UNIVERSIDAD INTERNACIONAL DE LA RIOJA

Universidad Internacional de La Rioja
Máster Universitario en Seguridad Informática

Análisis del estado actual de la gestión de la seguridad de la información en la sede principal de Corporinoquia

Trabajo fin de máster presentado por: Jacksons Medina Romero

Director: Dr. Luis Enrique Sánchez Crespo

Ciudad: Yopal

Fecha: 14/09/2015

Firmado por:

DEDICATORIA Y AGRADECIMIENTOS

Quiero dar gracias a Dios y a la virgen santísima por regalarme tantas bendiciones, por brindarme su misericordia y perdón cada vez que la he necesitado, sin su luz difícilmente podría mantener mis sueños vivos para cumplirlos cada día. Gracias a mis hermanos y a la gente de mi gran Yopal, que están ahí para demostrarles con humildad que si se puede; a mi esposa que es mi mano derecha en todo lo que he emprendido, gracias mujer maravillosa por permitirme observar y disfrutar lo valiosa que eres; a mis padres que con su paciencia y forma de brindarme su amor y cariño me impulsan cada segundo para ser mejor y brindarles mi crecimiento, como resultado de su esfuerzo y dedicación por mantenerme con vida y enseñarme a sobrevivir de forma honrada, con trabajo, esfuerzo y disciplina. Gracias a todos estos seres maravillosos, espero poder cumplir en esta vida la tarea que Dios me ha encomendado en el libro de la vida.

TABLA DE CONTENIDO

INDICE DE TABLAS

INDICE DE ILUSTRACIONES

RESUMEN

En este documento se presenta un análisis de las diferentes herramientas de gestión de la seguridad de la información a nivel mundial y nacional y sobre todo se hace énfasis en la familia de la norma ISO 27000, realizando un estudio con la norma ISO 27001:2013. Con dicha norma se realiza una verificación del estado actual en materia de seguridad de la información en la Corporación Autónoma Regional de la Orinoquia, Corporinoquia, lo cual busca realizar y presentar un modelo de Política de Gestión de la Seguridad de la información, para esto se utilizará la metodología Magerit, con la cual se identificaran los activos de dicha organización, se revisara su importancia y la información básica de cada uno, seguidamente se identificaran las amenazas y los impactos a que están expuestos los activos, las salvaguardas para contra atacar estas amenazas, su grado de eficacia y efectividad en la protección de dichos activos y la identificación de los riesgos a que están expuestos los bienes Corporativos.

Por último, se presentara un modelo de política de seguridad de la información para la Corporinoquia, el cual busca reducir la materialización de vulnerabilidades a través de la implementación de controles en la administración de la información generada en Corporinoquia y su relación con el personal que hace uso de la misma, bien sea interno y externo.

PALABRAS CLAVE

Seguridad de la información, Política de Seguridad de la información, Riesgos, activos, salvaguardas, controles, gestión del riesgo, vulnerabilidades, metodologías, procedimientos de seguridad, valoración de los activos.

ABSTRACK

This document shows an analysis of the different management tools for information security at global and national levels making emphasis on the ISO 27000 family of standards, getting a focus on the study of ISO 27001: 2013. According to the terms of this standard an analysis of information security is performed for the Autonomous Regional Corporation of the Orinoco, Corporinoquia. This analysis aims to make and present a model which will be defined as an Information Security Policy Management. In order to achieve this policy, the Magerit methodology will be used, allowing us to identify their assets and property, their importance and the basic information about each one, also the threats and impacts that can affect every asset will be exposed as well the necessary safeguards that will strike back these threats, showing their efficiency and effectiveness protecting the assets while it´s possible to identify the risks to which the corporate assets are exposed.

Finally, a model of Information Security Policy will be presented for Corporinoquia, which pretends to reduce the vulnerabilities through the implementation of controls in the management of the information generated in Corporinoquia and its relationship with the staff that every day use it, either internal and external.

KEY WORDS

Information Security, Policy Information Security, Risk assets, safeguards, controls, risk management, vulnerabilities, methods, safety procedures, valuation of assets.

1 INTRODUCCIÓN

El desarrollo del presente trabajo busca identificar las potencialidades y aplicación de las normas internacionales de estandarización para el área de gestión de la seguridad de la información, como es el caso de las normas ISO 27000, en cada uno de sus componentes, los cuales servirán para dar a conocer su proceso de implementación, su forma de gestión, los elementos a tener en cuenta al momento de querer implementar la estandarización de controles de seguridad en la protección de información en las organizaciones.

En el proyecto se desarrollara un modelo de aplicación de gestión de la seguridad de la información, dicho modelo se validará con la gestión actual de la seguridad de la información de la Corporación Autónoma Regional de la Orinoquia, Corporinoquia, la cual es una organización Gubernamental, cuyo objeto es: “la ejecución de las políticas planes, programas y proyectos sobre medio ambiente y recursos naturales renovables, así como dar cumplida y oportuna aplicación a las disposiciones legales vigentes sobre su disposición, administración, manejo y aprovechamiento, conforme a las regulaciones, pautas y directrices expedidas por el Ministerio del Medio Ambiente” (CORPORINOQUIA, 2015).

El trabajo busca hacer un análisis del contexto a nivel nacional e internacional del uso, implementación y gestión de la seguridad de la información, identificando las potencialidades de la misma, experiencias exitosas y aplicarlas de forma aterrizada en un modelo de gestión de seguridad de la información, que permita adaptarlo y sacar unas conclusiones que brinden apoyo en la decisión de implementación de un sistema de gestión de la Seguridad en la entidad pública a analizar.

1.1 ANTECEDENTES

La seguridad de la información comprende dos campos muy importantes como es la seguridad de la información digital y la seguridad de la información física y toda esta se concentra en el nivel de importancia que tiene de acuerdo a la clasificación dada en cada una de las organizaciones donde se genera.

La seguridad de la información se empezó a gestionar desde la segunda guerra mundial y los orígenes de la norma ISO /IEC 27001, iniciaron en el año 1995, con el Código de Buenas prácticas BS 7799, seguidamente en el año 1998, apareció la BS 7799, en su segunda versión como Especificación de SGSI, para el año 1999 se hizo una revisión de las

versiones BS-7799-1, BS-7799-2, en el año 2000 se adopta la BS-7799-1 de 1999 como ISO/IEC 17799, en el año 2002 se hace la revisión de la versión BS-7799-2-2002, en junio de 2005 se hace una revisión de la norma ISO 17799:2005, en octubre de 2005 la versión BS7799-2:2002, se adopta como ISO/IEC 27001 y para el año 2013 se realiza la Revisión y aprobación de las normas ISO/IEC 27001:2013, ISO/IEC 27002:2013 y se aprueban el 25 de Septiembre de 2013 (ISO 27000.es, 2015).

Ilustración 1. Historia de la ISO 27001

Fuente: Adaptación de imagen de la web iso27000 - http://www.iso27000.es/iso27000.html

La norma ISO 27001[1] permite a las organizaciones certificarse. Esta norma, especifica los requisitos para la implantación de un Sistema de Gestión de la Seguridad de la Información – SGSI. Adopta un enfoque de gestión de riesgos y promueve la mejora continua de procesos a través de la estandarización y definición de parámetros o criterios que se deben tener en cuenta a la hora de mantener segura la información, generar controles estratégicos para salvaguardar cada uno de los activos identificados en la misma, gracias a la identificación clara de todos los riesgos posibles por los cuales tendría que enfrentar un activo de la organización a través de la valoración de los mismos y del impacto que llegase a tener en caso de materializarse (WIKIPEDIA, 2015).

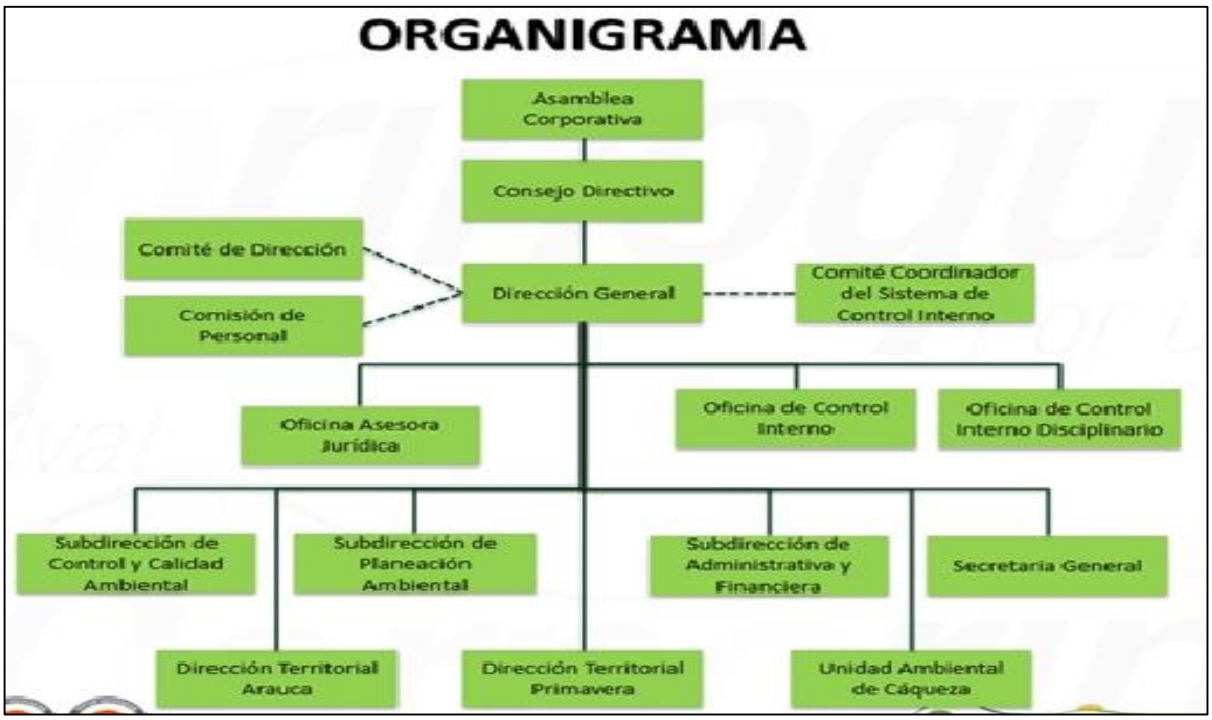
Para el desarrollo de este trabajo investigativo se trabajara con la organización pública Corporación Autónoma Regional de la Orinoquia, Corporinoquia cuya misión es:

[1] ISO 27001: Norma mediante el cual se obtiene certificación en seguridad de la información. https://es.wikipedia.org/wiki/ISO/IEC_27000-series

La corporación está conformada por cuatro sedes: sede principal en Yopal, Casanare, Dirección Territorial de Corporinoquia en Arauca, Arauca y la Primavera Vichada y la oficina ambiental en el municipio de Caqueza, Cundinamarca, en donde en cada sede se cuenta con conectividad y también con su infraestructura tecnológica. Por razones de alcance del proyecto se ha definido realizarlo en la sede principal de Corporinoquia en Yopal, Casanare, por lo que la temática del proyecto enfatizara en dicha sede (CORPORINOQUIA, 2015).

A continuación se muestra la estructura organizacional de Corporinoquia, la cual se plasma en su organigrama.

Ilustración 2. Organigrama de Corporinoquia



Fuente: Organigrama de Corporinoquia, tomado de http://l.corporinoquia.gov.co/index.php/inicio/corporinoquia

Cada una de las áreas de la corporación, es generadora de información, la cual está codificada a través de las Tablas de Retención Documental – TRD, y su estructura se realiza con base al organigrama corporativo y estas son aprobadas por el Archivo General de la Nación de Colombia, previo cumplimiento de los parámetros de evaluación definidos en la

Ley 594 de 2000[2], y el Acuerdo No. 005 del 15 de marzo de 2013[3] del Gobierno Nacional (ARCHIVO GENERAL DE LA NACION, 2015).

Corporinoquia dentro de su organigrama cuenta con la oficina de sistemas, la cual está bajo el direccionamiento estratégico de la Subdirección de Planeación Ambiental, y desde allí se lidera todo lo relacionado con la gestión tecnológica, la cual se enmarca dentro del Plan de Acción Trianual 2012-2015 "Por una Región Viva", en el eje "Fortalecimiento Institucional", proyecto "Herramientas Tecnológicas para la eficiencia", la cual establece unas metas de cumplimiento, que buscan renovar y actualizar la infraestructura tecnológica en cuanto a hardware y software, adelantos que ya se han realizado en la presente administración de la misma.

Para el caso de la gestión de la seguridad de la información en la Corporación autónoma regional de la Orinoquia, Corporinoquia, no se ha implementado el proceso de certificación en ISO 27001, pero ya se encuentra con certificación de proceso de la ISO 9001, la cual está para renovación en el presente año 2015, y se está adelantando el proceso de gestión de la certificación en la ISO 14000, sin embargo a través de la oficina de sistemas de Corporinoquia, se han venido adelantando las gestiones necesarias para protección de la información digital a través de implementación de mecanismos básicos de seguridad como es el acceso a la red de datos e información compartida a través de Directorio Activo, con la asignación de usuario y contraseña, utilizando este a través de un proceso de autenticación de usuarios, donde a través de este se accede a los recursos compartidos en red para el desarrollo de las actividades de gestión de información y autorización de permisos de usuarios.

De acuerdo a lo anteriormente expuesto, se evidencia que Corporinoquia no cuenta con la definición de políticas adecuadas en cuanto a seguridad de la información se refiere, ni procedimientos establecidos que se enmarquen dentro del contexto del tratamiento del riesgo de los activos, y los controles con que cuenta para proteger la información son muy básicos, debido a que se están enfocando a actividades básicas que realiza un usuario en un activo, como por ejemplo publicar o no publicar un artículo en el sitio web, pero lo

[2] Ley 594 de 2000 del Gobierno Nacional, "Por medio de la cual se dicta la Ley General de Archivos y se dictan otras disposiciones" (ARCHIVO GENERAL DE LA NACION, 2015).
[3] Acuerdo No. 005 del 15 de marzo de 2013, del Archivo General de la Nación, "Por medio del cual se establecen los criterios básicos para la clasificación, ordenación y descripción de los archivos en las entidades públicas y privadas que cumplen con funciones públicas, y se dictan otras disposiciones" (ARCHIVO GENERAL DE LA NACION_AGN, 2015).

importante como es protección de la información, no se tiene contemplado de forma rigurosa.

Como resultado de visitas de inspección, se identificó que Corporinoquia no cuenta con un Sistema de Gestión de Seguridad de la Información, SGSI, implementado, ni se han tenido en cuenta los controles de la norma ISO/IEC 27002:2013, dentro del sistema de Gestión de Calidad ISO 9001, cuentan con el proceso TIC, en donde se gestionan algunos riesgos muy alejados a la realidad de lo que podría llegar a ocurrir o de la forma como deberían estar siendo tratados. La gestión informática en Corporinoquia ha estado enfocada a la adquisición y actualización de infraestructura tecnológica como equipos de cómputo, licencias de software y adquisición del nuevo servidor, con el cual se ha mejorado la gestión de la información, así como mejorar las comunicaciones internas de datos con la adquisición de switch de velocidades de 1 gigabits por segundo, sin embargo, la seguridad de la información no se gestiona con estándares ISO/IEC 27001:2013 y ya se han presentado perdidas de información en años anteriores.

Con lo anterior se evidencia la necesidad de hacer un análisis de la situación actual o estado del arte el cual servirá de herramienta para proponer un modelo de aplicación de la norma ISO/IEC 27001:2013.

1.2 PLANTEAMIENTO DEL TRABAJO

El presente proyecto que se desarrollara, pertenece a un proyecto piloto experimental por que busca efectuar un proceso investigativo acerca de la aplicación de la norma ISO/IEC 27001:2013, con la cual se realizará un análisis de la situación actual o el estado del arte de la aplicación de la gestión de la seguridad de la información en Colombia, se desarrollará un modelo de aplicación de la gestión de la seguridad de la información y se validará su viabilidad para una futura implementación en la Corporación Autónoma Regional de la Orinoquia, Corporinoquia.

Con el fin de garantizar el cumplimiento de un proceso de gestión de seguridad de la información y la aplicación de la norma ISO/IEC 27001:2013, el proceso se enmarca dentro del ciclo PHVA, el cual consiste en llevar a cabo la ejecución de las fases de Planificación (P), fase de ejecución (H), fase de Seguimiento (V) y fase de Mejora (A), para lo cual es importante definir un alcance, una política de seguridad, organización de la seguridad y definir la concienciación y formación del personal (WIKIPEDIA, 2015).

El modelo a desarrollar de gestión de seguridad de la información, estará enfocado a los procesos de Planeación de la Gestión Ambiental, Gestión de Trámites y Servicios Ambientales, Gestión de Archivo y Correspondencia y Gestión TICS, como procesos críticos y de gran importancia por el cumulo de información que se genera y adicionalmente, por la importancia de administración de la misma y la gestión del riesgo a que se encuentra expuesta.

Se tendrán en cuenta las áreas físicas de la Subdirección de Planeación Ambiental, Secretaria General, Control y Calidad Ambiental, Oficina de Sistemas y Dirección General. No se tendrá en cuenta la oficina jurídica, ni la Subdirección Administrativa y Financiera.

Para esta actividad, se destina un profesional especializado para la gestión de la seguridad de la información, quien es el desarrollador del presente proyecto, quien se encargara de la elaboración del modelo a desarrollar de ISO/IEC 27001:2013.

1.3 ESTRUCTURA DEL TRABAJO

Una vez realizada la parte introductoria del presente proyecto se describe cada uno de los capítulos que se desarrollaran, de forma breve y resumida, lo cual, facilitará al lector la identificación de la temática a tratar:

En el capítulo 2, se describirá los objetivos y metodología del trabajo a realizar.

En el capítulo 3, se realizará un despliegue de información de las normas más importantes en materia de estandarización y sistemas de gestión de seguridad de la información a nivel mundial, los adelantos que en materia de seguridad de la información se han llevado a cabo en Colombia, la normatividad que la regula y a nivel regional, se presentara una síntesis de los avances en seguridad de la información de la Corporación Autónoma Regional de la Orinoquia, Corporinoquia, como entidad pública de estudio del presente proyecto .

En el capítulo 4, Se realizara un análisis de riesgos, a través de la identificación de activos más importantes relacionados con la seguridad de la información de Corporinoquia, las amenazas, a las cuales se les realizara su valoración, la identificación de salvaguardas y por último la estimación del riesgo, sus impactos y la valoración de las salvaguardas.

En el capítulo 5, se realizará un modelo de política de gestión de la seguridad de la información para Corporinoquia.

En el Capítulo 6, se presentaran las conclusiones del presente proyecto.

2 OBJETIVOS Y METODOLOGÌA DEL TRABAJO

2.1 OBJETIVO GENERAL

Realizar un análisis del estado actual de la gestión de la seguridad de la información en la sede principal de Corporinoquia, a través del planteamiento de una Política de Gestión de la Seguridad de la Información, tomando como guía la norma ISO 27001:2013.

2.2 OBJETIVOS ESPECIFICOS

Realizar un análisis del estado del arte de la normatividad vigente a nivel Internacional y nacional de seguridad informática, así como identificar el estado actual en cuanto a la gestión de la Seguridad de la información en Corporinoquia, tomando como base el anexo A – Objetivos de control y controles de referencia de la ISO 27001:2013.

Identificar los activos más importantes con que cuenta la organización, relacionados con el uso y acceso a la información física y digital.

Identificar los riesgos a que están expuestos los activos de la organización y definir controles que reduzcan la materialización de los mismos.

Proponer un modelo de política de Gestión de Seguridad de la información como mecanismos de protección de la información de la sede principal de la Corporación Autónoma Regional de la Orinoquia, Corporinoquia.

2.3 METODOLOGIA DEL TRABAJO

La metodología a seguir dentro de la gestión del presente proyecto está basado en la exploración de la gestión de la Seguridad de la Información con la familia de las ISO/IEC 27001, en la Corporación Autónoma Regional de la Orinoquia, Corporinoquia, entidad pública del Gobierno Nacional, en donde no se ha iniciado el proceso de seguridad de la información, gestionado a través de las normas ISO, ni ninguna otra norma de estandarización que permita minimizar los riesgos de perdida de información. Adicionalmente, la temática a tratar es nueva, debido a que no se había tenido la oportunidad de profundizar sobre el tema por parte del desarrollador del proyecto.

Por lo anterior, se busca realizar un estado del arte de las normas ISO 27000, para conocer su estructura, como está conformada, como se complementan, los beneficios de certificarse en ISO/IEC 27001:2013, que compromisos y responsabilidades se adquieren al asumir este reto, entre otros.

Una vez identificada la información necesaria se procederá a realizar el modelo de aplicación del sistema de gestión de seguridad de la información y se realizará la validación con la gestión de la seguridad de la información actual de Corporinoquia.

Finalmente, se presentaran las conclusiones del resultado del trabajo desarrollado. Todo esto será el componente y gestión del proyecto a entregar.

3 CONTEXTO Y ESTADO DEL ARTE

3.1 NORMAS Y ESTANDARES DE GESTIÒN DE LA SEGURIDAD DE LA INFORMACIÒN A NIVEL INTERNACIONAL

La gestión de la seguridad de la información, nació por la necesidad de protección de la información que se generaba en algunos estados, empresas o personas, debido a que no la debían conocer otras personas, ni debía ser difundida, alterada o destruida sin permiso alguno, de allí nace el concepto de confidencialidad, integridad y disponibilidad de la información. También tuvo sus orígenes en la segunda guerra mundial, con la necesidad de transmisión de mensajes seguros entre los ejércitos alemanes y con la creación de la

maquina descifradora de mensajes enigma que facilito la caída del imperio nazi en conjunto con las tropas aliadas contra Alemania.

Adicionalmente, la gestión de la seguridad de la información ha venido sufriendo transformaciones y adelantos hasta lograr la actual familia ISO 27000, donde a través del cumplimiento de la ISO 27001:2013, las organizaciones logran su proceso de certificación en seguridad de la información.

Otras importantes normas, modelos de madurez y entidades que brindan certificación profesional acerca de la gestión en seguridad de la información son:

3.1.1 El Consorcio internacional de Certificación de Seguridad de Sistemas de Información o (ISC)2

(International Information Systems Security Certification Consortium – ISC2[4]), fundado en 1989, es una organización sin ánimo de lucro con sede en Florida, dedicada fundamentalmente a la formación y certificación en seguridad de la información (WIKIPEDIA_ISC2, 2015).

Para lograr las certificaciones (ISC)2 incluyen:

La más conocida y extendida de todas ellas, Certified Information Systems Security Professional (CISSP), que es una certificación profesional generalista que incluye:

- Information Systems Security Architecture Professional (CISSP-ISSAP)
- Information Systems Security Engineering Professional (CISSP-ISSEP)
- Information Systems Security Management Professional (CISSP-ISSMP)
- Certified Secure Software Lifecycle Professional (CSSLP)
- Certification and Accreditation Professional (CAP)
- Systems Security Certified Practitioner (SSCP) (WIKIPEDIA_ISC2, 2015).

[4] ISC: International Información Systems Security Certification Consortium (WIKIPEDIA_ISC2, 2015). Tomado de https://es.wikipedia.org/wiki/ISC2

3.1.2 El modelo O-ISM3

Es un estándar para la creación de sistemas de gestión de la seguridad de la información que se alinea a la misión empresarial. Pretende alcanzar un nivel de seguridad definido, conocido como el riesgo aceptable, puede usarse por sí solo o para mejorar sistemas basados en ITIL, ISO27001 o Cobit, su objetivo en cuanto a la seguridad es garantizar la continuidad de los objetivos de negocio (SLIDESHARE, 2015). Los objetivos de seguridad como control de accesos a usuarios, están relacionados directamente a los objetivos misionales del negocio, todo está ligado, para que se den los niveles de seguridad, si uno falla el otro también, por lo tanto el proceso debe ser complementario.

El modelo O-ISM3, hace de la seguridad de la información un proceso medible, trazable, mediante métricas de gestión de procesos, lo que permite la mejora del proceso, a través de criterios que miden la eficacia y la eficiencia de los sistemas de gestión de la seguridad (SLIDESHARE, 2015). El modelo se basa en tres elementos de la gestión de la seguridad como es: gestión de los riesgos, controles de seguridad y gestión de la seguridad mediante un sistema de políticas y herramientas que las implantan. Dicho estándar se basa en procesos, capacidad y madurez (SLIDESHARE, 2015).

O-ISM3 cuenta con cinco niveles de madurez, los cuales se adaptan a los objetivos de la seguridad de la organización y a los recursos que están disponibles, por lo tanto, se adapta a organizaciones grandes, medianas y pequeñas. Su desarrollo está basado en procesos, adoptando las mejores prácticas a través de la distribución explicita de las responsabilidades entre líderes, gestores y personal técnico, bajo el concepto de gestión estratégica, tatica y operativa. Su proceso de certificación se puede realizar bajo la norma ISO 9001 o ISO 27001 (SLIDESHARE, 2015).

3.1.3 Cobit

Como lo indica la sigla Cobit en ingles Control Objectives for Information and Related Technology, es un conjunto de buenas prácticas para el manejo de información creado por la Asociación para la Auditoría y Control de Sistemas de Información (ISACA), y el Instituto de Administración de las Tecnologías de la Información (ITGI) en 1992 (SEGURIDADINFORMACIONCOLOMBIA, 2015).

Cobit es un marco de referencia para la dirección de IT, así como también de herramientas de soporte que permite a la alta dirección reducir la brecha entre las necesidades de control, cuestiones técnicas y los riesgos del negocio. Cobit permite el desarrollo de políticas claras y buenas prácticas para el control de TI en las organizaciones. Cobit enfatiza el cumplimiento normativo, ayuda a las organizaciones a aumentar el valor obtenido de TI, facilita su alineación y simplifica la implementación del marco de referencia de Cobit (SEGURIDADINFORMACIONCOLOMBIA, 2015).

Cobit, brinda a la alta dirección de las organizaciones, confianza en los sistemas de información y en la información que estos generan; permite entender como dirigir, gestionar y administrar el uso de los sistemas, estableciendo un código de buenas prácticas a ser utilizado por los proveedores de sistemas. Así mismo, Cobit facilita las herramientas para supervisar todas las actividades relacionadas con IT (WIKIPEDIA_COBIT, 2015).

Ventajas y Características de Cobit (SEGURIDADINFORMACIONCOLOMBIA, 2015):

- Cobit es un marco de referencia aceptado mundialmente de gobierno IT basado en estándares y mejores prácticas de la industria. Una vez implementado, es posible asegurarse de que IT se encuentra efectivamente alineado con las metas del negocio, y orientar su uso para obtener ventajas competitivas (SEGURIDADINFORMACIONCOLOMBIA, 2015).
- Proporciona las mejores prácticas y herramientas para monitorear y gestionar las actividades de IT. El uso de sistemas usualmente requiere de una inversión que necesita ser adecuadamente gestionada (SEGURIDADINFORMACIONCOLOMBIA, 2015).
- Cobit permite el desarrollo de políticas claras y buenas prácticas para la gestión de IT. Su marco de referencia permite gestionar los riesgos de IT y asegurar el cumplimiento, la continuidad, seguridad y privacidad (SEGURIDADINFORMACIONCOLOMBIA, 2015). Está alineado con estándares de control y auditoria (COSO, IFAC, IIA, ISACA, AICPA).
- Ayuda a los ejecutivos a entender y gestionar las inversiones en IT a través de sus ciclo de vida, así como también proporcionándoles métodos para asegurarse que IT entregara los beneficios esperados. Entendimiento compartido entre todos los interesados basados en un lenguaje común (SEGURIDADINFORMACIONCOLOMBIA, 2015).
- Suministra un lenguaje común que permite a los ejecutivos de negocios comunicar sus metas, objetivos y resultados con Auditores, IT y otros profesionales. Visión

comprensible de TI para su administración. Proporciona una clara definición de propiedad y responsabilidad (SEGURIDADINFORMACIONCOLOMBIA, 2015).

La adecuada implementación de un modelo COBIT en una organización, provee una herramienta automatizada, para evaluar de manera ágil y consistente el cumplimiento de los objetivos de control y controles detallados, que aseguran que los procesos y recursos de información y tecnología contribuyen al logro de los objetivos del negocio en un mercado cada vez más exigente, complejo y diversificado (SLIDESHARE, 2015).

El marco de referencia de Cobit propone un rango de acción donde se evalúan los criterios de información como son la seguridad y la calidad de la misma, se auditan los recursos que integran la tecnología de la información, como el recurso humano, sistemas e instalaciones, entre otras, así como la evaluación de los procesos involucrados en la organización.

El modelo Cobit implementado en una organización provee una herramienta automatizada, que evalúa de forma ágil el cumplimiento de los objetivos de control y controles detallados que aseguran que los procesos y recursos de información y tecnología, contribuyan al logro de los objetivos del negocio de las organizaciones (MONOGRAFIAS_COBIT, 2015).

Cobit se enmarca en cuatro grandes dominios, que son:

Planificación y Organización: cubre la estrategia y las tácticas y se refiere a la identificación de la forma como la tecnologías de la información pueden contribuir al logro de los objetivos del negocio. Permite planificar, comunicar y administrar la gestión de la visión estratégica de la organización, esto permitirá establecer una infraestructura tecnológica apropiada en la empresa u organización.

En este dominio están presentes los siguientes procesos:

PO1 Definir el plan estratégico de TI.
PO2 Definir la arquitectura de la información
PO3 Determinar la dirección tecnológica.
PO4 Definir procesos, organización y relaciones de TI.
PO5 Administrar la inversión en TI.
PO6 Comunicar las aspiraciones y la dirección de la gerencia.
PO7 Administrar recursos humanos de TI.

PO8 Administrar calidad.
PO9 Evaluar y administrar riesgos de TI
PO10 Administrar proyectos.
PO11Administración de Calidad (DAMETAREAS, 2015)

Adquisición e Implantación: Para llevar a cabo la estrategia de TI, es necesario hacer un diagnóstico, identificar las necesidades e identificar las soluciones, para el proceso de adquisición e implementación de las mismas e integrarlas al proceso de negocio.

En este dominio están presentes los siguientes procesos:

AI1 Identificar soluciones automatizadas.
AI2 Adquirir y mantener el software aplicativo.
AI3 Adquirir y mantener la infraestructura tecnológica
AI4 Facilitar la operación y el uso.
AI5 Adquirir recursos de TI.
AI6 Administrar cambios (SLIDESHARE, 2015).

Soporte y Servicios: abarca desde las operaciones tradicionales hasta el entrenamiento, la seguridad y continuidad del negocio. Se debe establecer el proceso de soporte. También se realiza la actividad de procesamiento de los datos por sistema de aplicación, clasificados como controles de aplicación.

En este dominio están presentes los siguientes procesos:

DS1 Definir y administrar niveles de servicio.
DS2 Administrar servicios de terceros.
DS3 Administrar desempeño y capacidad.
DS4 Garantizar la continuidad del servicio.
DS5 Garantizar la seguridad de los sistemas.
DS6 Identificar y asignar costos.
DS7 Educar y entrenar a los usuarios.
DS8 Administrar la mesa de servicio y los incidentes.
DS9 Administrar la configuración.
DS10 Administrar los problemas.
DS11 Administrar los datos.

DS12 Administrar el ambiente físico.
DS13 Administrar las operaciones (BIBLIOTECA DIGITAL ICESI, 2015).

Monitoreo: Los procesos es necesario tenerlos controlados mediante monitoreo para evaluar su eficacia y efectividad. Estos dominios y objetivos de control facilitan que el procesamiento de la información cumpla con las características de efectividad, eficiencia, confidencialidad, integridad, disponibilidad, cumplimiento confiabilidad.

COBIT es un marco general, su flexibilidad permite adaptarlo a cualquier tipo y tamaño de empresa, realizando una implementación gradual y progresiva acorde a los recursos disponibles y alineados a la estrategia empresarial (AUDITORIADESISTEMASADRIMELI, 2015).

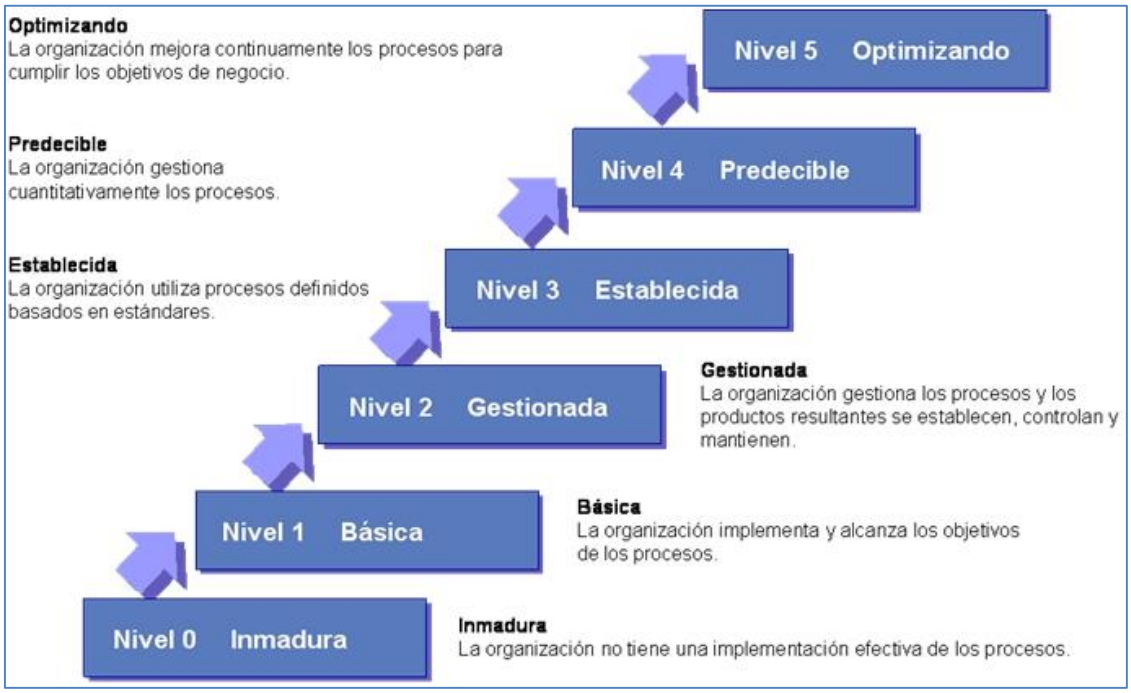
3.1.4 Capability Maturity Model Integration (CMMI[5])

Integración de Modelos de madurez de capacidades, es un modelo para la mejora y evaluación de procesos para el desarrollo, mantenimiento y operación de sistemas de software. CMMI proporciona un conjunto de prácticas para la mejora de los procesos, también tiene practicas integradas que ayudan a mejorar el modo de usar cualquier enfoque de mejora del rendimiento. CMMI está diseñado para comparar los procesos existentes de una organización a las mejores prácticas probadas desarrolladas por miembros de la industria, el gobierno y el mundo. El resultado de CMMI ayuda a construir y gestionar sistemas de mejora de rendimiento que se adapta al entorno único de la organización. Su primera versión fue publicada en 1991.

CMMi cuenta con 25 áreas de proceso, que son un conjunto de prácticas que se deben realizar en forma colectiva con el objetivo de lograr una cierta meta, y que están agrupadas en 4 niveles de madurez. El primero (Nivel 2), cuenta con 7 áreas de proceso, el Nivel 3 con 14 adicionales, el Nivel 4 con 2 adicionales y finalmente el Nivel 5 con 2 más (CMMIINSTITUTE, 2015).

[5] CMMI: Integración de Modelos de madurez de capacidades, tomado de http://cmmiinstitute.com/get-started, (CMMIINSTITUTE, 2015).

Ilustración 3. Niveles de Madurez CMMI



Fuente: Tomado de http://www2.tecnova.cl/servicios/descripcion_cmmi.html, (TECNOVA-CMMI, 2015)

Uno de los métodos que usan los organismos acreditadores para evaluar si una organización cumple con el modelo CMMi, es el SCAMPI (Standard CMMI Appraisal Method for Process Improvement), que es el método oficial que utiliza el SEI (Software Engineering Institute). Una evaluación SCAMPI se usa para identificar fortalezas, debilidades y riesgos de los procesos, para determinar finalmente el nivel de madurez de los procesos de la organización (TECNOVA-CMMI, 2015).

Los niveles de madurez de CMMI se describen a continuación:

Nivel 0 (Inmaduro)

La organización no tiene una implementación efectiva de los procesos.

Nivel 1: Inicial o Básico:

El proceso se ejecuta y se producen productos basados en productos de entrada identificados. En este nivel se encuentran las empresas que no tienen procesos documentados: es donde el proceso se ejecuta y se logra su objetivo, así sea fuera de presupuesto y de cronograma.

En este nivel de madurez, el desarrollo del proyecto es totalmente opaco, no se sabe lo que pasa en él.

Nivel 2: Administrado ò Gestionado

El proceso es reactivo y se caracteriza por su aplicación a proyectos. La principal diferencia entre este nivel y el anterior es que el proyecto es gestionado y controlado durante el desarrollo del mismo, se decir: además de ejecutarse, el proceso se planifica, se revisa y se evalúa para comprobar que cumple los requisitos. El desarrollo no es opaco y se puede saber el estado del proyecto en todo momento (TARINGA, 2015).

Nivel 3: Definido ò establecido

El proceso es proactivo y se ve a nivel de la organización. Significa que la forma de desarrollar proyectos está definida, establecida, documentada y que existen métricas (obtención de datos objetivos) para la consecución de objetivos concretos (ELKIN COELLO_ BLOG, 2015).

Nivel 4: Administrado Cuantitativamente ò predecible

El proceso es medido y controlado. Los proyectos usan objetivos medibles y cuantificables para alcanzar a cubrir las necesidades de los clientes y la organización. Se gestiona la organización a través de métricas.

Nivel 5: Optimizado:

El proceso se enfoca en la mejora continua. Los procesos de los proyectos y de la organización están orientados a la mejora de las actividades, que mediante métricas son identificadas, evaluadas y puestas en práctica (ELKIN COELLO_ BLOG, 2015).

La mayoría de las empresas llegan hasta el nivel 3, ya que es un nivel con el cual muchas empresas no ven la necesidad de ir más allá. A la vez, las empresas que intentan alcanzar los niveles 4 y 5, lo realizan simultáneamente ya que estos están muy relacionados (SLIDESHARE, 2015).

El objetivo fundamental de estos niveles de madurez es lograr un nivel de estandarización adecuado para el desarrollo de los procesos de desarrollo de software de las organizaciones, con la finalidad de gestionar los proyectos de software adecuadamente y así lograr cumplir con los objetivos planificados para cada proyecto (SLIDESHARE, 2015).

3.1.5 La familia de las normas ISO 27000

Las normas ISO 27000 hacen referencia a la gestión de la seguridad de la información y está alineada con las normas ISO 9001 de gestión de procesos y la 14000 que es la encargada de la gestión medio ambiental de las organizaciones.

Dentro de esta familia de normas, la ISO 27001, es la norma mediante el cual, la organizaciones buscan certificarse como entidades con un sistema de gestión de seguridad de la información – SGSI, es de destacar que estas normas han venido sufriendo cambios constantes y para el caso de la ISO 27001, la versión actual en funcionamiento es la ISO 27001:2013. La norma ISO 27001 a nivel mundial se conoce como ISO/IEC 27001:2013, para la unión europea se conoce como UNE-ISO/IEC 27001:2013. En Colombia se identifica como NTC-ISO-IEC 27001:2013.

La norma ISO 27002:2013, proporciona directrices para las normas de seguridad de la información de la organización y las prácticas de gestión de seguridad de la información, incluyendo la selección, implementación y gestión de los controles, teniendo en cuenta el medio ambiente, riesgo de seguridad de la información de las organizaciones (ISO27002, 2015).

Está diseñado para ser utilizado por las empresas que quieran seleccionar los controles dentro del proceso de implantación de un Sistema de Gestión de Seguridad de la Información basado en ISO / IEC 27001, e implementar controles de seguridad de la información generalmente aceptadas; desarrollar sus propias directrices de gestión de seguridad de la información (ISO9000CONSULTORES, 2015).

La norma ISO 27003[6], es un estándar internacional que hace parte de las ISO 27000, del sistema de gestión de seguridad de la información, y constituye una guía para la implantación de un SGSI. Está adaptada para los que quieran implantar un Sistema de Gestión de la Seguridad de la Información, SGSI y para el uso de los consultores en la resolución de criterios relacionados con la gestión de la seguridad. Se centra en los aspectos importantes y requeridos para un diseño exitoso y una buena implantación según la norma ISO 27001. Además, contiene la descripción del proceso de delimitación de un Sistema de Gestión de Seguridad de la Información, SGSI, el diseño y ejecución de distintos planes de implementación, instrucciones para abordar la planificación de la gestión para implementar un SGSI y el proceso a seguir para obtener aprobación del SGSI en una organización (PMG-SSI_27003, 2015).

La norma ISO 27004, es una guía para el desarrollo y utilización de métricas y técnicas de medida aplicables para determinar la eficacia de un SGSI y de los controles o grupos de controles implementados según ISO/IEC 27001 (PMG-SSI-ISO_27004, 2015).

La norma ISO 27005, proporciona directrices para la gestión del riesgo en la seguridad de la información, apoya los conceptos generales especificados en la norma ISO/IEC 27001:2005 y está diseñada para ayudar a la aplicación satisfactoria de la seguridad de la información basada en un enfoque de gestión de riesgos. Su primera publicación revisó y retiró las normas ISO/IEC TR 13335-3:1998 e ISO/IEC TR 13335-4:2000. La norma 27005:2011, trata temas como tecnologías de la información, técnica de seguridad y administración de riesgos de seguridad de la información (PMG-SSI-ISO_27005, 2015).

3.1.6 Normatividad de la Seguridad de la información en Colombia

A nivel nacional el Ministerio de las Tecnologías de la Información y las Comunicaciones, MinTic, es el encargado de regular las políticas en cuanto a gestión de la seguridad de la información se refiere. Su misión es “El Ministerio de Tecnologías de la Información y las Comunicaciones promueve el acceso, uso efectivo y apropiación masivos de las TIC, a través de políticas y programas, para mejorar la calidad de vida de cada colombiano y el incremento sostenible del desarrollo del país (MINTIC, 2015).

[6] ISO 27003: Guía para la implementación de un Sistema de Gestión de la Seguridad de la Información, SGSI, tomado de: http://www.pmg-ssi.com/2014/01/isoiec-27003-guia-para-la-implementacion-de-un-sistema-de-gestion-de-seguridad-de-la-informacion, (PMG-SSI_27003, 2015).

A nivel nacional Colombia ha venido avanzando con la gestión de la seguridad de la información, tanto así que a través del documento Conpes 3701 del 14 de julio de 2011, el Consejo Nacional de Política Económica y Social, entrega Lineamientos de Política para Ciberseguridad y Ciberdefensa a aplicar en los Ministerios del Interior y de Justicia, Ministerio de Relaciones Exteriores, Ministerio de Defensa Nacional, Ministerio de Tecnologías de la Información y las Comunicaciones, Departamento Administrativo de Seguridad, Departamento Nacional de Planeación-DJSG-DIFP-DIES-OI y la Fiscalía General de la Nación (MINTIC_CONPES, 2015).

Este documento busca generar lineamientos de política en Ciberseguridad y Ciberdefensa para contrarrestar el incremento de amenazas informáticas en el país. Este documento es una herramienta que le permite a Colombia su aplicabilidad como medio de protección y defensa contra los posibles ataques a la seguridad de la información nacional.

Colombia ha venido realizando esfuerzos importantes en cuanto a la gestión de la seguridad de la información, para lo cual es importante presentar algunas de las normas que regula y orientan los avances en materia de seguridad y uso de tecnologías, dentro de las cuales están:

Ley 527 de 1999, “Por medio del cual se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firma digitales, y se establecen entidades de certificación y se dictan otras disposiciones” (ARCHIVO GENERAL DE LA NACIÒN-L527, 2015).

Ley 599 de 2000, Por la cual se expide el código penal. En esta se mantiene la estructura del tipo penal de “Violación ilícita de comunicaciones”, se creó el bien jurídico de los derechos de autor y se incorporaron algunas conductas relacionadas indirectamente con el delito informático, tales como el ofrecimiento, venta, o compra de instrumento apto para interpretar la comunicación privada entre personas. Se tipifico el acceso abusivo a un sistema informático, dentro de su artículo 195 (SECRETARIA SENADO, 2015).

Ley 962 de 2005, “Por la cual se dictan disposiciones sobre racionalización de trámites y procedimientos administrativos de los organismos y entidades del estado y de los particulares que ejercen funciones públicas o prestan servicios públicos. Prevé el uso de medios tecnológicos integrados para disminuir los tiempos y costos de realización de los trámites por parte de los administradores (SECRETARIA SENADO-L962, 2015).

Ley 1150 de 2007, Por medio de la cual se introducen medidas para la eficiencia y la transparencia en la Ley 80 de 1993. Se permite que la administración pública expida actos administrativos y documentos y haga notificaciones por medios electrónicos, para lo cual prevé el desarrollo del Sistema electrónico para la contratación Pública-SECOP (SECRETARIA SENADO-L1150, 2015).

Ley 1273 de 2009, por medio del cual se modifica el código penal, se crea un nuevo bien jurídico tutelado, denominado “De la protección de la información y los datos” y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones (MINTIC-L1273, 2015).

Ley 1341 de 2009, por la cual se definen principios y conceptos sobre la sociedad de la información y la organización de las tecnologías de la información y las comunicaciones-TIC se crea la Agencia Nacional del Espectro (MINTIC-L1341, 2015).

Resolución 2258 de 2009, resolución de la Comisión Nacional de Regulación de Comunicaciones. Sobre seguridad de las redes de los proveedores de redes y servicios de telecomunicaciones (internet), que contribuyan a mejorar la seguridad de sus redes de acceso, cumpliendo con los principios de confidencialidad, integridad y disponibilidad de datos (ALCALDIA DE BOGOTA, 2015).

Modelo de Seguridad de la Información para la estrategia de gobierno en línea. Hace referencia al conjunto de políticas estratégicas que soportan objetivos de gobierno en línea como la protección de la información del individuo y la credibilidad y confianza en el gobierno en línea (DNP, 2015).

Manual 3.1 de la estrategia de Gobierno en Línea – Vive Digital, del Gobierno Nacional (GOBIERNO EN LINEA, 2015).

Adicionalmente se cuenta con el Centro de coordinación de atención de incidentes de seguridad informática colombiano para proveedores de servicios de internet (ISP), el cual está en contacto directo con los centros de seguridad de las empresas afiliadas (empresas proveedoras de internet en Colombia) (DNP, 2015). Coordina solicitudes y denuncias y solución de problemas de seguridad informática.

El avance de las corporaciones autónomas regionales en Colombia en cuanto a la gestión de la seguridad de la información, está enfocado a cumplir con el manual 3.1 de Gobierno en línea, en lo que tiene que ver con cada uno de sus componentes, como es: elementos transversales, información en línea, interacción en línea, transacción en línea, transformación, democracia en línea (GOBIERNO EN LINEA, 2015).

El componente "Elementos transversales", habla del cumplimiento actividades como: 1. Institucionalizar la estrategia de gobierno en línea. 2. Centrar la atención en el usuario. 3. Implementar un sistema de gestión de tecnologías de la información. 4. Implementar un sistema de seguridad de la información (SGSI) (GOBIERNO EN LINEA, 2015).

3.1.7 Avances de la gestión de la Seguridad de la información en Corporinoquia.

De acuerdo a las visitas y entrevistas realizadas con diferentes funcionarios del área de sistemas y del área de Planeación Ambiental, Corporinoquia en cuestiones de gestión de seguridad de la información y por ser entidad pública del Gobierno Nacional, se rige por el Manual 3.1 de Gobierno en Línea, en donde ha avanzado tecnológicamente con la renovación de hardware y software en su sede principal, cuenta con la implementación de sistemas de información del orden nacional, como es la Ventanilla Integral de Tramites Ambientales en Línea, VITAL, el cual sirve como medio de interacción con el ciudadano para que este instaure sus quejas de tipo ambiental y radique sus solicitudes de tramite ambiental, esto es administrado por la Oficina de Tecnología de la Agencia Nacional de Licencias Ambientales, en Bogotá, D.C.

En la actualidad, Corporinoquia cuenta con una central de datos donde se encuentra un chasis con tres cuchillas de servidor, los cuales se encuentran integrados a dos arreglos de discos configurados en RAID 5, desde allí se administran las aplicaciones de software y se gestionan todos los permisos y accesos al sistema. En dicha sala también se cuenta con un rack de comunicaciones al cual están conectados tres switch de un (1) Gigabits de velocidad (dos (2) de 48 puertos y uno (1) de 24 puertos). Desde esta área central salen dos backbone, uno se conecta a un switch principal de 24 puertos y en cascada le brinda conexión a otro switch de 48 puertos, los cuales se conectan al patch panel, brindando conectividad a todas las subareas de la Subdirección Administrativa y Financiera. El otro backbone interconecta la Subdirección Administrativa y el Centro de Documentos de la

Corporación a través de dos switch de 24 y 48 puertos y el patch panel que interconecta los diferentes equipos de tecnología de las áreas mencionadas. El total de puntos utilizados son aproximadamente doscientos ochenta (280) puntos de red. Adicionalmente se brinda conexión inalámbrica a treinta equipos más, para un total general de trescientos diez equipos de cómputo conectados a la red de datos de la Corporinoquia.

La topología de red utilizada en Corporinoquia, es topología en estrella, pero debido al crecimiento de usuarios la corporación se ha visto en la obligación de extender la red de datos a través de switch que se interconectan desde los puntos de red existentes en las nuevas áreas para dar cobertura a los nuevos equipos (usuarios) y mejorar la conectividad, debido a que la conectividad inalámbrica es limitada y se cae constantemente.

