo con la implementación de los controles 5.1.1 – 5.1.2 – 6.1.1 -6.1.2 – 6.1.3 – 6.1.4 – 6.1.5 – 8.1.1 - 8.1.2 – 8.1.3 – 8.1.4 – 9.1.1 -9.1.2 – 10.1.2 - 16.1.1 – 16.1.2 – 16.1.3 – 16.1.4 – 16.1.5 – 16.1.6 – 16.1.7	Conjunto de políticas para la seguridad de la información.	**Proyecto 6-** Seguimiento y cumplimiento de la Política y Seguridad de la Información de la Entidad. Ver numeral 11.1
					Planificación de la continuidad de la seguridad de la información.	**Proyecto 7-** Gestión de incidentes de Seguridad de la Información. Ver numeral 11.1
		[E.2] Errores del administrador del sistema / de la seguridad E.18] Destrucción de la información	Alto	Se mitiga el riesgo con la implementación de los controles 5.1.1 – 5.1.2 – 6.1.1 -6.1.2 – 6.1.3 – 6.1.4 – 6.1.5 – 8.1.1 - 8.1.2 – 8.1.3 – 8.1.4 – 9.1.1 -9.1.2 – 9.2.1 - 9.2.2 - 9.2.3 - 9.2.4 - 9.2.5 - 9.2.6 - 9.3.1 - 9.4.1 - 9.4.2 - 9.4.3 -9.4.4 - 9.4.5 10.1.2 - 12.1.1 - 12.1.2 - 12.1.3 - 12.1.4 - 12.2.1 - 12.3.1 -12.4.1 - 12.4.2 - 12.4.3 - 12.4.4 - 12.5.1 - 12.6.1 - 12.6.2 - 12.7.1- 16.1.1 – 16.1.2 – 16.1.3 – 16.1.4 – 16.1.5 – 16.1.6 – 16.1.7	Gestión de acceso a usuarios. Manual de política de seguridad y controles básicos y específicos para el manejo de la información.	**Proyecto 2-** Responsabilidades y proyectos de operación. Ver numeral 11.1. **Proyecto 3-** Implementación y seguimiento de registros de actividad. Ver numeral 11.1 **Proyecto 4–** Control de acceso y responsabilidades de los usuarios a los sistemas y aplicaciones. Ver numeral 11.1 **Proyecto 6–** Seguimiento y cumplimiento de la política de Seguridad de la información de la Entidad. Ver numeral 11.1 7- Gestión de incidentes de Seguridad de la información. Ver numeral 11.1
		[E.24] caída del sistema por agotamiento de recursos			Copias de seguridad de la información.	
		[A.18] Destrucción de la información			Registro y gestión de eventos de seguridad.	

Tabla 33. (Continuación)

ACTIVOS	RIESGO	AMENAZAS	VALOR	TRATAMIENTO DE RIESGO	CONTROLES IMPLEMENTADOS	PROYECTOS DEFINIDOS
Controlador de dominio UPI La Florida	Pérdida de Disponibilidad del activo de información	[E.19] Fugas de información	Medio	Se mitiga el riesgo con la implementación de los controles 5.1.1 – 5.1.2 – 6.1.1 -6.1.2 – 6.1.3 – 6.1.4 – 6.1.5 – 8.1.1 - 8.1.2 – 8.1.3 – 8.1.4 – 9.1.1 -9.1.2 – 10.1.2 -11.1.1 - 11.1.2 - 11.1.3 - 11.1.4. -11.1.5 - 11.1.6 - 11.2.2 11.2.3	Manual de política de seguridad y controles básicos y específicos para el manejo de la información.	**Proyecto 1-** Control de acceso físico y protección de la información (Áreas seguras y seguridad de equipos).Ver numeral 11.1. **Proyecto 6–** Seguimiento y cumplimiento de la política de Seguridad de la información de la Entidad. Ver numeral 11.1
	Pérdida de la Integridad de la información, lo que implica el acceso indebido o fraudulento al activo de información	[E.19] Fugas de información	Muy Alto	Se mitiga el riesgo con la implementación de los controles 5.1.1 – 5.1.2 – 6.1.1 -6.1.2 – 6.1.3 – 6.1.4 – 6.1.5 – 8.1.1 - 8.1.2 – 8.1.3 – 8.1.4 – 9.1.1 -9.1.2 – 10.1.2 -11.1.1 - 11.1.2 - 11.1.3 - 11.1.4. -11.1.5 - 11.1.6 - 11.2.2 11.2.3	Manual de política de seguridad y controles básicos y específicos para el manejo de la información. Política de control de acceso. Gestión de contraseñas.	**Proyecto 1-** Control de acceso físico y protección de la información (Áreas seguras y seguridad de equipos).Ver numeral 11.1. **Proyecto 6–** Seguimiento y cumplimiento de la política de Seguridad de la información de la Entidad. Ver numeral 11.1
		[A.15] Modificación de la información			Gestión de derechos de acceso con privilegios especiales.	
		[A.5] suplantación de la identidad del usuario	Medio	Se mitiga el riesgo con la implementación de los controles 9.1.1 - 9.1.2 - 9.2.4 - 9.2.5 -11.1.1 - 11.1.2 - 11.1.3 - 11.1.4. -11.1.5 - 11.1.6 - 11.2.2 11.2.3	Manual de política de seguridad y controles básicos y específicos para el manejo de la información. Política de control de acceso. Gestión de contraseñas	**Proyecto 3-** Implementación y seguimiento de registros de actividad. Ver numeral 11.1 **Proyecto 4–** Control de acceso y responsabilidades de los usuarios a los sistemas y aplicaciones. Ver numeral 11.1
		[E.2] Errores del administrador del sistema / de la seguridad	Alto	Se mitiga el riesgo con la implementación de los controles 9.1.1 -9.1.2 – 9.2.1 - 9.2.2 - 9.2.3 - 9.2.4 - 9.2.5 - 9.2.6 - 9.3.1 - 9.4.1 - 9.4.2 - 9.4.3 -9.4.4 - 9.4.5	Gestión de acceso a usuarios. Gestión de derechos de acceso asignados a usuarios. Gestión de contraseñas de usuarios.	**Proyecto 4–** Control de acceso y responsabilidades de los usuarios a los sistemas y aplicaciones. Ver numeral 11.1
		[E.15] Alteración de la información				
		[E.18] Destrucción de la información				
		[A.6] Abuso de privilegios de acceso				
		[A.7] uso no previsto				
		[A.11] Acceso no autorizado				
		[A.18] Destrucción de la información				

Tabla 33. (Continuación)

ACTIVOS	RIESGO	AMENAZAS	VALOR	TRATAMIENTO DE RIESGO	CONTROLES IMPLEMENTADOS	PROYECTOS DEFINIDOS
Controlador de dominio UPI La Florida	Pérdida de la Confidencialidad, acceso no autorizado que permite la utilización indebida o no autorizada del activo de información	[E.19] Fugas de información	Muy Alto	Se mitiga el riesgo con la implementación de los controles 5.1.1 – 5.1.2 – 6.1.1 -6.1.2 – 6.1.3 – 6.1.4 – 6.1.5 – 8.1.1 - 8.1.2 – 8.1.3 – 8.1.4 – 9.1.1 -9.1.2 – 10.1.2 -11.1.1 - 11.1.2 - 11.1.3 - 11.1.4. -11.1.5 - 11.1.6 - 11.2.2 11.2.3	Manual de política de seguridad y controles básicos y específicos para el manejo de la información. Gestión de derechos de acceso con privilegios especiales.	**Proyecto 1-** Control de acceso físico y protección de la información (Áreas seguras y seguridad de equipos).Ver numeral 11.1. **Proyecto 6–** Seguimiento y cumplimiento de la política de Seguridad de la información de la Entidad. Ver numeral 11.1
		[E.2] Errores del administrador del sistema / de la seguridad	Alto	Se mitiga el riesgo con la implementación de los controles 5.1.1 – 5.1.2 – 6.1.1 -6.1.2 9.1.1 -9.1.2 – -11.1.1 - 11.1.2	Manual de política de seguridad y controles básicos y específicos para el manejo de la información. Política de control de acceso.	**Proyecto 1**- Control de acceso físico y protección de la información (Áreas seguras y seguridad de equipos).Ver numeral 11.1. **Proyecto 6–** Seguimiento y cumplimiento de la política de Seguridad de la información de la Entidad. Ver numeral 11.1
		[E.15] Alteración de la información			Gestión de contraseñas.	
		[E.18] Destrucción de la información				
		[A.6] Abuso de privilegios de acceso				
		[A.7] uso no previsto				
		[A.11] Acceso no autorizado				
		[A.19] revelación de información				
		[A.5] suplantación de la identidad del usuario	Medio	Se mitiga el riesgo con la implementación de los controles 9.1.1 - 9.1.2 - 9.2.4 - 9.2.5 -11.1.1 - 11.1.2 - 11.1.3 - 11.1.4. -11.1.5 - 11.1.6 - 11.2.2 11.2.3	Política de control de acceso. Política de derechos de acceso asignados a usuarios.	**Proyecto 3-** Implementación y seguimiento de registros de actividad. Ver numeral 11.1 **Proyecto 4–** Control de acceso y responsabilidades de los usuarios a los sistemas y aplicaciones. Ver numeral 11.1
	Pérdida de Autenticidad, en el comportamiento, resultado o uso del activo de información	[A.5] suplantación de la identidad del usuario	Alto	Se mitiga el riesgo con la implementación de los controles 9.1.1 - 9.1.2 - 9.2.4 - 9.2.5 -11.1.1 - 11.1.2 - 11.1.3 - 11.1.4. -11.1.5 - 11.1.6 - 11.2.2 11.2.3	Política de control de acceso. Política de derechos de acceso asignados a usuarios.	**Proyecto 3-** Implementación y seguimiento de registros de actividad. Ver numeral 11.1 **Proyecto 4–** Control de acceso y responsabilidades de los usuarios a los sistemas y aplicaciones. Ver numeral 11.1

Tabla 33. (Continuación)

ACTIVOS	RIESGO	AMENAZAS	VALOR	TRATAMIENTO DE RIESGO	CONTROLES IMPLEMENTADOS	PROYECTOS DEFINIDOS
Correo electrónico ZIMBRA MTA	Pérdida de Disponibilidad del activo de información	[E.1] Errores de los usuarios	Muy Alto	Se mitiga el riesgo con la implementación de los controles 5.1.1 – 5.1.2 – 6.1.1 -6.1.2 – 6.1.3 – 6.1.4 – 6.1.5 – 8.1.1 - 8.1.2 – 8.1.3 – 8.1.4 – 9.1.1 -9.1.2 – 9.2.1 - 9.2.2 - 9.2.3 - 9.2.4 - 9.2.5 - 9.2.6 - 9.3.1 - 9.4.1 - 9.4.2 - 9.4.3 -9.4.4 - 9.4.5 10.1.2 - 12.1.1 - 12.1.2 - 12.1.3 - 12.1.4 - 12.2.1 - 12.3.1 -12.4.1 - 12.4.2 - 12.4.3 - 12.4.4 - 12.5.1 - 12.6.1	Gestión de acceso a usuarios. Manual de política de seguridad y controles básicos y específicos para el manejo de la información.	**Proyecto 2-** Responsabilidades y proyectos de operación. Ver numeral 11.1.
		[E.18] Destrucción de la información			Planificación de la continuidad de la seguridad de la información.	**Proyecto 3-** Implementación y seguimiento de registros de actividad. Ver numeral 11.1
		[E.24] caída del sistema por agotamiento de recursos			Copias de seguridad de la información.	**Proyecto 4–** Control de acceso y responsabilidades de los usuarios a los sistemas y aplicaciones. Ver numeral 11.1
		[A.7] uso no previsto			Registro y gestión de eventos de seguridad.	**Proyecto 6–** Seguimiento y cumplimiento de la política de Seguridad de la información de la entidad. Ver numeral 11.1
		[A.24] Denegación de servicio				
		[E.2] Errores del administrador del sistema / de la seguridad	Alto	Se mitiga el riesgo con la implementación de los controles 5.1.1 – 5.1.2 – 6.1.1 -6.1.2 – 6.1.3 – 6.1.4 – 6.1.5 – 8.1.1 - 8.1.2 – 8.1.3 – 8.1.4 – 9.1.1 -9.1.2 – 9.2.1 - 9.2.2 - 9.2.3 - 9.2.4 - 9.2.5 - 9.2.6 - 9.3.1 - 9.4.1 - 9.4.2 - 9.4.3 -9.4.4 - 9.4.5 10.1.2 - 12.1.1 - 12.1.2 - 12.1.3 - 12.1.4 - 12.2.1 - 12.3.1 -12.4.1 - 12.4.2 - 12.4.3 - 12.4.4 - 12.5.1 - 12.6.1 - 12.6.2 - 12.7.1- 16.1.1 – 16.1.2 – 16.1.3 – 16.1.4 – 16.1.5 – 16.1.6 – 16.1.7	Política de control de acceso. Manual de política de seguridad y controles básicos y específicos para el manejo de la información. Registro y gestión de eventos de seguridad. Copias de seguridad de la información.	**Proyecto 2**- Responsabilidades y proyectos de operación. Ver numeral 11.1. **Proyecto 3-** Implementación y seguimiento de registros de actividad. Ver numeral 11.1 **Proyecto 4**– Control de acceso y responsabilidades de los usuarios a los sistemas y aplicaciones. Ver numeral 11.1 **Proyecto 6–** Seguimiento y cumplimiento de la política de Seguridad de la información de la Entidad. Ver numeral 11.1 **Proyecto 7-** Gestión de incidentes de Seguridad de la información. Ver numeral 11.1
		[A.18] Destrucción de la información				

Tabla 33. (Continuación)

ACTIVOS	RIESGO	AMENAZAS	VALOR	TRATAMIENTO DE RIESGO	CONTROLES IMPLEMENTADOS	PROYECTOS DEFINIDOS
Correo electrónico ZIMBRA MTA	Pérdida de la Integridad de la información, lo que implica el acceso indebido o fraudulento al activo de información	[E.1] Errores de los usuarios [E.18] Destrucción de la información [A.6] Abuso de privilegios de acceso [A.13] Repudio (negación de actuaciones)	Muy Alto	Se mitiga el riesgo con la implementación de los controles 5.1.1 – 5.1.2 – 6.1.1 -6.1.2 – 6.1.3 – 6.1.4 – 6.1.5 – 8.1.1 - 8.1.2 – 8.1.3 – 8.1.4 – 9.1.1 -9.1.2 – 10.1.2 -11.1.1 - 11.1.2 - 11.1.3 - 11.1.4. -11.1.5 - 11.1.6 - 11.2.2 11.2.3	Manual de política de seguridad y controles básicos y específicos para el manejo de la información. Política de control de acceso.	**Proyecto 1-** Control de acceso físico y protección de la información (Áreas seguras y seguridad de equipos).Ver numeral 11.1. **Proyecto 6–** Seguimiento y cumplimiento de la política de Seguridad de la información de la Entidad. Ver numeral 11.1
		[E.2] Errores del administrador del sistema / de la seguridad [E.15] Alteración de la información [A.5] suplantación de la identidad del usuario [A.7] uso no previsto [A.11] Acceso no autorizado	Alto	Se mitiga el riesgo con la implementación de los controles 9.1.1 - 9.1.2 - 9.2.1 - 9.2.2 - 9.2.3 - 9.2.4 - 9.2.5 -9.2.6 - 9.3.1 - 9.4.1 11.1.1 - 11.1.2 - 11.1.3 - 11.1.4. -11.1.5 - 11.1.6 - 11.2.2 11.2.3	Conjunto de políticas para la seguridad de la información. Gestión de acceso a usuarios. Gestión de derechos de acceso asignados a usuarios. Gestión de contraseñas de usuarios.	**Proyecto 1-** Control de acceso físico y protección de la información (Áreas Seguras y seguridad de equipos). **Proyecto 2-** Responsabilidades y proyectos de operación. **Proyecto 3-** Implementación y seguimiento de registros de actividad. Ver numeral 11.1 **Proyecto 4–** Control de acceso y responsabilidades de los usuarios a los sistemas y aplicaciones. Ver numeral 11.1

Tabla 33. (Continuación)

ACTIVOS	RIESGO	AMENAZAS	VALOR	TRATAMIENTO DE RIESGO	CONTROLES IMPLEMENTADOS	PROYECTOS DEFINIDOS
Correo electrónico ZIMBRA MTA	Pérdida de la Confidencialidad, acceso no autorizado que permite la utilización indebida o no autorizada del activo de información	[E.1] Errores de los usuarios	Muy Alto	Se mitiga el riesgo con la implementación de los controles 5.1.1 – 5.1.2 – 6.1.1 -6.1.2 – 6.1.3 – 6.1.4 – 6.1.5 – 8.1.1 - 8.1.2 – 8.1.3 – 8.1.4 – 9.1.1 -9.1.2 – 10.1.2 -11.1.1 - 11.1.2 - 11.1.3 - 11.1.4. -11.1.5 - 11.1.6 - 11.2.2 11.2.3	Gestión de derechos de acceso asignados a usuarios. Control de acceso. Gestión de altas/bajas en el registro de usuarios. Gestión de derechos de acceso con privilegios especiales.	**Proyecto 1**- Control de acceso físico y protección de la información (Áreas seguras y seguridad de equipos).Ver numeral 11.1. **Proyecto 6–** Seguimiento y cumplimiento de la política de Seguridad de la información de la Entidad. Ver numeral 11.1
		[E.19] Fugas de información				
		[A.6] Abuso de privilegios de acceso				
		[E.2] Errores del administrador del sistema / de la seguridad	Alto	Se mitiga el riesgo con la implementación de los controles 9.1.1 - 9.1.2 - 9.2.4 - 9.2.5 -11.1.1 - 11.1.2 - 11.1.3 - 11.1.4. -11.1.5 - 11.1.6 - 11.2.2 11.2.3	Conjunto de políticas para la seguridad de la información. Concientización, educación y capacitación en seguridad de la información.	**Proyecto 1**- Control de acceso físico y protección de la información (Áreas seguras y seguridad de equipos).Ver numeral 11.1. **Proyecto 6–** Seguimiento y cumplimiento de la política de Seguridad de la información de la Entidad. Ver numeral 11.1
		[A.5] suplantación de la identidad del usuario			Gestión de acceso a usuarios.	
		[A.7] uso no previsto			Gestión de derechos de acceso asignados a usuarios.	
		[A.11] Acceso no autorizado			Gestión de contraseñas de usuarios.	
		[A.19] revelación de información			Acuerdos de confidencialidad y secreto.	
	Pérdida de Autenticidad, en el comportamiento, resultado o uso del activo de información	[A.5] suplantación de la identidad del usuario	Alto	Se mitiga el riesgo con la implementación de los controles 9.1.1 - 9.1.2 - 9.2.4 - 9.2.5 -11.1.1 - 11.1.2 - 11.1.3 - 11.1.4. -11.1.5 - 11.1.6 - 11.2.2 11.2.3	Política de control de acceso. Política de derechos de acceso asignados a usuarios.	**Proyecto 3-** Implementación y seguimiento de registros de actividad. Ver numeral 11.1 **Proyecto 4–** Control de acceso y responsabilidades de los usuarios a los sistemas y aplicaciones. Ver numeral 11.1

Tabla 33. (Continuación)

ACTIVOS	RIESGO	AMENAZAS	VALOR	TRATAMIENTO DE RIESGO	CONTROLES IMPLEMENTADOS	PROYECTOS DEFINIDOS
Controlador de dominio UPI La Vega	Pérdida de Disponibilidad del activo de información	[A.7] uso no previsto	Muy Alto	Se mitiga el riesgo con la implementación de los controles 5.1.1 – 5.1.2 – 6.1.1 -6.1.2 – 6.1.3 – 6.1.4 – 6.1.5 – 8.1.1 - 8.1.2 – 8.1.3 – 8.1.4 – 9.1.1 -9.1.2 – 10.1.2 - 16.1.1 – 16.1.2 – 16.1.3 – 16.1.4 – 16.1.5 – 16.1.6 – 16.1.7	Conjunto de políticas para la seguridad de la información.	**Proyecto 6-** Seguimiento y cumplimiento de la Política y Seguridad de la Información de la Entidad. Ver numeral 11.1
					Planificación de la continuidad de la seguridad de la información.	**Proyecto 7-** Gestión de incidentes de Seguridad de la Información. Ver numeral 11.1
		[E.2] Errores del administrador del sistema / de la seguridad	Alto	Se mitiga el riesgo con la implementación de los controles 5.1.1 – 5.1.2 – 6.1.1 -6.1.2 – 6.1.3 – 6.1.4 – 6.1.5 – 8.1.1 - 8.1.2 – 8.1.3 – 8.1.4 – 9.1.1 -9.1.2 – 9.2.1 - 9.2.2 - 9.2.3 - 9.2.4 - 9.2.5 - 9.2.6 - 9.3.1 - 9.4.1 - 9.4.2 - 9.4.3 -9.4.4 - 9.4.5 10.1.2 - 12.1.1 - 12.1.2 - 12.1.3 - 12.1.4 - 12.2.1 - 12.3.1 -12.4.1 - 12.4.2 - 12.4.3 - 12.4.4 - 12.5.1 - 12.6.1 - 12.6.2 - 12.7.1- 16.1.1 – 16.1.2 – 16.1.3 – 16.1.4 – 16.1.5 – 16.1.6 – 16.1.7	Gestión de acceso a usuarios. Manual de política de seguridad y controles básicos y específicos para el manejo de la información. Planificación de la continuidad de la seguridad de la información. Copias de seguridad de la información. Registro y gestión de eventos de seguridad.	**Proyecto 2-** Responsabilidades y proyectos de operación. Ver numeral 11.1. **Proyecto 3-** Implementación y seguimiento de registros de actividad. Ver numeral 11.1 **Proyecto 4–** Control de acceso y responsabilidades de los usuarios a los sistemas y aplicaciones. Ver numeral 11.1 **Proyecto 6–** Seguimiento y cumplimiento de la política de Seguridad de la información de la Entidad. Ver numeral 11.1 **Proyecto 7-** Gestión de incidentes de Seguridad de la información. Ver numeral 11.1
		E.18] Destrucción de la información				
		[E.24] caída del sistema por agotamiento de recursos				
		[E.19] Fugas de información	Medio	Se mitiga el riesgo1 con la implementación de los controles 5.1.1 – 5.1.2 – 6.1.1 -6.1.2 – 6.1.3 – 6.1.4 – 6.1.5 – 8.1.1 - 8.1.2 – 8.1.3 – 8.1.4 – 9.1.1 -9.1.2 – 10.1.2 -11.1.1 - 11.1.2 - 11.1.3 - 11.1.4. -11.1.5 - 11.1.6 - 11.2.2 11.2.3	Manual de política de seguridad y controles básicos y específicos para el manejo de la información.	**Proyecto 1-** Control de acceso físico y protección de la información (Áreas seguras y seguridad de equipos).Ver numeral 11.1. **Proyecto 6–** Seguimiento y cumplimiento de la política de Seguridad de la información de la Entidad. Ver numeral 11.1
					Gestión de derechos de acceso con privilegios especiales.	

Tabla 33. (Continuación)

ACTIVOS	RIESGO	AMENAZAS	VALOR	TRATAMIENTO DE RIESGO	CONTROLES IMPLEMENTADOS	PROYECTOS DEFINIDOS
Controlador de dominio UPI La Vega	Pérdida de la Integridad de la información, lo que implica el acceso indebido o fraudulento al activo de información	[E.19] Fugas de información	Muy Alto	Se mitiga el riesgo con la implementación de los controles 5.1.1 – 5.1.2 – 6.1.1 -6.1.2 – 6.1.3 – 6.1.4 – 6.1.5 – 8.1.1 - 8.1.2 – 8.1.3 – 8.1.4 – 9.1.1 -9.1.2 – 10.1.2 -11.1.1 - 11.1.2 - 11.1.3 - 11.1.4. -11.1.5 - 11.1.6 - 11.2.2 11.2.3	Manual de política de seguridad y controles básicos y específicos para el manejo de la información. Política de control de acceso.	**Proyecto 1-** Control de acceso físico y protección de la información (Áreas seguras y seguridad de equipos).Ver numeral 11.1. **Proyecto 6–** Seguimiento y cumplimiento de la política de Seguridad de la información de la Entidad. Ver numeral 11.1
		[A.15] Modificación de la información			Gestión de contraseñas. Gestión de derechos de acceso con privilegios especiales.	
		[A.5] suplantación de la identidad del usuario	Medio	Se mitiga el riesgo con la implementación de los controles 9.1.1 - 9.1.2 - 9.2.4 - 9.2.5 -11.1.1 - 11.1.2 - 11.1.3 - 11.1.4. -11.1.5 - 11.1.6 - 11.2.2 11.2.3	Política de control de acceso. Política de derechos de acceso asignados a usuarios.	**Proyecto 3-** Implementación y seguimiento de registros de actividad. Ver numeral 11.1 **Proyecto 4–** Control de acceso y responsabilidades de los usuarios a los sistemas y aplicaciones. Ver numeral 11.1
		[E.2] Errores del administrador del sistema / de la seguridad	Alto	Se mitiga el riesgo con la implementación de los controles 9.1.1 -9.1.2 – 9.2.1 - 9.2.2 - 9.2.3 - 9.2.4 - 9.2.5 - 9.2.6 - 9.3.1 - 9.4.1 - 9.4.2 - 9.4.3 -9.4.4 - 9.4.5	Gestión de acceso a usuarios.	**Proyecto 4–** Control de acceso y responsabilidades de los usuarios a los sistemas y aplicaciones. Ver numeral 11.1
		[E.15] Alteración de la información			Gestión de derechos de acceso asignados a usuarios.	
		[E.18] Destrucción de la información			Gestión de contraseñas de usuarios.	
		[A.6] Abuso de privilegios de acceso				
		[A.7] uso no previsto				
		[A.11] Acceso no autorizado				
	Pérdida de la Confidencialidad, acceso no autorizado que permite la utilización indebida o no autorizada del activo de información	[E.19] Fugas de información	Muy Alto	Se mitiga el riesgo con la implementación de los controles 5.1.1 – 5.1.2 – 6.1.1 -6.1.2 – 6.1.3 – 6.1.4 – 6.1.5 – 8.1.1 - 8.1.2 – 8.1.3 – 8.1.4 – 9.1.1 -9.1.2 – 10.1.2 -11.1.1 - 11.1.2 - 11.1.3 - 11.1.4. -11.1.5 - 11.1.6 - 11.2.2 11.2.3	Manual de política de seguridad y controles básicos y específicos para el manejo de la información. Gestión de derechos de acceso con privilegios especiales.	**Proyecto 1-** Control de acceso físico y protección de la información (Áreas seguras y seguridad de equipos).Ver numeral 11.1. **Proyecto 6–** Seguimiento y cumplimiento de la política de Seguridad de la información de la Entidad. Ver numeral 11.1

Tabla 33. (Continuación)

ACTIVOS	RIESGO	AMENAZAS	VALOR	TRATAMIENTO DE RIESGO	CONTROLES IMPLEMENTADOS	PROYECTOS DEFINIDOS
Controlador de dominio UPI La Vega	Pérdida de la Confidencialidad, acceso no autorizado que permite la utilización indebida o no autorizada del activo de información	[E.2] Errores del administrador del sistema / de la seguridad	Alto	Se mitiga el riesgo con la implementación de los controles 5.1.1 – 5.1.2 – 6.1.1 -6.1.2 9.1.1 -9.1.2 – -11.1.1 - 11.1.2	Gestión de acceso a usuarios.	**Proyecto 1**- Control de acceso físico y protección de la información (Áreas seguras y seguridad de equipos).Ver numeral 11.1. **Proyecto 6–** Seguimiento y cumplimiento de la política de Seguridad de la información de la Entidad. Ver numeral 11.1
		[E.15] Alteración de la información			Gestión de derechos de acceso asignados a usuarios.	
		[E.18] Destrucción de la información			Gestión de contraseñas de usuarios.	
		[A.6] Abuso de privilegios de acceso			Conjunto de políticas para la seguridad de la información.	
		[A.7] uso no previsto			Implantación de la continuidad de la seguridad de la información.	
		[A.11] Acceso no autorizado				
		[A.5] suplantación de la identidad del usuario	Medio	Se mitiga el riesgo con la implementación de los controles 9.1.1 - 9.1.2 - 9.2.4 - 9.2.5 -11.1.1 - 11.1.2 - 11.1.3 - 11.1.4. -11.1.5 - 11.1.6 - 11.2.2 11.2.3	Política de control de acceso. Política de derechos de acceso asignados a usuarios.	**Proyecto 3-** Implementación y seguimiento de registros de actividad. Ver numeral 11.1 **Proyecto 4–** Control de acceso y responsabilidades de los usuarios a los sistemas y aplicaciones. Ver numeral 11.1
	Pérdida de Autenticidad, en el comportamiento, resultado o uso del activo de información	[A.5] suplantación de la identidad del usuario	Alto	Se mitiga el riesgo con la implementación de los controles 9.1.1 - 9.1.2 - 9.2.4 - 9.2.5 -11.1.1 - 11.1.2 - 11.1.3 - 11.1.4. -11.1.5 - 11.1.6 - 11.2.2 11.2.3	Política de control de acceso. Política de derechos de acceso asignados a usuarios.	**Proyecto 3-** Implementación y seguimiento de registros de actividad. Ver numeral 11.1 **Proyecto 4–** Control de acceso y responsabilidades de los usuarios a los sistemas y aplicaciones. Ver numeral 11.1
Controlador de dominio UPI El Perdomo	Pérdida de Disponibilidad del activo de información	[A.7] uso no previsto	Muy Alto	Se mitiga el riesgo con la implementación de los controles 5.1.1 – 5.1.2 – 6.1.1 -6.1.2 – 6.1.3 – 6.1.4 – 6.1.5 – 8.1.1 - 8.1.2 – 8.1.3 – 8.1.4 – 9.1.1 -9.1.2 – 10.1.2 - 16.1.1 – 16.1.2 – 16.1.3 – 16.1.4 – 16.1.5 – 16.1.6 – 16.1.7	Conjunto de políticas para la seguridad de la información.	**Proyecto 6-** Seguimiento y cumplimiento de la Política y Seguridad de la Información de la Entidad. Ver numeral 11.1 **Proyecto 7-** Gestión de incidentes de Seguridad de la Información. Ver numeral 11.1
		[A.24] Denegación de servicio				

Tabla 33. (Continuación)

ACTIVOS	RIESGO	AMENAZAS	VALOR	TRATAMIENTO DE RIESGO	CONTROLES IMPLEMENTADOS	PROYECTOS DEFINIDOS
Controlador de dominio UPI El Perdomo	Pérdida de Disponibilidad del activo de información	[E.2] Errores del administrador del sistema / de la seguridad	Alto	Se mitiga el riesgo con la implementación de los controles 5.1.1 – 5.1.2 – 6.1.1 -6.1.2 – 6.1.3 – 6.1.4 – 6.1.5 – 8.1.1 - 8.1.2 – 8.1.3 – 8.1.4 – 9.1.1 -9.1.2 – 9.2.1 - 9.2.2 - 9.2.3 - 9.2.4 - 9.2.5 - 9.2.6 - 9.3.1 - 9.4.1 - 9.4.2 - 9.4.3 -9.4.4 - 9.4.5 10.1.2 - 12.1.1 - 12.1.2 - 12.1.3 - 12.1.4 - 12.2.1 - 12.3.1 -12.4.1 - 12.4.2 - 12.4.3 - 12.4.4 - 12.5.1 - 12.6.1 - 12.6.2 - 12.7.1- 16.1.1 – 16.1.2 – 16.1.3 – 16.1.4 – 16.1.5 – 16.1.6 – 16.1.7	Gestión de acceso a usuarios. Manual de política de seguridad y controles básicos y específicos para el manejo de la información. Registro y gestión de eventos de seguridad.	**Proyecto 2-** Responsabilidades y proyectos de operación. Ver numeral 11.1. **Proyecto 3-** Implementación y seguimiento de registros de actividad. Ver numeral 11.1 **Proyecto 4–** Control de acceso y responsabilidades de los usuarios a los sistemas y aplicaciones. Ver numeral 11.1 **Proyecto 6–** Seguimiento y cumplimiento de la política de Seguridad de la información de la Entidad. Ver numeral 11.1 **Proyecto 7-** Gestión de incidentes de Seguridad de la información. Ver numeral 11.1
		[E.18] Destrucción de la información			Planificación de la continuidad de la seguridad de la información.	
		[E.24] caída del sistema por agotamiento de recursos			Copias de seguridad de la información.	
		[E.19] Fugas de información	Medio	Se mitiga el riesgo con la implementación de los controles 5.1.1 – 5.1.2 – 6.1.1 -6.1.2 – 6.1.3 – 6.1.4 – 6.1.5 – 8.1.1 - 8.1.2 – 8.1.3 – 8.1.4 – 9.1.1 -9.1.2 – 10.1.2 -11.1.1 - 11.1.2 - 11.1.3 - 11.1.4. -11.1.5 - 11.1.6 - 11.2.2 11.2.3	Manual de política de seguridad y controles básicos y específicos para el manejo de la información.	**Proyecto 1-** Control de acceso físico y protección de la información (Áreas seguras y seguridad de equipos).Ver numeral 11.1. **Proyecto 6–** Seguimiento y cumplimiento de la política de Seguridad de la información de la Entidad. Ver numeral 11.1
	Pérdida de la Integridad de la información, lo que implica el acceso indebido o fraudulento al activo de información	[E.19] Fugas de información	Muy Alto	Se mitiga el riesgo con la implementación de los controles 5.1.1 – 5.1.2 – 6.1.1 -6.1.2 – 6.1.3 – 6.1.4 – 6.1.5 – 8.1.1 - 8.1.2 – 8.1.3 – 8.1.4 – 9.1.1 -9.1.2 – 10.1.2 -11.1.1 - 11.1.2 - 11.1.3 - 11.1.4. -11.1.5 - 11.1.6 - 11.2.2 11.2.3	Manual de política de seguridad y controles básicos y específicos para el manejo de la información. Política de control de acceso. Retirada o adaptación de los derechos de acceso. Gestión de derechos de acceso con privilegios especiales.	**Proyecto 1-** Control de acceso físico y protección de la información (Áreas seguras y seguridad de equipos).Ver numeral 11.1. **Proyecto 6–** Seguimiento y cumplimiento de la política de Seguridad de la información de la Entidad. Ver numeral 11.1
		[A.15] Modificación de la información				
		[E.2] Errores del administrador del sistema / de la seguridad	Alto	Se mitiga el riesgo con la implementación de los controles 9.1.1 -9.1.2 – 9.2.1 - 9.2.2 - 9.2.3 - 9.2.4 - 9.2.5 - 9.2.6 - 9.3.1 - 9.4.1 - 9.4.2 - 9.4.3 -9.4.4 - 9.4.5	Gestión de acceso a usuarios.	**Proyecto 4–** Control de acceso y responsabilidades de los usuarios a los sistemas y aplicaciones. Ver numeral 11.1

Tabla 33. (Continuación)

ACTIVOS	RIESGO	AMENAZAS	VALOR	TRATAMIENTO DE RIESGO	CONTROLES IMPLEMENTADOS	PROYECTOS DEFINIDOS
Controlador de dominio UPI El Perdomo	Pérdida de la Integridad de la información, lo que implica el acceso indebido o fraudulento al activo de información	[A.6] Abuso de privilegios de acceso	Alto	Se mitiga el riesgo con la implementación de los controles 9.1.1 -9.1.2 – 9.2.1 - 9.2.2 - 9.2.3 - 9.2.4 - 9.2.5 - 9.2.6 - 9.3.1 - 9.4.1 - 9.4.2 - 9.4.3 -9.4.4 - 9.4.5	Gestión de derechos de acceso asignados a usuarios.	**Proyecto 4–** Control de acceso y responsabilidades de los usuarios a los sistemas y aplicaciones. Ver numeral 11.1
		[A.7] uso no previsto			Gestión de contraseñas de usuarios.	
		[E.15] Alteración de la información				
		[E.18] Destrucción de la información				
		[A.11] Acceso no autorizado				
		[A.5] suplantación de la identidad del usuario	Medio	Se mitiga el riesgo con la implementación de los controles 9.1.1 - 9.1.2 - 9.2.4 - 9.2.5 -11.1.1 - 11.1.2 - 11.1.3 - 11.1.4. -11.1.5 - 11.1.6 - 11.2.2 11.2.3	Política de control de acceso. Política de derechos de acceso asignados a usuarios.	**Proyecto 3-** Implementación y seguimiento de registros de actividad. Ver numeral 11.1 **Proyecto 4–** Control de acceso y responsabilidades de los usuarios a los sistemas y aplicaciones. Ver numeral 11.1
	Pérdida de la Confidencialidad, acceso no autorizado que permite la utilización indebida o no autorizada del activo de información	[E.19] Fugas de información	Muy Alto	Se mitiga el riesgo con la implementación de los controles 5.1.1 – 5.1.2 – 6.1.1 -6.1.2 – 6.1.3 – 6.1.4 – 6.1.5 – 8.1.1 - 8.1.2 – 8.1.3 – 8.1.4 – 9.1.1 -9.1.2 – 10.1.2 -11.1.1 - 11.1.2 - 11.1.3 - 11.1.4. -11.1.5 - 11.1.6 - 11.2.2 11.2.3	Manual de política de seguridad y controles básicos y específicos para el manejo de la información. Gestión de derechos de acceso con privilegios especiales.	**Proyecto 1-** Control de acceso físico y protección de la información (Áreas seguras y seguridad de equipos).Ver numeral 11.1. **Proyecto 6–** Seguimiento y cumplimiento de la política de Seguridad de la información de la Entidad. Ver numeral 11.1
		[E.2] Errores del administrador del sistema / de la seguridad	Alto	Se mitiga el riesgo con la implementación de los controles 5.1.1 – 5.1.2 – 6.1.1 -6.1.2 9.1.1 -9.1.2 – - 11.1.1 - 11.1.2	Gestión de acceso a usuarios.	**Proyecto 1**- Control de acceso físico y protección de la información (Áreas seguras y seguridad de equipos).Ver numeral 11.1. **Proyecto 6–** Seguimiento y cumplimiento de la política de Seguridad de la información de la Entidad. Ver numeral 11.1
		[E.15] Alteración de la información			Gestión de derechos de acceso asignados a usuarios.	
		[E.18] Destrucción de la información			Gestión de contraseñas de usuarios.	

Tabla 33. (Continuación)

ACTIVOS	RIESGO	AMENAZAS	VALOR	TRATAMIENTO DE RIESGO	CONTROLES IMPLEMENTADOS	PROYECTOS DEFINIDOS
Controlador de dominio UPI El Perdomo	Pérdida de la Confidencialidad, acceso no autorizado que permite la utilización indebida o no autorizada del activo de información	[A.6] Abuso de privilegios de acceso [A.7] uso no previsto [A.11] Acceso no autorizado [A.19] revelación de información	Alto	Se mitiga el riesgo con la implementación de los controles 5.1.1 – 5.1.2 – 6.1.1 -6.1.2 9.1.1 -9.1.2 – -11.1.1 - 11.1.2	Conjunto de políticas para la seguridad de la información. Planificación de la continuidad de la seguridad de la información.	**Proyecto 1**- Control de acceso físico y protección de la información (Áreas seguras y seguridad de equipos).Ver numeral 11.1. **Proyecto 6–** Seguimiento y cumplimiento de la política de Seguridad de la información de la Entidad. Ver numeral 11.1
		[A.5] suplantación de la identidad del usuario	Medio	Se mitiga el riesgo con la implementación de los controles 9.1.1 - 9.1.2 - 9.2.4 - 9.2.5 -11.1.1 - 11.1.2 - 11.1.3 - 11.1.4. -11.1.5 - 11.1.6 - 11.2.2 11.2.3	Política de control de acceso. Política de derechos de acceso asignados a usuarios.	**Proyecto 1-** Control de acceso físico y protección de la información (Áreas seguras y seguridad de equipos).Ver numeral 11.1. **Proyecto 6–** Seguimiento y cumplimiento de la política de Seguridad de la información de la Entidad. Ver numeral 11.1
	Pérdida de Autenticidad, en el comportamiento, resultado o uso del activo de información	[A.5] suplantación de la identidad del usuario	Alto	Se mitiga el riesgo con la implementación de los controles 9.1.1 - 9.1.2 - 9.2.4 - 9.2.5 -11.1.1 - 11.1.2 - 11.1.3 - 11.1.4. -11.1.5 - 11.1.6 - 11.2.2 11.2.3	Política de control de acceso. Política de derechos de acceso asignados a usuarios.	**Proyecto 3-** Implementación y seguimiento de registros de actividad. Ver numeral 11.1 **Proyecto 4–** Control de acceso y responsabilidades de los usuarios a los sistemas y aplicaciones. Ver numeral 11.1
Controlador de dominio UPI San Francisco	Pérdida de Disponibilidad del activo de información	[A.7] uso no previsto	Muy Alto	Se mitiga el riesgo con la implementación de los controles 5.1.1 – 5.1.2 – 6.1.1 -6.1.2 – 6.1.3 – 6.1.4 – 6.1.5 – 8.1.1 - 8.1.2 – 8.1.3 – 8.1.4 – 9.1.1 -9.1.2 – 10.1.2 - 16.1.1 – 16.1.2 – 16.1.3 – 16.1.4 – 16.1.5 – 16.1.6 – 16.1.7	Conjunto de políticas para la seguridad de la información. Planificación de la continuidad de la seguridad de la información.	**Proyecto 6-** Seguimiento y cumplimiento de la Política y Seguridad de la Información de la Entidad. Ver numeral 11.1 **Proyecto 7-** Gestión de incidentes de Seguridad de la Información. Ver numeral 11.1

Tabla 33. (Continuación)

ACTIVOS	RIESGO	AMENAZAS	VALOR	TRATAMIENTO DE RIESGO	CONTROLES IMPLEMENTADOS	PROYECTOS DEFINIDOS
Controlador de dominio UPI San Francisco	Pérdida de Disponibilidad del activo de información	[E.2] Errores del administrador del sistema / de la seguridad	Alto	Se mitiga el riesgo con la implementación de los controles 5.1.1 – 5.1.2 – 6.1.1 -6.1.2 – 6.1.3 – 6.1.4 – 6.1.5 – 8.1.1 - 8.1.2 – 8.1.3 – 8.1.4 – 9.1.1 -9.1.2 – 9.2.1 - 9.2.2 - 9.2.3 - 9.2.4 - 9.2.5 - 9.2.6 - 9.3.1 - 9.4.1 - 9.4.2 - 9.4.3 -9.4.4 - 9.4.5 10.1.2 - 12.1.1 - 12.1.2 - 12.1.3 - 12.1.4 - 12.2.1 - 12.3.1 -12.4.1 - 12.4.2 - 12.4.3 - 12.4.4 - 12.5.1 - 12.6.1 - 12.6.2 - 12.7.1- 16.1.1 – 16.1.2 – 16.1.3 – 16.1.4 – 16.1.5 – 16.1.6 – 16.1.7	Gestión de acceso a usuarios. Manual de política de seguridad y controles básicos y específicos para el manejo de la información.	**Proyecto 2-** Responsabilidades y proyectos de operación. Ver numeral 11.1. **Proyecto 3-** Implementación y seguimiento de registros de actividad. Ver numeral 11.1 **Proyecto 4–** Control de acceso y responsabilidades de los usuarios a los sistemas y aplicaciones. Ver numeral 11.1 **Proyecto 6–** Seguimiento y cumplimiento de la política de Seguridad de la información de la Entidad. Ver numeral 11.1 **Proyecto 7-** Gestión de incidentes de Seguridad de la información. Ver numeral 11.1
		E.18] Destrucción de la información			Planificación de la continuidad de la seguridad de la información.	
		[E.24] caída del sistema por agotamiento de recursos			Copias de seguridad de la información.	
		[A.18] Destrucción de la información			Registro y gestión de eventos de seguridad.	
		[E.19] Fugas de información	Medio	Se mitiga el riesgo con la implementación de los controles 5.1.1 – 5.1.2 – 6.1.1 -6.1.2 – 6.1.3 – 6.1.4 – 6.1.5 – 8.1.1 - 8.1.2 – 8.1.3 – 8.1.4 – 9.1.1 -9.1.2 – 10.1.2 -11.1.1 - 11.1.2 - 11.1.3 - 11.1.4. -11.1.5 - 11.1.6 - 11.2.2 11.2.3	Manual de política de seguridad y controles básicos y específicos para el manejo de la información.	**Proyecto 1-** Control de acceso físico y protección de la información (Áreas seguras y seguridad de equipos).Ver numeral 11.1. **Proyecto 6–** Seguimiento y cumplimiento de la política de Seguridad de la información de la Entidad. Ver numeral 11.1
	Pérdida de la Integridad de la información, lo que implica el acceso indebido o fraudulento al activo de información	[E.19] Fugas de información	Muy Alto	Se mitiga el riesgo con la implementación de los controles 5.1.1 – 5.1.2 – 6.1.1 -6.1.2 – 6.1.3 – 6.1.4 – 6.1.5 – 8.1.1 - 8.1.2 – 8.1.3 – 8.1.4 – 9.1.1 -9.1.2 – 10.1.2 -11.1.1 - 11.1.2 - 11.1.3 - 11.1.4. -11.1.5 - 11.1.6 - 11.2.2 11.2.3	Manual de política de seguridad y controles básicos y específicos para el manejo de la información. Política de control de acceso. Gestión de contraseñas. Gestión de derechos de acceso con privilegios especiales.	**Proyecto 1-** Control de acceso físico y protección de la información (Áreas seguras y seguridad de equipos).Ver numeral 11.1. **Proyecto 6–** Seguimiento y cumplimiento de la política de Seguridad de la información de la Entidad. Ver numeral 11.1
		[A.15] Modificación de la información				

Tabla 33. (Continuación)

ACTIVOS	RIESGO	AMENAZAS	VALOR	TRATAMIENTO DE RIESGO	CONTROLES IMPLEMENTADOS	PROYECTOS DEFINIDOS
Controlador de dominio UPI San Francisco	Pérdida de la Integridad de la información, lo que implica el acceso indebido o fraudulento al activo de información	[A.5] suplantación de la identidad del usuario	Medio	Se mitiga el riesgo con la implementación de los controles 9.1.1 - 9.1.2 - 9.2.4 - 9.2.5 -11.1.1 - 11.1.2 - 11.1.3 - 11.1.4. -11.1.5 - 11.1.6 - 11.2.2 11.2.3	Política de control de acceso. Política de derechos de acceso asignados a usuarios.	**Proyecto 3-** Implementación y seguimiento de registros de actividad. Ver numeral 11.1 **Proyecto 4–** Control de acceso y responsabilidades de los usuarios a los sistemas y aplicaciones. Ver numeral 11.1
		[E.2] Errores del administrador del sistema / de la seguridad	Alto	Se mitiga el riesgo con la implementación de los controles 9.1.1 -9.1.2 – 9.2.1 - 9.2.2 - 9.2.3 - 9.2.4 - 9.2.5 - 9.2.6 - 9.3.1 - 9.4.1 - 9.4.2 - 9.4.3 -9.4.4 - 9.4.5	Gestión de acceso a usuarios. Gestión de derechos de acceso asignados a usuarios. Gestión de contraseñas de usuarios.	**Proyecto 4–** Control de acceso y responsabilidades de los usuarios a los sistemas y aplicaciones. Ver numeral 11.1
		[E.15] Alteración de la información				
		[E.18] Destrucción de la información				
		[A.6] Abuso de privilegios de acceso				
		[A.7] uso no previsto				
		[A.11] Acceso no autorizado				
		[A.18] Destrucción de la información				
	Pérdida de la Confidencialidad, acceso no autorizado que permite la utilización indebida o no autorizada del activo de información	[E.19] Fugas de información	Muy Alto	Se mitiga el riesgo con la implementación de los controles 5.1.1 – 5.1.2 – 6.1.1 -6.1.2 – 6.1.3 – 6.1.4 – 6.1.5 – 8.1.1 - 8.1.2 – 8.1.3 – 8.1.4 – 9.1.1 -9.1.2 – 10.1.2 -11.1.1 - 11.1.2 - 11.1.3 - 11.1.4. -11.1.5 - 11.1.6 - 11.2.2 11.2.3	Manual de política de seguridad y controles básicos y específicos para el manejo de la información. Gestión de derechos de acceso con privilegios especiales.	**Proyecto 6–** Seguimiento y cumplimiento de la política de Seguridad de la información de la Entidad
		[E.2] Errores del administrador del sistema / de la seguridad	Alto	Se mitiga el riesgo con la implementación de los controles 5.1.1 – 5.1.2 – 6.1.1 -6.1.2 9.1.1 -9.1.2 – - 11.1.1 - 11.1.2	Gestión de acceso a usuarios. Gestión de derechos de acceso asignados a usuarios.	**Proyecto 1**- Control de acceso físico y protección de la información (Áreas seguras y seguridad de equipos).Ver numeral 11.1. **Proyecto 6–** Seguimiento y cumplimiento de la política de Seguridad de la información de la Entidad. Ver numeral 11.1

Tabla 33. (Continuación)

