MODELO PARA LA GESTIÓN DEL RIESGOS EN TI COMO APOYO A LAS ENTIDADES PÚBLICAS DEDICADAS A PROMOVER LA CIENCIA, CULTURA, TECNOLOGÍA E INNOVACIÓN TECNOLÓGICA DE LA CIUDAD DE CALI

ANTHONY CASTILLO TRIVIÑO.

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA - ECBTI
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
SANTIAGO DE CALI
2022

MODELO PARA LA GESTIÓN DEL RIESGOS EN TI COMO APOYO A LAS ENTIDADES PÚBLICAS DEDICADAS A PROMOVER LA CIENCIA, CULTURA, TECNOLOGÍA E INNOVACIÓN TECNOLÓGICA DE LA CIUDAD DE CALI

ANTHONY CASTILLO TRIVIÑO

Proyecto de Grado – Aplicado presentado para optar por el título de ESPECIALISTA EN SEGURIDAD INFORMÁTICA

Directora de trabajo de grado
Yenny Stella Núñez Alvarez

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA - ECBTI
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
SANTIAGO DE CALI
2022

NOTA DE ACEPTACIÓN

Firma del presidente de jurado

Firma del jurado

Firma del jurado

Ciudad, Fecha sustentación

DEDICATORIA

Como amplio amor dedico este trabajo a mi madre quien me ayudo desde sus posibilidades a salir adelante, quien hizo las veces de padre y madre, que desde su profesión me ayudo en los momentos en los que ya no sabía que pensar porque no entendía o que camino coger cuando ya no sabía qué hacer, desde su entendimiento me dio una Luz de conocimiento iluminando mi camino, gracias madre.

AGRADECIMIENTOS

Agradecimientos a la directora del curso PROYECTOS por disponer de su tiempo y de su conocimiento para ayudarme desde su experticia con vocación y solidaridad en el desarrollo de este proyecto; en segunda instancia a mi madre por brindarme su apoyo desde su profesión, su conocimiento en momentos que no sabía qué camino seguir.

CONTENIDO

LISTA DE TABLAS

pág.

LISTA DE FIGURAS

LISTA DE CUADROS

pág.

LISTA DE ANEXOS

GLOSARIO

Activo de Información: En el contexto que se establece en la ISO/IEC 27001, es un bien o de un servicio

Activo: Es un bien que le pertenece a la entidad, o persona y que hace parte de su patrimonio por tanto posee un valor que puede expresarse en forma de dinero.

Aire Acondicionado de precisión: es un equipo especializado en el acondicionamiento de ambiente para el control térmico y de húmeda utilizado en algunos laboratorios, centros de datos y algunas salas de cómputo.

Amenaza: Es cualquier tipo de incidencia que ocurren o que puede ocurrir afectando en forma negativa los activos de las entidades.

Análisis de Riesgos: Corresponde a un proceso sistemático y ordenado en la que se logra caracterizar los activos de la entidad, identificando las necesidades de seguridad en la entidad a partir de las vulnerabilidades.

Ataque Informático: Es una acción con la intencionalidad de acceder a los equipos de información de la entidad, mediante el uso de prácticas maliciosas con el objetivo de robar, alterar, sustraer o publicar información crítica de la entidad.

Aceptación del Riesgo: Decisión informada, documentada y aprobada por la alta gerencia para afrontar cierto nivel de riesgo o un riesgo.

Autenticación: Son los pasos a seguir que un usuario debe realizar para lograr obtener el acceso a los recursos y servicios que ofrece los sistemas de información de propiedad de la entidad, para el uso de sus funcionarios[1].

Causa: El motivo o razón por el cual se debe actuar de una manera u otra.

Cibercrimen: Es toda actividad ilegal (Delictiva) que se practica en el entorno digital bien sea en internet o una red local.

Ciberseguridad: Define el conjunto de acciones y procedimientos que son utilizados con el objetivo de proteger los datos que se procesan en los dispositivos móviles, en las estaciones de trabajo o dispositivo de cómputo (PC), y de los sistemas de información presentes en la red de datos.