Corporinoquia en su sede principal, cuenta con servicio de internet de veinte (20) megas de ancho de banda en fibra óptica, canal dedicado, reuso 1:1, el cual es distribuido en tres canales de internet, uno (1) con doce megabits para el servicio de gestión de trámites y servicios ambientales y acceso a usuarios de la subdirección de Control y Calidad Ambiental, Subdirección de Planeación Ambiental y Secretaria General y dos (2) canales más con cuatro megabits cada uno, brindan servicio de acceso a internet a la Subdirección Administrativa y Financiera y el otro brinda acceso de internet a personal directivo de la Corporación. Dichos canales están protegidos con tres servidores IPCOP Linux, con una configuración básica que no logra mantener seguro el tráfico de paquetes por la red de la Corporación, ocasionando en algunos momentos el acceso de los usuarios a páginas no autorizadas por la Corporación (CONTRATOS.GOV.CO, 2015).

Los servicios de acceso a red de datos y manejo de información se realizan a través de Directorio Activo, con la asignación de usuario, contraseña y privilegios de acceso, dependiendo del área o grupo de trabajo al que corresponda cada usuario de la organización. No hay implementado una política de gestión de seguridad de la información. Este documento será la base para iniciar el proceso en Corporinoquia.

A continuación se presenta una revisión del estado actual de Cumplimiento de Corporinoquia con respecto al anexo A de la norma ISO 27001:2013, “Objetivos de Control y Controles de Referencia”.

Tabla 1. Comparativo estado actual Corporinoquia Vs anexo A de la norma ISO 27001:2013, "Objetivos de Control y Controles de Referencia"

OBJETIVOS DE CONTROL Y CONTROLES DE REFERENCIA – ANEXO A ISO 27001:2013			CUMPLE (SI/NO)	OBSERVACIONES
A.5 POLÍTICAS DE LA SEGURIDAD DE LA INFORMACIÓN				
A.5.1 Orientación de la dirección para la gestión de la seguridad de la información				
Objetivo: Brindar orientación y soporte, por parte de la dirección, para la seguridad de la información de acuerdo con los requisitos del negocio y con las leyes y reglamentos pertinentes.				
A.5.1.1	Políticas para la seguridad de la información	*Control* Se debe 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.	NO	La entidad no cuenta con ningún documento de Política de Seguridad de la Información aprobado por la alta dirección.
A.5.1.2	Revisión de las políticas para la seguridad de la información	*Control* Las políticas para la seguridad de la información se deben revisar a intervalos planificados, o si ocurren cambios significativos, para asegurar su conveniencia, adecuación y eficacia continúas.	NO	Se hace revisión y actualización de algunos riesgos identificados en la oficina de Sistemas en lo relacionado con mantenimiento de equipos de cómputo, publicación de información en sitio web y backup de la información.
A.6 ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN				
A.6.1 Organización interna				
Objetivo: Establecer un marco de referencia de gestión para iniciar y controlar la implementación y la operación de la seguridad de la información dentro de la organización.				
A.6.1.1	Roles y responsabilidades para la seguridad de la información	*Control* Se deben definir y asignar todas las responsabilidades de la seguridad de la información.	NO	No están definidas en ningún documento las responsabilidades para la seguridad de la información.
A.6.1.2	Separación de deberes	*Control* Los deberes y áreas de responsabilidad en conflicto se deben separar para reducir las posibilidades de modificación no autorizada o no intencional, o el uso indebido de los activos de la organización.	SI	La Corporación cuenta con una estructura organizacional definida, mediante la cual se establecen unos roles y unas responsabilidades.
A.6.1.3	Contacto con las autoridades	*Control* Se deben mantener contactos apropiados con las autoridades pertinentes.	NO	No están definidas en ningún documento las responsabilidades para la seguridad de la información.
A.6.1.4	Contacto con grupos de interés especial	*Control* Se deben mantener contactos apropiados con grupos de interés especial u otros foros y asociaciones profesionales especializadas en seguridad.	NO	No se tiene definida una lista de autoridades para llamar en caso de necesitarse.
A.6.1.5	Seguridad de la información en la gestión de	*Control* La seguridad de la información se debe tratar en la gestión de proyectos,	SI	La seguridad de la información se realiza a través de cada

OBJETIVOS DE CONTROL Y CONTROLES DE REFERENCIA – ANEXO A ISO 27001:2013			CUMPLE (SI/NO)	OBSERVACIONES
	proyectos	independientemente del tipo de proyecto.		subdirección y supervisor delegado para controlar la gestión del proyecto.
A.6.2	**Dispositivos móviles y teletrabajo**			
Objetivo: Garantizar la seguridad del teletrabajo y el uso de dispositivos móviles.				
A.6.2.1	Política para dispositivos móviles	*Control* Se deben adoptar una política y unas medidas de seguridad de soporte, para gestionar los riesgos introducidos por el uso de dispositivos móviles.	NO	No existe política de seguridad ni se ha hecho el ejercicio de identificación de riesgos para el uso de dispositivos móviles en cuanto a la seguridad de la información corporativa.
A.6.2.2	Teletrabajo	*Control* Se deben 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.	NO	No se realiza teletrabajo. En algunos casos se habilita el acceso por IP`s autorizadas para el ingreso a los sistemas de información.
A.7	**SEGURIDAD DE LOS RECURSOS HUMANOS**			
A.7.1	**Antes de asumir el empleo**			
Objetivo: Asegurar que los empleados y contratistas comprenden sus responsabilidades y son idóneos en los roles para los que se consideran.				
A.7.1.1	Selección	*Control* Las verificaciones de los antecedentes de todos los candidatos a un empleo se deben 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.	SI	Existe un listado de requisitos que un candidato a un empleo debe cumplir, para acceder a una vacante.
A.7.1.2	Términos y condiciones del empleo	*Control* Los acuerdos contractuales con empleados y contratistas deben establecer sus responsabilidades y las de la organización en cuanto a la seguridad de la información.	SI	Los contratos se firman para su cumplimiento, pero en realidad no hay seguimiento y control del uso de la información de expedientes, en caso de pérdida de documentos. Y las cláusulas del contrato no son de estricto cumplimiento en cuanto a la confidencialidad de la información.
A.7.2	**Durante la ejecución del empleo**			
Objetivo: Asegurarse de que los empleados y contratistas tomen conciencia de sus responsabilidades de seguridad de la información y las cumplan.				
A.7.2.1	Responsabilidades de la dirección	*Control* La dirección debe exigir a todos los empleados y contratistas la aplicación de la seguridad de la información de acuerdo con las políticas y procedimientos establecidos por la	SI	La Dirección General mediante las cláusulas del contrato suscrito entre las partes, obliga dentro de sus actividades a cumplir con el sistema de Gestión

OBJETIVOS DE CONTROL Y CONTROLES DE REFERENCIA – ANEXO A ISO 27001:2013			CUMPLE (SI/NO)	OBSERVACIONES
		organización.		de Calidad de la entidad, dentro de los cuales se tienen en cuenta algunos controles para evitar el riesgo de pérdida de información.
A.7.2.2	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, deben 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.	NO	No se brinda formación a los usuarios acerca de la seguridad de la información. Al momento de ingreso del usuario, se le da acceso a la información que autoriza el jefe inmediato y se le informa la forma de acceso y de uso.
A.7.2.3	Proceso disciplinario	*Control* Se debe 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.	SI	Existe la oficina de control interno disciplinario, pero no existe definido un proceso formal para empleados que hayan cometido violación de la seguridad. Se han presentado casos de perdida de expedientes pero los procesos no han prosperado. En algunos casos los procesos no se abren.
A.7.3	**Terminación y cambio de empleo**			
Objetivo: Proteger los intereses de la organización como parte del proceso de cambio o terminación de empleo.				
A.7.3.1	Terminación o cambio de responsabilidades de empleo	*Control* Las responsabilidades y los deberes de seguridad de la información que permanecen válidos después de la terminación o cambio de empleo se deben definir, comunicar al empleado o contratista y se deben hacer cumplir.	SI	Dentro de los contratos se define un supervisor quien es el responsable de verificar el cumplimiento y entrega de todo lo pactado.

OBJETIVOS DE CONTROL Y CONTROLES DE REFERENCIA – ANEXO A ISO 27001:2013			CUMPLE (SI/NO)	OBSERVACIONES
A.8	**GESTIÓN DE ACTIVOS**			
A.8.1	**Responsabilidad por los activos**			
Objetivo: Identificar los activos organizacionales y definir las responsabilidades de protección apropiadas.				
A.8.1.1	Inventario de activos	*Control* Se deben identificar los activos asociados con información e instalaciones de procesamiento de información, y se debe elaborar y mantener un inventario de estos activos.	SI	Los activos de la Corporación están identificados y registrados en el módulo de almacén del sistema de información PCT, este software registra el activo y el nombre del funcionario a quien está asignado, así como el estado y el valor del mismo. La oficina de

OBJETIVOS DE CONTROL Y CONTROLES DE REFERENCIA – ANEXO A ISO 27001:2013			CUMPLE (SI/NO)	OBSERVACIONES
				sistemas cuenta con un inventario de los activos relacionados con el manejo de la información.
A.8.1.2	Propiedad de los activos	*Control* Los activos mantenidos en el inventario deben tener un propietario.	SI	Los activos asociados con los servicios de procesamiento de información están asignados al área de planeación y funcionarios de la oficina de sistemas.
A.8.1.3	Uso aceptable de los activos	*Control* Se deben identificar, documentar e implementar reglas para el uso aceptable de información y de activos asociados con información e instalaciones de procesamiento de información.	NO	No se encuentran documentados los activos, ni se encuentra definido su uso aceptable con la seguridad de la información.
A.8.1.4	Devolución de activos	*Control* Todos los empleados y usuarios de partes externas deben devolver todos los activos de la organización que se encuentren a su cargo, al terminar su empleo, contrato o acuerdo.	SI	Al momento de liquidar un contrato se expide un Paz y Salvo, al momento de firmarlo el contratista debe haber entregado todo lo que se le había asignado. Permisos de usuario, equipos, información, entre otros.
A.8.2 Clasificación de la información				
Objetivo: Asegurar que la información recibe un nivel apropiado de protección, de acuerdo con su importancia para la organización.				
A.8.2.1	Clasificación de la información	*Control* La información se debe clasificar en función de los requisitos legales, valor, criticidad y susceptibilidad a divulgación o a modificación no autorizada.	NO	La información no está clasificada, sin embargo por conocimiento se sabe que los expedientes de trámites ambientales, sancionatorios y preliminares son información clasificada que no todo los funcionarios pueden acceder a ella.
A.8.2.2	Etiquetado de la información	*Control* Se debe 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.	NO	No existen procedimientos para etiquetado y manejo de la información. El esquema de clasificación existe y es la estructuración de los mismos a través de las tablas de retención documental.
A.8.2.3	Manejo de activos	*Control* Se deben desarrollar e implementar procedimientos para el manejo de activos, de acuerdo con el esquema de clasificación de información adoptado por la organización.	NO	No existen procedimientos establecidos para el manejo de activos dentro de la organización.
A.8.3 Manejo de medios				
Objetivo: Evitar la divulgación, la modificación, el retiro o la destrucción no autorizados de información almacenada en los medios.				
A.8.3.1	Gestión de medios removibles	Control Se deben implementar procedimientos	NO	No hay procedimientos establecidos para la

OBJETIVOS DE CONTROL Y CONTROLES DE REFERENCIA – ANEXO A ISO 27001:2013			CUMPLE (SI/NO)	OBSERVACIONES
		para la gestión de medios removibles, de acuerdo con el esquema de clasificación adoptado por la organización.		gestión de medios removibles.
A.8.3.2	Disposición de los medios	Control Se debe disponer en forma segura de los medios cuando ya no se requieran, utilizando procedimientos formales.	NO	Cuando un medio no sirve o se daña se da de baja en el inventario. No hay control establecido para su disposición final.
A.8.3.3	Transferencia de medios físicos	Control Los medios que contienen información se deben proteger contra acceso no autorizado, uso indebido o corrupción durante el transporte.	NO	No hay establecido mecanismos de protección de medios físicos.
A.9	**CONTROL DE ACCESO**			
A.9.1	**Requisitos del negocio para control de acceso**			
Objetivo: Limitar el acceso a información y a instalaciones de				
A.9.1.1	Política de control de acceso	*Control* Se debe establecer, documentar y revisar una política de control de acceso con base en los requisitos del negocio y de seguridad de la información.	NO	No existe política de control de acceso a la información, establecida por la alta dirección.
A.9.1.2	Acceso a redes y a servicios en red	*Control* Solo se debe permitir acceso de los usuarios a la red y a los servicios de red para los que hayan sido autorizados específicamente.	SI	Existe un procedimiento establecido para brindar acceso a usuarios nuevos, en los servicios de red,
A.9.2	**Gestión de acceso de usuarios**			
Objetivo: Asegurar el acceso de los usuarios autorizados y evitar el acceso no autorizado a sistemas y servicios.				
A.9.2.1	Registro y cancelación del registro de usuarios	*Control* Se debe implementar un proceso formal de registro y de cancelación de registro de usuarios, para posibilitar la asignación de los derechos de acceso.	SI	El procedimiento se realiza pero no está documentado.
A.9.2.2	Suministro de acceso de usuarios	*Control* Se debe 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.	SI	Existe la creación de grupos de usuarios por área, en donde se le asignan privilegios y roles. No se encuentra documentado.
A.9.2.3	Gestión de derechos de acceso privilegiado	*Control* Se debe restringir y controlar la asignación y uso de derechos de acceso privilegiado.	SI	Los usuarios del área de sistemas tienen acceso como administrador al servidor y aplicaciones que se usan al interior de la Corporación.
A.9.2.4	Gestión de información de autenticación secreta de usuarios	*Control* La asignación de información de autenticación secreta se debe controlar por medio de un proceso de gestión formal.	NO	No está definido.

OBJETIVOS DE CONTROL Y CONTROLES DE REFERENCIA – ANEXO A ISO 27001:2013			CUMPLE (SI/NO)	OBSERVACIONES
A.9.2.5	Revisión de los derechos de acceso de usuarios	*Control* Los propietarios de los activos deben revisar los derechos de acceso de los usuarios, a intervalos regulares.	SI	Se revisan los permisos asignados a cada usuario, para evitar accesos indebidos, o falta de accesos autorizados por asignar.
A.9.2.6	Retiro o ajuste de los derechos de acceso	*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 deben retirar al terminar su empleo, contrato o acuerdo, o se deben ajustar cuando se hagan cambios.	SI	Al momento de firmar el Paz y Salvo de terminación de contrato se les quita todos los privilegios y permisos asignados. Además al momento de creación de usuario se le coloca el tempo de inactivación de la cuenta.
A.9.3	**Responsabilidades de los usuarios**			
Objetivo: Hacer que los usuarios rindan cuentas por la salvaguarda de su información de autenticación.				
A.9.3.1	Uso de información de autenticación secreta.	*Control* Se debe exigir a los usuarios que cumplan las prácticas de la organización para el uso de información de autenticación secreta.	NO	No se exige, ni se ha brindado socialización al respecto.
A.9.4	**Control de acceso a sistemas y aplicaciones**			
Objetivo: Evitar el acceso no autorizado a sistemas y aplicaciones.				
A.9.4.1	Restricción de acceso a la información	*Control* El acceso a la información y a las funciones de los sistemas de las aplicaciones se debe restringir de acuerdo con la política de control de acceso.	SI	Se restringe el acceso a la información y a los sistemas de información.
A.9.4.2	Procedimiento de ingreso seguro	*Control* Cuando lo requiere la política de control de acceso, el acceso a sistemas y aplicaciones se debe controlar mediante un proceso de ingreso seguro.	SI	En algunos sistemas de información se utiliza un certificado para acceder a realizar cambios dentro del sistema de información.
A.9.4.3	Sistema de gestión de contraseñas	*Control* Los sistemas de gestión de contraseñas deben ser interactivos y deben asegurar la calidad de las contraseñas.	NO	No esta implementado un sistema de gestión de Contraseñas seguras.
A.9.4.4	Uso de programas utilitarios privilegiados	*Control* Se debe restringir y controlar estrictamente el uso de programas utilitarios que podrían tener capacidad de anular el sistema y los controles de las aplicaciones.	NO	No está restringido
A.9.4.5	Control de acceso a códigos fuente de programas	*Control* Se debe restringir el acceso a los códigos fuente de los programas.	SI	El código fuente de las aplicaciones se encuentra restringido y solo el administrador del mismo tiene acceso a ellos.
A.10	**CRIPTOGRAFÍA**			
A.10.1	**Controles criptográficos**			
Objetivo: Asegurar el uso apropiado y eficaz de la criptografía para proteger la confidencialidad, la autenticidad y/o la integridad de la				

OBJETIVOS DE CONTROL Y CONTROLES DE REFERENCIA – ANEXO A ISO 27001:2013			CUMPLE (SI/NO)	OBSERVACIONES
información.				
A.10.1.1	Política sobre el uso de controles criptográficos	*Control* Se debe desarrollar e implementar una política sobre el uso de controles criptográficos para la protección de la información.	NO	No se encuentra implementada ninguna política sobre el uso de controles criptográficos para la protección de la información.
A.10.1.2	Gestión de llaves	*Control* Se debe desarrollar e implementar una política sobre el uso, protección y tiempo de vida de las llaves criptográficas, durante todo su ciclo de vida.	NO	No existe política para la gestión de llaves.
A.11	**SEGURIDAD FÍSICA Y DEL ENTORNO**			
A.11.1	**Áreas seguras**			
Objetivo: Prevenir el acceso físico no autorizado, el daño y la interferencia a la información y a las instalaciones de procesamiento de información de la organización.				
A.11.1.1	Perímetro de seguridad física	*Control* Se deben definir y usar perímetros de seguridad, y usarlos para proteger áreas que contengan información confidencial o crítica, e instalaciones de manejo de información.	SI	La información crítica se encuentra ubicada en la sala de datos, en la oficina de sistemas.
A.11.1.2	Controles de acceso físicos	*Control* Las áreas seguras se deben proteger mediante controles de acceso apropiados para asegurar que solo se permite el acceso a personal autorizado.	NO	No se cuenta con controles seguros apropiados que impidan el acceso a personal no autorizado a zonas de administración de información.
A.11.1.3	Seguridad de oficinas, recintos e instalaciones	*Control* Se debe diseñar y aplicar seguridad física a oficinas, recintos e instalaciones.	SI	La seguridad se aplica a través de cerraduras con llave en las puertas bajo la responsabilidad del control acceso a personal de cada área.
A.11.1.4	Protección contra amenazas externas y ambientales	*Control* Se debe diseñar y aplicar protección física contra desastres naturales, ataques maliciosos o accidentes.	NO	Se cuenta con extinguidores para combatir el fuego.
A.11.1.5	Trabajo en áreas seguras	*Control* Se deben diseñar y aplicar procedimientos para trabajo en áreas seguras.	SI	La corporación cuenta con una infraestructura física en buenas condiciones. A través del área de Seguridad Ocupacional se ha gestionado la señalización de las instalaciones como medio de evacuación en caso de emergencia.
A.11.1.6	Áreas de despacho y carga	*Control* Se deben controlar los puntos de acceso tales como 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.	SI	El ingreso a las instalaciones de la Corporación, se hace por la puerta principal y están controlados por el servicio de vigilancia. La puerta trasera de ingreso al parqueadero es controlada por la vigilancia y no está

OBJETIVOS DE CONTROL Y CONTROLES DE REFERENCIA – ANEXO A ISO 27001:2013			CUMPLE (SI/NO)	OBSERVACIONES
				permitido el acceso a personal no autorizado.
A.11.2 Equipos				
Objetivo: Prevenir la pérdida, daño, robo o compromiso de activos, y la interrupción de las operaciones de la organización.				
A.11.2.1	Ubicación y protección de los equipos	*Control* Los equipos deben estar ubicados y protegidos para reducir los riesgos de amenazas y peligros del entorno, y las posibilidades de acceso no autorizado.	SI	Los equipos de cómputo y servidores están ubicados estratégicamente en espacios que minimizan el riesgo de daños y amenazas del entorno.
A.11.2.2	Servicios de suministro	*Control* Los equipos se deben proteger contra fallas de energía y otras interrupciones causadas por fallas en los servicios de suministro.	NO	La red de corriente regulada no funciona normalmente debido a que se cuenta con dos UPS pero están dañadas, las baterías están deterioradas. El servidor cuenta con una PS de 6 kva.
A.11.2.3	Seguridad del cableado	*Control* El cableado de energía eléctrica y de telecomunicaciones que porta datos o brinda soporte a los servicios de información se debe proteger contra interceptación, interferencia o daño	SI	El cableado estructurado se transporta por canaleta metálica cubierta, al igual que la corriente alterna para los equipos de cómputo.
A.11.2.4	Mantenimiento de equipos	*Control* Los equipos se deben mantener correctamente para asegurar su disponibilidad e integridad continuas.	SI	Se cuenta con un procedimiento para mantenimiento de equipos de computadores.
A.11.2.5	Retiro de activos	*Control* Los equipos, información o software no se deben retirar de su sitio sin autorización previa.	SI	Las personas autorizadas para realizar cambio de equipos de cómputo, traslados o dar de baja, son los de la oficina de sistemas. Sin embargo en algunas ocasiones se ha presentado que los usuarios trasladan sus equipos sin comunicarlo hasta el momento de realizar la instalación en el nuevo sitio de trabajo dentro de la organización.
A.11.2.6	Seguridad de equipos y activos fuera de las instalaciones	*Control* Se deben 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.	SI	El acceso fuera de las instalaciones se realiza para actividades ajenas a sistemas de información corporativa. Este servicio solo se ofrece para consulta de correo electrónico.
A.11.2.7	Disposición segura o reutilización de equipos	*Control* Se deben verificar todos los elementos de equipos que contengan medios de almacenamiento para asegurar que cualquier dato confidencial o software licenciado haya sido retirado o sobre escrito en forma segura antes de su disposición o reuso.	SI	En el proceso de mantenimiento preventivo y correctivo se tienen en cuenta la disposición del activo y el estado de funcionalidad de cada una de sus partes, para posterior reutilización.

OBJETIVOS DE CONTROL Y CONTROLES DE REFERENCIA – ANEXO A ISO 27001:2013			CUMPLE (SI/NO)	OBSERVACIONES
A.11.2.8	Equipos de usuario desatendido	*Control* Los usuarios deben asegurarse de que a los equipos desatendidos se les da protección apropiada.	SI	Los equipos cuentan con una programación de mantenimiento, en donde el usuario informa sobre la aceptación del servicio. De esta manera se controla si se atendió con eficacia o no.
A.11.2.9	Política de escritorio limpio y pantalla limpia	*Control* Se debe 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.	NO	Se cuenta con la utilización de protector de pantalla del sistema de gestión de calidad, pero no se cuenta con la política de escritorio limpio.
A.12 SEGURIDAD DE LAS OPERACIONES				
A.12.1 Procedimientos operacionales y responsabilidades				
Objetivo: Asegurar las operaciones correctas y seguras de las instalaciones de procesamiento de información.				
A.12.1.1	Procedimientos de operación documentados	*Control* Los procedimientos de operación se deben documentar y poner a disposición de todos los usuarios que los necesitan.	SI	El proceso de TIC, cuenta con cinco procedimientos documentados: Mantenimiento de equipos de cómputo, implementación de sistemas de información, backup, publicación de información en sitio web.
A.12.1.2	Gestión de cambios	*Control* Se deben 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.	SI	Este proceso aplica para la gestión del sistema de gestión de calidad. Se lleva la trazabilidad del proceso de implementación.
A.12.1.3	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.	SI	Se realiza a través del plan de adquisiciones de la corporación.
A.12.1.4	Separación de los ambientes de desarrollo, pruebas, y operación	*Control* Se deben separar los ambientes de desarrollo, prueba y operación, para reducir los riesgos de acceso o cambios no autorizados al ambiente de operación.	NO	En la entidad existe una oficina de sistemas, en donde se lideran proyectos de diferentes temáticas como gestión de adquisición de tecnologías, gestión de desarrollo de software y gestión de soporte de servicios de tecnología en toda la organización.
A.12.2 Protección contra códigos maliciosos				
Objetivo: Asegurarse de que la información y las instalaciones de procesamiento de información estén protegidas contra códigos maliciosos.				

OBJETIVOS DE CONTROL Y CONTROLES DE REFERENCIA – ANEXO A ISO 27001:2013			CUMPLE (SI/NO)	OBSERVACIONES
A.12.2.1	Controles contra códigos maliciosos	*Control* Se deben implementar controles de detección, de prevención y de recuperación, combinados con la toma de conciencia apropiada de los usuarios, para proteger contra códigos maliciosos.	SI	Se cuenta con antivirus en todos los equipos de cómputo. Se implementó un Sistema de Detección de Intrusos.
A.12.3 Copias de respaldo				
Objetivo: Proteger contra la pérdida de datos.				
A.12.3.1	Respaldo de la información	*Control* Se deben 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.	SI	Se realizan copias de respaldo de la información almacenada por cada una de las áreas de la corporación, backup de bases de datos diarios, sistemas operativos, entre otros, y se ponen a prueba constantemente.
A.12.4 Registro y seguimiento				
Objetivo: Registrar eventos y generar evidencia.				
A.12.4.1	Registro de eventos	*Control* Se deben elaborar, conservar y revisar regularmente los registros acerca de actividades del usuario, excepciones, fallas y eventos de seguridad de la información.	SI	Se lleva el control de registro de eventos que entrega el servidor a diario, y los sistemas de información utilizados.
A.12.4.2	Protección de la información de registro	*Control* Las instalaciones y la información de registro se deben proteger contra alteración y acceso no autorizado.	NO	No se evidencia protección de la información de registros.
A.12.4.3	Registros del administrador y del operador.	*Control* Las actividades del administrador y del operador del sistema se deben registrar, y los registros se deben proteger y revisar con regularidad.	SI	Los registros del administrador y del operador se registran, pero no se revisan salvo algún caso fortuito.
A.12.4.4	Sincronización de relojes	*Control* Los relojes de todos los sistemas de procesamiento de información pertinentes dentro de una organización o ámbito de seguridad se deben sincronizar con una única fuente de referencia de tiempo.	NO	Esta actividad no se ha tenido en cuenta al momento de la revisión.
A.12.5 Control de software operacional				
Objetivo: Asegurarse de la integridad de los sistemas operacionales.				
A.12.5.1	Instalación de software en sistemas operativos	*Control* Se deben implementar procedimientos para controlar la instalación de software en sistemas operativos.	NO	Los diferentes equipos de los usuarios están como usuario administrador. No se controla la instalación de software en sistemas operativos.
A.12.6 Gestión de la vulnerabilidad técnica				
Objetivo: Prevenir el aprovechamiento de las vulnerabilidades técnicas.				

OBJETIVOS DE CONTROL Y CONTROLES DE REFERENCIA – ANEXO A ISO 27001:2013			CUMPLE (SI/NO)	OBSERVACIONES
A.12.6.1	Gestión de las vulnerabilidades técnicas	*Control* Se debe 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.	NO	No se cuenta con información acerca de vulnerabilidades técnicas de los sistemas de información, ni registro de medidas, tampoco se han presentado ataques. No se ha hecho levantamiento de riesgos de este tipo.
A.12.6.2	Restricciones sobre la instalación de software	*Control* Se debe establecer e implementar las reglas para la instalación de software por parte de los usuarios.	NO	No hay reglas establecidas para instalación de software por parte de los usuarios en cada uno de sus equipos asignados.
A.12.7 Consideraciones sobre auditorías de sistemas de información				
Objetivo: Minimizar el impacto de las actividades de auditoría sobre los sistemas operativos.				
A.12.7	Controles de auditorías de sistemas de información	*Control* Los requisitos y actividades de auditoría que involucran la verificación de los sistemas operativos se deben planificar y acordar cuidadosamente para minimizar las interrupciones en los procesos del negocio.	NO	No se realiza auditoria a los Sistemas de Información, en lo relacionado con su funcionamiento, las auditorias van enfocadas al avance de proceso dentro de los mismos.
A.13 SEGURIDAD DE LAS COMUNICACIONES				
A.13.1 Gestión de la seguridad de las redes				
Objetivo: Asegurar la protección de la información en las redes, y sus instalaciones de procesamiento de información de soporte.				
A.13.1.1	Controles de redes	*Control* Las redes se deben gestionar y controlar para proteger la información en sistemas y aplicaciones.	SI	El acceso a la red de datos se hace mediante usuario y contraseña. Los puntos de red están ubicados estratégicamente para que los usuarios internos ayuden a proteger los mismos.
A.13.1.2	Seguridad de los servicios de red	*Control* Se deben 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.	SI	Los servicios de red solo se autorizan desde y por personal de la oficina de sistemas de la Corporación. Estos servicios están identificados.
A.13.1.3	Separación en las redes	*Control* Los grupos de servicios de información, usuarios y sistemas de información se deben separar en las redes.	SI	Los grupos de servicios de información están separados, para que cada quien pueda ver solo lo autorizado.
A.13.2 Transferencia de información				
Objetivo: Mantener la seguridad de la información transferida dentro de una organización y con cualquier entidad externa.				
A.13.2.1	Políticas y procedimientos de transferencia de información	*Control* Se debe contar con políticas, procedimientos y controles de transferencia formales para proteger la transferencia de información mediante el	NO	No se cuenta con una política definida para transferencia de información.

OBJETIVOS DE CONTROL Y CONTROLES DE REFERENCIA – ANEXO A ISO 27001:2013			CUMPLE (SI/NO)	OBSERVACIONES
		uso de todo tipo de instalaciones de comunicaciones.		
A.13.2.2	Acuerdos sobre transferencia de información	*Control* Los acuerdos deben tratar la transferencia segura de información del negocio entre la organización y las partes externas.	NO	No existen acuerdos de transferencia de información.
A.13.2.3	Mensajería electrónica	*Control* Se debe proteger adecuadamente la información incluida en la mensajería electrónica.	SI	El uso de correo electrónico se cifra a través de los manejadores de correo electrónico.
A.13.2.4	Acuerdos de confidencialidad o de no divulgación	*Control* Se deben identificar, revisar regularmente y documentar los requisitos para los acuerdos de confidencialidad o no divulgación que reflejen las necesidades de la organización para la protección de la información.	NO	No se encuentran definidos claramente. Para el caso de contratistas en los contratos se estipula la confidencialidad de la información corporativa.
A.14 Adquisición, desarrollo y mantenimiento de sistemas				
A.14.1 Requisitos de seguridad de los sistemas de información				
Objetivo: Asegurar que la seguridad de la información sea una parte integral de los sistemas de información durante todo el ciclo de vida. Esto incluye también los requisitos para sistemas de información que prestan servicios sobre redes públicas.				
A.14.1.1	Análisis y especificación de requisitos de seguridad de la información	*Control* Los requisitos relacionados con seguridad de la información se deben incluir en los requisitos para nuevos sistemas de información o para mejoras a los sistemas de información existentes.	NO	Está enfocada a la asignación de usuario y contraseña.
A.14.1.2	Seguridad de servicios de las aplicaciones en redes públicas	*Control* La información involucrada en los servicios de las aplicaciones que pasan sobre redes públicas se debe proteger de actividades fraudulentas, disputas contractuales y divulgación y modificación no autorizadas.	NO	
A.14.1.3	Protección de transacciones de los servicios de las aplicaciones	*Control* La información involucrada en las transacciones de los servicios de las aplicaciones se debe proteger para evitar la transmisión incompleta, el enrutamiento errado, la alteración no autorizada de mensajes, la divulgación no autorizada, y la duplicación o reproducción de mensajes no autorizada.	NO	
A.14.2 Seguridad en los procesos de desarrollo y de soporte				
Objetivo: Asegurar que la seguridad de la información esté diseñada e implementada dentro del ciclo de vida de desarrollo de los sistemas de información.				
A.14.2.1	Política de desarrollo seguro	*Control* Se deben establecer y aplicar reglas para el desarrollo de software y de sistemas, a los desarrollos dentro de la organización.	NO	No existen políticas para el desarrollo de software seguro.
A.14.2.2	Procedimientos	*Control*	NO	No existen procedimientos

OBJETIVOS DE CONTROL Y CONTROLES DE REFERENCIA – ANEXO A ISO 27001:2013			CUMPLE (SI/NO)	OBSERVACIONES
	de control de cambios en sistemas	Los cambios a los sistemas dentro del ciclo de vida de desarrollo se deben controlar mediante el uso de procedimientos formales de control de cambios.		que permitan ver la trazabilidad del control de cambios.
A.14.2.3	Revisión técnica de las aplicaciones después de cambios en la plataforma de operación	*Control* Cuando se cambian las plataformas de operación, se deben 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.	NO	Se realizan pruebas básicas sujetas al funcionamiento del sistema.
A.14.2.4	Restricciones en los cambios a los paquetes de software	*Control* Se deben desalentar las modificaciones a los paquetes de software, los cuales se deben limitar a los cambios necesarios, y todos los cambios se deben controlar estrictamente.	SI	Cuando se solicitan modificaciones en los paquetes de software, siempre se verifica que la funcionalidad haya quedado bien desarrollada.
A.14.2.5	Principios de construcción de los sistemas seguros	*Control* Se deben establecer, documentar y mantener principios para la construcción de sistemas seguros, y aplicarlos a cualquier actividad de implementación de sistemas de información.	NO	No se cuenta con principios fundamentales de desarrollo seguro de software.
A.14.2.6	Ambiente de desarrollo seguro	*Control* Las organizaciones deben 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.	NO	No se cuenta con ambientes de desarrollo seguro de software.
A.14.2.7	Desarrollo contratado externamente	*Control* La organización debe supervisar y hacer seguimiento de la actividad de desarrollo de sistemas contratados externamente.	SI	Mediante los contratos de desarrollo de software se delega la supervisión o interventoría de los desarrollos de software.
A.14.2.8	Pruebas de seguridad de sistemas	*Control* Durante el desarrollo se deben llevar a cabo pruebas de funcionalidad de la seguridad.	SI	Se realizan pruebas de acuerdo a los requerimientos iniciales para el desarrollo de software contratado.
A.14.2.9	Prueba de aceptación de sistemas	*Control* Para los sistemas de información nuevos, actualizaciones y nuevas versiones, se deben establecer programas de prueba para aceptación y criterios de aceptación relacionados.	SI	Se realizan pruebas de funcionamiento y aceptación de cumplimiento de requerimientos una vez verificado el cumplimiento.
A.14.3 Datos de prueba				
Objetivo: Asegurar la protección de los datos usados para pruebas.				
A.14.3.1	Protección de datos de prueba	*Control* Los datos de prueba se deben seleccionar, proteger y controlar cuidadosamente.	NO	Los datos de prueba son seleccionados por el desarrollador para evidenciar el normal funcionamiento de la aplicación.
A.15 RELACIONES CON LOS PROVEEDORES				
A.15.1 Seguridad de la información en las relaciones con los proveedores				
Objetivo: Asegurar la protección de los activos de la organización que				

OBJETIVOS DE CONTROL Y CONTROLES DE REFERENCIA – ANEXO A ISO 27001:2013			CUMPLE (SI/NO)	OBSERVACIONES
sean accesibles a los proveedores.				
A.15.1.1	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 deben acordar con éstos y se deben documentar.	NO	No existe una política de seguridad relacionada con este ítem. Sin embargo el uso de información corporativa es restringido.
A.15.1.2	Tratamiento de la seguridad dentro de los acuerdos con proveedores	*Control* Se deben 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.	SI	No se cuenta establecido como proceso. Dentro del contrato suscrito se establece la importancia de salvaguardar y cuidar la información que se genere dentro del proceso contractual.
A.15.1.3	Cadena de suministro de tecnología de información y comunicación	*Control* Los acuerdos con proveedores deben 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.	SI	El acuerdo se establece con el levantamiento de requisitos que se establece en la descripción técnica de los elementos tecnológicos a adquirir, para que queden fijados en el proceso contractual y contrato a suscribir entre las partes.
A.15.2 Gestión de la prestación de servicios de proveedores				
Objetivo: Mantener el nivel acordado de seguridad de la información y de prestación del servicio en línea con los acuerdos con los proveedores.				
A.15.2.1	Seguimiento y revisión de los servicios de los proveedores	*Control* Las organizaciones deben hacer seguimiento, revisar y auditar con regularidad la prestación de servicios de los proveedores.	SI	Se realiza control a través del supervisor del contrato, quien se designa en una de las cláusulas del mismo, quien será el encargado de certificar el cumplimiento de ejecución del mismo, al contratista.
A.15.2.2	Gestión de cambios en los servicios de los proveedores	*Control* Se deben gestionar los cambios en el suministro de servicios por parte de los proveedores, incluido el mantenimiento y la 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 reevaluación de los riesgos.	SI	Los supervisores de los contratos realizan constante seguimiento y control a los posibles cambios en el suministro de servicios logrando así la prestación del servicio con buena calidad.
A.16 Gestión de incidentes de seguridad de la información				
A.16.1 Gestión de incidentes y mejoras en la seguridad de la información				
Objetivo: Asegurar un enfoque coherente y eficaz para la gestión de incidentes de seguridad de la información, incluida la comunicación sobre eventos de seguridad y debilidades.				
A.16.1.1	Responsabilidades y	*Control* Se deben establecer las	NO	No hay procedimientos de gestión para asegurar

OBJETIVOS DE CONTROL Y CONTROLES DE REFERENCIA – ANEXO A ISO 27001:2013			CUMPLE (SI/NO)	OBSERVACIONES
	procedimientos	responsabilidades y procedimientos de gestión para asegurar una respuesta rápida, eficaz y ordenada a los incidentes de seguridad de la información.		respuesta rápida y eficaz a incidentes de seguridad de la información. No están documentados.
A.16.1.2	Reporte de eventos de seguridad de la información	*Control* Los eventos de seguridad de la información se deben informar a través de los canales de gestión apropiados, tan pronto como sea posible.	SI	Se sigue el conducto de mando, para presentar los informes. Oficina de Sistemas, Jefe Inmediato y Dirección General.
A.16.1.3	Reporte de debilidades de seguridad de la información	*Control* Se debe 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.	SI	Esto se realiza mediante circular informativa a todo el personal.
A.16.1.4	Evaluación de eventos de seguridad de la información y decisiones sobre ellos.	*Control* Los eventos de seguridad de la información se deben evaluar y se debe decidir si se van a clasificar como incidentes de seguridad de la información.	SI	Se realiza reunión técnica de funcionarios de la oficina de sistemas y se define la clasificación de incidentes de seguridad.
A.16.1.5	Respuesta a incidentes de seguridad de la información	*Control* Se debe dar respuesta a los incidentes de seguridad de la información de acuerdo con procedimientos documentados.	SI	Se da respuesta pero no hay procedimientos documentados.
A.16.1.6	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 debe usar para reducir la posibilidad o el impacto de incidentes futuros.	SI	El conocimiento adquirido al resolver incidentes de seguridad se comparte pero no está documentado.
A.16.1.7	Recolección de evidencia	*Control* La organización debe definir y aplicar procedimientos para la identificación, recolección, adquisición y preservación de información que pueda servir como evidencia.	NO	No existen procedimientos para identificar, recolectar y adquirir evidencia y preservación de información que pueda servir como evidencia.
A.17 ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN DE LA GESTIÓN DE CONTINUIDAD DE NEGOCIO				
A.17.1 Continuidad de seguridad de la información				
Objetivo: La continuidad de seguridad de la información se debe incluir en los sistemas de gestión de la continuidad de negocio de la organización.				
A.17.1.1	Planificación de la continuidad de la seguridad de la información	*Control* La organización debe 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.	NO	No hay definido los requisitos para preservar información para la continuidad d la gestión de la seguridad de la información en situaciones adversas.
A.17.1.2	Implementación de la continuidad de la seguridad de la información	*Control* La organización debe establecer, documentar, implementar y mantener procesos, procedimientos y controles para asegurar el nivel de continuidad requerido para la seguridad de la	NO	La entidad cuenta con procesos de gestión de la calidad en toda su organización. Falta agregarle la continuidad en la seguridad de la

OBJETIVOS DE CONTROL Y CONTROLES DE REFERENCIA – ANEXO A ISO 27001:2013			CUMPLE (SI/NO)	OBSERVACIONES
		información durante una situación adversa.		información durante situaciones adversas.
A.17.1.3	Verificación, revisión y evaluación de la continuidad de la seguridad de la información	*Control* La organización debe 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.	NO	La entidad cuenta con procesos de gestión de la calidad en toda su organización, a los cuales les hace seguimiento y control, a través de auditorías para encontrar oportunidades de mejora. Falta agregar los controles necesarios en lo relacionado con la continuidad en la seguridad de la información durante situaciones adversas.
A.17.2 Redundancias				
Objetivo: Asegurar la disponibilidad de instalaciones de procesamiento de información.				
A.17.2.1	Disponibilidad de instalaciones de procesamiento de información.	*Control* Las instalaciones de procesamiento de información se deben implementar con redundancia suficiente para cumplir los requisitos de disponibilidad.	SI	La entidad cuenta con tres particiones raid 5, en donde se realizan copias de seguridad de la información y adicionalmente se guarda la información en otro servidor y unidades de disco.
A.18 CUMPLIMIENTO				
A.18.1 Cumplimiento de requisitos legales y contractuales				
Objetivo: Evitar el incumplimiento de las obligaciones legales, estatutarias, de reglamentación o contractuales relacionadas con seguridad de la información y de cualquier requisito de seguridad.				
A.18.1.1	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 deben identificar y documentar explícitamente, y mantenerlos actualizados para cada sistema de información y para la organización	SI	Esta información está identificada dentro de los procesos del sistema de gestión de calidad de la corporación.
A.18.1.2	Derechos de propiedad intelectual	*Control* Se deben 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.	SI	La corporación tiene licenciado el 100% de licencias de software de ofimática, antivirus, sistemas de información y sistemas operativos.
A.18.1.3	Protección de registros	*Control* Los registros se deben proteger contra pérdida, destrucción, falsificación, acceso no autorizado y liberación no autorizada, de acuerdo con los requisitos legislativos, de reglamentación, contractuales y de negocio.	SI	A través de los sistemas de información y sus backup de registros de base de datos se asegura la integridad de la información.

OBJETIVOS DE CONTROL Y CONTROLES DE REFERENCIA – ANEXO A ISO 27001:2013			CUMPLE (SI/NO)	OBSERVACIONES
A.18.1.4	Privacidad y protección de información de datos personales	*Control* Se deben asegurar la privacidad y la protección de la información de datos personales, como se exige en la legislación y la reglamentación pertinentes, cuando sea aplicable.	SI	El acceso a información personal de los usuarios externos y personal de la corporación es de carácter confidencial. No se permite su acceso. Es de uso restrictivo.
A.18.1.5	Reglamentación de controles criptográficos	*Control* Se deben usar controles criptográficos, en cumplimiento de todos los acuerdos, legislación y reglamentación pertinentes.	NO	No hay definido ningún procedimiento para el uso de controles criptográficos, dentro de la corporación.
A.18.2 Revisiones de seguridad de la información				
Objetivo: Asegurar que la seguridad de la información se implemente y opere de acuerdo con las políticas y procedimientos organizacionales.				
A.18.2.1	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 deben revisar independientemente a intervalos planificados o cuando ocurran cambios significativos.	NO	Esta actividad no se está realizando al detalle de toda la norma, pues solo hay algunos activos identificados y se le hace seguimiento a los riesgos de esos activos identificados, dentro del sistema de gestión de calidad existente en la entidad.
A.18.2.2	Cumplimiento con las políticas y normas de seguridad	*Control* Los directores deben 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.	NO	Esta actividad se realiza de forma muy general, a través de reuniones de informe.
A.18.2.3	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.	SI	La revisión se realiza dentro del alcance del sistema de gestión de calidad actual, enfocado a procesos.

Fuente: el autor

4 MODELO DE PROPUESTA PARA LA GESTIÒN DE SEGURIDAD DE LA INFORMACIÒN EN CORPORINOQUIA

El presente estudio busca ampliar los conocimientos en materia de gestión de la seguridad de la información y para esto se propone un modelo de gestión en la Corporación Autónoma Regional de la Orinoquia, Corporinoquia, el cual busca generar como resultado un documento guía generalizado que contemple las acciones necesarias para lograr mantener

estable el funcionamiento y en mejores condiciones de seguridad cada uno de los bienes de la organización donde se proyecta el modelo de trabajo y el desarrollo del mismo.

La metodología que se busca seguir en el presente trabajo está basada en la exploración de la gestión de la Seguridad de la Información con la norma ISO/IEC 27001:2013, y aplicarla en Corporinoquia, para lo cual se proponen unas fases importantes en el desarrollo del mismo, como se detalla a continuación:

- Análisis e interpretación de documentación y normatividad para el desarrollo del proyecto.
- Entrevista con funcionarios de la Corporinoquia el desarrollo del análisis y estado actual de la seguridad de la información en Corporinoquia.
- Verificación y validación del estado actual de la seguridad de la información en Corporinoquia con los controles establecidos en el Anexo 1 de la norma ISO 27001:2013. Esta información se desarrollara en el contexto y estado del arte del presente documento.
- Desarrollo y aplicación práctica del modelo de gestión de la seguridad aplicable a Corporinoquia.

4.1 ANÁLISIS E INTERPRETACIÓN DE DOCUMENTACIÓN Y NORMATIVIDAD PARA EL DESARROLLO DEL PROYECTO

La documentación más relevante a explorar en el presente proyecto es la norma ISO 27001:2013 – Técnicas de Seguridad, Sistemas de Gestión de la Seguridad de la información y Requisitos, la norma ISO 31000 Gestión de Riesgo, principios y directrices y el documento “Metodología de análisis y gestión de riesgos de los sistemas de información de Magerit V3”.

Para la norma ISO 27001:2013, se realizará una lectura e interpretación de cada uno de los ítems que componen su estructura, analizando la importancia que tiene cada uno de ellos y la forma como se plasmara en el documento resultado del presente proyecto. Es importante tener en cuenta los compromisos de la alta dirección y el liderazgo frente a un proceso de implementación y aplicación de esta norma, en el desarrollo de políticas de gestión de la seguridad en una organización.

Para el caso de la norma ISO 31000, se realizará una lectura y análisis de cada uno de los conceptos allí descritos. Para la gestión de riesgos del presente trabajo se realizara mediante la metodología de análisis de gestión de riesgos de los sistemas de información de Magerit V3, donde se debe realizar un proceso juicioso en la identificación y caracterización de los activos de la organización, estableciendo el grado de importancia, responsables, ubicación espacial y el estándar básico de funcionalidad. Adicionalmente, se realizará un proceso de caracterización de las posibles amenazas que tienen los diferentes activos identificados. Estas amenazas deben contar con una descripción clara, donde se evidencie el origen dela misma, y se debe clasificar de acuerdo a los requerimientos de Magerit. Se debe identificar el impacto que puede llegar a causar en cuanto a la disponibilidad, confidencialidad e integridad y la probabilidad de ocurrencia en una vigencia o periodo de tiempo.

Una vez identificados los activos y las amenazas de estos activos, es necesario realizar la caracterización de Salvaguardas, que serán los posibles controles que restringirán o disminuirán el impacto causado en caso de materializarse una amenaza. También se debe identificar el grado de eficacia de cada una de las salvaguardas.

Es necesario realizar una estimación del riesgo y e impacto en los activos de la corporación, así como la identificación de objetivos de control, los cuales quedaran plasmados en el documento con cada uno de sus controles y mecanismos de verificación de cumplimiento, una vez se aplique la política de gestión de la seguridad de la información por la empresa, lo cual no está dentro del alcance del proyecto. Solo está contemplado la elaboración del documento.

4.2 ENTREVISTA CON FUNCIONARIOS DE CORPORINOQUIA EL DESARROLLO DEL ANÁLISIS Y ESTADO ACTUAL DE LA SEGURIDAD DE LA INFORMACIÓN EN CORPORINOQUIA.

Para el desarrollo del trabajo de campo es necesario realizar entrevistas con cada uno de los miembros involucrados en el proceso de gestión de la seguridad de la información, en donde, de los cuales es necesario involucrar dentro del proceso a:

Subdirector de Planeación Ambiental, como líder del área de tecnología y será quien brinde la información necesaria y apoye a través de su conocimiento todo lo relacionado con la información del área de Planeación Ambiental.

Funcionarios de la oficina de sistemas que administran sistemas de información, red de datos, mantenimiento, administradores de red y encargados de la seguridad de la información, entre otros.

Funcionaria encargada del área de recursos Físicos y Subdirector de Control y Calidad Ambiental como grandes generadores de información misional y líderes de administración de activos en la corporación.

4.3 VERIFICACIÓN Y VALIDACIÓN DEL ESTADO ACTUAL DE LA SEGURIDAD DE LA INFORMACIÓN EN CORPORINOQUIA VS CONTROLES ANEXO 1 DE LA NORMA ISO 27001:2013.

Para verificar el estado actual de cumplimiento de la corporación en cuanto a gestión de la seguridad de la información con respecto a la norma ISO 27001:2013, de anexo A, se realizara una lista de chequeo, si la corporación cumple o no, y se presentaran algunas observaciones en los ítems donde sea necesario especificar y ampliar, los avances por parte de la corporación.

Por lo anterior, se deberá realizar un cuadro similar al anexo A de la norma ISO 27001:2013 y desarrollarlo como se propone en el párrafo anterior. Esta información se desarrollara en el contexto y estado del arte del presente documento.

4.4 DESARROLLO Y APLICACIÓN PRÁCTICA DEL MODELO DE GESTIÓN DE LA SEGURIDAD APLICABLE A CORPORINOQUIA

Una vez se haya realizado el levantamiento de la información correspondiente a los activos, amenazas, salvaguardas y controles en la gestión de riesgos de acuerdo a la metodología Magerit, se debe realizar el modelo de política de gestión de la seguridad de la información

enfocado a Corporinoquia. Este documento reflejara claramente la introducción al tema a desarrollar, los objetivos, alcance, establecer unos términos y definiciones que sean claros para el lector. También establecerá unas directrices de compromiso de la alta dirección, la forma como deberá estar organizada y establecida la seguridad dentro de la organización, la seguridad de la información e las áreas de talento humano durante las etapas de vinculación y desvinculación de un funcionario, las políticas relacionadas con la gestión de activos, la responsabilidad de su protección y la definición de responsables para cada uno de ellos.

El documento deberá plasmar unas políticas claras de control de acceso a la información, a las secciones y áreas, a la corporación en general, a cada uno de los activos. Los usuarios deben estar gestionados y controlados a través de políticas para el manejo y administración de la información bien sea física como digital.