ACTIVOS	RIESGO	AMENAZAS	VALOR	TRATAMIENTO DE RIESGO	CONTROLES IMPLEMENTADOS	PROYECTOS DEFINIDOS
Controlador de dominio UPI San Francisco	Pérdida de la Confidencialidad, acceso no autorizado que permite la utilización indebida o no autorizada del activo de información	[E.15] Alteración de la información	Alto	Se mitiga el riesgo con la implementación de los controles 5.1.1 – 5.1.2 – 6.1.1 -6.1.2 9.1.1 -9.1.2 – -11.1.1 - 11.1.2	Gestión de contraseñas de usuarios.	**Proyecto 1**- Control de acceso físico y protección de la información (Áreas seguras y seguridad de equipos).Ver numeral 11.1. **Proyecto 6–** Seguimiento y cumplimiento de la política de Seguridad de la información de la Entidad. Ver numeral 11.1
		[E.18] Destrucción de la información				
		[A.6] Abuso de privilegios de acceso			Conjunto de políticas para la seguridad de la información.	
		[A.7] uso no previsto				
		[A.11] Acceso no autorizado			Concientización, educación y capacitación en seguridad de la información.	
		[A.19] revelación de información				
		[A.5] suplantación de la identidad del usuario	Medio	Se mitiga el riesgo con la implementación de los controles 9.1.1 - 9.1.2 - 9.2.4 - 9.2.5 -11.1.1 - 11.1.2 - 11.1.3 - 11.1.4. -11.1.5 - 11.1.6 - 11.2.2 11.2.3	Política de control de acceso. Política de derechos de acceso asignados a usuarios.	**Proyecto 3-** Implementación y seguimiento de registros de actividad. Ver numeral 11.1 **Proyecto 4–** Control de acceso y responsabilidades de los usuarios a los sistemas y aplicaciones. Ver numeral 11.1
	Pérdida de Autenticidad, en el comportamiento, resultado o uso del activo de información	[A.5] suplantación de la identidad del usuario	Alto	Se mitiga el riesgo con la implementación de los controles 9.1.1 - 9.1.2 - 9.2.4 - 9.2.5 -11.1.1 - 11.1.2 - 11.1.3 - 11.1.4. -11.1.5 - 11.1.6 - 11.2.2 11.2.3	Política de control de acceso. Política de derechos de acceso asignados a usuarios.	**Proyecto 3-** Implementación y seguimiento de registros de actividad. Ver numeral 11.1 **Proyecto 4–** Control de acceso y responsabilidades de los usuarios a los sistemas y aplicaciones. Ver numeral 11.1
Portal Académico	Pérdida de Disponibilidad del activo de información	[E.4] Errores de configuración	Muy Alto	Se mitiga el riesgo con la implementación de los controles 5.1.1 – 5.1.2 – 6.1.1 -6.1.2 – 6.1.3 – 6.1.4 – 6.1.5 – 8.1.1 - 8.1.2 – 8.1.3 – 8.1.4 – 9.1.1 -9.1.2 – 9.2.1 - 9.2.2 - 9.2.3 - 9.2.4 - 9.2.5 - 9.2.6 - 9.3.1 - 9.4.1 - 9.4.2 - 9.4.3 -9.4.4 - 9.4.5 10.1.2 - 12.1.1 - 12.1.2 - 12.1.3 - 12.1.4 - 12.2.1 - 12.3.1 -12.4.1 - 12.4.2 - 12.4.3 - 12.4.4 - 12.5.1 - 12.6.1	Responsabilidades y procedimientos.	**Proyecto 2-** Responsabilidades y proyectos de operación. Ver numeral 11.1 **Proyecto 3-** Implementación y seguimiento de registros de actividad. Ver numeral 11.1. **Proyecto 7-** Gestión de incidentes de Seguridad de la Información. Ver numeral 11.1
		[E.2] Errores del administrador del sistema / de la seguridad [E.24] caída del sistema por agotamiento de recursos	Alto	Se mitiga el riesgo con la implementación de los controles 5.1.1 – 5.1.2 – 6.1.1 -6.1.2 – 6.1.3 – 6.1.4 – 6.1.5 – 8.1.1 - 8.1.2 – 8.1.3 – 8.1.4 – 9.1.1 -9.1.2 – 9.2.1 - 9.2.2 - 9.2.3 - 9.2.4 - 9.2.5 - 9.2.6 - 9.3.1 - 9.4.1 - 9.4.2 - 9.4.3 -9.4.4 - 9.4.5 10.1.2 - 12.1.1 - 12.1.2 - 12.1.3 - 12.1.4 - 12.2.1 - 12.3.1 -12.4.1 - 12.4.2 - 12.4.3 - 12.4.4 - 12.5.1 - 12.6.1 - 12.6.2 - 12.7.1- 16.1.1 – 16.1.2 – 16.1.3 – 16.1.4 – 16.1.5 – 16.1.6 – 16.1.7	Gestión de acceso a usuarios. Manual de política de seguridad y controles básicos y específicos para el manejo de la información. Planificación de la continuidad de la seguridad de la información.	**Proyecto 2-** Responsabilidades y proyectos de operación. Ver numeral 11.1. **Proyecto 3-** Implementación y seguimiento de registros de actividad. Ver numeral 11.1 **Proyecto 4**– Control de acceso y responsabilidades de los usuarios a los sistemas y aplicaciones. Ver numeral

Tabla 33. (Continuación)

ACTIVOS	RIESGO	AMENAZAS	VALOR	TRATAMIENTO DE RIESGO	CONTROLES IMPLEMENTADOS	PROYECTOS DEFINIDOS
Portal Académico	Pérdida de Disponibilidad del activo de información	[A.5] suplantación de la identidad del usuario	Alto	Se mitiga el riesgo con la implementación de los controles 5.1.1 – 5.1.2 – 6.1.1 -6.1.2 – 6.1.3 – 6.1.4 – 6.1.5 – 8.1.1 - 8.1.2 – 8.1.3 – 8.1.4 – 9.1.1 -9.1.2 – 9.2.1 - 9.2.2 - 9.2.3 - 9.2.4 - 9.2.5 - 9.2.6 - 9.3.1 - 9.4.1 - 9.4.2 - 9.4.3 -9.4.4 - 9.4.5 10.1.2 - 12.1.1 - 12.1.2 - 12.1.3 - 12.1.4 - 12.2.1 - 12.3.1 -12.4.1 - 12.4.2 - 12.4.3 - 12.4.4 - 12.5.1 - 12.6.1 - 12.6.2 - 12.7.1- 16.1.1 – 16.1.2 – 16.1.3 – 16.1.4 – 16.1.5 – 16.1.6 – 16.1.7	Copias de seguridad de la información.	**Proyecto 6–** Seguimiento y cumplimiento de la política de Seguridad de la información de la Entidad. Ver numeral 11.1 **Proyecto 7-** Gestión de incidentes de Seguridad de la información. Ver numeral 11.1
		[A.8] Difusión de software dañino			Registro y gestión de eventos de seguridad.	
		[A.11] Acceso no autorizado			Responsabilidades y procedimientos ante incidentes de seguridad	
		[A.24] Denegación de servicio			Control contra código malicioso. Registro y gestión de eventos de seguridad.	
		[E.3] Errores de monitorización (log)	Medio	Se mitiga el riesgo con la implementación de los controles 5.1.1 – 5.1.2 – 6.1.1 -6.1.2 – 6.1.3 – 6.1.4 – 6.1.5 – 8.1.1 - 8.1.2 – 8.1.3 – 8.1.4 – 9.1.1 -9.1.2 – 9.2.1 - 9.2.2 - 9.2.3 - 9.2.4 - 9.2.5 - 9.2.6 - 9.3.1 - 9.4.1 - 9.4.2 - 9.4.3 -9.4.4 - 9.4.5 10.1.2 - 11.1.1 - 11.1.2 - 11.1.3 - 11.1.4 - 11.1.5 - 11.1.6 -11.2.2 - 11.2.3 - 12.1.1 - 12.1.2 - 12.1.3 - 12.1.4 - 12.2.1 - 12.3.1 - 12.4.1 - 12.4.2 - 12.4.3 - 12.4.4 - 12.5.1 - 12.6.1 - 12.6.2 - 12.7.1- 1 - 17.1.1 - 17.1.2 - 17.1.3 - 17.2.1.	Política de control de acceso. Restricción de acceso a la información. Proceso disciplinario. Restricciones a los cambios en los paquetes de software.	**Proyecto 1-** Control de acceso físico y protección de la información (Áreas Seguras y seguridad de equipos)
		[E.18] Destrucción de la información				**Proyecto 2-** Responsabilidades y proyectos de operación.
		[E.20] vulnerabilidades de los programas (software)				**Proyecto 3-** Implementación y seguimiento de registros de actividad.
		[E.21] Errores de mantenimiento / actualización de programas (software)				
		[E.28] Indisponibilidad del personal				
		[A.6] Abuso de privilegios de acceso				
		[A.15] Modificación de la información				**Proyecto 5-** Adaptación plan de contingencia TICS, como marco de Gestión del Plan de Continuidad del Negocio

Tabla 33. (Continuación)

ACTIVOS	RIESGO	AMENAZAS	VALOR	TRATAMIENTO DE RIESGO	CONTROLES IMPLEMENTADOS	PROYECTOS DEFINIDOS
Portal Académico	Pérdida de Disponibilidad del activo de información	[A.18] Destrucción de la información				**Proyecto 5-** Adaptación plan de contingencia TICS, como marco de Gestión del Plan de Continuidad del Negocio
		[A.22] Manipulación de programas				
	Pérdida de la Integridad de la información, lo que implica el acceso indebido o fraudulento al activo de información	[E.4] Errores de configuración	Muy Alto	Se mitiga el riesgo con la implementación de los controles 5.1.1 – 5.1.2 – 6.1.1 -6.1.2 – 6.1.3 – 6.1.4 – 6.1.5 – 8.1.1 - 8.1.2 – 8.1.3 – 8.1.4 – 9.1.1 -9.1.2 – 10.1.2 -11.1.1 - 11.1.2 - 11.1.3 - 11.1.4. -11.1.5 - 11.1.6 - 11.2.2 11.2.3	Manual de política de seguridad y controles básicos y específicos para el manejo de la información. Política de control de acceso.	**Proyecto 1-** Control de acceso físico y protección de la información (Áreas seguras y seguridad de equipos).Ver numeral 11.1. **Proyecto 6–** Seguimiento y cumplimiento de la política de Seguridad de la información de la Entidad. Ver numeral 11.1
		[E.2] Errores del administrador del sistema / de la seguridad	Alto	Se mitiga el riesgo con la implementación de los controles 9.1.1 - 9.1.2 - 9.2.4 - 9.2.5 -11.1.1 - 11.1.2 - 11.1.3 - 11.1.4. -11.1.5 - 11.1.6 - 11.2.2 11.2.3 - 12.2.1	Gestión de acceso a usuarios. Registro y gestión de eventos de seguridad.	**Proyecto 1-** Control de acceso físico y protección de la información (Áreas Seguras y seguridad de equipos). Ver numeral 11.1
		[E.24] caída del sistema por agotamiento de recursos			Gestión de derechos de acceso asignados a usuarios.	**Proyecto 3-** Implementación y seguimiento de registros de actividad. Ver numeral 11.1 **Proyecto 4–** Control de acceso y responsabilidades de los usuarios a los sistemas y aplicaciones. Ver numeral 11.1
		[A.5] suplantación de la identidad del usuario			Gestión de contraseñas de usuarios.	
		[A.8] Difusión de software dañino			Proceso disciplinario.	
		[A.11] Acceso no autorizado			Responsabilidades y procedimientos ante incidentes de seguridad.	
		[A.24] Denegación de servicio			Control contra código malicioso.	

Tabla 33. (Continuación)

ACTIVOS	RIESGO	AMENAZAS	VALOR	TRATAMIENTO DE RIESGO	CONTROLES IMPLEMENTADOS	PROYECTOS DEFINIDOS
Portal Académico	Pérdida de la Integridad de la información, lo que implica el acceso indebido o fraudulento al activo de información	[E.3] Errores de monitorización (log)	Medio	Se mitiga el riesgo con la implementación de los controles 5.1.1 – 5.1.2 – 6.1.1 -6.1.2 – 6.1.3 – 6.1.4 – 6.1.5 – 8.1.1 - 8.1.2 – 8.1.3 – 8.1.4 – 9.1.1 -9.1.2 – 10.1.2 -11.1.1 - 11.1.2 - 11.1.3 - 11.1.4. -11.1.5 - 11.1.6 - 11.2.2 11.2.3 - 12.4.1 -12.4.2	Política de control de acceso.	**Proyecto 3-** Implementación y seguimiento de registros de actividad. Ver numeral 11.1 **Proyecto 4–** Control de acceso y responsabilidades de los usuarios a los sistemas y aplicaciones. Ver numeral 11.1
		[E.18] Destrucción de la información				
		[E.20] vulnerabilidades de los programas (software)			Restricción de acceso a la información	
		[E.21] Errores de mantenimiento / actualización de programas (software)			Proceso disciplinario.	
		[E.28] Indisponibilidad del personal			Restricciones a los cambios en los paquetes de software.	
		[A.6] Abuso de privilegios de acceso			Registro de eventos	
		[A.15] Modificación de la información			Protección de la información de registro	
		[A.18] Destrucción de la información				
		[A.22] Manipulación de programas				

Tabla 33. (Continuación)

ACTIVOS	RIESGO	AMENAZAS	VALOR	TRATAMIENTO DE RIESGO	CONTROLES IMPLEMENTADOS	PROYECTOS DEFINIDOS
Portal Académico	Pérdida de la Confidencialidad, acceso no autorizado que permite la utilización indebida o no autorizada del activo de información	[A.5] suplantación de la identidad del usuario [A.8] Difusión de software dañino [A.11] Acceso no autorizado	Muy Alto	Se mitiga el riesgo con la implementación de los controles 9.1.1 - 9.1.2 - 9.2.4 - 9.2.5 -11.1.1 - 11.1.2 - 11.1.3 - 11.1.4. -11.1.5 - 11.1.6 - 11.2.2 11.2.3	Gestión de acceso a usuarios. Gestión de derechos de acceso asignados a usuarios. Gestión de contraseñas de usuarios. Control contra código malicioso.	**Proyecto 3-** Implementación y seguimiento de registros de actividad. Ver numeral 11.1 **Proyecto 4–** Control de acceso y responsabilidades de los usuarios a los sistemas y aplicaciones. Ver numeral 11.1
Portal Institucional	Pérdida de Disponibilidad del activo de información	[E.4] Errores de configuración [E.20] vulnerabilidades de los programas (software) [E.24] caída del sistema por agotamiento de recursos [A.18] Destrucción de la información	Muy Alto	Se mitiga el riesgo con la implementación de los controles 5.1.1 – 5.1.2 – 6.1.1 -6.1.2 – 6.1.3 – 6.1.4 – 6.1.5 – 8.1.1 - 8.1.2 – 8.1.3 – 8.1.4 – 9.1.1 -9.1.2 – 9.2.1 - 9.2.2 - 9.2.3 - 9.2.4 - 9.2.5 - 9.2.6 - 9.3.1 - 9.4.1 - 9.4.2 - 9.4.3 -9.4.4 - 9.4.5 10.1.2 - 12.1.1 - 12.1.2 - 12.1.3 - 12.1.4 - 12.2.1 - 12.3.1 -12.4.1 - 12.4.2 - 12.4.3 - 12.4.4 - 12.5.1 - 12.6.1 - 12.6.2 - 12.7.1- 16.1.1 – 16.1.2 – 16.1.3 – 16.1.4 – 16.1.5 – 16.1.6 – 16.1.7	Gestión de acceso a usuarios. Copias de seguridad de la información. Registro y gestión de eventos de seguridad. Manual de política de seguridad y controles básicos y específicos para el manejo de la información. Planificación de la continuidad de la seguridad de la información.	**Proyecto 2-** Responsabilidades y proyectos de operación. Ver numeral 11.1. **Proyecto 3**- Implementación y seguimiento de registros de actividad. Ver numeral 11.1 **Proyecto 4–** Control de acceso y responsabilidades de los usuarios a los sistemas y aplicaciones. Ver numeral 11.1 **Proyecto 6–** Seguimiento y cumplimiento de la política de Seguridad de la información de la Entidad. Ver numeral 11.1 **Proyecto 7-** Gestión de incidentes de Seguridad de la información. Ver numeral 11.1
		[E.21] Errores de mantenimiento / actualización de programas (software)	Alto	Se mitiga el riesgo con la implementación de los controles 5.1.1 – 5.1.2 – 6.1.1 -6.1.2 – 6.1.3 – 6.1.4 – 6.1.5 – 8.1.1 - 8.1.2 – 8.1.3 – 8.1.4 – 9.1.1 -9.1.2 – 9.2.1 - 9.2.2 - 9.2.3 - 9.2.4 - 9.2.5 - 9.2.6 - 9.3.1 - 9.4.1 - 9.4.2 - 9.4.3 -9.4.4 - 9.4.5 10.1.2 - 12.1.1 - 12.1.2 - 12.1.3 - 12.1.4 - 12.2.1 - 12.3.1 -12.4.1 - 12.4.2 - 12.4.3 - 12.4.4 - 12.5.1 - 12.6.1 - 12.6.2 - 12.7.1- 16.1.1 – 16.1.2 – 16.1.3 – 16.1.4 – 16.1.5 – 16.1.6 – 16.1.7	Gestión de derechos de acceso asignados a usuarios. Cadena de suministro de tecnologías de la información y comunicaciones. Restricción de acceso a la información. Copias de seguridad de la información. Control contra código malicioso.	**Proyecto 2-** Responsabilidades y proyectos de operación. Ver numeral 11.1. **Proyecto 3-** Implementación y seguimiento de registros de actividad. Ver numeral 11.1. **Proyecto 4–** Control de acceso y responsabilidades de los usuarios a los sistemas y aplicaciones. Ver numeral 11.**1**

Tabla 33. (Continuación)

ACTIVOS	RIESGO	AMENAZAS	VALOR	TRATAMIENTO DE RIESGO	CONTROLES IMPLEMENTADOS	PROYECTOS DEFINIDOS
Portal Institucional	Pérdida de Disponibilidad del activo de información	[A.8] Difusión de software dañino	Alto	Se mitiga el riesgo con la implementación de los controles 5.1.1 – 5.1.2 – 6.1.1 -6.1.2 – 6.1.3 – 6.1.4 – 6.1.5 – 8.1.1 - 8.1.2 – 8.1.3 – 8.1.4 – 9.1.1 -9.1.2 – 9.2.1 - 9.2.2 - 9.2.3 - 9.2.4 - 9.2.5 - 9.2.6 - 9.3.1 - 9.4.1 - 9.4.2 - 9.4.3 -9.4.4 - 9.4.5 10.1.2 - 12.1.1 - 12.1.2 - 12.1.3 - 12.1.4 - 12.2.1 - 12.3.1 -12.4.1 - 12.4.2 - 12.4.3 - 12.4.4 - 12.5.1 - 12.6.1 - 12.6.2 - 12.7.1- 16.1.1 – 16.1.2 – 16.1.3 – 16.1.4 – 16.1.5 – 16.1.6 – 16.1.7	Gestión de derechos de acceso asignados a usuarios. Cadena de suministro de tecnologías de la información y comunicaciones. Restricción de acceso a la información. Copias de seguridad de la información. Control contra código malicioso.	**Proyecto 6–** Seguimiento y cumplimiento de la política de Seguridad de la información de la Entidad. Ver numeral 11.1
		[A.24] Denegación de servicio				**Proyecto 7-** Gestión de incidentes de Seguridad de la información. Ver numeral 11.1
		[E.2] Errores del administrador del sistema / de la seguridad	Medio	Se mitiga el riesgo con la implementación de los controles 12.1.1 - 12.1.2 - 12.1.3 - 12.1.4 - 12.2.1.	Copias de seguridad de la información.	**Proyecto 2-** Responsabilidades y proyectos de operación. Ver numeral 11.1.
	Pérdida de la Integridad de la información, lo que implica el acceso indebido o fraudulento al activo de información	[E.4] Errores de configuración	Muy Alto	Se mitiga el riesgo con la implementación de los controles 5.1.1 – 5.1.2 – 6.1.1 -6.1.2 – 6.1.3 – 6.1.4 – 6.1.5 – 8.1.1 - 8.1.2 – 8.1.3 – 8.1.4 – 9.1.1 -9.1.2 – 10.1.2 -11.1.1 - 11.1.2 - 11.1.3 - 11.1.4. -11.1.5 - 11.1.6 - 11.2.2 11.2.3	Manual de política de seguridad y controles básicos y específicos para el manejo de la información.	**Proyecto 1-** Control de acceso físico y protección de la información (Áreas seguras y seguridad de equipos).Ver numeral 11.1. **Proyecto 6–** Seguimiento y cumplimiento de la política de Seguridad de la información de la Entidad. Ver numeral 11.1
		[E.18] Destrucción de la información				
		[E.20] vulnerabilidades de los programas (software)			Política de control de acceso.	
		[E.24] caída del sistema por agotamiento de recursos			Control contra código malicioso.	
		[A.8] Difusión de software dañino			Restricciones a los cambios en los paquetes de software.	
		[A.11] Acceso no autorizado			Registro y gestión de eventos de seguridad.	
		[A.18] Destrucción de la información				
		[E.15] Alteración de la información	Alto	Se mitiga el riesgo con la implementación de los controles 9.1.1 -9.1.2 – 9.2.2 - 9.4.1 - 9.4.2 - 12.5.1	Gestión de acceso a usuarios. Gestión de derechos de acceso asignados a usuarios. Gestión de contraseñas de usuarios. Restricciones a los cambios en los paquetes de software.	**Proyecto 1-** Control de acceso físico y protección de la información (Áreas Seguras y seguridad de equipos)

Tabla 33. (Continuación)

ACTIVOS	RIESGO	AMENAZAS	VALOR	TRATAMIENTO DE RIESGO	CONTROLES IMPLEMENTADOS	PROYECTOS DEFINIDOS
Portal Institucional	Pérdida de la Integridad de la información, lo que implica el acceso indebido o fraudulento al activo de información	[E.21] Errores de mantenimiento / actualización de programas (software)	Alto	Se mitiga el riesgo con la implementación de los controles 9.1.1 -9.1.2 – 9.2.2 - 9.4.1 - 9.4.2 - 12.5.1	Gestión de acceso a usuarios. Gestión de derechos de acceso asignados a usuarios. Gestión de contraseñas de usuarios. Restricciones a los cambios en los paquetes de software.	**Proyecto 1-** Control de acceso físico y protección de la información (Áreas Seguras y seguridad de equipos)
		[E.2] Errores del administrador del sistema / de la seguridad	Medio	Se mitiga el riesgo con la implementación de los controles 9.1.1 - 9.1.2 -9.4.1 - 9.4.2	Gestión de derechos de acceso asignados a usuarios. Restricciones a los cambios en los paquetes de software.	**Proyecto 4-** Control de acceso y responsabilidades de los usuarios a los sistemas de información
		[A.15] Modificación de la información				
	Pérdida de Autenticidad, en el comportamiento, resultado o uso del activo de información	[A.11] Acceso no autorizado	Medio	Se mitiga el riesgo con la implementación de los controles 9.1.1 -9.1.2 – 9.2.2 - 9.4.1 - 9.4.2 - 12.5.1	Gestión de acceso a usuarios. Gestión de derechos de acceso asignados a usuarios. Gestión de contraseñas de usuarios.	**Proyecto 1-** Control de acceso físico y protección de la información (Áreas Seguras y seguridad de equipos)
Controlador de dominio secundario	Pérdida de Disponibilidad del activo de información	[E.2] Errores del administrador del sistema / de la seguridad	Alto	Se mitiga el riesgo con la implementación de los controles 5.1.1 – 5.1.2 – 6.1.1 -6.1.2 – 6.1.3 – 6.1.4 – 6.1.5 – 8.1.1 - 8.1.2 – 8.1.3 – 8.1.4 – 9.1.1 -9.1.2 – 9.2.1 - 9.2.2 - 9.2.3 - 9.2.4 - 9.2.5 - 9.2.6 - 9.3.1 - 9.4.1 - 9.4.2 - 9.4.3 -9.4.4 - 9.4.5 10.1.2 - 12.1.1 - 12.1.2 - 12.1.3 - 12.1.4 - 12.2.1 - 12.3.1 -12.4.1 - 12.4.2 - 12.4.3 - 12.4.4 - 12.5.1 - 12.6.1 - 12.6.2 - 12.7.1- 16.1.1 – 16.1.2 – 16.1.3 – 16.1.4 –	Manual de política de seguridad y controles básicos y específicos para el manejo de la información. Planificación de la continuidad de la seguridad de la información. Copias de seguridad de la información. Registro y gestión de eventos de seguridad.	**Proyecto 2-** Responsabilidades y proyectos de operación. Ver numeral 11.1. **Proyecto 6–** Seguimiento y cumplimiento de la política de Seguridad de la información de la Entidad. Ver numeral 11.1 **Proyecto 7-** Gestión de incidentes de Seguridad de la información. Ver numeral 11.1
		[E.4] Errores de configuración	Medio	Se mitiga el riesgo con la implementación de los controles 12.4.3 - 12.5.1 - 17.1.1	Restricciones a los cambios en los paquetes de software.	**Proyecto 3-** Implementación y seguimiento de registros de actividad. Ver anexo 11.1.1
		[E.21] Errores de mantenimiento / actualización de programas (software)				

Tabla 33. (Continuación)

ACTIVOS	RIESGO	AMENAZAS	VALOR	TRATAMIENTO DE RIESGO	CONTROLES IMPLEMENTADOS	PROYECTOS DEFINIDOS
Controlador de dominio secundario	Pérdida de la Integridad de la información, lo que implica el acceso indebido o fraudulento al activo de información	[E.2] Errores del administrador del sistema / de la seguridad	Muy Alto	Se mitiga el riesgo con la implementación de los controles 5.1.1 – 5.1.2 – 6.1.1 -6.1.2 – 6.1.3 – 6.1.4 – 6.1.5 – 8.1.1 - 8.1.2 – 8.1.3 – 8.1.4 – 9.1.1 -9.1.2 – 10.1.2 -11.1.1 - 11.1.2 - 11.1.3 - 11.1.4. -11.1.5 - 11.1.6 - 11.2.2 11.2.3	Manual de política de seguridad y controles básicos y específicos para el manejo de la información. Política de control de acceso.	**Proyecto 1-** Control de acceso físico y protección de la información (Áreas seguras y seguridad de equipos).Ver numeral 11.1. **Proyecto 6–** Seguimiento y cumplimiento de la política de Seguridad de la información de la Entidad. Ver numeral 11.1
		[E.4] Errores de configuración	Alto	Se mitiga el riesgo con la implementación de los controles 5.1.1 – 5.1.2 – 6.1.1 -6.1.2 – 6.1.3 – 6.1.4 – 6.1.5 – 8.1.1 - 8.1.2 – 8.1.3 – 8.1.4 – 9.1.1 -9.1.2 – 9.2.1 - 9.2.2 - 9.2.3 - 9.2.4 - 9.2.5 - 9.2.6 - 9.3.1 - 9.4.1 - 9.4.2 - 9.4.3 -9.4.4 - 9.4.5 10.1.2 - 12.1.1 - 12.1.2 - 12.1.3 - 12.1.4 - 12.2.1 - 12.3.1 -12.4.1 - 12.4.2 - 12.4.3 - 12.4.4 - 12.5.1 - 12.6.1 - 12.6.2 - 12.7.1- 16.1.1 – 16.1.2 – 16.1.3 – 16.1.4 –	Restricciones a los cambios en los paquetes de software.	**Proyecto 2-** Responsabilidades y proyectos de operación. Ver numeral 11.1. **Proyecto 6–** Seguimiento y cumplimiento de la política de Seguridad de la información de la Entidad. Ver numeral 11.1 **Proyecto 7-** Gestión de incidentes de Seguridad de la información. Ver numeral 11.1
		[E.21] Errores de mantenimiento / actualización de programas (software)				
	Pérdida de Disponibilidad del activo de información	[N.*] Desastres naturales	Alto	Se mitiga el riesgo con la implementación de los controles 11.1.1 - 11.1.2 - 11.1.3 - 11.1.4 - 11.1.5 - 11.1.6 - 11.2.2. - 11.2.3 - 16.1.2 - 17.1. - 17.1.2 - 17.1.3 - 17.2.1	Manipulación de los activos.	**Proyecto 1-** Control de acceso físico y protección de la información (Áreas Seguras y seguridad de equipos). Ver anexo 11.1
		[I.1] Fuego			Política de control de acceso.	
		[I.2] Daños por agua			Protección contra las amenazas externas y ambientales.	
		[I.5] Avería de origen físico o lógico			Registros de actividad del administrador y operador de los sistemas.	**Proyecto 5-** Adaptación plan de contingencia TICS, como marco de Gestión del Plan de Continuidad del Negocio. Ver anexo 11.1 **Proyecto 7-** Gestión de incidentes de Seguridad de la Información. Ver anexo 11.1
		[I.6] Corte del suministro eléctrico			Respuesta a los incidentes de seguridad.	

Tabla 33. (Continuación)

ACTIVOS	RIESGO	AMENAZAS	VALOR	TRATAMIENTO DE RIESGO	CONTROLES IMPLEMENTADOS	PROYECTOS DEFINIDOS
Sistema de Acceso Biométrico	Pérdida de Disponibilidad del activo de información	[A.25] Robo de equipos	Alto	Se mitiga el riesgo con la implementación de los controles 11.1.1 - 11.1.2 - 11.1.3 - 11.1.4 - 11.1.5 - 11.1.6 - 11.2.2. - 11.2.3 - 16.1.2 - 17.1. - 17.1.2 - 17.1.3 - 17.2.1	Cadena de suministro en tecnologías de la información y comunicaciones.	**Proyecto 5-** Adaptación plan de contingencia TICS, como marco de Gestión del Plan de Continuidad del Negocio. Ver anexo 11.1 **Proyecto 7-** Gestión de incidentes de Seguridad de la Información. Ver anexo 11.1
		[A.26] Ataque destructivo			Implantación de la continuidad de la seguridad de la información.	
	Pérdida de Autenticidad, en el comportamiento, resultado o uso del activo de información	[N.*] Desastres naturales	Alto	Se mitiga el riesgo con la implementación de los controles 9.1.1 - 9.2.2 - 9.2.3 -11.1.1 - 11.1.2 - 11.1.3 - 11.1.4 - 11.1.5 - 11.1.6 - 11.2.2. - 11.2.3 - - 15.1.1 15.1.3 - 15.2.1 -16.1.2 - 17.1. - 17.1.2 - 17.1.3 - 17.2.1	Política de control de acceso. Propiedad de los activos.	**Proyecto 1-** Control de acceso físico y protección de la información (Áreas Seguras y seguridad de equipos). Ver anexo 11.1 **Proyecto 5-** Adaptación plan de contingencia TICS, como marco de Gestión del Plan de Continuidad del Negocio. Ver anexo 11.1 **Proyecto 7-** Gestión de incidentes de Seguridad de la Información. Ver anexo 11.1
		[I.1] Fuego			Gestión de derechos de acceso con privilegios especiales.	
		[I.2] Daños por agua			Protección contra las amenazas externas y ambientales.	
		[I.5] Avería de origen físico o lógico			Registros de actividad del administrador y operador de los sistemas.	
		[I.6] Corte del suministro eléctrico			Respuesta a los incidentes de seguridad.	
		[A.25] Robo de equipos			Cadena de suministro en tecnologías de la información y comunicaciones.	
		[A.26] Ataque destructivo			Implantación de la continuidad de la seguridad de la información.	
Canal de internet y red MPLS	Pérdida de Disponibilidad del activo de información	[I.6] Corte del suministro eléctrico	Muy Alto	Se mitiga el riesgo con la implementación de los controles 5.1.1 – 5.1.2 – 6.1.1 -6.1.2 – 6.1.3 – 6.1.4 – 6.1.5 – 8.1.1 - 8.1.2 – 12.1.1 - 12.1.2 - 12.1.3 - 12.1.4 - 12.2.1 -	Responsabilidades y procedimientos.	**Proyecto 2-** Responsabilidades y proyectos de operación. Ver numeral 11.1

Tabla 33. (Continuación)

ACTIVOS	RIESGO	AMENAZAS	VALOR	TRATAMIENTO DE RIESGO	CONTROLES IMPLEMENTADOS	PROYECTOS DEFINIDOS
Canal de internet y red MPLS	Pérdida de Disponibilidad del activo de información	[I.8.12] Interrupción deliberada por un agente externo	Muy Alto	Se mitiga el riesgo con la implementación de los controles 5.1.1 – 5.1.2 – 6.1.1 -6.1.2 – 6.1.3 – 6.1.4 – 6.1.5 – 8.1.1 - 8.1.2 – 12.1.1 - 12.1.2 - 12.1.3 - 12.1.4 - 12.2.1 -	Conjunto de políticas para la seguridad de la información.	**Proyecto 7-** Gestión de incidentes de Seguridad de la Información
		[A.25] Robo de equipos				
		[N.1] Fuego	Alto	Se mitiga el riesgo con la implementación de los controles 11.1.1 - 11.1.2 - 11.1.3 - 11.1.4 - 11.1.5 - 11.1.6 - 11.2.2. - 11.2.3 - 16.1.2 - 17.1. - 17.1.2 - 17.1.3 - 17.2.1	Protección contra amenazas externas y ambientales. Implementación de la continuidad de la seguridad de la información.	**Proyecto 5-** Adaptación plan de contingencia TICS, como marco de Gestión del Plan de Continuidad del Negocio. Ver anexo 11.1 **Proyecto 7-** Gestión de incidentes de Seguridad de la Información. Ver anexo 11.1
		[N.2] Daños por agua				
		[N.*] Desastres naturales				
		[I.1] Fuego				
		[I.5] Avería de origen físico o lógico				
		[I.7] Condiciones inadecuadas de temperatura o humedad				
		[E.4] Errores de configuración				
		[E.24] caída del sistema por agotamiento de recursos				
		[E.23] Errores de mantenimiento / actualización de equipos (hardware)	Medio	Se mitiga el riesgo con la implementación de los controles 5.1.1 – 5.1.2 – 6.1.1 -6.1.2 – 6.1.3 – 6.1.4 – 6.1.5 – 8.1.1 - 8.1.2 – 12.1.1 - 12.1.2 - 12.1.3 - 12.1.4 - 12.2.1 -	Cadena de suministro en tecnologías de la información y comunicaciones.	**Proyecto 5-** Adaptación plan de contingencia TICS, como marco de Gestión del Plan de Continuidad del Negocio. Ver anexo 11.1 **Proyecto 7-** Gestión de incidentes de Seguridad de la Información. Ver anexo 11.1

Fuente: el autor

10.2 Plan Tratamiento de Riesgos: [SW] APLICACIONES

Tabla 37. Plan tratamiento de riesgos: aplicaciones

ACTIVOS	RIESGO	AMENAZAS	VALOR	TRATAMIENTO DE RIESGO	CONTROLES IMPLEMENTADOS	PROYECTOS DEFINIDOS
Software de Aplicaciones (medios)	Pérdida de Disponibilidad del activo de información	[N.1] Fuego [I.5] Avería de origen físico o lógico [A.7] uso no previsto	Alto	Se mitiga el riesgo con la implementación de los controles 9.2.2-11.1.4 - 11.2.4 - 12.4.1 - 12.6.1 - 16.1.4 - 16.1.5	Suministro de acceso de usuarios. Protección contra amenazas externas y ambientales. Mantenimiento de equipos. Registro de eventos. Gestión de las vulnerabilidades técnicas. Evaluación de eventos de seguridad de la información y decisiones sobre ellos. Respuesta a incidentes de seguridad de la información.	**Proyecto 1-** Control de acceso físico y protección de la información (Áreas seguras y seguridad de equipos).Ver numeral 11.1 **Proyecto 3-** Implementación y seguimiento de registro de actividad. Ver numeral 11.1 **Proyecto 7-** Gestión de incidentes de Seguridad de la Información.
	Pérdida de la Integridad de la información, lo que implica el acceso indebido o fraudulento al activo de información	[N.1] Fuego [I.5] Avería de origen físico o lógico [A.7] uso no previsto	Alto	Se mitiga el riesgo con la implementación de los controles 9.2.2-11.1.4 - 11.2.4 - 12.4.1 - 12.6.1 - 16.1.4 - 16.1.5	Suministro de acceso de usuarios. Protección contra amenazas externas y ambientales. Mantenimiento de equipos Registro de eventos. Gestión de las vulnerabilidades técnicas. Evaluación de eventos de seguridad de la información y decisiones sobre ellos. Respuesta a incidentes de seguridad de la información.	**Proyecto 1-** Control de acceso físico y protección de la información (Áreas seguras y seguridad de equipos).Ver numeral 11.1 **Proyecto 3-** Implementación y seguimiento de registros de actividad. Ver numeral 11.1 **Proyecto 7-** Gestión de incidentes de Seguridad de la Información.
Software de Sistemas operativos (medios)	Pérdida de Disponibilidad del activo de información	[N.1] Fuego [I.5] Avería de origen físico o lógico [A.7] uso no previsto	Alto	Se mitiga el riesgo con la implementación de los controles 9.2.2-11.1.4 - 11.2.4 - 12.4.1 - 12.6.1 - 16.1.4 - 16.1.5	Suministro de acceso de usuarios. Protección contra amenazas externas y ambientales. Mantenimiento de equipos. Registro de eventos. Gestión de las vulnerabilidades técnicas. Evaluación de eventos de seguridad de la información y decisiones sobre ellos. Respuesta a incidentes de seguridad de la información.	**Proyecto 1-** Control de acceso físico y protección de la información (Áreas seguras y seguridad de equipos).Ver numeral 11.1 **Proyecto 3-** Implementación y seguimiento de registros de actividad. Ver numeral 11.1 **Proyecto 7-** Gestión de incidentes de Seguridad de la Información.

Tabla 34. (Continuación)

ACTIVOS	RIESGO	AMENAZAS	VALOR	TRATAMIENTO DE RIESGO	CONTROLES IMPLEMENTADOS	PROYECTOS DEFINIDOS
Software de Sistemas operativos (medios)	Pérdida de la Integridad de la información, lo que implica el acceso indebido o fraudulento al activo de información	[N.1] Fuego [I.5] Avería de origen físico o lógico [A.7] uso no previsto	Alto	Se mitiga el riesgo con la implementación de los controles 9.2.2-11.1.4 - 11.2.4 - 12.4.1 - 12.6.1 - 16.1.4 - 16.1.5	Suministro de acceso de usuarios. Protección contra amenazas externas y ambientales. Mantenimiento de equipos. Registro de eventos. Gestión de las vulnerabilidades técnicas. Evaluación de eventos de seguridad de la información y decisiones sobre ellos. Respuesta a incidentes de seguridad de la información.	**Proyecto 1- C**ontrol de acceso físico y protección de la información (Áreas seguras y seguridad de equipos).Ver numeral 11.1 **Proyecto 3-** Implementación y seguimiento de registros de actividad. Ver numeral 11.1 **Proyecto 7-** Gestión de incidentes de Seguridad de la Información.
Software de Base de Datos (medios)	Pérdida de Disponibilidad del activo de información	[N.1] Fuego [I.5] Avería de origen físico o lógico [A.7] uso no previsto	Alto	Se mitiga el riesgo con la implementación de los controles 9.2.2-11.1.4 - 11.2.4 - 12.4.1 - 12.6.1 - 16.1.4 - 16.1.5	Suministro de acceso de usuarios. Protección contra amenazas externas y ambientales. Mantenimiento de equipos. Registro de eventos. Gestión de las vulnerabilidades técnicas. Evaluación de eventos de seguridad de la información y decisiones sobre ellos. Respuesta a incidentes de seguridad de la información.	**Proyecto 1-** Control de acceso físico y protección de la información (Áreas seguras y seguridad de equipos).Ver numeral 11.1 **Proyecto 3-** Implementación y seguimiento de registros de actividad. Ver numeral 11.1 **Proyecto 7-** Gestión de incidentes de Seguridad de la Información.
Medios con claves de licenciamiento	Pérdida de Disponibilidad del activo de información	[N.1] Fuego [I.5] Avería de origen físico o lógico [A.7] uso no previsto	Alto	Se mitiga el riesgo con la implementación de los controles 9.2.2-11.1.4 - 11.2.4 - 12.4.1 - 12.6.1 - 16.1.4 - 16.1.5	Suministro de acceso de usuarios. Protección contra amenazas externas y ambientales. Mantenimiento de equipos. Registro de eventos. Gestión de las vulnerabilidades técnicas. Evaluación de eventos de seguridad de la información y decisiones sobre ellos. Respuesta a incidentes de seguridad de la información.	**Proyecto 1-** Control de acceso físico y protección de la información (Áreas seguras y seguridad de equipos).Ver numeral 11.1 **Proyecto 3-** Implementación y seguimiento de registros de actividad. Ver numeral 11.1 **Proyecto 7-** Gestión de incidentes de Seguridad de la Información.
	Pérdida de la Integridad de la información, lo que implica el acceso indebido o fraudulento al activo de información	[N.1] Fuego [N.2] Daños por agua [I.5] Avería de origen físico o lógico [A.7] uso no previsto	Alto	Se mitiga el riesgo con la implementación de los controles 9.2.2-11.1.4 - 11.2.4 - 12.4.1 - 12.6.1 - 16.1.4 - 16.1.5	Suministro de acceso de usuarios. Protección contra amenazas externas y ambientales. Mantenimiento de equipos. Registro de eventos. Gestión de las vulnerabilidades técnicas. Evaluación de eventos de seguridad de la información y decisiones sobre ellos. Respuesta a incidentes de seguridad de la información.	**Proyecto 1-** Control de acceso físico y protección de la información (Áreas seguras y seguridad de equipos).Ver numeral 11.1 **Proyecto 3-** Implementación y seguimiento de registros de actividad. Ver numeral 11.1 **Proyecto 7-** Gestión de incidentes de Seguridad de la Información.

Tabla 34. (Continuación)

ACTIVOS	RIESGO	AMENAZAS	VALOR	TRATAMIENTO DE RIESGO	CONTROLES IMPLEMENTADOS	PROYECTOS DEFINIDOS
Aplicación SIMI – AP	Pérdida de Disponibilidad del activo de información	[E.15] Alteración de la información [E.20.dos] Denegación de Servicio	Muy Alto	Se mitiga el riesgo con la implementación de los controles 8.2.2 - 9.1.1- 9.1.1 - 9.2.1 - 9.2.2 - 9.2.5- 11.1.4	Suministro de acceso de usuarios. Protección contra amenazas externas y ambientales. Mantenimiento de equipos. Registro de eventos. Gestión de las vulnerabilidades técnicas. Evaluación de eventos de seguridad de la información y decisiones sobre ellos. Respuesta a incidentes de seguridad de la información.	**Proyecto 1-** Control de acceso físico y protección de la información (Áreas seguras y seguridad de equipos).Ver numeral 11.1 **Proyecto 3-** Implementación y seguimiento de registros de actividad. Ver numeral 11.1 **Proyecto 7**- Gestión de incidentes de Seguridad de la Información.
		[E.2] Errores del administrador del sistema / de la seguridad [E.3] Errores de monitorización (log) [E.4] Errores de configuración	Alto	Se mitiga el riesgo con la implementación de los controles 12.1.1 - 12.4.1 - 12.4.2 - 12.4.3	Procedimientos de operación documentados. Registro de eventos. Protección de la información de registro. Registros del administrador y del operador.	**Proyecto 2-** Responsabilidades y procedimientos de operación.
	Pérdida de la Integridad de la información, lo que implica el acceso indebido o fraudulento al activo de información	[E.1] Errores de los usuarios [E.15] Alteración de la información	Muy Alto	Se mitiga el riesgo con la implementación de los controles 8.2.2 - 9.1.1- 9.1.1 - 9.2.1 - 9.2.2 - 9.2.5- 11.1.4	Suministro de acceso de usuarios. Protección contra amenazas externas y ambientales. Mantenimiento de equipos. Registro de eventos. Gestión de las vulnerabilidades técnicas. Evaluación de eventos de seguridad de la información y decisiones sobre ellos. Respuesta a incidentes de seguridad de la información.	**Proyecto 1-** Control de acceso físico y protección de la información (Áreas seguras y seguridad de equipos).Ver numeral 11.1 **Proyecto 3-** Implementación y seguimiento de registros de actividad. Ver numeral 11.1 **Proyecto 7-** Gestión de incidentes de Seguridad de la Información. Ver numeral 11.1
	Pérdida de la Confidencialidad, acceso no autorizado que permite la utilización indebida o no autorizada del activo de información	[A.5.1] Por personal interno	Muy Alto	Se mitiga el riesgo con la implementación de los controles 7.1.1 - 8.1.3 - 8.2.3 - 9.1.1 - 9.1.2 - 9.2.3	Uso aceptable de los activos. Clasificación de la información. Política de control de acceso. Acceso a redes y a Servicios de red. Gestión de derechos de acceso privilegiado.	**Proyecto 3-** Implementación y seguimiento de registros de actividad. Ver numeral 11.1 **Proyecto 4-** Control de acceso y responsabilidades de los usuarios a los sistemas y aplicaciones. Ver numeral 11.1

Tabla 34. (Continuación)

ACTIVOS	RIESGO	AMENAZAS	VALOR	TRATAMIENTO DE RIESGO	CONTROLES IMPLEMENTADOS	PROYECTOS DEFINIDOS
Aplicación SIMI – AP	Pérdida de la Confidencialidad, acceso no autorizado que permite la utilización indebida o no autorizada del activo de información	[E.19.1] A personal interno que no necesita conocerlo [A.7.1] Por personal interno [A.15.1] Sin beneficio para nadie	Alto	Se mitiga el riesgo con la implementación de los controles 7.1.1 - 8.1.3 - 8.2.3 - 9.1.1 - 9.1.2 - 9.2.3	Uso aceptable de los activos. Clasificación de la información. Política de control de acceso. Acceso a redes y a Servicios de red. Gestión de derechos de acceso privilegiado.	**Proyecto 3-** Implementación y seguimiento de registros de actividad. Ver numeral 11.1 **Proyecto 4-** Control de acceso y responsabilidades de los usuarios a los sistemas y aplicaciones. Ver numeral 11.1
	Pérdida de Autenticidad, en el comportamiento, resultado o uso del activo de información	[E.1] Errores de los usuarios [E.15] Alteración de la información	Muy Alto	Se mitiga el riesgo con la implementación de los controles 8.2.2 - 9.1.1- 9.1.1 - 9.2.1 - 9.2.2 - 9.2.5- 11.1.4	Suministro de acceso de usuarios. Protección contra amenazas externas y ambientales. Mantenimiento de equipos. Registro de eventos. Gestión de las vulnerabilidades técnicas. Evaluación de eventos de seguridad de la información y decisiones sobre ellos. Respuesta a incidentes de seguridad de la información.	**Proyecto 1-** Control de acceso físico y protección de la información (Áreas seguras y seguridad de equipos).Ver numeral 11.1 **Proyecto 3-** Implementación y seguimiento de registros de actividad. Ver numeral 11.1 **Proyecto 7-** Gestión de incidentes de Seguridad de la Información. Ver numeral 11.1.
	Trazabilidad, pérdida de los registros de actividad en los activos informáticos	[E.15] Alteración de la información [E.28.4] Personal insuficiente	Muy Alto	Se mitiga el riesgo con la implementación de los controles 8.2.2 - 9.1.1- 9.1.1 - 9.2.1 - 9.2.2 - 9.2.5- 11.1.4	Suministro de acceso de usuarios. Protección contra amenazas externas y ambientales. Mantenimiento de equipos. Registro de eventos. Gestión de las vulnerabilidades técnicas. Evaluación de eventos de seguridad de la información y decisiones sobre ellos. Respuesta a incidentes de seguridad de la información.	**Proyecto 1-** Control de acceso físico y protección de la información (Áreas seguras y seguridad de equipos).Ver numeral 11.1 **Proyecto 3-** Implementación y seguimiento de registros de actividad. Ver numeral 11.1 **Proyecto 7-** Gestión de incidentes de Seguridad de la Información. Ver numeral 11.1.
Servidor aplicativo SPRAI	Pérdida de la Confidencialidad, acceso no autorizado que permite la utilización indebida o no autorizada del activo de información	[E.19.1] A personal interno que no necesita conocerlo	Muy Alto	Se mitiga el riesgo con la implementación de los controles 7.1.1 - 8.1.3 - 8.2.3 - 9.1.1 - 9.1.2 - 9.2.3	Uso aceptable de los activos. Clasificación de la información. Política de control de acceso. Acceso a redes y a Servicios de red. Gestión de derechos de acceso privilegiado.	**Proyecto 3-** Implementación y seguimiento de registros de actividad. Ver numeral 11.1 **Proyecto 4-** Control de acceso y responsabilidades de los usuarios a los sistemas y aplicaciones. Ver numeral 11.1
Consola Vcenter	Pérdida de Disponibilidad del activo de información	[N.1] Fuego [N.2] Daños por agua [I.1] Fuego [I.2] Daños por agua	Muy Alto	Se mitiga el riesgo con la implementación de los controles 11.1.3 11.1.4 - 11.1.5	Seguridad de oficinas, recinto e instalaciones. Protección contra amenazas externas y ambientales. Trabajo en áreas seguras.	**Proyecto 1-** Control de acceso físico y protección de la información (Áreas seguras y seguridad de equipos).Ver numeral 11.1

Tabla 34. (Continuación)