[1]MAGERIT, 2018. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información (p, 101)

Controles: Son todos los mecanismos necesarios para evaluar y gestionar las actividades que interactúan con los activos de información, para mejorar la seguridad en la entidad

Declaración de aplicabilidad: a partir del análisis de riesgo se establece un conjunto de controles que se pueden identificar como salvaguardas, además de indicar si es aplicable o no, para el sistema de información.

Incidente de seguridad: Evento fortuito de cualquier tipo que presentar alteración o daños en el sistema de información.

Integridad: Características del activo que garanticen que no ha sido alterado sin autorización previa.

Política de seguridad: Es un conjunto de normas formalmente constituidas a partir de la actividad de análisis y gestión del riesgo, con la finalidad de preservar un grado de seguridad o inseguridad formalmente aceptado por la entidad.

Probabilidad: es el nivel de certidumbre de que un evento se materialice.

Riesgo: Manifiesta el nivel de exposición que existe, en el que una incidencia sea negativa, siendo así una amenaza pudiendo afectar cualquiera de los activos de propiedad de la entidad.

Riesgo residual: corresponde a todo residuo que queda en el sistema de información después de haber tratado el o los riesgos con los controles o salvaguardas.

Salvaguarda: controles o mecanismos técnicos o tecnológicos que trabaja en eliminar o de mitigar el riesgo.

Seguridad: Es la capacidad que tienen los sistemas de información para contrarrestar o controlar cada una de las acciones ilícitas, maliciosas o accidentales que afectan los activos de Información con relación a los pilares de la seguridad.

Seguridad de la Información: Es tener la tranquilidad y confiar que el sistema de información está exento de cualquier tipo de peligro o presencia de algún tipo de daño inaceptable[2].

[2] Ibidem.

RESUMEN

Este proyecto busca diseñar un Modelo para la gestión del riesgos en ti como apoyo a las entidades públicas dedicadas a promover la ciencia, cultura, tecnología e innovación tecnológica de la ciudad de Cali, y así plantear una adecuada asesoría a las entidades públicas en términos que se relacionan con la gestión del riesgo de la información , reconociendo la necesidad en adoptar una adecuada dirección y control en la entidad, que le brinde la facultad de poder dar cumplimiento a su objeto social y el alcance de sus objetivos en beneficio de la comunidad caleña, lo que a su vez permite agilizar el cumplimiento de las metas trazadas para cada vigencia en el plan de acción anual. Plan que se propone por cada uno de los procesos administrativos (apoyo) y misionales (trabajan en relación al objeto social de la entidad), En consecuencia, se hace necesario interiorizar el conocimiento para formalizar los requisitos y procesos idóneos para garantizar una adecuada Gestión del Riesgo en infraestructura tecnológica de la información, bajo un enfoque de aplicabilidad, directamente relacionado con la capacidad técnica operativa y financiera de cada entidad pública.

Por todo lo anterior, es importante un adecuado modelo de gestión del riesgo, que sea sistemático produciendo resultados claros y puntuales en búsqueda de tener un equilibrio entre el alto nivel de complejidad y la facilidad de su correcta interpretación por la capacidad de generar informes pormenorizados y ejecutivos, que ayuden en la elaboración de planes estratégicos de la entidad. Garantizando una adecuada alineación de las tecnologías de la información, en apoyo del cumplimiento del objeto social de la entidad pública.

ABSTRACT

This project seeks to design a Model for risk management in you as support for public entities dedicated to promoting science, culture, technology and technological innovation in the city of Cali, and thus propose adequate advice to public entities in terms that are related to information risk management, recognizing the need to adopt adequate direction and control in the entity, which gives it the power to comply with its corporate purpose and the scope of its objectives for the benefit of the community of Cali , which in turn allows speeding up the fulfillment of the goals set for each term in the annual action plan. Plan that is proposed for each of the administrative (support) and mission processes (they work in relation to the corporate purpose of the entity), Consequently, it is necessary to internalize the knowledge to formalize the requirements and suitable processes to guarantee an adequate Management of the Risk in information technology infrastructure, under an applicability approach, directly related to the technical, operational and financial capacity of each public entity.