Se deben establecer políticas en cuanto a requisitos mínimos de seguridad en el entorno físico, como las diferentes áreas, el acceso a los equipos y la seguridad en las operaciones de las actividades realizadas por el personal operario, donde se oriente en líneas gruesas el uso adecuado que se le debe dar la información y a cada uno de los activos para fortalecer y ampliar el tiempo de vida de los activos.

El presente documento recomendara a través de la política de seguridad en las comunicaciones, la gestión de seguridad a tener en cuenta en las redes de datos, la forma de transferir información y las políticas relacionadas con el ciclo de vida de desarrollo de software seguro.

Se deben establecer parámetros importantes para la seguridad de la información en el relacionamiento con terceros, contratistas, y personal vinculado a la Corporación. También se deberá recomendar lo aspectos a tener en cuenta para la continuidad del negocio en caso de catástrofes, recomendar como políticas de gestión de la seguridad, el garantizar el cuidado de la información a través de copias de respaldo y backup de información sensible, entre otros.

Dentro del presente documento se contemplara la inclusión de políticas que hablen sobre el cumplimiento al uso de software licenciado, teniendo en cuenta hasta donde se puede usar y que osos son prohibidos.

Finalmente, se presentaran las conclusiones del resultado del trabajo desarrollado y el trabajo futuro que se podría alcanzar por el autor u otros autores que deseen investigar el presente trabajo. Todo esto será el componente y gestión del proyecto a entregar.

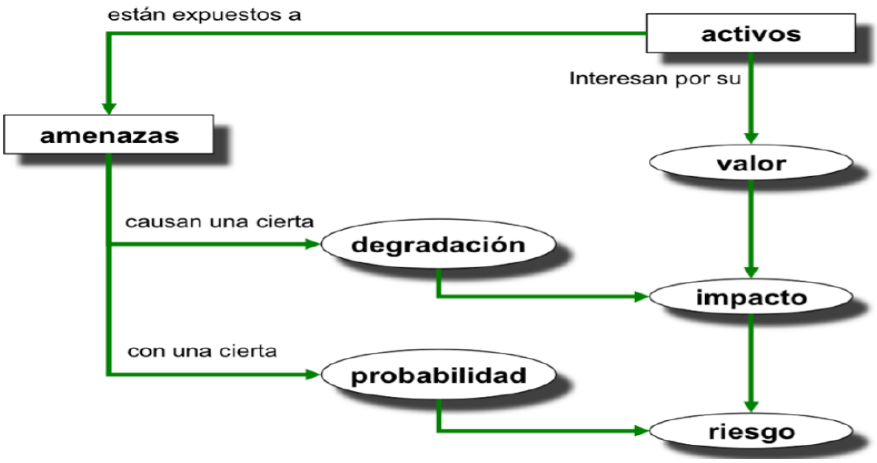
5 APLICACIÒN DEL MODELO DE GESTIÒN DE LA SEGURIDAD DE LA INFORMACIÒN PARA CORPORINOQUIA

5.1 ANALISIS Y GESTIÓN DE RIESGOS DE LA SEGURIDAD DE LA INFORMACIÓN SEGÚN METODOLOGIA MAGERIT

A continuación se presenta el análisis del estado actual de la seguridad de la información de la empresa Corporinoquia, para lo cual se utilizará la metodología Magerit, con el ánimo de identificar los activos, amenazas, salvaguardas y en general, su proceso de gestión y tratamiento de los mismos.

La siguiente grafica brinda a grandes rasgos el proceso por el cual se debe pasar para lograr la identificación de los riesgos y el tratamiento de los mismos, para lo cual, es importante seguir paso a paso la identificación de los activos, identificar el valor de cada uno dentro de la organización y como está relacionado con el manejo de la información, las posibles amenazas que puede tener, cual puede ser su impacto al materializarse las vulnerabilidades y su probabilidad de ocurrencia.

Ilustración 4.Elementos del análisis de riesgos potenciales



Fuente:http://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html#.VcTJY_l_Okp

La metodología de Magerit, brinda la ruta necesaria para la identificación de los activos, se verificará la dependencia entre los mismos y seguidamente se realizará una valoración para cada uno de los activos identificados, como se muestra a continuación:

5.1.1 Caracterización de los activos

5.1.1.1 Identificación de activos de Corporinoquia

Los activos más importantes, identificados en la Corporación Autónoma Regional de la Orinoquia, Corporinoquia, y que se relacionan con el uso y la seguridad de información se muestran en la siguiente tabla:

Tabla 2. Identificación de Activos de Corporinoquia

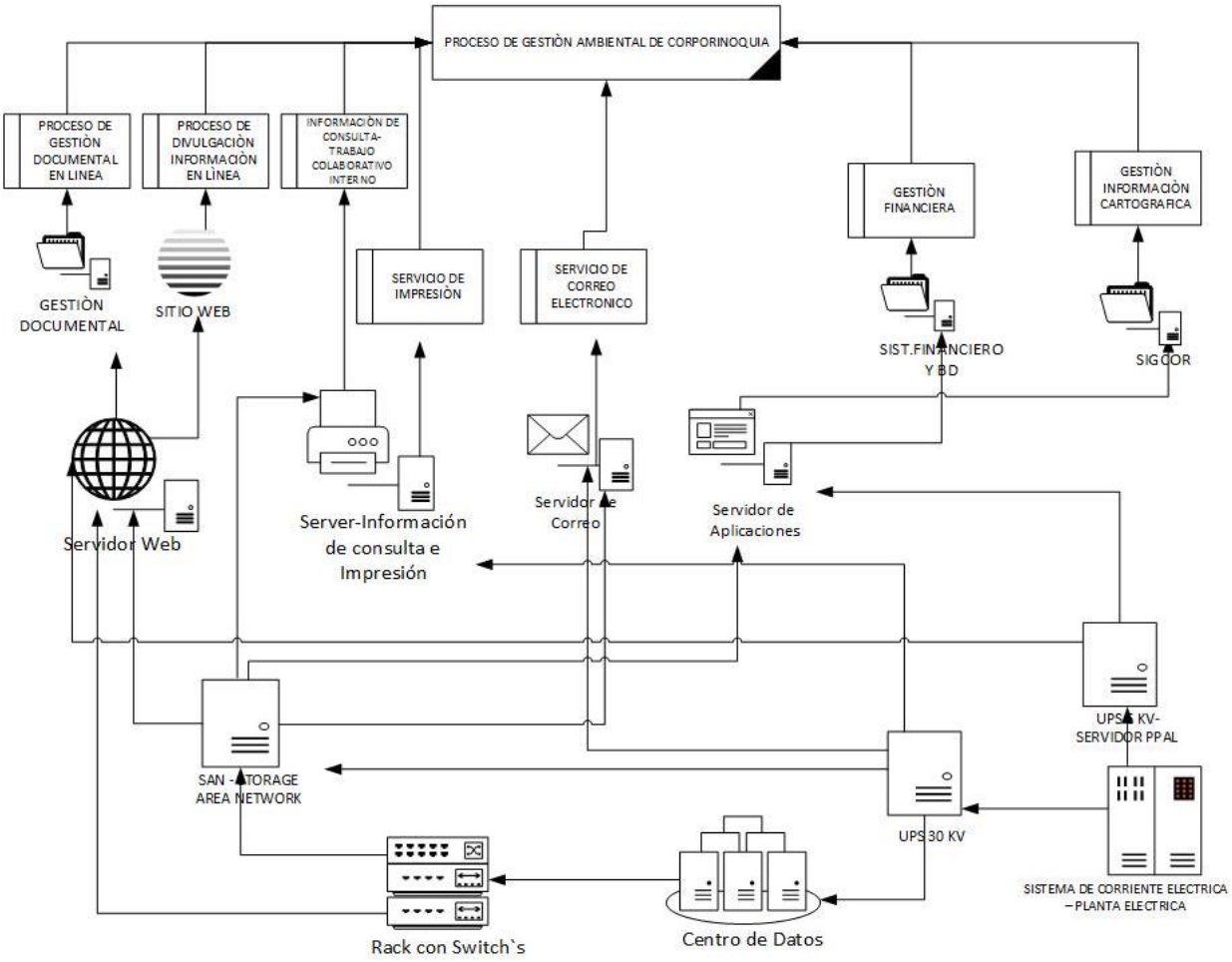
ITEM	COD	NOMBRE CORTO	DESCRIPCIÒN	TIPO	UNIDAD REPONSABLE	PERSONA RESPONSABLE (CARGO)	UBICACIÓN	CANT	OTRAS CARACTERISTICAS ESPECIFICAS DEL TIPO DE ACTIVO (USO ACEPTABLE DEL ACTIVO)
1	2028	SERVIDOR	SERVIDOR DE APLICACIONES (SISTEMAS DE INFORMACIÒN FINANCIERO Y BASE DE DATOS)	SERVIDORES	SUBDIRECCIÓN DE PLANEACIÓN AMBIENTAL	SUBDIRECTOR DE PLANEACIÒN AMBIENTAL	CENTRO DE DATOS DE CORPORINOQUIA	1	FUNCIONAMIENTO DEL SERVIDOR Y LAS APLICACIONES. CONFIGURACIÒN SEGURA PARA ACCESO SEGURO AL SISTEMA.
2	1920	SERVIDOR	SERVIDOR DE ACCESO A INFORMACIÒN Y CONTROL DE IMPRESIÒN	SERVIDORES	SUBDIRECCIÓN DE PLANEACIÓN AMBIENTAL	PROFESIONAL UNIVERSITARIO OFICINA DE SISTEMAS	CENTRO DE DATOS DE CORPORINOQUIA	1	FUNCIONAMIENTO DEL SERVIDOR CON ACCESO A INFORMACIÒN DISPONIBLE. PRIVILEGIOS ACTIVOS PARA INGRESO SEGURO AL SISTEMA.
3	1934	SERVIDOR	SERVIDOR DE APLICACIONES WEB (SISTEMA DE INFORMACIÒN DE GESTIÒN DOCUMENTAL Y BASE DE DATOS)	SERVIDORES	SUBDIRECCIÓN DE PLANEACIÓN AMBIENTAL	SUBDIRECTOR DE PLANEACIÒN AMBIENTAL	CENTRO DE DATOS DE CORPORINOQUIA	1	FUNCIONAMIENTO DEL SERVIDOR Y LA APLICACIÓN ACTIVA. CONFIGURACIÒN SEGURA PARA ACCESO DE USUARIOS SEGURA AL SISTEMA.
4	2033	SERVIDOR	SERVIDOR DE APLICACIONES - SISTEMA DE INFORMACIÒN GEOGRAFICO - SIGCOR.	SERVIDORES	SUBDIRECCIÓN DE PLANEACIÓN AMBIENTAL	PROFESIONAL UNIVERSITARIO OFICINA DE SIG	CENTRO DE DATOS DE CORPORINOQUIA	1	FUNCIONAMIENTO DEL SERVIDOR Y LA APLICACIÓN ACTIVA. CONFIGURACIÒN SEGURA PARA ACCESO DE USUARIOS SEGURA AL SISTEMA.
5	2154	PCT	SISTEMA DE INFORMACIÓN FINANCIERO	SISTEMAS DE INFORMACIÓN	SUBDIRECCIÓN ADMINISTRATIVA Y FINANCIERA	SUBDIRECTORA ADMINITRATIVA Y FINANCIERA	CENTRO DE DATOS DE CORPORINOQUIA	1	APLICACIÓN ACTIVA FUNCIONAL
6	1923	PAGINA WEB	PAGINA WEB CORPORINOQUIA	PAGINA WEB	SUBDIRECCIÓN DE PLANEACIÓN AMBIENTAL	SUBDIRECTOR DE PLANEACIÒN AMBIENTAL	CENTRO DE DATOS DE CORPORINOQUIA	1	APLICACIÓN ACTIVA FUNCIONAL
7	2329	ATHENTO	SISTEMA DE INFORMACIÓN DE GESTIÓN DOCUMENTAL	SISTEMAS DE INFORMACIÓN	SUBDIRECCIÓN DE PLANEACIÓN AMBIENTAL	SUBDIRECTOR DE PLANEACIÒN AMBIENTAL	CENTRO DE DATOS DE CORPORINOQUIA	1	APLICACIÓN ACTIVA FUNCIONAL
8	SIN	CORREO ELECTRONICO	CORREO ELECTRONICO CORPORATIVO	CORREO ELECTRONICO	SUBDIRECCIÓN DE PLANEACIÓN AMBIENTAL	SUBDIRECTOR DE PLANEACIÒN AMBIENTAL	CENTRO DE DATOS DE CORPORINOQUIA	1	APLICACIÓN ACTIVA FUNCIONAL
9	2023	SAN	SAN - STORAGE AREA NETWORK.	UNIDADES DE ALMACENAMIENTO	SUBDIRECCIÓN DE PLANEACIÓN AMBIENTAL	SUBDIRECTOR DE PLANEACIÒN AMBIENTAL	CENTRO DE DATOS DE CORPORINOQUIA	1	FUNCIONAMIENTO ACTIVO. INGRESO A TRAVÈS DE USUARIO Y CONTRASEÑA, CN PRIVILEGIOS ACTIVOS.
10	2044	UPS	UPS RACK DE SERVIDOR PRINCIPAL - 6 KVA - CENTRO DE DATOS	UPS	SUBDIRECCIÓN DE PLANEACIÓN AMBIENTAL	SUBDIRECTOR DE PLANEACIÒN AMBIENTAL	CENTRO DE DATOS DE CORPORINOQUIA	1	UPS FUNCIONAL. BATERIAS CARGADAS Y ACTIVAS AL MOMENTO DE INTERRUPCIONES DE ENERGIA ELECTRICA.
11	1287	RACK	RACK PRINCIPAL DE COMUNICACIONES - CENTRAL DE	RACKS	SUBDIRECCIÓN DE PLANEACIÓN	SUBDIRECTOR DE PLANEACIÒN	CENTRO DE DATOS DE CORPORINOQUIA	1	RACK EN BUEN ESTADO. INTEGRANDO LOS DIFERENTES EQUIPOS Y CABLEADO.

ITEM	COD	NOMBRE CORTO	DESCRIPCIÒN	TIPO	UNIDAD REPONSABLE	PERSONA RESPONSABLE (CARGO)	UBICACIÓN	CANT	OTRAS CARACTERISTICAS ESPECIFICAS DEL TIPO DE ACTIVO (USO ACEPTABLE DEL ACTIVO)
			DATOS.		AMBIENTAL	AMBIENTAL			
12	2027	SWITCH	SWITCH CORE 24 PUERTOS - 10/100/1000 - CENTRO DE DATOS.	SWITCHS	SUBDIRECCIÓN DE PLANEACIÓN AMBIENTAL	SUBDIRECTOR DE PLANEACIÒN AMBIENTAL	CENTRO DE DATOS DE CORPORINOQUIA	1	SWITCH ACTIVO Y FUNCIONAL. FACILITA CONEXIÒN A OTROS SWITCH A TRAVÈS DE BACKBONE. PERMITE ADMINISTRACIÒN POR RED.
13	2026	SWITCH	SWITCH 48 PUERTOS - 10/100/1000 - CENTRO DE DATOS	SWITCHS	SUBDIRECCIÓN DE PLANEACIÓN AMBIENTAL	SUBDIRECTOR DE PLANEACIÒN AMBIENTAL	CENTRO DE DATOS DE CORPORINOQUIA	1	SWITCH ACTIVO Y FUNCIONAL. FACILITA CONEXIÒN A PUNTOS DE LA RED DE DATOS. PERMITE ADMINISTRACIÒN POR RED.
14	2025	SWITCH	SWITCH 48 PUERTOS - 10/100/1000 - CENTRO DE DATOS	SWITCHS	SUBDIRECCIÓN DE PLANEACIÓN AMBIENTAL	SUBDIRECTOR DE PLANEACIÒN AMBIENTAL	CENTRO DE DATOS DE CORPORINOQUIA	1	SWITCH ACTIVO Y FUNCIONAL. FACILITA CONEXIÒN A PUNTOS DE LA RED DE DATOS. PERMITE ADMINISTRACIÒN POR RED.
15	1220	RACK	RACK SECUNDARIO DE COMUNICACIONES- SUBDIRECCIÒN ADMINISTRATIVA Y FINANCIERA.	RACKS	SUBDIRECCIÓN DE PLANEACIÓN AMBIENTAL	SUBDIRECTOR DE PLANEACIÒN AMBIENTAL	SUBDIRECCIÒN ADMINISTRATIVA Y FINANCIERA	1	RACK EN BUEN ESTADO. INTEGRANDO LOS DIFERENTES EQUIPOS Y CABLEADO.
16	2024	SWITCH	SWITCH CORE 24 PUERTOS - 10/100/1000 - SUBDIRECCIÒN ADMINISTRATIVA Y FINANCIERA.	SWITCHS	SUBDIRECCIÓN DE PLANEACIÓN AMBIENTAL	SUBDIRECTOR DE PLANEACIÒN AMBIENTAL	SUBDIRECCIÒN ADMINISTRATIVA Y FINANCIERA	1	SWITCH ACTIVO Y FUNCIONAL. FACILITA CONEXIÒN A PUNTOS DE LA RED DE DATOS. PERMITE ADMINISTRACIÒN POR RED.
17	2034	SWITCH	SWITCH 48 PUERTOS - 10/100/1000 - CENTRO DE DATOS - SUBDIRECCIÒN ADMINISTRATIVA Y FINANCIERA.	SWITCHS	SUBDIRECCIÓN DE PLANEACIÓN AMBIENTAL	SUBDIRECTOR DE PLANEACIÒN AMBIENTAL	SUBDIRECCIÒN ADMINISTRATIVA Y FINANCIERA	1	SWITCH ACTIVO Y FUNCIONAL. FACILITA CONEXIÒN A PUNTOS DE LA RED DE DATOS. PERMITE ADMINISTRACIÒN POR RED.
18	1218	RACK	RACK SECUNDARIO DE COMUNICACIONES - SUBDIRECCIÒN DE PLANEACIÒN AMBIENTAL.	RACKS	SUBDIRECCIÓN DE PLANEACIÓN AMBIENTAL	SUBDIRECTOR DE PLANEACIÒN AMBIENTAL	SUBDIRECCIÒN DE PLANEACIÒN AMBIENTAL	1	RACK EN BUEN ESTADO. INTEGRANDO LOS DIFERENTES EQUIPOS Y CABLEADO DE LA SPA.
19	2022	SWITCH	SWITCH CORE 24 PUERTOS - 10/100/1000 - SUBDIRECCIÒN DE PLANEACIÒN AMBIENTAL.	SWITCHS	SUBDIRECCIÓN DE PLANEACIÓN AMBIENTAL	SUBDIRECTOR DE PLANEACIÒN AMBIENTAL	SUBDIRECCIÒN DE PLANEACIÒN AMBIENTAL	1	SWITCH ACTIVO Y FUNCIONAL. FACILITA CONEXIÒN A PUNTOS DE LA RED DE DATOS. PERMITE ADMINISTRACIÒN POR RED.
20	2021	SWITCH	SWITCH 48 PUERTOS - 10/100/1000 - SUBDIRECCIÒN DE PLANEACIÒN AMBIENTAL.	SWITCHS	SUBDIRECCIÓN DE PLANEACIÓN AMBIENTAL	SUBDIRECTOR DE PLANEACIÒN AMBIENTAL	SUBDIRECCIÒN DE PLANEACIÒN AMBIENTAL	1	SWITCH ACTIVO Y FUNCIONAL. FACILITA CONEXIÒN A PUNTOS DE LA RED DE DATOS. PERMITE ADMINISTRACIÒN POR RED.

ITEM	COD	NOMBRE CORTO	DESCRIPCIÒN	TIPO	UNIDAD REPONSABLE	PERSONA RESPONSABLE (CARGO)	UBICACIÓN	CANT	OTRAS CARACTERISTICAS ESPECIFICAS DEL TIPO DE ACTIVO (USO ACEPTABLE DEL ACTIVO)
21	1276	CABLEADO ESTRUCTURADO	CABLEADO ESTRUCTURADO CATEGORIA 6 Y RED DE DATOS y CANALETA.	CABLEADO DE DATOS	SUBDIRECCIÓN DE PLANEACIÓN AMBIENTAL	SUBDIRECTOR DE PLANEACIÒN AMBIENTAL	TODA LA SEDE PRINCIPAL DE LA CORPORACIÒN	1	COMUNICACIÒN FUNCIONAL.
22	1232	CORRIENTE REGULADA	CABLEADO DE COBRE DE CORRIENTE REGULADA PARA EQUIPOS DE CÓMPUTO.	CABLEADO DE CORRIENTE REGULADA	SUBDIRECCIÓN ADMINISTRATIVA Y FINANCIERA	PROFESIONAL UNIVERSITARIO OFICINA DE RECURSOS FISICOS	TODA LA SEDE PRINCIPAL DE LA CORPORACIÒN	1	CORRIENTE REGULADA FUNCIONAL SIN INTERRUPCIONES DE ENERGIA.
23	1256	UPS	UPS DE 20 KVA, PROTECCIÒN DE EQUIPOS DE COMPUTO SUBDIRECCIÒN DE PLANEACIÒN Y CENTRO DE DOCUMENTOS.	UPS	SUBDIRECCIÓN ADMINISTRATIVA Y FINANCIERA	PROFESIONAL UNIVERSITARIO OFICINA DE RECURSOS FISICOS	ZONA DE MAQUINAS DE CORPORINOQUIA.	1	UPS FUNCIONAL. BATERIAS CARGADAS Y ACTIVAS AL MOMENTO DE INTERRUPCIONES DE ENERGIA ELECTRICA.
24	1257	UPS	UPS DE 30 KVA, PROTECCIÒN DE EQUIPOS DE COMPUTO SUBDIRECCIÒN DE CONTROL Y CALIDAD AMBIENTAL, SUBDIRECCIÒN ADMINISTRATIVA Y FINANCIERA Y DIRECCIÒN GENERAL.	UPS	SUBDIRECCIÓN ADMINISTRATIVA Y FINANCIERA	PROFESIONAL UNIVERSITARIO OFICINA DE RECURSOS FISICOS	ZONA DE MAQUINAS DE CORPORINOQUIA.	1	UPS FUNCIONAL. BATERIAS CARGADAS Y ACTIVAS AL MOMENTO DE INTERRUPCIONES DE ENERGIA ELECTRICA.
25	SIN	DOCUMENTOS IMPRESOS	INFORMACIÒN FISICA DEL CENTRO DE DOCUMENTOS DE CORPORINOQUIA, SEDE PRINCIPAL.	DOCUMENTOS FISICOS	SECRETARIA GENERAL	SECRETARIA GENERAL - TECNICO ADMINISTRATIVO CENTRO DE DOCUMENTOS.	CENTRO DE DOCUMENTOS DE CORPORINOQUIA	1	INFORMACIÒN EN BUEN ESTADO. CONTROL DE INFORMACIÒN Y DOCUMENTOS ALMACENADOS. GESTIÒN OPORTUNA DE INFORMACIÒN.
26	1253	PLANTA ELECTRICA	PLANTA ELECTRICA LISTER DE 30 KVA	PLANTA ELECTRICA	SUBDIRECCIÓN ADMINISTRATIVA Y FINANCIERA	PROFESIONAL UNIVERSITARIO OFICINA DE RECURSOS FISICOS	ZONA DE MAQUINAS DE CORPORINOQUIA.	1	PLANTA ELECTRICA FUNCIONAL. ENCENDIDO AUTOMATICO. SOPORTE DE CORRIENTE ELECTRICA AL MOMENTO DE INTERRUPCIONES DE ENERGIA.
27	DIF. CODIGOS	EQUIPO DE COMPUTO	EQUIPOS DE COMPUTO DE ESCRITORIO.	COMPUTADOR DE ESCRITORIO	DIFERENTES AREAS DE LA SEDE PRINCIPAL DE LA CORPORACIÒN	179	TODA LAS OFICINA DE LA SEDE PRINCIPAL DE LA CORPORACIÒN	179	EQUIPOS FUNCIONANDO CON SEGURIDAD.

5.1.1.2 Dependencias entre los activos identificados en Corporinoquia

Ilustración 5. Dependencia entre los activos identificados en Corporinoquia



Fuente: el autor

5.1.1.3 Valoración de los activos identificados

Para la valoración de cada uno de los activo se debe tener en cuenta las dimensiones en las que el activo es relevante y la estimación de la valoración en cada dimensión.

Adicionalmente se presenta los criterios de valoración de los diferentes activos identificados, los cuales fueron levantados en conjunto con el Subdirector de Planeación Ambiental, Profesional Universitaria de la oficina de sistemas, y profesional del área de gestión documental de la Corporación, y de acuerdo a la escala de valoración propuesta por Magerit:

Tabla 3. Criterios de Valoración de los activos

NIVEL	CRITERIO DE VALORACIÓN	CRITERIO
10	Extremo	Daño extremadamente grave
9	Muy Alto	Daño muy grave
6 - 8	Alto	Daño Grave
3 - 5	Medio	Daño importante
1 - 2	Bajo	Daño menor
0	Despreciable	Irrelevante

Fuente: MAGERIT – versión 3.0 Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información, Libro II - Catálogo de Elementos

Estos criterios de evaluación serán aplicados a las dimensiones de Confidencialidad, integridad, disponibilidad, Autenticidad y Trazabilidad de la información y de cada uno de los activos identificados.

Adicionalmente se identificara la probabilidad de coste para la organización la cual supone la destrucción del activo.

El puntaje dado a cada una de las dimensiones en cada uno de los activos, obedece a la importancia de cumplimiento de controles de seguridad que se debe tener con cada activo para evitar el aprovechamiento de vulnerabilidades, y a su vez el alto coste que se puede llegar a asumir, para recuperar el sistema de un ataque a vulnerabilidad existentes en el mismo.

Tabla 4. Valoración de los activos de Corporinoquia

ITEM	CODIGO	NOMBRE CORTO	DESCRIPCIÒN	PROBABILIDAD DE COSTE QUE PARA LA ORGANIZACIÓN SUPONE LA DESTRUCCIÓN DEL ACTIVO	CONFIDENCIALIDAD	INTEGRIDAD	DISPONIBILIDAD	AUTENTICIDAD	TRAZABILIDAD
1	2028	SERVIDOR	SERVIDOR DE APLICACIONES (SISTEMAS DE INFORMACIÒN FINANCIERO Y BASE DE DATOS)	8	7	9	9	9	10
2	1920	SERVIDOR	SERVIDOR DE ACCESO A INFORMACIÒN Y CONTROL DE IMPRESIÒN	5	6	3	7	9	10

ITEM	CODIGO	NOMBRE CORTO	DESCRIPCIÒN	PROBABILIDAD DE COSTE QUE PARA LA ORGANIZACIÓN SUPONE LA DESTRUCCIÓN DEL ACTIVO	CONFIDENCIALIDAD	INTEGRIDAD	DISPONIBILIDAD	AUTENTICIDAD	TRAZABILIDAD
3	1934	SERVIDOR	SERVIDOR DE APLICACIONES WEB (SISTEMA DE INFORMACIÒN DE GESTIÒN DOCUMENTAL Y BASE DE DATOS)	8	7	9	9	9	10
4	2033	SERVIDOR	SERVIDOR DE APLICACIONES - SISTEMA DE INFORMACIÒN GEOGRAFICO - SIGCOR.	8	7	8	8	9	10
5	2154	PCT	SISTEMA DE INFORMACIÓN FINANCIERO	8	8	9	9	9	10
6	1923	PAGINA WEB	PAGINA WEB CORPORINOQUIA	8	8	8	9	9	10
7	2329	ATHENTO	SISTEMA DE INFORMACIÓN DE GESTIÓN DOCUMENTAL	9	9	9	9	9	10
8	SIN	CORREO ELECTRONICO	CORREO ELECTRONICO CORPORATIVO	9	9	9	9	9	10
9	2023	SAN	SAN - STORAGE AREA NETWORK.	9	9	9	9	9	10
10	2044	UPS	UPS RACK DE SERVIDOR PRINCIPAL - 6 KVA - CENTRO DE DATOS	7	8	8	9	6	6
11	1287	RACK	RACK PRINCIPAL DE COMUNICACIONES - CENTRAL DE DATOS.	4	5	5	5	5	5
12	2027	SWITCH	SWITCH CORE 24 PUERTOS - 10/100/1000 - CENTRO DE DATOS.	7	7	7	7	8	8
13	2026	SWITCH	SWITCH 48 PUERTOS - 10/100/1000 - CENTRO DE DATOS	7	7	7	9	8	8
14	2025	SWITCH	SWITCH 48 PUERTOS - 10/100/1000 - CENTRO DE DATOS	7	7	7	9	8	8
15	1220	RACK	RACK SECUNDARIO DE COMUNICACIONES- SUBDIRECCIÒN ADMINISTRATIVA Y FINANCIERA.	4	5	5	7	5	5
16	2024	SWITCH	SWITCH CORE 24 PUERTOS - 10/100/1000 - SUBDIRECCIÒN ADMINISTRATIVA Y FINANCIERA.	7	7	7	9	8	8
17	2034	SWITCH	SWITCH 48 PUERTOS - 10/100/1000 - CENTRO DE DATOS - SUBDIRECCIÒN	7	7	7	9	8	8

ITEM	CODIGO	NOMBRE CORTO	DESCRIPCIÒN	PROBABILIDAD DE COSTE QUE PARA LA ORGANIZACIÓN SUPONE LA DESTRUCCIÓN DEL ACTIVO	CONFIDENCIALIDAD	INTEGRIDAD	DISPONIBILIDAD	AUTENTICIDAD	TRAZABILIDAD
			ADMINISTRATIVA Y FINANCIERA.						
18	1218	RACK	RACK SECUNDARIO DE COMUNICACIONES - SUBDIRECCIÒN DE PLANEACIÒN AMBIENTAL.	4	5	5	8	5	5
19	2022	SWITCH	SWITCH CORE 24 PUERTOS - 10/100/1000 - SUBDIRECCIÒN DE PLANEACIÒN AMBIENTAL.	7	7	7	9	8	8
20	2021	SWITCH	SWITCH 48 PUERTOS - 10/100/1000 - SUBDIRECCIÒN DE PLANEACIÒN AMBIENTAL.	7	7	7	9	8	8
21	1276	CABLEADO ESTRUCTURADO	CABLEADO ESTRUCTURADO CATEGORIA 6 Y RED DE DATOS y CANALETA.	7	7	8	9	8	6
22	1232	CORRIENTE REGULADA	CABLEADO DE COBRE DE CORRIENTE REGULADA PARA EQUIPOS DE CÓMPUTO.	6	4	7	8	8	6
23	1256	UPS	UPS DE 20 KVA, PROTECCIÒN DE EQUIPOS DE COMPUTO SUBDIRECCIÒN DE PLANEACIÒN Y CENTRO DE DOCUMENTOS.	6	5	7	9	6	6
24	1257	UPS	UPS DE 30 KVA, PROTECCIÒN DE EQUIPOS DE COMPUTO SUBDIRECCIÒN DE CONTROL Y CALIDAD AMBIENTAL, SUBDIRECCIÒN ADMINISTRATIVA Y FINANCIERA Y DIRECCIÒN GENERAL.	6	5	7	9	6	6
25	SIN	DOCUMENTOS IMPRESOS	INFORMACIÒN FISICA DEL CENTRO DE DOCUMENTOS DE CORPORINOQUIA, SEDE PRINCIPAL.	8	8	8	9	7	8
26	1253	PLANTA ELECTRICA	PLANTA ELECTRICA LISTER DE 30 KVA	7	5	7	9	7	7
27	CODIGOS	EQUIPOS DE COMPUTO	EQUIPOS DE COMPUTO DE ESCRITORIO	7	6	6	8	8	8

Fuente: el autor

5.1.2 Caracterización de las amenazas

A continuación se identificaran las amenazas a las que están expuestos los activos seleccionados de la Corporación Autónoma Regional de la Orinoquia Corporinoquia.

5.1.2.1 Identificación de las amenazas

De acuerdo a la metodología de Magerit, se identifican diferentes tipos de amenazas como son: desastres naturales, de origen industrial, errores y fallos no intencionados, ataques intencionados, correlación de errores y ataques y amenazas XML, entre otras.

Con el presente ejercicio se identificaran las amenazas de los activos que se viene trabajando en el alcance del proyecto, y se mostraran una vez se valoren las amenazas.

5.1.2.2 Valorización de las Amenazas

Una vez identificados los activos y las amenazas que pueden afectar a esos activos, se evaluara la influencia en el valor de los activos en relación a la degradación que puede sufrir el activo, en caso de ocurrir la materialización de la amenaza y la probabilidad de que ocurra la amenaza.

Por lo anterior, se clasificara de la siguiente manera la probabilidad de que ocurra o se materialice una amenaza:

Tabla 5. Degradación del valor del activo

SIGLA	DESCRIPCIÒN	PROBABILIDAD DE DEGRADACIÒN	OCURRENCIA
MA	Muy Alta	Casi Seguro	Fácil
A	Alta	Muy Alto	Medio
M	Media	Posible	Difícil
B	Baja	Poco Probable	Muy Fácil
MB	Muy Baja	Muy Raro	Extremadamente Difícil

Fuente: Magerit 3.0 – Metodología de Análisis y gestión de Riesgos de los sistemas de información, pagina 28.

Para el modelamiento de probabilidad de ocurrencia en la materialización de las amenazas, se tendrá en cuenta la frecuencia de ocurrencia en una vigencia y su modelamiento será numérico, como se detalla a continuación:

Tabla 6. Probabilidad de Ocurrencia

SIGLA	DESCRIPCIÒN	PROBABILIDAD DE OCURRENCIA	PERIODICIDAD
MA	100	Muy Frecuente	A diario
A	10	Frecuente	Mensualmente
M	1	Normal	Una Vez al año
B	1/10	Poco Frecuente	Cada varios años
MB	1/1000	Muy poco frecuente	Siglos

Fuente: Magerit 3.0 – Metodología de Análisis y gestión de Riesgos de los sistemas de información, página 28.

Estos criterios de evaluación serán aplicados a cada uno de los activos y amenazas que se identificaron en cada uno de los activos, de acuerdo a la siguiente tabla:

Tabla 7. Amenazas identificadas en los Activos – Mapa de Riesgos

ACTIVO	AMENAZAS	DESCRIPCIÓN	ORIGEN DE LA AMENAZA	ORIGEN DE LA AMENAZA (Clasificación Según Magerit)	IMPACTO Y DEGRADACIÒN DEL ACTIVO			PROBABILIDAD DE OCURRENCIA	DISPONIBILIDAD EN EL TIEMPO				
					CONFIDENCIALIDAD [C]	INTEGRIDAD [I]	DISPONIBILIDAD [D]		> A 8 HORAS	> 1 DIA	> 3 DIAS	> 8 DIAS	> 1 MES
SERVIDOR DE APLICACIONES (SISTEMAS DE INFORMACIÒN FINANCIERO Y BASE DE DATOS)	Sobrecalentamiento e incendio de equipos por deficiencia en la aclimatación ambiental del servidor.	Incendios por sobrecalentamiento en el hardware de procesamiento, memoria o disco duro por exceso de altas temperaturas de forma prolongada y sin control. El fuego se puede propagar causando daños irreversibles en los equipos y en la información.	Bajo nivel de revisión y controles de temperatura en la sala de servidores.	5.2.1. (I.1) Fuego	Muy Baja	Alta	Alta	1/100 - Muy Poco Frecuente	Baja	Baja	Media	Alta	Muy Alta
	Incendio accidental o deliberado por personal interno o externo de la Corporación.	Personas que acceden a las áreas restringidas sin control alguno y producen fuego ocasionando daños en los equipos.	Entorno (Accidental) Humano (Accidental o delibrado)	5.3. (E) Errores de los usuarios 5.4.3. (A.5) Suplantación de la identidad del usuario. 5.4.9. (A.11) Acceso no autorizado.	Muy Baja	Alta	Alta	1/100 - Muy Poco Frecuente	Baja	Baja	Media	Alta	Muy Alta
	Daños en la estructura del servidor por caída de concreto y hierro reforzado por temblor (Desastre Natural)	Por desastre natural, temblor o terremoto se puede caer la infraestructura del edificio y dañar los equipos servidores.	Desastre Natural	5.1.3. 8N.*) Desastres Naturales.	Muy Baja	Alta	Alta	1/100 - Muy Poco Frecuente	Baja	Baja	Media	Alta	Muy Alta
	Daños en el servidor por sobrecargas de alto voltaje	La corriente eléctrica es muy variable en Yopal, por lo cual al no contar con buena protección de supresor de	Bajo nivel de protección de los equipos con supresor de picos	5.2.3. (I. *) Desastres Industriales.	Muy Baja	Alta	Alta	1/10 - Poco Frecuente	Baja	Baja	Media	Alta	Muy Alta

ACTIVO	AMENAZAS	DESCRIPCIÓN	ORIGEN DE LA AMENAZA	ORIGEN DE LA AMENAZA (Clasificación Según Magerit)	IMPACTO Y DEGRADACIÒN DEL ACTIVO			PROBABILIDAD DE OCURRENCIA	DISPONIBILIDAD EN EL TIEMPO				
					CONFIDENCIALIDAD [C]	INTEGRIDAD [I]	DISPONIBILIDAD [D]		> A 8 HORAS	> 1 DIA	> 3 DIAS	> 8 DIAS	> 1 MES
	eléctrico en el mismo.	picos y regulación de voltaje, los equipos se pueden quemar o sufrir daños.	de corriente eléctrica.										
	Fallas de funcionamiento en el servidor por defectos en el software.	Una mala configuración del software del servidor puede generar fallas en el funcionamiento del mismo.	Software no licenciado, mala configuración del software instalado, bajo nivel de actualizaciones de software.	5.3.4. (E4) Errores de Configuración.	Media	Alta	Alta	1/100 - Muy Poco Frecuente	Baja	Baja	Media	Alta	Muy Alta
	Fallas en el funcionamiento del servidor por daños en el hardware.	Desperfectos en el hardware o mala configuración al momento de ensamblar el servidor ocasionara fallas en el funcionamiento del mismo.	Mala configuración del hardware, bajo nivel de compatibilidad de partes.	5.3.4. (E4) Errores de Configuración. 5.3.5. (E.7) Deficiencia en la Organización.	Muy Baja	Media	Alta	1 - Normal	Baja	Baja	Media	Alta	Muy Alta
	Fallas en el funcionamiento del servidor por cortes del suministro eléctrico	La ausencia de energía eléctrica o cortes repentinos en el servicio de fluido eléctrico ocasiona apagones inesperados de los equipos tecnológicos y servidores, afectando la disponibilidad del servicio.	Entorno (Accidental) Humano (Accidental o delibrado)	5.2.3. (I. *) Desastres Industriales.	Muy Baja	Baja	Alta	1/100 - Muy Poco Frecuente	Baja	Baja	Media	Alta	Muy Alta
	Accesos no autorizados al servidor.	Ataques de hacker ocasionando accesos no autorizados al servidor, suplantación de identidad, o aplicación de ingeniería social	Bajo nivel de control de accesos, No existencia de políticas de seguridad de la	5.4.3. (A.5) Suplantación de la identidad del usuario.	Alta	Alta	Media	1/10 - Poco Frecuente	Baja	Baja	Media	Alta	Muy Alta

ACTIVO	AMENAZAS	DESCRIPCIÓN	ORIGEN DE LA AMENAZA	ORIGEN DE LA AMENAZA (Clasificación Según Magerit)	IMPACTO Y DEGRADACIÒN DEL ACTIVO			PROBABILIDAD DE OCURRENCIA	DISPONIBILIDAD EN EL TIEMPO				
					CONFIDENCIALIDAD [C]	INTEGRIDAD [I]	DISPONIBILIDAD [D]		> A 8 HORAS	> 1 DIA	> 3 DIAS	> 8 DIAS	> 1 MES
		para obtener contraseñas y usuarios y as acceder al servidor y ocasionar daños al sistema.	información.	5.4.9. (A.11) Acceso no autorizado.									
	Fallas en el funcionamiento por ataque de virus.	Disminución de controles de seguridad con antivirus a los servidores, o antivirus desactualizados lo que puede ocasionar el aprovechamiento de vulnerabilidades.	Antivirus desactualizados o inactivos o equipos no protegidos con antivirus.	5.3.14. (E.21) Errores de mantenimiento /Actualización de programas (software).	Media	Media	Media	1/10 - Poco Frecuente	Baja	Baja	Media	Alta	Muy Alta
	Ataques de denegación de servicio.	Ataques de hacker ocasionando ataques de denegación de servicios, por falta de controles que identifiquen y protejan al sistema de intrusos.	Falta de controles de seguridad, detección y protección de intrusos.	5.4.3. (A.5) Suplantación de la identidad del usuario. 5.4.9. (A.11) Acceso no autorizado.	Baja	Baja	Alta	1/10 - Poco Frecuente	Baja	Baja	Media	Alta	Muy Alta
SERVIDOR DE ACCESO A INFORMACIÒN Y CONTROL DE IMPRESIÒN	Sobrecalentamiento e incendio de equipos por deficiencia en la aclimatación ambiental del servidor.	Incendios por sobre calentamiento en el hardware de procesamiento, memoria o disco duro por exceso de altas temperaturas de forma prolongada y sin control. El fuego se puede propagar causando daños irreversibles en los equipos y en la información.	Bajo nivel de revisión y controles de temperatura en la sala de servidores.	5.2.1. (I.1) FUEGO	Muy Baja	Alta	Alta	1/100 - Muy Poco Frecuente	Baja	Baja	Media	Alta	Muy Alta

ACTIVO	AMENAZAS	DESCRIPCIÓN	ORIGEN DE LA AMENAZA	ORIGEN DE LA AMENAZA (Clasificación Según Magerit)	IMPACTO Y DEGRADACIÒN DEL ACTIVO			PROBABILIDAD DE OCURRENCIA	DISPONIBILIDAD EN EL TIEMPO				
					CONFIDENCIALIDAD [C]	INTEGRIDAD [I]	DISPONIBILIDAD [D]		> A 8 HORAS	> 1 DIA	> 3 DIAS	> 8 DIAS	> 1 MES
	Incendio deliberado por personal interno o externo de la Corporación.	Personas que acceden a las áreas restringidas sin control alguno y producen fuego ocasionando daños en los equipos.	Entorno (Accidental) Humano (Accidental o delibrado)	5.3. (E) Errores de los usuarios 5.4.3. (A.5) Suplantación de la identidad del usuario. 5.4.9. (A.11) Acceso no autorizado.	Muy Baja	Alta	Alta	1/100 - Muy Poco Frecuente	Baja	Baja	Media	Alta	Muy Alta
	Daños en la estructura del servidor por caída de concreto y hierro reforzado por temblor (Desastre Natural)	Por desastre natural, temblor o terremoto se puede caer la infraestructura del edificio y dañar los equipos servidores.	Desastre Natural	5.1.3. 8N.*) Desastres Naturales.	Muy Baja	Alta	Alta	1/100 - Muy Poco Frecuente	Baja	Baja	Media	Alta	Muy Alta
	Daños en el servidor por sobrecargas de alto voltaje eléctrico en el mismo.	La corriente eléctrica es muy variable en Yopal, por lo cual al no contar con buena protección de supresor de picos y regulación de voltaje, los equipos se pueden quemar o sufrir daños.	Bajo nivel de protección de los equipos con supresor de picos de corriente eléctrica.	5.2.3. (I. *) Desastres Industriales.	Muy Baja	Alta	Alta	1/10 - Poco Frecuente	Baja	Baja	Media	Alta	Muy Alta

ACTIVO	AMENAZAS	DESCRIPCIÓN	ORIGEN DE LA AMENAZA	ORIGEN DE LA AMENAZA (Clasificación Según Magerit)	IMPACTO Y DEGRADACIÒN DEL ACTIVO			PROBABILIDAD DE OCURRENCIA	DISPONIBILIDAD EN EL TIEMPO				
					CONFIDENCIALIDAD [C]	INTEGRIDAD [I]	DISPONIBILIDAD [D]		> A 8 HORAS	> 1 DIA	> 3 DIAS	> 8 DIAS	> 1 MES
	Fallas de funcionamiento en el servidor por defectos en el software.	Una mala configuración del software del servidor puede generar fallas en el funcionamiento del mismo.	Software no licenciado, mala configuración del software instalado, bajo nivel de actualizaciones de software.	5.3.4. (E4) Errores de Configuración.	Media	Alta	Alta	1/100 - Muy Poco Frecuente	Baja	Baja	Media	Alta	Muy Alta
	Fallas en el funcionamiento del servidor por el hardware.	Desperfectos en el hardware o mala configuración al momento de ensamblar el servidor ocasionara fallas en el funcionamiento del mismo.	Mala configuración del hardware, bajo nivel de compatibilidad de partes.	5.3.4. (E4) Errores de Configuración. 5.3.5. (E.7) Deficiencia en la Organización.	Muy Baja	Media	Alta	1 - Normal	Baja	Baja	Media	Alta	Muy Alta
	Fallas en el funcionamiento por cortes del suministro eléctrico	La ausencia de energía eléctrica o cortes repentinos en el servicio de fluido eléctrico ocasiona apagones inesperados de los equipos tecnológicos y servidores, afectando la disponibilidad del servicio.	Entorno (Accidental) Humano (Accidental o delibrado)	5.2.3. (I. *) Desastres Industriales.	Muy Baja	Baja	Alta	1/100 - Muy Poco Frecuente	Baja	Baja	Media	Alta	Muy Alta
	Accesos no autorizados al servidor.	Ataques de hacker ocasionando accesos no autorizados al servidor, suplantación de identidad, o aplicación de ingeniería social para obtener contraseñas y usuarios y as acceder al servidor y ocasionar daños al	Bajo nivel de control de accesos, No existencia de políticas de seguridad de la información.	5.4.3. (A.5) Suplantación de la identidad del usuario. 5.4.9. (A.11) Acceso no autorizado.	Alta	Alta	Media	1/10 - Poco Frecuente	Baja	Baja	Media	Alta	Muy Alta

ACTIVO	AMENAZAS	DESCRIPCIÓN	ORIGEN DE LA AMENAZA	ORIGEN DE LA AMENAZA (Clasificación Según Magerit)	IMPACTO Y DEGRADACIÒN DEL ACTIVO			PROBABILIDAD DE OCURRENCIA	DISPONIBILIDAD EN EL TIEMPO				
					CONFIDENCIALIDAD [C]	INTEGRIDAD [I]	DISPONIBILIDAD [D]		> A 8 HORAS	> 1 DIA	> 3 DIAS	> 8 DIAS	> 1 MES
		sistema.											
	Ataque de virus.	Disminución de controles de seguridad con antivirus a los servidores, o antivirus desactualizados lo que puede ocasionar el aprovechamiento de vulnerabilidades.	Antivirus desactualizados o inactivos o equipos no protegidos con antivirus.	5.3.14. (E.21) Errores de mantenimiento /Actualización de programas (software).	Media	Media	Media	1/10 - Poco Frecuente	Baja	Baja	Media	Alta	Muy Alta
	Ataques de denegación de servicio.	Ataques de hacker ocasionando ataques de denegación de servicios, por falta de controles que identifiquen y protejan al sistema de intrusos.	Falta de controles de seguridad, detección y protección de intrusos.	5.4.3. (A.5) Suplantación de la identidad del usuario. 5.4.9. (A.11) Acceso no autorizado.	Baja	Baja	Alta	1/10 - Poco Frecuente	Baja	Baja	Media	Alta	Muy Alta
SERVIDOR DE APLICACIONES WEB (SISTEMA DE INFORMACIÒN DE GESTIÒN DOCUMENTAL Y BASE DE DATOS)	Sobrecalentamiento e incendio de equipos por deficiencia en la aclimatación ambiental del servidor.	Incendios por sobre-calentamiento en el hardware de procesamiento, memoria o disco duro por exceso de altas temperaturas de forma prolongada y sin control. El fuego se puede propagar causando daños irreversibles en los equipos y en la información.	Bajo nivel de revisión y controles de temperatura en la sala de servidores.	5.2.1. (I.1) Fuego	Muy Baja	Alta	Alta	1/100 - Muy Poco Frecuente	Baja	Baja	Media	Alta	Muy Alta
	Incendio deliberado por personal interno o	Personas que acceden a las áreas restringidas sin control alguno y producen fuego ocasionando daños en los	Entorno (Accidental) Humano (Accidental o	5.3. (E) Errores de los usuarios 5.4.3. (A.5)	Muy Baja	Alta	Alta	1/100 - Muy Poco Frecuente	Baja	Baja	Media	Alta	Muy Alta

ACTIVO	AMENAZAS	DESCRIPCIÓN	ORIGEN DE LA AMENAZA	ORIGEN DE LA AMENAZA (Clasificación Según Magerit)	IMPACTO Y DEGRADACIÒN DEL ACTIVO			PROBABILIDAD DE OCURRENCIA	DISPONIBILIDAD EN EL TIEMPO				
					CONFIDENCIALIDAD [C]	INTEGRIDAD [I]	DISPONIBILIDAD [D]		> A 8 HORAS	> 1 DIA	> 3 DIAS	> 8 DIAS	> 1 MES
	externo de la Corporación.	equipos.	delibrado)	Suplantación de la identidad del usuario. 5.4.9. (A.11) Acceso no autorizado.									
	Daños en la estructura del servidor por caída de concreto y hierro reforzado por temblor (Desastre Natural)	Por desastre natural, temblor o terremoto se puede caer la infraestructura del edificio y dañar los equipos servidores.	Desastre Natural	5.1.3. 8N.*) Desastres Naturales.	Muy Baja	Alta	Alta	1/100 - Muy Poco Frecuente	Baja	Baja	Media	Alta	Muy Alta
	Daños en el servidor por sobrecargas de alto voltaje eléctrico en el mismo.	La corriente eléctrica es muy variable en Yopal, por lo cual al no contar con buena protección de supresor de picos y regulación de voltaje, los equipos se pueden quemar o sufrir daños.	Bajo nivel de protección de los equipos con supresor de picos de corriente eléctrica.	5.2.3. (I. *) Desastres Industriales.	Muy Baja	Alta	Alta	1/10 - Poco Frecuente	Baja	Baja	Media	Alta	Muy Alta
	Fallas de funcionamiento en el servidor por defectos en el software.	Una mala configuración del software del servidor puede generar fallas en el funcionamiento del mismo.	Software no licenciado, mala configuración del software instalado, bajo nivel de actualizaciones de software.	5.3.4. (E4) Errores de Configuración.	Media	Alta	Alta	1/100 - Muy Poco Frecuente	Baja	Baja	Media	Alta	Muy Alta