ACTIVOS	RIESGO	AMENAZAS	VALOR	TRATAMIENTO DE RIESGO	CONTROLES IMPLEMENTADOS	PROYECTOS DEFINIDOS
Consola Vcenter	Pérdida de Disponibilidad del activo de información	[E.24] caída del sistema por agotamiento de recursos [A.8] Difusión de software dañino [A.23] Manipulación del hardware [A.26] Ataque destructivo	Alto	Se mitiga el riesgo con la implementación de los controles 8.2.3 - 9.1.1 - 11.1.1 - 11.1.2 - 11.1.3 - 11.2.1 - 11.2.4 - 12.1.3 - 12.2.1	Seguridad de oficinas, recinto e instalaciones. Protección contra amenazas externas y ambientales. Trabajo en áreas seguras.	**Proyecto 1-** Control de acceso físico y protección de la información (Áreas seguras y seguridad de equipos).Ver numeral 11.1
		[E.2] Errores del administrador del sistema / de la seguridad [E.4] Errores de configuración [A.24] Denegación de servicio	Medio	Se mitiga el riesgo con la implementación de los controles 8.2.2 - 9.1.1- 9.1.1 - 9.2.1 - 9.2.2 - 9.2.5- 11.1.4	Suministro de acceso de usuarios. Protección contra amenazas externas y ambientales. Mantenimiento de equipos. Registro de eventos. Gestión de las vulnerabilidades técnicas. Evaluación de eventos de seguridad de la información y decisiones sobre ellos. Respuesta a incidentes de seguridad de la información.	**Proyecto 1-** Control de acceso físico y protección de la información (Áreas seguras y seguridad de equipos).Ver numeral 11.1 **Proyecto 3-** Implementación y seguimiento de registros de actividad. Ver numeral 11.1 **Proyecto 7-** Gestión de incidentes de Seguridad de la Información. Ver numeral 11.1
	Pérdida de la Integridad de la información, lo que implica el acceso indebido o fraudulento al activo de información	[N.1] Fuego [N.2] Daños por agua [I.1] Fuego [I.2] Daños por agua	Muy Alto	Se mitiga el riesgo con la implementación de los controles 11.1.3 11.1.4 - 11.1.5	Uso aceptable de los activos. Clasificación de la información. Política de control de acceso. Acceso a redes y a Servicios de red. Gestión de derechos de acceso privilegiado.	**Proyecto 1-** Control de acceso físico y protección de la información (Áreas seguras y seguridad de equipos).Ver numeral 11.1
		[E.24] caída del sistema por agotamiento de recursos [A.8] Difusión de software dañino [A.23] Manipulación del hardware [A.26] Ataque destructivo	Alto	Se mitiga el riesgo con la implementación de los controles 8.2.3 - 9.1.1 - 11.1.1 - 11.1.2 - 11.1.3 - 11.2.1 - 11.2.4 - 12.1.3 - 12.2.1	Seguridad de oficinas, recinto e instalaciones. Protección contra amenazas externas y ambientales. Trabajo en áreas seguras.	**Proyecto 1-** Control de acceso físico y protección de la información (Áreas seguras y seguridad de equipos).Ver numeral 11.1

Tabla 34. (Continuación)

ACTIVOS	RIESGO	AMENAZAS	VALOR	TRATAMIENTO DE RIESGO	CONTROLES IMPLEMENTADOS	PROYECTOS DEFINIDOS
Consola Vcenter	Pérdida de la Integridad de la información, lo que implica el acceso indebido o fraudulento al activo de información	[E.2] Errores del administrador del sistema / de la seguridad [E.4] Errores de configuración [A.24] Denegación de servicio	Medio	Se mitiga el riesgo con la implementación de los controles 8.2.2 - 9.1.1- 9.1.1 - 9.2.1 - 9.2.2 - 9.2.5- 11.1.4	Suministro de acceso de usuarios. Protección contra amenazas externas y ambientales. Mantenimiento de equipos. Registro de eventos. Gestión de las vulnerabilidades técnicas. Evaluación de eventos de seguridad de la información y decisiones sobre ellos. Respuesta a incidentes de seguridad de la información.	**Proyecto 1-** Control de acceso físico y protección de la información (Áreas seguras y seguridad de equipos).Ver numeral 11.1 **Proyecto 3- Implementación** y seguimiento de registros de actividad. Ver numeral 11.1 **Proyecto 7-** Gestión de incidentes de Seguridad de la Información. Ver numeral 11.1
Aplicación Idocument	Pérdida de Disponibilidad del activo de información	[E.2] Errores del administrador del sistema / de la seguridad	Alto	Se mitiga el riesgo con la implementación de los controles 8.2.2 - 9.1.1- 9.1.1 - 9.2.1 - 9.2.2 - 9.2.5- 11.1.4	Suministro de acceso de usuarios. Protección contra amenazas externas y ambientales. Mantenimiento de equipos. Registro de eventos. Gestión de las vulnerabilidades técnicas Evaluación de eventos de seguridad de la información y decisiones sobre ellos. Respuesta a incidentes de seguridad de la información.	**Proyecto 1-** Control de acceso físico y protección de la información (Áreas seguras y seguridad de equipos).Ver numeral 11.1 **Proyecto 3-** Implementación y seguimiento de registros de actividad. Ver numeral 11.1 **Proyecto 7-** Gestión de incidentes de Seguridad de la Información.
	Pérdida de la Integridad de la información, lo que implica el acceso indebido o fraudulento al activo de información	[E.2] Errores del administrador del sistema / de la seguridad [E.15] Alteración de la información	Alto	Se mitiga el riesgo con la implementación de los controles 8.2.2 - 9.1.1- 9.2.1 - 9.2.2 - 9.2.5-11.1.4	Suministro de acceso de usuarios. Protección contra amenazas externas y ambientales. Mantenimiento de equipos. Registro de eventos. Gestión de las vulnerabilidades técnicas. Evaluación de eventos de seguridad de la información y decisiones sobre ellos. Respuesta a incidentes de seguridad de la información.	**Proyecto 1-** Control de acceso físico y protección de la información (Áreas seguras y seguridad de equipos).Ver numeral 11.1 **Proyecto 3**- Implementación y seguimiento de registros de actividad. Ver numeral 11.1 **Proyecto 7-** Gestión de incidentes de Seguridad de la Información.
Base de datos Oracle 11g	Pérdida de Disponibilidad del activo de información	[E.2] Errores del administrador del sistema / de la seguridad [E.18] Destrucción de la información	Alto	Se mitiga el riesgo con la implementación de los controles 8.2.2 - 9.1.1- 9.1.1 - 9.2.1 - 9.2.2 - 9.2.5- 11.1.4	Suministro de acceso de usuarios. Protección contra amenazas externas y ambientales. Mantenimiento de equipos. Registro de eventos. Gestión de las vulnerabilidades técnicas. Evaluación de eventos de seguridad de la información y decisiones sobre ellos. Respuesta a incidentes de seguridad de la información.	**Proyecto 1-** Control de acceso físico y protección de la información (Áreas seguras y seguridad de equipos).Ver numeral 11.1 **Proyecto 3-** Implementación y seguimiento de registros de actividad. Ver numeral 11.1 **Proyecto 7-** Gestión de incidentes de Seguridad de la Información. Ver numeral 11.1

Tabla 34. (Continuación)

ACTIVOS	RIESGO	AMENAZAS	VALOR	TRATAMIENTO DE RIESGO	CONTROLES IMPLEMENTADOS	PROYECTOS DEFINIDOS
Base de datos Oracle 11g	Pérdida de Disponibilidad del activo de información	[N.1] Fuego [N.*] Desastres naturales [E.1] Errores de los usuarios [A.6] Abuso de privilegios de acceso	Medio	Se mitiga el riesgo con la implementación de los controles 11.1.3 11.1.4 - 11.1.5	Uso aceptable de los activos. Clasificación de la información. Política de control de acceso. Acceso a redes y a Servicios de red. Gestión de derechos de acceso privilegiado.	**Proyecto 1-** Control de acceso físico y protección de la información (Áreas seguras y seguridad de equipos).Ver numeral 11.1
	Pérdida de la Integridad de la información, lo que implica el acceso indebido o fraudulento al activo de información	[E.1] Errores de los usuarios [E.15] Alteración de la información [E.18] Destrucción de la información [A.6] Abuso de privilegios de acceso [A.15] Modificación de la información	Alto	Se mitiga el riesgo con la implementación de los controles 8.2.2 - 9.1.1- 9.2.1 - 9.2.2 - 9.2.3 - 9.2.5- 11.1.4 -11.2.8 - 12.1.2	Suministro de acceso de usuarios. Protección contra amenazas externas y ambientales. Mantenimiento de equipos. Registro de eventos. Gestión de las vulnerabilidades técnicas Evaluación de eventos de seguridad de la información y decisiones sobre ellos. Respuesta a incidentes de seguridad de la información. Manejo de activos. Gestión de derechos de acceso privilegiado. Equipos de usuario desatendido. Procedimientos de operación documentados.	**Proyecto 2-** Responsabilidades y procedimientos de operación. Ver numeral 11.1 **Proyecto 4-** Control de acceso y responsabilidades de los usuarios a los sistemas y aplicaciones. Ver numeral 11.1
		[N.1] Fuego [N.2] Daños por agua [N.*] Desastres naturales [E.2] Errores del administrador del sistema / de la seguridad	Medio	Se mitiga el riesgo con la implementación de los controles 11.1.3 11.1.4 - 11.1.5	Uso aceptable de los activos. Clasificación de la información. Política de control de acceso. Acceso a redes y a Servicios de red. Gestión de derechos de acceso privilegiado.	**Proyecto 1-** Control de acceso físico y protección de la información (Áreas seguras y seguridad de equipos).Ver numeral 11.1

Tabla 34. (Continuación)

ACTIVOS	RIESGO	AMENAZAS	VALOR	TRATAMIENTO DE RIESGO	CONTROLES IMPLEMENTADOS	PROYECTOS DEFINIDOS
Base de datos Oracle 11g	Pérdida de la Confidencialidad, acceso no autorizado que permite la utilización indebida o no autorizada del activo de información	[E.2] Errores del administrador del sistema / de la seguridad [E.14] Fugas de información [E.15] Alteración de la información [E.18] Destrucción de la información [A.6] Abuso de privilegios de acceso [A.15] Modificación de la información	Medio	Se mitiga el riesgo con la implementación de los controles 8.2.2- 8.2.3 - 9.1.1 - 9.1.4 - 9.2.1 - 9.2.2 - 9.2.3 - 9.2.5 - 11.2.8 - 12.1.2	Suministro de acceso de usuarios. Protección contra amenazas externas y ambientales. Mantenimiento de equipos. Registro de eventos. Gestión de las vulnerabilidades técnicas. Evaluación de eventos de seguridad de la información y decisiones sobre ellos. Respuesta a incidentes de seguridad de la información. Manejo de activos. Gestión de derechos de acceso privilegiado. Equipos de usuario desatendido. Procedimientos de operación documentados.	**Proyecto 2-** Responsabilidades y procedimientos de operación. Ver numeral 11.1 **Proyecto 4-** Control de acceso y responsabilidades de los usuarios a los sistemas y aplicaciones. Ver numeral 11.1
Aplicaciones Aranda Software - Parte Misional	Pérdida de Disponibilidad del activo de información	[I.6] Corte del suministro eléctrico	Alto	Se mitiga el riesgo con la implementación del control 11.2.2 - 15.2.1	Servicios de suministro. Seguimiento y revisión de los servicios de los proveedores.	**Proyecto 1-** Control de acceso físico y protección de la información (Áreas seguras y seguridad de equipos).Ver numeral 11.1
		[N.*] Desastres naturales [I.7] Condiciones inadecuadas de temperatura o humedad [E.2] Errores del administrador del sistema / de la seguridad [E.4] Errores de configuración [E.24] caída del sistema por agotamiento de recursos [A.8] Difusión de software dañino	Medio	Se mitiga el riesgo con la implementación de los controles 11.1.3 - 11.1.4 - 11.1.5 - 12.2.1	Uso aceptable de los activos. Clasificación de la información. Política de control de acceso. Acceso a redes y a Servicios de red. Gestión de derechos de acceso privilegiado.	**Proyecto 1-** Control de acceso físico y protección de la información (Áreas seguras y seguridad de equipos).Ver numeral 11.1 **Proyecto 2**- Responsabilidades y procedimientos de operación. Ver numeral 11.1

Tabla 34. (Continuación)

ACTIVOS	RIESGO	AMENAZAS	VALOR	TRATAMIENTO DE RIESGO	CONTROLES IMPLEMENTADOS	PROYECTOS DEFINIDOS
Aplicaciones Aranda Software - Parte Misional	Pérdida de la Integridad de la información, lo que implica el acceso indebido o fraudulento al activo de información	[E.21] Errores de mantenimiento / actualización de programas (software)	Alto	Se mitiga el riesgo con la implementación de los controles 8.2.2 - 9.1.1- 9.1.1 - 9.2.1 - 9.2.2 - 9.2.5- 11.1.4	Suministro de acceso de usuarios. Protección contra amenazas externas y ambientales. Mantenimiento de equipos. Registro de eventos. Gestión de las vulnerabilidades técnicas. Evaluación de eventos de seguridad de la información y decisiones sobre ellos. Respuesta a incidente.	**Proyecto 1-** Control de acceso físico y protección de la información (Áreas seguras y seguridad de equipos).Ver numeral 11.1 **Proyecto 3-** Implementación y seguimiento de registros de actividad. Ver numeral 11.1 **Proyecto 7-** Gestión de incidentes de Seguridad de la Información. Ver numeral 11.1
		[E.18] Destrucción de la información [A.8] Difusión de software dañino	Medio	Se mitiga el riesgo con la implementación de los controles 9.2.2 - 11.1.4 - 12.2.1 - 12.4.1 - 12.2.4 - 12.4.2	Protección contra amenazas externas y ambientales. Mantenimiento de equipos. Registro de eventos. Controles contra código malicioso. Suministro de acceso de usuarios. Protección de la información de registro.	**Proyecto 1-** Control de acceso físico y protección de la información (Áreas seguras y seguridad de equipos).Ver numeral 11.1 **Proyecto 2-** Responsabilidades y procedimientos de operación. Ver numeral 11.1 **Proyecto 3-** Implementación y seguimiento de registros de actividad. Ver numeral 11.1
	Pérdida de la Confidencialidad, acceso no autorizado que permite la utilización indebida o no autorizada del activo de información	[A.11] Acceso no autorizado	Medio	Se mitiga el riesgo con la implementación de los controles 9.1.1 - 9.1.2 - 9.2.1 - 9.2.2 - 9.2.3	Gestión de acceso a usuarios. Gestión de derechos de acceso asignados a usuarios. Acceso a redes y a Servicios de red. Suministro de acceso de usuarios. Gestión de derechos de acceso privilegiado.	**Proyecto 4-** Control de acceso y responsabilidades de los usuarios a los sistemas y aplicaciones. Ver numeral 11.1
Aplicaciones Aranda Software - Parte Administrativa	Pérdida de Disponibilidad del activo de información	[I.6] Corte del suministro eléctrico	Alto	Se mitiga el riesgo con la implementación del control 11.2.2 - 15.2.1	Servicios de suministro. Seguimiento y revisión de los servicios de los proveedores.	**Proyecto 1-** Control de acceso físico y protección de la información (Áreas seguras y seguridad de equipos).Ver numeral 11.1

Tabla 34. (Continuación)

ACTIVOS	RIESGO	AMENAZAS	VALOR	TRATAMIENTO DE RIESGO	CONTROLES IMPLEMENTADOS	PROYECTOS DEFINIDOS
Aplicaciones Aranda Software - Parte Administrativa	Pérdida de Disponibilidad del activo de información	[N.*] Desastres naturales [I.7] Condiciones inadecuadas de temperatura o humedad [E.2] Errores del administrador del sistema / de la seguridad [E.4] Errores de configuración [E.24] caída del sistema por agotamiento de recursos [A.8] Difusión de software dañino	Medio	Se mitiga el riesgo con la implementación de los controles 11.1.3 - 11.1.4 - 11.1.5 - 12.2.1	Uso aceptable de los activos. Clasificación de la información. Política de control de acceso. Acceso a redes y a Servicios de red. Gestión de derechos de acceso privilegiado.	**Proyecto 1-** Control de acceso físico y protección de la información (Áreas seguras y seguridad de equipos).Ver numeral 11.1 **Proyecto 2-** Responsabilidades y procedimientos de operación. Ver numeral 11.1
	Pérdida de la Integridad de la información, lo que implica el acceso indebido o fraudulento al activo de información	[E.21] Errores de mantenimiento / actualización de programas (software)	Alto	Se mitiga el riesgo con la implementación de los controles 12.4.3 - 12.5.1 - 12.6.2 - 14.2.4	Registros del administrador y del operador. Instalación de software en sistemas operativos. Restricciones sobre la instalación de software. Restricciones en los cambios o los paquetes de software.	**Proyecto 3-** Implementación y seguimiento de registros de actividad. Ver numeral 11.1
		[E.18] Destrucción de la información [A.8] Difusión de software dañino	Medio	Se mitiga el riesgo con la implementación de los controles 9.2.2 - 11.1.4 - 12.2.1 - 12.4.1 - 12.2.4 - 12.4.2	Protección contra amenazas externas y ambientales. Mantenimiento de equipos. Registro de eventos. Controles contra código malicioso. Suministro de acceso de usuarios. Protección de la información de registro.	**Proyecto 1-** Control de acceso físico y protección de la información (Áreas seguras y seguridad de equipos).Ver numeral 11.1 **Proyecto 2-** Responsabilidades y procedimientos de operación. Ver numeral 11.1
	Pérdida de la Confidencialidad, acceso no autorizado que permite la utilización indebida o no autorizada del activo de información	[A.11] Acceso no autorizado	Medio	Se mitiga el riesgo con la implementación de los controles 11.1.3 - 11.1.4 - 11.1.5 - 12.2.1	Copias de seguridad de la información. Restricciones a los cambios en los paquetes de software. Cadena de suministro en tecnologías de la información y comunicaciones. Responsabilidades y procedimientos. Protección contra las amenazas externas y ambientales. Implantación de la continuidad de la seguridad de la información.	**Proyecto 1-** Control de acceso físico y protección de la información (Áreas Seguras y seguridad de equipos)

Tabla 34. (Continuación)

ACTIVOS	RIESGO	AMENAZAS	VALOR	TRATAMIENTO DE RIESGO	CONTROLES IMPLEMENTADOS	PROYECTOS DEFINIDOS
SYSMAN	Pérdida de Disponibilidad del activo de información	[I.8] Fallos de servicios de comunicación [E.2] Errores del administrador [E.18] Destrucción de información [E.21] Errores de mantenimiento / actualización de programas (software) [E.24] Caída del sistema por agotamiento de recursos [A.18] Destrucción la información	Muy Alto	Se mitiga el riesgo con la implementación de los controles 11.1.3 - 11.1.4 - 11.1.5 - 12.2.1	Uso aceptable de los activos. Clasificación de la información. Política de control de acceso. Acceso a redes y a Servicios de red. Gestión de derechos de acceso privilegiado.	**Proyecto 1-** Control de acceso físico y protección de la información (Áreas seguras y seguridad de equipos).Ver numeral 11.1 **Proyecto 2-** Responsabilidades y procedimientos de operación. Ver numeral 11.1
		[E.1] Errores de los usuarios [A.6] Abuso de privilegios de acceso [A.7] Uso no previsto	Alto	Se mitiga el riesgo con la implementación de los controles 8.2.2 - 9.1.1- 9.2.1 - 9.2.2 - 9.2.3 - 9.2.5- 11.1.4 -11.2.8 - 12.1.2	Gestión de derechos de acceso asignados a usuarios. Control de acceso. Restricciones a los cambios en los paquetes de software.	**Proyecto 1-** Control de acceso físico y protección de la información (Áreas Seguras y seguridad de equipos). Ver numeral 11.1
	Pérdida de la Integridad de la información, lo que implica el acceso indebido o fraudulento al activo de información	[E.4] Errores de configuración [E.15] Alteración accidental de la información [E.20] Vulnerabilidades de los programas (software) [E.21] Errores de mantenimiento / actualización de programas (software)	Muy Alto	Se mitiga el riesgo con la implementación de los controles 8.2.2 - 9.1.1- 9.1.1 - 9.2.1 - 9.2.2 - 9.2.5- 11.1.4	Suministro de acceso de usuarios. Protección contra amenazas externas y ambientales. Mantenimiento de equipos. Registro de eventos. Gestión de las vulnerabilidades técnicas. Evaluación de eventos de seguridad de la información y decisiones sobre ellos. Respuesta a incidente.	**Proyecto 1-** Control de acceso físico y protección de la información (Áreas seguras y seguridad de equipos).Ver numeral 11.1 **Proyecto 3-** Implementación y seguimiento de registros de actividad. Ver numeral 11.1 **Proyecto 7-** Gestión de incidentes de Seguridad de la Información.

Tabla 34. (Continuación)

ACTIVOS	RIESGO	AMENAZAS	VALOR	TRATAMIENTO DE RIESGO	CONTROLES IMPLEMENTADOS	PROYECTOS DEFINIDOS
SYSMAN	Pérdida de la Integridad de la información, lo que implica el acceso indebido o fraudulento al activo de información	[A.5] Suplantación de la identidad del usuario [A.6] Abuso de privilegios de acceso [A.7] Uso no previsto [A.11] Acceso no autorizado [A.15] Modificación de la información [A.17] Corrupción de la información	Muy Alto	Se mitiga el riesgo con la implementación de los controles 8.2.2 - 9.1.1- 9.1.1 - 9.2.1 - 9.2.2 - 9.2.5- 11.1.4	Suministro de acceso de usuarios. Protección contra amenazas externas y ambientales. Mantenimiento de equipos. Registro de eventos. Gestión de las vulnerabilidades técnicas. Evaluación de eventos de seguridad de la información y decisiones sobre ellos. Respuesta a incidente.	**Proyecto 1-** Control de acceso físico y protección de la información (Áreas seguras y seguridad de equipos).Ver numeral 11.1 **Proyecto 3-** Implementación y seguimiento de registros de actividad. Ver numeral 11.1 **Proyecto 7-** Gestión de incidentes de Seguridad de la Información.
		[E.1] Errores de los usuarios [E.2] Errores del administrador	Alto	Se mitiga el riesgo con la implementación de los controles 8.2.2 - 9.1.1- 9.1.1 - 9.2.1 - 9.2.2 - 9.2.5- 11.1.4	Suministro de acceso de usuarios. Protección contra amenazas externas y ambientales. Mantenimiento de equipos. Registro de eventos. Gestión de las vulnerabilidades técnicas. Evaluación de eventos de seguridad de la información y decisiones sobre ellos. Respuesta a incidente.	**Proyecto 1-** Control de acceso físico y protección de la información (Áreas seguras y seguridad de equipos).Ver numeral 11.1 **Proyecto 3-** Implementación y seguimiento de registros de actividad. Ver numeral 11.1 **Proyecto 7-** Gestión de incidentes de Seguridad de la Información. Ver numeral 11.1
	Pérdida de la Confidencialidad, acceso no autorizado que permite la utilización indebida o no autorizada del activo de información	[E.2] Errores del administrador [E.14] Escapes de información [E.20] Vulnerabilidades de los programas (software) [A.5] Suplantación de la identidad del usuario [A.6] Abuso de privilegios de acceso	Alto	Se mitiga el riesgo con la implementación de los controles 7.2.3 - 9.1.1 - 9.2.1 - 9.2.2 - 9.2.5 - 9.4.1 - 11.1.2 - 11.2.8 - 12-2.1 - 12.4.1	Proceso disciplinario. Política de control de acceso. Registro y cancelación del registro de usuarios. Suministro de acceso de usuarios. Revisión de los derechos de acceso de usuarios. Restricción de acceso a la información. Controles de acceso físicos. Equipos de usuario desatendido. Controles contra códigos maliciosos. Registro de eventos.	**Proyecto 1-** Control de acceso físico y protección de la información (Áreas seguras y seguridad de equipos).Ver numeral 11.1 **Proyecto 2-** Responsabilidades y procedimientos de operación. Ver numeral 11.1 **Proyecto 3-** Implementación y seguimiento de registros de actividad. Ver numeral 11.1 **Proyecto 4-** Control de acceso y responsabilidades de los usuarios a los sistemas y aplicaciones. Ver numeral 11.1

Tabla 34. (Continuación)

ACTIVOS	RIESGO	AMENAZAS	VALOR	TRATAMIENTO DE RIESGO	CONTROLES IMPLEMENTADOS	PROYECTOS DEFINIDOS
SYSMAN	Pérdida de la Confidencialidad, acceso no autorizado que permite la utilización indebida o no autorizada del activo de información	[A.7] Uso no previsto [A.11] Acceso no autorizado [A.17] Corrupción de la información [A.19] Divulgación de información	Alto	Se mitiga el riesgo con la implementación de los controles 7.2.3 - 9.1.1 - 9.2.1 - 9.2.2 - 9.2.5 - 9.4.1 - 11.1.2 - 11.2.8 - 12-2.1 - 12.4.1	Proceso disciplinario. Política de control de acceso. Registro y cancelación del registro de usuarios. Suministro de acceso de usuarios. Revisión de los derechos de acceso de usuarios. Restricción de acceso a la información. Controles de acceso físicos. Equipos de usuario desatendido. Controles contra códigos maliciosos. Registro de eventos.	**Proyecto 1-** Control de acceso físico y protección de la información (Áreas seguras y seguridad de equipos).Ver numeral 11.1 **Proyecto 2-** Responsabilidades y procedimientos de operación. Ver numeral 11.1 **Proyecto 3-** Implementación y seguimiento de registros de actividad. Ver numeral 11.1
		[E.1] Errores de los usuarios	Medio	Se mitiga el riesgo con la implementación de los controles 8.2.2 - 9.1.1- 9.2.1 - 9.2.2 - 9.2.3 - 9.2.5- 11.1.4 -11.2.8 - 12.1.2	Gestión de derechos de acceso asignados a usuarios. Control de acceso. Restricciones a los cambios en los paquetes de software.	**Proyecto 2-** Responsabilidades y procedimientos de operación. Ver numeral 11.1 **Proyecto 4-** Control de acceso y responsabilidades de los usuarios a los sistemas y aplicaciones. Ver numeral 11.1
	Pérdida de Autenticidad, en el comportamiento, resultado o uso del activo de información	[A.5] Suplantación de la identidad del usuario	Muy Alto	Se mitiga el riesgo con la implementación de los controles 8.2.2 - 9.1.1- 9.1.1 - 9.2.1 - 9.2.2 - 9.2.5- 11.1.4	Suministro de acceso de usuarios. Protección contra amenazas externas y ambientales. Mantenimiento de equipos. Registro de eventos. Gestión de las vulnerabilidades técnicas. Evaluación de eventos de seguridad de la información y decisiones sobre ellos. Respuesta a incidente.	**Proyecto 1-** Control de acceso físico y protección de la información (Áreas seguras y seguridad de equipos).Ver numeral 11.1 **Proyecto 3-** Implementación y seguimiento de registros de actividad. Ver numeral 11.1 **Proyecto 7-** Gestión de incidentes de Seguridad de la Información. ver numeral 11.1
SICAPITAL	Pérdida de Disponibilidad del activo de información	[E.7] Deficiencias en la organización [E.28] Indisponibilidad del personal	Muy Alto	Se mitiga el riesgo con la implementación de los controles 6.1.1 - 7.2.1 - 16.1.1	Roles y responsabilidades para la seguridad de la información. Responsabilidades de la dirección. Responsabilidades y procedimientos.	**Proyecto 6-** Seguimiento y cumplimiento de la Política de Seguridad de la información de la entidad. **Proyecto 7-** Gestión de incidentes de Seguridad de la Información. ver numeral 11.1
		[E.1] Errores de los usuarios [E.2] Errores del administrador [E.18] Destrucción de información [E.20] Vulnerabilidades de los programas (software) E.24] Caída del sistema por agotamiento de recursos	Alto	Se mitiga el riesgo con la implementación de los controles 9.1.1- 9.2.1 - 9.2.2 - 9.2.3 - 9.2.5- 11.1.4 - 11.2.4 -12.6.1	Política de control de acceso. Registro y cancelación del registro de usuarios. Suministro de acceso de usuarios. Gestión de derechos de acceso privilegiado. Revisión de los derechos de acceso de usuarios. Protección contra amenazas externas y ambientales. Mantenimiento de equipos. Gestión de las vulnerabilidades técnicas.	**Proyecto 1-** Control de acceso físico y protección de la información (Áreas seguras y seguridad de equipos).Ver numeral 11.1 **Proyecto 3- Implementación** y seguimiento de registros de actividad. Ver numeral 11.1 **Proyecto 4-** Control de acceso y responsabilidades de los usuarios a los sistemas y aplicaciones. Ver numeral 11.1

Tabla 34. (Continuación)

ACTIVOS	RIESGO	AMENAZAS	VALOR	TRATAMIENTO DE RIESGO	CONTROLES IMPLEMENTADOS	PROYECTOS DEFINIDOS
SICAPITAL	Pérdida de Disponibilidad del activo de información	[E.21] Errores de mantenimiento / actualización de programas (software)	Medio	Se mitiga el riesgo con la implementación de los controles 12.4.3 - 12.5.1 - 12.6.2 - 14.2.4	Registros del administrador y del operador. Instalación de software en sistemas operativos. Restricciones sobre la instalación de software. Restricciones en los cambios o los paquetes de software.	**Proyecto 3-** Implementación y seguimiento de registros de actividad. Ver numeral 11.1
	Pérdida de la Integridad de la información, lo que implica el acceso indebido o fraudulento al activo de información	[E.1] Errores de los usuarios [E.4] Errores de configuración [E.15] Alteración accidental de la información [E.20] Vulnerabilidades de los programas (software)	Alto	Se mitiga el riesgo con la implementación de los controles 9.1.1- 9.2.1 - 9.2.2 - 9.2.3 - 9.2.5- 11.1.4 - 11.2.4 -12.6.1	Política de control de acceso. Registro y cancelación del registro de usuarios. Suministro de acceso de usuarios. Gestión de derechos de acceso privilegiado. Revisión de los derechos de acceso de usuarios. Protección contra amenazas externas y ambientales. Mantenimiento de equipos. Gestión de las vulnerabilidades técnicas.	**Proyecto 1-** Control de acceso físico y protección de la información (Áreas seguras y seguridad de equipos).Ver numeral 11.1 **Proyecto 3-** Implementación y seguimiento de registros de actividad. Ver numeral 11.1 **Proyecto 4-** Control de acceso y responsabilidades de los usuarios a los sistemas y aplicaciones. Ver numeral 11.1
		[E.2] Errores del administrador [E.21] Errores de mantenimiento / actualización de programas (software)	Medio	Se mitiga el riesgo con la implementación de los controles 12.4.3 - 12.5.1 - 12.6.2 - 14.2.4	Registros del administrador y del operador. Instalación de software en sistemas operativos. Restricciones sobre la instalación de software. Restricciones en los cambios o los paquetes de software.	**Proyecto 3-** Implementación y seguimiento de registros de actividad.
	Pérdida de la Confidencialidad, acceso no autorizado que permite la utilización indebida o no autorizada del activo de información	[E.1] Errores de los usuarios [E.2] Errores del administrador	Alto	Se mitiga el riesgo con la implementación de los controles 8.2.2 - 9.1.1- 9.1.1 - 9.2.1 - 9.2.2 - 9.2.5- 11.1.4	Procedimientos de operación documentados. Registro de eventos. Protección de la información de registro. Registros del administrador y del operador.	**Proyecto 2-** Responsabilidades y procedimientos de operación.
		[E.20] Vulnerabilidades de los programas (software)	Medio	Se mitiga el riesgo con la implementación de los controles 12.4.3 - 12.5.1 - 12.6.2 - 14.2.4	Registros del administrador y del operador. Instalación de software en sistemas operativos. Restricciones sobre la instalación de software. Restricciones en los cambios o los paquetes de software.	**Proyecto 3-** Implementación y seguimiento de registros de actividad. Ver numeral 11.1

Tabla 34. (Continuación)

ACTIVOS	RIESGO	AMENAZAS	VALOR	TRATAMIENTO DE RIESGO	CONTROLES IMPLEMENTADOS	PROYECTOS DEFINIDOS
Antivirus Kaspersky	Pérdida de Disponibilidad del activo de información	[E.1] Errores de los usuarios	Alto	Se mitiga el riesgo con la implementación de los controles 8.2.2 - 9.1.1- 9.1.1 - 9.2.1 - 9.2.2 - 9.2.5- 11.1.4	Suministro de acceso de usuarios. Protección contra amenazas externas y ambientales. Mantenimiento de equipos. Registro de eventos. Gestión de las vulnerabilidades técnicas Evaluación de eventos de seguridad de la información y decisiones sobre ellos. Respuesta a incidentes de seguridad de la información.	**Proyecto 1-** Control de acceso físico y protección de la información (Áreas seguras y seguridad de equipos).Ver numeral 11.1 **Proyecto 3-** Implementación y seguimiento de registros de actividad. Ver numeral 11.1 **Proyecto 7-** Gestión de incidentes de Seguridad de la Información. Ver numeral 11.1
		[E.2] Errores del administrador del sistema / de la seguridad [E.3] Errores de monitorización (log) [E.4] Errores de configuración [E.20] vulnerabilidades de los programas (software) [A.8] Difusión de software dañino [A.22] Manipulación de programas	Medio	Se mitiga el riesgo con la implementación de los controles 12.1.1 - 12.2.1 - 12.4.1 - 12.4.2 - 12.4.3 -	Procedimientos de operación documentados. Registro de eventos. Protección de la información de registro. Registros del administrador y del operador. Controles contra códigos maliciosos.	**Proyecto 2-** Responsabilidades y procedimientos de operación.
	Pérdida de la Integridad de la información, lo que implica el acceso indebido o fraudulento al activo de información	[E.1] Errores de los usuarios	Alto	Se mitiga el riesgo con la implementación de los controles 8.2.2 - 9.1.1- 9.1.1 - 9.2.1 - 9.2.2 - 9.2.5- 11.1.4	Suministro de acceso de usuarios. Protección contra amenazas externas y ambientales. Mantenimiento de equipos. Registro de eventos. Gestión de las vulnerabilidades técnicas. Evaluación de eventos de seguridad de la información y decisiones sobre ellos. Respuesta a incidentes de seguridad de la información.	**Proyecto 1- C**ontrol de acceso físico y protección de la información (Áreas seguras y seguridad de equipos).Ver numeral 11.1 **Proyecto 3-** Implementación y seguimiento de registros de actividad. Ver numeral 11.1 **Proyecto 7-** Gestión de incidentes de Seguridad de la Información. Ver numeral 11.1

Tabla 34. (Continuación)

ACTIVOS	RIESGO	AMENAZAS	VALOR	TRATAMIENTO DE RIESGO	CONTROLES IMPLEMENTADOS	PROYECTOS DEFINIDOS
Antivirus Kaspersky	Pérdida de la Integridad de la información, lo que implica el acceso indebido o fraudulento al activo de información	[E.2] Errores del administrador del sistema / de la seguridad [E.3] Errores de monitorización (log) [E.4] Errores de configuración [E.20] vulnerabilidades de los programas (software) [A.8] Difusión de software dañino [A.22] Manipulación de programas	Medio	Se mitiga el riesgo con la implementación de los controles 12.1.1 - 12.2.1 - 12.4.1 - 12.4.2 - 12.4.3 -	Procedimientos de operación documentados. Registro de eventos. Protección de la información de registro. Registros del administrador y del operador. Controles contra códigos maliciosos.	**Proyecto 2-** Responsabilidades y procedimientos de operación.

Fuente: el autor.

10.3 Plan Tratamiento de Riesgos: [HW] EQUIPOS

Tabla 38. Plan tratamiento de riesgos: equipos

ACTIVOS	RIESGO	AMENAZAS	VALOR	TRATAMIENTO DE RIESGO	CONTROLES IMPLEMENTADOS	PROYECTOS DEFINIDOS
Antispam Barracuda	Pérdida de Disponibilidad del activo de información	[E.2] Errores del administrador del sistema / de la seguridad	Alto	Se mitiga el riesgo con la implementación de los controles 12.1.1 - 12.4.1 - 12.4.2 - 12.4.3	Procedimientos de operación documentados. Registro de eventos. Protección de la información de registro. Registros del administrador y del operador.	**Proyecto 2-** Responsabilidades y procedimientos de operación.

Tabla 35. (Continuación)

ACTIVOS	RIESGO	AMENAZAS	VALOR	TRATAMIENTO DE RIESGO	CONTROLES IMPLEMENTADOS	PROYECTOS DEFINIDOS
Antispam Barracuda	Pérdida de Disponibilidad del activo de información	[N.1] Fuego [I.1] Fuego [I.6] Corte del suministro eléctrico [E.23] Errores de mantenimiento / actualización de equipos (hardware) [E.25] Pérdida de equipos [A.23] Manipulación del hardware [A.24] Denegación de servicio [A.26] Ataque destructivo	Medio	Se mitiga el riesgo con la implementación de los controles 9.2.5 11.1.2 - 11.1.4 - 11.1.5 - 11.2.1 - 11.2.4. - 11.2.3 - 12.1.1 - 12.2.1 - 15.1.3	Protección contra las amenazas externas y ambientales. Trabajo en áreas seguras. Cadena de suministro de tecnología de información y comunicación. Procedimientos de operación documentados. Mantenimiento de equipos. Revisión de los derechos de acceso de usuarios. Controles de acceso físicos. Ubicación y protección de los equipos. Controles contra códigos maliciosos.	**Proyecto 1-** Control de acceso físico y protección de la información (Áreas seguras y seguridad de equipos).Ver numeral 11.1 **Proyecto 2-** Responsabilidades y procedimientos de operación. Ver numeral 11.1 **Proyecto 4-** Control de acceso y responsabilidades de los usuarios. Ver numeral 11.1.
	Pérdida de la Integridad de la información, lo que implica el acceso indebido o fraudulento al activo de información	[E.2] Errores del administrador del sistema / de la seguridad	Alto	Se mitiga el riesgo con la implementación de los controles 12.1.1 - 12.4.1 - 12.4.2 - 12.4.3	Procedimientos de operación documentados. Registro de eventos. Protección de la información de registro. Registros del administrador y del operador.	**Proyecto 2-** Responsabilidades y procedimientos de operación.
		[A.11] Acceso no autorizado	Medio	Se mitiga el riesgo con la implementación de los controles 9.1.1 - 9.1.2 - 9.2.1 - 9.2.2 - 9.2.3	Gestión de acceso a usuarios. Gestión de derechos de acceso asignados a usuarios. Acceso a redes y a Servicios de red. Suministro de acceso de usuarios. Gestión de derechos de acceso privilegiado.	**Proyecto 4-** Control de acceso y responsabilidades de los usuarios a los sistemas y aplicaciones. Ver numeral 11.1
Impresora Datacard CP 40 Plus	Pérdida de Disponibilidad del activo de información	[I.5] Avería de origen físico o lógico [I.6] Corte del suministro eléctrico [E.23] Errores de mantenimiento / actualización de equipos (hardware) [A.23] Manipulación del hardware	Muy Alto	Se mitiga el riesgo con la implementación de los controles 9.2.5 11.1.2 - 11.1.4 - 11.1.5 - 11.2.1 - 11.2.4. - 11.2.3 - 12.1.1 - 12.2.1 - 15.1.3	Protección contra las amenazas externas y ambientales. Trabajo en áreas seguras. Cadena de suministro de tecnología de información y comunicación. Procedimientos de operación documentados. Mantenimiento de equipos. Revisión de los derechos de acceso de usuarios. Controles de acceso físicos. Ubicación y protección de los equipos. Controles contra códigos maliciosos.	**Proyecto 1-** Control de acceso físico y protección de la información (Áreas seguras y seguridad de equipos).Ver numeral 11.1 **Proyecto 2-** Responsabilidades y procedimientos de operación. Ver numeral 11.1 **Proyecto 4-** Control de acceso y responsabilidades de los usuarios. Ver numeral 11.1.

Tabla 35. (Continuación)

ACTIVOS	RIESGO	AMENAZAS	VALOR	TRATAMIENTO DE RIESGO	CONTROLES IMPLEMENTADOS	PROYECTOS DEFINIDOS
Impresora Datacard CP 40 Plus	Pérdida de Disponibilidad del activo de información	[N.1] Fuego [N.2] Daños por agua [N.*] Desastres naturales [I.1] Fuego [I.2] Daños por agua [I.*] Desastres industriales [E.24] caída del sistema por agotamiento de recursos [E.25] Pérdida de equipos [A.25] Robo de equipos [A.26] Ataque destructivo	Alto	Se mitiga el riesgo con la implementación de los controles 11.1.1 - 11.1.2 - 11.1.3 - 11.1.4 - 11.1.5 - 11.2.2. - 12.2.1 - 16.1.2 - 17.1.1 -	Perímetro de seguridad física. Controles de acceso físicos. Seguridad de oficinas, recinto e instalaciones. Protección contra amenazas externas y ambientales. Trabajo en áreas seguras. Servicios de suministro. ubicación y protección de los equipos. Reporte de eventos de seguridad de la información. Planificación de la continuidad de la seguridad de la información. Controles contra códigos maliciosos.	**Proyecto 1-** Control de acceso físico y protección de la información (Áreas seguras y seguridad de equipos).Ver numeral 11.1 **Proyecto 2-** Responsabilidades y procedimientos de operación. Ver numeral 11.1 **Proyecto 5-** Adaptación Plan de contingencia TICS, como marco de Gestión del Plan de Continuidad del Negocio. Ver numeral 11.1 **Proyecto 7-** Gestión de incidentes de seguridad de la información. Ver numeral 11.1
		[I.3] Contaminación medioambiental [I.4] Contaminación electromagnética [I.7] Condiciones inadecuadas de temperatura o humedad [E.2] Errores del administrador del sistema / de la seguridad	Medio	Se mitiga el riesgo con la implementación de los controles 11.1.4 - 12.1.1 - 12.4.1 - 12.4.2 - 12.4.3	Procedimientos de operación documentados. Registro de eventos. Protección de la información de registro. Registros del administrador y del operador. Protección contra las amenazas externas y ambientales.	**Proyecto 1-** Control de acceso físico y protección de la información (Áreas seguras y seguridad de equipos).Ver numeral 11.1 **Proyecto 2-** Responsabilidades y procedimientos de operación. Ver numeral 11.1
Servidor UPI El Perdomo	Pérdida de Disponibilidad del activo de información	[I.6] Corte del suministro eléctrico	Muy Alto	Se mitiga el riesgo con la implementación del control 11.2.2 - 15.2.1	Servicios de suministro. Seguimiento y revisión de los servicios de los proveedores.	**Proyecto 1-** Control de acceso físico y protección de la información (Áreas seguras y seguridad de equipos).Ver numeral 11.1
		[N.1] Fuego [N.2] Daños por agua [N.*] Desastres naturales [I.7] Condiciones inadecuadas de temperatura o humedad [E.8] Difusión de software dañino [A.24] Denegación de servicio	Alto	Se mitiga el riesgo con la implementación de los controles 9.2.5 11.1.2 - 11.1.4 - 11.1.5 - 11.2.1 - 11.2.4. - 11.2.3 - 12.1.1 - 12.2.1 - 15.1.3	Perímetro de seguridad física. Controles de acceso físicos. Seguridad de oficinas, recinto e instalaciones. Protección contra amenazas externas y ambientales. Trabajo en áreas seguras. Servicios de suministro ubicación y protección de los equipos. Reporte de eventos de seguridad de la información. Planificación de la continuidad de la seguridad de la información. Controles contra códigos maliciosos.	**Proyecto 1-** Control de acceso físico y protección de la información (Áreas seguras y seguridad de equipos).Ver numeral 11.1 **Proyecto 2-** Responsabilidades y procedimientos de operación. Ver numeral 11.1 **Proyecto 4-** Control de acceso y responsabilidades de los usuarios. Ver numeral 11.1.