For all of the above, an adequate risk management model is important, one that is systematic, producing clear and punctual results in search of having a balance between the high level of complexity and the ease of its correct interpretation due to the ability to generate detailed reports and executives, who help in the development of strategic plans of the entity. Guaranteeing an adequate alignment of information technologies, in support of compliance with the corporate purpose of the public entity.

INTRODUCCIÓN

El departamento sistemas que para algunas entidades se reconoce como proceso de sistemas o telemática dado que trabaja con Tecnologías de la información, hoy en día es transversal a los distintos departamentos o procesos de una empresa legalmente constituida, provee los servicios que soportan el normal ejercicio de las operaciones, en cumplimiento de su misión, visión y su objeto social.

Las tecnologías de la información evolución a diario, propiciando la necesidad de agilizar procesos de evaluación es necesario tener una guía muy concreta que permita una adecuada Gestión del Riesgo para las infraestructuras en los Sistemas de Información de las entidades, facilitando el trabajo en forma adecuada en la gestión y análisis de riesgos informáticos, contribuyendo en la documentación de aplicabilidad en las entidades a partir de estándares internacionales como la ISO 27001 mediante la metodología MAGERIT; busca lograr un análisis pormenorizado de los riesgos del área informática dentro de la entidad, contemplando la ubicación jerarquizara en la que se encuentra el área de TI en el organigrama de la entidad, lo que puede determinar o reflejar su nivel de importancia dentro de la organización , de igual forma identificar la planta de cargos del área de informática, de la misma forma generar un inventario de activos informáticos categorizados, lo que incluye el alcance, los organigramas, la definición de activos, amenazas, vulnerabilidades, evaluación del proceso de control interno, evaluación de amenazas, con el objetivo de poder determinar los niveles de riesgos que presenta el área de informática y pudiese llevar a afectar el normal desempeño de las actividades cotidianas de los funcionarios dentro de la entidad.

Lo anterior, permite a las entidades aprender de sus errores en relación a la adecuada Gestión de Seguridad Informática presente en la infraestructura tecnológica de sistemas de información. Por ende, ayuda a fortalecer sus esquemas de seguridad dando origen a un plan estratégico de seguridad informática que apoye el plan estratégico en las tecnologías de información, no para contar con nivel de seguridad inquebrantable, dado que ningún sistema se puede garantizar como 100% seguro, sino para mitigar las vulnerabilidades hasta lograr un nivel de riesgos asumible por la compañía previo apoyo de la alta gerencia.

1. DEFINICIÓN DEL PROBLEMA

1.1. Presentación

Diagnóstico Inicial

En la Ciudad de Cali existen entidades dedicadas en ofrecer servicios como:

Promover la ciencia, cultura, tecnología e innovación tecnológica.

Para el normal desarrollo de sus procesos administrativos y misionales, se realiza diferentes actividades educativas para fortalecer los eventos culturales, con el fin de dar cumplimiento a lo establecido en su objeto social, en este sentido la tecnología de sistemas de cómputo se convierte en un pilar muy importante de apoyo respondiendo de manera oportuna a los requerimientos de la comunidad; de la misma forma atender las responsabilidades legales y financieras.

Por lo general, este tipo de entidades ante el público típicamente está dividido en dos sub grupos como lo son los grupos misionales que pertenecen a **Dirección Técnica**, los grupos de apoyo que dependen de **Dirección administrativa y financiera**, por otra parte, se encuentra Jurídica, Control interno, planeación, mercado y comunicaciones, Gerencia general (Representante legal).

Los grupos de trabajo como los misional típicamente depende del objeto social de la entidad, los grupos de apoyo, como su nombre lo dice son grupos que apoyan las actividades misionales, dentro de este grupo se encuentra Telemática o sistemas, contabilidad, tesorería, almacén, recurso físico, entre otros. Lo anterior, debido a que el grupo de telemática o sistemas por lo general pertenece al grupo de apoyo y es transversal a todos los departamentos su análisis de gestión del riesgo es susceptible a mejorar. Existen para el área de TI un catálogo de servicios como, por ejemplo:

- Soporte a incidencias de estaciones de trabajo y servidores de propiedad de la entidad.
- Soporte impresoras.
- Gestión de servidor de directorio activo.
- Gestión de servidor de bases de datos.