ACTIVO	AMENAZAS	DESCRIPCIÓN	ORIGEN DE LA AMENAZA	ORIGEN DE LA AMENAZA (Clasificación Según Magerit)	IMPACTO Y DEGRADACIÒN DEL ACTIVO			PROBABILIDAD DE OCURRENCIA	DISPONIBILIDAD EN EL TIEMPO				
					CONFIDENCIALIDAD [C]	INTEGRIDAD [I]	DISPONIBILIDAD [D]		> A 8 HORAS	> 1 DIA	> 3 DIAS	> 8 DIAS	> 1 MES
	Fallas en el funcionamiento del servidor por el hardware.	Desperfectos en el hardware o mala configuración al momento de ensamblar el servidor ocasionara fallas en el funcionamiento del mismo.	Mala configuración del hardware, bajo nivel de compatibilidad de partes.	5.3.4. (E4) Errores de Configuración .5.3.5. (E.7) Deficiencia en la Organización.	Muy Baja	Media	Alta	1 - Normal	Baja	Baja	Media	Alta	Muy Alta
	Fallas en el funcionamiento por cortes del suministro eléctrico	La ausencia de energía eléctrica o cortes repentinos en el servicio de fluido eléctrico ocasiona apagones inesperados de los equipos tecnológicos y servidores, afectando la disponibilidad del servicio.	Entorno (Accidental) Humano (Accidental o delibrado)	5.2.3. (I. *) Desastres Industriales.	Muy Baja	Baja	Alta	1/100 - Muy Poco Frecuente	Baja	Baja	Media	Alta	Muy Alta
	Accesos no autorizados al servidor.	Ataques de hacker ocasionando accesos no autorizados al servidor, suplantación de identidad, o aplicación de ingeniería social para obtener contraseñas y usuarios y as acceder al servidor y ocasionar daños al sistema.	Bajo nivel de control de accesos, No existencia de políticas de seguridad de la información.	5.4.3. (A.5) Suplantación de la identidad del usuario. 5.4.9. (A.11) Acceso no autorizado.	Alta	Alta	Media	1/10 - Poco Frecuente	Baja	Baja	Media	Alta	Muy Alta
	Ataque de virus.	Disminución de controles de seguridad con antivirus a los servidores, o antivirus desactualizados lo que puede ocasionar el aprovechamiento de vulnerabilidades.	Antivirus desactualizados o inactivos o equipos no protegidos con antivirus.	5.3.14. (E.21) Errores de mantenimiento /Actualización de programas (software).	Media	Media	Media	1/10 - Poco Frecuente	Baja	Baja	Media	Alta	Muy Alta

ACTIVO	AMENAZAS	DESCRIPCIÓN	ORIGEN DE LA AMENAZA	ORIGEN DE LA AMENAZA (Clasificación Según Magerit)	IMPACTO Y DEGRADACIÒN DEL ACTIVO			PROBABILIDAD DE OCURRENCIA	DISPONIBILIDAD EN EL TIEMPO				
					CONFIDENCIALIDAD [C]	INTEGRIDAD [I]	DISPONIBILIDAD [D]		> A 8 HORAS	> 1 DIA	> 3 DIAS	> 8 DIAS	> 1 MES
	Ataques de denegación de servicio.	Ataques de hacker ocasionando ataques de denegación de servicios, por falta de controles que identifiquen y protejan al sistema de intrusos.	Falta de controles de seguridad, detección y protección de intrusos.	5.4.3. (A.5) Suplantación de la identidad del usuario. 5.4.9. (A.11) Acceso no autorizado.	Baja	Baja	Alta	1/10 - Poco Frecuente	Baja	Baja	Media	Alta	Muy Alta
SERVIDOR DE APLICACIONES - SISTEMA DE INFORMACIÒN GEOGRAFICO - SIGCOR.	Sobrecalentamiento e incendio de equipos por deficiencia en la aclimatación ambiental del servidor.	Incendios por sobre-calentamiento en el hardware de procesamiento, memoria o disco duro por exceso de altas temperaturas de forma prolongada y sin control. El fuego se puede propagar causando daños irreversibles en los equipos y en la información.	Bajo nivel de revisión y controles de temperatura en la sala de servidores.	5.2.1. (I.1) Fuego	Muy Baja	Alta	Alta	1/100 - Muy Poco Frecuente	Baja	Baja	Media	Alta	Muy Alta
	Incendio deliberado por personal interno o externo de la Corporación.	Personas que acceden a las áreas restringidas sin control alguno y producen fuego ocasionando daños en los equipos.	Entorno (Accidental) Humano (Accidental o delibrado)	5.3. (E) Errores de los usuarios 5.4.3. (A.5) Suplantación de la identidad del usuario. 5.4.9. (A.11) Acceso no autorizado.	Muy Baja	Alta	Alta	1/100 - Muy Poco Frecuente	Baja	Baja	Media	Alta	Muy Alta

ACTIVO	AMENAZAS	DESCRIPCIÓN	ORIGEN DE LA AMENAZA	ORIGEN DE LA AMENAZA (Clasificación Según Magerit)	IMPACTO Y DEGRADACIÒN DEL ACTIVO			PROBABILIDAD DE OCURRENCIA	DISPONIBILIDAD EN EL TIEMPO				
					CONFIDENCIALIDAD [C]	INTEGRIDAD [I]	DISPONIBILIDAD [D]		> A 8 HORAS	> 1 DIA	> 3 DIAS	> 8 DIAS	> 1 MES
	Daños en la estructura del servidor por caída de concreto y hierro reforzado por temblor (Desastre Natural)	Por desastre natural, temblor o terremoto se puede caer la infraestructura del edificio y dañar los equipos servidores.	Desastre Natural	5.1.3. 8N.*) Desastres Naturales.	Muy Baja	Alta	Alta	1/100 - Muy Poco Frecuente	Baja	Baja	Media	Alta	Muy Alta
	Daños en el servidor por sobrecargas de alto voltaje eléctrico en el mismo.	La corriente eléctrica es muy variable en Yopal, por lo cual al no contar con buena protección de supresor de picos y regulación de voltaje, los equipos se pueden quemar o sufrir daños.	Bajo nivel de protección de los equipos con supresor de picos de corriente eléctrica.	5.2.3. (I. *) Desastres Industriales.	Muy Baja	Alta	Alta	1/10 - Poco Frecuente	Baja	Baja	Media	Alta	Muy Alta
	Fallas de funcionamiento en el servidor por defectos en el software.	Una mala configuración del software del servidor puede generar fallas en el funcionamiento del mismo.	Software no licenciado, mala configuración del software instalado, bajo nivel de actualizaciones de software.	5.3.4. (E4) Errores de Configuración.	Media	Alta	Alta	1/100 - Muy Poco Frecuente	Baja	Baja	Media	Alta	Muy Alta
	Fallas en el funcionamiento del servidor por el hardware.	Desperfectos en el hardware o mala configuración al momento de ensamblar el servidor ocasionara fallas en el funcionamiento del mismo.	Mala configuración del hardware, bajo nivel de compatibilidad de partes.	5.3.4. (E4) Errores de Configuración .5.3.5. (E.7) Deficiencia en la Organización.	Muy Baja	Media	Alta	1 - Normal	Baja	Baja	Media	Alta	Muy Alta

ACTIVO	AMENAZAS	DESCRIPCIÓN	ORIGEN DE LA AMENAZA	ORIGEN DE LA AMENAZA (Clasificación Según Magerit)	IMPACTO Y DEGRADACIÒN DEL ACTIVO			PROBABILIDAD DE OCURRENCIA	DISPONIBILIDAD EN EL TIEMPO				
					CONFIDENCIALIDAD [C]	INTEGRIDAD [I]	DISPONIBILIDAD [D]		> A 8 HORAS	> 1 DIA	> 3 DIAS	> 8 DIAS	> 1 MES
	Fallas en el funcionamiento por cortes del suministro eléctrico	La ausencia de energía eléctrica o cortes repentinos en el servicio de fluido eléctrico ocasiona apagones inesperados de los equipos tecnológicos y servidores, afectando la disponibilidad del servicio.	Entorno (Accidental) Humano (Accidental o delibrado)	5.2.3. (I. *) Desastres Industriales.	Muy Baja	Baja	Alta	1/100 - Muy Poco Frecuente	Baja	Baja	Media	Alta	Muy Alta
	Accesos no autorizados al servidor.	Ataques de hacker ocasionando accesos no autorizados al servidor, suplantación de identidad, o aplicación de ingeniería social para obtener contraseñas y usuarios y as acceder al servidor y ocasionar daños al sistema.	Bajo nivel de control de accesos, No existencia de políticas de seguridad de la información.	5.4.3. (A.5) Suplantación de la identidad del usuario. 5.4.9. (A.11) Acceso no autorizado.	Alta	Alta	Media	1/10 - Poco Frecuente	Baja	Baja	Media	Alta	Muy Alta
	Ataque de virus.	Disminución de controles de seguridad con antivirus a los servidores, o antivirus desactualizados lo que puede ocasionar el aprovechamiento de vulnerabilidades.	Antivirus desactualizados o inactivos o equipos no protegidos con antivirus.	5.3.14. (E.21) Errores de mantenimiento /Actualización de programas (software).	Media	Media	Media	1/10 - Poco Frecuente	Baja	Baja	Media	Alta	Muy Alta
	Ataques de denegación de servicio.	Ataques de hacker ocasionando ataques de denegación de servicios, por falta de controles que identifiquen y protejan al sistema de intrusos.	Falta de controles de seguridad, detección y protección de intrusos.	5.4.3. (A.5) Suplantación de la identidad del usuario. 5.4.9. (A.11) Acceso no	Baja	Baja	Alta	1/10 - Poco Frecuente	Baja	Baja	Media	Alta	Muy Alta

ACTIVO	AMENAZAS	DESCRIPCIÓN	ORIGEN DE LA AMENAZA	ORIGEN DE LA AMENAZA (Clasificación Según Magerit)	IMPACTO Y DEGRADACIÒN DEL ACTIVO			PROBABILIDAD DE OCURRENCIA	DISPONIBILIDAD EN EL TIEMPO				
					CONFIDENCIALIDAD [C]	INTEGRIDAD [I]	DISPONIBILIDAD [D]		> A 8 HORAS	> 1 DIA	> 3 DIAS	> 8 DIAS	> 1 MES
				autorizado.									
SISTEMA DE INFORMACIÓN FINANCIERO	Accesos no autorizados al Sistema de Información y escalamiento de privilegios.	Hackers o usuarios que intentan ingresar al sistema sin la autorización respectiva, con el fin de realizar ataques a la confidencialidad, integridad o disponibilidad de la información financiera.	No existencia de política de seguridad para el control de accesos.	5.3.5. (E. 7) Deficiencias en la Organización. 5.4.9. (A.11) Acceso no autorizado.	Alta	Alta	Media	1/10 - Poco Frecuente					
	Ataques de denegación de servicio.	Hackers o usuarios que atacan el sistema o generan bucles de peticiones al sistema hasta hacerlo colapsar.	Falta de controles de seguridad, detección y protección de intrusos.	5.3.5. (E. 7) Deficiencias en la Organización. 5.4.9. (A.11) Acceso no autorizado.	Baja	Media	Alta	1/10 - Poco Frecuente	Baja	Baja	Media	Alta	Muy Alta
	Ataques de SQL Injection	Hackers o usuarios que atacan el sistema con código SQL Injection para robar información y causar daños en el sistema.	Ataque de Hacker o personal con conocimiento en este tipo de ataques.	5.3.5. (E. 7) Deficiencias en la Organización. 5.4.9. (A.11) Acceso no autorizado.	Alta	Media	Media	1/10 - Poco Frecuente					
PAGINA WEB CORPORINOQUIA	Accesos no autorizados al Sitio Web y escalamiento de privilegios.	Hackers o usuarios que intentan ingresar al sistema sin la autorización respectiva, con el fin de realizar ataques a la confidencialidad, integridad o disponibilidad de la información financiera.	No existencia de política de seguridad para el control de accesos.	5.3.5. (E. 7) Deficiencias en la Organización. 5.4.9. (A.11) Acceso no autorizado.	Alta	Alta	Media	1/10 - Poco Frecuente					

ACTIVO	AMENAZAS	DESCRIPCIÓN	ORIGEN DE LA AMENAZA	ORIGEN DE LA AMENAZA (Clasificación Según Magerit)	IMPACTO Y DEGRADACIÒN DEL ACTIVO			PROBABILIDAD DE OCURRENCIA	DISPONIBILIDAD EN EL TIEMPO				
					CONFIDENCIALIDAD [C]	INTEGRIDAD [I]	DISPONIBILIDAD [D]		> A 8 HORAS	> 1 DIA	> 3 DIAS	> 8 DIAS	> 1 MES
	Ataques de denegación de servicio.	Hackers o usuarios que atacan el sistema o generan bucles de peticiones al sistema hasta hacerlo colapsar.	Falta de controles de seguridad, detección y protección de intrusos.	5.3.5. (E. 7) Deficiencias en la Organización. 5.4.9. (A.11) Acceso no autorizado.	Baja	Media	Alta	1/10 - Poco Frecuente	Baja	Baja	Media	Alta	Muy Alta
	Ataques de SQL Injection	Hackers o usuarios que atacan el sistema con código SQL Injection para robar información y causar daños en el sistema.	Ataque de Hacker o personal con conocimiento en este tipo de ataques.	5.3.5. (E. 7) Deficiencias en la Organización. 5.4.9. (A.11) Acceso no autorizado.	Alta	Media	Media	1/10 - Poco Frecuente					
SISTEMA DE INFORMACIÓN DE GESTIÓN DOCUMENTAL	Accesos no autorizados al Sistema de Información y escalamiento de privilegios.	Hackers o usuarios que intentan ingresar al sistema sin la autorización respectiva, con el fin de realizar ataques a la confidencialidad, integridad o disponibilidad de la información financiera.	No existencia de política de seguridad para el control de accesos.	5.3.5. (E. 7) Deficiencias en la Organización. 5.4.9. (A.11) Acceso no autorizado.	Alta	Alta	Media	1/10 - Poco Frecuente					
	Ataques de denegaciòn de servicio.	Hackers o usuarios que atacan el sistema o generan bucles de peticiones al sistema hasta hacerlo colapsar.	Falta de controles de seguridad, detección y protección de intrusos.	5.3.5. (E. 7) Deficiencias en la Organización. 5.4.9. (A.11) Acceso no autorizado.	Baja	Media	Alta	1/10 - Poco Frecuente	Baja	Baja	Media	Alta	Muy Alta

ACTIVO	AMENAZAS	DESCRIPCIÓN	ORIGEN DE LA AMENAZA	ORIGEN DE LA AMENAZA (Clasificación Según Magerit)	IMPACTO Y DEGRADACIÒN DEL ACTIVO			PROBABILIDAD DE OCURRENCIA	DISPONIBILIDAD EN EL TIEMPO				
					CONFIDENCIALIDAD [C]	INTEGRIDAD [I]	DISPONIBILIDAD [D]		> A 8 HORAS	> 1 DIA	> 3 DIAS	> 8 DIAS	> 1 MES
	Ataques de SQL Injection	Hackers o usuarios que atacan el sistema con código SQL Injection para robar información y causar daños en el sistema.	Ataque de Hacker o personal con conocimiento en este tipo de ataques.	5.3.5. (E. 7) Deficiencias en la Organización. 5.4.9. (A.11) Acceso no autorizado.	Alta	Media	Media	1/10 - Poco Frecuente					
CORREO ELECTRONICO CORPORATIVO	Ataque de denegación de servicio.	Hackers o usuarios que atacan el sistema o generan bucles de peticiones al sistema hasta hacerlo colapsar.	Falta de controles de seguridad, detección y protección de intrusos.	5.3.5. (E. 7) Deficiencias en la Organización. 5.4.9. (A.11) Acceso no autorizado.	Baja	Media	Alta	1/10 - Poco Frecuente	Baja	Baja	Media	Alta	Muy Alta
	Caídas del servicio de Correo por bajo nivel de espacio de almacenamiento.	Corporinoquia cuenta con un hosting de 50 GB y los correos de directivos deben trabajarlos por el protocolo IMAP, en algunos casos el sistema se cae por que el espacio de almacenamiento se llena y colapsa.	Incremento de cuentas de correo. Bajo espacio en el disco de gestión y administración del correo corporativo (hosting).	5.2.6. (I.5) Avería de origen físico o lógico.	Muy Baja	Muy Baja	Alta	10 - Frecuente	Media	Media	Alta	Muy Alta	Muy Alta
	Accesos no autorizados a la administración del servidor de correo electrónico.	Ataques de hacker ocasionando accesos no autorizados al servidor de correo o a las cuentas de correo, suplantación de identidad, o aplicación de ingeniería social para obtener contraseñas y usuarios y as acceder al servidor y	No existencia de política de seguridad para el control de accesos.	5.3.5. (E. 7) Deficiencias en la Organización. 5.4.9. (A.11) Acceso no autorizado.	Alta	Alta	Media	1/10 - Poco Frecuente					

ACTIVO	AMENAZAS	DESCRIPCIÓN	ORIGEN DE LA AMENAZA	ORIGEN DE LA AMENAZA (Clasificación Según Magerit)	IMPACTO Y DEGRADACIÒN DEL ACTIVO			PROBABILIDAD DE OCURRENCIA	DISPONIBILIDAD EN EL TIEMPO				
					CONFIDENCIALIDAD [C]	INTEGRIDAD [I]	DISPONIBILIDAD [D]		> A 8 HORAS	> 1 DIA	> 3 DIAS	> 8 DIAS	> 1 MES
		ocasionar daños al sistema.											
	Suplantación de correos electrónicos.	Suplantación de correos, ataques de hombre en medio a través de la interceptación de mensaje de correo y entregando correos modificados, o eliminando los mismos para que no lleguen a su destino.	Falta de controles de seguridad, detección y protección de intrusos.	5.3.5. (E. 7) Deficiencias en la Organización. 5.4.9. (A.11) Acceso no autorizado.	Media	Media	Baja	1/10 - Poco Frecuente					
SAN - STORAGE AREA NETWORK.	Cese de capacidad de transmitir datos para consulta y guardado de información a los usuarios y el sistema.	Mala configuración y conexión de cableado a los equipos de administración de la información.	Configuración errónea de la SAN.	5.3.4. (E.4) Errores de Configuración.	Baja	Baja	Alta	1/10 - Poco Frecuente	Baja	Baja	Media	Alta	Muy Alta
	Fallas en el hardware de almacenamiento por falta de mantenimiento, sobrecalentamiento e incendio por deficiencia en la aclimatación ambiental.	Fallas de la SAN, por falta de mantenimiento preventivo y correctivo en el paso del tiempo.	Bajo nivel de mantenimiento de la SAN.	5.3.5. (E.7) Deficiencias en la Organización. 5.3.15. (E.23) Errores de Mantenimiento /Actualización de equipos (Hardware).	Baja	Media	Alta	1/10 - Poco Frecuente					

ACTIVO	AMENAZAS	DESCRIPCIÓN	ORIGEN DE LA AMENAZA	ORIGEN DE LA AMENAZA (Clasificación Según Magerit)	IMPACTO Y DEGRADACIÒN DEL ACTIVO			PROBABILIDAD DE OCURRENCIA	DISPONIBILIDAD EN EL TIEMPO				
					CONFIDENCIALIDAD [C]	INTEGRIDAD [I]	DISPONIBILIDAD [D]		> A 8 HORAS	> 1 DIA	> 3 DIAS	> 8 DIAS	> 1 MES
	Daño lógico por la configuración de la SAN.	Mala configuración del software que administra la SAN y la información almacenada.	Configuración errónea de la SAN.	5.3.4. (E.4) Errores de Configuración.	Baja	Alta	Alta	1/10 - Poco Frecuente	Baja	Baja	Media	Alta	Muy Alta
UPS RACK DE SERVIDOR PRINCIPAL - 6 KVA - CENTRO DE DATOS	Fallas en el sistema de UPS por baterías en mal estado de funcionamiento.	Mal funcionamiento de las UPS por baterías en mal estado, esto tiende a que no haya disponibilidad del servicio de la UPS al momento de requerirse.	Falta de verificación de alertas de la UPS. Falta de mantenimiento preventivo y correctivo de la UPS.	5.3.15. (E.23) Errores de Mantenimiento /Actualización de equipos (Hardware).	Baja	Media	Alta	10 - Frecuente	Media	Media	Alta	Alta	Muy Alta
	Fallas o daños por voltaje excesivo en la ups que protege el servidor.	La variación del fluido eléctrico ocasiona daños en los resistores eléctricos de la UPS, ocasionando daños en la tarjeta de administración de UPS, y ocasionando daños en las baterías, lo que dificulta la respuesta de las mismas al momento de requerirse.	Ausencia de supresor de picos eléctricos que salvaguardan a las UPS.	5.2.3. (I.*) Desastres Industriales. 5.2.7. (I.6) Corte del Suministro Eléctrico.	Baja	Media	Alta	1/10 - Poco Frecuente	Media	Alta	Alta	Alta	Muy Alta
	Mal funcionamiento por falta de mantenimiento.	Al no programar el mantenimiento de la UPS, ni tener controles que indiquen las posibles fallas que se pueden presentar, la UPS tiende a colapsar y no brindar el servicio en el momento requerido.	No realización de mantenimiento de UPS.	5.3.15. (E.23) Errores de Mantenimiento /Actualización de equipos (Hardware).	Baja	Baja	Alta	1/10 - Poco Frecuente	Media	Alta	Alta	Alta	Muy Alta

ACTIVO	AMENAZAS	DESCRIPCIÓN	ORIGEN DE LA AMENAZA	ORIGEN DE LA AMENAZA (Clasificación Según Magerit)	IMPACTO Y DEGRADACIÒN DEL ACTIVO			PROBABILIDAD DE OCURRENCIA	DISPONIBILIDAD EN EL TIEMPO				
					CONFIDENCIALIDAD [C]	INTEGRIDAD [I]	DISPONIBILIDAD [D]		> A 8 HORAS	> 1 DIA	> 3 DIAS	> 8 DIAS	> 1 MES
RACK PRINCIPAL DE COMUNICACIONES - CENTRAL DE DATOS.	Perdida de estabilidad y robustez del rack principal por mal armado en su estructura.	Posibles caídas de equipos empotrados en el rack de comunicaciones por mala configuración, mal ajuste de tornillos y demás elementos que componen la estructura del mismo.	Personal no capacitado para armar estructurar de rack y redes de datos.	5.3.4. (E.4) Errores de Configuración.	Baja	Baja	Media	1/10 - Poco Frecuente	Muy Baja	Baja	Baja	Media	Media
	Daños causados por manipulación y accesos de personal no autorizado.	Personas ajenas a la organización o no autorizadas para la manipulación de los equipos del área ingresan sin autorización y ocasionan daños en el rack de comunicaciones.	Ausencia de control de accesos a personal no autorizado en manipulación del rack de comunicaciones	5.4.9. (A.11) Acceso no Autorizado. 5.4.2. (A.4) Manipulación de la Configuración.	Baja	Baja	Media	1/10 - Poco Frecuente	Muy Baja	Baja	Baja	Media	Media
SWITCH CORE 24 PUERTOS - 10/100/1000 - CENTRO DE DATOS.	Fallas en el hardware por falta de mantenimiento, sobrecalentamiento y/o incendio por deficiencia en la aclimatación ambiental.	Fallas de los switch por sobrecalentamiento, al no existir o funcionar el servicio de aire acondicionados o regulación de la temperatura en los cuartos de equipos switch`s.	Falta de mantenimiento de Switch. Ausencia de equipos reguladores de temperatura ambiente en las zonas de ubicación de rack de switch`s.	5.3.15. (E.23) Errores de Mantenimiento /Actualización de equipos (Hardware). 5.2.8. (I.7) Condiciones inadecuadas de temperatura o humedad.	Baja	Media	Muy Alta	1/100 - Muy Poco Frecuente	Media	Media	Alta	Muy Alta	Muy Alta
	Interrupción del servicio causado por	Las áreas de central de datos no se encuentran debidamente aseguradas,	Ausencia de política de seguridad en lo	5.3.5. (E. 7) Deficiencias en la	Media	Media	Alta	1/10 - Poco Frecuente	Media	Media	Alta	Muy Alta	Muy Alta

ACTIVO	AMENAZAS	DESCRIPCIÓN	ORIGEN DE LA AMENAZA	ORIGEN DE LA AMENAZA (Clasificación Según Magerit)	IMPACTO Y DEGRADACIÒN DEL ACTIVO			PROBABILIDAD DE OCURRENCIA	DISPONIBILIDAD EN EL TIEMPO				
					CONFIDENCIALIDAD [C]	INTEGRIDAD [I]	DISPONIBILIDAD [D]		> A 8 HORAS	> 1 DIA	> 3 DIAS	> 8 DIAS	> 1 MES
	manipulación física realizada a los switch´s por personal no autorizado.	permitiendo el acceso a personal no autorizado a manipular los switchs y demás equipos ocasionando fallos y cortes en los servicios tecnológicos de la red de datos.	relacionado con el control de accesos a operatividad de switchs.	Organización. 5.4.9. (A.11) Acceso no autorizado.									
	Mal funcionamiento por falta de mantenimiento.	No planificación de mantenimiento preventivo de switchs. No realización del mantenimiento de los switch ocasionando fallas en su funcionamiento normal.	Ausencia de política de seguridad en lo relacionado con la programación y gestión de mantenimiento preventivo.	5.3.15. (E.23) Errores de Mantenimiento /Actualización de equipos (Hardware).	Baja	Media	Alta	1/10 - Poco Frecuente	Media	Media	Alta	Muy Alta	Muy Alta
	Denegación del servicio por accesos lógicos no autorizados a los switch´s.	Ataques de hackers a la red de datos y administración de switch y denegar el servicio de red a los usuarios de la misma.	Ausencia de política de seguridad en lo relacionado con gestión y control de accesos.	5.3.5. (E. 7) Deficiencias en la Organización. 5.4.9. (A.11) Acceso no autorizado.	Baja	Baja	Muy Alta	1/10 - Poco Frecuente	Media	Media	Alta	Muy Alta	Muy Alta
	Fallas por interrupciones del servicio eléctrico.	Ausencia de energía eléctrica y nula respuesta de equipos UPS ocasionando fallas en el funcionamiento de los Switch`s.	Ausencia de Procedimientos y mecanismos de activación de energía ante fallos de energía externa.	5.3.5. (E. 7) Deficiencias en la Organización. 5.2.7. (I.6) Corte del Suministro Eléctrico.	Baja	Baja	Muy Alta	1/10 - Poco Frecuente	Media	Media	Alta	Muy Alta	Muy Alta

ACTIVO	AMENAZAS	DESCRIPCIÓN	ORIGEN DE LA AMENAZA	ORIGEN DE LA AMENAZA (Clasificación Según Magerit)	IMPACTO Y DEGRADACIÒN DEL ACTIVO			PROBABILIDAD DE OCURRENCIA	DISPONIBILIDAD EN EL TIEMPO				
					CONFIDENCIALIDAD [C]	INTEGRIDAD [I]	DISPONIBILIDAD [D]		> A 8 HORAS	> 1 DIA	> 3 DIAS	> 8 DIAS	> 1 MES
SWITCH 48 PUERTOS - 10/100/1000 - CENTRO DE DATOS	Fallas en el hardware por falta de mantenimiento, sobrecalentamiento y/o incendio por deficiencia en la aclimatación ambiental.	Fallas de los switch por sobrecalentamiento, al no existir o funcionar el servicio de aire acondicionados o regulación de la temperatura en los cuartos de equipos switch`s.	Falta de mantenimiento de Switch. Ausencia de equipos reguladores de temperatura ambiente en las zonas de ubicación de rack de switch`s.	5.2.8. (I.7) Condiciones inadecuadas de temperatura o humedad. 5.3.15. (E.23) Errores de Mantenimiento /Actualización de equipos (Hardware).	Baja	Media	Muy Alta	1/100 - Muy Poco Frecuente	Media	Media	Alta	Muy Alta	Muy Alta
	Interrupción del servicio causado por manipulación física realizada a los switch´s por personal no autorizado.	Las áreas de central de datos no se encuentran debidamente aseguradas, permitiendo el acceso a personal no autorizado a manipular los switchs y demás equipos ocasionando fallos y cortes en los servicios tecnológicos de la red de datos.	Ausencia de política de seguridad en lo relacionado con el control de accesos a operatividad de switchs.	5.3.5. (E. 7) Deficiencias en la Organización. 5.4.9. (A.11) Acceso no autorizado.	Media	Media	Alta	1/10 - Poco Frecuente	Media	Media	Alta	Muy Alta	Muy Alta
	Mal funcionamiento por falta de mantenimiento.	No planificación de mantenimiento preventivo de switchs. No realización del mantenimiento de los switch ocasionando fallas en su funcionamiento normal.	Ausencia de política de seguridad en lo relacionado con la programación y gestión de mantenimiento preventivo.	5.3.15. (E.23) Errores de Mantenimiento /Actualización de equipos (Hardware).	Baja	Media	Alta	1/10 - Poco Frecuente	Media	Media	Alta	Muy Alta	Muy Alta

ACTIVO	AMENAZAS	DESCRIPCIÓN	ORIGEN DE LA AMENAZA	ORIGEN DE LA AMENAZA (Clasificación Según Magerit)	IMPACTO Y DEGRADACIÒN DEL ACTIVO			PROBABILIDAD DE OCURRENCIA	DISPONIBILIDAD EN EL TIEMPO				
					CONFIDENCIALIDAD [C]	INTEGRIDAD [I]	DISPONIBILIDAD [D]		> A 8 HORAS	> 1 DIA	> 3 DIAS	> 8 DIAS	> 1 MES
	Denegación del servicio por accesos lógicos no autorizados a los switch´s.	Ataques de hackers a la red de datos y administración de switch y denegar el servicio de red a los usuarios de la misma.	Ausencia de política de seguridad en lo relacionado con gestión y control de accesos.	5.3.5. (E. 7) Deficiencias en la Organización. 5.4.9. (A.11) Acceso no autorizado.	Baja	Baja	Muy Alta	1/10 - Poco Frecuente	Media	Media	Alta	Muy Alta	Muy Alta
	Fallas por interrupciones del servicio eléctrico.	Ausencia de energía eléctrica y nula respuesta de equipos UPS ocasionando fallas en el funcionamiento de los Switch`s.	Ausencia de Procedimientos y mecanismos de activación de energía ante fallos de energía externa.	5.2.7. (I.6) Corte del suministro eléctrico.	Baja	Baja	Muy Alta	1/10 - Poco Frecuente	Media	Media	Alta	Muy Alta	Muy Alta
SWITCH 48 PUERTOS - 10/100/1000 - CENTRO DE DATOS	Fallas en el hardware por falta de mantenimiento, sobrecalentamiento y/o incendio por deficiencia en la aclimatación ambiental.	Fallas de los switch por sobrecalentamiento, al no existir o funcionar el servicio de aire acondicionados o regulación de la temperatura en los cuartos de equipos switch`s.	Falta de mantenimiento de Switch. Ausencia de equipos reguladores de temperatura ambiente en las zonas de ubicación de rack de switch`s.	5.2.8. (I.7) Condiciones inadecuadas de temperatura o humedad. 5.3.15. (E.23) Errores de Mantenimiento /Actualización de equipos (Hardware).	Baja	Media	Muy Alta	1/100 - Muy Poco Frecuente	Media	Media	Alta	Muy Alta	Muy Alta

ACTIVO	AMENAZAS	DESCRIPCIÓN	ORIGEN DE LA AMENAZA	ORIGEN DE LA AMENAZA (Clasificación Según Magerit)	IMPACTO Y DEGRADACIÒN DEL ACTIVO			PROBABILIDAD DE OCURRENCIA	DISPONIBILIDAD EN EL TIEMPO				
					CONFIDENCIALIDAD [C]	INTEGRIDAD [I]	DISPONIBILIDAD [D]		> A 8 HORAS	> 1 DIA	> 3 DIAS	> 8 DIAS	> 1 MES
	Interrupción del servicio causado por manipulación física realizada a los switch´s por personal no autorizado.	Las áreas de central de datos no se encuentran debidamente aseguradas, permitiendo el acceso a personal no autorizado a manipular los switchs y demás equipos ocasionando fallos y cortes en los servicios tecnológicos de la red de datos.	Ausencia de política de seguridad en lo relacionado con el control de accesos a operatividad de switchs.	5.3.5. (E. 7) Deficiencias en la Organización. 5.4.9. (A.11) Acceso no autorizado.	Media	Media	Alta	1/10 - Poco Frecuente	Media	Media	Alta	Muy Alta	Muy Alta
	Mal funcionamiento por falta de mantenimiento.	No planificación de mantenimiento preventivo de switchs. No realización del mantenimiento de los switch ocasionando fallas en su funcionamiento normal.	Ausencia de política de seguridad en lo relacionado con la programación y gestión de mantenimiento preventivo.	5.3.15. (E.23) Errores de Mantenimiento /Actualización de equipos (Hardware).	Baja	Media	Alta	1/10 - Poco Frecuente	Media	Media	Alta	Muy Alta	Muy Alta
	Denegación del servicio por accesos lógicos no autorizados a los switch´s.	Ataques de hackers a la red de datos y administración de switch y denegar el servicio de red a los usuarios de la misma.	Ausencia de política de seguridad en lo relacionado con gestión y control de accesos.	5.3.5. (E. 7) Deficiencias en la Organización. 5.4.9. (A.11) Acceso no autorizado.	Baja	Baja	Muy Alta	1/10 - Poco Frecuente	Media	Media	Alta	Muy Alta	Muy Alta

ACTIVO	AMENAZAS	DESCRIPCIÓN	ORIGEN DE LA AMENAZA	ORIGEN DE LA AMENAZA (Clasificación Según Magerit)	IMPACTO Y DEGRADACIÒN DEL ACTIVO			PROBABILIDAD DE OCURRENCIA	DISPONIBILIDAD EN EL TIEMPO				
					CONFIDENCIALIDAD [C]	INTEGRIDAD [I]	DISPONIBILIDAD [D]		> A 8 HORAS	> 1 DIA	> 3 DIAS	> 8 DIAS	> 1 MES
	Fallas por interrupciones del servicio eléctrico.	Ausencia de energía eléctrica y nula respuesta de equipos UPS ocasionando fallas en el funcionamiento de los Switch`s.	Ausencia de Procedimientos y mecanismos de activación de energía ante fallos de energía externa.	5.2.7. (I.6) Corte del suministro eléctrico.	Baja	Baja	Muy Alta	1/10 - Poco Frecuente	Media	Media	Alta	Muy Alta	Muy Alta
RACK SECUNDARIO DE COMUNICACIONES- SUBDIRECCIÒN ADMINISTRATIVA Y FINANCIERA.	Perdida de estabilidad y robustez del rack principal por mala configuración en su estructura.	Posibles caídas de equipos empotrados en el rack de comunicaciones por mala configuración, mal ajuste de tornillos y demás elementos que componen la estructura del mismo.	Personal no capacitado para armar estructurar de rack y redes de datos.	5.3.4. (E.4) Errores de Configuración.	Baja	Media	Alta	1/10 - Poco Frecuente	Media	Alta	Alta	Alta	Muy Alta
	Daños causados por manipulación y accesos de personal no autorizado.	Personas ajenas a la organización o no autorizadas para la manipulación de los equipos del área ingresan sin autorización y ocasionan daños en el rack de comunicaciones.	Ausencia de control de accesos a personal no autorizado en manipulación del rack de comunicaciones	5.3.5. (E. 7) Deficiencias en la Organización. 5.4.9. (A.11) Acceso no autorizado.	Baja	Baja	Alta	1/10 - Poco Frecuente	Media	Alta	Alta	Alta	Muy Alta
SWITCH CORE 24 PUERTOS - 10/100/1000 - SUBDIRECCIÒN ADMINIS	Fallas en el hardware por falta de mantenimiento, sobrecalentamiento y/o incendio por deficiencia en la aclimatación	Fallas de los switch por sobrecalentamiento, al no existir o funcionar el servicio de aire acondicionados o regulación de la temperatura en los cuartos de equipos switch`s.	Falta de mantenimiento de Switch. Ausencia de equipos reguladores de temperatura ambiente en las zonas de ubicación	5.2.8. (I.7) Condiciones inadecuadas de temperatura o humedad. 5.3.15. (E.23) Errores de Mantenimient	Baja	Media	Muy Alta	1/100 - Muy Poco Frecuente	Media	Media	Alta	Muy Alta	Muy Alta

ACTIVO	AMENAZAS	DESCRIPCIÓN	ORIGEN DE LA AMENAZA	ORIGEN DE LA AMENAZA (Clasificación Según Magerit)	IMPACTO Y DEGRADACIÒN DEL ACTIVO			PROBABILIDAD DE OCURRENCIA	DISPONIBILIDAD EN EL TIEMPO				
					CONFIDENCIALIDAD [C]	INTEGRIDAD [I]	DISPONIBILIDAD [D]		> A 8 HORAS	> 1 DIA	> 3 DIAS	> 8 DIAS	> 1 MES
TRATIVA Y FINANCIERA.	ambiental.		de rack de switch`s.	o /Actualización de equipos (Hardware).									
	Interrupción del servicio causado por manipulación física realizada a los switch´s por personal no autorizado.	Las áreas de central de datos no se encuentran debidamente aseguradas, permitiendo el acceso a personal no autorizado a manipular los switchs y demás equipos ocasionando fallos y cortes en los servicios tecnológicos de la red de datos.	Ausencia de política de seguridad en lo relacionado con el control de accesos a operatividad de switchs.	5.3.5. (E. 7) Deficiencias en la Organización. 5.4.9. (A.11) Acceso no autorizado.	Media	Media	Alta	1/10 - Poco Frecuente	Media	Media	Alta	Muy Alta	Muy Alta
	Mal funcionamiento por falta de mantenimiento.	No planificación de mantenimiento preventivo de switchs. No realización del mantenimiento de los switch ocasionando fallas en su funcionamiento normal.	Ausencia de política de seguridad en lo relacionado con la programación y gestión de mantenimiento preventivo.	5.3.15. (E.23) Errores de Manteamiento /Actualización de equipos (Hardware).	Baja	Media	Alta	1/10 - Poco Frecuente	Media	Media	Alta	Muy Alta	Muy Alta
	Denegación del servicio por accesos lógicos no autorizados a los switch´s.	Ataques de hackers a la red de datos y administración de switch y denegar el servicio de red a los usuarios de la misma.	Ausencia de política de seguridad en lo relacionado con gestión y control de accesos.	5.3.5. (E. 7) Deficiencias en la Organización. 5.4.9. (A.11) Acceso no autorizado.	Baja	Baja	Muy Alta	1/10 - Poco Frecuente	Media	Media	Alta	Muy Alta	Muy Alta

ACTIVO	AMENAZAS	DESCRIPCIÓN	ORIGEN DE LA AMENAZA	ORIGEN DE LA AMENAZA (Clasificación Según Magerit)	IMPACTO Y DEGRADACIÒN DEL ACTIVO			PROBABILIDAD DE OCURRENCIA	DISPONIBILIDAD EN EL TIEMPO				
					CONFIDENCIALIDAD [C]	INTEGRIDAD [I]	DISPONIBILIDAD [D]		> A 8 HORAS	> 1 DIA	> 3 DIAS	> 8 DIAS	> 1 MES
	Fallas por interrupciones del servicio eléctrico.	Ausencia de energía eléctrica y nula respuesta de equipos UPS ocasionando fallas en el funcionamiento de los Switch`s.	Ausencia de Procedimientos y mecanismos de activación de energía ante fallos de energía externa.	5.2.7. (I.6) Corte del suministro eléctrico.	Baja	Baja	Muy Alta	1/10 - Poco Frecuente	Media	Media	Alta	Muy Alta	Muy Alta
SWITCH 48 PUERTOS - 10/100/1000 - CENTRO DE DATOS - SUBDIRECCIÒN ADMINISTRATIVA Y FINANCIERA.	Fallas en el hardware por falta de mantenimiento, sobrecalentamiento y/o incendio por deficiencia en la aclimatación ambiental.	Fallas de los switch por sobrecalentamiento, al no existir o funcionar el servicio de aire acondicionados o regulación de la temperatura en los cuartos de equipos switch`s.	Falta de mantenimiento de Switch. Ausencia de equipos reguladores de temperatura ambiente en las zonas de ubicación de rack de switch`s.	5.2.8. (I.7) Condiciones inadecuadas de temperatura o humedad. 5.3.15. (E.23) Errores de Mantenimiento /Actualización de equipos (Hardware).	Baja	Media	Muy Alta	1/100 - Muy Poco Frecuente	Media	Media	Alta	Muy Alta	Muy Alta
	Interrupción del servicio causado por manipulación física realizada a los switch´s por personal no autorizado.	Las áreas de central de datos no se encuentran debidamente aseguradas, permitiendo el acceso a personal no autorizado a manipular los switchs y demás equipos ocasionando fallos y cortes en los servicios tecnológicos de la red de datos.	Ausencia de política de seguridad en lo relacionado con el control de accesos a operatividad de switchs.	5.3.5. (E. 7) Deficiencias en la Organización. 5.4.9. (A.11) Acceso no autorizado.	Media	Media	Alta	1/10 - Poco Frecuente	Media	Media	Alta	Muy Alta	Muy Alta

ACTIVO	AMENAZAS	DESCRIPCIÓN	ORIGEN DE LA AMENAZA	ORIGEN DE LA AMENAZA (Clasificación Según Magerit)	IMPACTO Y DEGRADACIÒN DEL ACTIVO			PROBABILIDAD DE OCURRENCIA	DISPONIBILIDAD EN EL TIEMPO				
					CONFIDENCIALIDAD [C]	INTEGRIDAD [I]	DISPONIBILIDAD [D]		> A 8 HORAS	> 1 DIA	> 3 DIAS	> 8 DIAS	> 1 MES
	Mal funcionamiento por falta de mantenimiento.	No planificación de mantenimiento preventivo de switchs. No realización del mantenimiento de los switch ocasionando fallas en su funcionamiento normal.	Ausencia de política de seguridad en lo relacionado con la programación y gestión de mantenimiento preventivo.	5.3.15. (E.23) Errores de Manteamiento /Actualización de equipos (Hardware).	Baja	Media	Alta	1/10 - Poco Frecuente	Media	Media	Alta	Muy Alta	Muy Alta
	Denegación del servicio por accesos lógicos no autorizados a los switch´s.	Ataques de hackers a la red de datos y administración de switch y denegar el servicio de red a los usuarios de la misma.	Ausencia de política de seguridad en lo relacionado con gestión y control de accesos.	5.3.5. (E. 7) Deficiencias en la Organización. 5.4.9. (A.11) Acceso no autorizado.	Baja	Baja	Muy Alta	1/10 - Poco Frecuente	Media	Media	Alta	Muy Alta	Muy Alta
	Fallas por interrupciones del servicio eléctrico.	Ausencia de energía eléctrica y nula respuesta de equipos UPS ocasionando fallas en el funcionamiento de los Switch`s.	Ausencia de Procedimientos y mecanismos de activación de energía ante fallos de energía externa.	5.2.7. (I.6) Corte del suministro eléctrico.	Baja	Baja	Muy Alta	1/10 - Poco Frecuente	Media	Media	Alta	Muy Alta	Muy Alta
RACK SECUNDARIO DE COMUNICACIONES - SUBDIRECCIÒN	Perdida de estabilidad y robustez del rack principal por mala configuración en su estructura.	Posibles caídas de equipos empotrados en el rack de comunicaciones por mala configuración, mal ajuste de tornillos y demás elementos que componen la estructura del mismo.	Personal no capacitado para armar estructurar de rack y redes de datos.	5.3.4. (E.4) Errores de Configuración.	Baja	Media	Alta	1/10 - Poco Frecuente	Media	Alta	Alta	Alta	Muy Alta

ACTIVO	AMENAZAS	DESCRIPCIÓN	ORIGEN DE LA AMENAZA	ORIGEN DE LA AMENAZA (Clasificación Según Magerit)	IMPACTO Y DEGRADACIÒN DEL ACTIVO			PROBABILIDAD DE OCURRENCIA	DISPONIBILIDAD EN EL TIEMPO				
					CONFIDENCIALIDAD [C]	INTEGRIDAD [I]	DISPONIBILIDAD [D]		> A 8 HORAS	> 1 DIA	> 3 DIAS	> 8 DIAS	> 1 MES
DE PLANEACIÒN AMBIENTAL.	Daños causados por manipulación y accesos de personal no autorizado.	Personas ajenas a la organización o no autorizadas para la manipulación de los equipos del área ingresan sin autorización y ocasionan daños en el rack de comunicaciones.	Ausencia de control de accesos a personal no autorizado en manipulación del rack de comunicaciones	5.3.5. (E. 7) Deficiencias en la Organización. 5.4.9. (A.11) Acceso no autorizado.	Baja	Baja	Alta	1/10 - Poco Frecuente	Media	Alta	Alta	Alta	Muy Alta
SWITCH CORE 24 PUERTOS - 10/100/1000 - SUBDIRECCIÒN DE PLANEACIÒN AMBIENTAL.	Fallas en el hardware por falta de mantenimiento, sobrecalentamiento y/o incendio por deficiencia en la aclimatación ambiental.	Fallas de los switch por sobrecalentamiento, al no existir o funcionar el servicio de aire acondicionados o regulación de la temperatura en los cuartos de equipos switch`s.	Falta de mantenimiento de Switch. Ausencia de equipos reguladores de temperatura ambiente en las zonas de ubicación de rack de switch`s.	5.2.8. (I.7) Condiciones inadecuadas de temperatura o humedad. 5.3.15. (E.23) Errores de Mantenimiento /Actualización de equipos (Hardware).	Baja	Media	Muy Alta	1/100 - Muy Poco Frecuente	Media	Media	Alta	Muy Alta	Muy Alta
	Interrupción del servicio causado por manipulación física realizada a los switch´s por personal no autorizado.	Las áreas de central de datos no se encuentran debidamente aseguradas, permitiendo el acceso a personal no autorizado a manipular los switchs y demás equipos ocasionando fallos y cortes en los servicios tecnológicos de la red de datos.	Ausencia de política de seguridad en lo relacionado con el control de accesos a operatividad de switchs.	5.3.5. (E. 7) Deficiencias en la Organización. 5.4.9. (A.11) Acceso no autorizado.	Media	Media	Alta	1/10 - Poco Frecuente	Media	Media	Alta	Muy Alta	Muy Alta

ACTIVO	AMENAZAS	DESCRIPCIÓN	ORIGEN DE LA AMENAZA	ORIGEN DE LA AMENAZA (Clasificación Según Magerit)	IMPACTO Y DEGRADACIÒN DEL ACTIVO			PROBABILIDAD DE OCURRENCIA	DISPONIBILIDAD EN EL TIEMPO				
					CONFIDENCIALIDAD [C]	INTEGRIDAD [I]	DISPONIBILIDAD [D]		> A 8 HORAS	> 1 DIA	> 3 DIAS	> 8 DIAS	> 1 MES
	Mal funcionamiento por falta de mantenimiento.	No planificación de mantenimiento preventivo de switchs. No realización del mantenimiento de los switch ocasionando fallas en su funcionamiento normal.	Ausencia de política de seguridad en lo relacionado con la programación y gestión de mantenimiento preventivo.	5.3.15. (E.23) Errores de Mantenimiento /Actualización de equipos (Hardware).	Baja	Media	Alta	1/10 - Poco Frecuente	Media	Media	Alta	Muy Alta	Muy Alta
	Denegación del servicio por accesos lógicos no autorizados a los switch´s.	Ataques de hackers a la red de datos y administración de switch y denegar el servicio de red a los usuarios de la misma.	Ausencia de política de seguridad en lo relacionado con gestión y control de accesos.	5.3.5. (E. 7) Deficiencias en la Organización. 5.4.9. (A.11) Acceso no autorizado.	Baja	Baja	Muy Alta	1/10 - Poco Frecuente	Media	Media	Alta	Muy Alta	Muy Alta
	Fallas por interrupciones del servicio eléctrico.	Ausencia de energía eléctrica y nula respuesta de equipos UPS ocasionando fallas en el funcionamiento de los Switch`s.	Ausencia de Procedimientos y mecanismos de activación de energía ante fallos de energía externa.	5.2.7. (I.6) Corte del suministro eléctrico.	Baja	Baja	Muy Alta	1/10 - Poco Frecuente	Media	Media	Alta	Muy Alta	Muy Alta
SWITCH 48 PUERTOS - 10/100/1000 - SUBDIRECCIÒN DE	Fallas en el hardware por falta de mantenimiento, sobrecalentamiento y/o incendio por deficiencia en la aclimatación	Fallas de los switch por sobrecalentamiento, al no existir o funcionar el servicio de aire acondicionados o regulación de la temperatura en los cuartos de equipos switch`s.	Falta de mantenimiento de Switch. Ausencia de equipos reguladores de temperatura ambiente en las zonas de ubicación	5.2.8. (I.7) Condiciones inadecuadas de temperatura o humedad. 5.3.15. (E.23) Errores de Mantenimient	Baja	Media	Muy Alta	1/100 - Muy Poco Frecuente	Media	Media	Alta	Muy Alta	Muy Alta