Tabla 35. (Continuación)

ACTIVOS	RIESGO	AMENAZAS	VALOR	TRATAMIENTO DE RIESGO	CONTROLES IMPLEMENTADOS	PROYECTOS DEFINIDOS
Servidor UPI El Perdomo	Pérdida de Disponibilidad del activo de información	[E.25] Pérdida de equipos [A.23] Manipulación del hardware [A.25] Robo de equipos [A.26] Ataque destructivo	Medio	Se mitiga el riesgo con la implementación de los controles 5.1.1 - 8.1.2 - 9.1.1 - 11.1.1 -11.1.2 - 11.1.3 - 11.1.4 - 11.1.5	Políticas para la seguridad de la Información. Propiedad de los Activos. Política de control de acceso. Perímetro de seguridad física. Controles de acceso físicos. Seguridad de oficinas, recinto e instalaciones. Protección contra amenazas externas y ambientales. Trabajo en áreas seguras.	**Proyecto 1-** Control de acceso físico y protección de la información (Áreas seguras y seguridad de equipos).Ver numeral 11.1 **Proyecto 6-** Seguimiento y cumplimiento de la Política de Seguridad de la Información de la entidad. Ver numeral 11.1.
	Pérdida de la Integridad de la información, lo que implica el acceso indebido o fraudulento al activo de información	[E.8] Difusión de software dañino	Alto	Se mitiga el riesgo con la implementación de los controles 9.2.2 - 11.1.4 - 12.2.1 - 12.4.1 - 12.2.4 - 12.4.2	Protección contra amenazas externas y ambientales. Mantenimiento de equipos. Registro de eventos. Controles contra código malicioso. Suministro de acceso de usuarios. Protección de la información de registro.	**Proyecto 1-** Control de acceso físico y protección de la información (Áreas seguras y seguridad de equipos).Ver numeral 11.1 **Proyecto 2-** Responsabilidades y procedimientos de operación. Ver numeral 11.1 **Proyecto 3- Implementación** y seguimiento de registros de actividad. Ver numeral 11.1
		[A.6] Abuso de privilegios de acceso	Medio	Se mitiga el riesgo con la implementación de los controles 9.1.1 - 9.1.2 – 9.2.1 - 9.2.2 - 9.2.3 - 9.2.4 - 9.2.5 - 9.2.6 - 9.3.1 - 9.4.1 - 9.4.2 - 9.4.3	Política de control de acceso. Acceso a redes y a Servicios de red. Registro y cancelación del registro de usuarios. Gestión de derechos de acceso privilegiado. Suministro de acceso de usuarios. Revisión de los derechos de acceso de usuarios. Retiro o ajuste de los derechos de usuario. Uso de información de información secreta para la autenticación. Restricción de acceso a la información. Procedimiento de ingreso seguro. Sistema de gestión de contraseñas. Controles de acceso físicos. Seguridad de oficinas, recinto e instalaciones.	**Proyecto 4–** Control de acceso y responsabilidades de los usuarios a los sistemas y aplicaciones. Ver numeral 11.1

Tabla 35. (Continuación)

ACTIVOS	RIESGO	AMENAZAS	VALOR	TRATAMIENTO DE RIESGO	CONTROLES IMPLEMENTADOS	PROYECTOS DEFINIDOS
Servidor UPI El Perdomo	Pérdida de la Confidencialidad, acceso no autorizado que permite la utilización indebida o no autorizada del activo de información	[A.11] Acceso no autorizado [A.23] Manipulación del hardware	Alto	Se mitiga el riesgo con la implementación de los controles 9.1.1 - 9.1.2 – 9.2.1 - 9.2.2 - 9.2.3 - 9.2.4 - 9.2.5 - 9.2.6 - 9.3.1 - 9.4.1 - 9.4.2 - 9.4.3 - 11.1.2 - 11.1.3	Política de control de acceso. Acceso a redes y a Servicios de red. Registro y cancelación del registro de usuarios. Gestión de derechos de acceso privilegiado. Suministro de acceso de usuarios. Revisión de los derechos de acceso de usuarios. Retiro o ajuste de los derechos de usuario. Uso de información de información secreta para la autenticación. Restricción de acceso a la información. Procedimiento de ingreso seguro. Sistema de gestión de contraseñas.	**Proyecto 4–** Control de acceso y responsabilidades de los usuarios a los sistemas y aplicaciones. Ver numeral 11.1
		[E.2] Errores del administrador del sistema / de la seguridad [A.6] Abuso de privilegios de acceso	Medio	Se mitiga el riesgo con la implementación de los controles 9.1.1 - 9.1.2 – 9.2.1 - 9.2.2 - 9.2.3 - 9.2.4 - 9.2.5 - 9.2.6 - 9.3.1 - 9.4.1 - 9.4.2 - 9.4.3	Política de control de acceso. Acceso a redes y a Servicios de red. Registro y cancelación del registro de usuarios. Gestión de derechos de acceso privilegiado. Suministro de acceso de usuarios. Revisión de los derechos de acceso de usuarios. Retiro o ajuste de los derechos de usuario. Uso de información de información secreta para la autenticación. Restricción de acceso a la información. Procedimiento de ingreso seguro. Sistema de gestión de contraseñas. Copias de seguridad de la información.	**Proyecto 4**– Control de acceso y responsabilidades de los usuarios a los sistemas y aplicaciones. Ver numeral 11.1
Servidor UPI La 27 Sur	Pérdida de Disponibilidad del activo de información	[I.6] Corte del suministro eléctrico	Muy Alto	Se mitiga el riesgo con la implementación del control 11.2.2 - 15.2.1	Servicios de suministro. Seguimiento y revisión de los servicios de los proveedores.	**Proyecto 1-** Control de acceso físico y protección de la información (Áreas seguras y seguridad de equipos).Ver numeral 11.1

Tabla 35. (Continuación)

ACTIVOS	RIESGO	AMENAZAS	VALOR	TRATAMIENTO DE RIESGO	CONTROLES IMPLEMENTADOS	PROYECTOS DEFINIDOS
Servidor UPI La 27 Sur	Pérdida de Disponibilidad del activo de información	[N.1] Fuego [N.2] Daños por agua [N.*] Desastres naturales [I.7] Condiciones inadecuadas de temperatura o humedad [E.8] Difusión de software dañino [A.24] Denegación de servicio	Alto	Se mitiga el riesgo con la implementación de los controles 9.2.5 11.1.2 - 11.1.4 - 11.1.5 - 11.2.1 - 11.2.4. - 11.2.3 - 12.1.1 - 12.2.1 - 15.1.3	Protección contra las amenazas externas y ambientales. Trabajo en áreas seguras. Cadena de suministro de tecnología de información y comunicación. Procedimientos de operación documentados. Mantenimiento de equipos. Revisión de los derechos de acceso de usuarios. Controles de acceso físicos ubicación y protección de los equipos. Controles contra código malicioso.	**Proyecto 1-** Control de acceso físico y protección de la información (Áreas seguras y seguridad de equipos).Ver numeral 11.1 **Proyecto 2-** Responsabilidades y procedimientos de operación. Ver numeral 11.1 **Proyecto 4-** Control de acceso y responsabilidades de los usuarios. Ver numeral 11.1.
		[E.25] Pérdida de equipos [A.23] Manipulación del hardware [A.25] Robo de equipos [A.26] Ataque destructivo	Medio	Se mitiga el riesgo con la implementación de los controles 5.1.1 - 8.1.2 - 9.1.1 - 11.1.1 -11.1.2 - 11.1.3 - 11.1.4 - 11.1.5	Políticas para la seguridad de la Información. Propiedad de los Activos. Política de control de acceso. Perímetro de seguridad física. Controles de acceso físicos. Seguridad de oficinas, recinto e instalaciones. Protección contra amenazas externas y ambientales. Trabajo en áreas seguras.	**Proyecto 1-** Control de acceso físico y protección de la información (Áreas seguras y seguridad de equipos).Ver numeral 11.1 **Proyecto 6**- Seguimiento y cumplimiento de la Política de Seguridad de la Información de la entidad. Ver numeral 11.1.
	Pérdida de la Integridad de la información, lo que implica el acceso indebido o fraudulento al activo de información	[E.8] Difusión de software dañino	Alto	Se mitiga el riesgo con la implementación de los controles 9.2.2 - 11.1.4 - 12.2.1 - 12.4.1 - 12.2.4 - 12.4.2	Protección contra amenazas externas y ambientales. Mantenimiento de equipos Registro de eventos. Controles contra código malicioso. Suministro de acceso de usuarios. Protección de la información de registro.	**Proyecto 1-** Control de acceso físico y protección de la información (Áreas seguras y seguridad de equipos).Ver numeral 11.1 **Proyecto 2-** Responsabilidades y procedimientos de operación. Ver numeral 11.1 **Proyecto 3-** Implementación y seguimiento de registros de actividad. Ver numeral 11.1

Tabla 35. (Continuación)

ACTIVOS	RIESGO	AMENAZAS	VALOR	TRATAMIENTO DE RIESGO	CONTROLES IMPLEMENTADOS	PROYECTOS DEFINIDOS
Servidor UPI La 27 Sur	Pérdida de la Integridad de la información, lo que implica el acceso indebido o fraudulento al activo de información	[A.6] Abuso de privilegios de acceso	Medio	Se mitiga el riesgo con la implementación de los controles 9.1.1 - 9.1.2 – 9.2.1 - 9.2.2 - 9.2.3 - 9.2.4 - 9.2.5 - 9.2.6 - 9.3.1 - 9.4.1 - 9.4.2 - 9.4.3	Política de control de acceso. Acceso a redes y a Servicios de red. Registro y cancelación del registro de usuarios. Gestión de derechos de acceso privilegiado. Suministro de acceso de usuarios. Revisión de los derechos de acceso de usuarios. Retiro o ajuste de los derechos de usuario. Uso de información de información secreta para la autenticación. Restricción de acceso a la información. Procedimiento de ingreso seguro Sistema de gestión de contraseñas.	**Proyecto 4–** Control de acceso y responsabilidades de los usuarios a los sistemas y aplicaciones. Ver numeral 11.1
	Pérdida de la Confidencialidad, acceso no autorizado que permite la utilización indebida o no autorizada del activo de información	[A.11] Acceso no autorizado [A.23] Manipulación del hardware	Alto	Se mitiga el riesgo con la implementación de los controles 9.1.1 - 9.1.2 – 9.2.1 - 9.2.2 - 9.2.3 - 9.2.4 - 9.2.5 - 9.2.6 - 9.3.1 - 9.4.1 - 9.4.2 - 9.4.3 - 11.1.2 - 11.1.3	Gestión de acceso a usuarios. Gestión de derechos de acceso asignados a usuarios. Acceso a redes y a Servicios de red. Suministro de acceso de usuarios. Gestión de derechos de acceso privilegiado.	**Proyecto 4-** Control de acceso y responsabilidades de los usuarios a los sistemas y aplicaciones. Ver numeral 11.1
		[E.2] Errores del administrador del sistema / de la seguridad [A.6] Abuso de privilegios de acceso	Medio	Se mitiga el riesgo con la implementación de los controles 9.1.1 - 9.2.2 - 9.2.3 - 9.2.6 - 12.1.1	Política de control de acceso. Suministro de acceso a usuarios. Gestión de derechos de acceso privilegiado. Retiro o ajuste de los derechos de usuarios. Procedimientos de operación documentados.	**Proyecto 4–** Control de acceso y responsabilidades de los usuarios a los sistemas y aplicaciones. Ver numeral 11.1
Servidor UPI La 32	Pérdida de Disponibilidad del activo de información	[I.6] Corte del suministro eléctrico	Muy Alto	Se mitiga el riesgo con la implementación del control 11.2.2 - 15.2.1	Servicios de suministro. Seguimiento y revisión de los servicios de los proveedores.	**Proyecto 1-** Control de acceso físico y protección de la información (Áreas seguras y seguridad de equipos).Ver numeral 11.1

Tabla 35. (Continuación)

ACTIVOS	RIESGO	AMENAZAS	VALOR	TRATAMIENTO DE RIESGO	CONTROLES IMPLEMENTADOS	PROYECTOS DEFINIDOS
Servidor UPI La 32	Pérdida de Disponibilidad del activo de información	[N.1] Fuego [N.2] Daños por agua [N.*] Desastres naturales [I.7] Condiciones inadecuadas de temperatura o humedad [E.8] Difusión de software dañino [A.24] Denegación de servicio	Alto	Se mitiga el riesgo con la implementación de los controles 9.2.5 11.1.2 - 11.1.4 - 11.1.5 - 11.2.1 - 11.2.4. - 11.2.3 - 12.1.1 - 12.2.1 - 15.1.3	Perímetro de seguridad física. Controles de acceso físicos. Seguridad de oficinas, recinto e instalaciones. Protección contra amenazas externas y ambientales. Trabajo en áreas seguras. Servicios de suministro ubicación y protección de los equipos. Reporte de eventos de seguridad de la información. Planificación de la continuidad de la seguridad de la información. Controles contra códigos maliciosos.	**Proyecto 1-** Control de acceso físico y protección de la información (Áreas seguras y seguridad de equipos).Ver numeral 11.1 **Proyecto 2-** Responsabilidades y procedimientos de operación. Ver numeral 11.1 **Proyecto 4-** Control de acceso y responsabilidades de los usuarios. Ver numeral 11.1.
		[E.25] Pérdida de equipos [A.23] Manipulación del hardware [A.25] Robo de equipos [A.26] Ataque destructivo	Medio	Se mitiga el riesgo con la implementación de los controles 9.2.5 11.1.2 - 11.1.4 - 11.1.5 - 11.2.1 - 11.2.4. - 11.2.3 - 12.1.1 - 12.2.1 - 15.1.3	Protección contra las amenazas externas y ambientales. Trabajo en áreas seguras. Cadena de suministro de tecnología de información y comunicación. Procedimientos de operación documentados. Mantenimiento de equipos. Revisión de los derechos de acceso de usuarios. Controles de acceso físicos ubicación y protección de los equipos Controles contra código malicioso.	**Proyecto 1-** Control de acceso físico y protección de la información (Áreas seguras y seguridad de equipos).Ver numeral 11.1 **Proyecto 2-** Responsabilidades y procedimientos de operación. Ver numeral 11.1 **Proyecto 4-** Control de acceso y responsabilidades de los usuarios. Ver numeral 11.1.
	Pérdida de la Integridad de la información, lo que implica el acceso indebido o fraudulento al activo de información	[E.8] Difusión de software dañino	Alto	Se mitiga el riesgo con la implementación de los controles 9.2.2 - 11.1.4 - 12.2.1 - 12.4.1 - 12.2.4 - 12.4.2	Protección contra amenazas externas y ambientales. Mantenimiento de equipos. Registro de eventos. Controles contra código malicioso. Suministro de acceso de usuarios. Protección de la información de registro.	**Proyecto 1-** Control de acceso físico y protección de la información (Áreas seguras y seguridad de equipos).Ver numeral 11.1 **Proyecto 2-** Responsabilidades y procedimientos de operación. Ver numeral 11.1 **Proyecto 3-** Implementación y seguimiento de registros de actividad. Ver numeral 11.1

Tabla 35. (Continuación)

ACTIVOS	RIESGO	AMENAZAS	VALOR	TRATAMIENTO DE RIESGO	CONTROLES IMPLEMENTADOS	PROYECTOS DEFINIDOS
Servidor UPI La 32	Pérdida de la Integridad de la información, lo que implica el acceso indebido o fraudulento al activo de información	[A.6] Abuso de privilegios de acceso	Medio	Se mitiga el riesgo con la implementación de los controles 9.1.1 - 9.1.2 - 9.2.1 - 9.2.2 - 9.2.3	Gestión de acceso a usuarios. Gestión de derechos de acceso asignados a usuarios. Acceso a redes y a Servicios de red. Suministro de acceso de usuarios. Gestión de derechos de acceso privilegiado.	**Proyecto 4–** Control de acceso y responsabilidades de los usuarios a los sistemas y aplicaciones. Ver numeral 11.1
	Pérdida de la Confidencialidad, acceso no autorizado que permite la utilización indebida o no autorizada del activo de información	[A.11] Acceso no autorizado [A.23] Manipulación del hardware	Alto	Se mitiga el riesgo con la implementación de los controles 9.1.1 - 9.1.2 - 9.2.1 - 9.2.2 - 9.2.3	Gestión de acceso a usuarios. Gestión de derechos de acceso asignados a usuarios. Acceso a redes y a Servicios de red. Suministro de acceso de usuarios. Gestión de derechos de acceso privilegiado.	**Proyecto 4-** Control de acceso y responsabilidades de los usuarios a los sistemas y aplicaciones. Ver numeral 11.1
		[E.2] Errores del administrador del sistema / de la seguridad [A.6] Abuso de privilegios de acceso	Medio	Se mitiga el riesgo con la implementación de los controles 9.1.1 - 9.1.2 – 9.2.1 - 9.2.2 - 9.2.3 - 9.2.4 - 9.2.5 - 9.2.6 - 9.3.1 - 9.4.1 - 9.4.2 - 9.4.3	Política de control de acceso. Suministro de acceso a usuarios. Gestión de derechos de acceso privilegiado. Retiro o ajuste de los derechos de usuarios. Procedimientos de operación documentados.	**Proyecto 4–** Control de acceso y responsabilidades de los usuarios a los sistemas y aplicaciones. Ver numeral 11.1
Servidor UPI La Florida	Pérdida de Disponibilidad del activo de información	[I.6] Corte del suministro eléctrico	Muy Alto	Se mitiga el riesgo con la implementación del control 11.2.2 - 15.2.1	Servicios de suministro. Seguimiento y revisión de los servicios de los proveedores.	**Proyecto 1-** Control de acceso físico y protección de la información (Áreas seguras y seguridad de equipos).Ver numeral 11.1
		[N.1] Fuego [N.2] Daños por agua [N.*] Desastres naturales [I.7] Condiciones inadecuadas de temperatura o humedad [E.8] Difusión de software dañino [A.24] Denegación de servicio	Alto	Se mitiga el riesgo con la implementación de los controles 9.2.5 11.1.2 - 11.1.4 - 11.1.5 - 11.2.1 - 11.2.4. - 11.2.3 - 12.1.1 - 12.2.1 - 15.1.3	Protección contra las amenazas externas y ambientales. Trabajo en áreas seguras. Cadena de suministro de tecnología de información y comunicación. Procedimientos de operación documentados. Mantenimiento de equipos. Revisión de los derechos de acceso de usuarios. Controles de acceso físicos ubicación y protección de los equipos. Controles contra código malicioso.	**Proyecto 1-** Control de acceso físico y protección de la información (Áreas seguras y seguridad de equipos).Ver numeral 11.1 **Proyecto 2-** Responsabilidades y procedimientos de operación. Ver numeral 11.1 **Proyecto 4-** Control de acceso y responsabilidades de los usuarios. Ver numeral 11.1.

Tabla 35. (Continuación)

ACTIVOS	RIESGO	AMENAZAS	VALOR	TRATAMIENTO DE RIESGO	CONTROLES IMPLEMENTADOS	PROYECTOS DEFINIDOS
Servidor UPI La Florida	Pérdida de Disponibilidad del activo de información	[E.25] Pérdida de equipos [A.23] Manipulación del hardware [A.25] Robo de equipos [A.26] Ataque destructivo	Medio	Se mitiga el riesgo con la implementación de los controles 9.2.5 11.1.2 - 11.1.4 - 11.1.5 - 11.2.1 - 11.2.4. - 11.2.3 - 12.1.1 - 12.2.1 - 15.1.3	Protección contra las amenazas externas y ambientales. Trabajo en áreas seguras. Cadena de suministro de tecnología de información y comunicación. Procedimientos de operación documentados. Mantenimiento de equipos. Revisión de los derechos de acceso de usuarios. Controles de acceso físicos ubicación y protección de los equipos. Controles contra código malicioso.	**Proyecto 1-** Control de acceso físico y protección de la información (Áreas seguras y seguridad de equipos).Ver numeral 11.1 **Proyecto 2-** Responsabilidades y procedimientos de operación. Ver numeral 11.1 **Proyecto 4-** Control de acceso y responsabilidades de los usuarios. Ver numeral 11.1.
	Pérdida de la Integridad de la información, lo que implica el acceso indebido o fraudulento al activo de información	[E.8] Difusión de software dañino	Alto	Se mitiga el riesgo con la implementación de los controles 9.2.2 - 11.1.4 - 12.2.1 - 12.4.1 - 12.2.4 - 12.4.2	Protección contra amenazas externas y ambientales. Mantenimiento de equipos. Registro de eventos. Controles contra código malicioso. Suministro de acceso de usuarios. Protección de la información de registro.	**Proyecto 1-** Control de acceso físico y protección de la información (Áreas seguras y seguridad de equipos).Ver numeral 11.1 **Proyecto 2-** Responsabilidades y procedimientos de operación. Ver numeral 11.1 **Proyecto 3-** Implementación y seguimiento de registros de actividad. Ver numeral 11.1
		[A.6] Abuso de privilegios de acceso	Medio	Se mitiga el riesgo con la implementación de los controles 9.1.1 - 9.1.2 – 9.2.1 - 9.2.2 - 9.2.3 - 9.2.4 - 9.2.5 - 9.2.6 - 9.3.1 - 9.4.1 - 9.4.2 - 9.4.3	Política de control de acceso. Acceso a redes y a Servicios de red. Registro y cancelación del registro de usuarios. Gestión de derechos de acceso privilegiado. Suministro de acceso de usuarios. Revisión de los derechos de acceso de usuarios. Retiro o ajuste de los derechos de usuario. Uso de información de información secreta para la autenticación. Restricción de acceso a la información. Procedimiento de ingreso seguro. Sistema de gestión de contraseñas. Controles de acceso físicos. Seguridad de oficinas, recinto e instalaciones.	**Proyecto 4–** Control de acceso y responsabilidades de los usuarios a los sistemas y aplicaciones. Ver numeral 11.1

Tabla 35. (Continuación)

ACTIVOS	RIESGO	AMENAZAS	VALOR	TRATAMIENTO DE RIESGO	CONTROLES IMPLEMENTADOS	PROYECTOS DEFINIDOS
Servidor UPI La Florida	Pérdida de la Confidencialidad, acceso no autorizado que permite la utilización indebida o no autorizada del activo de información	[A.11] Acceso no autorizado [A.23] Manipulación del hardware	Alto	Se mitiga el riesgo con la implementación de los controles 9.1.1 - 9.1.2 – 9.2.1 - 9.2.2 - 9.2.3 - 9.2.4 - 9.2.5 - 9.2.6 - 9.3.1 - 9.4.1 - 9.4.2 - 9.4.3 - 11.1.2 - 11.1.3	Gestión de acceso a usuarios. Gestión de derechos de acceso asignados a usuarios. Acceso a redes y a Servicios de red. Suministro de acceso de usuarios. Gestión de derechos de acceso privilegiado.	**Proyecto 4-** Control de acceso y responsabilidades de los usuarios a los sistemas y aplicaciones. Ver numeral 11.1
		[E.2] Errores del administrador del sistema / de la seguridad [A.6] Abuso de privilegios de acceso	Medio	Se mitiga el riesgo con la implementación de los controles 9.1.1 - 9.1.2 – 9.2.1 - 9.2.2 - 9.2.3 - 9.2.4 - 9.2.5 - 9.2.6 - 9.3.1 - 9.4.1 - 9.4.2 - 9.4.3 -9.4.4 - 9.4.5	Política de control de acceso. Suministro de acceso a usuarios. Gestión de derechos de acceso privilegiado. Retiro o ajuste de los derechos de usuarios. Procedimientos de operación documentados.	**Proyecto 4–** Control de acceso y responsabilidades de los usuarios a los sistemas y aplicaciones. Ver numeral 11.1
Servidor UPI La Vega	Pérdida de Disponibilidad del activo de información	[I.6] Corte del suministro eléctrico	Muy Alto	Se mitiga el riesgo con la implementación del control 11.2.2 - 15.2.1	Servicios de suministro. Seguimiento y revisión de los servicios de los proveedores.	**Proyecto 1-** Control de acceso físico y protección de la información (Áreas seguras y seguridad de equipos).Ver numeral 11.1
		[N.1] Fuego [N.2] Daños por agua [N.*] Desastres naturales [I.7] Condiciones inadecuadas de temperatura o humedad [E.8] Difusión de software dañino [A.24] Denegación de servicio	Alto	Se mitiga el riesgo con la implementación de los controles 11.1.1 - 11.1.2 - 11.1.3 - 11.1.4 - 11.1.5 - 11.2.2. - 12.2.1 - 16.1.2 - 17.1.1 -	Perímetro de seguridad física. Controles de acceso físicos. Seguridad de oficinas, recinto e instalaciones. Protección contra amenazas externas y ambientales. Trabajo en áreas seguras. Servicios de suministro ubicación y protección de los equipos. Reporte de eventos de seguridad de la información. Planificación de la continuidad de la seguridad de la información. Controles contra códigos maliciosos.	**Proyecto 1-** Control de acceso físico y protección de la información (Áreas seguras y seguridad de equipos).Ver numeral 11.1 **Proyecto 2-** Responsabilidades y procedimientos de operación. Ver numeral 11.1 **Proyecto 4-** Control de acceso y responsabilidades de los usuarios. Ver numeral 11.1.

Tabla 35. (Continuación)

ACTIVOS	RIESGO	AMENAZAS	VALOR	TRATAMIENTO DE RIESGO	CONTROLES IMPLEMENTADOS	PROYECTOS DEFINIDOS
Servidor UPI La Vega	Pérdida de Disponibilidad del activo de información	[E.25] Pérdida de equipos [A.23] Manipulación del hardware [A.25] Robo de equipos [A.26] Ataque destructivo	Medio	Se mitiga el riesgo con la implementación de los controles 9.2.5 11.1.2 - 11.1.4 - 11.1.5 - 11.2.1 - 11.2.4. - 11.2.3 - 12.1.1 - 12.2.1 - 15.1.3	Protección contra las amenazas externas y ambientales. Trabajo en áreas seguras. Cadena de suministro de tecnología de información y comunicación. Procedimientos de operación documentados. Mantenimiento de equipos. Revisión de los derechos de acceso de usuarios. Controles de acceso físicos ubicación y protección de los equipos. Controles contra código malicioso.	**Proyecto 1-** Control de acceso físico y protección de la información (Áreas seguras y seguridad de equipos).Ver numeral 11.1 **Proyecto 6-** Seguimiento y cumplimiento de la Política de Seguridad de la Información de la entidad. Ver numeral 11.1.
	Pérdida de la Integridad de la información, lo que implica el acceso indebido o fraudulento al activo de información	[E.8] Difusión de software dañino	Alto	Se mitiga el riesgo con la implementación de los controles 9.2.2 - 11.1.4 - 12.2.1 - 12.4.1 - 12.2.4 - 12.4.2	Gestión de acceso a usuarios. Gestión de derechos de acceso asignados a usuarios. Acceso a redes y a Servicios de red. Suministro de acceso de usuarios. Gestión de derechos de acceso privilegiado.	**Proyecto 1-** Control de acceso físico y protección de la información (Áreas seguras y seguridad de equipos).Ver numeral 11.1 **Proyecto 2-** Responsabilidades y procedimientos de operación. Ver numeral 11.1 **Proyecto 3-** Implementación y seguimiento de registros de actividad. Ver numeral 11.1
		[A.6] Abuso de privilegios de acceso	Medio	Se mitiga el riesgo con la implementación de los controles 9.1.1 - 9.1.2 – 9.2.1 - 9.2.2 - 9.2.3 - 9.2.4 - 9.2.5 - 9.2.6 - 9.3.1 - 9.4.1 - 9.4.2 - 9.4.3	Política de control de acceso. Acceso a redes y a Servicios de red. Registro y cancelación del registro de usuarios. Gestión de derechos de acceso privilegiado. Suministro de acceso de usuarios. Revisión de los derechos de acceso de usuarios. Retiro o ajuste de los derechos de usuario. Uso de información de información secreta para la autenticación. Restricción de acceso a la información. Procedimiento de ingreso seguro. Sistema de gestión de contraseñas. Controles de acceso físicos Seguridad de oficinas, recinto e instalaciones.	**Proyecto 4–** Control de acceso y responsabilidades de los usuarios a los sistemas y aplicaciones. Ver numeral 11.1

Tabla 35. (Continuación)

ACTIVOS	RIESGO	AMENAZAS	VALOR	TRATAMIENTO DE RIESGO	CONTROLES IMPLEMENTADOS	PROYECTOS DEFINIDOS
Servidor UPI La Vega	Pérdida de la Confidencialidad, acceso no autorizado que permite la utilización indebida o no autorizada del activo de información	[A.11] Acceso no autorizado [A.23] Manipulación del hardware	Alto	Se mitiga el riesgo con la implementación de los controles 9.1.1 - 9.1.2 - 9.2.1 - 9.2.2 - 9.2.3	Gestión de acceso a usuarios. Gestión de derechos de acceso asignados a usuarios. Acceso a redes y a Servicios de red. Suministro de acceso de usuarios. Gestión de derechos de acceso privilegiado.	**Proyecto 4-** Control de acceso y responsabilidades de los usuarios a los sistemas y aplicaciones. Ver numeral 11.1
		[E.2] Errores del administrador del sistema / de la seguridad [A.6] Abuso de privilegios de acceso	Medio	Se mitiga el riesgo con la implementación de los controles 9.1.1 - 9.1.2 – 9.2.1 - 9.2.2 - 9.2.3 - 9.2.4 - 9.2.5 - 9.2.6 - 9.3.1 - 9.4.1 - 9.4.2 - 9.4.3 -9.4.4 - 9.4.5	Política de control de acceso. Suministro de acceso a usuarios. Gestión de derechos de acceso privilegiado. Retiro o ajuste de los derechos de usuarios. Procedimientos de operación documentados.	**Proyecto 4–** Control de acceso y responsabilidades de los usuarios a los sistemas y aplicaciones. Ver numeral 11.1
Access Point	Pérdida de Disponibilidad del activo de información	[N.2] Daños por agua [I.5.3] Equipos de comunicaciones [E.25] Pérdida de equipos [A.25] Robo de equipos	Medio	Se mitiga el riesgo con la implementación de los controles 11.1.1 - 11.1.2 - 11.1.3 - 11.1.4 - 11.1.5 - 11.2.2. - 12.2.1 - 16.1.2 - 17.1.1 -	Perímetro de seguridad física. Controles de acceso físicos. Seguridad de oficinas, recinto e instalaciones. Protección contra amenazas externas y ambientales. Trabajo en áreas seguras. Servicios de suministro ubicación y protección de los equipos. Reporte de eventos de seguridad de la información. Planificación de la continuidad de la seguridad de la información. Controles contra códigos maliciosos.	**Proyecto 1-** Control de acceso físico y protección de la información (Áreas seguras y seguridad de equipos).Ver numeral 11.1 **Proyecto 2-** Responsabilidades y procedimientos de operación. Ver numeral 11.1 **Proyecto 5-** Adaptación Plan de contingencia TICS, como marco de Gestión del Plan de Continuidad del Negocio. Ver numeral 11.1 **Proyecto 7-** Gestión de incidentes de seguridad de la información. Ver numeral 11.1
	Pérdida de la Confidencialidad, acceso no autorizado que permite la utilización indebida o no autorizada del activo de información	[A.11] Acceso no autorizado [A.23] Manipulación del hardware	Alto	Se mitiga el riesgo con la implementación de los controles 9.1.1 - 9.1.2 - 9.2.1 - 9.2.2 - 9.2.3	Gestión de acceso a usuarios. Gestión de derechos de acceso asignados a usuarios. Acceso a redes y a Servicios de red. Suministro de acceso de usuarios. Gestión de derechos de acceso privilegiado.	**Proyecto 4-** Control de acceso y responsabilidades de los usuarios a los sistemas y aplicaciones. Ver numeral 11.1

Tabla 35. (Continuación)

ACTIVOS	RIESGO	AMENAZAS	VALOR	TRATAMIENTO DE RIESGO	CONTROLES IMPLEMENTADOS	PROYECTOS DEFINIDOS
Access Point	Pérdida de la Confidencialidad, acceso no autorizado que permite la utilización indebida o no autorizada del activo de información	[I.8] Fallo de servicios de comunicaciones [E.2] Errores del administrador del sistema / de la seguridad [E.4] Errores de configuración [E.19] Fugas de información [E.23] Errores de mantenimiento / actualización de equipos (hardware) [A.5] suplantación de la identidad del usuario	Medio	Se mitiga el riesgo con la implementación de los controles 11.1.3 - 11.1.4 - 11.1.5 - 12.2.1	Uso aceptable de los activos. Clasificación de la información. Política de control de acceso. Acceso a redes y a Servicios de red. Gestión de derechos de acceso privilegiado.	**Proyecto 1-** Control de acceso físico y protección de la información (Áreas seguras y seguridad de equipos).Ver numeral 11.1 **Proyecto 2-** Responsabilidades y procedimientos de operación. Ver numeral 11.1
	Pérdida de Autenticidad, en el comportamiento, resultado o uso del activo de información	[A.11] Acceso no autorizado	Alto	Se mitiga el riesgo con la implementación de los controles 9.1.1 - 9.1.2 - 9.2.1 - 9.2.2 - 9.2.3	Gestión de acceso a usuarios. Gestión de derechos de acceso asignados a usuarios. Acceso a redes y a Servicios de red. Suministro de acceso de usuarios. Gestión de derechos de acceso privilegiado.	**Proyecto 4-** Control de acceso y responsabilidades de los usuarios a los sistemas y aplicaciones. Ver numeral 11.1
		[A.5] suplantación de la identidad del usuario	Medio	Se mitiga el riesgo con la implementación de los controles 9.1.1 - 9.1.2 – 9.2.1 - 9.2.2 - 9.2.3 - 9.2.4 - 9.2.5 - 9.2.6 - 9.3.1 - 9.4.1 - 9.4.2 - 9.4.3	Política de control de acceso. Acceso a redes y a Servicios de red. Registro y cancelación del registro de usuarios. Suministro de acceso de usuarios. Gestión de derechos de acceso privilegiado. Gestión de información de autenticación secreta de usuarios. Revisión de los derechos de acceso de usuarios. Retiro o ajuste de los derechos de usuario. Uso de información de información secreta para la autenticación. Restricción de acceso a la información.	**Proyecto 4-** Control de acceso y responsabilidades de los usuarios a los sistemas y aplicaciones. Ver numeral 11.
Servidor UPI La Arcadia	Pérdida de Disponibilidad del activo de información	[I.6] Corte del suministro eléctrico	Muy Alto	Se mitiga el riesgo con la implementación del control 11.2.2 - 15.2.1	Servicios de suministro. Seguimiento y revisión de los servicios de los proveedores.	**Proyecto 1-** Control de acceso físico y protección de la información (Áreas seguras y seguridad de equipos).Ver numeral 11.1

Tabla 35. (Continuación)

ACTIVOS	RIESGO	AMENAZAS	VALOR	TRATAMIENTO DE RIESGO	CONTROLES IMPLEMENTADOS	PROYECTOS DEFINIDOS
Servidor UPI La Arcadia	Pérdida de Disponibilidad del activo de información	[N.1] Fuego [N.2] Daños por agua [N.*] Desastres naturales [I.7] Condiciones inadecuadas de temperatura o humedad [E.8] Difusión de software dañino [A.24] Denegación de servicio	Alto	Se mitiga el riesgo con la implementación de los controles 9.2.5 11.1.2 - 11.1.4 - 11.1.5 - 11.2.1 - 11.2.4. - 11.2.3 - 12.1.1 - 12.2.1 - 15.1.3	Protección contra las amenazas externas y ambientales. Trabajo en áreas seguras. Cadena de suministro de tecnología de información y comunicación. Procedimientos de operación documentados. Mantenimiento de equipos. Revisión de los derechos de acceso de usuarios. Controles de acceso físicos ubicación y protección de los equipos. Controles contra código malicioso.	**Proyecto 1-** Control de acceso físico y protección de la información (Áreas seguras y seguridad de equipos).Ver numeral 11.1 **Proyecto 2-** Responsabilidades y procedimientos de operación. Ver numeral 11.1 **Proyecto 4-** Control de acceso y responsabilidades de los usuarios. Ver numeral 11.1.
		[E.25] Pérdida de equipos [A.23] Manipulación del hardware [A.25] Robo de equipos [A.26] Ataque destructivo	Medio	Se mitiga el riesgo con la Implementación de los controles 5.1.1 - 8.1.2 - 9.1.1 - 11.1.1 -11.1.2 - 11.1.3 - 11.1.4 - 11.1.5	Políticas para la seguridad de la Información. Propiedad de los Activos. Política de control de acceso. Perímetro de seguridad física. Controles de acceso físicos. Seguridad de oficinas, recinto e instalaciones. Protección contra amenazas externas y ambientales. Trabajo en áreas seguras.	**Proyecto 1-** Control de acceso físico y protección de la información (Áreas seguras y seguridad de equipos).Ver numeral 11.1 **Proyecto 6-** Seguimiento y cumplimiento de la Política de Seguridad de la Información de la entidad. Ver numeral 11.1.
	Pérdida de la Integridad de la información, lo que implica el acceso indebido o fraudulento al activo de información	[E.8] Difusión de software dañino	Alto	Se mitiga el riesgo con la implementación de los controles 9.2.2 - 11.1.4 - 12.2.1 - 12.4.1 - 12.2.4 - 12.4.2	Protección contra amenazas externas y ambientales. Mantenimiento de equipos. Registro de eventos. Controles contra código malicioso. Suministro de acceso de usuarios. Protección de la información de registro.	**Proyecto 1-** Control de acceso físico y protección de la información (Áreas seguras y seguridad de equipos).Ver numeral 11.1 **Proyecto 2-** Responsabilidades y procedimientos de operación. Ver numeral 11.1 **Proyecto 3-** Implementación y seguimiento de registros de actividad. Ver numeral 11.1

Tabla 35. (Continuación)

ACTIVOS	RIESGO	AMENAZAS	VALOR	TRATAMIENTO DE RIESGO	CONTROLES IMPLEMENTADOS	PROYECTOS DEFINIDOS
Servidor UPI La Arcadia	Pérdida de la Integridad de la información, lo que implica el acceso indebido o fraudulento al activo de información	[A.6] Abuso de privilegios de acceso	Medio	Se mitiga el riesgo con la implementación de los controles 9.1.1 - 9.1.2 – 9.2.1 - 9.2.2 - 9.2.3 - 9.2.4 - 9.2.5 - 9.2.6 - 9.3.1 - 9.4.1 - 9.4.2 - 9.4.3	Política de control de acceso. Acceso a redes y a Servicios de red. Registro y cancelación del registro de usuarios. Gestión de derechos de acceso privilegiado. Suministro de acceso de usuarios. Revisión de los derechos de acceso de usuarios. Retiro o ajuste de los derechos de usuario. Uso de información de información secreta para la autenticación. Restricción de acceso a la información. Procedimiento de ingreso seguro. Sistema de gestión de contraseñas. Controles de acceso físicos. Seguridad de oficinas, recinto e instalaciones.	**Proyecto 4–** Control de acceso y responsabilidades de los usuarios a los sistemas y aplicaciones. Ver numeral 11.1
	Pérdida de la Confidencialidad, acceso no autorizado que permite la utilización indebida o no autorizada del activo de información	[A.11] Acceso no autorizado [A.23] Manipulación del hardware	Alto	Se mitiga el riesgo con la implementación de los controles 9.1.1 - 9.1.2 - 9.2.1 - 9.2.2 - 9.2.3	Gestión de acceso a usuarios. Gestión de derechos de acceso asignados a usuarios. Acceso a redes y a Servicios de red. Suministro de acceso de usuarios. Gestión de derechos de acceso privilegiado.	**Proyecto 4-** Control de acceso y responsabilidades de los usuarios a los sistemas y aplicaciones. Ver numeral 11.1
		[E.2] Errores del administrador del sistema / de la seguridad [A.6] Abuso de privilegios de acceso	Medio	Se mitiga el riesgo con la implementación de los controles 9.1.1 - 9.2.2 - 9.2.3 - 9.2.6 - 12.1.1	Política de control de acceso. Suministro de acceso a usuarios. Gestión de derechos de acceso privilegiado. Retiro o ajuste de los derechos de usuarios. Procedimientos de operación documentados.	**Proyecto 4–** Control de acceso y responsabilidades de los usuarios a los sistemas y aplicaciones. Ver numeral 11.1
Equipos de cómputo	Pérdida de Disponibilidad del activo de información	[E.23] Errores de mantenimiento / actualización de equipos (hardware)	Alto	Se mitiga el riesgo con la implementación de los controles 12.1.1 - 12.4.1 - 12.4.2 - 12.4.3	Procedimientos de operación documentados. Gestión de cambios. Gestión de capacidad. Separación de los ambientes de desarrollo, prueba y operación.	**Proyecto 1-** Control de acceso físico y protección de la información (Áreas seguras y seguridad de equipos).Ver numeral 11.1

Tabla 35. (Continuación)

ACTIVOS	RIESGO	AMENAZAS	VALOR	TRATAMIENTO DE RIESGO	CONTROLES IMPLEMENTADOS	PROYECTOS DEFINIDOS
Equipos de cómputo	Pérdida de Disponibilidad del activo de información	[I.5] Avería de origen físico o lógico [I.6] Corte del suministro eléctrico [E.25] Pérdida de equipos [A.6] Abuso de privilegios de acceso [A.7] uso no previsto [A.25] Robo de equipos	Medio	Se mitiga el riesgo con la implementación de los controles 11.1.1 - 11.1.2 - 11.1.3 - 11.1.4 - 11.1.5 - 11.2.2. - 12.2.1 - 16.1.2 - 17.1.1 -	Protección contra las amenazas externas y ambientales. Trabajo en áreas seguras. Cadena de suministro de tecnología de información y comunicación. Procedimientos de operación documentados. Mantenimiento de equipos. Revisión de los derechos de acceso de usuarios. Controles de acceso físicos ubicación y protección de los equipos. Controles contra códigos maliciosos.	**Proyecto 1-** Control de acceso físico y protección de la información (Áreas seguras y seguridad de equipos).Ver numeral 11.1 **Proyecto 2-** Responsabilidades y procedimientos de operación. Ver numeral 11.1 **Proyecto 4-** Control de acceso y responsabilidades de los usuarios. Ver numeral 11.1.
	Pérdida de la Integridad de la información, lo que implica el acceso indebido o fraudulento al activo de información	[I.6] Corte del suministro eléctrico [E.23] Errores de mantenimiento / actualización de equipos (hardware) [E.25] Pérdida de equipos [A.6] Abuso de privilegios de acceso [A.7] uso no previsto [A.11] Acceso no autorizado [A.23] Manipulación del hardware [A.25] Robo de equipos	Muy Alto	Se mitiga el riesgo con la implementación de los controles 11.1.1 - 11.1.2 - 11.1.3 - 11.1.4 - 11.1.5 - 11.2.2. - 12.2.1 - 16.1.2 - 17.1.1 -	Gestión de acceso a usuarios. Gestión de derechos de acceso asignados a usuarios. Acceso a redes y a Servicios de red. Suministro de acceso de usuarios. Gestión de derechos de acceso privilegiado. Protección contra las amenazas externas y ambientales. Trabajo en áreas seguras. Cadena de suministro de tecnología de información y comunicación. Procedimientos de operación documentados. Mantenimiento de equipos. Revisión de los derechos de acceso de usuarios. Controles de acceso físicos ubicación y protección de los equipos. Controles contra código malicioso.	**Proyecto 1-** Control de acceso físico y protección de la información (Áreas seguras y seguridad de equipos).Ver numeral 11.1 **Proyecto 6-** Seguimiento y cumplimiento de la Política de Seguridad de la Información de la entidad. Ver numeral 11.1.

Tabla 35. (Continuación)

ACTIVOS	RIESGO	AMENAZAS	VALOR	TRATAMIENTO DE RIESGO	CONTROLES IMPLEMENTADOS	PROYECTOS DEFINIDOS
Equipos de cómputo	Pérdida de la Integridad de la información, lo que implica el acceso indebido o fraudulento al activo de información	[N.1] Fuego [N.2] Daños por agua [N.*] Desastres naturales [I.1] Fuego [I.2] Daños por agua [I.3] Contaminación medioambiental [I.5] Avería de origen físico o lógico [I.7] Condiciones inadecuadas de temperatura o humedad [A.26] Ataque destructivo	Alto	Se mitiga el riesgo con la implementación de los controles 11.1.1 - 11.1.2 - 11.1.3 - 11.1.4 - 11.1.5 - 11.2.2. - 12.2.1 - 16.1.2 - 17.1.1 -	Protección contra las amenazas externas y ambientales. Trabajo en áreas seguras. Cadena de suministro de tecnología de información y comunicación. Procedimientos de operación documentados. Mantenimiento de equipos. Revisión de los derechos de acceso de usuarios. Controles de acceso físicos ubicación y protección de los equipos. Controles contra código malicioso.	**Proyecto 1-** Control de acceso físico y protección de la información (Áreas seguras y seguridad de equipos).Ver numeral 11.1 **Proyecto 2-** Responsabilidades y procedimientos de operación. Ver numeral 11.1 Proyecto 5- Adaptación Plan de contingencia TICS, como marco de Gestión del Plan de Continuidad del Negocio. Ver numeral 11.1 **Proyecto 7-** Gestión de incidentes de seguridad de la información. Ver numeral 11.1
	Pérdida de la Confidencialidad, acceso no autorizado que permite la utilización indebida o no autorizada del activo de información	[I.5] Avería de origen físico o lógico [I.6] Corte del suministro eléctrico [E.23] Errores de mantenimiento / actualización de equipos (hardware) [E.25] Pérdida de equipos[A.6] Abuso de privilegios de acceso [A.7] uso no previsto [A.11] Acceso no autorizado [A.25] Robo de equipos	Muy Alto	Se mitiga el riesgo con la implementación de los controles 9.1.1 - 9.1.2 - 9.2.1 - 9.2.2 - 9.2.3 - 9.2.5 11.1.2 - 11.1.4 - 11.1.5 - 11.2.1 - 11.2.4. - 11.2.3 - 12.1.1 - 12.2.1 - 15.1.3	Gestión de acceso a usuarios. Gestión de derechos de acceso asignados a usuarios. Gestión de contraseñas de usuarios. Cadena de suministro en tecnologías de la información y comunicaciones. Respuesta a los incidentes de seguridad.	**Proyecto 1-** Control de acceso físico y protección de la información (Áreas seguras y seguridad de equipos).Ver numeral 11.1 **Proyecto 4-** Control de acceso y responsabilidades de los usuarios a los sistemas y aplicaciones. Ver numeral 11.1 **Proyecto 6-** Seguimiento y cumplimiento de la Política de Seguridad de la Información de la entidad. Ver numeral 11.1.
		[N.1] Fuego [N.2] Daños por agua [N.*] Desastres naturales [I.1] Fuego [I.2] Daños por agua [I.*] Desastres industriales [I.3] Contaminación medioambiental [I.7] Condiciones inadecuadas de temperatura o humedad [A.23] Manipulación del hardware [A.26] Ataque destructivo	Alto	Se mitiga el riesgo con la implementación de los controles 11.1.1 - 11.1.2 - 11.1.3 - 11.1.4 - 11.1.5 - 11.2.2. - 12.2.1 - 16.1.2 - 17.1.1 -	Protección contra las amenazas externas y ambientales. Trabajo en áreas seguras. Cadena de suministro de tecnología de información y comunicación. Procedimientos de operación documentados. Mantenimiento de equipos. Revisión de los derechos de acceso de usuarios. Controles de acceso físicos ubicación y protección de los equipos. Controles contra código malicioso.	**Proyecto 1-** Control de acceso físico y protección de la información (Áreas seguras y seguridad de equipos).Ver numeral 11.1 **Proyecto 2-** Responsabilidades y procedimientos de operación. Ver numeral 11.1 **Proyecto 5-** Adaptación Plan de contingencia TICS, como marco de Gestión del Plan de Continuidad del Negocio. Ver numeral 11.1 **Proyecto 7-** Gestión de incidentes de seguridad de la información. Ver numeral 11.1

Tabla 35. (Continuación)

ACTIVOS	RIESGO	AMENAZAS	VALOR	TRATAMIENTO DE RIESGO	CONTROLES IMPLEMENTADOS	PROYECTOS DEFINIDOS
Equipos de cómputo	Pérdida de Autenticidad, en el comportamiento, resultado o uso del activo de información	[I.5] Avería de origen físico o lógico	Muy Alto	Se mitiga el riesgo con la implementación de los controles 9.2.5 11.1.2 - 11.1.4 - 11.1.5 - 11.2.1 - 11.2.4. - 11.2.3 - 12.1.1 - 12.2.1 - 15.1.3	Registros de actividad del administrador y operador de los sistemas. Respuesta a los incidentes de seguridad. Cadena de suministro en tecnologías de la información y comunicaciones.	**Proyecto 1-** Control de acceso físico y protección de la información (Áreas seguras y seguridad de equipos).Ver numeral 11.1 **Proyecto 2-** Responsabilidades y procedimientos de operación. Ver numeral 11.1 **Proyecto 4-** Control de acceso y responsabilidades de los usuarios. Ver numeral 11.1.
		[I.6] Corte del suministro eléctrico [E.23] Errores de mantenimiento / actualización de equipos (hardware) [E.25] Pérdida de equipos [A.6] Abuso de privilegios de acceso [A.7] uso no previsto [A.25] Robo de equipos	Alto	Se mitiga el riesgo con la Implementación de los controles 5.1.1 - 8.1.2 - 9.1.1 - 11.1.1 -11.1.2 - 11.1.3 - 11.1.4 - 11.1.5	Políticas para la seguridad de la Información. Propiedad de los Activos. Política de control de acceso. Perímetro de seguridad física. Controles de acceso físicos. Seguridad de oficinas, recinto e instalaciones. Protección contra amenazas externas y ambientales. Trabajo en áreas seguras.	**Proyecto 1-** Control de acceso físico y protección de la información (Áreas seguras y seguridad de equipos).Ver numeral 11.1 **Proyecto 4-** Control de acceso y responsabilidades de los usuarios a los sistemas y aplicaciones. Ver numeral 11.1 **Proyecto 6-** Seguimiento y cumplimiento de la Política de Seguridad de la Información de la entidad. Ver numeral 11.1.
		[N.1] Fuego [N.2] Daños por agua [N.*] Desastres naturales [I.1] Fuego [I.*] Desastres industriales [I.3] Contaminación medioambiental [I.7] Condiciones inadecuadas de temperatura o humedad [A.11] Acceso no autorizado [A.23] Manipulación del hardware	Medio	Se mitiga el riesgo con la implementación de los controles 11.1.1 - 11.1.2 - 11.1.3 - 11.1.4 - 11.1.5 - 11.2.2. - 12.2.1 - 16.1.2 - 17.1.1 -	Gestión de derechos de acceso con privilegios especiales. Protección contra las amenazas externas y ambientales. Implantación de la continuidad de la seguridad de la información.	**Proyecto 1-** Control de acceso físico y protección de la información (Áreas seguras y seguridad de equipos).Ver numeral 11.1 **Proyecto 2-** Responsabilidades y procedimientos de operación. Ver numeral 11.1 **Proyecto 5-** Adaptación Plan de contingencia TICS, como marco de Gestión del Plan de Continuidad del Negocio. Ver numeral 11.1 **Proyecto 7-** Gestión de incidentes de seguridad de la información. Ver numeral 11.1
Servidor UPI San Francisco	Pérdida de Disponibilidad del activo de información	[I.6] Corte del suministro eléctrico	Muy Alto	Se mitiga el riesgo con la implementación del control 11.2.2 - 15.2.1	Servicios de suministro. Seguimiento y revisión de los servicios de los proveedores.	**Proyecto 1-** Control de acceso físico y protección de la información (Áreas seguras y seguridad de equipos).Ver numeral 11.1

Tabla 35. (Continuación)

ACTIVOS	RIESGO	AMENAZAS	VALOR	TRATAMIENTO DE RIESGO	CONTROLES IMPLEMENTADOS	PROYECTOS DEFINIDOS
Servidor UPI San Francisco	Pérdida de Disponibilidad del activo de información	[N.1] Fuego [N.2] Daños por agua [N.*] Desastres naturales [I.7] Condiciones inadecuadas de temperatura o humedad [E.8] Difusión de software dañino [A.24] Denegación de servicio	Alto	Se mitiga el riesgo con la implementación de los controles 9.2.5 11.1.2 - 11.1.4 - 11.1.5 - 11.2.1 - 11.2.4. - 11.2.3 - 12.1.1 - 12.2.1 - 15.1.3	Protección contra las amenazas externas y ambientales. Trabajo en áreas seguras. Cadena de suministro de tecnología de información y comunicación. Procedimientos de operación documentados. Mantenimiento de equipos. Revisión de los derechos de acceso de usuarios. Controles de acceso físicos ubicación y protección de los equipos. Controles contra código malicioso.	**Proyecto 1-** Control de acceso físico y protección de la información (Áreas seguras y seguridad de equipos).Ver numeral 11.1 **Proyecto 2-** Responsabilidades y procedimientos de operación. Ver numeral 11.1 **Proyecto 4-** Control de acceso y responsabilidades de los usuarios. Ver numeral 11.1.
		[E.25] Pérdida de equipos [A.23] Manipulación del hardware [A.25] Robo de equipos [A.26] Ataque destructivo	Medio	Se mitiga el riesgo con la Implementación de los controles 5.1.1 - 8.1.2 - 9.1.1 - 11.1.1 -11.1.2 - 11.1.3 - 11.1.4 - 11.1.5	Perímetro de seguridad física. Controles de acceso físicos. Seguridad de oficinas, recinto e instalaciones. Protección contra amenazas externas y ambientales. Trabajo en áreas seguras. Servicios de suministro ubicación y protección de los equipos. Reporte de eventos de seguridad de la información. Planificación de la continuidad de la seguridad de la información. Controles contra códigos.	**Proyecto 1-** Control de acceso físico y protección de la información (Áreas seguras y seguridad de equipos).Ver numeral 11.1 **Proyecto 2-** Responsabilidades y procedimientos de operación. Ver numeral 11.1 **Proyecto 5-** Adaptación Plan de contingencia TICS, como marco de Gestión del Plan de Continuidad del Negocio. Ver numeral 11.1 **Proyecto 7-** Gestión de incidentes de seguridad de la información. Ver numeral 11.1
	Pérdida de la Integridad de la información, lo que implica el acceso indebido o fraudulento al activo de información	[E.8] Difusión de software dañino	Alto	Se mitiga el riesgo con la implementación de los controles 9.2.2 - 11.1.4 - 12.2.1 - 12.4.1 - 12.2.4 - 12.4.2	Protección contra amenazas externas y ambientales. Mantenimiento de equipos. Registro de eventos. Controles contra código malicioso. Suministro de acceso de usuarios. Protección de la información de registro.	**Proyecto 1-** Control de acceso físico y protección de la información (Áreas seguras y seguridad de equipos).Ver numeral 11.1 **Proyecto 2-** Responsabilidades y procedimientos de operación. Ver numeral 11.1 Proyecto 3- Implementación y seguimiento de registros de actividad. Ver numeral 11.1

Tabla 35. (Continuación)