- Gestión de servidor de aplicaciones.
- Soporte a infraestructura de red de datos (LOCAL y WI-FI).
- Gestión de contratación servicios de correo y servicios de alojamiento web son tercerizados.
- Gestión de contratación de herramientas de hardware y software tercerizados.
- Conexión libre a usuario externo, préstamo de estaciones de trabajo con acceso controlado a internet (Opcional).
- Conexión wi-fi libre a usuario externo con acceso controlado a internet, (Opcional).

Una característica típica entre este tipo de entidades al brindar servicios de conexión WIFI, es que realizan control por categorías, entre las cuales esta negar el acceso a sitios con contenido solo para adultos, hacking, descargas p2p, drogas, alcohol, entre otros. Algunas entidades dedicadas a promover la ciencia, cultura, tecnología e innovación tecnológica para obtener ingresos de terceros es posible que en la edificación se preste el servicio de alquiler de auditorios para eventos, o convenios para facilitar oficinas a entidades externas, estas últimas algunas veces puede o no tener su propia infraestructura de datos por lo cual es muy probable que no se tenga en cuenta en el momento de evaluar un riesgo a nivel de TI.

De esta manera, el área de TI al final de todas las operaciones y servicios, termina siendo un pilar muy importante para el normal ejercicio del objeto social de la entidad, sin embargo su análisis de riesgos se realiza típicamente para el área de Tecnologías de la Información, bajo un modelo general estándar propio de cada entidad, posiblemente sea idóneo para los grupos misionales y para alguna parte de los grupos de apoyo, lo anterior implica que la gestión del riesgo para el área de TI es susceptible a mejoras, porque sus riesgos son especializados y no deberían de ser evaluados con características generales, pudiendo tener características de reconocimiento más amplias lo que incluye la identificación de la planta de cargos del área de informática, de la misma forma generar o evaluar un inventario de activos informáticos en forma organizada y categorizada, lo que incluye el alcance, los organigramas, la definición de activos, evaluación de amenazas, vulnerabilidades, evaluación del sistema de control interno, con la finalidad de poder determinar los niveles de riesgos a los que está expuesto el área de informática específicamente lo relacionado con la infraestructura de la entidad, el no abordar de forma organizada los riesgos, es posible que como efecto para la entidad, no se reconozca el impacto negativo de algunas incidencias, es decir es posible que existan riesgos desconocidos que pudiese llevar a afectar el normal desempeño de las actividades cotidianas de los funcionarios dentro de la entidad; es consecuencia, es necesario un modelo específico para evaluar la infraestructura

tecnológica que esté acorde a la naturaleza de su catálogo de servicios en TI, es decir la metodología de gestión del riesgo para la infraestructura tecnológica es susceptible a mejoras.

1.2. Formulación del problema

¿Cómo un modelo para la gestión de riesgos puede servir para definir las mejores prácticas de gestión de tecnología informática y de gobierno, para mejorar la seguridad de la información en las entidades públicas dedicadas a promover la ciencia, cultura, tecnología e innovación tecnológica de la ciudad de Cali?

2. JUSTIFICACIÓN

En apoyo de las tecnologías informáticas las entidades públicas dedicadas a promover la ciencia, cultura, tecnología e innovación tecnológica de la ciudad de Cali, bajo una adecuada dirección y control en la entidad, les permite el cumplimiento de su objeto social en beneficio para la comunidad caleña, agilizando el alcance y cumplimiento de las metas propuestas durante cada vigencia en el plan de acción anual. Plan que se propone por cada uno de los procesos administrativos y misionales, dando origen a diferentes actividades educativas, culturales, tecnologías, innovación y en algunos casos hasta de carácter patrimonial, por lo anterior es importante un adecuado modelo de gestión del riesgo, que garantice una adecuada alineación de las tecnologías de la información, en apoyo del cumplimiento del objeto social de la entidad.