ACTIVO	AMENAZAS	DESCRIPCIÓN	ORIGEN DE LA AMENAZA	ORIGEN DE LA AMENAZA (Clasificación Según Magerit)	IMPACTO Y DEGRADACIÒN DEL ACTIVO			PROBABILIDAD DE OCURRENCIA	DISPONIBILIDAD EN EL TIEMPO				
					CONFIDENCIALIDAD [C]	INTEGRIDAD [I]	DISPONIBILIDAD [D]		> A 8 HORAS	> 1 DIA	> 3 DIAS	> 8 DIAS	> 1 MES
PLANEACIÒN AMBIENTAL.	ambiental.		de rack de switch`s.	o /Actualización de equipos (Hardware).									
	Interrupción del servicio causado por manipulación física realizada a los Switch's por personal no autorizado.	Las áreas de central de datos no se encuentran debidamente aseguradas, permitiendo el acceso a personal no autorizado a manipular los Switch's y demás equipos ocasionando fallos y cortes en los servicios tecnológicos de la red de datos.	Ausencia de política de seguridad en lo relacionado con el control de accesos a operatividad de Switch's.	5.3.5. (E. 7) Deficiencias en la Organización. 5.4.9. (A.11) Acceso no autorizado.	Media	Media	Alta	1/10 - Poco Frecuente	Media	Media	Alta	Muy Alta	Muy Alta
	Mal funcionamiento por falta de mantenimiento.	No planificación de mantenimiento preventivo de Switch's. No realización del mantenimiento de los switch ocasionando fallas en su funcionamiento normal.	Ausencia de política de seguridad en lo relacionado con la programación y gestión de mantenimiento preventivo.	5.3.15. (E.23) Errores de Mantenimiento o /Actualización de equipos (Hardware).	Baja	Media	Alta	1/10 - Poco Frecuente	Media	Media	Alta	Muy Alta	Muy Alta
	Denegación del servicio por accesos lógicos no autorizados a los Switch's.	Ataques de hackers a la red de datos y administración de switch y denegar el servicio de red a los usuarios de la misma.	Ausencia de política de seguridad en lo relacionado con gestión y control de accesos.	5.3.5. (E. 7) Deficiencias en la Organización. 5.4.9. (A.11) Acceso no autorizado.	Baja	Baja	Muy Alta	1/10 - Poco Frecuente	Media	Media	Alta	Muy Alta	Muy Alta

ACTIVO	AMENAZAS	DESCRIPCIÓN	ORIGEN DE LA AMENAZA	ORIGEN DE LA AMENAZA (Clasificación Según Magerit)	IMPACTO Y DEGRADACIÒN DEL ACTIVO			PROBABILIDAD DE OCURRENCIA	DISPONIBILIDAD EN EL TIEMPO				
					CONFIDENCIALIDAD [C]	INTEGRIDAD [I]	DISPONIBILIDAD [D]		> A 8 HORAS	> 1 DIA	> 3 DIAS	> 8 DIAS	> 1 MES
	Fallas por interrupciones del servicio eléctrico.	Ausencia de energía eléctrica y nula respuesta de equipos UPS ocasionando fallas en el funcionamiento de los Switch`s.	Ausencia de Procedimientos y mecanismos de activación de energía ante fallos de energía externa.	5.2.7. (I.6) Corte del suministro eléctrico.	Baja	Baja	Muy Alta	1/10 - Poco Frecuente	Media	Media	Alta	Muy Alta	Muy Alta
CABLEADO ESTRUCTURADO CATEGORIA 6 Y RED DE DATOS y CANALETA.	Daños en el cableado estructurado por canaletas abiertas al aire libre y por mala manipulación de personal no autorizado.	Cables de canaleta salidos con daños por mordedura de ratones, líquidos regados, cables reventados, causan daños en el cableado estructurado.	Ausencia de política de seguridad en lo relacionado con el tratamiento y control de puntos de red y canaleta de red de datos.	5.3.5. (E. 7) Deficiencias en la Organización. 5.4.9. (A.11) Acceso no autorizado.	Baja	Media	Alta	1 - Normal	Media	Media	Alta	Muy Alta	Muy Alta
	Fallas en las comunicaciones por daños en cableado estructurado.		Ausencia de política de seguridad en lo relacionado con el mantenimiento preventivo y correctivo de canaleta de la red de datos.	5.3.5. (E. 7) Deficiencias en la Organización. 5.4.9. (A.11) Acceso no autorizado.	Baja	Alta	Alta	1/10 - Poco Frecuente	Media	Media	Alta	Muy Alta	Muy Alta
	Accesos no autorizados a los puntos de red del cableado estructurado.	Personal no autorizado conectando equipos de cómputo a través de puntos de la red de datos de la Corporación.	Ausencia de Política de seguridad en lo relacionado con control de acceso a la red de datos.	5.3.5. (E. 7) Deficiencias en la Organización. 5.4.9. (A.11) Acceso no	Alta	Media	Baja	1 - Normal	Media	Alta	Alta	Muy Alta	Muy Alta

ACTIVO	AMENAZAS	DESCRIPCIÓN	ORIGEN DE LA AMENAZA	ORIGEN DE LA AMENAZA (Clasificación Según Magerit)	IMPACTO Y DEGRADACIÒN DEL ACTIVO			PROBABILIDAD DE OCURRENCIA	DISPONIBILIDAD EN EL TIEMPO				
					CONFIDENCIALIDAD [C]	INTEGRIDAD [I]	DISPONIBILIDAD [D]		> A 8 HORAS	> 1 DIA	> 3 DIAS	> 8 DIAS	> 1 MES
				autorizado.									
	Incendio deliberado por personal interno o externo de la Corporación, o por corto circuitos producidos en la red de corriente eléctrica.	Incendio de cableado estructurado y canaleta por cables de corriente regulada no protegidos y debidamente aislados.	Incumplimiento de las normas de implementación de cableado de red de datos, eléctrico, voz y canaleta.	5.3.5. (E. 7) Deficiencias en la Organización.	Baja	Alta	Alta	1/100 - Muy Poco Frecuente	Media	Media	Alta	Muy Alta	Muy Alta
CABLEADO DE COBRE DE CORRIENTE REGULADA PARA EQUIPOS DE CÓMPUTO.	Daños en el cableado de corriente regulada, canaletas abiertas al aire libre y por mala manipulación de personal no autorizado.	Fallos por falta de mantenimiento del cableado de corriente regulada y canaleta de protección.	Ausencia de política de seguridad para el manejo de canaleta de cableado de datos, eléctrico y voz.	5.3.5. (E. 7) Deficiencias en la Organización. 5.3.1. (E.1) Errores de los Usuarios.	Baja	Media	Media	10 - Frecuente	Media	Media	Alta	Muy Alta	Muy Alta
	Fallas en el cableado de corriente regulada por Corto circuito.	Corto circuito en la canaleta y cable de corriente regulada ocasionando fallas y suspensión del servicio de energía a los equipos de la red de datos.	Incumplimiento de las normas de implementación de cableado de red de datos, eléctrico, voz y canaleta.	5.3.5. (E. 7) Deficiencias en la Organización.	Muy Baja	Media	Alta	1/10 - Poco Frecuente	Media	Media	Alta	Muy Alta	Muy Alta

ACTIVO	AMENAZAS	DESCRIPCIÓN	ORIGEN DE LA AMENAZA	ORIGEN DE LA AMENAZA (Clasificación Según Magerit)	IMPACTO Y DEGRADACIÒN DEL ACTIVO			PROBABILIDAD DE OCURRENCIA	DISPONIBILIDAD EN EL TIEMPO				
					CONFIDENCIALIDAD [C]	INTEGRIDAD [I]	DISPONIBILIDAD [D]		> A 8 HORAS	> 1 DIA	> 3 DIAS	> 8 DIAS	> 1 MES
	Daños en el cableado de corriente regulada y disminución en la capacidad de respuesta de las UPS, por conexión de equipos no autorizados (Mal uso).		Ausencia de política de seguridad para el uso de la red de corriente regulada de la entidad	5.3.5. (E. 7) Deficiencias en la Organización. 5.3.1. (E.1) Errores de los Usuarios.	Muy Baja	Media	Alta	10 - Frecuente	Media	Media	Alta	Muy Alta	Muy Alta
	Incendio deliberado o accidental, causado por personal interno o externo de la Corporación, o por corto circuitos producidos en la red de corriente eléctrica.	Personal externo o interno ocasiona incendios de forma deliberada o accidental en la red eléctrica regulada, ocasionando cortes en el servicio.	Ausencia de política de seguridad para el manejo de canaleta de cableado de datos, eléctrico y voz. Ausencia de política de seguridad en el control de accesos a la red de datos y corriente regulada.	5.3.5. (E. 7) Deficiencias en la Organización. 5.3.1. (E.1) Errores de los Usuarios.	Media	Alta	Alta	1/100 - Muy Poco Frecuente	Media	Media	Alta	Muy Alta	Muy Alta
UPS DE 20 KVA, PROTECCIÒN DE EQUIPOS	Fallas en el sistema de UPS por baterías en mal estado de	Mal funcionamiento de las UPS por baterías en mal estado, esto tiende a que no haya disponibilidad del servicio de la UPS al	Falta de verificación de alertas de la UPS. Falta de mantenimiento	5.3.5. (E. 7) Deficiencias en la Organización. 5.3.15. (E.23)	Baja	Media	Alta	10 - Frecuente	Alta	Alta	Muy Alta	Muy Alta	Muy Alta

ACTIVO	AMENAZAS	DESCRIPCIÓN	ORIGEN DE LA AMENAZA	ORIGEN DE LA AMENAZA (Clasificación Según Magerit)	IMPACTO Y DEGRADACIÒN DEL ACTIVO			PROBABILIDAD DE OCURRENCIA	DISPONIBILIDAD EN EL TIEMPO				
					CONFIDENCIALIDAD [C]	INTEGRIDAD [I]	DISPONIBILIDAD [D]		> A 8 HORAS	> 1 DIA	> 3 DIAS	> 8 DIAS	> 1 MES
DE COMPUTO SUBDIRECCIÒN DE PLANEACIÒN Y CENTRO DE DOCUMENTOS.	funcionamiento.	momento de requerirse.	preventivo y correctivo de la UPS.	Errores de Mantenimiento /Actualización de equipos (Hardware).									
	Fallas o daños por voltaje excesivo en la UPS.	La variación del fluido eléctrico ocasiona daños en los resistores eléctricos de la UPS, ocasionando daños en la tarjeta de administración de UPS, y ocasionando daños en las baterías, lo que dificulta la respuesta de las mismas al momento de requerirse.	Ausencia de supresor de picos eléctricos que salvaguardan a las UPS.	5.3.5. (E. 7) Deficiencias en la Organización.	Baja	Media	Alta	1/10 - Poco Frecuente	Alta	Alta	Muy Alta	Muy Alta	Muy Alta
	Daños en la UPS por mala configuración y/o disminución de mantenimiento de la red de corriente regulada.	Configuración de funcionamiento de la UPS por personal sin las competencias necesarias, ni el conocimiento de instalación e implementación.	Ausencia de políticas de seguridad para la instalación, configuración y mantenimiento de las UPS.	5.3.5. (E. 7) Deficiencias en la Organización. 5.3.4. (E.4) Errores de Configuración.	Muy Baja	Media	Alta	1 - Normal	Alta	Alta	Muy Alta	Muy Alta	Muy Alta
	Mal funcionamiento por falta de mantenimiento.	Al no programar el mantenimiento de la UPS, ni tener controles que indiquen las posibles fallas que se pueden presentar, la UPS tiende a colapsar y no brindar	No realización de mantenimiento de UPS.	5.3.5. (E. 7) Deficiencias en la Organización. 5.3.15. (E.23) Errores de	Muy Baja	Alta	Alta	10 - Frecuente	Alta	Alta	Muy Alta	Muy Alta	Muy Alta

ACTIVO	AMENAZAS	DESCRIPCIÓN	ORIGEN DE LA AMENAZA	ORIGEN DE LA AMENAZA (Clasificación Según Magerit)	IMPACTO Y DEGRADACIÒN DEL ACTIVO			PROBABILIDAD DE OCURRENCIA	DISPONIBILIDAD EN EL TIEMPO				
					CONFIDENCIALIDAD [C]	INTEGRIDAD [I]	DISPONIBILIDAD [D]		> A 8 HORAS	> 1 DIA	> 3 DIAS	> 8 DIAS	> 1 MES
		el servicio en el momento requerido.		Mantenimiento /Actualización de equipos (Hardware).									
UPS DE 30 KVA, PROTECCIÒN DE EQUIPOS DE COMPUTO SUBDIRECCIÒN DE CONTROL Y CALIDAD AMBIENTAL, SUBDIRECCIÒN ADMINISTRATIVA Y FINANCIERA Y DIRECCIÒN GENERA	Fallas en el sistema de UPS por baterías en mal estado de funcionamiento.	Mal funcionamiento de las UPS por baterías en mal estado, esto tiende a que no haya disponibilidad del servicio de la UPS al momento de requerirse.	Falta de verificación de alertas de la UPS. Falta de mantenimiento preventivo y correctivo de la UPS.	5.3.5. (E. 7) Deficiencias en la Organización. 5.3.15. (E.23) Errores de Mantenimiento /Actualización de equipos (Hardware).	Baja	Media	Alta	10 - Frecuente	Alta	Alta	Muy Alta	Muy Alta	Muy Alta
	Fallas o daños por voltaje excesivo en la UPS.	La variación del fluido eléctrico ocasiona daños en los resistores eléctricos de la UPS, ocasionando daños en la tarjeta de administración de UPS, y ocasionando daños en las baterías, lo que dificulta la respuesta de las mismas al momento de requerirse.	Ausencia de supresor de picos eléctricos que salvaguardan a las UPS.	5.3.5. (E. 7) Deficiencias en la Organización.	Baja	Media	Alta	1/10 - Poco Frecuente	Alta	Alta	Muy Alta	Muy Alta	Muy Alta
	Daños en la UPS por mala configuración y/o disminución de	Configuración de funcionamiento de la UPS por personal sin las competencias necesarias, ni el conocimiento de instalación e	Ausencia de políticas de seguridad para la instalación, configuración y	5.3.5. (E. 7) Deficiencias en la Organización. 5.3.4. (E.4)	Muy Baja	Media	Alta	1 - Normal	Alta	Alta	Muy Alta	Muy Alta	Muy Alta

ACTIVO	AMENAZAS	DESCRIPCIÓN	ORIGEN DE LA AMENAZA	ORIGEN DE LA AMENAZA (Clasificación Según Magerit)	IMPACTO Y DEGRADACIÒN DEL ACTIVO			PROBABILIDAD DE OCURRENCIA	DISPONIBILIDAD EN EL TIEMPO				
					CONFIDENCIALIDAD [C]	INTEGRIDAD [I]	DISPONIBILIDAD [D]		> A 8 HORAS	> 1 DIA	> 3 DIAS	> 8 DIAS	> 1 MES
L.	mantenimiento de la red de corriente regulada.	implementación.	mantenimiento de las UPS.	Errores de Configuración.									
	Mal funcionamiento por falta de mantenimiento.	Al no programar el mantenimiento de la UPS, ni tener controles que indiquen las posibles fallas que se pueden presentar, la UPS tiende a colapsar y no brindar el servicio en el momento requerido.	Ausencia de mantenimiento de UPS.	5.3.5. (E. 7) Deficiencias en la Organización. 5.3.15. (E.23) Errores de Mantenimiento /Actualización de equipos (Hardware).	Muy Baja	Alta	Alta	10 - Frecuente	Alta	Alta	Muy Alta	Muy Alta	Muy Alta
INFORMACIÒN FISICA DEL CENTRO DE DOCUMENTOS DE CORPORINOQUIA, SEDE PRINCIPAL.	Incendio deliberado por personal interno o externo de la Corporación, o por corto circuitos producidos en la red de corriente eléctrica.	Incendio por personal interno o externo de la corporación, en los documentos del centro de documentos, ocasionando perdida de la información de la Corporación.	Ausencia de políticas de control de accesos a la información física y digital	5.3.5. (E. 7) Deficiencias en la Organización. 5.3.1. (E.1) Errores de los Usuarios.	Baja	Alta	Muy Alta	1/100 - Muy Poco Frecuente	Alta	Alta	Muy Alta	Muy Alta	Muy Alta
	Robo de información.	Personal interno o externo que se apropia de información física del centro de documentos, ocasionando			Alta	Alta	Muy Alta	1/100 - Muy Poco Frecuente	Alta	Alta	Muy Alta	Muy Alta	Muy Alta

ACTIVO	AMENAZAS	DESCRIPCIÓN	ORIGEN DE LA AMENAZA	ORIGEN DE LA AMENAZA (Clasificación Según Magerit)	IMPACTO Y DEGRADACIÒN DEL ACTIVO			PROBABILIDAD DE OCURRENCIA	DISPONIBILIDAD EN EL TIEMPO				
					CONFIDENCIALIDAD [C]	INTEGRIDAD [I]	DISPONIBILIDAD [D]		> A 8 HORAS	> 1 DIA	> 3 DIAS	> 8 DIAS	> 1 MES
		perdida de la información, atacando la disponibilidad, confidencialidad de la misma.											
	Accesos no autorizados a la información.	No existen los mecanismos necesarios de seguridad de la información física, por lo tanto cualquier persona puede acceder a la información, ocasionando daños irremediables en la información.			Alta	Alta	Muy Alta	1/100 - Muy Poco Frecuente	Alta	Alta	Muy Alta	Muy Alta	Muy Alta
PLANTA ELECTRICA LISTER DE 30 KVA	Corto circuito por alto voltaje.	Fallas en la configuración de la planta eléctrica con respecto a la energía eléctrica externa e interna produciendo corto circuito por alto voltaje.	Ausencia de supresor de picos eléctricos que salvaguardan a las UPS.	5.3.5. (E. 7) Deficiencias en la Organización.	Muy Baja	Media	Alta	1/10 - Poco Frecuente	Muy Baja	Baja	Media	Alta	Muy Alta
	Incendio deliberado por personal interno o externo de la Corporación, o por corto circuitos producidos en la red de corriente eléctrica.	Al no existir políticas de seguridad que restrinjan el acceso a personas no autorizadas a los sectores donde se encuentra la planta eléctrica pueden causar incendios deliberados o accidentales ocasionando daños irreversibles a la planta eléctrica.	Ausencia de Políticas de Seguridad para el control de acceso a manipulación no autorizada de las áreas donde se encuentra ubicada la planta eléctrica.	5.3.5. (E. 7) Deficiencias en la Organización. 5.3.1. (E.1) Errores de los Usuarios.	Muy Baja	Media	Media	1/100 - Muy Poco Frecuente	Muy Baja	Baja	Media	Alta	Muy Alta

ACTIVO	AMENAZAS	DESCRIPCIÓN	ORIGEN DE LA AMENAZA	ORIGEN DE LA AMENAZA (Clasificación Según Magerit)	IMPACTO Y DEGRADACIÒN DEL ACTIVO			PROBABILIDAD DE OCURRENCIA	DISPONIBILIDAD EN EL TIEMPO				
					CONFIDENCIALIDAD [C]	INTEGRIDAD [I]	DISPONIBILIDAD [D]		> A 8 HORAS	> 1 DIA	> 3 DIAS	> 8 DIAS	> 1 MES
	Mal manejo y Accesos no autorizados.	La ausencia de políticas de seguridad y procedimientos de uso e implementación de plantas eléctricas de alto voltaje, permite que personas sin conocimientos técnicos o funcionarios sin autorización ingresen a manipular la planta eléctrica.	Ausencia de Políticas de Seguridad para el control de acceso a manipulación no autorizada de las áreas donde se encuentra ubicada la planta eléctrica.	5.3.5. (E. 7) Deficiencias en la Organización. 5.3.1. (E.1) Errores de los Usuarios.	Media	Media	Media	1/100 - Muy Poco Frecuente	Muy Baja	Muy Baja	Media	Alta	Muy Alta
	Daños por mala configuración.	Personas sin conocimientos técnicos en el uso e implementación de plantas eléctricas de estas características realizan instalaciones sin el lleno de requisitos, dejando vulnerabilidades habilitadas produciendo daños en la planta eléctrica.	Ausencia de Políticas de Seguridad para la instalación, configuración e implementación de la planta eléctrica.	5.3.5. (E. 7) Deficiencias en la Organización. 5.3.4. (E.4) Errores de Configuración.	Muy Baja	Baja	Media	1/10 - Poco Frecuente	Muy Baja	Muy Baja	Media	Alta	Muy Alta
	Mal funcionamiento por falta de mantenimiento.	Ausencia de políticas de seguridad y procedimientos de mantenimiento preventivo y correctivo, ocasionan falta de atención seguimiento a los controles de la planta eléctrica, permitiendo el mal funcionamiento de la misma hasta dañarse y no estar activa cuando se requiere para su servicio.	Ausencia de Políticas de Seguridad y procedimientos establecidos para realizar mantenimiento preventivo y correctivo de la Planta Eléctrica.	5.3.5. (E. 7) Deficiencias en la Organización.	Muy Baja	Baja	Media	1/10 - Poco Frecuente	Media	Media	Media	Alta	Alta

ACTIVO	AMENAZAS	DESCRIPCIÓN	ORIGEN DE LA AMENAZA	ORIGEN DE LA AMENAZA (Clasificación Según Magerit)	IMPACTO Y DEGRADACIÒN DEL ACTIVO			PROBABILIDAD DE OCURRENCIA	DISPONIBILIDAD EN EL TIEMPO				
					CONFIDENCIALIDAD [C]	INTEGRIDAD [I]	DISPONIBILIDAD [D]		> A 8 HORAS	> 1 DIA	> 3 DIAS	> 8 DIAS	> 1 MES
	No funciona por falta de combustible.	El responsable de proveer el suministro de combustible a la planta eléctrica no la tanquea o no eta definida la responsabilidad de mantener tanqueado de combustible la planta eléctrica.	Ausencia de controles y seguimiento a los mismos para los casos de dotación de combustible.	5.3.5. (E. 7) Deficiencias en la Organización.	Muy Baja	Baja	Media	1/10 - Poco Frecuente	Media	Media	Media	Alta	Alta
EQUIPOS DE COMPUTO DE ESCRITORIO	Sobrecalentamiento e incendio de equipos por aumento en la temperatura ambiental.	Los equipos se recalientan debido a las altas temperaturas y mala costumbre de dejar encendido los equipos de cómputo por parte de funcionarios, ocasionando recalentamiento e incendio en los equipos de computo	Ausencia de Políticas de Seguridad para el mantenimiento de equipos de cómputo.	5.3.5. (E. 7) Deficiencias en la Organización.	Muy Baja	Media	Alta	1/100 - Muy Poco Frecuente	Muy Baja	Baja	Media	Alta	Muy Alta
	Incendio deliberado por personal interno o externo de la Corporación.	Personas con acceso no autorizado a los equipos de cómputo producen incendios, causando daños irreparables a los mismos.	Ausencia de Políticas de Seguridad para el control de accesos a equipos de cómputo.	5.3.5. (E. 7) Deficiencias en la Organización.	Muy Baja	Media	Alta	1/100 - Muy Poco Frecuente	Muy Baja	Baja	Media	Alta	Muy Alta
	Daños en la estructura del equipo de cómputo por caída de concreto y hierro reforzado por temblor (Desastre	Debido a desastres naturales los equipos están expuestos a daños en su estructura y funcionamiento.	Desastres naturales	5.1. (N) Desastres naturales. 5.2.8. (I.7) Condiciones inadecuadas de temperatura o humedad.	Muy Baja	Media	Alta	1/100 - Muy Poco Frecuente	Muy Baja	Baja	Media	Alta	Muy Alta

ACTIVO	AMENAZAS	DESCRIPCIÓN	ORIGEN DE LA AMENAZA	ORIGEN DE LA AMENAZA (Clasificación Según Magerit)	IMPACTO Y DEGRADACIÒN DEL ACTIVO			PROBABILIDAD DE OCURRENCIA	DISPONIBILIDAD EN EL TIEMPO				
					CONFIDENCIALIDAD [C]	INTEGRIDAD [I]	DISPONIBILIDAD [D]		> A 8 HORAS	> 1 DIA	> 3 DIAS	> 8 DIAS	> 1 MES
	Natural)												
	Daños en el equipo de cómputo por sobrecargas de alto voltaje eléctrico en el mismo.	Los continuos picos de corriente y apagones de energía eléctrica ocasionan daño en los equipos de cómputo, ocasionando daños en las partes de los mismos y en ocasiones en todo el equipo de cómputo.	Ausencia de políticas de seguridad para el cuidado de equipos de cómputo en lo relacionado con acceso a electricidad.	5.3.5. (E. 7) Deficiencias en la Organización.	Muy Baja	Alta	Alta	1/100 - Muy Poco Frecuente	Muy Baja	Baja	Media	Alta	Muy Alta
	Fallas de funcionamiento de los equipos de cómputo por defectos en el software y hardware.	Algunos equipos de cómputo vienen con partes defectuosas ocasionando daños en el funcionamiento del mismo.	Ausencia de Políticas de seguridad en la adquisición de equipos de cómputo.	5.3.5. (E. 7) Deficiencias en la Organización.	Muy Baja	Media	Alta	1/100 - Muy Poco Frecuente	Muy Baja	Baja	Media	Alta	Muy Alta
	Ataque de virus.	Lentitud o negación del servicio de los equipos de cómputo, en cuanto a memoria, procesamiento de datos o lectura y escritura de datos en el sistema se ocasiona debido a virus que se descargan al acceder a internet, memorias USB, entre otros, y si el equipo esta desprotegido con antivirus actualizados, pues son infectados, causando daño en	Ausencia de políticas de seguridad para la protección lógica de equipos de cómputo.	5.3.5. (E. 7) Deficiencias en la Organización.	Baja	Media	Media	1/100 - Muy Poco Frecuente	Muy Baja	Baja	Media	Alta	Muy Alta

ACTIVO	AMENAZAS	DESCRIPCIÓN	ORIGEN DE LA AMENAZA	ORIGEN DE LA AMENAZA (Clasificación Según Magerit)	IMPACTO Y DEGRADACIÒN DEL ACTIVO			PROBABILIDAD DE OCURRENCIA	DISPONIBILIDAD EN EL TIEMPO				
					CONFIDENCIALIDAD [C]	INTEGRIDAD [I]	DISPONIBILIDAD [D]		> A 8 HORAS	> 1 DIA	> 3 DIAS	> 8 DIAS	> 1 MES
		el servicio de los mismos.											
	Fallas en el funcionamiento de los equipos de cómputo por cortes del suministro eléctrico	Ausencia de energía eléctrica interrumpe el servicio de los equipos de cómputo y la disponibilidad del servicio de los mismos.	Ausencia de Políticas de seguridad para que los equipos de respaldo funcionen de manera adecuada en el momento en que se requiere.	5.3.5. (E. 7) Deficiencias en la Organización.	Muy Baja	Media	Alta	1/100 - Muy Poco Frecuente	Muy Baja	Baja	Media	Alta	Muy Alta
	Accesos no autorizados al equipo de cómputo y la red de datos.	Sucede cuando usuarios o personal no autorizado ingresan a la red de datos, equipos de cómputo y servidores y causan daños en los mismos.	Ausencia de Política de seguridad en el control de acceso a los equipos de cómputo de los usuarios y servicios de la red de datos.	5.3.5. (E. 7) Deficiencias en la Organización.	Alta	Alta	Media	1/10 - Poco Frecuente	Muy Baja	Baja	Media	Alta	Muy Alta
	Ataques de denegación de servicio.	La falta de controles de acceso al sistema ocasiona que usuarios o atacantes intenten realizar ataques para denegar los servicios de la red de datos y los servidores.	Ausencia de Política de seguridad relacionada con la defensa del sistema.	5.3.5. (E. 7) Deficiencias en la Organización.	Baja	Baja	Alta	1/10 - Poco Frecuente	Muy Baja	Baja	Media	Alta	Muy Alta

Fuente: el autor

5.1.3 Caracterización y Valoración de las Salvaguardas

Una vez identificadas las amenazas y valoradas en cada una de sus componentes de acuerdo a la confidencialidad, integridad y disponibilidad se procede a identificar las salvaguardas por cada una de las amenazas detectadas en los activos de la Corporación, establecidos para el presente proceso. Las salvaguardas propuestas serán valoradas de acuerdo a su eficacia y su efectividad, de la siguiente manera:

Tabla 8. Caracterización y Valoración de las Salvaguardas

NOMBRE CORTO	ACTIVO	AMENAZAS	SALVAGUARDAS	VALORACIÒN DE SALVAGUARDAS	
				EFICACIA	EFECTIVIDAD
SERVIDOR	SERVIDOR DE APLICACIONES (SISTEMAS DE INFORMACIÒN FINANCIERO Y BASE DE DATOS)	Sobrecalentamiento e incendio de equipos por deficiencia en la aclimatación ambiental del servidor.	Instalación de aires acondicionados nuevos y funcionales. Implementar medidores de temperatura con alertas.	Los aires acondicionados en normal funcionamiento permiten mantener estable la temperatura y evitar sobrecalentamientos en los servidores. Los mecanismos de alerta a cambios bruscos de temperatura controlaran la estabilidad del ambiente en la sala de servidores	100%
		Incendio accidental o deliberado por personal interno o externo de la Corporación.	Control de acceso a través de tarjetas de acceso. Usuario y contraseña al centro de datos de la Corporación.	Restringir el acceso a través de usuario y contraseña, o control de acceso biométrico permite controlar de forma eficaz y efectiva la administración de elementos tecnológicos que se encuentren en la sala de servidores y centro de datos.	100%
		Daños en la estructura del servidor por caída de concreto y hierro reforzado por temblor (Desastre Natural)	Mantener Backup de la información en la Nube, como garantía para reestablecer los servicios de información.	Contar con copias de respaldo de toda la información que se maneja en la Corporación permite recuperar rápidamente el funcionamiento del sistema.	100%
		Daños en el servidor por sobrecargas de alto voltaje eléctrico en el mismo.	Adquirir UPS y supresor de picos de alto voltaje para proteger los servidores.	Con el estabilizador y la UPS funcional, los servidores no tendrán fallas en su funcionamiento.	100%
		Fallas de funcionamiento en el servidor por defectos en el software.	Implementar procedimiento para ingreso y entrada de bienes de tecnología a la corporación.	Con procedimientos claros y responsabilidades asignadas a cada funcionario del área de sistemas, se controlará que los elementos adquiridos sean de excelente calidad.	100%
		Fallas en el funcionamiento del servidor por daños en el hardware.	Implementar procedimiento para ingreso y entrada de bienes de tecnología a la corporación.	Con procedimientos claros y responsabilidades asignadas a cada funcionario del área de sistemas, se controlará que los elementos adquiridos sean de excelente calidad.	100%

NOMBRE CORTO	ACTIVO	AMENAZAS	SALVAGUARDAS	VALORACIÒN DE SALVAGUARDAS	
				EFICACIA	EFECTIVIDAD
		Fallas en el funcionamiento del servidor por cortes del suministro eléctrico	Realizar mantenimiento a la planta eléctrica y a la UPS que suministra corriente eléctrica y alterna a los servidores.	Los servidores deben contar con la energía necesaria, por lo tanto, el mantenimiento preventivo y correctivo de fallas de UPS y planta eléctrica debe ser constante. Esto evitara fallas o apagones del servidor, por esta causa.	100%
		Accesos no autorizados al servidor.	Implementar IPS e IDS, para detección de intrusos. Implementar firewall para la red de datos y para los sistemas de información web.	Los Sistemas de Protección y Detección de intrusos ayudan a detectar los accesos no autorizados al sistema, así mismo, con los IPS, se lograra contener los ataques. También la implementación de Firewall reducirá el número de ataques de virus y páginas con código malicioso en la red de datos.	100%
		Fallas en el funcionamiento por ataque de virus.	Actualizar las licencias de antivirus para servidores.	Cada uno de los servidores y equipos debe contar con su antivirus licenciado y actualizado, brindando seguridad optima a los mismos.	100%
		Ataques de denegación de servicio.	Realizar una política de seguridad de la información, socializarla y cumplirla dentro de la Organización. Documentar el procedimiento contra este tipo de ataque de denegación de servicios. Las experiencias exitosas de solución. Identificar los tipos de paquetes de bloqueo que se envían a la red y bloquearlos en los equipos de red o redirigiéndolos.	La política de seguridad permite que a través de su gestión se logre contener este tipo de ataques, para lo cual se requiere la gestión de todos los involucrados en la corporación.	85%
SERVIDOR	SERVIDOR DE ACCESO A INFORMACIÒN Y CONTROL DE IMPRESIÒN	Sobrecalentamiento e incendio de equipos por deficiencia en la aclimatación ambiental del servidor.	Instalación de aires acondicionados nuevos y funcionales. Implementar medidores de temperatura con alertas.	Los aires acondicionados en normal funcionamiento permiten mantener estable la temperatura y evitar sobrecalentamientos en los servidores. Los mecanismos de alerta a cambios bruscos de temperatura controlaran la estabilidad del ambiente en la sala de servidores	100%

NOMBRE CORTO	ACTIVO	AMENAZAS	SALVAGUARDAS	VALORACIÒN DE SALVAGUARDAS	
				EFICACIA	EFECTIVIDAD
		Incendio deliberado por personal interno o externo de la Corporación.	Control de acceso a través de tarjetas de acceso. Usuario y contraseña al centro de datos de la Corporación.	Restringir el acceso a través de usuario y contraseña, o control de acceso biométrico permite controlar de forma eficaz y efectiva la administración de elementos tecnológicos que se encuentren en la sala de servidores y centro de datos.	100%
		Daños en la estructura del servidor por caída de concreto y hierro reforzado por temblor (Desastre Natural)	Mantener Backup de la información en la Nube, como garantía para reestablecer los servicios de información.	Contar con copias de respaldo de toda la información que se maneja en la Corporación permite recuperar rápidamente el funcionamiento del sistema.	100%
		Daños en el servidor por sobrecargas de alto voltaje eléctrico en el mismo.	Adquirir UPS y supresor de picos de alto voltaje para proteger los servidores.	Con el estabilizador y la UPS funcional, los servidores no tendrán fallas en su funcionamiento.	100%
		Fallas de funcionamiento en el servidor por defectos en el software.	Implementar procedimiento para ingreso y entrada de bienes de tecnología a la corporación.	Con procedimientos claros y responsabilidades asignadas a cada funcionario del área de sistemas, se controlará que los elementos adquiridos sean de excelente calidad.	100%
		Fallas en el funcionamiento del servidor por el hardware.	Implementar procedimiento para ingreso y entrada de bienes de tecnología a la corporación.	Con procedimientos claros y responsabilidades asignadas a cada funcionario del área de sistemas, se controlará que los elementos adquiridos sean de excelente calidad.	100%
		Fallas en el funcionamiento por cortes del suministro eléctrico	Realizar mantenimiento a la planta eléctrica y a la UPS que suministra corriente eléctrica y alterna a los servidores.	Los servidores deben contar con la energía necesaria, por lo tanto, el mantenimiento preventivo y correctivo de fallas de UPS y planta eléctrica debe ser constante. Esto evitara fallas o apagones del servidor, por esta causa.	100%
		Accesos no autorizados al servidor.	Implementar IPS e IDS, para detección de intrusos. Implementar firewall para la red de datos y para los sistemas de información web.	Los Sistemas de Protección y Detección de intrusos ayudan a detectar los accesos no autorizados al sistema, así mismo, con los IPS, se lograra contener los ataques. También la implementación de Firewall reducirá el número de ataques de virus y páginas con código malicioso en la red de datos.	100%
		Ataque de virus.	Actualizar las licencias de antivirus para servidores.	Cada uno de los servidores y equipos debe contar con su antivirus licenciado y actualizado, brindando	100%

NOMBRE CORTO	ACTIVO	AMENAZAS	SALVAGUARDAS	VALORACIÒN DE SALVAGUARDAS	
				EFICACIA	EFECTIVIDAD
				seguridad optima a los mismos.	
		Ataques de denegación de servicio.	Documentar el procedimiento contra este tipo de ataque de denegación de servicios. Identificar los tipos de paquetes de bloqueo que se envían a la red y bloquearlos en los equipos de red o redirigiéndolos.	La política de seguridad permite que a través de su gestión se logre contener este tipo de ataques, para lo cual se requiere la gestión de todos los involucrados en la corporación.	85%
SERVIDOR	SERVIDOR DE APLICACIONES WEB (SISTEMA DE INFORMACIÒN DE GESTIÒN DOCUMENTAL Y BASE DE DATOS)	Sobrecalentamiento e incendio de equipos por deficiencia en la aclimatación ambiental del servidor.	Instalación de aires acondicionados nuevos y funcionales. Implementar medidores de temperatura con alertas.	Los aires acondicionados en normal funcionamiento permiten mantener estable la temperatura y evitar sobrecalentamientos en los servidores. Los mecanismos de alerta a cambios bruscos de temperatura controlaran la estabilidad del ambiente en la sala de servidores	100%
		Incendio deliberado por personal interno o externo de la Corporación.	Control de acceso a través de tarjetas de acceso. Usuario y contraseña al centro de datos de la Corporación.	Restringir el acceso a través de usuario y contraseña, o control de acceso biométrico permite controlar de forma eficaz y efectiva la administración de elementos tecnológicos que se encuentren en la sala de servidores y centro de datos.	100%
		Daños en la estructura del servidor por caída de concreto y hierro reforzado por temblor (Desastre Natural)	Mantener Backup de la información en la Nube, como garantía para reestablecer los servicios de información.	Contar con copias de respaldo de toda la información que se maneja en la Corporación permite recuperar rápidamente el funcionamiento del sistema.	100%
		Daños en el servidor por sobrecargas de alto voltaje eléctrico en el mismo.	Adquirir UPS y supresor de picos de alto voltaje para proteger los servidores.	Con el estabilizador y la UPS funcional, los servidores no tendrán fallas en su funcionamiento.	100%
		Fallas de funcionamiento en el servidor por defectos en el software.	Implementar procedimiento para ingreso y entrada de bienes de tecnología a la corporación.	Con procedimientos claros y responsabilidades asignadas a cada funcionario del área de sistemas, se controlará que los elementos adquiridos sean de excelente calidad.	100%
		Fallas en el funcionamiento del servidor por el hardware.	Implementar procedimiento para ingreso y entrada de bienes de tecnología a la corporación.	Con procedimientos claros y responsabilidades asignadas a cada funcionario del área de sistemas, se controlará que los elementos adquiridos	100%

NOMBRE CORTO	ACTIVO	AMENAZAS	SALVAGUARDAS	VALORACIÒN DE SALVAGUARDAS	
				EFICACIA	EFECTIVIDAD
				sean de excelente calidad.	
		Fallas en el funcionamiento por cortes del suministro eléctrico	Realizar mantenimiento a la planta eléctrica y a la UPS que suministra corriente eléctrica y alterna a los servidores.	Los servidores deben contar con la energía necesaria, por lo tanto, el mantenimiento preventivo y correctivo de fallas de UPS y planta eléctrica debe ser constante. Esto evitara fallas o apagones del servidor, por esta causa.	100%
		Accesos no autorizados al servidor.	Implementar IPS e IDS, para detección de intrusos. Implementar firewall para la red de datos y para los sistemas de información web.	Los Sistemas de Protección y Detección de intrusos ayudan a detectar los accesos no autorizados al sistema, así mismo, con los IPS, se lograra contener los ataques. También la implementación de Firewall reducirá el número de ataques de virus y páginas con código malicioso en la red de datos.	100%
		Ataque de virus.	Actualizar las licencias de antivirus para servidores.	Cada uno de los servidores y equipos debe contar con su antivirus licenciado y actualizado, brindando seguridad optima a los mismos.	100%
		Ataques de denegación de servicio.	Documentar el procedimiento contra este tipo de ataque de denegación de servicios. Identificar los tipos de paquetes de bloqueo que se envían a la red y bloquearlos en los equipos de red o redirigiéndolos.	La política de seguridad permite que a través de su gestión se logre contener este tipo de ataques, para lo cual se requiere la gestión de todos los involucrados en la corporación.	85%
SERVIDOR	SERVIDOR DE APLICACIONES - SISTEMA DE INFORMACIÒN GEOGRAFICO - SIGCOR.	Sobrecalentamiento e incendio de equipos por deficiencia en la aclimatación ambiental del servidor.	Instalación de aires acondicionados nuevos y funcionales. Implementar medidores de temperatura con alertas.	Los aires acondicionados en normal funcionamiento permiten mantener estable la temperatura y evitar sobrecalentamientos en los servidores. Los mecanismos de alerta a cambios bruscos de temperatura controlaran la estabilidad del ambiente en la sala de servidores	100%
		Incendio deliberado por personal interno o externo de la Corporación.	Control de acceso a través de tarjetas de acceso. Usuario y contraseña al centro de datos de la Corporación.	Restringir el acceso a través de usuario y contraseña, o control de acceso biométrico permite controlar de forma eficaz y efectiva la administración de elementos tecnológicos que se encuentren en la sala de servidores y centro de datos.	100%

NOMBRE CORTO	ACTIVO	AMENAZAS	SALVAGUARDAS	VALORACIÒN DE SALVAGUARDAS	
				EFICACIA	EFECTIVIDAD
		Daños en la estructura del servidor por caída de concreto y hierro reforzado por temblor (Desastre Natural)	Mantener Backup de la información en la Nube, como garantía para reestablecer los servicios de información.	Contar con copias de respaldo de toda la información que se maneja en la Corporación permite recuperar rápidamente el funcionamiento del sistema.	100%
		Daños en el servidor por sobrecargas de alto voltaje eléctrico en el mismo.	Adquirir UPS y supresor de picos de alto voltaje para proteger los servidores.	Con el estabilizador y la UPS funcional, los servidores no tendrán fallas en su funcionamiento.	100%
		Fallas de funcionamiento en el servidor por defectos en el software.	Implementar procedimiento para ingreso y entrada de bienes de tecnología a la corporación.	Con procedimientos claros y responsabilidades asignadas a cada funcionario del área de sistemas, se controlará que los elementos adquiridos sean de excelente calidad.	100%
		Fallas en el funcionamiento del servidor por el hardware.	Implementar procedimiento para ingreso y entrada de bienes de tecnología a la corporación.	Con procedimientos claros y responsabilidades asignadas a cada funcionario del área de sistemas, se controlará que los elementos adquiridos sean de excelente calidad.	100%
		Fallas en el funcionamiento por cortes del suministro eléctrico	Realizar mantenimiento a la planta eléctrica y a la UPS que suministra corriente eléctrica y alterna a los servidores.	Los servidores deben contar con la energía necesaria, por lo tanto, el mantenimiento preventivo y correctivo de fallas de UPS y planta eléctrica debe ser constante. Esto evitara fallas o apagones del servidor, por esta causa.	100%
		Accesos no autorizados al servidor.	Implementar IPS e IDS, para detección de intrusos. Implementar firewall para la red de datos y para los sistemas de información web.	Los Sistemas de Protección y Detección de intrusos ayudan a detectar los accesos no autorizados al sistema, así mismo, con los IPS, se lograra contener los ataques. También la implementación de Firewall reducirá el número de ataques de virus y páginas con código malicioso en la red de datos.	100%
		Ataque de virus.	Actualizar las licencias de antivirus para servidores.	Cada uno de los servidores y equipos debe contar con su antivirus licenciado y actualizado, brindando seguridad optima a los mismos.	100%
		Ataques de denegación de servicio.	Documentar el procedimiento contra este tipo de ataque de denegación de servicios. Identificar los tipos de paquetes de bloqueo que se	La política de seguridad permite que a través de su gestión se logre contener este tipo de ataques, para lo cual se requiere la gestión de todos los involucrados en la corporación.	85%

NOMBRE CORTO	ACTIVO	AMENAZAS	SALVAGUARDAS	VALORACIÒN DE SALVAGUARDAS	
				EFICACIA	EFECTIVIDAD
			envían a la red y bloquearlos en los equipos de red o redirigiéndolos.		
PCT	SISTEMA DE INFORMACIÓN FINANCIERO	Accesos no autorizados al Sistema de Información y escalamiento de privilegios.	Realizar procedimiento de control de accesos para usuarios del sistema de información. Implementar Firewall para seguridad del sistema de información.	La salvaguarda es eficaz para proteger accesos no autorizados.	100%
		Ataques de SQL Injection	Realizar procedimiento para aplicar en el desarrollo de software seguro, que impidan lo ataques de SQL Injection. Implementar Firewall para seguridad del sistema de información.	El procedimiento para desarrollo de software seguro, permitirá cubrir todas las posibles vulnerabilidades y sobre todo las relacionadas con SQL Injection.	100%
PAGINA WEB	PAGINA WEB CORPORINOQUIA	Accesos no autorizados al Sitio Web y escalamiento de privilegios.	Realizar procedimiento de control de accesos para usuarios del sitio web.	La salvaguarda es eficaz para proteger accesos no autorizados.	100%
		Ataques de SQL Injection	Realizar procedimiento para aplicar en el desarrollo de software seguro, que impidan lo ataques de SQL Injection. Implementar Firewall para seguridad del Sitio Web.	El procedimiento para desarrollo de software seguro, permitirá cubrir todas las posibles vulnerabilidades y sobre todo las relacionadas con SQL Injection.	100%
ATHENTO	SISTEMA DE INFORMACIÓN DE GESTIÓN DOCUMENTAL	Accesos no autorizados al Sistema de Información y escalamiento de privilegios.	Realizar procedimiento de control de accesos para usuarios del sitio web.	La salvaguarda es eficaz para proteger accesos no autorizados.	100%
		Ataques de SQL Injection	Realizar procedimiento para aplicar en el desarrollo de software seguro, que impidan lo ataques de SQL Injection.	El procedimiento para desarrollo de software seguro, permitirá cubrir todas las posibles vulnerabilidades y sobre todo las relacionadas con SQL Injection.	100%
CORREO ELECTRONICO	CORREO ELECTRONICO CORPORATIVO	Caídas del servicio de Correo por bajo nivel de espacio de almacenamiento.	Adquirir un servidor dedicado en la nube con amplio espacio de almacenamiento para el correo electrónico Corporativo.		