ACTIVOS	RIESGO	AMENAZAS	VALOR	TRATAMIENTO DE RIESGO	CONTROLES IMPLEMENTADOS	PROYECTOS DEFINIDOS
Servidor UPI San Francisco	Pérdida de la Integridad de la información, lo que implica el acceso indebido o fraudulento al activo de información	[A.6] Abuso de privilegios de acceso	Medio	Se mitiga el riesgo con la implementación de los controles 9.1.1 - 9.1.2 – 9.2.1 - 9.2.2 - 9.2.3 - 9.2.4 - 9.2.5 - 9.2.6 - 9.3.1 - 9.4.1 - 9.4.2 - 9.4.3	Protección contra amenazas externas y ambientales. Mantenimiento de equipos. Registro de eventos. Controles contra código malicioso. Suministro de acceso de usuarios. Protección de la información de registro.	**Proyecto 4–** Control de acceso y responsabilidades de los usuarios a los sistemas y aplicaciones. Ver numeral 11.1
	Pérdida de la Confidencialidad, acceso no autorizado que permite la utilización indebida o no autorizada del activo de información	[E.25] Pérdida de equipos [A.6] Abuso de privilegios de acceso [A.11] Acceso no autorizado [A.23] Manipulación del hardware [A.25] Robo de equipos	Alto	Se mitiga el riesgo con la Implementación de los controles 5.1.1 - 8.1.2 - 9.1.1 - 11.1.1 -11.1.2 - 11.1.3 - 11.1.4 - 11.1.5	Perímetro de seguridad física. Controles de acceso físicos. Seguridad de oficinas, recinto e instalaciones. Protección contra amenazas externas y ambientales. Trabajo en áreas seguras. Servicios de suministro ubicación y protección de los equipos. Reporte de eventos de seguridad de la información. Planificación de la continuidad de la seguridad de la información. Controles contra códigos.	**Proyecto 1-** Control de acceso físico y protección de la información (Áreas seguras y seguridad de equipos).Ver numeral 11.1 **Proyecto 6-** Seguimiento y cumplimiento de la Política de Seguridad de la Información de la entidad. Ver numeral 11.1.
		[E.2] Errores del administrador del sistema / de la seguridad [E.4] Errores de configuración [A.7] uso no previsto	Medio	Se mitiga el riesgo con la 12.1.1 - 12.1.2 - 12.1.3 - 12.1.4 -	Procedimientos de operación documentados. Registro de eventos. Protección de la información de registro. Registros del administrador y del operador.	**Proyecto 2-** Responsabilidades y procedimientos de operación.
Switch de borde 4210G	Pérdida de Disponibilidad del activo de información	[I.3] Contaminación medioambiental [I.6] Corte del suministro eléctrico	Alto	Se mitiga el riesgo con la implementación del control 11.2.2 - 15.2.1	Servicios de suministro. Seguimiento y revisión de los servicios de los proveedores.	**Proyecto 1-** Control de acceso físico y protección de la información (Áreas seguras y seguridad de equipos).Ver numeral 11.1

Tabla 35. (Continuación)

ACTIVOS	RIESGO	AMENAZAS	VALOR	TRATAMIENTO DE RIESGO	CONTROLES IMPLEMENTADOS	PROYECTOS DEFINIDOS
Switch de borde 4210G	Pérdida de Disponibilidad del activo de información	[N.2] Daños por agua [N.*] Desastres naturales [I.1] Fuego [I.7] Condiciones inadecuadas de temperatura o humedad [E.4] Errores de configuración [E.23] Errores de mantenimiento / actualización de equipos (hardware) [A.25] Robo de equipos	Medio	Se mitiga el riesgo con la implementación de los controles 11.1.1 - 11.1.2 - 11.1.3 - 11.1.4 - 11.1.5 - 11.2.2. - 12.2.1 - 16.1.2 - 17.1.1 -	Protección contra las amenazas externas y ambientales. Trabajo en áreas seguras. Cadena de suministro de tecnología de información y comunicación. Procedimientos de operación documentados. Mantenimiento de equipos. Revisión de los derechos de acceso de usuarios. Controles de acceso físicos ubicación y protección de los equipos. Controles contra código malicioso.	**Proyecto 1-** Control de acceso físico y protección de la información (Áreas seguras y seguridad de equipos).Ver numeral 11.1 **Proyecto 2-** Responsabilidades y procedimientos de operación. Ver numeral 11.1 **Proyecto 5-** Adaptación Plan de contingencia TICS, como marco de Gestión del Plan de Continuidad del Negocio. Ver numeral 11.1 **Proyecto 7-** Gestión de incidentes de seguridad de la información. Ver numeral 11.1
Sistema de almacenamiento formato rack	Pérdida de Disponibilidad del activo de información	[I.6.12] Interrupción deliberada por un agente externo	Muy Alto	Se mitiga el riesgo con la implementación de los controles 11.2.4 - 12.1.1 - 12.6.1	Mantenimiento de equipos. Procedimientos de operación documentados. Gestión de las vulnerabilidades técnicas.	**Proyecto 2-** Responsabilidades y procedimientos de operación. Ver numeral 11.1 **Proyecto 3-** Implementación y seguimiento de registro de actividad. Ver numeral 11.1
	Pérdida de la Integridad de la información, lo que implica el acceso indebido o fraudulento al activo de información	[I.6.12] Interrupción deliberada por un agente externo	Muy Alto	Se mitiga el riesgo con la implementación de los controles 11.2.4 - 12.1.1 - 12.6.1	Mantenimiento de equipos. Procedimientos de operación documentados. Gestión de las vulnerabilidades técnicas.	**Proyecto 2-** Responsabilidades y procedimientos de operación. Ver numeral 11.1 **Proyecto 3-** Implementación y seguimiento de registro de actividad. Ver numeral 11.1
Gabinete de 8 blades	Pérdida de Disponibilidad del activo de información	[E.24] caída del sistema por agotamiento de recursos	Muy Alto	Se mitiga el riesgo con la Implementación de los controles 12.1.1 - 12.1.3 - 12.4.1	Procedimientos de operación documentados. Registro y gestión de eventos de seguridad. Gestión de capacidad.	**Proyecto 2-** Responsabilidades y procedimientos de operación. Ver numeral 11.1

Tabla 35. (Continuación)

ACTIVOS	RIESGO	AMENAZAS	VALOR	TRATAMIENTO DE RIESGO	CONTROLES IMPLEMENTADOS	PROYECTOS DEFINIDOS
Gabinete de 8 blades	Pérdida de Disponibilidad del activo de información	[E.23] Errores de mantenimiento / actualización de equipos (hardware)	Alto	Se mitiga el riesgo con la implementación de los controles 9.2.5 11.1.2 - 11.1.4 - 11.1.5 - 11.2.1 - 11.2.4. - 11.2.3 - 12.1.1 - 12.2.1 - 15.1.3	Protección contra las amenazas externas y ambientales. Trabajo en áreas seguras. Cadena de suministro de tecnología de información y comunicación. Procedimientos de operación documentados. Mantenimiento de equipos. Revisión de los derechos de acceso de usuarios. Controles de acceso físicos ubicación y protección de los equipos. Controles contra códigos maliciosos.	**Proyecto 1-** Control de acceso físico y protección de la información (Áreas seguras y seguridad de equipos).Ver numeral 11.1 **Proyecto 2-** Responsabilidades y procedimientos de operación. Ver numeral 11.1 **Proyecto 4-** Control de acceso y responsabilidades de los usuarios. Ver numeral 11.1.
	Pérdida de la Integridad de la información, lo que implica el acceso indebido o fraudulento al activo de información	[E.24] caída del sistema por agotamiento de recursos	Muy Alto	Se mitiga el riesgo con la Implementación de los controles 12.1.1 - 12.1.3 - 12.4.1	Procedimientos de operación documentados. Registro y gestión de eventos de seguridad. Gestión de capacidad.	**Proyecto 2-** Responsabilidades y procedimientos de operación. Ver numeral 11.1
		[E.23] Errores de mantenimiento / actualización de equipos (hardware)	Alto	Se mitiga el riesgo con la implementación de los controles 9.2.5 11.1.2 - 11.1.4 - 11.1.5 - 11.2.1 - 11.2.4. - 11.2.3 - 12.1.1 - 12.2.1 - 15.1.3	Protección contra las amenazas externas y ambientales. Trabajo en áreas seguras. Cadena de suministro de tecnología de información y comunicación. Procedimientos de operación documentados. Mantenimiento de equipos. Revisión de los derechos de acceso de usuarios. Controles de acceso físicos ubicación y protección de los equipos. Controles contra códigos maliciosos.	**Proyecto 1-** Control de acceso físico y protección de la información (Áreas seguras y seguridad de equipos).Ver numeral 11.1 **Proyecto 2-** Responsabilidades y procedimientos de operación. Ver numeral 11.1 **Proyecto 4-** Control de acceso y responsabilidades de los usuarios. Ver numeral 11.1.

Tabla 35. (Continuación)

ACTIVOS	RIESGO	AMENAZAS	VALOR	TRATAMIENTO DE RIESGO	CONTROLES IMPLEMENTADOS	PROYECTOS DEFINIDOS
Equipo de Seguridad Perimetral	Pérdida de Disponibilidad del activo de información	[N.1] Fuego [N.2] Daños por agua [N.*] Desastres naturales [E.2] Errores del administrador del sistema / de la seguridad [E.4] Errores de configuración [E.21] Errores de mantenimiento / actualización de programas (software) [A.23] Manipulación del hardware	Muy Alto	Se mitiga el riesgo con la implementación de los controles 9.1.1 - 9.1.2 - 9.2.1 - 9.2.2 - 9.2.3 - 9.2.5 11.1.2 - 11.1.4 - 11.1.5 - 11.2.1 - 11.2.4. - 11.2.3 - 12.1.1 - 12.2.1 - 15.1.3	Gestión de acceso a usuarios. Gestión de derechos de acceso asignados a usuarios. Acceso a redes y a Servicios de red. Suministro de acceso de usuarios. Gestión de derechos de acceso privilegiado. Protección contra las amenazas externas y ambientales. Trabajo en áreas seguras. Cadena de suministro de tecnología de información y comunicación. Procedimientos de operación documentados. Mantenimiento de equipos. Revisión de los derechos de acceso de usuarios. Controles de acceso físicos ubicación y protección de los equipos. Controles contra código malicioso. Procedimientos de operación documentados. Registro de eventos. Protección de la información de registro. Registros del administrador y del operador.	**Proyecto 1-** Control de acceso físico y protección de la información (Áreas seguras y seguridad de equipos).Ver numeral 11.1 **Proyecto 2-** Responsabilidades y procedimientos de operación. **Proyecto 4-** Control de acceso y responsabilidades de los usuarios a los sistemas y aplicaciones. Ver numeral 11.1 **Proyecto 6-** Seguimiento y cumplimiento de la Política de Seguridad de la Información de la entidad. Ver numeral 11.1.
		[A.11] Acceso no autorizado [A.24] Denegación de servicio	Alto	Se mitiga el riesgo con la implementación de los controles 9.1.1 - 9.1.2 - 9.2.1 - 9.2.2 - 9.2.3	Gestión de acceso a usuarios. Gestión de derechos de acceso asignados a usuarios. Acceso a redes y a Servicios de red. Suministro de acceso de usuarios. Gestión de derechos de acceso privilegiado.	**Proyecto 4-** Control de acceso y responsabilidades de los usuarios a los sistemas y aplicaciones. Ver numeral 11.1

Tabla 35. (Continuación)

ACTIVOS	RIESGO	AMENAZAS	VALOR	TRATAMIENTO DE RIESGO	CONTROLES IMPLEMENTADOS	PROYECTOS DEFINIDOS
Equipo de Seguridad Perimetral	Pérdida de la Integridad de la información, lo que implica el acceso indebido o fraudulento al activo de información	[N.1] Fuego [N.2] Daños por agua [N.*] Desastres naturales [E.3] Errores de monitorización (log) [E.4] Errores de configuración [E.21] Errores de mantenimiento / actualización de programas (software) [A.12] Análisis de tráfico [A.23] Manipulación del hardware	Alto	Se mitiga el riesgo con la implementación de los controles 9.1.1 - 9.1.2 - 9.2.1 - 9.2.2 - 9.2.3 - 9.2.5 11.1.2 - 11.1.4 - 11.1.5 - 11.2.1 - 11.2.4. - 11.2.3 - 12.1.1 - 12.2.1 - 15.1.3	Protección contra las amenazas externas y ambientales. Trabajo en áreas seguras. Cadena de suministro de tecnología de información y comunicación. Procedimientos de operación documentados. Mantenimiento de equipos. Revisión de los derechos de acceso de usuarios. Controles de acceso físicos ubicación y protección de los equipos. Controles contra códigos maliciosos.	**Proyecto 1-** Control de acceso físico y protección de la información (Áreas seguras y seguridad de equipos).Ver numeral 11.1 **Proyecto 2-** Responsabilidades y procedimientos de operación. **Proyecto 4-** Control de acceso y responsabilidades de los usuarios a los sistemas y aplicaciones. Ver numeral 11.1
		[A.3] Manipulación de los registros de actividad (log) [A.11] Acceso no autorizado [A.24] Denegación de servicio	Medio	Se mitiga el riesgo con la implementación de los controles 9.1.1 - 9.1.2 - 9.2.1 - 9.2.2 - 9.2.3 - 9.2.5 11.1.2 - 11.1.4 - 11.1.5 - 11.2.1 - 11.2.4. - 11.2.3 - 12.1.1 - 12.2.1 - 12.4.1 - 12.4.2 - 12.4.3 - 15.1.3	Procedimientos de operación documentados. Registro de eventos. Protección de la información de registro. Registros del administrador y del operador. Protección contra las amenazas externas y ambientales. Trabajo en áreas seguras. Cadena de suministro de tecnología de información y comunicación. Procedimientos de operación documentados. Mantenimiento de equipos. Revisión de los derechos de acceso de usuarios. Controles de acceso físicos ubicación y protección de los equipos. Controles contra códigos maliciosos.	**Proyecto 1-** Control de acceso físico y protección de la información (Áreas seguras y seguridad de equipos).Ver numeral 11.1 **Proyecto 2-** Responsabilidades y procedimientos de operación. Ver numeral 11.1 **Proyecto 4-** Control de acceso y responsabilidades de los usuarios. Ver numeral 11.1.

Tabla 35. (Continuación)

ACTIVOS	RIESGO	AMENAZAS	VALOR	TRATAMIENTO DE RIESGO	CONTROLES IMPLEMENTADOS	PROYECTOS DEFINIDOS
Equipo de Seguridad Perimetral	Pérdida de la Confidencialidad, acceso no autorizado que permite la utilización indebida o no autorizada del activo de información	[E.2] Errores del administrador del sistema / de la seguridad [E.3] Errores de monitorización (log) [E.4] Errores de configuración [E.21] Errores de mantenimiento / actualización de programas (software)	Medio	Se mitiga el riesgo con la implementación de los controles 9.1.1 - 9.1.2 - 9.2.1 - 9.2.2 - 9.2.3 - 9.2.5 11.1.2 - 11.1.4 - 11.1.5 - 11.2.1 - 11.2.4. - 11.2.3 - 12.1.1 - 12.2.1 - 15.1.3	Protección contra las amenazas externas y ambientales. Trabajo en áreas seguras. Cadena de suministro de tecnología de información y comunicación. Procedimientos de operación documentados. Mantenimiento de equipos. Revisión de los derechos de acceso de usuarios. Controles de acceso físicos ubicación y protección de los equipos. Controles contra códigos maliciosos.	**Proyecto 1-** Control de acceso físico y protección de la información (Áreas seguras y seguridad de equipos).Ver numeral 11.1 **Proyecto 2-** Responsabilidades y procedimientos de operación. Ver numeral 11.1 **Proyecto 4-** Control de acceso y responsabilidades de los usuarios. Ver numeral 11.1.
		[A.3] Manipulación de los registros de actividad (log) [A.12] Análisis de tráfico [A.23] Manipulación del hardware	Medio	Se mitiga el riesgo con la implementación de los controles 9.1.1 - 9.1.2 - 9.2.1 - 9.2.2 - 9.2.3 - 9.2.5 11.1.2 - 11.1.4 - 11.1.5 - 11.2.1 - 11.2.4. - 11.2.3 - 12.1.1 - 12.2.1 - 15.1.3	Procedimientos de operación documentados. Registro de eventos. Protección de la información de registro. Registros del administrador y del operador. Protección contra las amenazas externas y ambientales. Trabajo en áreas seguras. Cadena de suministro de tecnología de información y comunicación. Procedimientos de operación documentados. Mantenimiento de equipos. Revisión de los derechos de acceso de usuarios. Controles de acceso físicos ubicación y protección de los equipos. Controles contra códigos maliciosos.	**Proyecto 1-** Control de acceso físico y protección de la información (Áreas seguras y seguridad de equipos).Ver numeral 11.1 **Proyecto 2-** Responsabilidades y procedimientos de operación. Ver numeral 11.1 **Proyecto 4-** Control de acceso y responsabilidades de los usuarios. Ver numeral 11.1.
Servidor formato blade marca Hewlett Packard Modelo proliant BL460C G1	Pérdida de Disponibilidad del activo de información	[I.6] Corte del suministro eléctrico	Muy Alto	Se mitiga el riesgo con la implementación del control 11.2.2 - 15.2.1	Servicios de suministro. Seguimiento y revisión de los servicios de los proveedores.	**Proyecto 1-** Control de acceso físico y protección de la información (Áreas seguras y seguridad de equipos).Ver numeral 11.1

Tabla 35. (Continuación)

ACTIVOS	RIESGO	AMENAZAS	VALOR	TRATAMIENTO DE RIESGO	CONTROLES IMPLEMENTADOS	PROYECTOS DEFINIDOS
Servidor formato blade marca Hewlett Packard Modelo proliant BL460C G1	Pérdida de Disponibilidad del activo de información	[N.1] Fuego [N.2] Daños por agua [N.*] Desastres naturales [I.7] Condiciones inadecuadas de temperatura o humedad [E.8] Difusión de software dañino [A.24] Denegación de servicio	Alto	Se mitiga el riesgo con la implementación de los controles 9.2.5 11.1.2 - 11.1.4 - 11.1.5 - 11.2.1 - 11.2.4. - 11.2.3 - 12.1.1 - 12.2.1 - 15.1.3	Protección contra las amenazas externas y ambientales. Trabajo en áreas seguras. Cadena de suministro de tecnología de información y comunicación. Procedimientos de operación documentados. Mantenimiento de equipos. Revisión de los derechos de acceso de usuarios. Controles de acceso físicos ubicación y protección de los equipos. Controles contra código malicioso.	**Proyecto 1-** Control de acceso físico y protección de la información (Áreas seguras y seguridad de equipos).Ver numeral 11.1 **Proyecto 4-** Control de acceso y responsabilidades de los usuarios a los sistemas y aplicaciones. Ver numeral 11.1 **Proyecto 6-** Seguimiento y cumplimiento de la Política de Seguridad de la Información de la entidad. Ver numeral 11.1.
		[E.25] Pérdida de equipos [A.23] Manipulación del hardware [A.25] Robo de equipos [A.26] Ataque destructivo	Medio	Se mitiga el riesgo con la implementación de los controles 5.1.1 - 8.1.2 - 9.1.1 - 11.1.1 -11.1.2 - 11.1.3 - 11.1.4 - 11.1.5	Políticas para la seguridad de la Información. Propiedad de los Activos. Política de control de acceso. Perímetro de seguridad física. Controles de acceso físicos. Seguridad de oficinas, recinto e instalaciones. Protección contra amenazas externas y ambientales. Trabajo en áreas seguras.	**Proyecto 1-** Control de acceso físico y protección de la información (Áreas seguras y seguridad de equipos).Ver numeral 11.1 **Proyecto 6-** Seguimiento y cumplimiento de la Política de Seguridad de la Información de la entidad. Ver numeral 11.1
	Pérdida de la Integridad de la información, lo que implica el acceso indebido o fraudulento al activo de información	[E.8] Difusión de software dañino [A.6] Abuso de privilegios de acceso	Alto	Se mitiga el riesgo con la implementación de los controles 9.2.2 - 11.1.4 - 12.2.1 - 12.4.1 - 12.2.4 - 12.4.2	Protección contra amenazas externas y ambientales. Mantenimiento de equipos. Registro de eventos. Controles contra código malicioso. Suministro de acceso de usuarios. Protección de la información de registro.	Proyecto 4– Control de acceso y responsabilidades de los usuarios a los sistemas y aplicaciones. Ver numeral 11.1
	Pérdida de la Confidencialidad, acceso no autorizado que permite la utilización indebida o no autorizada del activo de información	[E.25] Pérdida de equipos [A.6] Abuso de privilegios de acceso [A.11] Acceso no autorizado [A.23] Manipulación del hardware [A.25] Robo de equipos	Alto	Se mitiga el riesgo con la Implementación de los controles 5.1.1 - 8.1.2 - 9.1.1 - 11.1.1 -11.1.2 - 11.1.3 - 11.1.4 - 11.1.5	Políticas para la seguridad de la Información. Propiedad de los Activos. Política de control de acceso. Perímetro de seguridad física. Controles de acceso físicos. Seguridad de oficinas, recinto e instalaciones. Protección contra amenazas externas y ambientales. Trabajo en áreas seguras.	**Proyecto 1-** Control de acceso físico y protección de la información (Áreas seguras y seguridad de equipos).Ver numeral 11.1 **Proyecto 6-** Seguimiento y cumplimiento de la Política de Seguridad de la Información de la entidad. Ver numeral 11.1

Tabla 35. (Continuación)

ACTIVOS	RIESGO	AMENAZAS	VALOR	TRATAMIENTO DE RIESGO	CONTROLES IMPLEMENTADOS	PROYECTOS DEFINIDOS
Servidor formato blade marca Hewlett Packard Modelo proliant BL460C G1	Pérdida de la Confidencialidad, acceso no autorizado que permite la utilización indebida o no autorizada del activo de información	[E.2] Errores del administrador del sistema / de la seguridad	Medio	Se mitiga el riesgo con la implementación de los controles 9.1.1 - 9.1.2 - 9.2.1 - 9.2.2 - 9.2.3 - 9.2.5 11.1.2 - 11.1.4 - 11.1.5 - 11.2.1 - 11.2.4. - 11.2.3 - 12.1.1 - 12.2.1 - 15.1.3	Procedimientos de operación documentados. Registro de eventos. Protección de la información de registro. Registros del administrador y del operador.	**Proyecto 1-** Control de acceso físico y protección de la información (Áreas seguras y seguridad de equipos).Ver numeral 11.1 **Proyecto 2-** Responsabilidades y procedimientos de operación. Ver numeral 11.1 **Proyecto 4-** Control de acceso y responsabilidades de los usuarios. Ver numeral 11.1.
		[E.4] Errores de configuración			Gestión de cambios en los servicios prestados por terceros.	
		[A.7] uso no previsto			Responsabilidades y procedimientos.	
Servidor formato blade marca Hewlett Packard. Modelo proliant BL460C G7	Pérdida de Disponibilidad del activo de información	[I.6] Corte del suministro eléctrico	Muy Alto	Se mitiga el riesgo con la implementación del control 11.2.2 - 15.2.1	Servicios de suministro. Seguimiento y revisión de los servicios de los proveedores.	**Proyecto 1-** Control de acceso físico y protección de la información (Áreas seguras y seguridad de equipos).Ver numeral 11.1
		[N.1] Fuego [N.2] Daños por agua [N.*] Desastres naturales [I.7] Condiciones inadecuadas de temperatura o humedad [E.8] Difusión de software dañino [A.24] Denegación de servicio	Alto	Se mitiga el riesgo con la implementación de los controles 9.2.5 11.1.2 - 11.1.4 - 11.1.5 - 11.2.1 - 11.2.4. - 11.2.3 - 12.1.1 - 12.2.1 - 15.1.3	Protección contra las amenazas externas y ambientales. Trabajo en áreas seguras. Cadena de suministro de tecnología de información y comunicación. Procedimientos de operación documentados. Mantenimiento de equipos. Revisión de los derechos de acceso de usuarios. Controles de acceso físicos ubicación y protección de los equipos. Controles contra código malicioso.	**Proyecto 1-** Control de acceso físico y protección de la información (Áreas seguras y seguridad de equipos).Ver numeral 11.1 **Proyecto 2-** Responsabilidades y procedimientos de operación. Ver numeral 11.1 **Proyecto 4-** Control de acceso y responsabilidades de los usuarios. Ver numeral 11.1.
		[E.25] Pérdida de equipos [A.23] Manipulación del hardware [A.25] Robo de equipos [A.26] Ataque destructivo	Medio	Se mitiga el riesgo con la Implementación de los controles 5.1.1 - 8.1.2 - 9.1.1 - 11.1.1 -11.1.2 - 11.1.3 - 11.1.4 - 11.1.5	Políticas para la seguridad de la Información. Propiedad de los Activos. Política de control de acceso. Perímetro de seguridad física. Controles de acceso físicos. Seguridad de oficinas, recinto e instalaciones. Protección contra amenazas externas y ambientales. Trabajo en áreas seguras.	**Proyecto 1-** Control de acceso físico y protección de la información (Áreas seguras y seguridad de equipos).Ver numeral 11.1 **Proyecto 6-** Seguimiento y cumplimiento de la Política de Seguridad de la Información de la entidad. Ver numeral 11.1

Tabla 35. (Continuación)

ACTIVOS	RIESGO	AMENAZAS	VALOR	TRATAMIENTO DE RIESGO	CONTROLES IMPLEMENTADOS	PROYECTOS DEFINIDOS
Servidor formato blade marca Hewlett Packard. Modelo proliant BL460C G7	Pérdida de la Integridad de la información, lo que implica el acceso indebido o fraudulento al activo de información	[E.8] Difusión de software dañino [A.6] Abuso de privilegios de acceso	Alto	Se mitiga el riesgo con la implementación de los controles 9.2.2 - 11.1.4 - 12.2.1 - 12.4.1 - 12.2.4 - 12.4.2	Protección contra amenazas externas y ambientales. Mantenimiento de equipos Registro de eventos. Controles contra código malicioso. Suministro de acceso de usuarios. Protección de la información de registro.	**Proyecto 1-** Control de acceso físico y protección de la información (Áreas seguras y seguridad de equipos).Ver numeral 11.1 **Proyecto 2-** Responsabilidades y procedimientos de operación. Ver numeral 11.1 **Proyecto 3-** Implementación y seguimiento de registros de actividad. Ver numeral 11.1
	Pérdida de la Confidencialidad, acceso no autorizado que permite la utilización indebida o no autorizada del activo de información	[E.25] Pérdida de equipos [A.6] Abuso de privilegios de acceso [A.11] Acceso no autorizado [A.23] Manipulación del hardware [A.25] Robo de equipos	Alto	Se mitiga el riesgo con la implementación de los controles 5.1.1 - 8.1.2 - 9.1.1 - 11.1.1 -11.1.2 - 11.1.3 - 11.1.4 - 11.1.5	Políticas para la seguridad de la Información. Propiedad de los Activos. Política de control de acceso. Perímetro de seguridad física. Controles de acceso físicos. Seguridad de oficinas, recinto e instalaciones. Protección contra amenazas externas y ambientales. Trabajo en áreas seguras.	**Proyecto 1-** Control de acceso físico y protección de la información (Áreas seguras y seguridad de equipos).Ver numeral 11.1 **Proyecto 6-** Seguimiento y cumplimiento de la Política de Seguridad de la Información de la entidad. Ver numeral 11.1.
		[E.2] Errores del administrador del sistema / de la seguridad [E.4] Errores de configuración [A.7] uso no previsto	Medio	Se mitiga el riesgo con la implementación de los controles 9.1.1 - 9.1.2 - 9.2.1 - 9.2.2 - 9.2.3 - 9.2.5 11.1.2 - 11.1.4 - 11.1.5 - 11.2.1 - 11.2.4. - 11.2.3 - 12.1.1 - 12.2.1 - 15.1.3	Procedimientos de operación documentados. Registro de eventos. Protección de la información de registro. Registros del administrador y del operador. Gestión de cambios en los servicios prestados por terceros Responsabilidades y procedimientos.	**Proyecto 1-** Control de acceso físico y protección de la información (Áreas seguras y seguridad de equipos).Ver numeral 11.1 **Proyecto 2-** Responsabilidades y procedimientos de operación. Ver numeral 11.1 **Proyecto 4-** Control de acceso y responsabilidades de los usuarios. Ver numeral 11.1.
Servidor Proliant 120 G5	Pérdida de Disponibilidad del activo de información	[I.6] Corte del suministro eléctrico	Muy Alto	Se mitiga el riesgo con la implementación del control 11.2.2 - 15.2.1	Servicios de suministro. Seguimiento y revisión de los servicios de los proveedores.	**Proyecto 1-** Control de acceso físico y protección de la información (Áreas seguras y seguridad de equipos).Ver numeral 11.1

Tabla 35. (Continuación)

ACTIVOS	RIESGO	AMENAZAS	VALOR	TRATAMIENTO DE RIESGO	CONTROLES IMPLEMENTADOS	PROYECTOS DEFINIDOS
Servidor Proliant 120 G5	Pérdida de Disponibilidad del activo de información	[N.1] Fuego [N.2] Daños por agua [N.*] Desastres naturales [I.7] Condiciones inadecuadas de temperatura o humedad [E.8] Difusión de software dañino [A.24] Denegación de servicio	Alto	Se mitiga el riesgo con la implementación de los controles 9.2.5 11.1.2 - 11.1.4 - 11.1.5 - 11.2.1 - 11.2.4. - 11.2.3 - 12.1.1 - 12.2.1 - 15.1.3	Protección contra las amenazas externas y ambientales. Trabajo en áreas seguras. Cadena de suministro de tecnología de información y comunicación. Procedimientos de operación documentados. Mantenimiento de equipos. Revisión de los derechos de acceso de usuarios. Controles de acceso físicos ubicación y protección de los equipos. Controles contra código malicioso.	**Proyecto 1-** Control de acceso físico y protección de la información (Áreas seguras y seguridad de equipos).Ver numeral 11.1 **Proyecto 2-** Responsabilidades y procedimientos de operación. Ver numeral 11.1 **Proyecto 4-** Control de acceso y responsabilidades de los usuarios. Ver numeral 11.1.
		[E.25] Pérdida de equipos [A.23] Manipulación del hardware [A.25] Robo de equipos [A.26] Ataque destructivo	Medio	Se mitiga el riesgo con la Implementación de los controles 5.1.1 - 8.1.2 - 9.1.1 - 11.1.1 -11.1.2 - 11.1.3 - 11.1.4 - 11.1.5	Políticas para la seguridad de la Información. Propiedad de los Activos. Política de control de acceso. Perímetro de seguridad física. Controles de acceso físicos. Seguridad de oficinas, recinto e instalaciones. Protección contra amenazas externas y ambientales. Trabajo en áreas seguras.	**Proyecto 1-** Control de acceso físico y protección de la información (Áreas seguras y seguridad de equipos).Ver numeral 11.1 **Proyecto 6-** Seguimiento y cumplimiento de la Política de Seguridad de la Información de la entidad. Ver numeral 11.1
	Pérdida de la Integridad de la información, lo que implica el acceso indebido o fraudulento al activo de información	[E.8] Difusión de software dañino [A.6] Abuso de privilegios de acceso	Alto	Se mitiga el riesgo con la implementación de los controles 9.2.2 - 11.1.4 - 12.2.1 - 12.4.1 - 12.2.4 - 12.4.2	Protección contra amenazas externas y ambientales. Mantenimiento de equipos. Registro de eventos. Controles contra código malicioso. Suministro de acceso de usuarios. Protección de la información de registro.	**Proyecto 1-** Control de acceso físico y protección de la información (Áreas seguras y seguridad de equipos).Ver numeral 11.1 **Proyecto 2-** Responsabilidades y procedimientos de operación. Ver numeral 11.1 **Proyecto 3-** Implementación y seguimiento de registros de actividad. Ver numeral 11.1

Tabla 35. (Continuación)

ACTIVOS	RIESGO	AMENAZAS	VALOR	TRATAMIENTO DE RIESGO	CONTROLES IMPLEMENTADOS	PROYECTOS DEFINIDOS
Servidor Proliant 120 G5	Pérdida de la Confidencialidad, acceso no autorizado que permite la utilización indebida o no autorizada del activo de información	[E.25] Pérdida de equipos [A.6] Abuso de privilegios de acceso [A.11] Acceso no autorizado [A.23] Manipulación del hardware [A.25] Robo de equipos	Alto	Se mitiga el riesgo con la Implementación de los controles 5.1.1 - 8.1.2 - 9.1.1 - 11.1.1 -11.1.2 - 11.1.3 - 11.1.4 - 11.1.5	Gestión de acceso a usuarios. Gestión de derechos de acceso asignados a usuarios. Acceso a redes y a Servicios de red. Suministro de acceso de usuarios. Gestión de derechos de acceso privilegiado. Protección contra las amenazas externas y ambientales. Trabajo en áreas seguras. Cadena de suministro de tecnología de información y comunicación. Procedimientos de operación documentados. Mantenimiento de equipos. Revisión de los derechos de acceso de usuarios. Controles de acceso físicos ubicación y protección de los equipos. Controles contra código malicioso.	**Proyecto 1-** Control de acceso físico y protección de la información (Áreas seguras y seguridad de equipos).Ver numeral 11.1 **Proyecto 6-** Seguimiento y cumplimiento de la Política de Seguridad de la Información de la entidad. Ver numeral 11.1
		[E.2] Errores del administrador del sistema / de la seguridad [E.4] Errores de configuración [A.7] uso no previsto	Medio	Se mitiga el riesgo con la implementación de los controles 9.1.1 - 9.1.2 - 9.2.1 - 9.2.2 - 9.2.3 - 9.2.5 11.1.2 - 11.1.4 - 11.1.5 - 11.2.1 - 11.2.4. - 11.2.3 - 12.1.1 - 12.2.1 - 15.1.3	Procedimientos de operación documentados. Registro de eventos. Protección de la información de registro. Registros del administrador y del operador.	**Proyecto 2-** Responsabilidades y procedimientos de operación.
Servidor Proyecto Misión Bogotá	Pérdida de Disponibilidad del activo de información	[I.6] Corte del suministro eléctrico	Muy Alto	Se mitiga el riesgo con la implementación del control 11.2.2 - 15.2.1	Servicios de suministro. Seguimiento y revisión de los servicios de los proveedores.	**Proyecto 1-** Control de acceso físico y protección de la información (Áreas seguras y seguridad de equipos).Ver numeral 11.1

Tabla 35. (Continuación)

ACTIVOS	RIESGO	AMENAZAS	VALOR	TRATAMIENTO DE RIESGO	CONTROLES IMPLEMENTADOS	PROYECTOS DEFINIDOS
Servidor Proyecto Misión Bogotá	Pérdida de Disponibilidad del activo de información	[N.1] Fuego [N.2] Daños por agua [N.*] Desastres naturales [I.7] Condiciones inadecuadas de temperatura o humedad [E.8] Difusión de software dañino [A.24] Denegación de servicio	Alto	Se mitiga el riesgo con la implementación de los controles 9.2.5 11.1.2 - 11.1.4 - 11.1.5 - 11.2.1 - 11.2.4. - 11.2.3 - 12.1.1 - 12.2.1 - 15.1.3	Protección contra las amenazas externas y ambientales. Trabajo en áreas seguras. Cadena de suministro de tecnología de información y comunicación. Procedimientos de operación documentados. Mantenimiento de equipos. Revisión de los derechos de acceso de usuarios. Controles de acceso físicos ubicación y protección de los equipos. Controles contra código malicioso.	**Proyecto 1-** Control de acceso físico y protección de la información (Áreas seguras y seguridad de equipos).Ver numeral 11.1 **Proyecto 2-** Responsabilidades y procedimientos de operación. Ver numeral 11.1 **Proyecto 4-** Control de acceso y responsabilidades de los usuarios. Ver numeral 11.1.
		[E.25] Pérdida de equipos [A.23] Manipulación del hardware [A.25] Robo de equipos [A.26] Ataque destructivo	Medio	Se mitiga el riesgo con la Implementación de los controles 5.1.1 - 8.1.2 - 9.1.1 - 11.1.1 -11.1.2 - 11.1.3 - 11.1.4 - 11.1.5	Políticas para la seguridad de la Información. Propiedad de los Activos. Política de control de acceso. Perímetro de seguridad física. Controles de acceso físicos. Seguridad de oficinas, recinto e instalaciones. Protección contra amenazas externas y ambientales. Trabajo en áreas seguras.	**Proyecto 1-** Control de acceso físico y protección de la información (Áreas seguras y seguridad de equipos).Ver numeral 11.1 **Proyecto 6-** Seguimiento y cumplimiento de la Política de Seguridad de la Información de la entidad. Ver numeral 11.1.
	Pérdida de la Integridad de la información, lo que implica el acceso indebido o fraudulento al activo de información	[E.8] Difusión de software dañino [A.6] Abuso de privilegios de acceso	Alto	Se mitiga el riesgo con la implementación de los controles 9.2.2 - 11.1.4 - 12.2.1 - 12.4.1 - 12.2.4 - 12.4.2	Protección contra amenazas externas y ambientales. Mantenimiento de equipos. Registro de eventos. Controles contra código malicioso. Suministro de acceso de usuarios. Protección de la información de registro.	**Proyecto 4–** Control de acceso y responsabilidades de los usuarios a los sistemas y aplicaciones. Ver numeral 11.1

Tabla 35. (Continuación)

ACTIVOS	RIESGO	AMENAZAS	VALOR	TRATAMIENTO DE RIESGO	CONTROLES IMPLEMENTADOS	PROYECTOS DEFINIDOS
Servidor Proyecto Misión Bogotá	Pérdida de la Confidencialidad, acceso no autorizado que permite la utilización indebida o no autorizada del activo de información	[E.25] Pérdida de equipos [A.6] Abuso de privilegios de acceso [A.11] Acceso no autorizado [A.23] Manipulación del hardware [A.25] Robo de equipos	Alto	Se mitiga el riesgo con la implementación de los controles 9.1.1 - 9.1.2 – 9.2.1 - 9.2.2 - 9.2.3 - 9.2.4 - 9.2.5 - 9.2.6 - 9.3.1 - 9.4.1 - 9.4.2 - 9.4.3 -9.4.4 - 9.4.5	Gestión de acceso a usuarios. Gestión de derechos de acceso asignados a usuarios. Acceso a redes y a Servicios de red. Suministro de acceso de usuarios. Gestión de derechos de acceso privilegiado. Protección contra las amenazas externas y ambientales. Trabajo en áreas seguras. Cadena de suministro de tecnología de información y comunicación. Procedimientos de operación documentados. Mantenimiento de equipos. Revisión de los derechos de acceso de usuarios. Controles de acceso físicos ubicación y protección de los equipos. Controles contra código malicioso.	**Proyecto 1-** Control de acceso físico y protección de la información (Áreas seguras y seguridad de equipos).Ver numeral 11.1 **Proyecto 6-** Seguimiento y cumplimiento de la Política de Seguridad de la Información de la entidad. Ver numeral 11.1.
		[E.2] Errores del administrador del sistema / de la seguridad	Medio	Se mitiga el riesgo con la implementación de los controles 9.1.1 - 9.1.2 - 9.2.1 - 9.2.2 - 9.2.3 - 9.2.5 11.1.2 - 11.1.4 - 11.1.5 - 11.2.1 - 11.2.4. - 11.2.3 - 12.1.1 - 12.2.1 - 15.1.3	Procedimientos de operación documentados. Registro de eventos. Protección de la información de registro. Registros del administrador y del operador.	**Proyecto 1-** Control de acceso físico y protección de la información (Áreas seguras y seguridad de equipos).Ver numeral 11.1 **Proyecto 2-** Responsabilidades y procedimientos de operación. Ver numeral 11.1 **Proyecto 4-** Control de acceso y responsabilidades de los usuarios. Ver numeral 11.1.
		[E.4] Errores de configuración			Gestión de cambios en los servicios prestados por terceros.	
		[A.7] uso no previsto			Responsabilidades y procedimientos.	
Impresora para código de barras	Pérdida de Disponibilidad del activo de información	[I.6] Corte del suministro eléctrico [A.23] Manipulación del hardware	Muy Alto	Se mitiga el riesgo con la implementación del control 11.2.2 - 15.2.1	Servicios de suministro. Seguimiento y revisión de los servicios de los proveedores.	**Proyecto 1-** Control de acceso físico y protección de la información (Áreas seguras y seguridad de equipos).Ver numeral 11.1

Tabla 35. (Continuación)

ACTIVOS	RIESGO	AMENAZAS	VALOR	TRATAMIENTO DE RIESGO	CONTROLES IMPLEMENTADOS	PROYECTOS DEFINIDOS
Impresora para código de barras	Pérdida de Disponibilidad del activo de información	[N.1] Fuego [N.2] Daños por agua [N.*] Desastres naturales [I.1] Fuego [I.2] Daños por agua [I.*] Desastres industriales [I.3] Contaminación medioambiental [I.5] Avería de origen físico o lógico [I.7] Condiciones inadecuadas de temperatura o humedad [E.23] Errores de mantenimiento / actualización de equipos (hardware) [E.24] caída del sistema por agotamiento de recursos [E.25] Pérdida de equipos [A.25] Robo de equipos [A.26] Ataque destructivo	Alto	Se mitiga el riesgo con la implementación de los controles 11.1.1 - 11.1.2 - 11.1.3 - 11.1.4 - 11.1.5 - 11.2.2. - 12.2.1 - 16.1.2 - 17.1.1 -	Protección contra las amenazas externas y ambientales. Trabajo en áreas seguras. Cadena de suministro de tecnología de información y comunicación. Procedimientos de operación documentados. Mantenimiento de equipos. Revisión de los derechos de acceso de usuarios. Controles de acceso físicos ubicación y protección de los equipos. Controles contra código malicioso. Procedimientos de operación documentados. Registro y gestión de eventos de seguridad. Gestión de capacidad.	**Proyecto 1-** Control de acceso físico y protección de la información (Áreas seguras y seguridad de equipos).Ver numeral 11.1 **Proyecto 2-** Responsabilidades y procedimientos de operación. Ver numeral 11.1 **Proyecto 4-** Control de acceso y responsabilidades de los usuarios a los sistemas y aplicaciones. Ver numeral 11.1 **Proyecto 6-** Seguimiento y cumplimiento de la Política de Seguridad de la Información de la entidad. Ver numeral 11.1.
		[I.4] Contaminación electromagnética [E.2] Errores del administrador del sistema / de la seguridad	Medio	Se mitiga el riesgo con la implementación de los controles 9.4.2 - 11.1.4 - 11.1.5 - 11.2.1 -	Procedimiento de ingreso seguro. Protección contra amenazas externas y ambientales ubicación y protección de los equipos.	**Proyecto 1-** Control de acceso físico y protección de la información (Áreas seguras y seguridad de equipos).Ver numeral 11.1 **Proyecto 2-** Responsabilidades y procedimientos de operación. Ver numeral 11.1 **Proyecto 4-** Control de acceso y responsabilidades de los usuarios. Ver numeral 11.1.
Servidor controlador de dominio principal	Pérdida de Disponibilidad del activo de información	[I.6] Corte del suministro eléctrico	Muy Alto	Se mitiga el riesgo con la implementación del control 11.2.2 - 15.2.1	Servicios de suministro. Seguimiento y revisión de los servicios de los proveedores.	**Proyecto 1-** Control de acceso físico y protección de la información (Áreas seguras y seguridad de equipos).Ver numeral 11.1
		[N.1] Fuego [N.2] Daños por agua [N.*] Desastres naturales [I.7] Condiciones inadecuadas de temperatura o humedad [E.8] Difusión de software dañino [A.24] Denegación de servicio	Alto	Se mitiga el riesgo con la implementación de los controles 9.2.5 11.1.2 - 11.1.4 - 11.1.5 - 11.2.1 - 11.2.4. - 11.2.3 - 12.1.1 - 12.2.1 - 15.1.3	Protección contra las amenazas externas y ambientales. Trabajo en áreas seguras. Cadena de suministro de tecnología de información y comunicación. Procedimientos de operación documentados. Mantenimiento de equipos. Revisión de los derechos de acceso de usuarios. Controles de acceso físicos ubicación y protección de los equipos. Controles contra código malicioso.	**Proyecto 1-** Control de acceso físico y protección de la información (Áreas seguras y seguridad de equipos).Ver numeral 11.1 **Proyecto 2-** Responsabilidades y procedimientos de operación. Ver numeral 11.1 **Proyecto 4-** Control de acceso y responsabilidades de los usuarios. Ver numeral 11.1.

o

Tabla 35. (Continuación)

ACTIVOS	RIESGO	AMENAZAS	VALOR	TRATAMIENTO DE RIESGO	CONTROLES IMPLEMENTADOS	PROYECTOS DEFINIDOS
Servidor controlador de dominio principal	Pérdida de Disponibilidad del activo de información	[E.25] Pérdida de equipos [A.23] Manipulación del hardware [A.25] Robo de equipos [A.26] Ataque destructivo	Medio	Se mitiga el riesgo con la implementación de los controles 5.1.1 - 8.1.2 - 9.1.1 - 11.1.1 -11.1.2 - 11.1.3 - 11.1.4 - 11.1.5	Políticas para la seguridad de la Información. Propiedad de los Activos. Política de control de acceso. Perímetro de seguridad física. Controles de acceso físicos. Seguridad de oficinas, recinto e instalaciones. Protección contra amenazas externas y ambientales. Trabajo en áreas seguras.	**Proyecto 1-** Control de acceso físico y protección de la información (Áreas seguras y seguridad de equipos).Ver numeral 11.1 **Proyecto 6-** Seguimiento y cumplimiento de la Política de Seguridad de la Información de la entidad. Ver numeral 11.1
	Pérdida de la Integridad de la información, lo que implica el acceso indebido o fraudulento al activo de información	[E.8] Difusión de software dañino [A.6] Abuso de privilegios de acceso	Alto	Se mitiga el riesgo con la implementación de los controles 9.1.1 - 9.1.2 – 9.2.1 - 9.2.2 - 9.2.3 - 9.2.4 - 9.2.5 - 9.2.6 - 9.3.1 - 9.4.1 - 9.4.2 - 9.4.3	Protección contra amenazas externas y ambientales. Mantenimiento de equipos Registro de eventos. Controles contra código malicioso. Suministro de acceso de usuarios. Protección de la información de registro.	**Proyecto 1-** Control de acceso físico y protección de la información (Áreas seguras y seguridad de equipos).Ver numeral 11.1 **Proyecto 2-** Responsabilidades y procedimientos de operación. Ver numeral 11.1 **Proyecto 3-** Implementación y seguimiento de registros de actividad. Ver numeral 11.1
	Pérdida de la Confidencialidad, acceso no autorizado que permite la utilización indebida o no autorizada del activo de información	[E.25] Pérdida de equipos [A.6] Abuso de privilegios de acceso [A.11] Acceso no autorizado [A.23] Manipulación del hardware [A.25] Robo de equipos	Alto	Se mitiga el riesgo con la Implementación de los controles 5.1.1 - 8.1.2 - 9.1.1 - 11.1.1 -11.1.2 - 11.1.3 - 11.1.4 - 11.1.5	Políticas para la seguridad de la Información. Propiedad de los Activos. Política de control de acceso. Perímetro de seguridad física. Controles de acceso físicos Seguridad de oficinas, recinto e instalaciones. Protección contra amenazas externas y ambientales. Trabajo en áreas seguras.	**Proyecto 1-** Control de acceso físico y protección de la información (Áreas seguras y seguridad de equipos).Ver numeral 11.1 **Proyecto 6-** Seguimiento y cumplimiento de la Política de Seguridad de la Información de la entidad. Ver numeral 11.1
		[E.2] Errores del administrador del sistema / de la seguridad [E.4] Errores de configuración [A.7] uso no previsto	Medio	Se mitiga el riesgo con la implementación de los controles 12.1.1 - 12.4.1 - 12.4.2 - 12.4.3	Procedimientos de operación documentados. Registro de eventos. Protección de la información de registro. Registros del administrador y del operador.	**Proyecto 2-** Responsabilidades y procedimientos de operación
Switch de borde 4800	Pérdida de Disponibilidad del activo de información	[I.3] Contaminación medioambiental [I.6] Corte del suministro eléctrico	Alto	Se mitiga el riesgo con la implementación del control 11.2.2 - 15.2.1	Servicios de suministro. Seguimiento y revisión de los servicios de los proveedores.	**Proyecto 1-** Control de acceso físico y protección de la información (Áreas seguras y seguridad de equipos).Ver numeral 11.1

Tabla 35. (Continuación)