Por otra parte, con el pasar de los tiempos y las exponencial evolución de las tecnologías de la información se presentan nuevos retos en seguridad, retos que se deben de enfrentar, con la meta de brindar a la entidad niveles de seguridad asumibles, partiendo de la premisa que ningún sistemas es 100% seguro, pero si debe de tomar decisión dentro del plan de tratamiento, creando unos controles que se rijan a partir de la norma ISO 27001 , estableciendo procesos , actividades y/o medidas para evitar que algún riesgo se materialice, contemplando la posibilidad de aceptar , mitigar, eliminar o transferir la responsabilidad de su abordaje, a partir del cambio de conciencia de la existencia de amenazas, vulnerabilidades y riesgos que puedan afectar el normal ejercicio de las actividades cotidianas dentro de las funciones en la entidad, por lo cual es necesario establecer una metodología adecuada para analizar e identificar los riesgos latentes en infraestructura de redes de comunicación.

3. OBJETIVOS

3.1. Objetivo general

Diseñar un modelo para la gestión de los riesgos en Ti como apoyo a las entidades públicas dedicadas a promover la ciencia, cultura, tecnología e innovación tecnológica de la ciudad de Cali.

3.2. Objetivos específicos

Analizar el estado actual en las entidades públicas dedicadas a promover la ciencia, cultura, tecnología e innovación tecnológica de la ciudad de Cali en referencia a las tecnologías de la información y de la comunicación bajo el enfoque de la gestión del riesgo.

Evaluar el impacto de los riesgos latentes por el uso de las tecnologías de la información que pueden afectar la operación y cumplimiento misional de las entidades.

Establecer una metodología para el análisis de riesgos que contribuya a la aplicación de medidas de prevención para evitar peligros potenciales o reducir su impacto en la infraestructura TI de las entidades.

Proponer un modelo de gestión de riesgos TI como aporte de seguridad de la información para las entidades públicas dedicadas a promover la ciencia, tecnología e innovación tecnológica de la ciudad de Cali.

4. MARCO REFERENCIAL

4.1. Marco teórico

- Fortalecimiento en la Gestión de Tecnologías de la Información.

Se ha evidenciado una evolución constante de las tecnologías en todo el mundo , alcanzando tanto entidades privadas como públicas, principal en lo relacionado con las comunicaciones propiciando que las infraestructuras de redes de comunicación sean más robustas , escalables procurando proyectar su ciclo de vida a nivel tecnológico sea lo más extenso posible en el tiempo, todo lo anterior acorde a el alto flujo de procesamiento y transmisión de datos, y de la misma forma el volumen de almacenamiento que se evidencia en la actualidad propiciando que las entidades evolucionen muy rápido casi de forma exponencial con un alto nivel competitivo en todos los ámbitos y se encuentran caracterizados por distintos factores como lo son:

- Globalización de los negocios.
- Innovación.
- Aumento en el uso de tecnologías.
- Restructuración Organizativa.
- Reinvención de los procesos.

Estos factores generan incertidumbre lo que propicia adquirir un nivel de riesgo. En consecuencia, a lo anterior se promueven la adopción de modelos de gestión del riesgo, pretendiendo minimizar los riesgos adquiridos por la entidad, convirtiendo los riesgos en fortalezas fomentando la elaboración de oportunidades en producción y de gestión a partir de su diseño, garantizando condiciones aceptables de seguridad para el futuro.

- Como proceso

La gestión de riesgos no debe de ser considerada en la entidad como un proceso o practica aislada del negocio, debe de ser considerada como un componente trasversal, íntegro del desarrollo funcional global y multidisciplinario que aplique en todos los ámbitos de acción de la compañía, sea el ámbito, social, cultura, sectorial, entre otras, en las cuales pueda incidir su campo de acción.