NOMBRE CORTO	ACTIVO	AMENAZAS	SALVAGUARDAS	VALORACIÒN DE SALVAGUARDAS	
				EFICACIA	EFECTIVIDAD
		Accesos no autorizados a la administración del servidor de correo electrónico.	Realizar procedimiento de control de accesos para usuarios del correo electrónico Corporativo.	La salvaguarda es eficaz para proteger accesos no autorizados.	100%
		Suplantación de correos electrónicos.	Realizar procedimiento de control de accesos para usuarios del correo electrónico Corporativo y cuidado que los usuarios debe tener con ataques de ingeniería social, uso de usuarios y contraseñas.	El procedimiento de control de accesos permitirá a los usuarios ser cuidadosos con sus cuentas de correo, proteger la información corporativa y garantizar que la información no sea alterada.	100%
SAN	SAN - STORAGE AREA NETWORK.	Cese de capacidad de transmitir datos para consulta y guardado de información a los usuarios y el sistema.	Adquirir una SAN con mayor capacidad de almacenamiento que permita guardar la totalidad de la información producida en la Corporación.	Es necesario ampliar el espacio de almacenamiento de la información generada en Corporinoquia, para lo cual adquirir una nueva SAN ayudará con esta necesidad.	100%
		Fallas en el hardware de almacenamiento por falta de mantenimiento, sobrecalentamiento e incendio por deficiencia en la aclimatación ambiental.	Realizar procedimiento para el mantenimiento de la SAN y adquirir elementos de protección y aclimatación ambiental para el centro de datos.	El procedimiento de mantenimiento preventivo y correctivo de equipos, permitirá mayor durabilidad y funcionalidad de la SAN y los demás equipos de tecnología.	100%
		Daño lógico por la configuración de la SAN.	Realizar procedimiento para la adquisición de elementos tecnológicos y pruebas de elementos a adquirir e implementar en la Corporación.	Con procedimientos claros y responsabilidades asignadas a cada funcionario del área de sistemas, se controlará que los elementos adquiridos sean de excelente calidad y cuenten con la debida configuración de los mismos.	100%
UPS	UPS RACK DE SERVIDOR PRINCIPAL - 6 KVA - CENTRO DE DATOS	Fallas en el sistema de UPS por baterías en mal estado de funcionamiento.	Realizar procedimiento de mantenimiento para UPS y establecer controles que permitan identificar el estado de funcionamiento de la UPS.	Activar los controles de aviso de las UPS al momento de quedarse sin energía eléctrica es fundamentales para evitar apagones en los equipos a los cuales están conectados. El procedimiento de mantenimiento de UPS permita controlar rápidamente las posibles fallas en los mismos.	100%

NOMBRE CORTO	ACTIVO	AMENAZAS	SALVAGUARDAS	VALORACIÒN DE SALVAGUARDAS	
				EFICACIA	EFECTIVIDAD
		Fallas o daños por voltaje excesivo en la ups que protege el servidor.	Realizar procedimiento que permita el control del estado de funcionamiento de la UPS.	El procedimiento de control incluye la instalación de estabilizador de energía para control de picos de energía.	100%
		Mal funcionamiento por falta de mantenimiento.	Realizar procedimiento de mantenimiento para UPS.	El procedimiento de mantenimiento de UPS permitirá establecer claramente las actividades de control para que las UPS estén en continuo funcionamiento.	100%
RACK	RACK PRINCIPAL DE COMUNICACIONES - CENTRAL DE DATOS.	Perdida de estabilidad y robustez del rack principal por mal armado en su estructura.	Realizar procedimiento de adquisición de elementos estructurales y tecnología en la Corporación.	El procedimiento permitirá a los supervisores de contratos de adquisición de tecnología verificar que se cumpla con el 100% de requisitos.	100%
		Daños causados por manipulación y accesos de personal no autorizado.	Realizar procedimiento de Control de Accesos y manipulación de elementos y tecnología en la central de datos.	El procedimiento de control de acceso permitirá restringir el acceso de personas a este tipo de elementos y zonas de centro de datos.	100%
SWITCH	SWITCH CORE 24 PUERTOS - 10/100/1000 - CENTRO DE DATOS.	Fallas en el hardware por falta de mantenimiento, sobrecalentamiento y/o incendio por deficiencia en la aclimatación ambiental.	Realizar procedimiento para el desarrollo de mantenimiento preventivo y correctivo de Switch's. Adquirir elementos de protección y aclimatación ambiental para el centro de datos.	El procedimiento de manteamiento de los Switch`s permitirá claramente definir las actividades de mantenimiento de los mismos. Y la adquisición de equipos de aclimatación ambiental facilitará el ambiente adecuado de funcionalidad de los mismos.	100%
		Interrupción del servicio causado por manipulación física realizada a los Switch's por personal no autorizado.	Realizar procedimiento de control de accesos a manipulación de Switch's.	El procedimiento establecerá las personas que están autorizadas para intervenir los Switch's de la Corporación y los permisos necesarios para acceder a ellos.	100%
		Mal funcionamiento por falta de mantenimiento.	Realizar procedimiento de mantenimiento de Switch's.	El procedimiento de manteamiento de los Switch`s permitirá claramente definir las actividades de mantenimiento de los mismos.	100%
		Denegación del servicio por accesos lógicos no autorizados a los Switch's.	Implementar procedimiento para defender la red de datos de la Corporación.	Este procedimiento permitirá mantener el control de los accesos y los mecanismos necesarios para proteger la red de datos y los equipos de cómputo, incluido servidores.	100%

NOMBRE CORTO	ACTIVO	AMENAZAS	SALVAGUARDAS	VALORACIÒN DE SALVAGUARDAS	
				EFICACIA	EFECTIVIDAD
		Fallas por interrupciones del servicio eléctrico.	Implementar procedimiento para garantizar la estabilidad de energía eléctrica y regulada a los equipos tecnológicos de la Corporación.	Este procedimiento busca fortalecer los mecanismos de suministro de energía eléctrica y regulada para los diferentes equipos de la red de datos.	100%
SWITCH	SWITCH 48 PUERTOS - 10/100/1000 - CENTRO DE DATOS	Fallas en el hardware por falta de mantenimiento, sobrecalentamiento y/o incendio por deficiencia en la aclimatación ambiental.	Realizar procedimiento para el desarrollo de mantenimiento preventivo y correctivo de Switch's. Adquirir elementos de protección y aclimatación ambiental para el centro de datos.	El procedimiento de manteamiento de los Switch`s permitirá claramente definir las actividades de mantenimiento de los mismos. Y la adquisición de equipos de aclimatación ambiental facilitará el ambiente adecuado de funcionalidad de los mismos.	100%
		Interrupción del servicio causado por manipulación física realizada a los Switch's por personal no autorizado.	Realizar procedimiento de control de accesos a manipulación de Switch's.	El procedimiento establecerá las personas que están autorizadas para intervenir los Switch's de la Corporación y los permisos necesarios para acceder a ellos.	100%
		Mal funcionamiento por falta de mantenimiento.	Realizar procedimiento de mantenimiento de Switch's.	El procedimiento de manteamiento de los Switch`s permitirá claramente definir las actividades de mantenimiento de los mismos.	100%
		Denegación del servicio por accesos lógicos no autorizados a los Switch's.	Implementar procedimiento para defender la red de datos de la Corporación.	Este procedimiento permitirá mantener el control de los accesos y los mecanismos necesarios para proteger la red de datos y los equipos de cómputo, incluido servidores.	100%
		Fallas por interrupciones del servicio eléctrico.	Implementar procedimiento para garantizar la estabilidad de energía eléctrica y regulada a los equipos tecnológicos de la Corporación.	Este procedimiento busca fortalecer los mecanismos de suministro de energía eléctrica y regulada para los diferentes equipos de la red de datos.	100%
SWITCH	SWITCH 48 PUERTOS - 10/100/1000 - CENTRO DE DATOS	Fallas en el hardware por falta de mantenimiento, sobrecalentamiento y/o incendio por deficiencia en la aclimatación ambiental.	Realizar procedimiento para el desarrollo de mantenimiento preventivo y correctivo de Switch's. Adquirir elementos de protección y aclimatación ambiental para el centro de datos.	El procedimiento de manteamiento de los Switch`s permitirá claramente definir las actividades de mantenimiento de los mismos. Y la adquisición de equipos de aclimatación ambiental facilitará el ambiente adecuado de funcionalidad de los mismos.	100%

NOMBRE CORTO	ACTIVO	AMENAZAS	SALVAGUARDAS	VALORACIÒN DE SALVAGUARDAS	
				EFICACIA	EFECTIVIDAD
		Interrupción del servicio causado por manipulación física realizada a los Switch's por personal no autorizado.	Realizar procedimiento de control de accesos a manipulación de Switch's.	El procedimiento establecerá las personas que están autorizadas para intervenir los Switch's de la Corporación y los permisos necesarios para acceder a ellos.	100%
		Mal funcionamiento por falta de mantenimiento.	Realizar procedimiento de mantenimiento de Switch's.	El procedimiento de manteamiento de los Switch`s permitirá claramente definir las actividades de mantenimiento de los mismos.	100%
		Denegación del servicio por accesos lógicos no autorizados a los Switch's.	Implementar procedimiento para defender la red de datos de la Corporación.	Este procedimiento permitirá mantener el control de los accesos y los mecanismos necesarios para proteger la red de datos y los equipos de cómputo, incluido servidores.	100%
		Fallas por interrupciones del servicio eléctrico.	Implementar procedimiento para garantizar la estabilidad de energía eléctrica y regulada a los equipos tecnológicos de la Corporación.	Este procedimiento busca fortalecer los mecanismos de suministro de energía eléctrica y regulada para los diferentes equipos de la red de datos.	100%
RACK	RACK SECUNDARIO DE COMUNICACIONES-SUBDIRECCIÒN ADMINISTRATIVA Y FINANCIERA.	Perdida de estabilidad y robustez del rack principal por mala configuración en su estructura.	Realizar procedimiento de adquisición de elementos estructurales y tecnología en la Corporación.	El procedimiento permitirá a los supervisores de contratos de adquisición de tecnología verificar que se cumpla con el 100% de requisitos.	100%
		Daños causados por manipulación y accesos de personal no autorizado.	Realizar procedimiento de Control de Accesos y manipulación de elementos y tecnología en la central de datos.	El procedimiento de control de acceso permitirá restringir el acceso de personas a este tipo de elementos y zonas de centro de datos.	100%
SWITCH	SWITCH CORE 24 PUERTOS - 10/100/1000 - SUBDIRECCIÒN ADMINISTRATIVA Y FINANCIERA.	Fallas en el hardware por falta de mantenimiento, sobrecalentamiento y/o incendio por deficiencia en la aclimatación ambiental.	Realizar procedimiento para el desarrollo de mantenimiento preventivo y correctivo de Switch's. Adquirir elementos de protección y aclimatación ambiental para el centro de datos.	El procedimiento de manteamiento de los Switch`s permitirá claramente definir las actividades de mantenimiento de los mismos. Y la adquisición de equipos de aclimatación ambiental facilitará el ambiente adecuado de funcionalidad de los mismos.	100%
		Interrupción del servicio causado por manipulación física realizada a los Switch's por personal no	Realizar procedimiento de control de accesos a manipulación de Switch's.	El procedimiento establecerá las personas que están autorizadas para intervenir los Switch's de la Corporación y los permisos necesarios para acceder a	100%

NOMBRE CORTO	ACTIVO	AMENAZAS	SALVAGUARDAS	VALORACIÒN DE SALVAGUARDAS	
				EFICACIA	EFECTIVIDAD
		autorizado.		ellos.	
		Mal funcionamiento por falta de mantenimiento.	Realizar procedimiento de mantenimiento de Switch's.	El procedimiento de manteamiento de los Switch`s permitirá claramente definir las actividades de mantenimiento de los mismos.	100%
		Denegación del servicio por accesos lógicos no autorizados a los Switch's.	Implementar procedimiento para defender la red de datos de la Corporación.	Este procedimiento permitirá mantener el control de los accesos y los mecanismos necesarios para proteger la red de datos y los equipos de cómputo, incluido servidores.	100%
		Fallas por interrupciones del servicio eléctrico.	Implementar procedimiento para garantizar la estabilidad de energía eléctrica y regulada a los equipos tecnológicos de la Corporación.	Este procedimiento busca fortalecer los mecanismos de suministro de energía eléctrica y regulada para los diferentes equipos de la red de datos.	100%
SWITCH	SWITCH 48 PUERTOS - 10/100/1000 - CENTRO DE DATOS - SUBDIRECCIÒN ADMINISTRATIVA Y FINANCIERA.	Fallas en el hardware por falta de mantenimiento, sobrecalentamiento y/o incendio por deficiencia en la aclimatación ambiental.	Realizar procedimiento para el desarrollo de mantenimiento preventivo y correctivo de Switch's. Adquirir elementos de protección y aclimatación ambiental para el centro de datos.	El procedimiento de manteamiento de los Switch`s permitirá claramente definir las actividades de mantenimiento de los mismos. Y la adquisición de equipos de aclimatación ambiental facilitará el ambiente adecuado de funcionalidad de los mismos.	100%
		Interrupción del servicio causado por manipulación física realizada a los Switch's por personal no autorizado.	Realizar procedimiento de control de accesos a manipulación de Switch's.	El procedimiento establecerá las personas que están autorizadas para intervenir los Switch's de la Corporación y los permisos necesarios para acceder a ellos.	100%
		Mal funcionamiento por falta de mantenimiento.	Realizar procedimiento de mantenimiento de Switch's.	El procedimiento de manteamiento de los Switch`s permitirá claramente definir las actividades de mantenimiento de los mismos.	100%
		Denegación del servicio por accesos lógicos no autorizados a los Switch's.	Implementar procedimiento para defender la red de datos de la Corporación.	Este procedimiento permitirá mantener el control de los accesos y los mecanismos necesarios para proteger la red de datos y los equipos de cómputo, incluido servidores.	100%
		Fallas por interrupciones del servicio eléctrico.	Implementar procedimiento para garantizar la	Este procedimiento busca fortalecer los mecanismos de suministro de energía	100%

NOMBRE CORTO	ACTIVO	AMENAZAS	SALVAGUARDAS	VALORACIÒN DE SALVAGUARDAS	
				EFICACIA	EFECTIVIDAD
			estabilidad de energía eléctrica y regulada a los equipos tecnológicos de la Corporación.	eléctrica y regulada para los diferentes equipos de la red de datos.	
RACK	RACK SECUNDARIO DE COMUNICACIONES - SUBDIRECCIÒN DE PLANEACIÒN AMBIENTAL.	Perdida de estabilidad y robustez del rack principal por mala configuración en su estructura.	Realizar procedimiento de adquisición de elementos estructurales y tecnología en la Corporación.	El procedimiento permitirá a los supervisores de contratos de adquisición de tecnología verificar que se cumpla con el 100% de requisitos.	100%
		Daños causados por manipulación y accesos de personal no autorizado.	Realizar procedimiento de Control de Accesos y manipulación de elementos y tecnología en la central de datos.	El procedimiento de control de acceso permitirá restringir el acceso de personas a este tipo de elementos y zonas de centro de datos.	100%
SWITCH	SWITCH CORE 24 PUERTOS - 10/100/1000 - SUBDIRECCIÒN DE PLANEACIÒN AMBIENTAL.	Fallas en el hardware por falta de mantenimiento, sobrecalentamiento y/o incendio por deficiencia en la aclimatación ambiental.	Realizar procedimiento para el desarrollo de mantenimiento preventivo y correctivo de Switch's. Adquirir elementos de protección y aclimatación ambiental para el centro de datos.	El procedimiento de manteamiento de los Switch`s permitirá claramente definir las actividades de mantenimiento de los mismos. Y la adquisición de equipos de aclimatación ambiental facilitará el ambiente adecuado de funcionalidad de los mismos.	100%
		Interrupción del servicio causado por manipulación física realizada a los Switch's por personal no autorizado.	Realizar procedimiento de control de accesos a manipulación de Switch's.	El procedimiento establecerá las personas que están autorizadas para intervenir los Switch's de la Corporación y los permisos necesarios para acceder a ellos.	100%
		Mal funcionamiento por falta de mantenimiento.	Realizar procedimiento de mantenimiento de Switch's.	El procedimiento de manteamiento de los Switch`s permitirá claramente definir las actividades de mantenimiento de los mismos.	100%
		Denegación del servicio por accesos lógicos no autorizados a los Switch's.	Implementar procedimiento para defender la red de datos de la Corporación.	Este procedimiento permitirá mantener el control de los accesos y los mecanismos necesarios para proteger la red de datos y los equipos de cómputo, incluido servidores.	100%
		Fallas por interrupciones del servicio eléctrico.	Implementar procedimiento para garantizar la estabilidad de energía eléctrica y regulada a los equipos tecnológicos de la Corporación.	Este procedimiento busca fortalecer los mecanismos de suministro de energía eléctrica y regulada para los diferentes equipos de la red de datos.	100%

NOMBRE CORTO	ACTIVO	AMENAZAS	SALVAGUARDAS	VALORACIÒN DE SALVAGUARDAS	
				EFICACIA	EFECTIVIDAD
SWITCH	SWITCH 48 PUERTOS - 10/100/1000 - SUBDIRECCIÒN DE PLANEACIÒN AMBIENTAL.	Fallas en el hardware por falta de mantenimiento, sobrecalentamiento y/o incendio por deficiencia en la aclimatación ambiental.	Realizar procedimiento para el desarrollo de mantenimiento preventivo y correctivo de Switch's. Adquirir elementos de protección y aclimatación ambiental para el centro de datos.	El procedimiento de manteamiento de los Switch`s permitirá claramente definir las actividades de mantenimiento de los mismos. Y la adquisición de equipos de aclimatación ambiental facilitará el ambiente adecuado de funcionalidad de los mismos.	100%
		Interrupción del servicio causado por manipulación física realizada a los Switch's por personal no autorizado.	Realizar procedimiento de control de accesos a manipulación de Switch's.	El procedimiento establecerá las personas que están autorizadas para intervenir los Switch's de la Corporación y los permisos necesarios para acceder a ellos.	100%
		Mal funcionamiento por falta de mantenimiento.	Realizar procedimiento de mantenimiento de Switch's.	El procedimiento de manteamiento de los Switch`s permitirá claramente definir las actividades de mantenimiento de los mismos.	100%
		Denegación del servicio por accesos lógicos no autorizados a los Switch's.	Implementar procedimiento para defender la red de datos de la Corporación.	Este procedimiento permitirá mantener el control de los accesos y los mecanismos necesarios para proteger la red de datos y los equipos de cómputo, incluido servidores.	100%
		Fallas por interrupciones del servicio eléctrico.	Implementar procedimiento para garantizar la estabilidad de energía eléctrica y regulada a los equipos tecnológicos de la Corporación.	Este procedimiento busca fortalecer los mecanismos de suministro de energía eléctrica y regulada para los diferentes equipos de la red de datos.	100%
CABLEADO ESTRUCTURADO	CABLEADO ESTRUCTURADO CATEGORIA 6 Y RED DE DATOS y CANALETA.	Daños en el cableado estructurado por canaletas abiertas al aire libre y por mala manipulación de personal no autorizado.	Realizar procedimiento para realizar mantenimiento preventivo y correctivo al cableado estructurado de la red de datos de la Corporación, el uso y su implementación. Disponer de los elementos y personal idóneo para realizar el mantenimiento del cableado.	Contar con el procedimiento, el personal y los materiales de mantenimiento preventivo y correctivo del cableado de la red de datos permite mantener funcional la misma.	100%

NOMBRE CORTO	ACTIVO	AMENAZAS	SALVAGUARDAS	VALORACIÒN DE SALVAGUARDAS	
				EFICACIA	EFECTIVIDAD
		Fallas en las comunicaciones por daños en cableado estructurado.	Realizar procedimiento para realizar mantenimiento preventivo y correctivo al cableado estructurado de la red de datos de la Corporación, el uso y su implementación.	Contar con el procedimiento, el personal y los materiales de mantenimiento preventivo y correctivo del cableado de la red de datos permite mantener funcional la misma.	100%
		Accesos no autorizados a los puntos de red del cableado estructurado.	Realizar procedimiento de control de accesos a la red de datos de la Corporación y divulgarlo.	Con el procedimiento de acceso a la red de datos y hacer su respectiva divulgación todos cuidaran de la red y no se presentaran ataques de accesos no autorizados.	100%
		Incendio deliberado por personal interno o externo de la Corporación, o por corto circuitos producidos en la red de corriente eléctrica.	Realizar procedimiento de control de accesos a la red de datos de la Corporación.	Con el procedimiento de acceso a la red de datos y hacer su respectiva divulgación todos cuidaran de la red y no se presentaran ataques de accesos no autorizados.	100%
CORRIENTE REGULADA	CABLEADO DE COBRE DE CORRIENTE REGULADA PARA EQUIPOS DE CÓMPUTO.	Daños en el cableado de corriente regulada, canaletas abiertas al aire libre y por mala manipulación de personal no autorizado.	Realizar procedimiento para realizar mantenimiento preventivo y correctivo al cableado de la red de corriente regulada de la Corporación, el uso y su implementación. Disponer de los elementos y personal idóneo para realizar el mantenimiento del cableado.	Contar con el procedimiento, el personal y los materiales de mantenimiento preventivo y correctivo del cableado de corriente eléctrica y regulada permite mantener funcional la misma.	100%
		Fallas en el cableado de corriente regulada por Corto circuito.	Realizar procedimiento para realizar salvaguardarle cableado de corriente regulada de la Corporación y el uso que deben dar los usuarios.	Contar con el procedimiento, el personal y los materiales de mantenimiento preventivo y correctivo del cableado de corriente eléctrica y regulada permite mantener funcional la misma.	100%
		Daños en el cableado de corriente regulada y disminución en la capacidad de respuesta de las UPS, por conexión de equipos no autorizados (Mal	Realizar procedimiento para realizar salvaguardar el cableado de corriente regulada de la Corporación y el uso que deben dar los usuarios.	Con el procedimiento de acceso a la red de del cableado de corriente eléctrica y regulada y hacer su respectiva divulgación todos cuidaran de la red y no se presentaran ataques de accesos no autorizados.	100%

NOMBRE CORTO	ACTIVO	AMENAZAS	SALVAGUARDAS	VALORACIÒN DE SALVAGUARDAS	
				EFICACIA	EFECTIVIDAD
		uso).	Garantizar el mantenimiento y funcionamiento normal de las UPS.		
		Incendio deliberado o accidental, causado por personal interno o externo de la Corporación, o por corto circuitos producidos en la red de corriente eléctrica.	Realizar procedimiento de control de accesos y mantenimiento a la red de corriente eléctrica y regulada de la Corporación.	Con el procedimiento de acceso a la red de del cableado de corriente eléctrica y regulada y hacer su respectiva divulgación todos cuidaran de la red y no se presentaran ataques de accesos no autorizados.	100%
UPS	UPS DE 20 KVA, PROTECCIÒN DE EQUIPOS DE COMPUTO SUBDIRECCIÒN DE PLANEACIÒN Y CENTRO DE DOCUMENTOS.	Fallas en el sistema de UPS por baterías en mal estado de funcionamiento.	Realizar procedimiento de mantenimiento preventivo y correctivo de UPS.	El procedimiento de mantenimiento de UPS permitirá establecer claramente las actividades de control para que las UPS estén en continuo funcionamiento.	100%
		Fallas o daños por voltaje excesivo en la UPS.	Realizar procedimiento de mantenimiento, seguimiento y control al funcionamiento de UPS.	El procedimiento de mantenimiento de UPS permitirá establecer claramente las actividades de control para que las UPS estén en continuo funcionamiento.	100%
		Daños en la UPS por mala configuración y/o disminución de mantenimiento de la red de corriente regulada.	Realizar procedimiento para la adquisición de elementos tecnológicos (UPS) y pruebas de elementos a adquirir e implementar en la Corporación.	El procedimiento brindará herramientas para que todos los elementos tecnológicos que ingresen cumplan con el 100% de características funcionales.	100%
		Mal funcionamiento por falta de mantenimiento.	Realizar procedimiento de mantenimiento preventivo y correctivo de UPS. Generar controles para detectar fallos en el normal funcionamiento de las UPS.	El procedimiento de mantenimiento de UPS permitirá establecer claramente las actividades de control para que las UPS estén en continuo funcionamiento.	100%
UPS	UPS DE 30 KVA, PROTECCIÒN DE EQUIPOS DE COMPUTO	Fallas en el sistema de UPS por baterías en mal estado de funcionamiento.	Realizar procedimiento de mantenimiento preventivo y correctivo de UPS.	El procedimiento de mantenimiento de UPS permitirá establecer claramente las actividades de control para que las UPS estén en continuo funcionamiento.	100%

NOMBRE CORTO	ACTIVO	AMENAZAS	SALVAGUARDAS	VALORACIÒN DE SALVAGUARDAS	
				EFICACIA	EFECTIVIDAD
	SUBDIRECCIÒN DE CONTROL Y CALIDAD AMBIENTAL, SUBDIRECCIÒN ADMINISTRATIVA Y FINANCIERA Y DIRECCIÒN GENERAL.	Fallas o daños por voltaje excesivo en la UPS.	Realizar procedimiento de mantenimiento, seguimiento y control al funcionamiento de UPS.	El procedimiento de mantenimiento de UPS permitirá establecer claramente las actividades de control para que las UPS estén en continuo funcionamiento.	100%
		Daños en la UPS por mala configuración y/o disminución de mantenimiento de la red de corriente regulada.	Realizar procedimiento para la adquisición de elementos tecnológicos (UPS) y pruebas de elementos a adquirir e implementar en la Corporación.	El procedimiento brindará herramientas para que todos los elementos tecnológicos que ingresen cumplan con el 100% de características funcionales.	100%
		Mal funcionamiento por falta de mantenimiento.	Realizar procedimiento de mantenimiento preventivo y correctivo de UPS. Generar controles para detectar fallos en el normal funcionamiento de las UPS.	El procedimiento de mantenimiento de UPS permitirá establecer claramente las actividades de control para que las UPS estén en continuo funcionamiento.	100%
DOCUMENTOS IMPRESOS	INFORMACIÒN FISICA DEL CENTRO DE DOCUMENTOS DE CORPORINOQUIA, SEDE PRINCIPAL.	Incendio deliberado por personal interno o externo de la Corporación, o por corto circuitos producidos en la red de corriente eléctrica.	Realizar procedimiento de control de accesos a la información almacenada en el Centro de Documentos de la Corporación.	El procedimiento establece la forma como se debe prestar documentos y el acceso de los usuarios a dicha información, lo cual permitirá mantener controlada dicha información.	100%
		Robo de información.	Realizar procedimiento de control de accesos a la información almacenada en el Centro de Documentos de la Corporación.	El procedimiento establece la forma como se debe prestar documentos y el acceso de los usuarios a dicha información, lo cual permitirá mantener controlada dicha información.	100%
		Accesos no autorizados a la información.	Realizar procedimiento de control de accesos a la información almacenada en el Centro de Documentos de la Corporación.	El procedimiento establece la forma como se debe prestar documentos y el acceso de los usuarios a dicha información, lo cual permitirá mantener controlada dicha información.	100%
PLANTA ELECTRICA	PLANTA ELECTRICA LISTER DE 30 KVA	Corto circuito por alto voltaje.	Realizar procedimiento de implementación y uso de la Planta eléctrica de la Corporación. Instalar resistores que impidan daños por altos voltajes en la misma.	El procedimiento permitirá implementar controles que eviten daños en la planta eléctrica por corto circuito.	100%

NOMBRE CORTO	ACTIVO	AMENAZAS	SALVAGUARDAS	VALORACIÒN DE SALVAGUARDAS	
				EFICACIA	EFECTIVIDAD
		Incendio deliberado por personal interno o externo de la Corporación, o por corto circuitos producidos en la red de corriente eléctrica.	Realizar procedimiento de control de accesos a las áreas industriales donde se encuentra la planta eléctrica. Garantizar el normal funcionamiento de las UPS.	El procedimiento control de acceso a zonas industriales (planta eléctrica) permitirá el cuidado y funcionalidad de la planta eléctrica, evitando que personas no autorizadas ingresen a las instalaciones.	100%
		Mal manejo y Accesos no autorizados.	Realizar procedimiento de control de accesos a las áreas industriales donde se encuentra la planta eléctrica.	El procedimiento control de acceso a zonas industriales (planta eléctrica) permitirá el cuidado y funcionalidad de la planta eléctrica, evitando que personas no autorizadas ingresen a las instalaciones.	100%
		Daños por mala configuración.	Realizar procedimiento de implementación de elementos industriales y plantas eléctricas.	El procedimiento de uso e implementación de Plantas eléctricas en la entidad, permitirá realizar la configuración y uso de la planta de la mejor manera y por personal idóneo.	100%
		Mal funcionamiento por falta de mantenimiento.	Realizar procedimiento de mantenimiento preventivo y correctivo de la Planta Eléctrica.	El procedimiento de mantenimiento preventivo y correctivo de la planta eléctrica establecerá las actividades necesarias para intervenir la planta eléctrica y los requerimientos del personal que la intervenga para realizar mantenimiento.	100%
		No funciona por falta de combustible.	Realizar procedimiento para el cargue y tanquea de combustible a plantas eléctricas.	El procedimiento de cargue de combustible de la planta eléctrica, definirá el personal a realizar esta actividad, los momentos y los controles necesarios para realizar el cargue de combustible.	100%
EQUIPOS DE COMPUTO	EQUIPOS DE COMPUTO DE ESCRITORIO	Sobrecalentamiento e incendio de equipos por aumento en la temperatura ambiental.	Realizar procedimiento para mantener las áreas de trabajo de equipos tecnológicos debidamente aclimatadas. Establecer controles para identificar la variación de temperatura.	El procedimiento de implantación de áreas climatizadas facilitará la forma como se deben instalar, mantener y controlar las áreas donde se encuentran los equipos de cómputo y sala de servidores para mantener la estabilidad ambiental, evitando daños por sobrecalentamientos en los equipos.	100%
		Incendio deliberado por personal interno o externo de la Corporación.	Realizar procedimiento de Control de Acceso a las instalaciones de la Corporación y equipos de cómputo.	El procedimiento control de acceso y su divulgación permitirá el cuidado y funcionalidad de los equipos, evitando que personas no autorizadas ingresen a las instalaciones.	100%

NOMBRE CORTO	ACTIVO	AMENAZAS	SALVAGUARDAS	VALORACIÒN DE SALVAGUARDAS	
				EFICACIA	EFECTIVIDAD
		Daños en la estructura del equipo de cómputo por caída de concreto y hierro reforzado por temblor (Desastre Natural)	Implementar proceso de backup y recuperación de información.	Las copias de seguridad del 100% de la información brindaran apoyo en la restauración de los sistemas.	100%
		Daños en el equipo de cómputo por sobrecargas de alto voltaje eléctrico en el mismo.	Realizar procedimiento para asegurar los equipos de cómputo contra daños por alto voltaje eléctrico.	El procedimiento definirá como deben estar conectados los equipos de cómputo, las personas autorizadas para instalar y usar y los cuidados necesarios que deben tener los usuarios.	100%
		Fallas de funcionamiento de los equipos de cómputo por defectos en el software y hardware.	Realizar procedimiento de control en la adquisición de elementos tecnológicos a la corporación. Realizar procedimiento de mantenimiento preventivo y correctivo de equipos de cómputo.	El procedimiento de control de ingreso de elementos facilitara la verificación de cumplimiento del 100% de requisitos exigidos en la adquisición de nuevos elementos tecnológicos.	100%
		Ataque de virus.	Realizar procedimiento de salvaguarda, protección de equipos a nivel lógico y actualización de software antivirus en los equipos de cómputo de la Corporación.	El procedimiento brindará herramientas para que todos los equipos de cómputo mantengan actualizado su sistema de antivirus.	100%
		Fallas en el funcionamiento de los equipos de cómputo por cortes del suministro eléctrico	Realizar procedimiento para asegurar los equipos de cómputo contra daños por alto voltaje eléctrico.	El procedimiento establece que los equipos de cómputo estarán conectados a la corriente regulada de la UPS, y que esta deberá estar en normal funcionamiento y así evitar cortes de servicio de energía a los equipos de cómputo.	100%
		Accesos no autorizados al equipo de cómputo y la red de datos.	Realizar procedimiento de control de accesos a los equipos y red de datos de la Corporación.	La aplicación del procedimiento Control de Accesos, permitirá mantener estricto control de uso e implementación de los equipos de cómputo.	100%
		Ataques de denegación de servicio.	Realizar procedimiento de salvaguarda de la red de datos y equipos de cómputo.	El procedimiento de salvaguarda de los equipos de cómputo permitirá mantener controlado y funcionando los equipos de cómputo de la Corporación.	100%

5.1.4 Estimación del Estado del Riesgo y su impacto en los Activos de Corporinoquia

Tabla 9. Estimación del estado del riesgo en los activos de Corporinoquia

ITEM	CODIGO	NOMBRE CORTO	ACTIVO QUE SE PUEDE VER AMENAZADO	AMENAZAS	IMPACTO	
					POTENCIAL	RESIDUAL
	2028	SERVIDOR	SERVIDOR DE APLICACIONES (SISTEMAS DE INFORMACIÒN FINANCIERO Y BASE DE DATOS)	Sobrecalentamiento e incendio de equipos por deficiencia en la aclimatación ambiental del servidor.	Perdida de información	Sobrecostos en el mantenimiento y recuperación del sistema.
				Incendio accidental o deliberado por personal interno o externo de la Corporación.		
				Daños en la estructura del servidor por caída de concreto y hierro reforzado por temblor (Desastre Natural)		
				Daños en el servidor por sobrecargas de alto voltaje eléctrico en el mismo.		
				Fallas de funcionamiento en el servidor por defectos en el software.		
				Fallas en el funcionamiento del servidor por daños en el hardware.		
				Fallas en el funcionamiento del servidor por cortes del suministro eléctrico		
				Accesos no autorizados al servidor.		
				Fallas en el funcionamiento por ataque de virus.		
				Ataques de denegación de servicio.		
2	1920	SERVIDOR	SERVIDOR DE ACCESO A INFORMACIÒN Y CONTROL DE IMPRESIÒN	Sobrecalentamiento e incendio de equipos por deficiencia en la aclimatación ambiental del servidor.	Perdida de información	Sobrecostos en el mantenimiento y recuperación del sistema.
				Incendio deliberado por personal interno o externo de la Corporación.		
				Daños en la estructura del servidor por caída de concreto y hierro reforzado por temblor (Desastre Natural)		
				Daños en el servidor por sobrecargas de alto voltaje eléctrico en el mismo.		
				Fallas de funcionamiento en el servidor por defectos en el software.		
				Fallas en el funcionamiento del servidor por el hardware.		
				Fallas en el funcionamiento por cortes del suministro eléctrico		
				Accesos no autorizados al servidor.		

ITEM	CODIGO	NOMBRE CORTO	ACTIVO QUE SE PUEDE VER AMENAZADO	AMENAZAS	IMPACTO	
					POTENCIAL	RESIDUAL
				Ataque de virus.		
				Ataques de denegación de servicio.		
3	1934	SERVIDOR	SERVIDOR DE APLICACIONES WEB (SISTEMA DE INFORMACIÒN DE GESTIÒN DOCUMENTAL Y BASE DE DATOS)	Sobrecalentamiento e incendio de equipos por deficiencia en la aclimatación ambiental del servidor.	Perdida de información	Sobrecostos en el mantenimiento y recuperación del sistema.
				Incendio deliberado por personal interno o externo de la Corporación.		
				Daños en la estructura del servidor por caída de concreto y hierro reforzado por temblor (Desastre Natural)		
				Daños en el servidor por sobrecargas de alto voltaje eléctrico en el mismo.		
				Fallas de funcionamiento en el servidor por defectos en el software.		
				Fallas en el funcionamiento del servidor por el hardware.		
				Fallas en el funcionamiento por cortes del suministro eléctrico		
				Accesos no autorizados al servidor.		
				Ataque de virus.		
				Ataques de denegación de servicio.		
4	2033	SERVIDOR	SERVIDOR DE APLICACIONES - SISTEMA DE INFORMACIÒN GEOGRAFICO - SIGCOR.	Sobrecalentamiento e incendio de equipos por deficiencia en la aclimatación ambiental del servidor.	Perdida de información	Sobrecostos en el mantenimiento y recuperación del sistema.
				Incendio deliberado por personal interno o externo de la Corporación.		
				Daños en la estructura del servidor por caída de concreto y hierro reforzado por temblor (Desastre Natural)		
				Daños en el servidor por sobrecargas de alto voltaje eléctrico en el mismo.		
				Fallas de funcionamiento en el servidor por defectos en el software.		
				Fallas en el funcionamiento del servidor por el hardware.		
				Fallas en el funcionamiento por cortes del suministro eléctrico		
				Accesos no autorizados al servidor.		
				Ataque de virus.		
				Ataques de denegación de servicio.		
5	2154	PCT	SISTEMA DE INFORMACIÓN	Accesos no autorizados al Sistema de Información y escalamiento de privilegios.	Ataques contra la integridad de	Vulnerabilidades del sistema para

ITEM	CODIGO	NOMBRE CORTO	ACTIVO QUE SE PUEDE VER AMENAZADO	AMENAZAS	IMPACTO	
					POTENCIAL	RESIDUAL
			FINANCIERO		la información. Borrado de información.	posteriores ataques.
				Ataques de SQL Injection	Ataques a la confidencialidad, disponibilidad e integridad de la información.	Vulnerabilidades del sistema para posteriores ataques.
6	1923	PAGINA WEB	PAGINA WEB CORPORINOQUIA	Accesos no autorizados al Sitio Web y escalamiento de privilegios.	Perdida de información	Denegación del Servicio
				Ataques de SQL Injection		
7	2329	ATHENTO	SISTEMA DE INFORMACIÓN DE GESTIÓN DOCUMENTAL	Accesos no autorizados al Sistema de Información y escalamiento de privilegios.	Perdida de información	Denegación del Servicio
				Ataques de SQL Injection		
8	SIN	CORREO ELECTRONICO	CORREO ELECTRONICO CORPORATIVO	Caídas del servicio de Correo por bajo nivel de espacio de almacenamiento.	Perdida de información	Disponibilidad del Servicio
				Accesos no autorizados a la administración del servidor de correo electrónico.		
				Suplantación de correos electrónicos.		
9	2023	SAN	SAN - STORAGE AREA NETWORK.	Cese de capacidad de transmitir datos para consulta y guardado de información a los usuarios y el sistema.	Perdida de información	Disponibilidad del servicio de consulta, creación y modificación.
				Fallas en el hardware de almacenamiento por falta de mantenimiento, sobrecalentamiento e incendio por deficiencia en la aclimatación ambiental.		
				Daño lógico por la configuración de la SAN.		
10	2044	UPS	UPS RACK DE SERVIDOR PRINCIPAL - 6 KVA - CENTRO DE DATOS	Fallas en el sistema de UPS por baterías en mal estado de funcionamiento.	Disponibilidad de funcionamiento de la UPS al momento de requerirse	Daño de equipos por ml funcionamiento.
				Fallas o daños por voltaje excesivo en la ups que protege el servidor.		
				Mal funcionamiento por falta de mantenimiento.		
11	1287	RACK	RACK PRINCIPAL DE COMUNICACIONES - CENTRAL DE DATOS.	Perdida de estabilidad y robustez del rack principal por mal armado en su estructura.	Mal funcionamiento de los equipos que soporta para el funcionamiento de la red por desestabilidad funcional.	
				Daños causados por manipulación y accesos de personal no autorizado.		
12	2027	SWITCH	SWITCH CORE 24 PUERTOS - 10/100/1000 -	Fallas en el hardware por falta de mantenimiento, sobrecalentamiento y/o incendio por deficiencia en la	Perdida de información por deficiencias en	

ITEM	CODIGO	NOMBRE CORTO	ACTIVO QUE SE PUEDE VER AMENAZADO	AMENAZAS	IMPACTO	
					POTENCIAL	RESIDUAL
			CENTRO DE DATOS.	aclimatación ambiental.	la entrega de paquetes entre nodos por caída de red y mal funcionamiento del Switch`s.	
				Interrupción del servicio causado por manipulación física realizada a los switch´s por personal no autorizado.		
				Mal funcionamiento por falta de mantenimiento.		
				Denegación del servicio por accesos lógicos no autorizados a los switch´s.		
				Fallas por interrupciones del servicio eléctrico.		
13	2026	SWITCH	SWITCH 48 PUERTOS - 10/100/1000 - CENTRO DE DATOS	Fallas en el hardware por falta de mantenimiento, sobrecalentamiento y/o incendio por deficiencia en la aclimatación ambiental.	Perdida de información por deficiencias en la entrega de paquetes entre nodos por caída de red y mal funcionamiento del Switch`s.	
				Interrupción del servicio causado por manipulación física realizada a los Switch’s por personal no autorizado.		
				Mal funcionamiento por falta de mantenimiento.		
				Denegación del servicio por accesos lógicos no autorizados a los Switch’s.		
				Fallas por interrupciones del servicio eléctrico.		
14	2025	SWITCH	SWITCH 48 PUERTOS - 10/100/1000 - CENTRO DE DATOS	Fallas en el hardware por falta de mantenimiento, sobrecalentamiento y/o incendio por deficiencia en la aclimatación ambiental.	Perdida de información por deficiencias en la entrega de paquetes entre nodos por caída de red y mal funcionamiento del Switch`s.	
				Interrupción del servicio causado por manipulación física realizada a los Switch’s por personal no autorizado.		
				Mal funcionamiento por falta de mantenimiento.		
				Denegación del servicio por accesos lógicos no autorizados a los Switch’s.		
				Fallas por interrupciones del servicio eléctrico.		
15	1220	RACK	RACK SECUNDARIO DE COMUNICACIONES-SUBDIRECCIÒN ADMINISTRATIVA Y FINANCIERA.	Perdida de estabilidad y robustez del rack principal por mala configuración en su estructura.	Mal funcionamiento de los equipos que soporta para el funcionamiento de la red por desestabilidad funcional.	
				Daños causados por manipulación y accesos de personal no autorizado.		
16	2024	SWITCH	SWITCH CORE 24 PUERTOS - 10/100/1000 -	Fallas en el hardware por falta de mantenimiento, sobrecalentamiento y/o incendio por deficiencia en la	Perdida de información por deficiencias en	

ITEM	CODIGO	NOMBRE CORTO	ACTIVO QUE SE PUEDE VER AMENAZADO	AMENAZAS	IMPACTO	
					POTENCIAL	RESIDUAL
			SUBDIRECCIÒN ADMINISTRATIVA Y FINANCIERA.	aclimatación ambiental.	la entrega de paquetes entre nodos por caída de red y mal funcionamiento del Switch`s.	
				Interrupción del servicio causado por manipulación física realizada a los Switch's por personal no autorizado.		
				Mal funcionamiento por falta de mantenimiento.		
				Denegación del servicio por accesos lógicos no autorizados a los Switch's.		
				Fallas por interrupciones del servicio eléctrico.		
17	2034	SWITCH	SWITCH 48 PUERTOS - 10/100/1000 - CENTRO DE DATOS - SUBDIRECCIÒN ADMINISTRATIVA Y FINANCIERA.	Fallas en el hardware por falta de mantenimiento, sobrecalentamiento y/o incendio por deficiencia en la aclimatación ambiental.	Perdida de información por deficiencias en la entrega de paquetes entre nodos por caída de red y mal funcionamiento del Switch`s.	
				Interrupción del servicio causado por manipulación física realizada a los Switch's por personal no autorizado.		
				Mal funcionamiento por falta de mantenimiento.		
				Denegación del servicio por accesos lógicos no autorizados a los Switch's.		
				Fallas por interrupciones del servicio eléctrico.		
18	1218	RACK	RACK SECUNDARIO DE COMUNICACIONES - SUBDIRECCIÒN DE PLANEACIÒN AMBIENTAL.	Perdida de estabilidad y robustez del rack principal por mala configuración en su estructura.	Mal funcionamiento de los equipos que soporta para el funcionamiento de la red por desestabilidad funcional.	
				Daños causados por manipulación y accesos de personal no autorizado.		
19	2022	SWITCH	SWITCH CORE 24 PUERTOS - 10/100/1000 - SUBDIRECCIÒN DE PLANEACIÒN AMBIENTAL.	Fallas en el hardware por falta de mantenimiento, sobrecalentamiento y/o incendio por deficiencia en la aclimatación ambiental.	Perdida de información por deficiencias en la entrega de paquetes entre nodos por caída de red y mal funcionamiento del Switch`s.	
				Interrupción del servicio causado por manipulación física realizada a los Switch's por personal no autorizado.		
				Mal funcionamiento por falta de mantenimiento.		
				Denegación del servicio por accesos lógicos no autorizados a los Switch's.		
				Fallas por interrupciones del servicio eléctrico.		
20	2021	SWITCH	SWITCH 48 PUERTOS - 10/100/1000 - SUBDIRECCI	Fallas en el hardware por falta de mantenimiento, sobrecalentamiento y/o incendio por deficiencia en la aclimatación ambiental.	Perdida de información por deficiencias en la entrega de	

ITEM	CODIGO	NOMBRE CORTO	ACTIVO QUE SE PUEDE VER AMENAZADO	AMENAZAS	IMPACTO	
					POTENCIAL	RESIDUAL
			ÒN DE PLANEACIÒN AMBIENTAL.	Interrupción del servicio causado por manipulación física realizada a los Switch's por personal no autorizado.	paquetes entre nodos por caída de red y mal funcionamiento del Switch`s.	
				Mal funcionamiento por falta de mantenimiento.		
				Denegación del servicio por accesos lógicos no autorizados a los Switch's.		
				Fallas por interrupciones del servicio eléctrico.		
21	1276	CABLEADO ESTRUCTURADO	CABLEADO ESTRUCTURADO CATEGORIA 6 Y RED DE DATOS y CANALETA.	Daños en el cableado estructurado por canaletas abiertas al aire libre y por mala manipulación de personal no autorizado.	Perdida de información por deficiencias en la entrega de paquetes entre nodos por cableado en mal estado.	
				Fallas en las comunicaciones por daños en cableado estructurado.		
				Accesos no autorizados a los puntos de red del cableado estructurado.		
				Incendio deliberado por personal interno o externo de la Corporación, o por corto circuitos producidos en la red de corriente eléctrica.		
22	1232	CORRIENTE REGULADA	CABLEADO DE COBRE DE CORRIENTE REGULADA PARA EQUIPOS DE CÓMPUTO.	Daños en el cableado de corriente regulada, canaletas abiertas al aire libre y por mala manipulación de personal no autorizado.	Perdida y disponibilidad de la información por daño a equipos por causa de cableado de corriente regulada y eléctrica en mal estado	Baja confiabilidad de funcionamiento de la red de corriente eléctrica y regulada.
				Fallas en el cableado de corriente regulada por Corto circuito.		
				Daños en el cableado de corriente regulada y disminución en la capacidad de respuesta de las UPS, por conexión de equipos no autorizados (Mal uso).		
				Incendio deliberado o accidental, causado por personal interno o externo de la Corporación, o por corto circuitos producidos en la red de corriente eléctrica.		
23	1256	UPS	UPS DE 20 KVA, PROTECCIÒN DE EQUIPOS DE COMPUTO SUBDIRECCIÒN DE PLANEACIÒN Y CENTRO DE DOCUMENTOS.	Fallas en el sistema de UPS por baterías en mal estado de funcionamiento.	Perdida de información en equipos de cómputo y servidores por baja protección en el suministro de corriente regulada.	Aumento de costos en mantenimiento de UPS.
				Fallas o daños por voltaje excesivo en la UPS.		
				Daños en la UPS por mala configuración y/o disminución de mantenimiento de la red de corriente regulada.		
				Mal funcionamiento por falta de mantenimiento.		

ITEM	CODIGO	NOMBRE CORTO	ACTIVO QUE SE PUEDE VER AMENAZADO	AMENAZAS	IMPACTO	
					POTENCIAL	RESIDUAL
24	1257	UPS	UPS DE 30 KVA, PROTECCIÒN DE EQUIPOS DE COMPUTO SUBDIRECCIÒN DE CONTROL Y CALIDAD AMBIENTAL, SUBDIRECCIÒN ADMINISTRATIVA Y FINANCIERA Y DIRECCIÒN GENERAL.	Fallas en el sistema de UPS por baterías en mal estado de funcionamiento.	Perdida de información en equipos de cómputo y servidores por baja protección en el suministro de corriente regulada.	Aumento de costos en mantenimiento de UPS.
				Fallas o daños por voltaje excesivo en la UPS.		
				Daños en la UPS por mala configuración y/o disminución de mantenimiento de la red de corriente regulada.		
				Mal funcionamiento por falta de mantenimiento.		
25	SIN	DOCUMENTOS IMPRESOS	INFORMACIÒN FISICA DEL CENTRO DE DOCUMENTOS DE CORPORINOQUIA, SEDE PRINCIPAL.	Incendio deliberado por personal interno o externo de la Corporación, o por corto circuitos producidos en la red de corriente eléctrica.	Perdida de información Física.	Disponibilidad de la información para consulta.
				Robo de información.		
				Accesos no autorizados a la información.		
26	1253	PLANTA ELECTRICA	PLANTA ELECTRICA LISTER DE 30 KVA	Corto circuito por alto voltaje.	Suspensión de actividades de los servicios misionales y de apoyo por ausencia del servicio de energía eléctrica interna y externa.	Disponibilidad del servicio y de la información.
				Incendio deliberado por personal interno o externo de la Corporación, o por corto circuitos producidos en la red de corriente eléctrica.		
				Mal manejo y Accesos no autorizados.		
				Daños por mala configuración.		
				Mal funcionamiento por falta de mantenimiento.		
				No funciona por falta de combustible.		
27	DIFERENTES CODIGOS	EQUIPOS DE COMPUTO	EQUIPOS DE COMPUTO DE ESCRITORIO	Sobrecalentamiento e incendio de equipos por aumento en la temperatura ambiental.	Perdida de información.	Sobrecostos en mantenimiento de equipos y reposición de partes.
				Incendio deliberado por personal interno o externo de la Corporación.		
				Daños en la estructura del equipo de cómputo por caída de concreto y hierro reforzado por temblor (Desastre Natural)		
				Daños en el equipo de cómputo por sobrecargas de alto voltaje eléctrico en el mismo.		
				Fallas de funcionamiento de los equipos de cómputo por defectos en el software y hardware.		
				Ataque de virus.		

ITEM	CODIGO	NOMBRE CORTO	ACTIVO QUE SE PUEDE VER AMENAZADO	AMENAZAS	IMPACTO	
					POTENCIAL	RESIDUAL
				Fallas en el funcionamiento de los equipos de cómputo por cortes del suministro eléctrico		
				Accesos no autorizados al equipo de cómputo y la red de datos.		
				Ataques de denegación de servicio.		

Fuente: el autor

5.1.5 Controles a tener en cuenta para los activos de Corporinoquia

A continuación se han identificado los riesgos a los que están expuestos los activos de Corporinoquia, se identifican algunos objetivos de control, controles a tener en cuenta para su cumplimiento y algunas pruebas para su verificación. Por lo anterior se ha tenido en cuenta la metodología Magerit complementándola con la metodología EDR, como se detalla a continuación:

Tabla 10.Estimación del Riesgo en los activos de Corporinoquia

ITEM	ACTIVO	RIESGO	OBJETIVO DEL RIESGO	CONTROL	PRUEBAS DE VERIFICACIÒN	PRUEBAS SUSTANTIVAS
1	SERVIDOR DE APLICACIONES (SISTEMAS DE INFORMACIÒN FINANCIERO Y BASE DE DATOS)	Perdida de información	Salvaguardar la información almacenada en el servidor.	Procedimiento para realizar copias de seguridad de la información corporativa	Verificación de la existencia del procedimiento para realizar copias de seguridad de la información corporativa.	Ampliar el rango de verificación de la funcionalidad de las copias de seguridad de la información.
		Accesos no autorizados al servidor.	Garantizar el acceso de forma segura a la sala de servidores, a personal autorizado a través de usuario y contraseña y mecanismos de autorización intransferible (Tarjetas electrónicas).	Procedimiento establecido para el ingreso a sala de servidores.	Verificación de existencia de procedimiento para el ingreso a la sala de servidores.	Ampliar el rango de verificación de usuarios autorizados para el ingreso a la sala de servidores. Verificación de usuarios autorizados Vs Registro de ingresos a la sala de servidores. Verificación personal de la existencia de controles a la sala de servidores de la entidad.
			Garantizar el acceso lógico al sistema del Servidor, a usuarios autorizados.	Procedimiento de asignación de permisos y privilegios para acceder a la información lógica de los servidores.	Verificación de existencia de procedimiento de asignación de permisos y privilegios para acceder a la información lógica de los servidores.	Ampliar el rango de verificación de usuarios autorizados para el ingreso al servidor. Verificación de log de registro de accesos Vs usuarios activos con privilegios de administrador del servidor.
		Ataques de denegación de servicio.	Implementar herramientas de detección y protección de intrusos en la zona desmilitarizada.	Procedimiento de implementación de IDS e IPS en la DMZ. IDS funcionando. IPS Funcionando.	Comprobar la existencia del procedimiento de implementación de IDS e IPS. Equipos de IDS e IPS instalados y funcionales.	Ampliar el rango de Verificación funcional de equipos IDS e IPS.
2	SERVIDOR DE ACCESO A INFORMACIÒN Y CONTROL DE IMPRESIÒN	Perdida de información	Salvaguardar la información almacenada en el servidor.	Procedimiento para realizar copias de seguridad de la información corporativa	Verificación de la existencia del procedimiento para realizar copias de seguridad de la información corporativa.	Ampliar el rango de verificación de la funcionalidad de las copias de seguridad de la información.
		Accesos no autorizados al servidor.	Garantizar el acceso de forma segura a la sala de servidores, a personal autorizado a través de usuario y contraseña y mecanismos de autorización intransferible (Tarjetas electrónicas).	Procedimiento establecido para el ingreso a sala de servidores.	Verificación de existencia de procedimiento para el ingreso a la sala de servidores.	Ampliar el rango de verificación de usuarios autorizados para el ingreso a la sala de servidores. Verificación de usuarios autorizados Vs Registro de ingresos a la sala de servidores.