ACTIVOS	RIESGO	AMENAZAS	VALOR	TRATAMIENTO DE RIESGO	CONTROLES IMPLEMENTADOS	PROYECTOS DEFINIDOS
Switch de borde 4800	Pérdida de Disponibilidad del activo de información	[N.2] Daños por agua [N.*] Desastres naturales [I.1] Fuego [I.7] Condiciones inadecuadas de temperatura o humedad [E.4] Errores de configuración [E.23] Errores de mantenimiento / actualización de equipos (hardware) [A.25] Robo de equipos	Medio	Se mitiga el riesgo con la implementación de los controles 11.1.1 - 11.1.2 - 11.1.3 - 11.1.4 - 11.1.5 - 11.2.2. - 12.2.1 - 16.1.2 - 17.1.1 -	Perímetro de seguridad física. Controles de acceso físicos. Seguridad de oficinas, recinto e instalaciones. Protección contra amenazas externas y ambientales. Trabajo en áreas seguras. Servicios de suministro ubicación y protección de los equipos. Reporte de eventos de seguridad de la información. Planificación de la continuidad de la seguridad de la información. Controles contra códigos maliciosos.	**Proyecto 1-** Control de acceso físico y protección de la información (Áreas seguras y seguridad de equipos).Ver numeral 11.1 **Proyecto 2-** Responsabilidades y procedimientos de operación. Ver numeral 11.1 **Proyecto 5-** Adaptación Plan de contingencia TICS, como marco de Gestión del Plan de Continuidad del Negocio. Ver numeral 11.1 **Proyecto 7-** Gestión de incidentes de seguridad de la información. Ver numeral 11.1
Switch de borde - Referencia 2410 - UPI La Rioja	Pérdida de Disponibilidad del activo de información	[I.3] Contaminación medioambiental [I.6] Corte del suministro eléctrico	Alto	Se mitiga el riesgo con la implementación del control 11.2.2 - 15.2.1	Servicios de suministro. Seguimiento y revisión de los servicios de los proveedores.	**Proyecto 1-** Control de acceso físico y protección de la información (Áreas seguras y seguridad de equipos).Ver numeral 11.1
		[N.2] Daños por agua [N.*] Desastres naturales [I.1] Fuego [I.7] Condiciones inadecuadas de temperatura o humedad [E.4] Errores de configuración [E.23] Errores de mantenimiento / actualización de equipos (hardware) [A.25] Robo de equipos	Medio	Se mitiga el riesgo con la implementación de los controles 11.1.1 - 11.1.2 - 11.1.3 - 11.1.4 - 11.1.5 - 11.2.2. - 12.2.1 - 16.1.2 - 17.1.1 -	Gestión de acceso a usuarios. Gestión de derechos de acceso asignados a usuarios. Acceso a redes y a Servicios de red. Suministro de acceso de usuarios. Gestión de derechos de acceso privilegiado. Protección contra las amenazas externas y ambientales. Trabajo en áreas seguras. Cadena de suministro de tecnología de información y comunicación. Procedimientos de operación documentados. Mantenimiento de equipos. Revisión de los derechos de acceso de usuarios. Controles de acceso físicos ubicación y protección de los equipos. Controles contra código malicioso.	**Proyecto 1-** Control de acceso físico y protección de la información (Áreas seguras y seguridad de equipos).Ver numeral 11.1 **Proyecto 2-** Responsabilidades y procedimientos de operación. Ver numeral 11.1 **Proyecto 4-** Control de acceso y responsabilidades de los usuarios. Ver numeral 11.1.
Switch de borde - Referencia 2920 - Proyecto Misión Bogotá	Pérdida de Disponibilidad del activo de información	[I.3] Contaminación medioambiental [I.6] Corte del suministro eléctrico	Alto	Se mitiga el riesgo con la implementación del control 11.2.2 - 15.2.1	Servicios de suministro. Seguimiento y revisión de los servicios de los proveedores.	**Proyecto 1-** Control de acceso físico y protección de la información (Áreas seguras y seguridad de equipos).Ver numeral 11.1

Tabla 35. (Continuación)

ACTIVOS	RIESGO	AMENAZAS	VALOR	TRATAMIENTO DE RIESGO	CONTROLES IMPLEMENTADOS	PROYECTOS DEFINIDOS
Switch de borde - Referencia 2920 - Proyecto Misión Bogotá	Pérdida de Disponibilidad del activo de información	[N.2] Daños por agua [N.*] Desastres naturales [I.1] Fuego [I.7] Condiciones inadecuadas de temperatura o humedad [E.4] Errores de configuración [E.23] Errores de mantenimiento / actualización de equipos (hardware) [A.25] Robo de equipos	Medio	Se mitiga el riesgo con la implementación de los controles 11.1.1 - 11.1.2 - 11.1.3 - 11.1.4 - 11.1.5 - 11.2.2. - 12.2.1 - 16.1.2 - 17.1.1 -	Protección contra las amenazas externas y ambientales. Trabajo en áreas seguras. Cadena de suministro de tecnología de información y comunicación. Procedimientos de operación documentados. Mantenimiento de equipos. Revisión de los derechos de acceso de usuarios. Controles de acceso físicos ubicación y protección de los equipos. Controles contra código malicioso.	**Proyecto 1-** Control de acceso físico y protección de la información (Áreas seguras y seguridad de equipos).Ver numeral 11.1 **Proyecto 2-** Responsabilidades y procedimientos de operación. Ver numeral 11.1 **Proyecto 4-** Control de acceso y responsabilidades de los usuarios. Ver numeral 11.1.
Switch de borde - Referencia 4250T	Pérdida de Disponibilidad del activo de información	[I.3] Contaminación medioambiental	Alto	Se mitiga el riesgo con la implementación del control 11.2.2 - 15.2.1	Servicios de suministro. Seguimiento y revisión de los servicios de los proveedores.	**Proyecto 1-** Control de acceso físico y protección de la información (Áreas seguras y seguridad de equipos).Ver numeral 11.1
		[N.2] Daños por agua [N.*] Desastres naturales [I.1] Fuego [I.7] Condiciones inadecuadas de temperatura o humedad [E.4] Errores de configuración [E.23] Errores de mantenimiento / actualización de equipos (hardware) [A.25] Robo de equipos	Medio	Se mitiga el riesgo con la implementación de los controles 9.1.1 - 9.1.2 - 9.2.1 - 9.2.2 - 9.2.3 - 9.2.5 11.1.2 - 11.1.4 - 11.1.5 - 11.2.1 - 11.2.4. - 11.2.3 - 12.1.1 - 12.2.1 - 15.1.3	Gestión de acceso a usuarios. Gestión de derechos de acceso asignados a usuarios. Acceso a redes y a Servicios de red. Suministro de acceso de usuarios. Gestión de derechos de acceso privilegiado. Protección contra las amenazas externas y ambientales. Trabajo en áreas seguras. Cadena de suministro de tecnología de información y comunicación. Procedimientos de operación documentados. Mantenimiento de equipos. Revisión de los derechos de acceso de usuarios. Controles de acceso físicos ubicación y protección de los equipos. Controles contra código malicioso.	**Proyecto 1-** Control de acceso físico y protección de la información (Áreas seguras y seguridad de equipos).Ver numeral 11.1 **Proyecto 4-** Control de acceso y responsabilidades de los usuarios a los sistemas y aplicaciones. Ver numeral 11.1 **Proyecto 6-** Seguimiento y cumplimiento de la Política de Seguridad de la Información de la entidad. Ver numeral 11.1.
Switch de borde - Referencia 4500G UPI La Florida	Pérdida de Disponibilidad del activo de información	[I.3] Contaminación medioambiental [I.6] Corte del suministro eléctrico	Alto	Se mitiga el riesgo con la implementación del control 11.2.2 - 15.2.1	Servicios de suministro. Seguimiento y revisión de los servicios de los proveedores.	**Proyecto 1-** Control de acceso físico y protección de la información (Áreas seguras y seguridad de equipos).Ver numeral 11.1

Tabla 35. (Continuación)

ACTIVOS	RIESGO	AMENAZAS	VALOR	TRATAMIENTO DE RIESGO	CONTROLES IMPLEMENTADOS	PROYECTOS DEFINIDOS
Switch de borde - Referencia 4500G UPI La Florida	Pérdida de Disponibilidad del activo de información	[N.2] Daños por agua [N.*] Desastres naturales [I.1] Fuego [I.7] Condiciones inadecuadas de temperatura o humedad [E.4] Errores de configuración [E.23] Errores de mantenimiento / actualización de equipos (hardware) [A.25] Robo de equipos	Medio	Se mitiga el riesgo con la implementación de los controles 11.1.1 - 11.1.2 - 11.1.3 - 11.1.4 - 11.1.5 - 11.2.2. - 12.2.1 - 16.1.2 - 17.1.1 -	Protección contra las amenazas externas y ambientales. Trabajo en áreas seguras. Cadena de suministro de tecnología de información y comunicación. Procedimientos de operación documentados. Mantenimiento de equipos. Revisión de los derechos de acceso de usuarios. Controles de acceso físicos ubicación y protección de los equipos. Controles contra código malicioso.	**Proyecto 1-** Control de acceso físico y protección de la información (Áreas seguras y seguridad de equipos).Ver numeral 11.1 **Proyecto 2-** Responsabilidades y procedimientos de operación. Ver numeral 11.1 **Proyecto 4-** Control de acceso y responsabilidades de los usuarios. Ver numeral 11.1.
Switch de borde - Referencia 4800G - UPI La 32	Pérdida de Disponibilidad del activo de información	[I.3] Contaminación medioambiental [I.6] Corte del suministro eléctrico	Alto	Se mitiga el riesgo con la implementación del control 11.2.2 - 15.2.1	Servicios de suministro. Seguimiento y revisión de los servicios de los proveedores.	**Proyecto 1-** Control de acceso físico y protección de la información (Áreas seguras y seguridad de equipos).Ver numeral 11.1
		[N.2] Daños por agua [N.*] Desastres naturales [I.1] Fuego [I.7] Condiciones inadecuadas de temperatura o humedad [E.4] Errores de configuración [E.23] Errores de mantenimiento / actualización de equipos (hardware) [A.25] Robo de equipos	Medio	Se mitiga el riesgo con la implementación de los controles 11.1.1 - 11.1.2 - 11.1.3 - 11.1.4 - 11.1.5 - 11.2.2. - 12.2.1 - 16.1.2 - 17.1.1 -	Protección contra las amenazas externas y ambientales. Trabajo en áreas seguras. Cadena de suministro de tecnología de información y comunicación. Procedimientos de operación documentados. Mantenimiento de equipos. Revisión de los derechos de acceso de usuarios. Controles de acceso físicos ubicación y protección de los equipos. Controles contra código malicioso.	**Proyecto 1-** Control de acceso físico y protección de la información (Áreas seguras y seguridad de equipos).Ver numeral 11.1 **Proyecto 2-** Responsabilidades y procedimientos de operación. Ver numeral 11.1 **Proyecto 4-** Control de acceso y responsabilidades de los usuarios. Ver numeral 11.1.
Switch de borde - Referencia 4800G - UPI El Perdomo	Pérdida de Disponibilidad del activo de información	[I.3] Contaminación medioambiental [I.6] Corte del suministro eléctrico	Alto	Se mitiga el riesgo con la implementación del control 11.2.2 - 15.2.1	Servicios de suministro. Seguimiento y revisión de los servicios de los proveedores.	**Proyecto 1-** Control de acceso físico y protección de la información (Áreas seguras y seguridad de equipos).Ver numeral 11.1
		[N.2] Daños por agua [N.*] Desastres naturales [I.1] Fuego [I.7] Condiciones inadecuadas de temperatura o humedad [E.4] Errores de configuración [E.23] Errores de mantenimiento / actualización de equipos (hardware) [A.25] Robo de equipos	Medio	Se mitiga el riesgo con la implementación de los controles 11.1.1 - 11.1.2 - 11.1.3 - 11.1.4 - 11.1.5 - 11.2.2. - 12.2.1 - 16.1.2 - 17.1.1 -	Protección contra las amenazas externas y ambientales. Trabajo en áreas seguras. Cadena de suministro de tecnología de información y comunicación. Procedimientos de operación documentados. Mantenimiento de equipos. Revisión de los derechos de acceso de usuarios. Controles de acceso físicos.	**Proyecto 1-** Control de acceso físico y protección de la información (Áreas seguras y seguridad de equipos).Ver numeral 11.1 **Proyecto 2-** Responsabilidades y procedimientos de operación. Ver numeral 11.1 **Proyecto 4-** Control de acceso y responsabilidades de los usuarios. Ver numeral 11.1.

Tabla 35. (Continuación)

ACTIVOS	RIESGO	AMENAZAS	VALOR	TRATAMIENTO DE RIESGO	CONTROLES IMPLEMENTADOS	PROYECTOS DEFINIDOS
Switch de borde - Referencia 4800G - UPI La Florida	Pérdida de Disponibilidad del activo de información	[I.3] Contaminación medioambiental [I.6] Corte del suministro eléctrico	Alto	Se mitiga el riesgo con la implementación de los controles 9.2.5 11.1.2 - 11.1.4 - 11.1.5 - 11.2.1 - 11.2.4. - 11.2.3 - 12.1.1 - 12.2.1 - 15.1.3	Protección contra las amenazas externas y ambientales. Trabajo en áreas seguras. Cadena de suministro de tecnología de información y comunicación. Procedimientos de operación documentados. Mantenimiento de equipos. Revisión de los derechos de acceso de usuarios. Controles de acceso físicos ubicación y protección de los equipos. Controles contra código malicioso.	**Proyecto 1-** Control de acceso físico y protección de la información (Áreas seguras y seguridad de equipos).Ver numeral 11.1 **Proyecto 2-** Responsabilidades y procedimientos de operación. Ver numeral 11.1 **Proyecto 4-** Control de acceso y responsabilidades de los usuarios. Ver numeral 11.1.
		[N.2] Daños por agua [N.*] Desastres naturales [I.1] Fuego [I.7] Condiciones inadecuadas de temperatura o humedad [E.4] Errores de configuración [E.23] Errores de mantenimiento / actualización de equipos (hardware) [A.25] Robo de equipos	Medio	Se mitiga el riesgo con la implementación de los controles 11.1.1 - 11.1.2 - 11.1.3 - 11.1.4 - 11.1.5 - 11.2.2. - 12.2.1 - 16.1.2 - 17.1.1 -	Protección contra las amenazas externas y ambientales. Trabajo en áreas seguras. Cadena de suministro de tecnología de información y comunicación. Procedimientos de operación documentados. Mantenimiento de equipos Revisión de los derechos de acceso de usuarios. Controles de acceso físicos ubicación y protección de los equipos. Controles contra código malicioso.	**Proyecto 1-** Control de acceso físico y protección de la información (Áreas seguras y seguridad de equipos).Ver numeral 11.1 **Proyecto 2-** Responsabilidades y procedimientos de operación. Ver numeral 11.1 **Proyecto 4-** Control de acceso y responsabilidades de los usuarios. Ver numeral 11.1.
Switch de borde - Referencia 4800G - UPI La 27 sur	Pérdida de Disponibilidad del activo de información	[I.3] Contaminación medioambiental [I.6] Corte del suministro eléctrico	Alto	Se mitiga el riesgo con la implementación de los controles 9.2.5 11.1.2 - 11.1.4 - 11.1.5 - 11.2.1 - 11.2.4. - 11.2.3 - 12.1.1 - 12.2.1 - 15.1.3	Protección contra las amenazas externas y ambientales. Trabajo en áreas seguras. Cadena de suministro de tecnología de información y comunicación. Procedimientos de operación documentados. Mantenimiento de equipos. Revisión de los derechos de acceso de usuarios. Controles de acceso físicos ubicación y protección de los equipos. Controles contra código malicioso.	**Proyecto 1-** Control de acceso físico y protección de la información (Áreas seguras y seguridad de equipos).Ver numeral 11.1 **Proyecto 2-** Responsabilidades y procedimientos de operación. Ver numeral 11.1 **Proyecto 4-** Control de acceso y responsabilidades de los usuarios. Ver numeral 11.1.

Tabla 35. (Continuación)

ACTIVOS	RIESGO	AMENAZAS	VALOR	TRATAMIENTO DE RIESGO	CONTROLES IMPLEMENTADOS	PROYECTOS DEFINIDOS
Switch de borde - Referencia 4800G - UPI La 27 sur	Pérdida de Disponibilidad del activo de información	[N.2] Daños por agua [N.*] Desastres naturales [I.1] Fuego [I.7] Condiciones inadecuadas de temperatura o humedad [E.4] Errores de configuración [E.23] Errores de mantenimiento / actualización de equipos (hardware) [A.25] Robo de equipos	Medio	Se mitiga el riesgo con la implementación de los controles 11.1.1 - 11.1.2 - 11.1.3 - 11.1.4 - 11.1.5 - 11.2.2. - 12.2.1 - 16.1.2 - 17.1.1 -	Protección contra las amenazas externas y ambientales. Trabajo en áreas seguras. Cadena de suministro de tecnología de información y comunicación. Procedimientos de operación documentados. Mantenimiento de equipos. Revisión de los derechos de acceso de usuarios. Controles de acceso físicos ubicación y protección de los equipos. Controles contra código malicioso.	**Proyecto 1-** Control de acceso físico y protección de la información (Áreas seguras y seguridad de equipos).Ver numeral 11.1 **Proyecto 2-** Responsabilidades y procedimientos de operación. Ver numeral 11.1 **Proyecto 4-** Control de acceso y responsabilidades de los usuarios. Ver numeral 11.1.
Switch de borde - Referencia 4800G - UPI San Francisco	Pérdida de Disponibilidad del activo de información	[I.3] Contaminación medioambiental [I.6] Corte del suministro eléctrico	Alto	Se mitiga el riesgo con la implementación de los controles 9.2.5 11.1.2 - 11.1.4 - 11.1.5 - 11.2.1 - 11.2.4. - 11.2.3 - 12.1.1 - 12.2.1 - 15.1.3	Protección contra las amenazas externas y ambientales. Trabajo en áreas seguras. Cadena de suministro de tecnología de información y comunicación. Procedimientos de operación documentados. Mantenimiento de equipos. Revisión de los derechos de acceso de usuarios. Controles de acceso físicos ubicación y protección de los equipos. Controles contra código malicioso.	**Proyecto 1-** Control de acceso físico y protección de la información (Áreas seguras y seguridad de equipos).Ver numeral 11.1 **Proyecto 2-** Responsabilidades y procedimientos de operación. Ver numeral 11.1 **Proyecto 4-** Control de acceso y responsabilidades de los usuarios. Ver numeral 11.1.
		[N.2] Daños por agua [N.*] Desastres naturales [I.1] Fuego [I.7] Condiciones inadecuadas de temperatura o humedad [E.4] Errores de configuración [E.23] Errores de mantenimiento / actualización de equipos (hardware) [A.25] Robo de equipos	Medio	Se mitiga el riesgo con la implementación de los controles 11.1.1 - 11.1.2 - 11.1.3 - 11.1.4 - 11.1.5 - 11.2.2. - 12.2.1 - 16.1.2 - 17.1.1 -	Perímetro de seguridad física. Controles de acceso físicos Seguridad de oficinas, recinto e instalaciones. Protección contra amenazas externas y ambientales. Trabajo en áreas seguras. Servicios de suministro ubicación y protección de los equipos. Reporte de eventos de seguridad de la información. Planificación de la continuidad de la seguridad de la información. Controles contra códigos maliciosos.	**Proyecto 1-** Control de acceso físico y protección de la información (Áreas seguras y seguridad de equipos).Ver numeral 11.1 **Proyecto 2-** Responsabilidades y procedimientos de operación. Ver numeral 11.1 **Proyecto 4-** Control de acceso y responsabilidades de los usuarios. Ver numeral 11.1.

Tabla 35. (Continuación)

ACTIVOS	RIESGO	AMENAZAS	VALOR	TRATAMIENTO DE RIESGO	CONTROLES IMPLEMENTADOS	PROYECTOS DEFINIDOS
Switch de borde - Referencia 4800G - UPI La Rioja	Pérdida de Disponibilidad del activo de información	[I.3] Contaminación medioambiental [I.6] Corte del suministro eléctrico	Alto	Se mitiga el riesgo con la implementación de los controles 9.2.5 11.1.2 - 11.1.4 - 11.1.5 - 11.2.1 - 11.2.4. - 11.2.3 - 12.1.1 - 12.2.1 - 15.1.3	Protección contra las amenazas externas y ambientales. Trabajo en áreas seguras. Cadena de suministro de tecnología de información y comunicación. Procedimientos de operación documentados. Mantenimiento de equipos. Revisión de los derechos de acceso de usuarios. Controles de acceso físicos ubicación y protección de los equipos. Controles contra código malicioso.	**Proyecto 1-** Control de acceso físico y protección de la información (Áreas seguras y seguridad de equipos).Ver numeral 11.1 **Proyecto 2-** Responsabilidades y procedimientos de operación. Ver numeral 11.1 **Proyecto 4-** Control de acceso y responsabilidades de los usuarios. Ver numeral 11.1.
		[N.2] Daños por agua [N.*] Desastres naturales [I.1] Fuego [I.7] Condiciones inadecuadas de temperatura o humedad [E.4] Errores de configuración [E.23] Errores de mantenimiento / actualización de equipos (hardware) [A.25] Robo de equipos	Medio	Se mitiga el riesgo con la implementación de los controles 11.1.1 - 11.1.2 - 11.1.3 - 11.1.4 - 11.1.5 - 11.2.2. - 12.2.1 - 16.1.2 - 17.1.1 -	Perímetro de seguridad física. Controles de acceso físicos. Seguridad de oficinas, recinto e instalaciones. Protección contra amenazas externas y ambientales. Trabajo en áreas seguras. Servicios de suministro ubicación y protección de los equipos. Reporte de eventos de seguridad de la información. Planificación de la continuidad de la seguridad de la información. Controles contra códigos maliciosos.	**Proyecto 1-** Control de acceso físico y protección de la información (Áreas seguras y seguridad de equipos).Ver numeral 11.1 **Proyecto 2-** Responsabilidades y procedimientos de operación. Ver numeral 11.1 **Proyecto 4-** Control de acceso y responsabilidades de los usuarios. Ver numeral 11.1.
Switch de borde - Referencia 4800G - UPI La Vega	Pérdida de Disponibilidad del activo de información	[I.3] Contaminación medioambiental [I.6] Corte del suministro eléctrico	Alto	Se mitiga el riesgo con la implementación del control 11.2.2 - 15.2.1	Servicios de suministro. Seguimiento y revisión de los servicios de los proveedores.	**Proyecto 1-** Control de acceso físico y protección de la información (Áreas seguras y seguridad de equipos).Ver numeral 11.1
		[N.2] Daños por agua [N.*] Desastres naturales [I.1] Fuego [I.7] Condiciones inadecuadas de temperatura o humedad [E.4] Errores de configuración [E.23] Errores de mantenimiento / actualización de equipos (hardware) [A.25] Robo de equipos	Medio	Se mitiga el riesgo con la implementación de los controles 9.2.5 11.1.2 - 11.1.4 - 11.1.5 - 11.2.1 - 11.2.4. - 11.2.3 - 12.1.1 - 12.2.1 - 15.1.3	Protección contra las amenazas externas y ambientales. Trabajo en áreas seguras. Cadena de suministro de tecnología de información y comunicación. Procedimientos de operación documentados. Mantenimiento de equipos. Revisión de los derechos de acceso de usuarios. Controles de acceso físicos.	**Proyecto 1-** Control de acceso físico y protección de la información (Áreas seguras y seguridad de equipos).Ver numeral 11.1 **Proyecto 2-** Responsabilidades y procedimientos de operación. Ver numeral 11.1 **Proyecto 4-** Control de acceso y responsabilidades de los usuarios. Ver numeral 11.1.

Tabla 35. (Continuación)

ACTIVOS	RIESGO	AMENAZAS	VALOR	TRATAMIENTO DE RIESGO	CONTROLES IMPLEMENTADOS	PROYECTOS DEFINIDOS
Switch de borde - Referencia 4800G - UPI Santa Lucia	Pérdida de Disponibilidad del activo de información	[I.3] Contaminación medioambiental [I.6] Corte del suministro eléctrico	Alto	Se mitiga el riesgo con la implementación de los controles 9.2.5 11.1.2 - 11.1.4 - 11.1.5 - 11.2.1 - 11.2.4. - 11.2.3 - 12.1.1 - 12.2.1 - 15.1.3	Servicios de suministro. Seguimiento y revisión de los servicios de los proveedores.	**Proyecto 1-** Control de acceso físico y protección de la información (Áreas seguras y seguridad de equipos).Ver numeral 11.1 **Proyecto 2-** Responsabilidades y procedimientos de operación. Ver numeral 11.1 **Proyecto 4-** Control de acceso y responsabilidades de los usuarios. Ver numeral 11.1.
		[N.2] Daños por agua [N.*] Desastres naturales [I.1] Fuego [I.7] Condiciones inadecuadas de temperatura o humedad [E.4] Errores de configuración [E.23] Errores de mantenimiento / actualización de equipos (hardware) [A.25] Robo de equipos	Medio	Se mitiga el riesgo con la implementación de los controles 11.1.1 - 11.1.2 - 11.1.3 - 11.1.4 - 11.1.5 - 11.2.2. - 12.2.1 - 16.1.2 - 17.1.1 -	Gestión de acceso a usuarios. Gestión de derechos de acceso asignados a usuarios. Acceso a redes y a Servicios de red. Suministro de acceso de usuarios. Gestión de derechos de acceso privilegiado. Protección contra las amenazas externas y ambientales. Trabajo en áreas seguras. Cadena de suministro de tecnología de información y comunicación. Procedimientos de operación documentados. Mantenimiento de equipos. Revisión de los derechos de acceso de usuarios. Controles de acceso físicos ubicación y protección de los equipos. Controles contra código malicioso.	**Proyecto 1-** Control de acceso físico y protección de la información (Áreas seguras y seguridad de equipos).Ver numeral 11.1 **Proyecto 4-** Control de acceso y responsabilidades de los usuarios a los sistemas y aplicaciones. Ver numeral 11.1 **Proyecto 6-** Seguimiento y cumplimiento de la Política de Seguridad de la Información de la entidad. Ver numeral 11.1.
Switch de borde - Referencia 4800G - UPI Servitá	Pérdida de Disponibilidad del activo de información	[I.3] Contaminación medioambiental [I.6] Corte del suministro eléctrico	Alto	Se mitiga el riesgo con la implementación de los controles 9.2.5 11.1.2 - 11.1.4 - 11.1.5 - 11.2.1 - 11.2.4. - 11.2.3 - 12.1.1 - 12.2.1 - 15.1.3	Protección contra las amenazas externas y ambientales. Trabajo en áreas seguras. Cadena de suministro de tecnología de información y comunicación. Procedimientos de operación documentados. Mantenimiento de equipos. Revisión de los derechos de acceso de usuarios. Controles de acceso físicos ubicación y protección de los equipos. Controles contra código malicioso.	**Proyecto 1-** Control de acceso físico y protección de la información (Áreas seguras y seguridad de equipos).Ver numeral 11.1 **Proyecto 2-** Responsabilidades y procedimientos de operación. Ver numeral 11.1 **Proyecto 4-** Control de acceso y responsabilidades de los usuarios. Ver numeral 11.1.

Tabla 35. (Continuación)

ACTIVOS	RIESGO	AMENAZAS	VALOR	TRATAMIENTO DE RIESGO	CONTROLES IMPLEMENTADOS	PROYECTOS DEFINIDOS
Switch de borde - Referencia 4800G - UPI Servitá	Pérdida de Disponibilidad del activo de información	[N.2] Daños por agua [N.*] Desastres naturales [I.1] Fuego [I.7] Condiciones inadecuadas de temperatura o humedad [E.4] Errores de configuración [E.23] Errores de mantenimiento / actualización de equipos (hardware) [A.25] Robo de equipos	Medio	Se mitiga el riesgo con la implementación de los controles 11.1.1 - 11.1.2 - 11.1.3 - 11.1.4 - 11.1.5 - 11.2.2. - 12.2.1 - 16.1.2 - 17.1.1 -	Gestión de acceso a usuarios. Gestión de derechos de acceso asignados a usuarios. Acceso a redes y a Servicios de red. Suministro de acceso de usuarios. Gestión de derechos de acceso privilegiado. Protección contra las amenazas externas y ambientales. Trabajo en áreas seguras. Cadena de suministro de tecnología de información y comunicación. Procedimientos de operación documentados. Mantenimiento de equipos. Revisión de los derechos de acceso de usuarios. Controles de acceso físicos ubicación y protección de los equipos. Controles contra código malicioso.	**Proyecto 1-** Control de acceso físico y protección de la información (Áreas seguras y seguridad de equipos).Ver numeral 11.1 **Proyecto 2-** Responsabilidades y procedimientos de operación. Ver numeral 11.1 **Proyecto 4-** Control de acceso y responsabilidades de los usuarios. Ver numeral 11.1.
Switch de borde - Referencia E2910 HP - UPI Bosa	Pérdida de Disponibilidad del activo de información	[I.3] Contaminación medioambiental [I.6] Corte del suministro eléctrico	Alto	Se mitiga el riesgo con la implementación de los controles 9.2.5 11.1.2 - 11.1.4 - 11.1.5 - 11.2.1 - 11.2.4. - 11.2.3 - 12.1.1 - 12.2.1 - 15.1.3	Protección contra las amenazas externas y ambientales. Trabajo en áreas seguras. Cadena de suministro de tecnología de información y comunicación. Procedimientos de operación documentados. Mantenimiento de equipos. Revisión de los derechos de acceso de usuarios. Controles de acceso físicos ubicación y protección de los equipos. Controles contra código malicioso.	**Proyecto 1-** Control de acceso físico y protección de la información (Áreas seguras y seguridad de equipos).Ver numeral 11.1 **Proyecto 2-** Responsabilidades y procedimientos de operación. Ver numeral 11.1 **Proyecto 4-** Control de acceso y responsabilidades de los usuarios. Ver numeral 11.1.

Tabla 35. (Continuación)

ACTIVOS	RIESGO	AMENAZAS	VALOR	TRATAMIENTO DE RIESGO	CONTROLES IMPLEMENTADOS	PROYECTOS DEFINIDOS
Switch de borde - Referencia E2910 HP - UPI Bosa	Pérdida de Disponibilidad del activo de información	[N.2] Daños por agua [N.*] Desastres naturales [I.1] Fuego [I.7] Condiciones inadecuadas de temperatura o humedad [E.4] Errores de configuración [E.23] Errores de mantenimiento / actualización de equipos (hardware) [A.25] Robo de equipos	Medio	Se mitiga el riesgo con la implementación de los controles 11.1.1 - 11.1.2 - 11.1.3 - 11.1.4 - 11.1.5 - 11.2.2. - 12.2.1 - 16.1.2 - 17.1.1 -	Gestión de acceso a usuarios. Gestión de derechos de acceso asignados a usuarios. Acceso a redes y a Servicios de red. Suministro de acceso de usuarios. Gestión de derechos de acceso privilegiado. Protección contra las amenazas externas y ambientales. Trabajo en áreas seguras. Cadena de suministro de tecnología de información y comunicación. Procedimientos de operación documentados. Mantenimiento de equipos Revisión de los derechos de acceso de usuarios. Controles de acceso físicos ubicación y protección de los equipos. Controles contra código malicioso.	**Proyecto 1-** Control de acceso físico y protección de la información (Áreas seguras y seguridad de equipos).Ver numeral 11.1 **Proyecto 4-** Control de acceso y responsabilidades de los usuarios a los sistemas y aplicaciones. Ver numeral 11.1 **Proyecto 6-** Seguimiento y cumplimiento de la Política de Seguridad de la Información de la entidad. Ver numeral 11.1.
Switch de borde - Referencia E2910 HP - Proyecto 968	Pérdida de Disponibilidad del activo de información	[I.3] Contaminación medioambiental [I.6] Corte del suministro eléctrico	Alto	Se mitiga el riesgo con la implementación de los controles 9.2.5 11.1.2 - 11.1.4 - 11.1.5 - 11.2.1 - 11.2.4. - 11.2.3 - 12.1.1 - 12.2.1 - 15.1.3	Protección contra las amenazas externas y ambientales. Trabajo en áreas seguras. Cadena de suministro de tecnología de información y comunicación. Procedimientos de operación documentados. Mantenimiento de equipos Revisión de los derechos de acceso de usuarios. Controles de acceso físicos ubicación y protección de los equipos. Controles contra código malicioso.	**Proyecto 1-** Control de acceso físico y protección de la información (Áreas seguras y seguridad de equipos).Ver numeral 11.1 **Proyecto 2-** Responsabilidades y procedimientos de operación. Ver numeral 11.1 **Proyecto 4-** Control de acceso y responsabilidades de los usuarios. Ver numeral 11.1.

Tabla 35. (Continuación)

ACTIVOS	RIESGO	AMENAZAS	VALOR	TRATAMIENTO DE RIESGO	CONTROLES IMPLEMENTADOS	PROYECTOS DEFINIDOS
Switch de borde - Referencia E2910 HP - Proyecto 968	Pérdida de Disponibilidad del activo de información	[N.2] Daños por agua [N.*] Desastres naturales [I.1] Fuego [I.7] Condiciones inadecuadas de temperatura o humedad [E.4] Errores de configuración [E.23] Errores de mantenimiento / actualización de equipos (hardware) [A.25] Robo de equipos	Medio	Se mitiga el riesgo con la implementación de los controles 11.1.1 - 11.1.2 - 11.1.3 - 11.1.4 - 11.1.5 - 11.2.2. - 12.2.1 - 16.1.2 - 17.1.1	Gestión de acceso a usuarios. Gestión de derechos de acceso asignados a usuarios. Acceso a redes y a Servicios de red. Suministro de acceso de usuarios. Gestión de derechos de acceso privilegiado. Protección contra las amenazas externas y ambientales. Trabajo en áreas seguras. Cadena de suministro de tecnología de información y comunicación. Procedimientos de operación documentados. Mantenimiento de equipos Revisión de los derechos de acceso de usuarios. Controles de acceso físicos ubicación y protección de los equipos. Controles contra código malicioso.	**Proyecto 1-** Control de acceso físico y protección de la información (Áreas seguras y seguridad de equipos).Ver numeral 11.1 **Proyecto 4-** Control de acceso y responsabilidades de los usuarios a los sistemas y aplicaciones. Ver numeral 11.1 **Proyecto 6-** Seguimiento y cumplimiento de la Política de Seguridad de la Información de la entidad. Ver numeral 11.1.
Switch de borde - Referencia V1910 - Proyecto Misión Bogotá	Pérdida de Disponibilidad del activo de información	[I.3] Contaminación medioambiental [I.6] Corte del suministro eléctrico	Alto	Se mitiga el riesgo con la implementación de los controles 9.2.5 11.1.2 - 11.1.4 - 11.1.5 - 11.2.1 - 11.2.4. - 11.2.3 - 12.1.1 - 12.2.1 - 15.1.3	Protección contra las amenazas externas y ambientales. Trabajo en áreas seguras. Cadena de suministro de tecnología de información y comunicación. Procedimientos de operación documentados. Mantenimiento de equipos. Revisión de los derechos de acceso de usuarios. Controles de acceso físicos ubicación y protección de los equipos. Controles contra código malicioso.	**Proyecto 1-** Control de acceso físico y protección de la información (Áreas seguras y seguridad de equipos).Ver numeral 11.1 **Proyecto 2-** Responsabilidades y procedimientos de operación. Ver numeral 11.1 **Proyecto 4-** Control de acceso y responsabilidades de los usuarios. Ver numeral 11.1.

Tabla 35. (Continuación)

ACTIVOS	RIESGO	AMENAZAS	VALOR	TRATAMIENTO DE RIESGO	CONTROLES IMPLEMENTADOS	PROYECTOS DEFINIDOS
Switch de borde - Referencia V1910 - Proyecto Misión Bogotá	Pérdida de Disponibilidad del activo de información	[N.2] Daños por agua [N.*] Desastres naturales [I.1] Fuego [I.7] Condiciones inadecuadas de temperatura o humedad [E.4] Errores de configuración [E.23] Errores de mantenimiento / actualización de equipos (hardware) [A.25] Robo de equipos	Medio	Se mitiga el riesgo con la implementación de los controles 11.1.1 - 11.1.2 - 11.1.3 - 11.1.4 - 11.1.5 - 11.2.2. - 12.2.1 - 16.1.2 - 17.1.1 -	Gestión de acceso a usuarios. Gestión de derechos de acceso asignados a usuarios. Acceso a redes y a Servicios de red. Suministro de acceso de usuarios. Gestión de derechos de acceso privilegiado. Protección contra las amenazas externas y ambientales. Trabajo en áreas seguras. Cadena de suministro de tecnología de información y comunicación. Procedimientos de operación documentados. Mantenimiento de equipos Revisión de los derechos de acceso de usuarios. Controles de acceso físicos ubicación y protección de los equipos. Controles contra código malicioso.	**Proyecto 1-** Control de acceso físico y protección de la información (Áreas seguras y seguridad de equipos).Ver numeral 11.1 **Proyecto 4-** Control de acceso y responsabilidades de los usuarios a los sistemas y aplicaciones. Ver numeral 11.1 **Proyecto 6-** Seguimiento y cumplimiento de la Política de Seguridad de la Información de la entidad. Ver numeral 11.1.
Switch de borde 4500G - Sede Administrativa	Pérdida de Disponibilidad del activo de información	[I.3] Contaminación medioambiental [I.6] Corte del suministro eléctrico	Alto	Se mitiga el riesgo con la implementación de los controles 9.2.5 11.1.2 - 11.1.4 - 11.1.5 - 11.2.1 - 11.2.4. - 11.2.3 - 12.1.1 - 12.2.1 - 15.1.3	Protección contra las amenazas externas y ambientales. Trabajo en áreas seguras. Cadena de suministro de tecnología de información y comunicación. Procedimientos de operación documentados. Mantenimiento de equipos Revisión de los derechos de acceso de usuarios. Controles de acceso físicos ubicación y protección de los equipos. Controles contra código malicioso.	**Proyecto 1-** Control de acceso físico y protección de la información (Áreas seguras y seguridad de equipos).Ver numeral 11.1 **Proyecto 2-** Responsabilidades y procedimientos de operación. Ver numeral 11.1 **Proyecto 4-** Control de acceso y responsabilidades de los usuarios. Ver numeral 11.1.
		[N.2] Daños por agua [N.*] Desastres naturales [I.1] Fuego [I.7] Condiciones inadecuadas de temperatura o humedad [E.4] Errores de configuración [E.23] Errores de mantenimiento / actualización de equipos (hardware) [A.25] Robo de equipos	Medio	Se mitiga el riesgo con la implementación de los controles 9.2.5 11.1.2 - 11.1.4 - 11.1.5 - 11.2.1 - 11.2.4. - 11.2.3 - 12.1.1 - 12.2.1 - 15.1.3	Protección contra las amenazas externas y ambientales. Trabajo en áreas seguras. Cadena de suministro de tecnología de información y comunicación. Procedimientos de operación documentados. Mantenimiento de equipos. Revisión de los derechos de acceso de usuarios. Controles de acceso físicos.	**Proyecto 1-** Control de acceso físico y protección de la información (Áreas seguras y seguridad de equipos).Ver numeral 11.1 **Proyecto 2-** Responsabilidades y procedimientos de operación. Ver numeral 11.1 **Proyecto 4-** Control de acceso y responsabilidades de los usuarios. Ver numeral 11.1.

Tabla 35. (Continuación)

ACTIVOS	RIESGO	AMENAZAS	VALOR	TRATAMIENTO DE RIESGO	CONTROLES IMPLEMENTADOS	PROYECTOS DEFINIDOS
Switch de borde. Referencia 4500G - UPI La Arcadia	Pérdida de Disponibilidad del activo de información	[I.3] Contaminación medioambiental [I.6] Corte del suministro eléctrico	Alto	Se mitiga el riesgo con la implementación de los controles 9.2.5 11.1.2 - 11.1.4 - 11.1.5 - 11.2.1 - 11.2.4. - 11.2.3 - 12.1.1 - 12.2.1 - 15.1.3	Protección contra las amenazas externas y ambientales. Trabajo en áreas seguras. Cadena de suministro de tecnología de información y comunicación. Procedimientos de operación documentados. Mantenimiento de equipos Revisión de los derechos de acceso de usuarios. Controles de acceso físicos ubicación y protección de los equipos. Controles contra código malicioso.	**Proyecto 1-** Control de acceso físico y protección de la información (Áreas seguras y seguridad de equipos).Ver numeral 11.1 **Proyecto 2-** Responsabilidades y procedimientos de operación. Ver numeral 11.1 **Proyecto 4-** Control de acceso y responsabilidades de los usuarios. Ver numeral 11.1.
		[N.2] Daños por agua [N.*] Desastres naturales [I.1] Fuego [I.7] Condiciones inadecuadas de temperatura o humedad [E.4] Errores de configuración [E.23] Errores de mantenimiento / actualización de equipos (hardware) [A.25] Robo de equipos	Medio	Se mitiga el riesgo con la implementación de los controles 9.1.1 - 9.1.2 - 9.2.1 - 9.2.2 - 9.2.3 - 9.2.5 11.1.2 - 11.1.4 - 11.1.5 - 11.2.1 - 11.2.4. - 11.2.3 - 12.1.1 - 12.2.1 - 15.1.3	Gestión de acceso a usuarios. Gestión de derechos de acceso asignados a usuarios. Acceso a redes y a Servicios de red. Suministro de acceso de usuarios. Gestión de derechos de acceso privilegiado. Protección contra las amenazas externas y ambientales. Trabajo en áreas seguras. Cadena de suministro de tecnología de información y comunicación. Procedimientos de operación documentados. Mantenimiento de equipos Revisión de los derechos de acceso de usuarios. Controles de acceso físicos ubicación y protección de los equipos. Controles contra código malicioso.	**Proyecto 1-** Control de acceso físico y protección de la información (Áreas seguras y seguridad de equipos).Ver numeral 11.1 **Proyecto 4-** Control de acceso y responsabilidades de los usuarios a los sistemas y aplicaciones. Ver numeral 11.1 **Proyecto 6-** Seguimiento y cumplimiento de la Política de Seguridad de la Información de la entidad. Ver numeral 11.1.
Switch de borde. Referencia 4800G - UPI La Arcadia	Pérdida de Disponibilidad del activo de información	[I.3] Contaminación medioambiental [I.6] Corte del suministro eléctrico	Alto	Se mitiga el riesgo con la implementación de los controles 9.2.5 11.1.2 - 11.1.4 - 11.1.5 - 11.2.1 - 11.2.4. - 11.2.3 - 12.1.1 - 12.2.1 - 15.1.3	Protección contra las amenazas externas y ambientales. Trabajo en áreas seguras. Cadena de suministro de tecnología de información y comunicación. Procedimientos de operación documentados. Mantenimiento de equipos. Revisión de los derechos de acceso de usuarios. Controles de acceso físicos.	**Proyecto 1-** Control de acceso físico y protección de la información (Áreas seguras y seguridad de equipos).Ver numeral 11.1 **Proyecto 2-** Responsabilidades y procedimientos de operación. Ver numeral 11.1 **Proyecto 4-** Control de acceso y responsabilidades de los usuarios. Ver numeral 11.1.

Tabla 35. (Continuación)

ACTIVOS	RIESGO	AMENAZAS	VALOR	TRATAMIENTO DE RIESGO	CONTROLES IMPLEMENTADOS	PROYECTOS DEFINIDOS
Switch de borde. Referencia 4800G - UPI La Arcadia	Pérdida de Disponibilidad del activo de información	[N.2] Daños por agua [N.*] Desastres naturales [I.1] Fuego [I.7] Condiciones inadecuadas de temperatura o humedad [E.4] Errores de configuración [E.23] Errores de mantenimiento / actualización de equipos (hardware) [A.25] Robo de equipos	Medio	Se mitiga el riesgo con la implementación de los controles 9.1.1 - 9.1.2 - 9.2.1 - 9.2.2 - 9.2.3 - 9.2.5 11.1.2 - 11.1.4 - 11.1.5 - 11.2.1 - 11.2.4. - 11.2.3 - 12.1.1 - 12.2.1 - 15.1.3	Gestión de acceso a usuarios. Gestión de derechos de acceso asignados a usuarios. Acceso a redes y a Servicios de red. Suministro de acceso de usuarios. Gestión de derechos de acceso privilegiado. Protección contra las amenazas externas y ambientales. Trabajo en áreas seguras. Cadena de suministro de tecnología de información y comunicación. Procedimientos de operación documentados. Mantenimiento de equipos. Revisión de los derechos de acceso de usuarios. Controles de acceso físicos ubicación y protección de los equipos. Controles contra código malicioso.	**Proyecto 1-** Control de acceso físico y protección de la información (Áreas seguras y seguridad de equipos).Ver numeral 11.1 **Proyecto 4-** Control de acceso y responsabilidades de los usuarios a los sistemas y aplicaciones. Ver numeral 11.1 **Proyecto 6-** Seguimiento y cumplimiento de la Política de Seguridad de la Información de la entidad. Ver numeral 11.1.
Switch de core. Referencia 5500G - Sede Administrativa	Pérdida de Disponibilidad del activo de información	[I.3] Contaminación medioambiental [I.6] Corte del suministro eléctrico	Alto	Se mitiga el riesgo con la implementación de los controles 9.2.5 11.1.2 - 11.1.4 - 11.1.5 - 11.2.1 - 11.2.4. - 11.2.3 - 12.1.1 - 12.2.1 - 15.1.3	Protección contra las amenazas externas y ambientales. Trabajo en áreas seguras. Cadena de suministro de tecnología de información y comunicación. Procedimientos de operación documentados. Mantenimiento de equipos Revisión de los derechos de acceso de usuarios. Controles de acceso físicos ubicación y protección de los equipos. Controles contra código malicioso.	**Proyecto 1-** Control de acceso físico y protección de la información (Áreas seguras y seguridad de equipos).Ver numeral 11.1 **Proyecto 2-** Responsabilidades y procedimientos de operación. Ver numeral 11.1 **Proyecto 4-** Control de acceso y responsabilidades de los usuarios. Ver numeral 11.1.
		[N.2] Daños por agua [N.*] Desastres naturales [I.1] Fuego [I.7] Condiciones inadecuadas de temperatura o humedad [E.4] Errores de configuración [E.23] Errores de mantenimiento / actualización de equipos (hardware) [A.25] Robo de equipos	Medio	Se mitiga el riesgo con la implementación de los controles 9.1.1 - 9.1.2 - 9.2.1 - 9.2.2 - 9.2.3 - 9.2.5 11.1.2 - 11.1.4 - 11.1.5 - 11.2.1 - 11.2.4. - 11.2.3 - 12.1.1 - 12.2.1 - 15.1.3	Gestión de acceso a usuarios. Gestión de derechos de acceso asignados a usuarios. Acceso a redes y a Servicios de red. Suministro de acceso de usuarios. Gestión de derechos de acceso privilegiado. Protección contra las amenazas externas y ambientales. Trabajo en áreas seguras.	**Proyecto 1-** Control de acceso físico y protección de la información (Áreas seguras y seguridad de equipos).Ver numeral 11.1 **Proyecto 2-** Responsabilidades y procedimientos de operación. Ver numeral 11.1 **Proyecto 4-** Control de acceso y responsabilidades de los usuarios. Ver numeral 11.1.

Tabla 35. (Continuación)

ACTIVOS	RIESGO	AMENAZAS	VALOR	TRATAMIENTO DE RIESGO	CONTROLES IMPLEMENTADOS	PROYECTOS DEFINIDOS
Copia de Respaldo	Pérdida de Disponibilidad del activo de información	[I.6] Corte del suministro eléctrico [I.9] Interrupción de otros servicios o suministros esenciales [E.4] Errores de configuración	Alto	Se mitiga el riesgo con la implementación de los controles 9.2.5 11.1.2 - 11.1.4 - 11.1.5 - 11.2.1 - 11.2.4. - 11.2.3 - 12.1.1 - 12.2.1 - 15.1.3	Protección contra las amenazas externas y ambientales. Trabajo en áreas seguras. Cadena de suministro de tecnología de información y comunicación. Procedimientos de operación documentados. Mantenimiento de equipos. Revisión de los derechos de acceso de usuarios. Controles de acceso físicos ubicación y protección de los equipos. Controles contra código malicioso.	**Proyecto 1-** Control de acceso físico y protección de la información (Áreas seguras y seguridad de equipos).Ver numeral 11.1 **Proyecto 2-** Responsabilidades y procedimientos de operación. Ver numeral 11.1 **Proyecto 4-** Control de acceso y responsabilidades de los usuarios. Ver numeral 11.1.
		[N.2] Daños por agua [N.*] Desastres naturales [I.1] Fuego [I.7] Condiciones inadecuadas de temperatura o humedad [E.4] Errores de configuración [E.23] Errores de mantenimiento / actualización de equipos (hardware) [A.25] Robo de equipos	Medio	Se mitiga el riesgo con la implementación de los controles 11.1.1 - 11.1.2 - 11.1.3 - 11.1.4 - 11.1.5 - 11.2.2. - 12.2.1 - 16.1.2 - 17.1.1 -	Gestión de acceso a usuarios. Gestión de derechos de acceso asignados a usuarios. Acceso a redes y a Servicios de red. Suministro de acceso de usuarios. Gestión de derechos de acceso privilegiado. Protección contra las amenazas externas y ambientales. Trabajo en áreas seguras. Cadena de suministro de tecnología de información y comunicación. Procedimientos de operación documentados. Mantenimiento de equipos. Revisión de los derechos de acceso de usuarios. Controles de acceso físicos ubicación y protección de los equipos. Controles contra código malicioso.	**Proyecto 1-** Control de acceso físico y protección de la información (Áreas seguras y seguridad de equipos).Ver numeral 11.1 **Proyecto 2-** Responsabilidades y procedimientos de operación. Ver numeral 11.1 **Proyecto 4-** Control de acceso y responsabilidades de los usuarios. Ver numeral 11.1.
	Pérdida de la Confidencialidad, acceso no autorizado que permite la utilización indebida o no autorizada del activo de información	[E.18] Destrucción de la información	Alto	Se mitiga el riesgo con la implementación de los controles 9.2.2 - 11.1.4 - 12.2.1 - 12.4.1 - 12.2.4 - 12.4.2	Protección contra amenazas externas y ambientales. Mantenimiento de equipos. Registro de eventos. Controles contra código malicioso. Suministro de acceso de usuarios. Protección de la información de registro.	**Proyecto 1-** Control de acceso físico y protección de la información (Áreas seguras y seguridad de equipos).Ver numeral 11.1 **Proyecto 2-** Responsabilidades y procedimientos de operación. Ver numeral 11.1 **Proyecto 3-** Implementación y seguimiento de registros de actividad. Ver numeral 11.1 **Proyecto 4-** Control de acceso y responsabilidades de los usuarios. Ver numeral 11.1.