- **Dualismo de la Seguridad Informática**

Esta tesis trata a grandes rasgos sobre la capacidad de anticiparse a los posibles riesgos, llevando cada uno de los servicios y subservicios al límite previa declaración expresa para ejecutarlo en el sistema real, o en un ambiente controlado simulando todo el sistema de información, su primicia es hallar los riesgos y fallas en los procesos antes que sucedan, en principio cultiva la experticia de los administradores para estar preparados ante cualquier tipo de incidencia que pueda afectar en forma negativa el normal desarrollo de todas las actividades productivas dentro de la entidad.

El pensamiento dual de la seguridad de la información; se basa en la primicia que todo sistema es inseguro, por tanto se basa en términos como la inseguridad de la información y su explotación haciendo uso de técnicas hacking ético y análisis de riesgos, permitiendo a la entidad retroalimentarse del hallazgo en sus fallas de seguridad y fortalecer su esquema de seguridad antes que sean explotadas por un atacante, o por configuraciones, o procesos propios de los sistemas de información que puedan colapsar los sistemas.

El pensamiento Dual es participe de un estándar no formal que propicia de forma más proactiva el fortalecimiento de los esquemas de seguridad ante riesgos latentes, cierre de brechas de eventos inesperados, y así crear estrategias que permitan salir avante ante cualquier eventualidad.

En Colombia adopta los estándares formalizados facilitado una serie de guías que merecen estudio, sirven como base para el Fortalecimiento en la Gestión de Tecnologías de la Información lo que incluye seguridad física y seguridad en la nube, guías que están basadas en estándares internacionales reconocidos como la ISO/IEC 27001 – Anexo de La ISO/IEC 27001 - ISO/IEC 31000 y el modelo de gestión del riesgo como lo es MAGERIT, lo que evidencia una clara importancia del reconocimiento de los riesgos y vulnerabilidades, con el fin de tener un cambio de estado de conciencia en cuanto seguridad de tecnologías de la información, en consecuencia sirve para el desarrollo de planes de gestión del riesgo, en búsqueda de establecer las acciones necesarias para mitigar las amenazas.

En Colombia “Estado se busca contribuir al incremento de la transparencia en la Gestión Pública, promoviendo el uso de las mejores prácticas de Seguridad de la Información como base de la aplicación del concepto de Seguridad Digital.”[3]

[3] Modelo de seguridad—fortalecimiento TI, 2020. [En Línea]. Disponible en: https://www.mintic.gov.co/gestion-ti/seguridad-ti/modelo-de-seguridad/

Por tanto, se implementar principios metodológicos puntuales y claros para su cumplimiento, de la misma forma deben de ser capaces de evolucionar en el tiempo permitiendo describir lo siguiente.

1 las vulnerabilidades que posiblemente pudiesen producir algún efecto negativo en la seguridad de los activos de información deben de ser reconocidas y cuantificadas.

2 las amenazas que pueden afectar la seguridad de los activos de información deben de ser reconocidas y cuantificadas.

3 a partir del reconocimiento de vulnerabilidades y amenazas se deben de establecer los controles necesarios logrando mitigar el impacto negativo sobre los distintos activos de información, hasta lograr un nivel de riesgo aceptable y aprobado por la alta gerencia.

4.2. Marco conceptual

Riesgo

Manifiesta el nivel de exposición que existe, para que una amenaza se materialice afectando uno o más activos, perjudicando a la entidad, existe la probabilidad de que estas amenazas pueden ser riesgos latentes que pueden ser potencialmente peligrosos para la entidad “Posibilidad de que se produzca un impacto determinado en un activo, en un dominio o en toda la Organización”.[4]

Modelo para la gestión del riesgo

Establece una serie de actividades coordinadas con procesos establecidos dentro de un marco de trabajo para la seguridad de la entidad, a partir de lo cual se identifican y tratan con prioridad los riesgos críticos, y trabajar de forma progresiva los de menor criticidad, ayudando a obtener un nivel aceptable del riesgo que no perjudique el normal desarrollo de sus actividades en cumplimiento del objeto sociales como resultado de