ITEM	ACTIVO	RIESGO	OBJETIVO DEL RIESGO	CONTROL	PRUEBAS DE VERIFICACIÒN	PRUEBAS SUSTANTIVAS
						Verificación personal de la existencia de controles a la sala de servidores de la entidad.
			Garantizar el acceso lógico al sistema del Servidor, a usuarios autorizados.	Procedimiento de asignación de permisos y privilegios para acceder a la información lógica de los servidores.	Verificación de existencia de procedimiento de asignación de permisos y privilegios para acceder a la información lógica de los servidores.	Ampliar el rango de verificación de usuarios autorizados para el ingreso al servidor. Verificación de log de registro de accesos Vs usuarios activos con privilegios de administrador del servidor.
		Ataques de denegación de servicio.	Implementar herramientas de detección y protección de intrusos en la zona desmilitarizada.	Procedimiento de implementación de IDS e IPS en la DMZ. IDS funcionando. IPS Funcionando.	Comprobar la existencia del procedimiento de implementación de IDS e IPS. Equipos de IDS e IPS instalados y funcionales.	Ampliar el rango de Verificación funcional de equipos IDS e IPS.
3	SERVIDOR DE APLICACIONES WEB (SISTEMA DE INFORMACIÒN DE GESTIÒN DOCUMENTAL Y BASE DE DATOS)	Perdida de información	Salvaguardar la información almacenada en el servidor.	Procedimiento para realizar copias de seguridad de la información corporativa	Verificación de la existencia del procedimiento para realizar copias de seguridad de la información corporativa.	Ampliar el rango de verificación de la funcionalidad de las copias de seguridad de la información.
		Accesos no autorizados al servidor.	Garantizar el acceso de forma segura a la sala de servidores, a personal autorizado a través de usuario y contraseña y mecanismos de autorización intransferible (Tarjetas electrónicas).	Procedimiento establecido para el ingreso a sala de servidores.	Verificación de existencia de procedimiento para el ingreso a la sala de servidores.	Ampliar el rango de verificación de usuarios autorizados para el ingreso a la sala de servidores. Verificación de usuarios autorizados Vs Registro de ingresos a la sala de servidores. Verificación personal de la existencia de controles a la sala de servidores de la entidad.

ITEM	ACTIVO	RIESGO	OBJETIVO DEL RIESGO	CONTROL	PRUEBAS DE VERIFICACIÒN	PRUEBAS SUSTANTIVAS
			Garantizar el acceso lógico al sistema del Servidor, a usuarios autorizados.	Procedimiento de asignación de permisos y privilegios para acceder a la información lógica de los servidores.	Verificación de existencia de procedimiento de asignación de permisos y privilegios para acceder a la información lógica de los servidores.	Ampliar el rango de verificación de usuarios autorizados para el ingreso al servidor. Verificación de log de registro de accesos Vs usuarios activos con privilegios de administrador del servidor.
		Ataques de denegación de servicio, SQL Injection.	Implementar herramientas de detección y protección de intrusos en la zona desmilitarizada. Instalar un firewall de base de datos.	Procedimiento de implementación de IDS e IPS en la DMZ e instalación de firewall de base de datos. IDS funcionando. IPS Funcionando. Firewall de base de datos funcionando.	Comprobar la existencia del procedimiento de implementación de IDS e IPS e instalación de firewall de base de datos. Equipos de IDS e IPS instalados y funcionales. Firewall de base de datos funcionando.	Ampliar el rango de Verificación funcional de equipos IDS e IPS y Firewall de base de datos funcionando (Configuración).
4	SERVIDOR DE APLICACIONES - SISTEMA DE INFORMACIÒN GEOGRAFICO - SIGCOR.	Perdida de información	Salvaguardar la información almacenada en el servidor.	Procedimiento para realizar copias de seguridad de la información corporativa	Verificación de la existencia del procedimiento para realizar copias de seguridad de la información corporativa.	Ampliar el rango de verificación de la funcionalidad de las copias de seguridad de la información.
		Accesos no autorizados al servidor.	Garantizar el acceso de forma segura a la sala de servidores, a personal autorizado a través de usuario y contraseña y mecanismos de autorización intransferible (Tarjetas electrónicas).	Procedimiento establecido para el ingreso a sala de servidores.	Verificación de existencia de procedimiento para el ingreso a la sala de servidores.	Ampliar el rango de verificación de usuarios autorizados para el ingreso a la sala de servidores. Verificación de usuarios autorizados Vs Registro de ingresos a la sala de servidores. Verificación personal de la existencia de controles a la sala de servidores de la entidad.
			Garantizar el acceso lógico al sistema del Servidor, a usuarios autorizados.	Procedimiento de asignación de permisos y privilegios para acceder a la información lógica de los servidores.	Verificación de existencia de procedimiento de asignación de permisos y privilegios para acceder a la información lógica de los servidores.	Ampliar el rango de verificación de usuarios autorizados para el ingreso al servidor. Verificación de log de registro de accesos Vs usuarios activos con privilegios de administrador del

ITEM	ACTIVO	RIESGO	OBJETIVO DEL RIESGO	CONTROL	PRUEBAS DE VERIFICACIÒN	PRUEBAS SUSTANTIVAS
						servidor.
		Ataques de denegación de servicio.	Implementar herramientas de detección y protección de intrusos en la zona desmilitarizada.	Procedimiento de implementación de IDS e IPS en la DMZ. IDS funcionando. IPS Funcionando.	Comprobar la existencia del procedimiento de implementación de IDS e IPS. Equipos de IDS e IPS instalados y funcionales.	Ampliar el rango de Verificación funcional de equipos IDS e IPS.
5	SAN - STORAGE AREA NETWORK.	Perdida de información	Salvaguardar la información almacenada en la SAN.	Procedimiento para realizar copias de seguridad de la información corporativa.	Verificación de la existencia del procedimiento para realizar copias de seguridad de la información corporativa. Verificación de copias de seguridad en la nube.	Ampliar el rango de verificación de la funcionalidad de las copias de seguridad de la información.
6	UPS RACK DE SERVIDOR PRINCIPAL - 6 KVA - CENTRO DE DATOS	Quemarse por alto voltaje	Estabilizar el flujo de corriente eléctrica a la que se conecta la UPS.	Procedimiento de protección de UPS y corriente regulada para los equipos de cómputo y servidores en la corporación. Instalación de un estabilizador de corriente eléctrica.	Verificación de la existencia del procedimiento de protección de UPS y corriente regulada para los equipos de cómputo y servidores de la Corporación.	Verificación del funcionamiento de la UPS en momentos de interrupciones de energía eléctrica.
		Mal funcionamiento	Garantizar el normal funcionamiento de la UPS.	Procedimiento de mantenimiento preventivo y correctivo de UPS.	Verificación de la existencia de procedimiento de mantenimiento preventivo y correctivo de UPS. Funcionamiento normal de la UPS.	Verificación hoja de registro de mantenimiento preventivo y correctivo de las UPS. Verificación del total de UPS funcionando.

ITEM	ACTIVO	RIESGO	OBJETIVO DEL RIESGO	CONTROL	PRUEBAS DE VERIFICACIÒN	PRUEBAS SUSTANTIVAS
7	RACK PRINCIPAL DE COMUNICACIONES - CENTRAL DE DATOS.	Violentar configuración de estructura del rack de comunicaciones de la Central de Datos.	Brindar la seguridad necesaria para proteger el rack de comunicaciones de la Central de Datos.	Procedimiento para asegurar los centros de datos y rack de comunicaciones internos y externos a la central de datos en las diferentes subdirecciones de la Corporación.	Verificación de la existencia y el cumplimiento del procedimiento para asegurar los centros de datos y rack de comunicaciones internos y externos a la central de datos en las diferentes subdirecciones de la Corporación.	Verificación del normal funcionamiento del rack de comunicaciones del Centro de Datos de la Corporación.
8	SWITCH CORE 24 PUERTOS - 10/100/1000 - CENTRO DE DATOS.	Mala configuración.	Realizar correcta configuración de los equipos de comunicaciones switch de la Corporación.	Procedimiento de instalación, configuración e implementación de Switch en la Corporación.	Verificar el cumplimiento y correcto uso del procedimiento de instalación, configuración e implementación de los switch de la corporación.	Verificar la correcta configuración y funcionamiento normal de los switch. Validar la seguridad de administración a través de usuario y contraseña de los switch instalados.
		Violentar configuración de cableado y seguridad de los switch.	Brindar la seguridad necesaria en la restricción de accesos y manipulación de los equipos switch de la central de datos de la corporación.	Procedimiento para el ingreso a la central de datos y zonas de centros de distribución de cableado estructurado (rack, patch panel y switch) de las subdirección Administrativa y Planeación Ambiental de la Corporación.	Verificar el cumplimiento y correcto uso del Procedimiento para el ingreso a la central de datos y zonas de centros de distribución de cableado estructurado (rack, patch panel y switch) de las subdirección Administrativa y Planeación Ambiental de la Corporación.	Control de Accesos restringidos bajo autenticación y autorización. Switch en funcionamiento normal.
9	SWITCH 48 PUERTOS - 10/100/1000 - CENTRO DE DATOS	Mala configuración.	Realizar correcta configuración de los equipos de comunicaciones Switch's de la Corporación.	Procedimiento de instalación, configuración e implementación de Switch en la Corporación.	Verificar el cumplimiento y correcto uso del procedimiento de instalación, configuración e implementación de los switch de la corporación.	Verificar la correcta configuración y funcionamiento normal de los Switch's. Validar la seguridad de administración a través de usuario y contraseña de los switch instalados.

ITEM	ACTIVO	RIESGO	OBJETIVO DEL RIESGO	CONTROL	PRUEBAS DE VERIFICACIÒN	PRUEBAS SUSTANTIVAS
		Violentar configuración de cableado y seguridad de los switch.	Brindar la seguridad necesaria en la restricción de accesos y manipulación de los equipos switch de la central de datos de la corporación.	Procedimiento para el ingreso a la central de datos y zonas de centros de distribución de cableado estructurado (rack, patch panel y switch) de las subdirección Administrativa y Planeación Ambiental de la Corporación.	Verificar el cumplimiento y correcto uso del Procedimiento para el ingreso a la central de datos y zonas de centros de distribución de cableado estructurado (rack, patch panel y switch) de las subdirección Administrativa y Planeación Ambiental de la Corporación.	Control de Accesos restringidos bajo autenticación y autorización. Switch en funcionamiento normal.
10	SWITCH 48 PUERTOS - 10/100/1000 - CENTRO DE DATOS	Mala configuración.	Realizar correcta configuración de los equipos de comunicaciones Switch's de la Corporación.	Procedimiento de instalación, configuración e implementación de Switch en la Corporación.	Verificar el cumplimiento y correcto uso del procedimiento de instalación, configuración e implementación de los switch de la corporación.	Verificar la correcta configuración y funcionamiento normal de los switch. Validar la seguridad de administración a través de usuario y contraseña de los switch instalados.
		Violentar configuración de cableado y seguridad de los switch.	Brindar la seguridad necesaria en la restricción de accesos y manipulación de los equipos switch de la central de datos de la corporación.	Procedimiento para el ingreso a la central de datos y zonas de centros de distribución de cableado estructurado (rack, patch panel y switch) de las subdirección Administrativa y Planeación Ambiental de la Corporación.	Verificar el cumplimiento y correcto uso del Procedimiento para el ingreso a la central de datos y zonas de centros de distribución de cableado estructurado (rack, patch panel y switch) de las subdirección Administrativa y Planeación Ambiental de la Corporación.	Control de Accesos restringidos bajo autenticación y autorización. Switch en funcionamiento normal.

ITEM	ACTIVO	RIESGO	OBJETIVO DEL RIESGO	CONTROL	PRUEBAS DE VERIFICACIÒN	PRUEBAS SUSTANTIVAS
11	RACK SECUNDARIO DE COMUNICACIONES-SUBDIRECCIÒN ADMINISTRATIVA Y FINANCIERA.	Violentar configuración de estructura del rack de comunicaciones de la Subdirección Administrativa y Financiera de la Corporación.	Brindar la seguridad necesaria para proteger el rack de comunicaciones de la Subdirección Administrativa y Financiera de la Corporación.	Procedimiento para asegurar los centros de datos y rack de comunicaciones internos y externos a la central de datos en las diferentes subdirecciones de la Corporación.	Verificación de la existencia y el cumplimiento del procedimiento para asegurar los centros de datos y rack de comunicaciones internos y externos a la central de datos en las diferentes subdirecciones de la Corporación.	Verificación del normal funcionamiento del rack de comunicaciones de la Subdirección Administrativa y Financiera de la Corporación.
12	SWITCH CORE 24 PUERTOS - 10/100/1000 - SUBDIRECCIÒN ADMINISTRATIVA Y FINANCIERA.	Mala configuración.	Realizar correcta configuración de los equipos de comunicaciones switch de la Corporación.	Procedimiento de instalación, configuración e implementación de Switch en la Corporación.	Verificar el cumplimiento y correcto uso del procedimiento de instalación, configuración e implementación de los switch de la corporación.	Verificar la correcta configuración y funcionamiento normal de los switch. Validar la seguridad de administración a través de usuario y contraseña de los switch instalados.
		Violentar configuración de cableado y seguridad de los switch.	Brindar la seguridad necesaria en la restricción de accesos y manipulación de los equipos switch de la central de datos de la corporación.	Procedimiento para el ingreso a la central de datos y zonas de centros de distribución de cableado estructurado (rack, patch panel y switch) de las subdirección Administrativa y Planeación Ambiental de la Corporación.	Verificar el cumplimiento y correcto uso del Procedimiento para el ingreso a la central de datos y zonas de centros de distribución de cableado estructurado (rack, patch panel y switch) de las subdirección Administrativa y Planeación Ambiental de la Corporación.	Control de Accesos restringidos bajo autenticación y autorización. Switch en funcionamiento normal.
13	SWITCH 48 PUERTOS - 10/100/1000 - CENTRO DE DATOS - SUBDIRECCIÒN ADMINISTRATIVA Y FINANCIERA.	Mala configuración.	Realizar correcta configuración de los equipos de comunicaciones Switch’s de la Corporación.	Procedimiento de instalación, configuración e implementación de Switch en la Corporación.	Verificar el cumplimiento y correcto uso del procedimiento de instalación, configuración e implementación de los switch de la corporación.	Verificar la correcta configuración y funcionamiento normal de los Switch’s. Validar la seguridad de administración a través de usuario y contraseña de los switch instalados.

ITEM	ACTIVO	RIESGO	OBJETIVO DEL RIESGO	CONTROL	PRUEBAS DE VERIFICACIÒN	PRUEBAS SUSTANTIVAS
		Violentar configuración de cableado y seguridad de los switch.	Brindar la seguridad necesaria en la restricción de accesos y manipulación de los equipos switch de la central de datos de la corporación.	Procedimiento para el ingreso a la central de datos y zonas de centros de distribución de cableado estructurado (rack, patch panel y switch) de las subdirección Administrativa y Planeación Ambiental de la Corporación.	Verificar el cumplimiento y correcto uso del Procedimiento para el ingreso a la central de datos y zonas de centros de distribución de cableado estructurado (rack, patch panel y switch) de las subdirección Administrativa y Planeación Ambiental de la Corporación.	Control de Accesos restringidos bajo autenticación y autorización. Switch en funcionamiento normal.
14	RACK SECUNDARIO DE COMUNICACIONES - SUBDIRECCIÒN DE PLANEACIÒN AMBIENTAL.	Violentar configuración de estructura del rack de comunicaciones de la Subdirección de Planeación Ambiental de la Corporación.	Brindar la seguridad necesaria para proteger el rack de comunicaciones de la Subdirección de Planeación Ambiental.	Procedimiento para asegurar los centros de datos y rack de comunicaciones internos y externos a la central de datos en las diferentes subdirecciones de la Corporación.	Verificación de la existencia y el cumplimiento del procedimiento para asegurar los centros de datos y rack de comunicaciones internos y externos a la central de datos en las diferentes subdirecciones de la Corporación.	Verificación del normal funcionamiento del rack de comunicaciones de la Subdirección de Planeación Ambiental.
15	SWITCH CORE 24 PUERTOS - 10/100/1000 - SUBDIRECCIÒN DE PLANEACIÒN AMBIENTAL.	Mala configuración.	Realizar correcta configuración de los equipos de comunicaciones Switch’s de la Corporación.	Procedimiento de instalación, configuración e implementación de Switch en la Corporación.	Verificar el cumplimiento y correcto uso del procedimiento de instalación, configuración e implementación de los switch de la corporación.	Verificar la correcta configuración y funcionamiento normal de los switch. Validar la seguridad de administración a través de usuario y contraseña de los switch instalados.

ITEM	ACTIVO	RIESGO	OBJETIVO DEL RIESGO	CONTROL	PRUEBAS DE VERIFICACIÒN	PRUEBAS SUSTANTIVAS
		Violentar configuración de cableado y seguridad de los switch.	Brindar la seguridad necesaria en la restricción de accesos y manipulación de los equipos switch de la central de datos de la corporación.	Procedimiento para el ingreso a la central de datos y zonas de centros de distribución de cableado estructurado (rack, patch panel y switch) de las subdirección Administrativa y Planeación Ambiental de la Corporación.	Verificar el cumplimiento y correcto uso del Procedimiento para el ingreso a la central de datos y zonas de centros de distribución de cableado estructurado (rack, patch panel y switch) de las subdirección Administrativa y Planeación Ambiental de la Corporación.	Control de Accesos restringidos bajo autenticación y autorización. Switch en funcionamiento normal.
16	SWITCH 48 PUERTOS - 10/100/1000 - SUBDIRECCIÒN DE PLANEACIÒN AMBIENTAL.	Mala configuración.	Realizar correcta configuración de los equipos de comunicaciones Switch's de la Corporación.	Procedimiento de instalación, configuración e implementación de Switch en la Corporación.	Verificar el cumplimiento y correcto uso del procedimiento de instalación, configuración e implementación de los switch de la corporación.	Verificar la correcta configuración y funcionamiento normal de los Switch's. Validar la seguridad de administración a través de usuario y contraseña de los switch instalados.
		Violentar configuración de cableado y seguridad de los switch.	Brindar la seguridad necesaria en la restricción de accesos y manipulación de los equipos switch de la central de datos de la corporación.	Procedimiento para el ingreso a la central de datos y zonas de centros de distribución de cableado estructurado (rack, patch panel y switch) de las subdirección Administrativa y Planeación Ambiental de la Corporación.	Verificar el cumplimiento y correcto uso del Procedimiento para el ingreso a la central de datos y zonas de centros de distribución de cableado estructurado (rack, patch panel y switch) de las subdirección Administrativa y Planeación Ambiental de la Corporación.	Control de Accesos restringidos bajo autenticación y autorización. Switch en funcionamiento normal.

ITEM	ACTIVO	RIESGO	OBJETIVO DEL RIESGO	CONTROL	PRUEBAS DE VERIFICACIÒN	PRUEBAS SUSTANTIVAS
17	CABLEADO ESTRUCTURADO CATEGORIA 6 Y RED DE DATOS.	Daños físicos del cableado.	Proteger la integridad del cableado estructurado.	Cumplimiento de la normatividad vigente para instalación e intervención de cableado estructurado Categoría 6. Mantenimiento del cableado estructurado de la red de datos de la corporación.	Verificación del cumplimiento de la aplicación de la normatividad y estandarización actual para instalación e intervención de cableado estructurado categoría 6. Cableado estructurado en funcionamiento normal.	Verificación de funcionalidad de puntos de red.
		Interceptación de paquetes y ataques de hombre en medio.	Disminuir los accesos indeseados a la red de datos.	Procedimiento de control de accesos de equipos de cómputo a la red de datos.	Verificación de procedimiento de control de accesos de equipos de cómputo a la red de datos.	
18	CABLEADO DE COBRE DE CORRIENTE REGULADA PARA EQUIPOS DE CÓMPUTO.	Daños físicos del cableado.	Proteger la integridad del cableado de corriente regulada.	Procedimiento y normatividad existente para instalación de cableado de corriente regulada.	Verificación de la existencia y aplicación de procedimientos y normatividad para instalación de corriente regulada. Cableado de corriente regulada protegido con canaleta.	Verificación del estado del cableado de corriente regulada. Cableado funcionando normalmente.
		Cortos eléctricos.	Disminuir las posibilidades de cortos y fallas eléctricas.	Procedimiento para intervenir la red de corriente regulada. Instalación de disparadores automáticos para prevenir fallos de corriente regulada.	Verificación de la existencia de procedimiento para intervenir la red de corriente regulada. Sensores de protección ante posibles cortos y fallas eléctricas.	Funcionamiento normal de la red de corriente regulada.

ITEM	ACTIVO	RIESGO	OBJETIVO DEL RIESGO	CONTROL	PRUEBAS DE VERIFICACIÒN	PRUEBAS SUSTANTIVAS
19	UPS DE 20 KVA, PROTECCIÒN DE EQUIPOS DE COMPUTO SUBDIRECCIÒN DE PLANEACIÒN Y CENTRO DE DOCUMENTOS.	Quemarse por alto voltaje	Estabilizar el flujo de corriente eléctrica a la que se conecta la UPS.	Procedimiento de protección de UPS y corriente regulada para los equipos de cómputo y servidores en la corporación. Instalación de un estabilizador de corriente eléctrica.	Verificación de la existencia del procedimiento de protección de UPS y corriente regulada para los equipos de cómputo y servidores de la Corporación.	Verificación del funcionamiento de la UPS en momentos de interrupciones de energía eléctrica.
		Mal funcionamiento	Garantizar el normal funcionamiento de la UPS.	Procedimiento de mantenimiento preventivo y correctivo de UPS.	Verificación de la existencia de procedimiento de mantenimiento preventivo y correctivo de UPS. Funcionamiento normal de la UPS.	Verificación hoja de registro de mantenimiento preventivo y correctivo de las UPS. Verificación del total de UPS funcionando.
20	UPS DE 30 KVA, PROTECCIÒN DE EQUIPOS DE COMPUTO SUBDIRECCIÒN DE CONTROL Y CALIDAD AMBIENTAL, SUBDIRECCIÒN ADMINISTRATIVA Y FINANCIERA Y DIRECCIÒN GENERAL.	Quemarse por alto voltaje	Estabilizar el flujo de corriente eléctrica a la que se conecta la UPS.	Procedimiento de protección de UPS y corriente regulada para los equipos de cómputo y servidores en la corporación. Instalación de un estabilizador de corriente eléctrica.	Verificación de la existencia del procedimiento de protección de UPS y corriente regulada para los equipos de cómputo y servidores de la Corporación.	Verificación del funcionamiento de la UPS en momentos de interrupciones de energía eléctrica.
		Mal funcionamiento	Garantizar el normal funcionamiento de la UPS.	Procedimiento de mantenimiento preventivo y correctivo de UPS.	Verificación de la existencia de procedimiento de mantenimiento preventivo y correctivo de UPS. Funcionamiento normal de la UPS.	Verificación hoja de registro de mantenimiento preventivo y correctivo de las UPS. Verificación del total de UPS funcionando.
21	INFORMACIÒN FISICA DEL CENTRO DE DOCUMENTOS DE CORPORINOQUIA, SEDE PRINCIPAL.	Perdida de información física	Disminuir y controlar la perdida de información física en el centro de documentos.	Procedimiento para el préstamo de información física del centro de documentos.	Verificación de la existencia y aplicación del procedimiento para el préstamo de información física del centro de documentos.	Libro o registro de préstamo y devolución de información física en el centro de documentos.

ITEM	ACTIVO	RIESGO	OBJETIVO DEL RIESGO	CONTROL	PRUEBAS DE VERIFICACIÒN	PRUEBAS SUSTANTIVAS
22	PLANTA ELECTRICA LISTER DE 30 KVA	Daños físicos en su funcionamiento	Garantizar el normal funcionamiento de la planta eléctrica de la corporación.	Procedimiento de mantenimiento preventivo y correctivo de la planta eléctrica. Procedimiento de funcionamiento de la planta eléctrica de la Corporación.	Verificación de la existencia y cumplimiento del procedimiento de mantenimiento preventivo y correctivo de la planta eléctrica. Verificación del cumplimiento y existencia del Procedimiento de funcionamiento de la planta eléctrica de la corporación.	Funcionamiento normal de la planta eléctrica en los momentos que se requiere.
23	USUARIOS (PERSONAS)	MAL MANEJO DE LA INFORMACIÒN	SENSIBILIZAR A LOS USUARIOS DE LA RESPONSABIIDAD EN EL USO, CUIDADO Y SEGURIDAD A TENER CON EL MANEJO DE LA INFORMACIÒN DE LA CORPORACIÒN.	POLITICA DE GESTIÒN DE LA SEGURIDAD DE LA INFORMACIÒN EN CORPORINOQUIA.	VERIFICACIÒN DE LA EXISTENCIA DE POLITICA DE GESTIÒN DE LA SEGURIDAD DE LA INFORMACIÒN DE CORPORINOQUIA. LISTAS DE ASISTENCIA A SOCIALIZACIÒN Y SENSIBILIZACIÒN EN EL USO Y PROTECCIÒN DE LA INFORMACIÒN DE LA CORPORACIÒN. LISTAS DE ASISTENCIA DE SOCIALIZACIÒN DE LA POLITICA DE GESTIÒN DE LA SEGURIDAD DE LA INFORMACIÒN DE CORPORINOQUIA.	

5.2 MODELO DE POLÌTICA DE GESTIÒN DE LA SEGURIDAD DE LA INFORMACIÒN

5.2.1 Introducción

Una vez realizado el contexto y el estado del arte de la gestión de la seguridad de la información, a nivel internacional, nacional, la verificación del estado de gestión de la seguridad de la información en cuanto al cumplimiento de la norma ISO 27001:2013, la identificación de activos, la identificación de riesgos y la definición de controles de los riesgos de los activos identificados en Corporinoquia, se procede a realizar el modelo de Política de Gestión de la Seguridad de la Información como mecanismo de seguridad de la Información en la Corporación Autónoma Regional de la Orinoquia, Corporinoquia, con la aplicación de la norma ISO/IEC 27001:2013, para lo cual se inicia con lo siguiente:

5.2.2 Objetivo

Brindar un instrumento guía para gestionar el uso, acceso y tratamiento de la información corporativa, como medio de gestión de la seguridad para la salvaguarda de los activos (información física, digital y herramientas tecnológicas (hardware y software)) de la Corporación Autónoma Regional de la Orinoquia, Corporinoquia.

5.2.3 Alcance

Este documento de política de gestión de la Seguridad de la Información, SGSI, aplica para la Corporación Autónoma Regional de la Orinoquia, Corporinoquia, en lo que tiene que ver con la seguridad de la información de los procesos de Planeación de la Gestión Ambiental, Gestión de Trámites y Servicios Ambientales, Gestión de Archivo y Correspondencia y Gestión de TICS, como procesos críticos y de gran importancia por el cumulo de información que se genera y por la importancia de administración de la misma y la gestión del riesgo a que se encuentra expuesta.

Se tendrán en cuenta las áreas físicas de la Subdirección de Planeación Ambiental, Secretaria General, Control y Calidad Ambiental, Oficina de Sistemas y Dirección General. No se tendrá en cuenta la oficina jurídica, ni la Subdirección Administrativa y Financiera. Adicionalmente, aplica para el personal interno y externo que esté vinculado a sus procesos Corporativos, bien sea por vinculación de planta, provisional o contratista.

Para esta actividad, se destina un profesional Especializado para la gestión de la seguridad de la información, quien es el desarrollador del presente proyecto, quien se encargara de la elaboración del modelo a desarrollar de ISO/IEC 27001:2013.

El liderazgo del proceso de gestión de la Seguridad de la Información será ejercido por la alta dirección de la organización.

5.2.4 Términos y Definiciones

Seguridad de la información: son todas las medidas necesarias utilizadas para prevenir ataques a la disponibilidad, confidencialidad e integridad de los activos de información y los sistemas de tecnología que permitir resguardarla y protegerla dentro de las organizaciones (WIKIPEDIA, 2015).

Control de acceso: Todos los procesos y procedimientos que debe cumplir un usuario o un elemento tecnológico para obtener la autorización de acceso a una aplicación, sistema de información, equipo o área restringida.

Autenticación: es el mecanismo de comprobación de la veracidad de la identidad de un usuario o activo tecnológico al intentar acceder a un recurso de procesamiento o sistema de administración de información.

Cifrado: combinación y transformación de datos mediante el uso de técnicas criptográficas para producir datos ininteligibles, asegurando su confidencialidad. A través del cifrado se previene la fuga de información, el acceso no autorizado a la misma y es utilizado como medio de protección de la misma.

Criptografía: Arte y técnica de escribir con procedimientos o claves secretas o de un modo enigmático, de tal forma que lo escrito solamente sea inteligible para quien sepa descifrarlo.

Confidencialidad: es la garantía de que la información esté disponible y habilitada solo para el personal, entidades o procesos autorizados mediante protocolos de control de acceso.

Disponibilidad: es la garantía de que a la información, equipos u otro tipo de activo, se tenga acceso en el momento que se requiera.

Integridad: es la protección del estado completo de los activos. Que se mantenga al 100% en todos sus componentes.

Perfiles de usuario: es la agrupación de varios usuarios con similares necesidades de información, autorizaciones y/o rango de permisos, sobre los diferentes recursos de tecnología y sistemas de información corporativos, facilitando los accesos de acuerdo con las funciones realizadas. Cuando se realizan modificaciones sobre perfiles de usuario, estas afectan a todos los usuarios pertenecientes al perfil.

Sistema de Información: conjunto organizado de datos, operaciones y transacciones que interactúan para el almacenamiento y procesamiento de la información, orientado al tratamiento y administración de datos que interactúan con activos de información para efectuar sus tareas e informes para la toma de decisiones.

Vulnerabilidades: son todas las debilidades de protección del activo y que en un momento determinado atenta contra la seguridad del mismo. Las vulnerabilidades pueden ser explotadas por factores externos y no controlables por la Corporación. Se pueden constituir en fuentes de riesgo que pueden llegar a ser vulneradas en un momento determinado.

5.2.5 Política de la Seguridad de la Información

La información de la Corporación Autónoma Regional de la Orinoquia, Corporinoquia es uno de los activos más importantes para la prestación eficaz, eficiente y efectiva de su objeto misional como es "*Corporinoquia como autoridad ambiental y administradora de los recursos naturales, gestiona el desarrollo sostenible, garantizando la oferta de bienes y servicios ambientales, mediante la implementación de acciones de prevención, protección y conservación Por una Región Viva*"[7] (CORPORINOQUIA, 2015). Dicha información ayuda en la toma de decisiones de forma eficiente, por dicho motivo existe un compromiso de protección hacia la información como una estrategia en la continuidad del negocio, administración de los riesgos de los activos, la construcción y aseguramiento de una cultura de seguridad de la información.

Esta guía pretende definir un conjunto de Políticas para la seguridad de la información, la cual a través del compromiso decidido de la alta dirección, se aprueba, se publica y se

[7] Misión Corporinoquia: Tomado del documento PGA-MAN-001 Manual de Calidad del Sistema de Gestión de Calidad de Corporinoquia.

comunica a todos los actores intervinientes dentro del proceso de gestión de la seguridad de la información.

Va dirigida a todos los funcionarios, personal externo, e interno y todo aquel que tenga responsabilidad con el uso de información física y digital de Corporinoquia, para que se adopten los lineamientos establecidos, para proteger y conservar la integridad, confidencialidad, garantizando la disponibilidad de la información física y digital, como medio de consulta y continuidad de todos los procesos misionales y de apoyo de la Corporación.

Esta política de gestión de la seguridad de la información está fundamentada en los dominios y objetivos de control del Anexo A de la norma ISO 27001:2013.

5.2.5.1 Compromiso de la Dirección

La Corporación está conformada por el Consejo Directivo quien es el órgano que autoriza y aprueba la Política de Seguridad de la información de Corporinoquia, como un compromiso de la alta dirección en la generación de políticas eficaces y eficientes que garanticen la seguridad de la información ambiental de la Orinoquia Colombiana.

El Consejo Directivo y la Alta Dirección de Corporinoquia demuestran su compromiso a través de:

- La verificación, análisis, validación y aprobación de las Políticas de Seguridad de la información de Corporinoquia, habilitadas en la Presente Política de Gestión de la Seguridad de la información.
- La sensibilización y promoción de una cultura de seguridad de la información.
- Divulgar a cada uno de los funcionarios de Corporinoquia, el documento “Política de Gestión de la Seguridad de la Información de Corporinoquia”.
- Asegurar los recursos necesarios para implementar y mantener las políticas de seguridad de la información de Corporinoquia.
- El seguimiento y control de cumplimiento de las políticas mencionadas en el presente documento.

La alta Dirección liderará el cumplimiento de la Política de Seguridad de la Información y gestionará la conformación de un Comité de Gestión de Seguridad del Información en Corporinoquia, el cual estará conformado por miembros de las siguientes áreas:

- Dirección General o su delegado
- Subdirección de Planeación Ambiental o su delegado
- Representante de la Oficina de Sistemas
- Subdirección Administrativa y Financiera o su delegado
- Subdirección de Control y Calidad Ambiental o su delegado
- Secretaria General o su delegado
- Oficina de Control Interno o su delegado
- Oficina Jurídica o su delegado
- Dirección Territorial de Arauca o su delegado
- Dirección Territorial la primavera o su delegado
- Oficina Ambiental de Caqueza o su delegado

Dicho Comité tendrá funciones específicas de generar estrategias y mecanismos que garanticen la seguridad de la información en Corporinoquia, así como brindar apoyo en la revisión de las políticas, de acuerdo a cambios significativos, asegurando su conveniencia, adecuación, y eficacia y mejoramiento continuo.

5.2.6 Política de Organización de la Seguridad de la Información

La presente política de gestión de la seguridad de la información busca enmarcarse dentro del objeto misional de Corporinoquia, como una herramienta que permite la gestión de la seguridad de la información para la continuidad y gestión de los procesos. Dichas normas van dirigidas al manejo que los usuarios de la Corporación, deben tener en cuenta en cada uno de sus áreas de trabajo y su relación con el uso de la información y los demás activos de la Corporación. Adicionalmente, se abordará con respecto a los roles y funciones desempeñadas dentro de la organización con respecto a administración, operatividad y gestión de la seguridad de la información.

Define la responsabilidad en el uso de activos, permitiendo la gestión de la seguridad de los mismos, a través de la identificación de cada uno de los riesgos de los activos relacionados con el uso de la información de la Corporación.

5.2.6.1 Política de Roles y Responsabilidades de Aplicación de la Política de Seguridad

La responsabilidad y aplicación de la seguridad de la información es de carácter obligatorio para todo el personal vinculado a la Corporación, cualquiera que sea su tipo de vinculación, la sede o Subdirección a la cual se encuentra adscrito y el nivel de funciones o actividades que desempeñe.

El Comité de Seguridad de la Información será el encargado de gestionar todo lo relacionado con la gestión de la seguridad de la información, para lo cual, deberá realizar un plan de acción para ejecutar en cada vigencia, este debe incluir las revisiones y actualizaciones a que haya lugar, en busca del mejoramiento continuo.

Dentro del Comité de gestión de la seguridad de la información se debe nombrar un representante que será quien lidere las acciones del comité, así como de impulsar e implementar el cumplimiento de la Política de Seguridad.

La oficina de Talento Humano deberá realizar la divulgación de la aplicación de la Política de Seguridad de la información, a todo el personal que se vincule a Corporinoquia, independientemente del tipo de vinculación que tenga. Todo el personal vinculado a la entidad deberá firmar un acuerdo o compromiso donde exprese la intención de cumplimiento de la Política de Gestión de la Seguridad de la información, el uso adecuado y cuidado de las herramientas TIC dentro y fuera de la corporación.

La oficina de sistemas debe asegurar los mecanismos para la difusión y aceptación de las condiciones por medio de registros y manuales en línea y deberá mantener este material siempre disponible para su consulta.

Los usuarios responsables de los activos de información son responsables de su clasificación, mantenimiento y actualización, así como de documentar. Se debe definir los usuarios que tengan acceso a estos activos y a que información pueden acceder, y deben definir los tipos de permisos y roles a tener par la respectiva autenticación y autorización de acceso. Los funcionarios de sistemas de Corporinoquia, serán los responsables de cumplir con la seguridad de los sistemas de información de la misma, lo que incluye la operación del Sistema de Gestión de la Seguridad de la Información SGSI y supervisión dentro del área de sistemas de lo definido en la política de Seguridad de la Información.

Dentro de las responsabilidades que se deben cumplir en el presente ítem, hace parte el apartado “6.5.1 Compromiso de la Dirección”.

5.2.6.2 Aspectos importantes en la organización Interna

Las políticas de seguridad de la información generados en el presente documento, son los lineamientos que buscan defender, proteger y resguardar la información en Corporinoquia, por lo tanto, cualquier violación a lo establecido en las mismas está sujeto a la aplicación de medidas correctivas de acuerdo a los niveles de clasificación de las violaciones y mitigar posibles afectaciones contra la seguridad de la información. Estas medidas de protección se enmarcan desde medidas administrativas, hasta apertura y ejecución de procesos disciplinarios y dependiendo del nivel o penal, dependiendo de la falta o tipo de ataque a la seguridad de la información que se haya identificado.

En los casos en que se materialice un riesgo o se presente una anomalía relacionada con el contenido de la política de seguridad de la información y dependiendo de la magnitud de la misma, se debe reportar de inmediato al jefe inmediato del área donde se presente el hallazgo, seguidamente a la oficina de Control Interno y Oficina de Control Interno Disciplinario. Si el caso da para investigación se debe hacer un llamado a las autoridades pertinentes que conozcan de la gestión de seguridad de la información, para que brinden el acompañamiento necesario, como lo es la Policía Nacional de delitos informáticos de Colombia, más exactamente la de Yopal, Casanare, para que realice la investigación o la asesoría necesaria en caso de llegar a necesitarse. Así mismo, dependiendo si la falta lo amerita, se deberá informar a los entes de control como son Procuraduría General de la Nación, Fiscalía General de la Nación y Contraloría General de la Nación.

Adicionalmente, la Corporación deberá realizar las acciones necesarias para mantenerse en constante actualización, para lo cual debe gestionar a través del Comité de Seguridad de la Información las capacitaciones necesarias e inscripciones a grupos de interés expertos en seguridad de la información en búsqueda de retroalimentación y el mejoramiento continuo del proceso.

5.2.6.3 Lineamientos para el uso y apropiación de dispositivos móviles y teletrabajo

Corporinoquia a través de la oficina de sistemas proveerá los mecanismos necesarios de seguridad y de acceso de los dispositivos móviles como teléfonos, tabletas, portátiles y

demás elementos de conexión inalámbrica de uso corporativo y personal que hagan uso de los servicios y equipos proporcionados por la Corporación, para lo cual se debe:

Investigar las tecnologías necesarias en materia de seguridad informática enfocada a dispositivos móviles, realizar las pruebas necesarias para la protección de los dispositivos

Realizar las configuraciones necesarias aceptables para cada uno de los dispositivos móviles personales o corporativos. Para lo cual se debe establecer métodos de bloqueo y control de acceso personalizado, como contraseñas, patrones de reconocimiento, biometría, reconocimiento de voz a cada uno de los usuarios y dispositivos móviles asignados. Deben tener control de tiempos de uso para el bloqueo automático de los dispositivos y aumentar la seguridad de la información.

Se debe facilitar la opción de cifrado a las memorias o discos de almacenamiento de dispositivos móviles, con el fin de evitar la copia o extracción de datos de forma fraudulenta y sin autorización.

Al momento de configurar los dispositivos móviles se debe activar la opción de administración remota para control de información (borrado o copiado) de cada dispositivo con el fin de evitar fugas de información en caso de pérdida de los dispositivos móviles, sin embargo cada dispositivo móvil contara con una copia de seguridad que se realizará en línea. Dicha copia de respaldo debe estar acorde a la Política de Backup de la información.

Todos los dispositivos móviles que se conecten a los servicios de tecnología de la Corporación, sin excepción deben contar con un antivirus.

Todos los dispositivos móviles entregados a los usuarios para su uso, se entregan configurados. Ningún usuario está autorizado para cambiar o modificar la configuración, instalar o desinstalar software. Cualquier necesidad al respecto debe ser solicitada al área de sistemas para su correspondiente viabilizarían. Solo se permitirán las actualizaciones que los programas instalados soliciten.

La oficina de sistemas debe llevar un registro de dispositivos móviles asignados y con acceso a la plataforma tecnológica corporativa, especificando los datos básicos del dispositivo, los permisos asignados y los datos del usuario al cual se le asigna el activo.

Los usuarios deben evitar el uso de dispositivos móviles Corporativos en redes externas a las autorizadas por la corporación, como medida de precaución y cuidado de la información que en estos equipos se maneje. Esto ayuda a evitar pérdida o robo de los activo (información y/o dispositivo). Se debe desactivar las opciones de Bluetooth e infrarrojo para evitar fuga de información.

El uso de los dispositivos móviles es para uso corporativo y la información que repose en los mismos debe ser de carácter laboral y corporativo.

Los usuarios deben evitar introducir los dispositivos móviles corporativos a otros equipos de cómputo de dudosa reputación como por ejemplo computadores públicos, de hoteles, entre otros.

Para los casos de teletrabajo la corporación a través de la Política de seguridad de la información establece:

Identificar los riesgos que tendrá cada uno de las posibles conexiones remotas, los tipos de acceso, permisos a otorgar, entre otros. Se deben definir los controles necesarios y su efectividad, los cuales serán verificados constantemente.

Las conexiones remotas a equipos de cómputo y servidores, se deben evitar. Solo personal autorizado por el Comité de Seguridad de la Información de la Corporación, podrá realizar actividades de acceso remoto y por un periodo de tiempo. Los permisos se otorgaran de acuerdo a las funciones desempeñadas. Los usuarios acataran las condiciones de uso establecida para las conexiones remotas. El acceso remoto se otorgara a equipos identificados por la corporación. Estas solicitudes de acceso remoto deberá estar justificada por el Jefe Inmediato del área, y será evaluada en reunión del comité mencionado.

La oficina de control interno de la Corporación dentro de su proceso de auditoría interna, deberá verificar la eficacia de los controles implantados para las conexiones de acceso remoto.

5.2.7 Políticas de Seguridad de los Recursos Humanos

5.2.7.1 Antes de Asumir el empleo

El recurso humano para Corporinoquia es uno de los activos más importantes en la gestión de los procesos misionales y de apoyo, por lo tanto, es importante garantizar contar con el personal mejor calificado, para lo cual, se deben definir unos estándares de seguridad que aseguren un proceso formal de selección, orientado a las funciones, cargo y roles que desempeñara al interior dela corporación cada funcionario, para lo cual se debe:

En los procesos de selección de personal para suplir vacantes, se debe verificar la veracidad y autenticidad de la información suministrada por el candidato a ocupar un cargo en Corporinoquia. Esta verificación será un requisito de cumplimiento antes de vincular al nuevo personal.

La oficina de Talento Humano deberá realizar la divulgación de la aplicación de la Política de Seguridad de la información, a todo el personal que se vincule a Corporinoquia, independientemente del tipo de vinculación que tenga. Todo el personal vinculado a la entidad deberá firmar un acuerdo o compromiso donde exprese la intención de cumplimiento de la Política de Gestión de la Seguridad de la información, el uso adecuado y cuidado de las herramientas TIC dentro y fuera de la corporación.

Cada supervisor o jefe inmediato deberá comprobar el cumplimiento de la firma de los acuerdos de confidencialidad de la información por parte de los contratistas o funcionarios asignados, antes de autorizar el acceso a la información. Esta política aplica para todo el personal inclusive al provisto por empresas contratistas que realicen labores en Corporinoquia.

5.2.7.2 Durante la ejecución del Empleo

Para iniciar a ejecutar labores del empleo el funcionario debe firmar el acuerdo de confidencialidad de la información. Y este debe aplicar la Política de Seguridad de la información con el fin de garantizar la integridad, confidencialidad y disponibilidad de la información en la Corporación.

El área de talento humano en conjunto con el área de sistemas de Corporinoquia, deben establecer jornadas de capacitación en temáticas relacionadas con la seguridad de la información. La asistencia de todo el personal de planta es de carácter obligatorio y la asistencia por parte de contratistas es obligatoria dependiendo del grado de relación con la información misional y de apoyo de la Corporación, según sus funciones y cargo.

La oficina de Control Interno Disciplinario debe establecer un proceso sancionatorio formal, el cual debe ser socializado y conocido por todos los funcionarios. Este procedimiento facilitará los mecanismos para emprender acciones contra empleados o contratistas que hayan cometido violaciones a la seguridad de la información.

5.2.7.3 Terminación y cambio de empleo

Se debe definir las responsabilidades y los deberes de la seguridad de la información que deben asumir los funcionarios o contratistas que terminen su vinculación laboral con Corporinoquia, en el acuerdo de confidencialidad de la información firmado por las partes, así como en el proceso contractual vinculante. El supervisor o jefe inmediato tendrá la responsabilidad de que toda la información administrada por el funcionario a retirar sea entregada en su totalidad y que se garantice su confidencialidad.

5.2.8 Política de Seguridad de Gestión de los Activos

Corporinoquia como propietaria de la información física e información digital procesada, almacenada y transmitida desde la infraestructura tecnológica, otorga responsabilidad sobre los activos de información asignada a cada una de las subdirecciones, Secretaria General y Direcciones Territoriales, asegurando el desempeño de la presente política de seguridad de la información.

Los sistemas de información, la información, los equipos de cómputo de escritorio y portátil, la red de datos, scanner, impresoras, UPS, planta eléctrica y todo el conjunto de plataforma tecnológica propiedad de Corporinoquia, son activos de la misma, y son asignados a cada uno de los funcionarios, contratistas y personal autorizado como herramientas de apoyo al cumplimiento del objeto misional de la Corporación.

Los activos donde se encuentre la información almacenada deben estar asignados a un responsable y se debe brindar las garantías de seguridad necesarias para su protección.

Los propietarios de los activos a quienes se encuentran asignados por inventario, deben mantener actualizado su inventario de activos de información, utilizarlos en cada uno de sus procesos y áreas y brindarles la seguridad necesaria.

5.2.8.1 Responsabilidades por los activos

La Dirección General, las Subdirecciones, las Direcciones Territoriales y la Secretaria General de Corporinoquia, debe actuar como propietarios de la información física y digital de la corporación, ejerciendo la autorización de accesos a la información con los permisos de acuerdo al rol que desempeñe el funcionario.

Los propietarios de los activos deben monitorear constantemente la validez de usuarios y perfiles autorizados al acceso de información. Para esto deben contar con un listado de activos del área que lideran, la clasificación de la información, los usuarios autorizados y permisos otorgados.

Todos los activos que procesan información son sujetos de auditoria por la oficina de control interno y de revisión de cumplimiento de los controles establecidos.

La oficina de Sistemas de Corporinoquia es la propietaria de los activos de información correspondiente a la plataforma e infraestructura tecnológica, por consiguiente, debe asegurar su operación y administración de forma eficaz.

Cualquier cambio a realizar en la estructura de la plataforma tecnológica debe ser autorizado por la oficina de sistemas en lo referente a instalación, cambio de equipos o traslados de la misma. Todos los recursos tecnológicos deben tener una configuración adecuada, que permita la preservación de la seguridad de la información.

La oficina de sistemas es la responsable de preparar los equipos tecnológicos para el uso adecuado de los mismos en la Infraestructura tecnológica de la Corporación (equipos de cómputo de escritorio y portátiles, impresoras, escáner, plotter, entre otros). Adicionalmente, es responsable de recibir los equipos tecnológicos para su asignación y reasignación e informar al almacén los cambios necesarios para el control de inventario, generar las copias de seguridad (backup) de la información de los funcionarios que se retiran o cambian de actividad o área, previa solicitud por parte del jefe inmediato del

funcionario que entrega el equipo de cómputo. Dicha solicitud se debe presentar vía correo electrónico al email: soporte@corporinoquia.gov.co.

Se debe revisar de manera periódica los riesgos de los activos, para identificar su estado y generar nuevas medidas de control en los casos que sea necesario, identificar nuevos riesgos y controlarlos.

Se debe realizar revisiones periódicas a la funcionalidad de los recursos de la plataforma tecnológica y los sistemas de información de Corporinoquia, para identificar su estado, y generar la protección de activos de información, tecnológicos y no tecnológicos, en caso de encontrarse o no vulnerable.

El uso de los servicios tecnológicos deben ser autorizados por: Director General, Subdirectores, Secretario General, Director Territorial, Coordinadores de Área, Jefes de oficina mediante solicitud a la oficina de sistemas de Corporinoquia, al email: soporte@corporinoquia.gov.co.

El Director General, Subdirectores, Secretario General, Director Territorial, o personal designado, deben recibir los equipos de tecnología asignados a sus funcionarios (Planta o contratista) cuando estos se retiran del área. El equipo debe quedar asignado en el área al que pertenece. Se deberá informar a la oficina de sistemas los cambios realizados al email: soporte@corporinoquia.gov.co.

Cuando un funcionario, contratista u otro tipo de personal vinculado con la corporación se retira de la empresa, este debe estar a paz y salvo por todo concepto de activos y servicios informáticos asignados, para lo cual, debe comparecer a la oficina de sistemas y almacén para la firma del respectivo Paz y Salvo, el que lo acredita que ya ha cumplido con la entrega de los activos y desactivación de servicios informáticos en la corporación.

Los recursos tecnológicos deben ser utilizados por todos los usuarios, de forma ética, eficiente y de forma exclusiva para el beneficio de Corporinoquia.

Los usuarios no deben utilizar software no autorizado en los equipos corporativos, y ningún otro elemento que afecte la infraestructura tecnología de Corporinoquia. Cualquier necesidad de software se debe informar a la oficina de sistemas para su evaluación y posterior decisión.

Los usuarios no deben conectar cargadores de celular, ventiladores, radios, u otro tipo de dispositivos diferentes a equipos de cómputo, en la red de corriente regulada de la Corporación.

Todas las estaciones de trabajo, dispositivos móviles, impresoras, scanner, plotter, entre otros, son asignadas a un responsable y este a su vez velara por la seguridad y cuidado de los mismos, a través del compromiso de uso adecuado y eficiente de dichos activos.

5.2.8.2 Clasificación de la Información

La Corporación a través del comité de seguridad de la información debe definir la Guía de clasificación de la información corporativa, identificando su importancia y sensibilidad. Los propietarios de la información la deben catalogar y deben determinar los controles requeridos para preservar la confidencialidad, integridad y disponibilidad de la misma. Los niveles de clasificación de la información y sus controles deben ser aprobados por el Consejo Directivo de Corporinoquia.

La guía de clasificación de la información de Corporinoquia debe ser socializada a todos los funcionarios de la corporación (planta y contratistas), una vez esté aprobada por el Consejo Directivo de la misma.

La oficina de sistemas debe gestionar las técnicas de cifrado de la información, así como realizar la administración el software que cifra y descifra la información, teniendo en cuenta la guía de clasificación de la información.

La Oficina de Sistemas debe generar las acciones para eliminar información de forma segura, en los equipos dados de baja o cuando cambian de usuario, evitando la recuperación y reconstrucción de la misma.