Tabla 35. (Continuación)

ACTIVOS	RIESGO	AMENAZAS	VALOR	TRATAMIENTO DE RIESGO	CONTROLES IMPLEMENTADOS	PROYECTOS DEFINIDOS
Sistema de Backups - Dataprotector	Pérdida de Disponibilidad del activo de información	[I.6] Corte del suministro eléctrico [I.9] Interrupción de otros servicios o suministros esenciales [E.4] Errores de configuración	Alto	Se mitiga el riesgo con la implementación de los controles 9.2.5 11.1.2 - 11.1.4 - 11.1.5 - 11.2.1 - 11.2.4. - 11.2.3 - 12.1.1 - 12.2.1 - 15.1.3	Protección contra las amenazas externas y ambientales. Trabajo en áreas seguras. Cadena de suministro de tecnología de información y comunicación. Procedimientos de operación documentados. Mantenimiento de equipos. Revisión de los derechos de acceso de usuarios. Controles de acceso físicos ubicación y protección de los equipos. Controles contra código malicioso.	**Proyecto 1-** Control de acceso físico y protección de la información (Áreas seguras y seguridad de equipos).Ver numeral 11.1 **Proyecto 2-** Responsabilidades y procedimientos de operación. Ver numeral 11.1 **Proyecto 4-** Control de acceso y responsabilidades de los usuarios. Ver numeral 11.1.
		[N.2] Daños por agua [N.*] Desastres naturales [I.7] Condiciones inadecuadas de temperatura o humedad [I.8] Fallo de servicios de comunicaciones [E.24] caída del sistema por agotamiento de recursos [A.23] Manipulación del hardware	Medio	Se mitiga el riesgo con la implementación de los controles 9.2.5 11.1.2 - 11.1.4 - 11.1.5 - 11.2.1 - 11.2.4. - 11.2.3 - 12.1.1 - 12.2.1 - 15.1.3	Protección contra las amenazas externas y ambientales. Trabajo en áreas seguras. Cadena de suministro de tecnología de información y comunicación. Procedimientos de operación documentados. Mantenimiento de equipos Revisión de los derechos de acceso de usuarios. Controles de acceso físicos ubicación y protección de los equipos. Controles contra código malicioso. Procedimientos de operación documentados. Registro y gestión de eventos de seguridad. Gestión de capacidad.	**Proyecto 1-** Control de acceso físico y protección de la información (Áreas seguras y seguridad de equipos).Ver numeral 11.1 **Proyecto 2-** Responsabilidades y procedimientos de operación. Ver numeral 11.1 **Proyecto 4-** Control de acceso y responsabilidades de los usuarios. Ver numeral 11.1.
	Pérdida de la Confidencialidad, acceso no autorizado que permite la utilización indebida o no autorizada del activo de información	[E.18] Destrucción de la información	Alto	Se mitiga el riesgo con la implementación de los controles 9.2.2 - 11.1.4 - 12.2.1 - 12.4.1 - 12.2.4 - 12.4.2	Protección contra amenazas externas y ambientales. Mantenimiento de equipos. Registro de eventos. Controles contra código malicioso. Suministro de acceso de usuarios. Protección de la información de registro.	**Proyecto 1-** Control de acceso físico y protección de la información (Áreas seguras y seguridad de equipos).Ver numeral 11.1 **Proyecto 2-** Responsabilidades y procedimientos de operación. Ver numeral 11.1 **Proyecto 3-** Implementación y seguimiento de registros de actividad. Ver numeral 11.1 **Proyecto 4-** Control de acceso y responsabilidades de los usuarios. Ver numeral 11.1.

Tabla 35. (Continuación)

ACTIVOS	RIESGO	AMENAZAS	VALOR	TRATAMIENTO DE RIESGO	CONTROLES IMPLEMENTADOS	PROYECTOS DEFINIDOS
Servidor de correo - Proliant DL 380 G5	Pérdida de Disponibilidad del activo de información	[I.6] Corte del suministro eléctrico [E.8] Difusión de software dañino [A.24] Denegación de servicio	Muy Alto	Se mitiga el riesgo con la implementación de los controles 9.2.2 - 9.2.5 11.1.2 - 11.1.4 - 11.1.5 - 11.2.1 - 11.2.3. - 11.2.4 - 12.1.1 - 12.2.1 - 12.2.4 - 12.4.1 - 12.4.2 - 15.1.3	Protección contra amenazas externas y ambientales. Mantenimiento de equipos. Registro de eventos. Controles contra código malicioso. Suministro de acceso de usuarios. Protección de la información de registro.	**Proyecto 1-** Control de acceso físico y protección de la información (Áreas seguras y seguridad de equipos).Ver numeral 11.1 **Proyecto 2-** Responsabilidades y procedimientos de operación. Ver numeral 11.1 **Proyecto 4-** Control de acceso y responsabilidades de los usuarios. Ver numeral 11.1.
		[N.1] Fuego [N.2] Daños por agua [N.*] Desastres naturales [I.7] Condiciones inadecuadas de temperatura o humedad [E.25] Pérdida de equipos [A.23] Manipulación del hardware [A.25] Robo de equipos [A.26] Ataque destructivo	Alto	Se mitiga el riesgo con la implementación de los controles 11.1.1 - 11.1.2 - 11.1.3 - 11.1.4 - 11.1.5 - 11.2.2. - 12.2.1 - 16.1.2 - 17.1.1 -	Gestión de acceso a usuarios. Gestión de derechos de acceso asignados a usuarios. Acceso a redes y a Servicios de red. Suministro de acceso de usuarios. Gestión de derechos de acceso privilegiado. Protección contra las amenazas externas y ambientales. Trabajo en áreas seguras. Cadena de suministro de tecnología de información y comunicación. Procedimientos de operación documentados. Mantenimiento de equipos. Revisión de los derechos de acceso de usuarios. Controles de acceso físicos ubicación y protección de los equipos. Controles contra código malicioso.	**Proyecto 1-** Control de acceso físico y protección de la información (Áreas seguras y seguridad de equipos).Ver numeral 11.1 **Proyecto 4-** Control de acceso y responsabilidades de los usuarios a los sistemas y aplicaciones. Ver numeral 11.1 **Proyecto 6-** Seguimiento y cumplimiento de la Política de Seguridad de la Información de la entidad. Ver numeral 11.1.
		[I.5] Avería de origen físico o lógico [E.2] Errores del administrador del sistema / de la seguridad [E.4] Errores de configuración [E.23] Errores de mantenimiento / actualización de equipos (hardware) [A.7] uso no previsto	Medio	Se mitiga el riesgo con la implementación de los controles 9.2.5 11.1.2 - 11.1.4 - 11.1.5 - 11.2.1 - 11.2.4. - 11.2.3 - 12.1.1 - 12.2.1 - 15.1.3	Protección contra las amenazas externas y ambientales. Trabajo en áreas seguras. Cadena de suministro de tecnología de información y comunicación. Procedimientos de operación documentados. Mantenimiento de equipos. Revisión de los derechos de acceso de usuarios. Controles de acceso físicos ubicación y protección de los equipos. Controles contra códigos maliciosos.	**Proyecto 1-** Control de acceso físico y protección de la información (Áreas seguras y seguridad de equipos).Ver numeral 11.1 **Proyecto 2-** Responsabilidades y procedimientos de operación. Ver numeral 11.1 **Proyecto 4-** Control de acceso y responsabilidades de los usuarios. Ver numeral 11.1.

Tabla 35. (Continuación)

ACTIVOS	RIESGO	AMENAZAS	VALOR	TRATAMIENTO DE RIESGO	CONTROLES IMPLEMENTADOS	PROYECTOS DEFINIDOS
Servidor de correo - Proliant DL 380 G5	Pérdida de la Integridad de la información, lo que implica el acceso indebido o fraudulento al activo de información	[E.2] Errores del administrador del sistema / de la seguridad [E.4] Errores de configuración [A.6] Abuso de privilegios de acceso [A.7] uso no previsto [A.11] Acceso no autorizado	Medio	Se mitiga el riesgo con la implementación de los controles 9.1.1 - 9.1.2 – 9.2.1 - 9.2.2 - 9.2.3 - 9.2.4 - 9.2.5 - 9.2.6 - 9.3.1 - 9.4.1 - 9.4.2 - 9.4.3 -9.4.4 - 9.4.5	Gestión de acceso a usuarios. Gestión de derechos de acceso asignados a usuarios. Acceso a redes y a Servicios de red. Suministro de acceso de usuarios. Gestión de derechos de acceso privilegiado. Protección contra las amenazas externas y ambientales. Trabajo en áreas seguras. Cadena de suministro de tecnología de información y comunicación. Procedimientos de operación documentados. Mantenimiento de equipos. Revisión de los derechos de acceso de usuarios. Controles de acceso físicos ubicación y protección de los equipos. Controles contra código malicioso.	**Proyecto 2-** Responsabilidades y procedimientos de operación.
	Pérdida de la Confidencialidad, acceso no autorizado que permite la utilización indebida o no autorizada del activo de información	[A.11] Acceso no autorizado [A.23] Manipulación del hardware	Alto	Se mitiga el riesgo con la implementación de los controles 9.1.1 - 9.1.2 - 9.2.1 - 9.2.2 - 9.2.3	Gestión de acceso a usuarios. Gestión de derechos de acceso asignados a usuarios. Acceso a redes y a Servicios de red. Suministro de acceso de usuarios. Gestión de derechos de acceso privilegiado.	**Proyecto 4-** Control de acceso y responsabilidades de los usuarios a los sistemas y aplicaciones. Ver numeral
		[E.2] Errores del administrador del sistema / de la seguridad [E.4] Errores de configuración [A.6] Abuso de privilegios de acceso [A.7] uso no previsto	Medio	Se mitiga el riesgo con la implementación de los controles 11.1.3 11.1.4 - 11.1.5	Uso aceptable de los activos. Clasificación de la información Política de control de acceso. Acceso a redes y a Servicios de red. Gestión de derechos de acceso privilegiado.	**Proyecto 1-** Control de acceso físico y protección de la información (Áreas seguras y seguridad de equipos).Ver numeral 11.1
Servidor de base de datos Nómina	Pérdida de Disponibilidad del activo de información	[E.2] Errores del administrador del sistema / de la seguridad [E.18] Destrucción de la información	Muy Alto	Se mitiga el riesgo con la implementación de los controles 9.1.1 - 9.2.2 - 9.2.3 - 9.2.6 - 12.1.1	Protección contra amenazas externas y ambientales. Mantenimiento de equipos Registro de eventos. Controles contra código malicioso. Suministro de acceso de usuarios. Protección de la información de registro.	**Proyecto 2-** Responsabilidades y procedimientos de operación.

Tabla 35. (Continuación)

ACTIVOS	RIESGO	AMENAZAS	VALOR	TRATAMIENTO DE RIESGO	CONTROLES IMPLEMENTADOS	PROYECTOS DEFINIDOS
Servidor de base de datos Nómina	Pérdida de Disponibilidad del activo de información	[N.1] Fuego [N.2] Daños por agua [N.*] Desastres naturales [E.1] Errores de los usuarios [A.6] Abuso de privilegios de acceso	Alto	Se mitiga el riesgo con la implementación de los controles 11.1.1 - 11.1.2 - 11.1.3 - 11.1.4 - 11.1.5 - 11.2.2. - 12.2.1 - 16.1.2 - 17.1.1 -	Perímetro de seguridad física. Controles de acceso físicos. Seguridad de oficinas, recinto e instalaciones. Protección contra amenazas externas y ambientales. Trabajo en áreas seguras. Servicios de suministro ubicación y protección de los equipos. Reporte de eventos de seguridad de la información. Planificación de la continuidad de la seguridad de la información. Controles contra códigos maliciosos Procedimientos de operación documentados. Registro y gestión de eventos de seguridad. Gestión de capacidad.	**Proyecto 1-** Control de acceso físico y protección de la información (Áreas seguras y seguridad de equipos).Ver numeral 11.1 **Proyecto 2-** Responsabilidades y procedimientos de operación. Ver numeral 11.1 **Proyecto 5-** Adaptación Plan de contingencia TICS, como marco de Gestión del Plan de Continuidad del Negocio. Ver numeral 11.1 **Proyecto 7-** Gestión de incidentes de seguridad de la información. Ver numeral 11.1
	Pérdida de la Integridad de la información, lo que implica el acceso indebido o fraudulento al activo de información	[E.1] Errores de los usuarios [E.15] Alteración de la información [E.18] Destrucción de la información [A.6] Abuso de privilegios de acceso	Muy Alto	Se mitiga el riesgo con la implementación de los controles 9.1.1 - 9.1.2 – 9.2.1 - 9.2.2 - 9.2.3 - 9.2.4 - 9.2.5 - 9.2.6 - 9.3.1 - 9.4.1 - 9.4.2 - 9.4.3 -9.4.4 - 9.4.5	Protección contra amenazas externas y ambientales. Mantenimiento de equipos. Registro de eventos. Controles contra código malicioso. Suministro de acceso de usuarios. Protección de la información de registro.	Proyecto 4– Control de acceso y responsabilidades de los usuarios a los sistemas y aplicaciones. Ver numeral 11.1
		[N.1] Fuego [N.2] Daños por agua [N.*] Desastres naturales [E.2] Errores del administrador del sistema / de la seguridad	Alto	Se mitiga el riesgo con la implementación de los controles 11.1.1 - 11.1.2 - 11.1.3 - 11.1.4 - 11.1.5 - 11.2.2. - 12.2.1 - 16.1.2 - 17.1.1 -	Perímetro de seguridad física. Controles de acceso físicos. Seguridad de oficinas, recinto e instalaciones. Protección contra amenazas externas y ambientales. Trabajo en áreas seguras. Servicios de suministro ubicación y protección de los equipos. Reporte de eventos de seguridad de la información. Planificación de la continuidad de la seguridad de la información. Controles contra códigos maliciosos. Procedimientos de operación documentados.	**Proyecto 1-** Control de acceso físico y protección de la información (Áreas seguras y seguridad de equipos).Ver numeral 11.1 **Proyecto 2-** Responsabilidades y procedimientos de operación. Ver numeral 11.1 **Proyecto 5-** Adaptación Plan de contingencia TICS, como marco de Gestión del Plan de Continuidad del Negocio. Ver numeral 11.1 **Proyecto 7-** Gestión de incidentes de seguridad de la información. Ver numeral 11.1

Tabla 35. (Continuación)

ACTIVOS	RIESGO	AMENAZAS	VALOR	TRATAMIENTO DE RIESGO	CONTROLES IMPLEMENTADOS	PROYECTOS DEFINIDOS
Servidor de base de datos Nómina	Pérdida de la Confidencialidad, acceso no autorizado que permite la utilización indebida o no autorizada del activo de información	[N.1] Fuego [N.2] Daños por agua [N.*] Desastres naturales	Alto	Se mitiga el riesgo con la implementación de los controles 11.1.1 - 11.1.2 - 11.1.3 - 11.1.4 - 11.1.5 - 11.2.2. - 12.2.1 - 16.1.2 - 17.1.1 -	Perímetro de seguridad física. Controles de acceso físicos. Seguridad de oficinas, recinto e instalaciones. Protección contra amenazas externas y ambientales. Trabajo en áreas seguras. Servicios de suministro ubicación y protección de los equipos. Reporte de eventos de seguridad de la información. Planificación de la continuidad de la seguridad de la información. Controles contra códigos maliciosos. Procedimientos de operación documentados. Registro y gestión de eventos de seguridad. Gestión de capacidad.	**Proyecto 1-** Control de acceso físico y protección de la información (Áreas seguras y seguridad de equipos).Ver numeral 11.1 **Proyecto 2-** Responsabilidades y procedimientos de operación. Ver numeral 11.1 **Proyecto 5-** Adaptación Plan de contingencia TICS, como marco de Gestión del Plan de Continuidad del Negocio. Ver numeral 11.1 **Proyecto 7-** Gestión de incidentes de seguridad de la información. Ver numeral 11.1
Servidor de Virtualización	Pérdida de Disponibilidad del activo de información	[N.1] Fuego [N.2] Daños por agua	Muy Alto	Se mitiga el riesgo con la implementación de los controles 11.1.1 - 11.1.2 - 11.1.3 - 11.1.4 - 11.1.5 - 11.2.2. - 12.2.1 - 16.1.2 - 17.1.1 -	Perímetro de seguridad física. Controles de acceso físicos. Seguridad de oficinas, recinto e instalaciones. Protección contra amenazas externas y ambientales. Trabajo en áreas seguras. Servicios de suministro ubicación y protección de los equipos. Reporte de eventos de seguridad de la información. Planificación de la continuidad de la seguridad de la información. Controles contra códigos maliciosos. Procedimientos de operación documentados. Registro y gestión de eventos de seguridad. Gestión de capacidad.	**Proyecto 1-** Control de acceso físico y protección de la información (Áreas seguras y seguridad de equipos).Ver numeral 11.1 **Proyecto 2-** Responsabilidades y procedimientos de operación. Ver numeral 11.1 **Proyecto 5-** Adaptación Plan de contingencia TICS, como marco de Gestión del Plan de Continuidad del Negocio. Ver numeral 11.1 **Proyecto 7-** Gestión de incidentes de seguridad de la información. Ver numeral 11.1

Tabla 35. (Continuación)

ACTIVOS	RIESGO	AMENAZAS	VALOR	TRATAMIENTO DE RIESGO	CONTROLES IMPLEMENTADOS	PROYECTOS DEFINIDOS
Servidor de Virtualización	Pérdida de Disponibilidad del activo de información	[E.24] caída del sistema por agotamiento de recursos [A.8] Difusión de software dañino [A.23] Manipulación del hardware [A.26] Ataque destructivo	Alto	Se mitiga el riesgo con la Implementación de los controles 12.1.1 - 12.1.3 - 12.4.1	Procedimientos de operación documentados. Registro y gestión de eventos de seguridad. Gestión de capacidad. Seguridad de oficina despachos y recursos. Proceso disciplinario. Implantación de la seguridad de la información. Control contra código malicioso. Registro y gestión de eventos de seguridad.	**Proyecto 2-** Responsabilidades y procedimientos de operación. Ver numeral 11.1
		[E.2] Errores del administrador del sistema / de la seguridad [E.4] Errores de configuración [A.24] Denegación de servicio	Medio	Se mitiga el riesgo con la implementación de los controles 9.1.1 - 9.1.2 – 9.2.1 - 9.2.2 - 9.2.3 - 9.2.4 - 9.2.5 - 9.2.6 - 9.3.1 - 9.4.1 - 9.4.2 - 9.4.3 -9.4.4 - 9.4.5	Procedimientos de operación documentados. Registro de eventos. Protección de la información de registro. Registros del administrador y del operador. Cadena de suministro en tecnologías de la información y comunicaciones. Responsabilidades y procedimientos.	**Proyecto 2-** Responsabilidades y procedimientos de operación.
	Pérdida de la Integridad de la información, lo que implica el acceso indebido o fraudulento al activo de información	[N.1] Fuego [N.2] Daños por agua [I.1] Fuego [I.2] Daños por agua	Muy Alto	Se mitiga el riesgo con la implementación de los controles 11.1.1 - 11.1.2 - 11.1.3 - 11.1.4 - 11.1.5 - 11.2.2. - 12.2.1 - 16.1.2 - 17.1.1 -	Perímetro de seguridad física. Controles de acceso físicos. Seguridad de oficinas, recinto e instalaciones. Protección contra amenazas externas y ambientales. Trabajo en áreas seguras. Servicios de suministro ubicación y protección de los equipos. Reporte de eventos de seguridad de la información. Planificación de la continuidad de la seguridad de la información. Controles contra códigos maliciosos. Procedimientos de operación documentados. Registro y gestión de eventos de seguridad. Gestión de capacidad.	**Proyecto 1-** Control de acceso físico y protección de la información (Áreas seguras y seguridad de equipos).Ver numeral 11.1 **Proyecto 2-** Responsabilidades y procedimientos de operación. Ver numeral 11.1 **Proyecto 5-** Adaptación Plan de contingencia TICS, como marco de Gestión del Plan de Continuidad del Negocio. Ver numeral 11.1 **Proyecto 7-** Gestión de incidentes de seguridad de la información. Ver numeral 11.1

Tabla 35. (Continuación)

ACTIVOS	RIESGO	AMENAZAS	VALOR	TRATAMIENTO DE RIESGO	CONTROLES IMPLEMENTADOS	PROYECTOS DEFINIDOS
Servidor de Virtualización	Pérdida de la Integridad de la información, lo que implica el acceso indebido o fraudulento al activo de información	[E.24] caída del sistema por agotamiento de recursos [A.8] Difusión de software dañino [A.23] Manipulación del hardware [A.26] Ataque destructivo	Alto	Se mitiga el riesgo con la Implementación de los controles 12.1.1 - 12.1.3 - 12.4.1	Procedimientos de operación documentados. Registro y gestión de eventos de seguridad. Gestión de capacidad. Seguridad de oficina despachos y recursos. Proceso disciplinario. Implantación de la seguridad de la información. Control contra código malicioso. Registro y gestión de eventos de seguridad.	**Proyecto 2-** Responsabilidades y procedimientos de operación. Ver numeral 11.1
		[E.2] Errores del administrador del sistema / de la seguridad [E.4] Errores de configuración [A.24] Denegación de servicio	Medio	Se mitiga el riesgo con la implementación de los controles 9.1.1 - 9.1.2 – 9.2.1 - 9.2.2 - 9.2.3 - 9.2.4 - 9.2.5 - 9.2.6 - 9.3.1 - 9.4.1 - 9.4.2 - 9.4.3 -9.4.4 - 9.4.5	Procedimientos de operación documentados. Registro de eventos. Protección de la información de registro. Registros del administrador y del operador.	**Proyecto 2-** Responsabilidades y procedimientos de operación.
Servidor base de datos SQL	Pérdida de Disponibilidad del activo de información	[A.8] Difusión de software dañino	Alto	Se mitiga el riesgo con la implementación de los controles 9.2.2 - 11.1.4 - 12.2.1 - 12.4.1 - 12.2.4 - 12.4.2	Protección contra amenazas externas y ambientales. Mantenimiento de equipos. Registro de eventos. Controles contra código malicioso Suministro de acceso de usuarios. Protección de la información de registro.	**Proyecto 1-** Control de acceso físico y protección de la información (Áreas seguras y seguridad de equipos).Ver numeral 11.1 **Proyecto 2-** Responsabilidades y procedimientos de operación. Ver numeral 11.1 **Proyecto 3-** Implementación y seguimiento de registros de actividad. Ver numeral 11.1
		[N.*] Desastres naturales	Medio	Se mitiga el riesgo con la implementación de los controles 11.1.1 - 17.1.1	Protección contra amenazas externas y ambientales. Planificación de la continuidad de la seguridad de la información.	**Proyecto 1-** Control de acceso físico y protección de la información (Áreas seguras y seguridad de equipos).Ver numeral 11.1 **Proyecto 5-** Adaptación Plan de contingencia TICS, como marco de Gestión del Plan de Continuidad del Negocio. Ver numeral 11.1
	Pérdida de la Integridad de la información, lo que implica el acceso indebido o fraudulento al activo de información	[A.8] Difusión de software dañino [A.15] Modificación de la información	Alto	Se mitiga el riesgo con la implementación de los controles 9.2.2 - 11.1.4 - 12.2.1 - 12.4.1 - 12.2.4 - 12.4.2	Protección contra amenazas externas y ambientales. Mantenimiento de equipos. Registro de eventos. Controles contra código malicioso. Suministro de acceso de usuarios. Protección de la información de registro.	**Proyecto 1-** Control de acceso físico y protección de la información (Áreas seguras y seguridad de equipos).Ver numeral 11.1 **Proyecto 2-** Responsabilidades y procedimientos de operación. Ver numeral 11.1 **Proyecto 3-** Implementación y seguimiento de registros de actividad. Ver numeral 11.1

Tabla 35. (Continuación)

ACTIVOS	RIESGO	AMENAZAS	VALOR	TRATAMIENTO DE RIESGO	CONTROLES IMPLEMENTADOS	PROYECTOS DEFINIDOS
Servidor base de datos SQL	Pérdida de la Integridad de la información, lo que implica el acceso indebido o fraudulento al activo de información	[N.*] Desastres naturales	Medio	Se mitiga el riesgo con la implementación de los controles 11.1.1 - 17.1.1	Protección contra amenazas externas y ambientales. Planificación de la continuidad de la seguridad de la información.	**Proyecto 1-** Control de acceso físico y protección de la información (Áreas seguras y seguridad de equipos).Ver numeral 11.1 **Proyecto 5-** Adaptación Plan de contingencia TICS, como marco de Gestión del Plan de Continuidad del Negocio. Ver numeral 11.1
	Pérdida de la Confidencialidad, acceso no autorizado que permite la utilización indebida o no autorizada del activo de información	[A.11] Acceso no autorizado [A.15] Modificación de la información	Alto	Se mitiga el riesgo con la implementación de los controles 9.1.1 - 9.1.2 - 9.2.1 - 9.2.2 - 9.2.3	Gestión de acceso a usuarios. Gestión de derechos de acceso asignados a usuarios. Acceso a redes y a Servicios de red. Suministro de acceso de usuarios. Gestión de derechos de acceso privilegiado.	**Proyecto 4-** Control de acceso y responsabilidades de los usuarios a los sistemas y aplicaciones. Ver numeral
Servidor de Archivos	Pérdida de Disponibilidad del activo de información	[I.3] Contaminación medioambiental [I.6] Corte del suministro eléctrico	Muy Alto	Se mitiga el riesgo con la implementación de los controles 9.2.5 11.1.2 - 11.1.4 - 11.1.5 - 11.2.1 - 11.2.4. - 11.2.3 - 12.1.1 - 12.2.1 - 15.1.3	Servicios de suministro. Seguimiento y revisión de los servicios de los proveedores.	**Proyecto 1-** Control de acceso físico y protección de la información (Áreas seguras y seguridad de equipos).Ver numeral 11.1 **Proyecto 2-** Responsabilidades y procedimientos de operación. Ver numeral 11.1 **Proyecto 4-** Control de acceso y responsabilidades de los usuarios. Ver numeral 11.1.
		[N.2] Daños por agua [N.*] Desastres naturales [E.24] caída del sistema por agotamiento de recursos	Alto	Se mitiga el riesgo con la implementación de los controles 11.1.1 - 11.1.2 - 11.1.3 - 11.1.4 - 11.1.5 - 11.2.2. - 12.1.1 - 12.1.3 - 12.4.1 - 12.2.1 - 16.1.2 - 17.1.1 -	Registro y gestión de eventos de seguridad. Protección contra amenazas externas y ambientales. Planificación de la continuidad de la seguridad de la información. Procedimientos de operación documentados. Registro y gestión de eventos de seguridad. Gestión de capacidad.	**Proyecto 1-** Control de acceso físico y protección de la información (Áreas seguras y seguridad de equipos).Ver numeral 11.1 **Proyecto 2-** Responsabilidades y procedimientos de operación. Ver numeral 11.1 **Proyecto 5-** Adaptación Plan de contingencia TICS, como marco de Gestión del Plan de Continuidad del Negocio. Ver numeral 11.1 **Proyecto 7-** Gestión de incidentes de seguridad de la información. Ver numeral 11.1

Tabla 35. (Continuación)

ACTIVOS	RIESGO	AMENAZAS	VALOR	TRATAMIENTO DE RIESGO	CONTROLES IMPLEMENTADOS	PROYECTOS DEFINIDOS
Servidor de Archivos	Pérdida de Disponibilidad del activo de información	[I.7] Condiciones inadecuadas de temperatura o humedad [A.8] Difusión de software dañino	Medio	Se mitiga el riesgo con la implementación de los controles 9.2.5 11.1.2 - 11.1.4 - 11.1.5 - 11.2.1 - 11.2.4. - 11.2.3 - 12.1.1 - 12.2.1 - 15.1.3	Protección contra las amenazas externas y ambientales. Trabajo en áreas seguras. Cadena de suministro de tecnología de información y comunicación. Procedimientos de operación documentados. Mantenimiento de equipos. Revisión de los derechos de acceso de usuarios. Controles de acceso físicos ubicación y protección de los equipos. Controles contra código malicioso.	**Proyecto 1-** Control de acceso físico y protección de la información (Áreas seguras y seguridad de equipos).Ver numeral 11.1 **Proyecto 2-** Responsabilidades y procedimientos de operación. Ver numeral 11.1 **Proyecto 4-** Control de acceso y responsabilidades de los usuarios. Ver numeral 11.1.
	Pérdida de la Integridad de la información, lo que implica el acceso indebido o fraudulento al activo de información	[E.1] Errores de los usuarios [E.15] Alteración de la información [E.18] Destrucción de la información [A.15] Modificación de la información [A.18] Destrucción de la información	Muy Alto	Se mitiga el riesgo con la implementación de los controles 8.2.2 - 9.1.1- 9.2.1 - 9.2.2 - 9.2.3 - 9.2.5- 11.1.4 -11.2.8 - 12.1.2	Suministro de acceso de usuarios. Protección contra amenazas externas y ambientales. Mantenimiento de equipos Registro de eventos. Gestión de las vulnerabilidades técnicas. Evaluación de eventos de seguridad de la información y decisiones sobre ellos. Respuesta a incidentes de seguridad de la información. Manejo de activos. Gestión de derechos de acceso privilegiado. Equipos de usuario desatendido. Procedimientos de operación documental.	**Proyecto 2-** Responsabilidades y procedimientos de operación. Ver numeral 11.1 **Proyecto 4-** Control de acceso y responsabilidades de los usuarios a los sistemas y aplicaciones. Ver numeral 11.1

Tabla 35. (Continuación)

ACTIVOS	RIESGO	AMENAZAS	VALOR	TRATAMIENTO DE RIESGO	CONTROLES IMPLEMENTADOS	PROYECTOS DEFINIDOS
Servidor de Archivos	Pérdida de la Integridad de la información, lo que implica el acceso indebido o fraudulento al activo de información	[N.2] Daños por agua [N.*] Desastres naturales [A.6] Abuso de privilegios de acceso [A.11] Acceso no autorizado	Alto	Se mitiga el riesgo con la implementación de los controles 9.1.1 - 9.1.2 – 9.2.1 - 9.2.2 - 9.2.3 - 9.2.4 - 9.2.5 - 9.2.6 - 9.3.1 - 9.4.1 - 9.4.2 - 9.4.3 -9.4.4 - 9.4.5 - 11.1.1 - 11.1.2 - 11.1.3 - 11.1.4 - 11.1.5 - 11.2.2. - 12.2.1 - 16.1.2 - 17.1.1 -	Perímetro de seguridad física. Controles de acceso físicos. Seguridad de oficinas, recinto e instalaciones. Protección contra amenazas externas y ambientales. Trabajo en áreas seguras. Servicios de suministro ubicación y protección de los equipos. Reporte de eventos de seguridad de la información. Planificación de la continuidad de la seguridad de la información. Controles contra códigos maliciosos. Procedimientos de operación documentados. Registro y gestión de eventos de seguridad. Gestión de capacidad.	**Proyecto 1-** Control de acceso físico y protección de la información (Áreas seguras y seguridad de equipos).Ver numeral 11.1 **Proyecto 2-** Responsabilidades y procedimientos de operación. Ver numeral 11.1 Proyecto 4– Control de acceso y responsabilidades de los usuarios a los sistemas y aplicaciones. Ver numeral 11.1 **Proyecto 5-** Adaptación Plan de contingencia TICS, como marco de Gestión del Plan de Continuidad del Negocio. Ver numeral 11.1 **Proyecto 7-** Gestión de incidentes de seguridad de la información. Ver numeral 11.1
		[A.8] Difusión de software dañino	Medio	Se mitiga el riesgo con la implementación de los controles 9.2.2 - 11.1.4 - 12.2.1 - 12.4.1 - 12.2.4 - 12.4.2	Protección contra amenazas externas y ambientales. Mantenimiento de equipos. Registro de eventos. Controles contra código malicioso. Suministro de acceso de usuarios. Protección de la información de registro.	**Proyecto 1-** Control de acceso físico y protección de la información (Áreas seguras y seguridad de equipos).Ver numeral 11.1 **Proyecto 2-** Responsabilidades y procedimientos de operación. Ver numeral 11.1 **Proyecto 3-** Implementación y seguimiento de registros de actividad. Ver numeral 11.1
	Pérdida de la Confidencialidad, acceso no autorizado que permite la utilización indebida o no autorizada del activo de información	[A.15] Modificación de la información [A.18] Destrucción de la información	Muy Alto	Se mitiga el riesgo con la implementación de los controles 8.2.2 - 9.1.1- 9.2.1 - 9.2.2 - 9.2.3 - 9.2.5- 11.1.4 -11.2.8 - 12.1.2	Suministro de acceso de usuarios. Protección contra amenazas externas y ambientales. Mantenimiento de equipos. Registro de eventos. Gestión de las vulnerabilidades técnicas. Evaluación de eventos de seguridad de la información y decisiones sobre ellos. Respuesta a incidentes de seguridad de la información. Manejo de activos.	**Proyecto 2-** Responsabilidades y procedimientos de operación. Ver numeral 11.1 **Proyecto 4-** Control de acceso y responsabilidades de los usuarios a los sistemas y aplicaciones. Ver numeral 11.1

Tabla 35. (Continuación)

ACTIVOS	RIESGO	AMENAZAS	VALOR	TRATAMIENTO DE RIESGO	CONTROLES IMPLEMENTADOS	PROYECTOS DEFINIDOS
Servidor de Archivos	Pérdida de la Confidencialidad, acceso no autorizado que permite la utilización indebida o no autorizada del activo de información	[A.6] Abuso de privilegios de acceso [A.11] Acceso no autorizado	Alto	Se mitiga el riesgo con la implementación de los controles 9.1.1 - 9.1.2 – 9.2.1 - 9.2.2 - 9.2.3 - 9.2.4 - 9.2.5 - 9.2.6 - 9.3.1 - 9.4.1 - 9.4.2 - 9.4.3	Política de control de acceso. Acceso a redes y a Servicios de red. Registro y cancelación del registro de usuarios. Gestión de derechos de acceso privilegiado. Suministro de acceso de usuarios. Revisión de los derechos de acceso de usuarios. Retiro o ajuste de los derechos de usuario. Uso de información de información secreta para la autenticación. Restricción de acceso a la información. Procedimiento de ingreso seguro Sistema de gestión de contraseñas. Controles de acceso físicos. Seguridad de oficinas, recinto e instalaciones.	**Proyecto 4–** Control de acceso y responsabilidades de los usuarios a los sistemas y aplicaciones. Ver numeral 11.1
	Pérdida de Autenticidad, en el comportamiento, resultado o uso del activo de información	[A.6] Abuso de privilegios de acceso	Alto	Se mitiga el riesgo con la implementación de los controles 9.1.1 - 9.1.2 – 9.2.1 - 9.2.2 - 9.2.3 - 9.2.4 - 9.2.5 - 9.2.6 - 9.3.1 - 9.4.1 - 9.4.2 - 9.4.3	Política de control de acceso. Acceso a redes y a Servicios de red. Registro y cancelación del registro de usuarios. Gestión de derechos de acceso privilegiado. Suministro de acceso de usuarios Revisión de los derechos de acceso de usuarios. Retiro o ajuste de los derechos de usuario. Uso de información de información secreta para la autenticación. Restricción de acceso a la información. Procedimiento de ingreso seguro Sistema de gestión de contraseñas. Controles de acceso físicos. Seguridad de oficinas, recinto e instalaciones.	**Proyecto 4–** Control de acceso y responsabilidades de los usuarios a los sistemas y aplicaciones. Ver numeral 11.1

Tabla 35. (Continuación)

ACTIVOS	RIESGO	AMENAZAS	VALOR	TRATAMIENTO DE RIESGO	CONTROLES IMPLEMENTADOS	PROYECTOS DEFINIDOS
Servidor de impresión	Pérdida de Disponibilidad del activo de información	[N.*] Desastres naturales [E.24] caída del sistema por agotamiento de recursos [A.8] Difusión de software dañino [A.24] Denegación de servicio [N.1] Fuego [N.2] Daños por agua	Muy Alto	Se mitiga el riesgo con la implementación de los controles 9.2.5 11.1.2 - 11.1.4 - 11.1.5 - 11.2.1 - 11.2.4. - 11.2.3 - 12.1.1 - 12.1.3 -12.2.1 - 12.4.1 -15.1.3	Protección contra las amenazas externas y ambientales. Trabajo en áreas seguras. Cadena de suministro de tecnología de información y comunicación. Procedimientos de operación documentados. Mantenimiento de equipos. Revisión de los derechos de acceso de usuarios. Controles de acceso físicos ubicación y protección de los equipos. Controles contra código malicioso. Procedimientos de operación documentados. Registro y gestión de eventos de seguridad. Gestión de capacidad.	**Proyecto 1-** Control de acceso físico y protección de la información (Áreas seguras y seguridad de equipos).Ver numeral 11.1 **Proyecto 2-** Responsabilidades y procedimientos de operación. Ver numeral 11.1 **Proyecto 4-** Control de acceso y responsabilidades de los usuarios. Ver numeral 11.1.
		[I.5] Avería de origen físico o lógico [I.6] Corte del suministro eléctrico [I.7] Condiciones inadecuadas de temperatura o humedad [I.8.11] Interrupción accidental [A.5] suplantación de la identidad del usuario [A.6] Abuso de privilegios de acceso [A.11] Acceso no autorizado	Alto	Se mitiga el riesgo con la implementación de los controles 9.2.5 11.1.2 - 11.1.4 - 11.1.5 - 11.2.1 - 11.2.4. - 11.2.3 - 12.1.1 - 12.2.1 - 15.1.3	Gestión de acceso a usuarios. Gestión de derechos de acceso asignados a usuarios. Protección contra las amenazas externas y ambientales. Trabajo en áreas seguras. Cadena de suministro de tecnología de información y comunicación. Procedimientos de operación documentados. Mantenimiento de equipos. Revisión de los derechos de acceso de usuarios. Controles de acceso físicos ubicación y protección de los equipos. Controles contra códigos maliciosos. Gestión de derechos de acceso con privilegios especiales. Protección contra las amenazas externas y ambientales. Cadena de suministro en tecnologías de la información y comunicaciones. Protección contra las amenazas externas y ambientales.	**Proyecto 1-** Control de acceso físico y protección de la información (Áreas seguras y seguridad de equipos).Ver numeral 11.1 **Proyecto 2-** Responsabilidades y procedimientos de operación. Ver numeral 11.1 **Proyecto 4-** Control de acceso y responsabilidades de los usuarios. Ver numeral 11.1.

Tabla 35. (Continuación)

ACTIVOS	RIESGO	AMENAZAS	VALOR	TRATAMIENTO DE RIESGO	CONTROLES IMPLEMENTADOS	PROYECTOS DEFINIDOS
Servidor de impresión	Pérdida de Disponibilidad del activo de información	[E.2] Errores del administrador del sistema / de la seguridad [E.4] Errores de configuración [E.21] Errores de mantenimiento / actualización de programas (software)	Medio	Se mitiga el riesgo con la implementación de los controles 9.1.1 - 9.1.2 – 9.2.1 - 9.2.2 - 9.2.3 - 9.2.4 - 9.2.5 - 9.2.6 - 9.3.1 - 9.4.1 - 9.4.2 - 9.4.3 -9.4.4 - 9.4.5	Procedimientos de operación documentados. Registro de eventos. Protección de la información de registro. Registros del administrador y del operador.	**Proyecto 2-** Responsabilidades y procedimientos de operación.
	Trazabilidad, pérdida de los registros de actividad en los activos informáticos	[N.*] Desastres naturales [E.24] caída del sistema por agotamiento de recursos [A.8] Difusión de software dañino [A.24] Denegación de servicio	Alto	Se mitiga el riesgo con la implementación de los controles 9.2.2 - 11.1.4 - 12.1.1 - 12.1.3 - 12.2.1 - 12.4.1 - 12.2.4 - 12.4.2	Protección contra amenazas externas y ambientales. Planificación de la continuidad de la seguridad de la información. Procedimientos de operación documentados. Registro y gestión de eventos de seguridad. Gestión de capacidad.	**Proyecto 1-** Control de acceso físico y protección de la información (Áreas seguras y seguridad de equipos).Ver numeral 11.1 **Proyecto 2-** Responsabilidades y procedimientos de operación. Ver numeral 11.1 **Proyecto 5-** Adaptación Plan de contingencia TICS, como marco de Gestión del Plan de Continuidad del Negocio. Ver numeral 11.1
		[N.1] Fuego [N.2] Daños por agua [I.5] Avería de origen físico o lógico [I.6] Corte del suministro eléctrico [I.7] Condiciones inadecuadas de temperatura o humedad [I.8.11] Interrupción accidental [A.5] suplantación de la identidad del usuario [A.6] Abuso de privilegios de acceso [A.11] Acceso no autorizado	Medio	Se mitiga el riesgo con la implementación de los controles 9.1.1 - 9.1.2 – 9.2.1 - 9.2.2 - 9.2.3 - 9.2.4 - 9.2.5 - 9.2.6 - 9.3.1 - 9.4.1 - 9.4.2 - 9.4.3 -9.4.4 - 9.4.5	Protección contra las amenazas externas y ambientales. Trabajo en áreas seguras. Cadena de suministro de tecnología de información y comunicación. Procedimientos de operación documentados. Mantenimiento de equipos. Revisión de los derechos de acceso de usuarios. Controles de acceso físicos ubicación y protección de los equipos. Controles contra códigos maliciosos.	**Proyecto 1-** Control de acceso físico y protección de la información (Áreas seguras y seguridad de equipos).Ver numeral 11.1 **Proyecto 4-** Control de acceso y responsabilidades de los usuarios a los sistemas y aplicaciones. Ver numeral 11.1 **Proyecto 6-** Seguimiento y cumplimiento de la Política de Seguridad de la Información de la entidad. Ver numeral 11.1.
		[I.6] Corte del suministro eléctrico [I.7] Condiciones inadecuadas de temperatura o humedad [E.4] Errores de configuración [A.24] Denegación de servicio	Alto	Se mitiga el riesgo con la implementación de los controles 9.1.1 - 9.1.2 – 9.2.1 - 9.2.2 - 9.2.3 - 9.2.4 - 9.2.5 - 9.2.6 - 9.3.1 - 9.4.1 - 9.4.2 - 9.4.3	Protección contra las amenazas externas y ambientales. Trabajo en áreas seguras. Cadena de suministro de tecnología de información y comunicación. Procedimientos de operación documentados. Mantenimiento de equipos. Revisión de los derechos de acceso de usuarios. Controles de acceso físicos ubicación y protección de los equipos.	**Proyecto 1-** Control de acceso físico y protección de la información (Áreas seguras y seguridad de equipos).Ver numeral 11.1 **Proyecto 2-** Responsabilidades y procedimientos de operación. Ver numeral 11.1 **Proyecto 4-** Control de acceso y responsabilidades de los usuarios. Ver numeral 11.1.

Tabla 35. (Continuación)

ACTIVOS	RIESGO	AMENAZAS	VALOR	TRATAMIENTO DE RIESGO	CONTROLES IMPLEMENTADOS	PROYECTOS DEFINIDOS
Servidor OAS – SICAPITAL	Pérdida de Disponibilidad del activo de información	[N.1] Fuego [N.2] Daños por agua [N.*] Desastres naturales [I.5] Avería de origen físico o lógico [E.2] Errores del administrador del sistema / de la seguridad [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 [A.4] Manipulación de los ficheros de configuración	Medio	Se mitiga el riesgo con la implementación de los controles 9.1.1 - 9.1.2 – 9.2.1 - 9.2.2 - 9.2.3 - 9.2.4 - 9.2.5 - 9.2.6 - 9.3.1 - 9.4.1 - 9.4.2 - 9.4.3 -9.4.4 - 9.4.5 - 11.1.2 - 11.1.4 - 11.1.5 - 11.2.1 - 11.2.4. - 11.2.3 - 12.1.1 - 12.2.1 - 12.1.3 - 12.1.4 - 15.1.3	Protección contra las amenazas externas y ambientales. Trabajo en áreas seguras. Cadena de suministro de tecnología de información y comunicación. Procedimientos de operación documentados. Mantenimiento de equipos Revisión de los derechos de acceso de usuarios. Controles de acceso físicos ubicación y protección de los equipos. Controles contra códigos maliciosos. Procedimientos de operación documentados. Registro de eventos. Protección de la información de registro. Registros del administrador y del operador.	**Proyecto 1-** Control de acceso físico y protección de la información (Áreas seguras y seguridad de equipos).Ver numeral 11.1 **Proyecto 2-** Responsabilidades y procedimientos de operación. Ver numeral 11.1 **Proyecto 4-** Control de acceso y responsabilidades de los usuarios. Ver numeral 11.1.
	Pérdida de la Integridad de la información, lo que implica el acceso indebido o fraudulento al activo de información	[I.5] Avería de origen físico o lógico [I.6] Corte del suministro eléctrico [I.7] Condiciones inadecuadas de temperatura o humedad [A.5] suplantación de la identidad del usuario [A.6] Abuso de privilegios de acceso [A.18] Destrucción de la información	Medio	Se mitiga el riesgo con la implementación de los controles 9.1.1 - 9.1.2 – 9.2.1 - 9.2.2 - 9.2.3 - 9.2.4 - 9.2.5 - 9.2.6 - 9.3.1 - 9.4.1 - 9.4.2 - 9.4.3	Protección contra las amenazas externas y ambientales. Trabajo en áreas seguras. Cadena de suministro de tecnología de información y comunicación. Procedimientos de operación documentados. Mantenimiento de equipos. Revisión de los derechos de acceso de usuarios. Controles de acceso físicos ubicación y protección de los equipos. Controles contra códigos maliciosos.	**Proyecto 1-** Control de acceso físico y protección de la información (Áreas seguras y seguridad de equipos).Ver numeral 11.1 **Proyecto 2-** Responsabilidades y procedimientos de operación. Ver numeral 11.1 **Proyecto 4-** Control de acceso y responsabilidades de los usuarios. Ver numeral 11.1.
	Pérdida de la Confidencialidad, acceso no autorizado que permite la utilización indebida o no autorizada del activo de información	[A.5] suplantación de la identidad del usuario [A.6] Abuso de privilegios de acceso	Medio	Se mitiga el riesgo con la implementación de los controles 9.1.1 - 9.1.2 – 9.2.1 - 9.2.2 - 9.2.3 - 9.2.4 - 9.2.5 - 9.2.6 - 9.3.1 - 9.4.1 - 9.4.2 - 9.4.3	Mantenimiento de equipos. Revisión de los derechos de acceso de usuarios. Controles de acceso físicos. Ubicación y protección de los equipos. Controles contra códigos maliciosos.	**Proyecto 4–** Control de acceso y responsabilidades de los usuarios a los sistemas y aplicaciones. Ver numeral 11.1

Tabla 35. (Continuación)

ACTIVOS	RIESGO	AMENAZAS	VALOR	TRATAMIENTO DE RIESGO	CONTROLES IMPLEMENTADOS	PROYECTOS DEFINIDOS
Servidor OAS – SICAPITAL	Pérdida de Autenticidad, en el comportamiento, resultado o uso del activo de información	[A.5] suplantación de la identidad del usuario	Medio	Se mitiga el riesgo con la implementación de los controles 9.1.1 - 9.1.2 – 9.2.1 - 9.2.2 - 9.2.3 - 9.2.4 - 9.2.5 - 9.2.6 - 9.3.1 - 9.4.1 - 9.4.2 - 9.4.3	Política de control de acceso. Acceso a redes y a Servicios de red. Registro y cancelación del registro de usuarios. Suministro de acceso de usuarios. Gestión de derechos de acceso privilegiado. Gestión de información de autenticación secreta de usuarios. Revisión de los derechos de acceso de usuarios. Retiro o ajuste de los derechos de usuario. Uso de información de información secreta para la autenticación. Restricción de acceso a la información.	**Proyecto 4-** Control de acceso y responsabilidades de los usuarios a los sistemas y aplicaciones. Ver numeral 11.

Fuente: el autor.