[4] Magerit, 2012. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Ministerio de Hacienda y Administraciones Públicas. [En Línea]. 127 p. Disponible en: https://administracionelectronica.gob.es/pae_Home/dam/jcr:fb373672-f804-4d05-8567-2d44b3020387/2012_Magerit_v3_libro1_metodo_es_NIPO_630-12-171-8.pdf

una adecuada selección de salvaguardas o controles de seguridad , “ seguridad adecuadas para conocer, prevenir, impedir, reducir o controlar los riesgos identificados y así reducir al mínimo su potencialidad o sus posibles perjuicios. La gestión de riesgos se basa en los resultados obtenidos en el análisis de los riesgos”.[5]

Entidad: Conjunto de personas con distintas habilidades, que se encuentran en función de una actividad laboral en cumplimiento del objeto social de la compañía.

Entidades públicas cultura: pueden ser de tipo descentralizadas que están constituidas por su propia personería jurídica lo que les brinda la potestad de ejercer derechos y de contraer obligaciones, lo anterior implica que está en la capacidad de tener su propio patrimonio y tener su autonomía financiera previa aprobación de recursos por el ente territorial. Estas entidades son creadas al igual que su planta de cargos por ley o en algunos casos por aprobación de asamblea o concejo, para este caso las entidades que promueven la ciencia, cultura, o entidades similares se encuentran adscriptas a la secretaria de cultura o de quien se encuentre encargado en cumplir sus funciones.

El enfoque que se va plantear para este trabajo está en el desarrollo de un modelo de gestión del riesgo que se acople a las Entidades públicas, que dentro de su objeto social trabajen para promover aspectos como puede ser la ciencia, Cultura, Tecnología e Innovación tecnológica propiciando una herramienta que colaboren a crear o identificar salvaguardas para el sistema de información ayudando a mitigar uno o más riesgos.[6]

[5] Ibidem, p.128.

[6] Documento de clasificación de entidades del sector público colombiano Versión 2. 2018. [En Línea]. 84 p. Disponible en: http://www.urf.gov.co/webcenter/ShowProperty?nodeId=/ConexionContent/WCC_CLUSTER-070104

4.3. Marco histórico o antecedentes

Se establece un referente en donde se evidencia las etapas por las que tiene que avanzar el objeto de estudio de principio a fin, para someterlo a investigación.

- Diseño de un plan de gestión de riesgos y vulnerabilidades del caso de estudio de la empresa qwerty s.a., basados en los estándar ntc-iso/iec 27001 y ntc-iso/iec 27032

  Autores: Jorge Emilio Saavedra Agudelo

  Año de Publicación: 2020.

Descripción: En este documento se plantea el uso sistemático técnico y metodológico para la implementación de un sistema de gestión y de seguridad de la información (SGSI) en el cual se utiliza como referencia las normas ISO/IEC 27001 e ISO/IEC 27032 bajo el ciclo PHVA.[7]

- Diseño de un plan de gestión de riesgos de la información en el instituto nacional de estudios sociales, INES de Colombia

  Autores: Carlos Barreto, Jaime Rodríguez.

  Año de Publicación: 2018.

Descripción: En este documento se plantea dar a conocer el estado actual de la entidad El Instituto Nacional de Estudios Sociales INES de Colombia en relación a la seguridad de la información, a partir de lo cual se definen objetivos dirigidos al desarrollo de proyectos, bajo una contextualización para el desarrollo de análisis y gestión de riesgo, a partir de lo cual se trabaja con la metodología MAGERIT.[8]

[7] Agudelo, 2020. Diseño de un plan de gestión de riesgos y vulnerabilidades del caso de estudio de la empresa QWERTY S.A., basados en los estándar NTC-ISO/IEC 27001 y NTC-ISO/IEC 27032. UNAD Tunja. [En Línea]. 156 p. Disponible en: http://repository.unad.edu.co/handle/10596/36866

[8] Barreto y Rodríguez, 2018. Diseño de un plan de gestión de riesgos de la información en el instituto nacional de estudios sociales, Inés de Colombia. [En Línea]. 217 p. Disponible en: http://repository.unipiloto.edu.co/bitstream/handle/20.500.12277/6149/00005166%20-%20ANEXO%201.pdf?sequence=2&isAllowed=y

- Diseño del sistema de gestión de seguridad de la información para una agencia de viajes y turismo

  Autores: Mónica Buesaquillo Osorio, Darwin Nicolás López herrera, Andrés Felipe García Henao

  Año de Publicación: 2017.