El comité de archivo debe autorizar la destrucción de información cuando se ha cumplido su ciclo de gestión y archivo, de acuerdo a las tablas de valoración documental de Corporinoquia. La Secretaria General como líder del proceso de gestión Documental de Corporinoquia, debe garantizar la destrucción correcta la documentación física, que ya perdió funcionalidad en el ciclo de vida documental, para evitar que pueda ser reconstruida. Los encargados de destruirla serán la Secretaria General

La Jefa de Archivo debe administrar los contratos relacionados con el resguardo de documentos físicos, de la Corporación. Debe contemplar toda la seguridad necesaria de los mismos, teniendo en cuenta las cláusulas de confidencialidad, integridad y disponibilidad.

Los usuarios responsables de activos de información deben monitorear la clasificación de sus activos de información y reclasificarlos cuando sea necesario. Toda la información física debe estar protegida, con controles de acceso físico y garantizar las condiciones adecuadas de almacenamiento y resguardo seguro.

Los usuarios deben acatar los lineamientos de la Guía de Clasificación de la información para el acceso, divulgación, almacenamiento, copia, transmisión, etiquetado y eliminación de la información contenida en los recursos tecnológicos, así como la información física de la Corporación.

La información de Corporinoquia está plenamente identificada en las tablas de retención documental, y allí se establecen los tiempos de almacenamiento para cada uno de los tipos documentales.

5.2.8.3 Manejo de Medios

La información de discos duros de copias de seguridad o información de manejo de información importante en el centro de datos de la Corporación, debe estar cifrada para evitar robos, alteración o pérdida de información. Para esto, la oficina de sistemas garantizara los medios necesarios para cifrar y descifrar los medios extraíbles correspondientes.

Todos los medios extraíbles asignados a funcionarios para manejo de información, deben ser registrados y dependiendo de la clasificación que se le dé a la información allí guardada es necesario generar técnicas de cifrado y descifrado. El funcionario a quien se le asigne un medio extraíble adquiere la responsabilidad de proteger la información y el activo entregado. En caso de querer devolverlo la oficina de sistemas debe brindar un concepto de la información que se tiene allí almacenada y generar los mecanismos necesarios para eliminar, o proteger la información a través de un backup de seguridad.

Los tokens de seguridad asignados a los funcionarios de la Subdirección Administrativa y Financiera son de carácter personal e intransferible y se debe mantener total seguridad por su alto grado de importancia en la realización de trámites de carácter presupuestal y financiero con el Gobierno Nacional. Los tokens asignados son de uso exclusivo en los equipos asignados por la corporación, para tal fin, en caso de pérdida se debe reportar de inmediato a la oficina de sistemas de Corporinoquia.

La oficina de sistemas debe implementar mecanismos que regulen el uso de periféricos y medios de almacenamiento en la plataforma tecnológica de Corporinoquia, así como los medios para su disposición final segura. La asignación de periféricos se debe autorizar dependiendo del perfil del cargo del funcionario solicitante.

El personal de la corporación a quienes se les asigne equipos periféricos debe acogerse a las normas de uso de periféricos y medios de almacenamiento.

5.2.9 Políticas de Seguridad de Control de Acceso

5.2.9.1 Acceso a la red de datos de Corporinoquia

La oficina de sistemas como responsable de la red de datos y los recursos instalados en la misma, debe protegerlos contra el control de accesos no autorizados a través de mecanismos de control de acceso lógico y proteger los puntos de red que se encuentren visibles y vulnerables de ataques.

Dentro del proceso TIC, de la oficina de sistemas se debe realizar el procedimiento de autorización y controles para restringir el acceso los recursos de la red de datos de la Corporación.

Se debe implementar métodos de autenticación en el servicio de red inalámbrica que evite accesos no autorizados.

Se debe verificar periódicamente los controles de acceso, permisos, tiempos de acceso, para todos los usuarios, validando que los usuarios autorizados tengan únicamente los permisos de red y la plataforma tecnológica para los que fueron autorizados.

Todo el personal antes de contar con acceso deben ser autorizados por el jefe inmediato, solicitando a través de correo electrónico a la oficina de sistemas, al email: soportecorporinoquia.gov.co, en donde debe enviar información básica del nuevo funcionario (nombre, identificación, profesión, área asignada, rol a desempeñar y autorización de información que puede ser consultada y que tipo de permisos se le concederán (crear, modificar, eliminar).

5.2.9.2 Gestión de Acceso de Usuarios

La oficina de sistemas debe elaborar el procedimiento para la administración de usuarios de la red de datos, los servicios tecnológicos y sistemas de información de la Corporación. Este debe contemplar la creación, modificación, eliminación y bloqueo de las cuentas de usuarios.

La oficina de sistemas es la encargada de crear, modificar o eliminar usuarios, de la red de datos y sistemas de información corporativa, previa solicitud de los jefes de área. Lo anterior, debe contemplar la generación de contraseñas seguras, con lineamientos como longitud, complejidad, cambio periódico, cambio de contraseña en el primer acceso, control histórico y bloqueo por número de intentos fallidos en la autenticación. Estos usuarios se deben comunicar vía correo electrónico a cada nuevo usuario.

Los propietarios de los activos de información deben validar periódicamente todas las autorizaciones sobre sus recursos de acuerdo a los perfiles otorgados e informar a la oficina de sistemas, las diferencias encontradas, para llevar a cabo los cambios y controles necesarios.

5.2.9.3 Responsabilidades de los usuarios

Los usuarios de los recursos tecnológicos y los sistemas de información de la corporación deben realizar un uso adecuado y responsable de los mismos, protegiendo la confidencialidad y salvaguardando la información autorizada, bien sea para consulta y/o modificación.

Los usuarios no deben compartir la información de cuentas de usuario y contraseñas. Esta información es intransferible y de uso únicamente corporativo.

Cuando se presente alguna alteración de la información y otro funcionario lo descubra, está en la obligación de informarlo al jefe inmediato del área donde se presenta el hallazgo.

5.2.9.4 Control de Accesos a sistemas y aplicativos

Las Subdirecciones, Secretaria General y Direcciones Territoriales, actuaran como propietarias y gestoras de los sistemas de información y demás aplicativos que apoyan los procesos misionales y de apoyo de la Corporación, velaran por la asignación, modificación y revocación de privilegios de acceso a sus aplicativos de forma responsable y controlada.

La oficina de sistemas propenderá porque los diferentes sistemas de información estén protegidos de accesos no autorizados a través de mecanismos de acceso lógico, así como las exigencias necesarias de seguridad para el desarrollo de software seguro en todas las etapas de desarrollo de software.

Los Jefes de área encargados de gestionar los sistemas de información, información física y digital, y aplicativos de software, serán quienes autorizan el acceso a funcionarios, estableciendo los permisos autorizados para acceder al sistema, para lo cual lo debe solicitar al email: soporte@corporinoquia.gov.co. Estos accesos deben ser monitoreados contantemente, por los propietarios del sistema de información.

La oficina de sistemas debe realizar e implantar el procedimiento de asignación de accesos a los sistemas y aplicativos de Corporinoquia.

Los ambientes de desarrollo, pruebas y producción, deben ser ambientes separados a nivel físico y lógico, contando cada uno con sus servidores, equipos, plataforma, aplicaciones y dispositivos, para evitar fallos en la integridad de la información en producción.

La oficina de sistemas debe establecer un procedimiento de requisitos básicos de seguridad, el cual contemple autenticación, autorización, auditoria, registro de eventos, entre otros, al momento de realizar desarrollos de software o tercerizarlos. A la vez, se deben definir claramente los requisitos necesarios al momento de gestionar un proyecto de desarrollo de software en la Corporación, y controlar que estos se cumplan en los tiempos de respuesta propuestos. Adicionalmente, velar por que el desarrollo de software cumpla con las etapas del ciclo de Vida de desarrollo de Software Seguro.

La oficina de sistemas debe contar con un repositorio de archivos fuente de los diferentes sistemas de información y además se debe restringir su acceso para evitar riesgo de pérdida de la integridad, confidencialidad y disponibilidad de los aplicativos de instalaciòn.

Los desarrolladores deben asegurar que los sistemas de información desarrollados requieran autenticación para todos los recursos y páginas del sistema, excepto las calificadas como informativas y de consulta a los usuarios externos. Adicionalmente deben tener en cuenta las diferentes restricciones de vulnerabilidades como SQL Injection y XSS, entre otras.

5.2.10 Políticas de Criptografía

La Guía de clasificación de la información permite identificar la información confidencial y de mayor seguridad, por esta razón la corporación deberá implementar los mecanismos necesarios para cifrar la información en formato digital, catalogada como de uso restringido bajo técnicas de cifrado para de proteger su confidencialidad e integridad.

La Corporación, desde la oficina de sistemas deberá crear e implantar un procedimiento para administración de llaves de cifrado y protocolos para la aplicación de controles criptográficos.

5.2.11 Políticas de Seguridad Física y del Entorno

Corporinoquia deberá velar por la gestión de controles efectivos de seguridad física y control de acceso que asegure el perímetro de las instalaciones en las sedes de la corporación y oficinas ambientales en toda su jurisdicción, evaluará los riesgos y amenazas físicas internas y externas y las condiciones medioambientales de las oficinas, los centros de documentos y los centros de datos de las mismas.

Las oficinas del centro de documentos y los centros de datos de las sedes, donde se encuentra información sensible, equipos, infraestructura tecnológica y de soporte de sistemas de información y red de comunicaciones, su acceso será restringido. La autorización la otorga la Secretaria General, al Centro de Documentos y el Subdirector de Planeación y el líder de la Oficina de Sistemas a todo lo relacionado con tecnología.

5.2.11.1 Normas de áreas seguras

Los accesos al centro de datos de cómputo o a los centros de cableado deben ser autorizados por el Subdirector de Planeación Ambiental o en su defecto el líder de la oficina de Sistemas. Los ingresos a estas áreas deben estar acompañadas por personal de planta de la Oficina de Sistemas de la Corporación y deben ser registrados los ingresos en una bitácora que se debe ubicar al ingreso del centro de datos.

Funcionarios o contratistas de la oficina de sistemas o personal que cuente con permisos y autorización de acceso a centro de datos de computo o centro de cableado y que sea descontinuado o trasladado de área, se le deben quitar de forma inmediata los privilegios de acceso al centro de cómputo (servidores) y centro de cableado.

La oficina de sistemas debe garantizar las condiciones físico-ambientales que permitan mantener la protección y normal funcionamiento de los recursos de la plataforma tecnológica ubicada en el centro de datos de cómputo y centro de cableado; se debe contar con sistemas de detección y extinción de incendios, sistemas de vigilancia y monitoreo, sistemas de control ambiental, en cuanto a flujos de temperatura y humedad, alarmas en caso de alteración de las condiciones medioambientales, sistemas de descarga eléctrica. Su monitoreo es permanente.

El mantenimiento de la red de datos, voz y eléctrica, se debe realizar bajo programación y lo debe realizar personal idóneo y calificado en el área respectiva.

Se debe asignar la responsabilidad a un funcionario de planta de la oficina de sistemas para que realice control y monitoreo de los sistemas de alarmas de los sistemas de seguridad de los equipos del centro de datos y centros de cableado de la Corporación.

La oficina de Recursos Físicos proporcionara los recursos y elementos necesarios para ayudar a proteger y velar por el normal funcionamiento y correcto estado de los controles físicos implantados en cada uno de los activos ubicados dentro de las instalaciones físicas de la Corporación. A la vez, evaluar la posibilidad de mejorar los mecanismos de control para proveer de seguridad las instalaciones de la misma.

Se debe llevar un registro del control de accesos de todo el personal a la Corporación y la oficina de recursos físicos se encargara de la custodia de dichos registros.

La oficina de recursos físicos será la responsable de controlar el ingreso de personal a los centros de cableado y espacios que están bajo su custodia, así como verificar que no se encuentren líquidos inflamables cerca de los centros de cableado.

La oficina de recursos físicos debe programar revisiones del cableado de la red de datos y red de corriente regulada, en conjunto con la oficina de sistemas, para disminuir las intercepciones o daños.

Los funcionarios vinculados a la Corporación (planta y contratista) deben portar el carné que lo identifica como funcionario de la misma; lo deben usar durante la su permanencia en sus instalaciones. En caso de pérdida deben reportarlo de forma inmediata a la oficina de Talento Humano.

Los funcionarios de la Corporación y personal previsto por empresas o terceras partes vinculadas a la misma, no deben intentar ingresar a sectores o áreas que no están autorizados. Deben estar autorizados para ingresar a oficinas diferentes a las asignadas en su objeto laboral.

5.2.11.2 Equipos

La Corporación a través de la oficina de sistemas, debe garantizar la seguridad necesaria de todos los equipos de cómputo con el fin de evitar robos, fallos o daños en los mismos. Se deben generar estrategias que protejan la confidencialidad, integridad y disponibilidad de los recursos tecnológicos dentro y fuera de la corporación.

Se debe prever dentro del plan de acción anual de la oficina de sistemas, la actividad de programación de mantenimiento preventivo y correctivo de equipos de cómputo y demás equipos de la plataforma tecnológica.

La oficina de sistemas debe emprender e implementar mecanismos de estandarización de seguridad para equipos de cómputo corporativos y configurarlos de acuerdo a los estándares y mecanismos generados.

La oficina de sistemas debe definir las condiciones básicas que deben cumplir los equipos de cómputo de personal contratista que necesiten conectarse a la red de datos, verificando su cumplimiento de dichas condiciones antes de dar acceso a los servicios de red.

Se deben aislar los equipos de tesorería para proteger su acceso de usuarios no autorizados o de funcionarios de la red de la Corporación. Adicionalmente, se deben brindar mecanismos de autenticación fuerte.

Se debe definir un procedimiento de altas y de bajas para la disposición final de equipos de cómputo de la corporación.

La oficina de control interno debe incluir dentro del plan anual de auditorías la verificación de equipos de cómputo de forma aleatoria en las diferentes subdirecciones y centros de atención de la Corporación.

La oficina de recursos físicos debe garantizar la restricción de acceso físico a los diferentes equipos de cómputo y a las áreas donde se procesa la información sensible de trámites ambientales y proceso sancionatorio.

La oficina de Recursos Físicos debe generar mecanismos y controles de seguridad que protejan los activos al ingreso y a la salida de la Corporación. Para esto, se debe contar con documento donde se autorice la entrada o salida de activos, por el profesional Universitario de Planta de Recursos Físicos.

Los equipos como servidores, panta eléctrica, red de datos, red de corriente regulada, UPS de 20 y 30 Kw, cuenten con pólizas de seguro todo riesgo.

Los funcionarios de la oficina de sistemas, sección soporte y mantenimiento, son los únicos autorizados para realizar movimientos y asignación de recursos tecnológicos. Está prohibida la disposición de elementos tecnológicos que pueda realizar cualquier funcionario de la Corporación, diferente a los ya mencionados.

Cuando se presente algún daño relacionado con su equipo de cómputo, o cualquier recurso tecnológico a su cargo, el usuario responsable deberá informar y solicitar su verificación al email: soporte@corporinoquia.gov.co. El usuario no debe intentar solucionar el problema. La instalación, reparación o retiro de cualquier componente de hardware o software de las

estaciones de trabajo, dispositivos móviles y demás recursos tecnológicos de la Corporación, solo puede ser realizado por los funcionarios de la Oficina de Sistemas o personal autorizado por la misma.

Los usuarios de los equipos de cómputo deben bloquearlos al momento de abandonar su puesto de trabajo.

Los usuarios de los equipos de cómputo de la corporación (planta y contratista), deben apagarlos en horas no laborales.

En caso de pérdida o robo de un equipo de cómputo corporativo, se debe informar de inmediato al jefe o líder del proceso para que se inicie el trámite interno. Se debe instaurar denuncia ante la autoridad competente más cercana.

Al terminar la jornada laboral, los funcionarios (planta y contratista) deben asegurarse de dejar sus sitios de trabajo en perfecto orden. No deben dejar documentación física expuesta. Toda la documentación corporativa se le debe garantizar su confidencialidad.

Se debe colocar el protector de pantalla autorizado en todos los equipos de cómputo, relacionados con el Sistema de Gestión de Calidad y el escritorio del computador debe permanecer limpio de archivos u otros iconos.

5.2.12 Políticas de Seguridad de las Operaciones

5.2.12.1 Procedimientos, Operaciones y Responsabilidades

La oficina de sistemas como responsable del proceso TIC, en la Corporación, deberá asignar a cada uno de sus funcionarios (planta y contratista) funciones y responsabilidades definidas. Estos deben generar estrategias para el soporte, operación y administración de los recursos tecnológicos, garantizando la mejora continua de los procesos operativos para el desarrollo de las actividades.

La oficina de sistemas deberá apoyar la formulación del Plan de Acción de la Corporación en lo relacionado con las proyecciones de crecimiento en la plataforma tecnológica y gestión de la misma.

La oficina de sistemas debe elaborar los manuales de configuración y operación de los diferentes servicios tecnológicos como es: servicios de red, sistemas de información, base de datos, sistemas operativos, como medio de continuidad y estandarización en el desarrollo de las actividades en la oficina.

La oficina de sistemas debe proveer a los funcionarios de la misma los espacios necesarios para la ejecución de actividades y sus respectivos controles de prestación de servicios de calidad, hacer seguimiento y gestión para el cumplimiento de los mismos.

5.2.12.2 Protección contra códigos maliciosos

Se debe asegurar que los equipos de cómputo cuenten con software antivirus, antimalware, y anti spam, que reduzcan el riesgo de software malicioso y respalden la seguridad de la información resguardada en la plataforma tecnológica. Dicho software de antivirus debe estar licenciado.

Se debe configurar el software antivirus de tal forma que no pueda ser modificada por los usuarios. Adicionalmente, la configuración debe permitir las actualizaciones automáticas y parches de seguridad, para mitigar las vulnerabilidades de la plataforma tecnológica.

Los usuarios deben asegurarse que los archivos recibidos por correo electrónico proceden de fuentes seguras y conocidas para evitar ataque de virus o instalación de software malicioso en los equipos. En caso de sospecha de archivos desconocidos se debe llamar a la oficina de sistemas para brindar la asesoría y acompañamiento.

Los archivos que son recibidos de dudosa procedencia y/o que son abiertos o ejecutados por primera vez, deben ser analizados con el antivirus. Los medios extraíbles deben ser evaluados por el antivirus antes de abrir, al igual que los archivos que provienen de correo electrónico.

5.2.12.3 Copias de Respaldo

El comité de seguridad de la información debe definir un procedimiento para la realización de copias de seguridad de la información sensible e importante relacionada con los procesos misionales y de apoyo, y debe hacer seguimiento y control a las copias de seguridad de la información, verificando su realización y funcionalidad y debe gestionar la

infraestructura tecnológica necesaria para que se lleven a cabo dentro y fuera de la Corporación.

La Oficina de sistemas deberá generar y adoptar el procedimiento para la generación, restauración, almacenamiento y tratamiento de copias de respaldo de la información, promoviendo su integridad y disponibilidad.

La oficina de sistema debe llevar a cabo los procedimientos para realizar pruebas de recuperación a las copias de respaldo, comprobando su integridad y funcionalidad, para uso en caso de ser necesario.

Los propietarios de los recursos tecnológicos y sistemas de información en conjunto con la oficina de sistemas, deben definir las estrategias para la generación, retención y rotación de las copias de respaldo de los activos de información.

Es responsabilidad de todos los usuarios de la plataforma tecnológica, ayudar a identificar la información sensible e importante que deba ser respaldada mediante copias de seguridad.

5.2.12.4 Registro y seguimiento

Corporinoquia realizará monitoreo constante al uso que dan los funcionarios y el personal contratado a los activos tecnológicos de la plataforma y sistemas de información. Así como la custodia de registros de acceso y auditoria del sistema a través de los registros de eventos.

El Comité de Seguridad de la información deberá determinar elementos y recursos tecnológicos importantes a los cuales se les debe generar log de auditoria, como medio de registro y verificación al suceso de eventos.

Se debe definir un procedimiento de revisión de logs, donde se indique la forma como se deben abordar dichas revisiones, y además, los registros de eventos a revisar y a que activo o proceso corresponden, y quienes serán los encargados de realizarlos.

Para el desarrollo de software, el equipo desarrollador debe tener en cuenta los logs de auditoria de los sistemas de información, teniendo en cuenta intentos de autenticación fallidos y exitosos, intento de evasión de controles, fallas en los controles de acceso, fallas

de validación, excepciones en los sistemas, funciones administrativas y cambios de configuración de seguridad, de acuerdo a los requerimientos de funcionalidad y seguridad, presentados en los estudios previos de los procesos de contratación de desarrollo de software. Este documento debe estar aprobado por el Comité de Seguridad de la información y la oficina de sistemas de la Corporación.

5.2.12.5 Control de software Operacional

La oficina de sistemas deberá establecer procedimientos y asignar responsabilidades para brindar soporte en la instalación de software operativo (misional y de apoyo), en los equipos de cómputo. Todo software instalado en los equipos corporativos debe ser licenciado y debe contar con soporte de proveedores. Así mismo se deben establecer de usuario, para la instalación de software operativo en los equipos de cómputo de la Corporación.

La oficina de sistemas debe tener en cuenta los riesgos a asumir ante la migración a nuevas versiones de software. Debe verificar el normal funcionamiento de sistemas de información sobre la plataforma tecnológica cuando este es actualizado.

5.2.12.6 Gestión de la Vulnerabilidad Técnica

La oficina de sistemas de Corporinoquia realizara revisiones periódicas de la aparición de vulnerabilidades técnicas sobre los sistemas de información y los demás recursos de la plataforma tecnológica, con el objeto de realizar correcciones sobre a hallazgos encontrados en las pruebas. Esta revisión se realizara por el personal encargado de la oficina de sistemas y será presentado al Comité de la Seguridad de la información quienes revisaran, valoraran y gestionaran las vulnerabilidades técnicas encontradas.

Se debe gestionar los trámites correspondientes para la realización de pruebas de vulnerabilidades y hacking ético por un ente externo contratado con el fin de encontrar las posibles vulnerabilidades a ataques y definir un plan de seguridad para las vulnerabilidades encontradas.

La oficina de sistemas de la corporación, debe generar y ejecutar planes de acción que mitiguen las vulnerabilidades detectadas en la plataforma tecnológica.

5.2.13 Políticas de Seguridad de las Comunicaciones

5.2.13.1 Gestión de la seguridad de las redes

La oficina de sistemas establecerá el procedimiento de autorización y controles para proteger el acceso a la red de datos y los demás activos tecnológicos de la red de la Corporación.

La red inalámbricas de la Corporación, deben contar con métodos de autenticación que eviten accesos no autorizados.

La oficina de sistemas de la Corporación debe estructurar la información a almacenar en el servidor donde se identifique claramente las áreas y temáticas a las que pertenece, y estructurar los oles y permisos que van a tener cada uno de los usuarios a la misma.

La oficina de sistemas debe instalar protección entre la red interna de Corporinoquia y la red externa (internet). Debe velar por mantener la confidencialidad de la información en el direccionamiento y enrutamiento de las redes de datos de la Corporación.

Los Subdirectores, Directora General y Jefes de área deben autorizar los privilegios de acceso a los recursos de la red de datos de la Corporación, para lo cual, deben informar los datos básicos del usuario, tipo de vinculación, función a realizar, información autorizada y tipo de rol a desempeñar con la información (creación, modificación o consulta) y área a la que pertenece, así como los diferentes accesos a sistemas de información y elementos tecnológicos de la red de datos. Dicha solicitud la debe presentar al email: soporte@corporinoquia.gov.co

Los usuarios que deseen el servicio de conexión de equipos de cómputo a la red de datos, deberán cumplir todos los requisitos para autenticarse y únicamente deberán realizar tareas para las que fueron autorizados. Es responsabilidad del usuario y jefe de área informar al área de sistemas cualquier anomalía o cambio en su equipo de trabajo acceso autorizado.

5.2.13.2 Transferencia de Información

La Corporación asegurara los controles y procedimientos para el intercambio de información y brindará la protección de la información al momento de ser transferida a otras organizaciones.

Desde la oficina jurídica al momento de realizar el proceso de contratación con terceros se debe dejar en el contenido de los contratos las cláusulas necesarias para pactar la confidencialidad y protección de la información Corporativa.

La Corporación deberá asegurar que los propietarios o administradores de activos de información brinden protección a la información, evitando su divulgación a terceros y brindando total confidencialidad a la misma, sobre todo en los casos de expedientes ambientales, preliminares y proceso sancionatorio, así como diferentes tipos documentales, como conceptos técnicos, resoluciones, Autos e informes Ambientales.

Se debe dejar registro de todas las transacciones de información en cada una de las dependencias de la Corporación, y estas deben estar autorizadas por el Subdirector de cada Área o Jefes Inmediatos, teniendo en cuenta las política de seguridad de la información Corporativa.

Los funcionarios responsables de activos de información realizaran intercambio de información digital, siempre y cuando este autorizada por el jefe de área, acatando la Política de seguridad de administración de red, acceso lógico y protección de datos de tipo personal de la Corporación, teniendo en cuenta el procedimiento de intercambio de información entre la Corporación y terceros.

El área de Secretaria General, como responsable de la implementación de directrices de Gestión Documental en la Corporación deberá elaborar e implementar el procedimiento de intercambio de información (documentos y medios de almacenamiento) con terceros y la adopción de controles para la protección de la información de acuerdo a su importancia y grado de confidencialidad a tener en cuenta.

La información a entregar a terceros debe quedar registrada a través de documento donde se autoriza y se envía (Comunicación Oficial), y debe ser entregada únicamente por los mecanismos de envío autorizado por la Secretaria General de Corporinoquia.

La oficina de Sistemas debe ofrecer herramientas tecnológicas de intercambio seguro de información digital o en medio magnética, que permitan el cumplimiento de las Políticas de Seguridad de la información de la Corporación,

La Corporación y las áreas responsables que den contestación a solicitudes de información, deberán evaluar la pertinencia y los cuidados en la entrega de información confidencial a terceros, estos deberán velar por proteger dicha información y evitar divulgaciones no autorizadas.

Los usuarios del correo corporativo, no deben utilizarlo para enviar información sensible de la corporación o de sus funcionarios. Tampoco está permitido brindar información Corporativa vía telefónica o conferencias remotas.

La Alta Dirección será la única autorizada para realizar comunicados de prensa y de información importante de la gestión ambiental, bien sea por los medios de comunicación como radio, televisión, pagina web, redes sociales entre otros.

5.2.14 Políticas de Adquisición, Desarrollo y Mantenimiento de Sistemas

5.2.14.1 Requisitos de Seguridad de los sistemas de información

La Corporación debe asegurar que el software adquirido y desarrollado interna y por terceros, debe cumplir con el 100% de requisitos de seguridad y calidad establecidos en los términos de referencia y documento técnico de requisitos elaborado por la Corporación. Las áreas relacionadas con el software a adquirir o desarrollar deberán aportar los requisitos correspondientes y deberán ayudar a verificar su cumplimiento, durante las pruebas de funcionamiento.

Cada software a desarrollar deberá tener un área específica asignada quienes serán los encargados de gestionarla dentro de la organización. La administración de los sistemas de información, la realizaran los funcionarios de la oficina de sistemas.

La oficina de sistemas deberá definir una metodología de desarrollo de software seguro dentro de la Corporación, garantizando el cumplimiento de requisitos de seguridad y calidad del software.

La definición de requisitos de seguridad de los sistemas de información a desarrollar

Todas las aplicaciones de software adquiridas o desarrolladas deben estar documentadas para su mejor adaptabilidad y entendimiento. Se debe exigir a los desarrolladores este requisito.

Los desarrolladores de software de la Corporación, deben implementar controles para la duración de sesiones activas del aplicativo software, con el fin de evitar suplantaciones de sesión, por usuarios descuidados con las sesiones al dejar equipos sin seguridad.

Para autorizar la creación de usuarios y contraseñas es necesario tener en cuenta la política de seguridad de control de accesos.

La Corporación se asegurara a través de las áreas involucradas en cada desarrollo de software, bien sea interno o a través de un tercero, que se cumpla con los requerimientos de seguridad del ciclo de vida de desarrollo de software seguro, de acuerdo a la metodología de desarrollo de software seleccionada. La Corporación debe asegurar que el software a adquirir debe contar con soporte técnico durante el funcionamiento del mismo.

Antes de poner en funcionamiento el software desarrollado o adquirido en la Corporación, los responsables del área de uso del mismo, deben verificar su funcionamiento y certificar el cumplimiento de los requerimientos de calidad y seguridad, para esto, el área correspondiente debe documentar la revisión. Se debe hacer cada vez que se haga entrega de funcionalidades del sistema. La oficina de sistemas de la Corporación, debe brindar el acompañamiento necesario en estas pruebas.

En caso de requerir migraciones de información de un sistema a otro, esta debe ser autorizada por el área propietaria de la misma. La oficina de sistemas y el personal en cargado de realizar las migraciones debe garantizar los controles necesarios para asegurar que la migración de información entre ambientes de desarrollo, pruebas y producción este autorizados por el área pertinente, así como gestionar la seguridad de la información a migrar.

Durante las etapas de desarrollo, la oficina de sistemas se encargara de contar con un repositorio de control de versiones del software que está en proceso de desarrollo o desarrollado. Para esto, el desarrollador o tercero deberá hacer entrega de la versión presentada del software, a la oficina de sistemas de la Corporación.

Los contratos con objeto de desarrollo o adquisición de software deben evidenciar el tipo de licenciamiento, los derechos de autor y el tipo de uso del software que va a tener la corporación. Esto se debe plasmar en los estudios previos del proceso contractual, que lo elaborara la oficina de sistemas de Corporinoquia.

Se debe definir un procedimiento donde se indique la realización de pruebas al software desarrollado, los requisitos mínimos que debe cumplir. Se debe tener en cuenta el documento técnico de requisitos elaborado para cada caso de desarrollo de software.

La oficina de sistemas deberá encargarse de la validación de funcionalidad del sistema en cuanto a: validación de entrada de datos y generación de los datos de forma confiable. Los campos de los formularios del sistema de información desarrollado debe facilitar la validación de la información, teniendo en cuenta: tipo de dato del campo, longitud, rangos válidos, lista de caracteres aceptados, caracteres peligrosos, entre otros.

Los sistemas de información desarrollados deben cumplir con los requerimientos del manual 3.1 de Gobierno en Línea de Colombia, en cuanto a seguridad, accesibilidad y navegabilidad. Los formularios deben brindar una guía de ruta de navegación, así como la opción de cierre de sesión de los aplicativos en cada uno de sus secciones.

5.2.15 Políticas de Seguridad en las Relaciones con los Proveedores

5.2.15.1 Seguridad de la Información en relación con los proveedores

La Corporación debe velar por que las empresas contratistas o terceros que tengan relación con la misma, cumplan a cabalidad los requerimientos, normatividad, procesos y procedimientos de seguridad de la información. El área jurídica encargada de la responsabilidad de firma y suscripción de contratos y convenios con terceros, apoyara la

socialización del compromiso de cumplimiento de la normatividad, políticas y procedimientos de seguridad de la información al interior de la corporaciòn.

Se debe generar compromisos de responsabilidad, de confidencialidad y seguridad de la información con terceros en cada uno de los contratos o convenios a suscribir con proveedores y prestadores de servicios.

La oficina de sistemas debe establecer las condiciones necesarias de seguridad para las conexiones de equipos de cómputo y dispositivos móviles de personal contratista a la red de datos Corporativa.

Los supervisores e interventores de contratos o convenios, deberán socializar las políticas y procedimientos de seguridad de la información de la Corporación, a cada uno de los intervinientes en los mismos, deben promover el acceso seguro a la información y a los recursos de almacenamiento, aplicando la política de seguridad de la información en la Corporación.

5.2.16 Políticas de Seguridad en Gestión de los Incidentes de Seguridad de la Información

5.2.16.1 Gestión de Incidentes y mejoras en la Seguridad de la Información

Se debe definir el procedimiento de reportes de incidentes relacionado con la seguridad de los activos de información, sus medios de procesamiento, y toda la plataforma tecnológica, incluyendo sistemas de información las personas. En este procedimiento se deben definir los responsables que intervendrán en el tratamiento de los incidentes.

Los propietarios de los activos de información deben informar a la oficina de control Interno y jefe inmediato del área correspondiente donde se haya identificado o presentado el incidente de seguridad identificado o que se reconozcan la probabilidad de materialización.

La oficina de sistemas deberá reportar al comité de Seguridad de la Información todos los incidentes relacionados con la seguridad de la información para su evaluación y tratamiento, con el fin de mitigar los daños a la información y generar los controles necesarios para su salvaguarda.

Se debe documentar los sucesos relacionados con daños y posibles ataques contra la seguridad de la información y los mecanismos utilizados como medio de protección para cada uno de los eventos registrados.

Los funcionarios de la Corporación, personal contratista y personal previsto por terceras partes (empresas), deberán reportar eventos o incidentes relacionados con los recursos tecnológicos y la seguridad de la información, en la Corporación. La oficina de control interno o la Subdirección Correspondiente son las encargadas de recibir los reportes de eventos mencionados en el presente ítem.

5.2.17 Políticas de Seguridad de La Información para la Gestión de la Continuidad del Negocio

5.2.17.1 Continuidad de la Seguridad de la información

La Corporación garantizará todos los recursos suficientes para proporcionar una respuesta efectiva y dar continuidad a procesos y servicios, en caso de contingencia o catástrofes que se presenten en las instalaciones de Corporinoquia y que afecten la continuidad del negocio. Se debe garantizar la seguridad de la información y el restablecimiento de la misma como apoyo a los procesos misionales de la Corporación.

El Comité de Riesgos y el Comité de Atención y Prevención de emergencias de la Corporación, deben estar alineados para apoyar y salvaguardar la información en caso de contingencias o eventos catastróficos. El Comité de Riesgos y atención de Emergencias en conjunto con la oficina de Sistemas y la Secretaria General de la Corporación, deberán valorar y analizar los impactos causados para el inicio de la recuperación ante desastres y continuidad de las labores misionales y de apoyo de la Corporación.

La oficina de sistemas debe realizar un plan de contingencia y de recuperación ante desastres, para volverá la normalidad la infraestructura tecnológica (red de datos, sistemas de información, centro de cómputo) y cada uno de los sistemas mencionados. Cualquier anormalidad detectada en la recuperación del sistema debe ser informada al comité de Seguridad de la Información y a la Dirección General de la Corporación.

5.2.17.2 Redundancias

La oficina de sistemas en conjunto con el Comité de Seguridad de la Información deberá analizar y establecer requerimientos de redundancia de los diferentes sistemas tecnológicos críticos para la Corporación, especialmente para los sistemas de información de Gestión Documental y Sistema de Información Financiera. Además, será la encargada de implementar y administrar las soluciones de redundancia tecnológica, garantizando su funcionalidad a través de pruebas periódicas, para asegurar el cumplimiento de requisitos y requerimientos de disponibilidad del servicio en la Corporación.

5.2.18 Políticas de Seguridad para el Cumplimiento

5.2.18.1 Cumplimiento de requisitos legales y contractuales

Corporinoquia como entidad Gubernamental, velará por el cumplimiento de la normatividad relacionada con la seguridad de la información, entre ellas, Manual 3.1 de Gobierno en Línea, derechos de autor (Software), por lo cual, forjara sus esfuerzos a cumplir que el software instalado en la plataforma y recursos tecnológicos cumpla con los requerimientos legales y de licenciamiento. A la vez, gestionar el cumplimiento de las normas establecidas por el Ministerio de las Tic, en cuanto a seguridad y protección de la información de las entidades gubernamentales de Colombia.

La oficina de sistemas debe presentar informes periódicos acerca de la legalidad del software instalado en los equipos de cómputo y centros de datos de la corporación. Dichos informes se deben presentar a la oficina de Control Interno de la Corporación.

La oficina de sistemas debe llevar un registro de inventario de software instalado en los equipos de cómputo y los centros de datos en donde especifique la licencia de funcionamiento a nombre de la Corporación. Se debe verificar periódicamente el software instalado en los diferentes equipos, que corresponda al permitido en cada estación y centro de datos autorizado.

Los usuarios de los equipos de cómputo corporativo, deben abstenerse de instalar software o aplicativos en sus equipos de cómputo asignados para el desarrollo de sus actividades. La oficina de sistemas es la encargada de este proceso.

El comité de seguridad de la información de la corporación, propenderá por el cumplimiento de la Ley 1582 de 2012, por medio de la cual se regula la protección de datos personales en Colombia.

Las áreas que procesan datos personales de usuarios internos y externos de la Corporación u otros, deberán cumplir con la política de seguridad de la información, cumplir la normatividad colombiana de seguridad de información e implementar controles necesarios para asegurar el tratamiento de la información sensible de los mismos, garantizando la confidencialidad, integridad y disponibilidad de la información.

La oficina de sistemas de la corporación debe implantar los controles necesarios para proteger la información personal interno y externo e información sensible almacenada en base de datos o cualquier otro repositorio, evitando su divulgación (confidencialidad), alteración (integridad) o eliminación (disponibilidad) sin la autorización respectiva.

Los usuarios de la información corporativa, deberán guardar total discreción y reserva con el uso de la misma; esta debe ser usada para el apoyo a la gestión y desarrollo de procesos misionales corporativos. Es necesario identificar la identidad de las personas o terceros a quienes se les entrega información. Esta entrega debe estar autorizada por un integrante de la alta dirección en cada una de las dependencias de la Corporación.

Los usuarios de los sistemas de información de la Corporación, deberán empoderase de la responsabilidad propia sobre las claves de acceso y autorizaciòn asignadas, para lo cual, deben cambiarla periódicamente para evitar ataques de ingeniería Social. Sus equipos de cómputo deben estar bloqueados en los momentos de inactividad o pausas activas, como mecanismo de seguridad y control.

6 CONCLUSIONES Y TRABAJO FUTURO

6.1 CONCLUSIONES

Corporinoquia cuenta con una serie de activos que requieren con urgencia ser protegidos debido a su alto costo y al servicio que prestan en cuanto al desarrollo de procesos misionales y de apoyo y al impacto que pueden causar al materializarse cualquiera de los riesgos identificados.

En la actualidad, Corporinoquia no cuenta con un documento que permita la seguridad de la información, no existen políticas de seguridad definidas para la protección, cuidado y continuidad del negocio en caso de materializarse una catástrofe que conlleve a la pérdida de la base de gestión como es la información generada a diario por cada una de las áreas involucradas.

El presente modelo de política de gestión de seguridad de la Información para Corporinoquia, que se ha desarrollado, es una herramienta para aplicar interior de la misma, permite identificar los activos más importantes con que se cuenta, las posibles amenazas existentes, el impacto que pueden causar si llegare a suceder y la forma de evitar a través de salvaguardas y controles su materialización, lo cual conlleva a iniciar un estado de gestión de la seguridad, la concientización de proteger y la sensibilización de todos sus funcionarios de empoderarse de la gestión de la seguridad dentro de sus procesos de gestión de la Calidad.

La existencia de una política de gestión de la seguridad de la información en Corporinoquia, acerca la administración Publica Corporativa, al logro de sus objetivos, debido a que fortalece el logro de la misión, brindando acompañamiento y empoderamiento en el manejo y administración de la información, ejerciendo y desarrollando procesos con calidad, con eficacia y efectividad de forma controlada, en cumplimiento del objeto misional ambiental para la región de la Orinoquia Colombiana.

El presente trabajo fortalece los conocimientos de gestión de la Seguridad de la información, permitiendo con la aplicación del mismo, el logro en la elaboración de una política de gestión de seguridad en una entidad pública Colombiana, desarrollando y adquiriendo competencias que fortalecen el conocimiento en la rama de la seguridad de la información como Master de Seguridad Informática de la Universidad Internacional de la Rioja, España.

La etapa de análisis de riesgos permite determinar con mayor objetividad los activos, las vulnerabilidades a que están expuestos y la identificación de salvaguardas eficaces en el proceso de gestión de procesos de una organización.

Corporinoquia requiere con urgencia implantar una política de gestión de la seguridad de la información, no solo por ser una entidad del orden gubernamental, sino porque es mucha la información importante que maneja, así como los activos diversos que se encuentran expuestos a vulnerabilidades que al materializarse causarían daños irreversibles en la gestión y continuidad del negocio, uno de ellos y el más importante, su información.

6.2 TRABAJO FUTURO

Para el futuro cercano se plantean algunas propuestas importantes con posibilidad de mejora continua del proceso, las cuales menciono a continuación:

El modelo de Política de Gestión de la Seguridad de la información puede llegar a presentarse en Corporinoquia para su posterior implementación, el cual estará sujeto a revisión por los organismos competentes de cada una de las áreas de la misma.

Es importante que acompañada de la política de gestión de la seguridad de la información se desarrollen cada uno de los procedimientos establecidos para la administración y gestión de la seguridad, los cuales brindaran un acercamiento detallado para cumplir con cada uno de los ítems de la política de seguridad propuesta.

El modelo de política de gestión de la seguridad para Corporinoquia, brinda unas directrices a implementar como medio de salvaguarda y protección de la información en cuanto a la restricción e implementación de mecanismos y aplicaciones que impidan el acceso de ataques a cada uno de los elementos tecnológicos de la red de datos, para lo cual es importante, retomarla, analizarla y proteger la infraestructura tecnológica de posibles vulnerabilidades que fueron identificadas, sobre todo para los activos que manejan información física y digital.

Con el presente documento de política y análisis de gestión de riesgos identificados en la Corporación, es necesario que Corporinoquia lo retome e inicie las gestiones necesarias para su implementación, con el ánimo de reducir el riesgo en cada uno de sus activos identificados.

El presente modelo de política de gestión de la seguridad de la información permitirá identificar una necesidad de control de amenazas en Corporinoquia, y será la herramienta inicial para la búsqueda de la certificación en gestión de la seguridad de la información a través de la norma ISO 27001:2013

EL desarrollo del presente trabajo brinda las herramientas y abre las puertas para definir la línea de profundización profesional del autor como Master en Seguridad Informática, aplicándolo a la gestión de la Seguridad de la Información, en lo relacionado a la implementación y certificación de organizaciones públicas y privadas, así como el área de auditoria de la seguridad de la información, gestor y analista de riesgos en la organización.

7 REFERENCIAS BIBLIOGRAFICAS

ALCALDIA DE BOGOTA. (16 de 06 de 2015). *ALCALDIA DE BOGOTA*. Obtenido de ALCALDIA DE BOGOTA: http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=38498

ARCHIVO GENERAL DE LA NACION. (10 de 06 de 2015). *ARCHIVO GENERAL DE LA NACION*. Obtenido de http://www.archivogeneral.gov.co/sites/all/themes/nevia/PDF/Transparencia/LEY_594_DE_2000.pdf

ARCHIVO GENERAL DE LA NACION_AGN. (10 de 06 de 2015). *ARCHIVO GENERAL DE LA NACION*. Obtenido de http://www.archivogeneral.gov.co/sites/all/themes/nevia/PDF/Transparencia/ACUERDO_05_DE_2013.pdf

ARCHIVO GENERAL DE LA NACIÒN-L527. (14 de 06 de 2015). *ARCHIVO GENERAL DE LA NACIÒN-L527*. Obtenido de ARCHIVO GENERAL DE LA NACIÒN-L527: http://www.archivogeneral.gov.co/sites/all/themes/nevia/PDF/Transparencia/LEY_527_DE_1999.pdf

AUDITORIADESISTEMASADRIMELI. (15 de 06 de 2015). *AUDITORIADESISTEMASADRIMELI*. Obtenido de AUDITORIADESISTEMASADRIMELI: http://auditoriadesistemasadrimeli.blogspot.mx/

BIBLIOTECA DIGITAL ICESI. (10 de 06 de 2015). *BIBLIOTECA DIGITAL ICESI*. Obtenido de BIBLIOTECA DIGITAL ICESI: http://bibliotecadigital.icesi.edu.co/biblioteca_digital/

CMMIINSTITUTE. (13 de 06 de 2015). *CMMIINSTITUTE*. Obtenido de CMMIINSTITUTE: http://cmmiinstitute.com/get-started

CONTRATOS.GOV.CO. (16 de 06 de 2015). *CONTRATOS.GOV.CO*. Obtenido de CONTRATOS.GOV.CO: https://www.contratos.gov.co/consultas/detalleProceso.do?numConstancia=14-9-391615

CORPORINOQUIA. (25 de 05 de 2015). *CORPORINOQUIA*. Obtenido de http://l.corporinoquia.gov.co/index.php/inicio/corporinoquia

DAMETAREAS. (10 de 06 de 2015). *DAMETAREAS*. Obtenido de DAMETAREAS: www.dametareas.com

DNP. (20 de 06 de 2015). *DNP*. Obtenido de www.dnp.gov.co

ELKIN COELLO_ BLOG. (05 de 06 de 2015). *ELKIN COELLO_ BLOG*. Obtenido de helkyncoello.wordpress.com

GOBIERNO EN LINEA. (16 de 06 de 2015). *GOBIERNO EN LINEA*. Obtenido de GOBIERNO EN LINEA: http://programa.gobiernoenlinea.gov.co/apc-aa-files/eb0df10529195223c011ca6762bfe39e/manual-3.1.pdf

ISO 27000.es. (25 de 05 de 2015). *ISO 27000*. Obtenido de http://www.iso27000.es/iso27000.html

ISO27002. (14 de 06 de 2015). *ISO27002*. Obtenido de ISO27002: http://www.iso27002.es/

ISO9000CONSULTORES. (15 de 06 de 2015). *ISO9000CONSULTORES*. Obtenido de iso9000consultores.blogspot.com

MINTIC. (15 de 06 de 2015). *MINTIC*. Obtenido de MINTIC: http://www.mintic.gov.co/portal/604/w3-propertyvalue-540.html

MINTIC_CONPES. (14 de 06 de 2015). *MINTIC_CONPES*. Obtenido de MINTIC_CONPES: http://www.mintic.gov.co/portal/604/articles-3510_documento.pdf

MINTIC-L1273. (15 de 06 de 2015). *MINTIC-L1273*. Obtenido de MINTIC-L1273: http://www.mintic.gov.co/portal/604/articles-3705_documento.pdf

MINTIC-L1341. (15 de 06 de 2015). *MINTIC-L1341*. Obtenido de MINTIC-L1341: http://www.mintic.gov.co/portal/604/articles-3707_documento.pdf

MONOGRAFIAS_COBIT. (13 de 06 de 2015). *MONOGRAFIAS*. Obtenido de MONOGRAFIAS: http://www.monografias.com/trabajos93/cobit-objetivo-contro-tecnologia-informacion-y-relacionadas/cobit-objetivo-contro-tecnologia-informacion-y-relacionadas.shtml#ixzz3lNXG5xTZ

PMG-SSI_27003. (14 de 06 de 2015). *PMG-SSI_27003*. Obtenido de PMG-SSI_27003: http://www.pmg-ssi.com/2014/01/isoiec-27003-guia-para-la-implementacion-de-un-sistema-de-gestion-de-seguridad-de-la-informacion

PMG-SSI-ISO_27004. (14 de 06 de 2015). *PMG-SSI-ISO_27004*. Obtenido de PMG-SSI-ISO_27004: http://www.pmg-ssi.com/2014/01/isoiec-27004-medicion-de-la-seguridad-de-la-informacion/

PMG-SSI-ISO_27005. (14 de 06 de 2015). *PMG-SSI-ISO_27005*. Obtenido de PMG-SSI-ISO_27005: http://www.pmg-ssi.com/2014/01/isoiec-27005-gestion-de-riesgos-de-la-seguridad-la-informacion/

SECRETARIA SENADO. (15 de 06 de 2015). *SECRETARIA SENADO*. Obtenido de SECRETARIA SENADO: http://www.secretariasenado.gov.co/senado/basedoc/ley_0599_2000.html

SECRETARIA SENADO-L1150. (15 de 06 de 2015). *SECRETARIA SENADO-L1150*. Obtenido de SECRETARIA SENADO-L1150: http://www.secretariasenado.gov.co/senado/basedoc/ley_1150_2007.html

SECRETARIA SENADO-L594. (15 de 06 de 2015). *SECRETARIA SENADO-L594*. Obtenido de SECRETARIA SENADO-L594: http://www.secretariasenado.gov.co/senado/basedoc/ley_1150_2007.html

SECRETARIA SENADO-L962. (15 de 06 de 2015). *SECRETARIA SENADO-L962*. Obtenido de SECRETARIA SENADO-L962: http://www.secretariasenado.gov.co/senado/basedoc/ley_0962_2005.html

SEGURIDADINFORMACIONCOLOMBIA. (13 de 06 de 2015). *SEGURIDADINFORMACIONCOLOMBIA*. Obtenido de http://seguridadinformacioncolombia.blogspot.com.co/2010/07/que-es-cobit.html

SLIDESHARE. (12 de 06 de 2015). *SLIDESHARE*. Obtenido de http://es.slideshare.net/vaceituno/analisis-de-riesgos-con-oism3-ra

TARINGA. (16 de 06 de 2015). *TARINGA*. Obtenido de TARINGA: www.taringa.net

TECNOVA-CMMI. (13 de 06 de 2015). *TECNOVA*. Obtenido de TECNOVA: http://www2.tecnova.cl/servicios/descripcion_cmmi.html

WIKIPEDIA. (25 de 05 de 2015). *WIKIPEDIA*. Obtenido de https://es.wikipedia.org/wiki/ISO/IEC_27000-series

WIKIPEDIA. (10 de 06 de 2015). *WIKIPEDIA_27001*. Obtenido de https://es.wikipedia.org/wiki/ISO/IEC_27001

WIKIPEDIA. (25 de 06 de 2015). *WIKIPEDIA_SEG INF*. Obtenido de https://es.wikipedia.org/wiki/Seguridad_de_la_informaci%C3%B3n

WIKIPEDIA_COBIT. (13 de 06 de 2015). *WIKIPEDIA_COBIT*. Obtenido de WIKIPEDIA_COBIT: https://es.wikipedia.org/wiki/Objetivos_de_control_para_la_informaci%C3%B3n_y_tecnolog%C3%ADas_relacionadas

WIKIPEDIA_ISC2. (11 de 06 de 2015). Obtenido de https://es.wikipedia.org/wiki/ISC2