10.4 Plan Tratamiento de Riesgos: [AUX] ELEMENTOS AUXILIARES

Tabla 39. Plan de tratamiento de riesgos: elementos auxiliares

ACTIVOS	RIESGO	AMENAZAS	VALOR	TRATAMIENTO DE RIESGO	CONTROLES IMPLEMENTADOS	PROYECTOS DEFINIDOS
Sistema de aire acondicionado	Pérdida de Disponibilidad del activo de información	[N.*] Desastres naturales [I.5] Avería de origen físico o lógico	Alto	Se mitiga el riesgo con la implementación de los controles 11.1.1 - 11.1.2 - 11.1.3 - 11.1.4 - 11.1.5 - 11.2.2. - 12.2.1 - 16.1.2 - 17.1.1	Registros de actividad del administrador y operador de los sistemas. Respuesta a los incidentes de seguridad. Implantación de la continuidad de la seguridad de la información.	**Proyecto 2-** Responsabilidades y proyectos de operación. **Proyecto 3-** Implementación y seguimiento de registros de actividad. **Proyecto 4-** Control de acceso y responsabilidades de los usuarios a los sistemas y aplicaciones.
		[I.6] Corte del suministro eléctrico	Medio	Se mitiga el riesgo con la implementación de los controles 11.2.2 - 11.2.3 - 11.2.4	Cadena de suministro en tecnologías de la información y comunicaciones. Implantación de la continuidad de la seguridad de la información.	**Proyecto 5-** Adaptación plan de contingencia TICS, como marco de Gestión del Plan de Continuidad del Negocio. **Proyecto 7-** Gestión de incidentes de Seguridad de la Información

Fuente: el autor

10.5 Plan Tratamiento de Riesgos: [D] DATOS / INFORMACIÓN

Tabla 40. Plan de tratamiento de riesgos: datos / información

ACTIVOS	RIESGO	AMENAZAS	VALOR	TRATAMIENTO DE RIESGO	CONTROLES IMPLEMENTADOS	PROYECTOS DEFINIDOS
Documentación Técnica	Pérdida de Disponibilidad del activo de información	[N.2] Daños por agua [N.*] Desastres naturales [I.1] Fuego [I.7] Condiciones inadecuadas de temperatura o humedad [E.18] Destrucción de la información	Medio	Se mitiga el riesgo con la implementación de los controles 9..4.3 - 11.1.3 11.1.4 - 11.1.5 - 12.3.1 - 17.1.1 - 17.1.2	Uso aceptable de los activos. Clasificación de la información. Política de control de acceso. Acceso a redes y a Servicios de red. Gestión de derechos de acceso privilegiado. Respaldo de la información. Sistema de Gestión de contraseñas de usuarios. Planificación de la continuidad de la seguridad de la información. Protección contra las amenazas externas y ambientales. Implementación de la continuidad de la seguridad de la información.	**Proyecto 1-** Control de acceso físico y protección de la información (Áreas seguras y seguridad de equipos).Ver numeral 11.1 **Proyecto 2-** Control de acceso y responsabilidades de los usuarios a los sistemas y aplicaciones. Ver numeral 11.1 **Proyecto 5-** Adaptación plan de contingencia Tics, como marco de gestión del plan de continuidad del negocio. Ver numeral 11.1
	Pérdida de la Integridad de la información, lo que implica el acceso indebido o fraudulento al activo de información	[N.2] Daños por agua [N.*] Desastres naturales [I.1] Fuego [I.7] Condiciones inadecuadas de temperatura o humedad [E.18] Destrucción de la información	Medio	Se mitiga el riesgo con la implementación de los controles 9..4.3 - 11.1.3 11.1.4 - 11.1.5 - 12.3.1 - 17.1.1 - 17.1.2	Uso aceptable de los activos. Clasificación de la información. Política de control de acceso. Acceso a redes y a Servicios de red. Gestión de derechos de acceso privilegiado. Respaldo de la información. Sistema de Gestión de contraseñas de usuarios. Planificación de la continuidad de la seguridad de la información. Protección contra las amenazas externas y ambientales. Implementación de la continuidad de la seguridad de la información	**Proyecto 1-** Control de acceso físico y protección de la información (Áreas seguras y seguridad de equipos).Ver numeral 11.1 **Proyecto 2-** Control de acceso y responsabilidades de los usuarios a los sistemas y aplicaciones. Ver numeral 11.1 **Proyecto 5-** Adaptación plan de contingencia Tics, como marco de gestión del plan de continuidad del negocio. Ver numeral 11.1

Fuente: el autor

10.6 Plan Tratamiento de Riesgos: [P] PERSONAL

Tabla 41. Plan de tratamiento de riesgos: Personal

ACTIVOS	RIESGO	AMENAZAS	VALOR	TRATAMIENTO DE RIESGO	CONTROLES IMPLEMENTADOS	PROYECTOS DEFINIDOS
Administradores de Sistemas	Pérdida de Disponibilidad del activo de información	[E.28] Indisponibilidad del personal	Alto	Se mitiga el riesgo con la implementación de los controles 6.1.1 - 7.2.1 - 16.1.1	Roles y responsabilidades para la seguridad de la información. Responsabilidades de la dirección. Responsabilidades y procedimientos.	**Proyecto 6-** Seguimiento y cumplimiento de la Política de Seguridad de la información de la entidad. **Proyecto 7-** Gestión de incidentes de Seguridad de la Información. ver numeral 11.1
		[E.7] Deficiencias en la organización	Medio	Se mitiga el riesgo con la implementación de los controles 6.1.1 - 7.2.1 - 16.1.1	Roles y responsabilidades para la seguridad de la información. Responsabilidades de la dirección. Responsabilidades y procedimientos.	**Proyecto 6-** Seguimiento y cumplimiento de la Política de Seguridad de la información de la entidad. **Proyecto 7**- Gestión de incidentes de Seguridad de la Información. ver numeral 11.1

Fuente: el autor

11. SISTEMA DE CONTROL INTERNO INFORMÁTICO

Con el fin de asegurar la protección de todos los recursos informáticos de la entidad y en base a los resultados obtenidos en el análisis de riesgos, a continuación se plantean 7 proyectos para que sean implementados y/o acoplados a los procedimientos, normas y prácticas de la entidad, para controlar las actividades relacionadas a los sistemas de información del IDIPRON.

Tabla 42. Prioridad de Proyectos para la entidad

CARACTERÍSTICAS DE LOS PROYECTOS				MITIGACIÓN DE RIESGOS POR CONTROLES				
Nº	**Proyecto**	**Controles sobre las cuales aplica el proyecto**	**Prioridad del Proyecto**	**Disponibilidad**	**Integridad**	**Confidencialidad**	**Autenticidad**	**Trazabilidad**
1	Control de acceso físico y protección de la información (Áreas seguras y seguridad de equipos)	11.1.1	ALTA	X	X	X	X	X
		11.1.2						
		11.1.3						
		11.1.4						
		11.1.5						
		11.1.6						
		11.2.2						
		11.2.3						

Tabla 39. (Continuación)

CARACTERÍSTICAS DE LOS PROYECTOS				MITIGACIÓN DE RIESGOS POR CONTROLES				
Nº	**Proyecto**	**Controles sobre las cuales aplica el proyecto**	**Prioridad del Proyecto**	**Disponibilidad**	**Integridad**	**Confidencialidad**	**Autenticidad**	**Trazabilidad**
2	Responsabilidades y procedimientos de operación	12.1.1 12.1.2 12.1.3 12.1.4 12.2.1	ALTA	X	X	X	X	X
3	Implementación y seguimiento de registros de actividad	12.4.1 12.4.2 12.4.3 12.4.4 12.5.1 12.6.1 12.6.2 12.7.1	ALTA	X	X	X	X	X
4	Control de Acceso y responsabilidades de los usuarios a los sistemas y aplicaciones	9.1.1 9.1.2 9.2.1	ALTA	X	X	X	X	X

Tabla 39. (Continuación)

CARACTERÍSTICAS DE LOS PROYECTOS				MITIGACIÓN DE RIESGOS POR CONTROLES				
Nº	**Proyecto**	**Controles sobre las cuales aplica el proyecto**	**Prioridad del Proyecto**	**Disponibilidad**	**Integridad**	**Confidencialidad**	**Autenticidad**	**Trazabilidad**
4	Control de Acceso y responsabilidades de los usuarios a los sistemas y aplicaciones	9.2.2	ALTA	X	X	X	X	X
		9.2.3						
		9.2.4						
		9.2.5						
		9.2.6						
		9.3.1						
		9.4.1						
		9.4.2						
		9.4.3						
		9.4.4						
		9.4.5						
5	Adaptación Plan de Contingencia TICS, como marco de Gestión del Plan de Continuidad del Negocio.	17.1.1	ALTA	X	X	X	X	X
		17.1.2						
		17.1.3						
		17.2.1						
6	Seguimiento y cumplimiento de la Política de Seguridad de la Información de la entidad.	5.1.1	ALTA	X	X	X	X	X
		5.1.2						

Tabla 39. (Continuación)

CARACTERÍSTICAS DE LOS PROYECTOS				MITIGACIÓN DE RIESGOS POR CONTROLES				
Nº	**Proyecto**	**Controles sobre las cuales aplica el proyecto**	**Prioridad del Proyecto**	**Disponibilidad**	**Integridad**	**Confidencialidad**	**Autenticidad**	**Trazabilidad**
6	Seguimiento y cumplimiento de la Política de Seguridad de la Información de la entidad.	6.1.1	ALTA	X	X	X	X	X
		6.1.2						
		6.1.3						
		6.1.4						
		6.1.5						
		8.1.1						
		8.1.2						
		8.1.3						
		8.1.4						
		9.1.1						
		9.1.2						
		10.1.2						
7	Gestión de incidentes de Seguridad de la Información	16.1.1	ALTA	X	X	X	X	X
		16.1.2						
		16.1.3						
		16.1.4						
		16.1.5						
		16.1.6						
		16.1.7						

Fuente: el autor

11.1 DESCRIPCIÓN DE PROYECTOS

A continuación se describen cada uno de los proyectos, indicando el objetivo, justificación, actividades a realizar, área o cargo responsable de desarrollar la medida y los controles relacionados de acuerdo a la norma 27001. Estos proyectos se crean con el fin de mitigar los riesgos, tal como se indica en cada una de las acciones del Plan de tratamiento de riesgos del numeral 10.

Tabla 43. Proyecto: Control de acceso físico y protección de la información

<table>
<tr><td rowspan="2">Proyecto Número:

1</td><td>Nombre del Proyecto: Control de acceso físico y protección de la información (Áreas seguras y seguridad de equipos)</td></tr>
<tr><td>Área/Cargo Responsable de desarrollar la medida: Comité de sistemas de tecnologías y seguridad de la información</td></tr>
<tr><td colspan="2">Objetivo del Proyecto:

Establecer procedimientos seguros para evitar el acceso físico no autorizado a las oficinas y proteger la información del Instituto en cualquier forma que se halle ésta.

El procedimiento debe contener los siguientes aspectos:

- Definir los mecanismos de protección e identificación de las Áreas.

- Definir los mecanismos para el acceso de los funcionarios del Instituto.

- Definir los mecanismos para el acceso al personal externo de las Áreas.

- Definir actividades y controles para definir áreas seguras de trabajo.</td></tr>
<tr><td colspan="2">Justificación:

En la entidad no existen procedimientos ni protocolos documentados ni directrices clara para el acceso a los sitios de trabajo, tampoco está definido un plan para la protección de la información lo que hace vulnerable a la entidad del ataques de ingeniería social.</td></tr>
<tr><td colspan="2">ACTIVIDADES A REALIZAR</td></tr>
<tr><td colspan="2">- Definir las áreas de protección
De acuerdo a la criticidad de la sede se recomienda definir medidas y reglas específicas para el ingreso a las sedes de acuerdo a sus labores.

- Definir las áreas u oficinas de acceso restringido
Establecer las áreas de acceso restringido, teniendo en cuenta la criticidad de la información que se maneja en ella o que son estrategias en la entidad.

- Definir los mecanismo de protección
Definir los mecanismos o medios de protección para el ingreso a las instalaciones, como lo son sistema biométrico, tarjetas de proximidad, lector de metales, etc.</td></tr>
</table>

Tabla 40. (Continuación)

Proyecto Número: 1	**Nombre del Proyecto:** Control de acceso físico y protección de la información (Áreas seguras y seguridad de equipos)
	Área/Cargo Responsable de desarrollar la medida: Comité de sistemas de tecnologías y seguridad de la información
- Definir aspectos para el manejo y entrega de información a personal externo El ingreso de personal externo debe ser autorizado y acompañado por el responsable de la dependencia o área con el cual trabajará. Se deberán registrar la entrada y salida del funcionario mediante sistema de autenticación o bitácora; las visitas fuera de horario de servicio deberá ser autorizada por la autoridad competente al interior de la entidad o por el Jefe estratégico de dicha dependencia.	
Medidas relacionadas (Controles norma ISO 27001)	
11.1.1 - 11.1.2 - 11.1.3 - 11.1.4 - 11.1.5 - 11.1.6 - 11.2.2 - 11.2.3 (ver anexo 2).	

Fuente: el autor

Tabla 44. Proyecto: Responsabilidades y procedimientos de operación

Proyecto Número: 2	**Nombre del Proyecto:** Responsabilidades y procedimientos de operación
	Área/Cargo Responsable de desarrollar la medida: Proceso Gestión tecnológica y de la información
Objetivo del Proyecto: Definir y asegurar la adecuada operación de los sistemas y salvaguardar los registros de operación.	
Justificación: La entidad no cuenta con instructivos, procedimientos ni registros de operación que permitan identificar los eventos sobre los cambios realizados en la operación diaria de los sistemas, como lo son procedimientos de configuración, registros de auditoria, instalación y recuperación de los sistemas ante fallas.	
ACTIVIDADES A REALIZAR	
Realizar procedimientos para: - Encendido y apagado de equipos. - Procedimientos de reinicio seguro de equipos ante fallas. - Formatos y registros de rastros de auditoría. - Manuales para el desarrollo de seguimiento a logs.	
Medidas relacionadas (Controles norma ISO 27001)	
12.1.1 - 12.1.2 - 12.1.3 - 12.1.4 - 12.2.1 (ver anexo 2).	

Fuente: el autor

Tabla 45. Proyecto: Implementación y seguimiento de registros de actividad.

Proyecto Número: 3	**Nombre del Proyecto:** Implementación y seguimiento de registros de actividad
	Área/Cargo Responsable de desarrollar la medida: Proceso Gestión tecnológica y de la información
Objetivo del Proyecto: Desarrollar los instrumentos necesarios para realizar monitoreo y realizar los registros de cada una de las actividades realizadas por los usuarios, las fallas o eventos generados en la red.	
Justificación: Esta medida no se encuentra desarrollada en la entidad, actualmente el instituto no cuenta con mecanismos que le permita identificar las actividades realizadas en los sistemas o en la red, no cuenta con mecanismos que permitan identificar los log o registros de transacciones de usuarios o administradores de los sistemas, eventos o incidentes sobre vulnerabilidades técnicas existentes.	
ACTIVIDADES A REALIZAR	
- Crear procedimientos para la realización y conservación de registros de log. - Crear mecanismo que permitan registrar y obtener los eventos de las actividades de acceso o conexión a los sistemas informáticos. - Crear los mecanismos de conservación de los registros de eventos y monitoreo.	
Medidas relacionadas (Controles norma ISO 27001)	
12.4.1 - 12.4.2 - 12.4.3 - 12.4.4 - 12.5.1 - 12.6.1 - 12.6.2 - 12.7.1 (ver anexo 2).	

Fuente: el autor

Tabla 46. Proyecto: Control de Acceso y responsabilidades de los usuarios a los sistemas y aplicaciones.

Proyecto Número: 4	**Nombre del Proyecto:** Control de Acceso y responsabilidades de los usuarios a los sistemas y aplicaciones.
	Área/Cargo Responsable de desarrollar la medida: Proceso Gestión tecnológica y de la información.
Objetivo del Proyecto: Implementar las políticas para el control de acceso a usuarios y usuarios con privilegios especiales.	
Justificación: Aunque se ha realizado el inicio de operación de un procedimiento bajo el sistema de gestión de calidad de la entidad, se puede evidenciar un grado de madurez bajo para lo cual se debe divulgar, capacitar y dar cumplimiento por parte del Área técnica al procedimiento establecido y a generar la respectiva documentación del caso de manera sistemática.	
ACTIVIDADES A REALIZAR	

Tabla 43. (Continuación)

Proyecto Número: 4	**Nombre del Proyecto:** Control de Acceso y responsabilidades de los usuarios a los sistemas y aplicaciones.
	Área/Cargo Responsable de desarrollar la medida: Proceso Gestión tecnológica y de la información.
- Realizar proceso de inducción y reinducción sobre las actividades del procedimiento creado. - Generar la documentación respectiva donde se pueda evidenciar el seguimiento de altas y bajas en el registro de usuarios. - Realizar el inventario de los usuarios con acceso privilegiados. - Realizar y documentar los derechos de acceso a usuarios. - Revisar y definir la viabilidad de actualización de la política de seguridad de la información reforzando los procedimientos seguros de inicio de sesión, gestión y creación de contraseñas.	
Medidas relacionadas (Controles norma ISO 27001)	
9.1.1 - 9.1.2 - 9.2.1 - 9.2.2 - 9.2.3 - 9.2.4 - 9.2.5 - 9.2.6 - 9.3.1 - 9.4.1 - 9.4.2 - 9.4.3 - 9.4.4 - 9.4.5 (ver anexo 2).	

Fuente: el autor

Tabla 47. Proyecto: Adaptación Plan de Contingencia TICS, como marco de Gestión del Plan de Continuidad del Negocio.

Proyecto Número: 5	**Nombre del Proyecto:** Adaptación Plan de Contingencia TICS, como marco de Gestión del Plan de Continuidad del Negocio.
	Área/Cargo Responsable de desarrollar la medida: Área de Sistemas – Comité de sistemas de tecnologías y seguridad de la información
Objetivo del Proyecto: - Replantear la elaboración del Plan de continuidad del Negocio (Plan de Contingencia TICs). - Realizar o llevar a cabo pruebas de Continuidad del Negocio en forma periódica. - Desarrollar el mantenimiento del Plan de Recuperación de Desastres.	
Justificación: Aunque en la entidad existe un documento que trata sobre el Plan de Contingencia TICs, es necesario replantearlo y actualizarlo, ya que la infraestructura de la entidad se ha venido ampliando considerablemente y existen parámetros que necesitan de cambio. La implantación de este proyecto permitiría a la entidad garantizar la continuidad de la operación tanto tecnológica como de procesos.	

Tabla 44. (Continuación)

Proyecto Número: 5	**Nombre del Proyecto:** Adaptación Plan de Contingencia TICS, como marco de Gestión del Plan de Continuidad del Negocio.
	Área/Cargo Responsable de desarrollar la medida: Área de Sistemas – Comité de sistemas de tecnologías y seguridad de la información
ACTIVIDADES A REALIZAR	
- Actualizar el Plan de contingencia TICs. - Llevar a cabo revisiones constantes al Plan de continuidad del negocio. - Realizar pruebas al Plan de continuidad del Negocio y actualizar los puntos débiles encontrados durante esta etapa. - Sensibilización y socialización del Plan de Continuidad del Negocio. - Realizar pruebas periódicas al Plan de continuidad del Negocio que se implemente (simulaciones, pruebas de recuperación técnica, pruebas de recuperación en lugar alterno, pruebas de los recursos y servicios del proveedor). - Definición de los escenarios y supuestos. - Evaluación de posibles impactos a las operaciones de producción.	
Medidas relacionadas (Controles norma ISO 27001)	
17.1.1 – 17.1.2 – 17.1.3 – 17.2.1 (ver anexo 2).	

Fuente: el autor

Tabla 48. Proyecto: Seguimiento y cumplimiento de la Política de Seguridad de la Información de la entidad.

Proyecto Número: 6	**Nombre del Proyecto:** Seguimiento y cumplimiento de la Política de Seguridad de la Información de la entidad.
	Área/Cargo Responsable de desarrollar la medida: Área de Sistemas – Comité de sistemas de tecnologías y seguridad de la información.
Objetivo del Proyecto: - Hacer seguimiento constante de la Política de Seguridad de la Información de la entidad, con el fin de garantizar el cumplimiento de la misma. - Divulgar la Política de Seguridad de la Información de la entidad en forma periódica.	
Justificación: Aunque el IDIPRON cuenta con una Política de Seguridad de la Información documentada y aprobada, ésta se ha evidenciado que adolece de incumplimiento y/o desconocimiento por parte de los funcionarios de la entidad.	
ACTIVIDADES A REALIZAR	
- Llevar a cabo la socialización, comunicación y/o divulgación de la Política de Seguridad de la Información de manera constante o periódica. - Hacer cumplir la Política de Seguridad de la Información de la entidad sin ninguna salvedad. En caso que exista alguna novedad u objeción ésta debe ser evaluada por el comité de sistemas de tecnologías y seguridad de la información.	

Tabla 45. (Continuación)

Proyecto Número: 6	**Nombre del Proyecto:** Seguimiento y cumplimiento de la Política de Seguridad de la Información de la entidad.
	Área/Cargo Responsable de desarrollar la medida: Área de Sistemas – Comité de sistemas de tecnologías y seguridad de la información.
- Entendimiento de la Política de Seguridad. Se debe evaluar el entendimiento de la misma por parte del público objetivo. - Registrar la actividad de la comunicación a través de actas o informes técnicos. - La Política de Seguridad de la Información se debe revisar en forma periódica por el Comité de Seguridad de la Información, o cuando se produzcan cambios significativos, para garantizar que siga siendo, adecuada, suficiente y eficaz.	
Medidas relacionadas (Controles norma ISO 27001)	
5.1.1 – 5.1.2 – 6.1.1 -6.1.2 – 6.1.3 – 6.1.4 – 6.1.5 – 8.1.1 - 8.1.2 – 8.1.3 – 8.1.4 – 9.1.1 -9.1.2 – 10.1.2 (ver anexo 2).	

Fuente: el autor

Tabla 49. Proyecto: Gestión de incidentes de Seguridad de la Información

Proyecto Número: 7	**Nombre del Proyecto:** Gestión de incidentes de Seguridad de la Información.
	Área/Cargo Responsable de desarrollar la medida: Área de Sistemas – Comité de sistemas de tecnologías y seguridad de la información.
Objetivo del Proyecto: - Asegurar que se aplique una orientación consistente y eficaz para la gestión de los incidentes de seguridad de la información. - Establecer las responsabilidades y los procedimientos para manejar los eventos y debilidades de la seguridad de la información de manera eficaz una vez se hayan sido reportados. - Establecer un proceso de mejora continua a la respuesta para monitorear, evaluar y gestionar los incidentes de seguridad de la información. - Generar un reporte de los eventos y debilidades de la seguridad de la información.	
Justificación: Es importante establecer un marco de Gestión de incidentes en la entidad, ya que al haber obtenido en el Análisis de Riesgos, unos niveles altos en cuanto al Riesgo Potencial, se hace necesario desarrollar e implementar la medición del estado de la seguridad de la información. De igual manera esto le permitiría al área de sistemas evolucionar en temas de seguridad, ya que garantiza mediante el mejoramiento continuo, una adecuada protección a las vulnerabilidades y amenazas existentes.	
ACTIVIDADES A REALIZAR	
- Reporte de incidentes de seguridad. - Reporte de debilidades de seguridad.	

Tabla 46. (Continuación)

Proyecto Número: 7	**Nombre del Proyecto:** Gestión de incidentes de Seguridad de la Información.
	Área/Cargo Responsable de desarrollar la medida: Área de Sistemas – Comité de sistemas de tecnologías y seguridad de la información.
- Establecer un procedimiento formal en el IDIPRON para el reporte de eventos en la seguridad de la información, junto con un procedimiento de respuesta y de intensificación de incidentes, estableciendo las acciones más adecuadas que se deben tomar, en el momento que se reciba un evento en la seguridad de la información. - Establecer un sistema o punto de contacto para el reporte de eventos en la seguridad de la información, éste debe ser conocido por toda la entidad, que esté siempre disponible y que pueda proporcionar una respuesta adecuada y oportuna. - Reportar las debilidades en la seguridad, esta actividad debe estar a cargo por todos los funcionarios de la entidad. - Gestión de los incidentes de seguridad, es decir: responsabilidades y procedimientos, base de conocimiento sobre incidentes de seguridad y recolección de evidencias.	
Medidas relacionadas (Controles norma ISO 27001)	
16.1.1 – 16.1.2 – 16.1.3 – 16.1.4 – 16.1.5 – 16.1.6 – 16.1.7 (ver anexo 2)	

Fuente: el autor

12. PLAN DE DIVULGACIÓN

La divulgación de la Implementación del Sistema de Gestión de Seguridad de la Información se desarrolla inicialmente en el Comité de Seguridad de Tecnologías de la Información del instituto, dando a conocer el avance y el cumplimiento del mismo en el marco de la Norma Técnica Colombiana y el instrumento de valoración dispuesto por la Alta Consejería de las Tics.

En segundo lugar la divulgación se realiza mediante el portal institucional a través del sitio dispuesto en el Manual de Procesos y procedimientos donde se publica toda la información (manuales, instructivos, procedimientos y formatos) creados dentro del Proceso de Gestión tecnológica que es donde se desarrolla este proyecto, a su vez a través del correo electrónico a todos los funcionarios del Instituto.

Se realiza capacitación y divulgación a todos los funcionarios y contratistas en las jornadas de capacitación realizadas por el Área de Sistemas.

13. RESULTADOS E IMPACTOS

Aunque las Entidades Estatales reconocen que el desarrollo de este tipo de proyectos es de vital importancia para contar con un Sistema de Gestión que les permita tener definida una ruta para poder tener manejo y control de la información y darle un tratamiento adecuado a la misma, generalmente se evidencia falta de compromisos, conocimiento y ruptura de procesos en curso por parte de los funcionarios públicos tanto en el Área técnica como el Área administrativa y gerencial, para definir y establecer definiciones y controles.

Se ha dado cumplimiento a los objetivos propuestos teniendo en cuenta que se realizó el levantamiento de los activos de información, su valoración, clasificación y se realizó la valoración de los activos de información con los administradores de cada activo de información a través de entrevistas utilizando el programa PILAR de la Metodología MAGERIT V3.

Se realizó la declaración de aplicabilidad teniendo en cuenta el grado de cumplimiento de los controles de la norma NTC-ISO/IEC 27001:2013, en la entidad, documento que ha sido puesto en consideración del Comité de sistemas de tecnologías y seguridad de la información del IDIPRON.

En el desarrollo de estas actividades se propuso el plan de tratamiento de riesgos, teniendo en cuenta la valoración de los activos y los resultados generados en cuanto a disponibilidad, confidencialidad, integridad y autenticidad de los activos que generaron resultados con valor, medio alto y muy alto y considerando la línea a seguir en cuanto al plan de recuperación de desastres en lo concerniente a administrar o tercerizar servicios.

Como plan de acción es importante revisar continuamente los resultados obtenidos en este proyecto con la finalidad de concretar la continuidad de los servicios y el plan adecuado de recuperación de desastres.

14. CONCLUSIONES

- En la actualidad en el Instituto Distrital para la Protección de la Niñez y la Juventud – IDIPRON, existen medidas para proteger los activos de información de TI, sin embargo la mayoría deben ser fortalecidas, mejoradas y divulgadas de tal forma que se dé cumplimiento a los procesos de mejora continua y adaptación al cambio, esto teniendo en cuenta que la gestión pública está sometida a constantes cambios en los lineamientos estratégicos los cuales tienden a ser diferentes en cada periodo de administración, de ahí la importancia que un sistema de gestión de seguridad informática se adapte a los diferentes lineamientos sin alterar la esencia del mismo en cuanto a sus principios de seguridad informática.

- En el proceso de implementación del sistema se evidencia muchas oportunidades de mejora en cuanto a la aplicación de acciones efectivas que contribuyen en el mejoramiento del sistema y garantizarían un proceso de implantación exitoso y trazable en la entidad, por cual resulta de gran importancia para avanzar en la implementación de un Sistema Integrado de Seguridad de la Información que efectué un plan de trabajo, que integre todas las áreas y oficinas y permita la coordinación de los diferentes aspectos que involucra cada una ya que si bien es cierto que está implementado el sistema en la entidad se puede evidenciar que algunos de los procedimientos están desarticulados con los demás procesos entre ellos con el Proceso de Gestión Tecnológica y de la información quien lidera la Implementación del SGSI, dicha situación reduce efectividad en el Sistema puesto que la información de la entidad se genera y gestiona en cada uno de ellos por lo tanto garantizar la seguridad de la misma es más efectivo en la medida que se cubra el mayor porcentaje posible de la información de la entidad, ya que como se evidencio durante el desarrollo del presente proyecto realizar la implementación en un solo proceso hace que muchas variables no se controlen y de una u otra forma terminan afectando el la funcionalidad tanto del sistema como del proceso de seguridad informática.

- Por último es importante reconocer que en la actualidad la información de las organizaciones se constituye como uno de los activos más importantes de competitividad y empoderamiento la gestión de seguridad de la misma es tal vez uno de los retos a los que se enfrentan hoy en día, dado que controlar variables internas y externas en un sistema que requiere que cada día sea más dinámico capaz de responder a los constantes cambios, procesos de mejora continua, actualizaciones tecnológicas y sociales; exige que un proyecto de gestión de seguridad informática desde las etapas de formulación,

implementación e implantación se realicen procesos rigurosos de investigación, análisis y documentación que garantice que el Sistema Integrado de seguridad informática sea suficientemente completo de tal forma garantice el cumplimiento y total cobertura de los sistemas de información de toda organización e involucre el mayor número posible de agentes funcionales que intervienen en la gestión de la información, Sin embargo los procesos de implementación gradual para organizaciones pequeñas resultan ser una buena alternativa dado que en la media de su crecimiento el sistema se puede ir adaptando a las necesidades y así mismo las variables tecnológicas, funcionales, culturales, sociales, normativas con más fácil de control y cobertura.

- Para la entidad contar con un análisis y valoración de riesgos a los activos informáticos le permite obtener una visión general de lo que tiene como infraestructura tecnológica, diagnosticar necesidades y oportunidades de mejora y a su vez genera en los diferentes niveles de la planeación estratégica de la entidad una proceso de concientización y cultura de la importancia de la Seguridad de la Información y los impactos que esta tiene a nivel organizacional , así mismo conocer la estructura tecnología de la entidad facilita los procesos de toma de decisiones y posibles inversiones presupuestales en el área de tecnología e informática que fortalezcan la gestión y seguridad de la información en la entidad.

BIBLIOGRAFÍA

ALCALDÍA MAYOR DE BOGOTÁ. Norma Técnica Distrital del Sistema Integrado de gestión para las entidades y organismos distritales NTD-SIG 001:2011. Bogotá. 2012.

INSTITUTO COLOMBIANO DE NORMAS TÉCNICAS Y CERTIFICACIÓN, ICONTEC. Norma Técnica Colombiana para el Sistema de Gestión de Seguridad de la Información NTC-ISO/IEC 27001. Disponible en: http://www.bogotaturismo.gov.co/sites/intranet.bogotaturismo.gov.co/files/file/Norma.%20NTC-ISO-IEC%2027001.pdf

--------. Norma Colombiana Guía de implementación de un sistema de gestión de seguridad de la información. Bogotá D.C. ICONTEC, 2015. 81p. NTC-ISO/IEC 27003.

--------. Norma Colombiana Guía de implementación de un sistema de gestión de seguridad de la información. Bogotá D.C. ICONTEC, 2015. 107p. NTC-ISO/IEC 27002.

--------. Norma Colombiana para la Gestión del riesgo en la Seguridad de la Información. Bogotá D.C. ICONTEC, 2015. 67p. NTC-ISO/IEC 27005.

--------. Norma Colombiana para la presentación de tesis, trabajos de grado y otros trabajos de investigación. Sexta edición. Bogotá D.C.: ICONTEC, 2008. 36p. NTC-1486.

INSTITUTO Distrital para la Protección de la Niñez y la Juventud – IIDPRON. MISIÓN. Disponible en: http://www.idipron.gov.co/index.php/idipron/mision

MINISTERIO DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES. Decreto 2573 de 2014. Disponible en: http://wp.presidencia.gov.co/sitios/normativa/decretos/2014/Decretos2014/DECRETO%202573%20DEL%2012%20DE%20DICIEMBRE%20DE%202014.pdf

SECRETARÍA GENERAL ALCALDÍA MAYOR DE BOGOTÁ D.C. - COMISIÓN DISTRITAL DE SISTEMAS - CDS. Disponible en: http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=33486

UNIVERIDAD NACIONAL ABIERTA Y A DISTANCIA - UNAD. Capitulo 2 - Construcción del Anteproyecto de Grado. Disponible en: http://152.186.37.83/ecbti01/pluginfile.php/31026/mod_resource/content/1/Metodolog%C3%ADa.pdf

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA - UNAD. Lección 13 Fases para la implantación del SGSI. Disponible en: http://datateca.unad.edu.co/contenidos/233003/modulo/modulo-233003-online/51_leccin_21_fases_para_la_implantacin_del_sgsi.html

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA - UNAD. Guía de Actividades. Disponible en: http://152.186.37.83/ecbti01/mod/forum/view.php?id=15243

ANEXOS

Anexo 1. Formato RAE

Universidad Nacional Abierta y a Distancia	FORMATO
	RESUMEN ANALÍTICO EN EDUCACIÓN - RAE
Código:	**Versión: 01**
Fecha de Aprobación:	**Página 413 de 422**

1. Información General	
Tipo de documento	Tesis de Grado
Acceso al documento	Universidad Nacional Abierta y a Distancia - UNAD
Título del documento	Implementación del Sistema de Gestión de Seguridad de la Información – SGSI, en el proceso de apoyo “Gestión Tecnológica y de la Información” del Instituto Distrital para la Protección de la Niñez y la Juventud – IDIPRON
Autores	CELIS, Carlos; FRANCO, Oralia
Director	GONZALEZ, Salomón
Publicación	Bogotá. Universidad Nacional Abierta y a Distancia, 2016. P. 339.
Unidad Patrocinante	Instituto Distrital para la Protección de la Niñez y la Juventud - IDIPRON
Palabras Claves	Seguridad informática, Seguridad de la información, Inventario de activos, Valoración de riesgos, MAGERIT v3.0, Amenazas, NTC- ISO/IEC 27001.

2. Descripción
El trabajo de grado diseña e implementa el Sistema de Gestión de la Seguridad de la información- SGSI en el proceso de apoyo **“**Gestión Tecnológica y de la

Información" del Instituto Distrital para la Protección de la Niñez y la Juventud – Idipron, bajo la norma NTC- ISO/IEC 27001.

Este proyecto implementa en el proyecto de Gestión Tecnológica de la Información del Instituto, el Sistema de gestión de Seguridad de la Información con lo cual se pretende identificar y valorar los riesgos de activos de la información y definir un plan de tratamiento de riesgos que le permita a la entidad asegurar la disponibilidad, confidencialidad, integridad y no repudio de la información de la institución; así mismo se implementaran estrategias y definirán controles con el fin de proveer los recursos y procedimientos necesarios para minimizar el impacto ante posibles eventualidades.

3. Fuentes

INSTITUTO COLOMBIANO DE NORMAS TÉCNICAS Y CERTIFICACIÓN, ICONTEC. Norma Técnica Colombiana para el Sistema de Gestión de Seguridad de la Información NTC-ISO/IEC 27001. Disponible en: http://www.bogotaturismo.gov.co/sites/intranet.bogotaturismo.gov.co/files/file/Norma.%20NTC-ISO-IEC%2027001.pdf

--------. Norma Colombiana Guía de implementación de un sistema de gestión de seguridad de la información. Bogotá D.C. ICONTEC, 2015. 107p. NTC-ISO/IEC 27002.

--------. Norma Colombiana Guía de implementación de un sistema de gestión de seguridad de la información. Bogotá D.C. ICONTEC, 2015. 81p. NTC-ISO/IEC 27003.

--------. Norma Colombiana para la Gestión del riesgo en la Seguridad de la Información. Bogotá D.C. ICONTEC, 2015. 67p. NTC-ISO/IEC 27005.

MINISTERIO DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES. Decreto 2573 de 2014. Disponible en: http://wp.presidencia.gov.co/sitios/normativa/decretos/2014/Decretos2014/DECRETO%202573%20DEL%2012%20DE%20DICIEMBRE%20DE%202014.pdf

UNIVERIDAD NACIONAL ABIERTA Y A DISTANCIA - UNAD. Capitulo 2 - Construcción del Anteproyecto de Grado. Disponible en: http://152.186.37.83/ecbti01/pluginfile.php/31026/mod_resource/content/1/Metodolog%C3%ADa.pdf

4. Contenido

Mediante este proyecto se pretende implementar el Sistema de Gestión de Seguridad de la Información con el fin de garantizar la seguridad de la información y la preservación de los activos informáticos del IDIPRON.

El trabajo de grado consta de:

Objetivo general

Implementar el sistema de Gestión de Seguridad de la Información en el proceso de "Gestión Tecnológica y de la Información" en el Instituto Distrital para la Protección de la Niñez y la Juventud – IDIPRON, basados en la norma técnica colombiana GT-ISO/IEC 27003.

Objetivos específicos

- Realizar el levantamiento de los activos de información del proceso de Gestión Tecnológica y de la Información de la entidad.
- Definir la metodología de evaluación, identificación y análisis de riesgos.
- Evaluar, aplicar y documentar los controles de seguridad de la información con la norma NTC-ISO/IEC 27002.
- Definir el plan de tratamiento de riesgos y el sistema de control interno informático.

Marco Referencial: contiene el Marco de antecedentes, marco contextual, marco conceptual, marco teórico y marco legal relacionado con el desarrollo del proyecto.

Diseño Metodológico: En esta etapa se describe la metodología para investigación y la metodología de desarrollo del proyecto como es la identificación de la población, la muestra, el análisis, tipo y fuente de recolección de la misma, los instrumentos utilizados para realizar el análisis de los datos y la metodología a utilizar para el desarrollo de la investigación.

Recursos Requeridos

Cronograma de actividades

Análisis del Sistema de información de Seguridad de la Información. Descripción de análisis de riesgos, identificación de activos y valoración realizada de acuerdo a metodología utilizada.

Recomendaciones:

Concientizar a los administradores de los activos de información al igual que a la alta dirección de la importancia de desarrollar y mantener actualizado el Sistema de Gestión de Seguridad de la Información en los aspectos legales, técnicos y financieros.

Bibliografía e infografía

5. Metodología

Para el desarrollo del proyecto se utilizará la Metodología MAGERIT v.3, con el fin de realizar el análisis y valoración del riesgo; en concordancia con la norma técnica Colombiana NTC-ISO/IEC 27001:2013 utilizando el ciclo PHVA (Planear, hacer, verificar y actuar).

Fase 1 – Planeación
Fase 2 – Hacer.
Fase 3 –Verificar.
Fase 4 – Actuar.

De acuerdo al análisis y diseño detallado del SGSI en el IDIPRON a través de la muestra realizada de los activos de información del proceso de “Gestión Tecnológica y de la Información” del Instituto Distrital para la Protección de la Niñez y la Juventud y el tratamiento de la información de acuerdo a la recolección de la información, los instrumentos utilizados, el procesamiento y análisis de dicha información.

6. Conclusiones

Se realiza el diseño y la implementación del Sistema de Gestión de Seguridad de la Información en la entidad, de acuerdo a la norma Técnica Colombiana NTC ISO/IEC 27001:2013, la guía de implementación NTC-ISO/IEC 27002 y la Guia NTC-ISO/IEC 27003, dando cumplimiento a sus lineamientos.

Se realiza la identificación, valoración y analisis de riesgos de acuerdo a la Metodología MAGERIT v.3 lo que permite diagnosticar los activos criticos de la

Entidad, el impacto que puede generar la caida o vulneración de un activo y la definición del plan de tratamiento de riesgos.

El sistema desarrollado se ha implementado en el proceso de TI de la entidad, así mismo ha permitido crear procedimientos, establecer controles y diseñar el plan de tratamiento de riesgos, en la Entidad, permitiendo aumentar el nivel de cumplimiento del Sistema de Gestión de Seguridad de la Información exigido a la entidad por la Alta Consejería de las TICs.

7. Plan de Divulgación
La divulgación de la Implementación del Sistema de Gestión de Seguridad de la Información se desarrolla inicialmente en el Comité de Seguridad de Tecnologías de la Información del instituto, dando a conocer el avance y el cumplimiento del mismo en el marco de la Norma Técnica Colombiana y el instrumento de valoración dispuesto por la Alta Consejería de las Tics. En segundo lugar la divulgación se realiza mediante el portal institucional a través del sitio dispuesto en el Manual de Procesos y procedimientos donde se publica toda la información (manuales, instructivos, procedimientos y formatos) creados dentro del Proceso de Gestión tecnológica que es donde se desarrolla este proyecto, a su vez a través del correo electrónico a todos los funcionarios del Instituto. Se realiza capacitación y divulgación a todos los funcionarios y contratistas en las jornadas de capacitación realizadas por el Área de Sistemas.

Elaborado por:	Celis Carlos, Franco Oralia
Revisado por:	González García Salomón

Fecha de elaboración del Resumen:	14	05	2016

Anexo 2. Dominios, objetivos, referencias y títulos de los controles norma ISO 27001

Dominio de Control	Objetivo de Control	Referencia del control	Título del control
POLITICAS DE SEGURIDAD DE LA INFORMACION	Orientación de la Dirección para la gestión de la seguridad de la información.	5.1.1	Políticas para la seguridad de la Información
		5.1.2	Revisión de las políticas para la seguridad de la información
ORGANIZACION DE LA SEGURIDAD DE LA INFORMACION	Organización Interna	6.1.1	Roles y responsabilidades para la seguridad de la información
		6.1.2	Separación de deberes
		6.1.3	Contacto con las autoridades
		6.1.4	Contacto con los grupos de interés especial
		6.1.5	Seguridad de la información en la gestión de proyectos
	Dispositivos Móviles y de Teletrabajo	6.2.1	Política para dispositivos móviles
		6.2.2	Teletrabajo
SEGURIDAD DE LOS RECURSOS HUMANOS	Antes de asumir el empleo	7.1.1	Selección
		7.1.2	Términos y Condiciones del empleo
	Durante la ejecución del empleo	7.2.1	Responsabilidades de la dirección
		7.2.2	Toma de conciencia, educación y formación en la seguridad de la Información.
		7.2.3	Proceso disciplinario
	Terminación y cambio de empleo	7.3.1	Terminación o cambio de responsabilidades de empleo
GESTION DE ACTIVOS	Responsabilidad por los activos	8.1.1	Inventario de activos
		8.1.2	Propiedad de los Activos
		8.1.3	Uso aceptable de los activos
		8.1.4	Devolución de Activos
	Clasificación de la información	8.2.1	Clasificación de la información
		8.2.2	Etiquetado de la información
		8.2.3	Manejo de activos
	Manejo de medios	8.3.1	Gestión de medios removibles
		8.3.2	Disposición de los medios
		8.3.3	Transferencia de medios físicos

Anexo 2. (Continuación)

Dominio de Control	Objetivo de Control	Referencia del control	Título del control
CONTROL DE ACCESO	Requisitos del negocio para el control de acceso	9.1.1	Política de control de acceso
		9.1.2	Acceso redes y a Servicios de red
	Gestión de acceso de usuarios	9.2.1	Registro y cancelación del registro de usuarios
		9.2.2	Suministro de acceso de usuarios
		9.2.3	Gestión de derechos de acceso privilegiado
		9.2.4	Gestión de información de autenticación secreta de usuarios
		9.2.5	Revisión de los derechos de acceso de usuarios
		9.2.6	Retiro o ajuste de los derechos de usuario
	Responsabilidades del usuario	9.3.1	Uso de información de autenticación secreta
	Control de acceso a sistemas y aplicaciones	9.4.1	Restricción de acceso a la información
		9.4.2	Procedimiento de ingreso seguro
		9.4.3	Sistema de gestión de contraseñas
		9.4.4	Uso de programas utilitarios privilegiados
		9.4.5	Control de acceso a códigos fuente de programas
CRIPTOGRAFIA	Controles criptográficos	10.1.1	Política sobre el uso de controles criptográficos
		10.1.2	Gestión de llaves
SEGURIDAD FISICA Y DEL ENTORNO	Áreas seguras	11.1.1	Perímetro de seguridad física
		11.1.2	Controles de acceso físicos
		11.1.3	Seguridad de oficinas, recinto e instalaciones
		11.1.4	Protección contra amenazas externas y ambientales
		11.1.5	Trabajo en áreas seguras
		11.1.6	Áreas de despacho y carga
	Equipos	11.2.1	ubicación y protección de los equipos
		11.2.2	Servicios de suministro
		11.2.3	Seguridad del cableado
		11.2.4	Mantenimiento de equipos
		11.2.5	Retiro de activos

Anexo 2. (Continuación)

Dominio de Control	Objetivo de Control	Referencia del control	Título del control
SEGURIDAD FISICA Y DEL ENTORNO	Equipos	11.2.6	Seguridad de activos y equipos fuera de las instalaciones
		11.2.7	Disposición segura o reutilización de los equipos
		11.2.8	Equipos de usuario desatendido
		11.2.9	Política de escritorio limpio y pantalla limpia
SEGURIDAD DE LAS OPERACIONES	Procedimientos operacionales y responsabilidades	12.1.1	Procedimientos de operación documentados
		12.1.2	Gestión de cambios
		12.1.3	Gestión de capacidad
		12.1.4	Separación de los ambientes de desarrollo, prueba y operación
	Protección contra los códigos maliciosos	12.2.1	Controles contra códigos maliciosos
	Copias de respaldo	12.3.1	Respaldo de la información
	Registro y seguimiento	12.4.1	Registro de eventos
		12.4.2	Protección de la información de registro
		12.4.3	Registros del administrador y del operador
		12.4.4	Sincronización de relojes
	Control de software operacional	12.5.1	Instalación de software en sistemas operativos
	Gestión de la vulnerabilidad técnica	12.6.1	Gestión de las vulnerabilidades técnicas
		12.6.2	Restricciones sobre la instalación de software
	Consideraciones sobre auditorias de sistemas de información	12.7.1	Controles de auditorías de sistemas de información
SEGURIDAD DE LAS COMUNICACIONES	Gestión de la seguridad de las redes	13.1.1	Controles de redes
		13.1.2	Seguridad de los servicios de red
		13.1.3	Separación en las redes
	Transferencia de información	13.2.1	Políticas y procedimientos de transferencia de información
		13.2.2	Acuerdos sobre transferencia de información
		13.2.3	Mensajería electrónica
		13.2.4	Acuerdos de confidencialidad o de no divulgación

Anexo 2. (Continuación)

Dominio de Control	Objetivo de Control	Referencia del control	Título del control
ADQUISICION, DESARROLLO Y MANTENIMIENTO DE LOS SISTEMAS	Requisitos de seguridad de los sistemas de información	14.1.1	Análisis y especificación de los requisitos de seguridad de la información
		14.1.2	Seguridad de los servicios de las aplicaciones en redes publicas
		14.1.3	Protección de transacciones de los servicios de las aplicaciones
	Seguridad en los procesos de desarrollo y soporte	14.2.1	Política de desarrollo seguro
		14.2.2	Procedimientos de control de cambio de sistemas
		14.2.3	Revisión técnica de las aplicaciones después de cambios en la plataforma de operación.
		14.2.4	Restricciones en los cambios a los paquetes de software
		14.2.5	Principios de construcción de los sistemas seguros
		14.2.6	Ambiente de desarrollo seguro
		14.2.7	Desarrollo contratado externamente
		14.2.8	Pruebas de seguridad de sistemas
		14.2.9	Prueba de aceptación de sistemas
	Datos de prueba	14.3.1	Protección de los datos de prueba
RELACIONES CON LOS PROVEEDORES	Seguridad de la información en las relaciones con los proveedores	15.1.1	Política de seguridad de la información para las relaciones con proveedores
		15.1.2	Tratamiento de la seguridad dentro de los acuerdos con proveedores.
		15.1.3	Cadena de suministro de tecnología de información y comunicación
	Gestión de la prestación de servicios de proveedores	15.2.1	Seguimiento y revisión de los servicios de los proveedores
		15.2.2	Gestión de cambios en los servicios de los proveedores
GESTION DE INCIDENTES DE SEGURIDAD DE LA INFORMACION	Gestión de incidentes y mejoras en la seguridad de la información.	16.1.1	Responsabilidades y procedimientos
		16.1.2	Reporte de eventos de seguridad de la información
		16.1.3	Reporte de debilidades de seguridad de seguridad de la información

Anexo 2. (Continuación)

Dominio de Control	Objetivo de Control	Referencia del control	Título del control
GESTION DE INCIDENTES DE SEGURIDAD DE LA INFORMACION	Gestión de incidentes y mejoras en la seguridad de la información	16.1.4	Evaluación de eventos de seguridad de la información y decisiones sobre ellos
		16.1.5	Respuesta a incidentes de seguridad de la información
		16.1.6	Aprendizaje obtenido de los incidentes de seguridad de la información.
		16.1.7	Recolección de evidencia
ASPECTOS DE SEGURIDAD DE LA INFORMACION DE LA GESTION DE LA CONTINUIDAD DEL NEGOCIO	Continuidad de la seguridad de la información	17.1.1	Planificación de la continuidad de la seguridad de la información
		17.1.2	Implementación de la continuidad de la seguridad de la información
		17.1.3	Verificación, revisión y evaluación de la continuidad de la seguridad de la información
	Redundancias	17.2.1	Disponibilidad de las instalaciones de procesamiento de información.
CUMPLIMIENTO	Cumplimiento de los requisitos legales y contractuales	18.1.1	Identificación de la legislación aplicable y de los requisitos contractuales
		18.1.2	Derechos de propiedad intelectual
		18.1.3	Protección de registros
		18.1.4	Privacidad y protección de la información de datos personales
		18.1.5	Reglamentación de controles criptográficos
	Revisiones de seguridad de la información	18.2.1	Revisión independiente de la seguridad de la información
		18.2.2	Cumplimiento de las políticas y normas de seguridad
		18.2.3	Revisión del cumplimiento técnico