Descripción: En este documento se plantea a la par del proceso de innovación tecnológica que presenta la agencia de viajes, realizar un análisis de seguridad de la infraestructura de la información a partir de esto evaluar el nivel del riego bajo las nuevas tendencias tecnológicas y cibercrimen que está presente en el mundo virtual, se logra evidenciar la existencia de vulnerabilidades internas y externas que afectan el normal funcionamiento de la empresa a partir de lo cual, parte la necesidad de establecer un SGSI mediante métricas que ayuden a proteger la información.
En relación a lo anterior se define el cumplimiento de la normativa ISO 27001.[9]

- Análisis y plan de tratamiento de riesgos para los activos de información del cuerpo de bomberos voluntarios de Tunja

  Autores: Samanta Lorena Sierra Mafla, Arley Felipe Gambasica Esquivel

  Año de Publicación: 2019.

Descripción: En este documento se plantea el Análisis y plan de tratamiento de riesgos para los activos de información del cuerpo de bomberos voluntarios de Tunja, por el medio de mecanismos de análisis del riesgo la mejora y el mantenimiento de la protección de la información con el objetivo de garantizar la prosperidad del negocio con apoyo del estándar internacional ISO/IEC 27001, en donde se enmarcan criterios y procedimientos, partiendo de lo cual se logra trabajar con la METODOLOGÍA MAGERIT.[10]

[9] Osorio, Mónica; Herrera, Darwin., y Henao, Andrés. Diseño del sistema de gestión de seguridad de la información para una agencia de viajes y turismo. Bogotá 2017. [En Línea]. 34 p. Disponible en: https://alejandria.poligran.edu.co/bitstream/handle/10823/999/EntregaFinal.pdf?sequence=1

[10] Mafla, Samanta., y Esquivel, Arley. Análisis y plan de tratamiento de riesgos para los activos de la información del cuerpo de bomberos voluntarios de tunja. Tunja 2019. [En Línea]. 208 p. Disponible en: https://repository.usta.edu.co/bitstream/handle/11634/21200/2019Samanthasierra?sequence=1&isAllowed=y

4.4. Marco legal

ISO 27001:2013 : Para las entidades públicas adscritas a cultura, aunque no se encuentren certificadas, deberían de reconocer y poner en práctica algunos estándares, aunque sea con el ánimo de mejorar su seguridad con la ayuda de la ISO 27001 es una norma o estándar internacional, que en su práctica ayuda a las entidades de cualquier tamaño en proteger la confidencialidad, disponibilidad e integridad de los datos con su información, de la misma forma ayuda a proteger los sistemas que la procesan.

De igual forma es importante en caso de iniciar actividades de certificación, reconocer la relación de los requerimientos que facilite los procesos de implementación de seguridad de las información , también es necesario conocer y asimilar los requerimientos pertinentes presentes en las cláusulas 4 a 10 en la ISO 27001:2013 que sirve como método de orientación para dar inicio, realizar actividades ordenas para la implementación y en lo posible impulsar actividades de perfeccionamiento en el SGSI para dar cumplimiento al ciclo de mejora continua que se conoce con el acrónimo de PHVA.

ISO/IEC 31000: Es una norma internacional que orienta por medio de una serie de directrices o técnicas, plantean la forma en que se debe de gestionar los riesgos coadyuva junto con la ISO 27001 dar cumplimiento al siclo de mejora continua a partir de la adecuada gestión de los riesgos sin importar el tamaño de la empresa o entidad.

MAGERIT : es un modelo de gestión de los riesgos trabaja de la mano con la ISO/IEC 31000 , en consecuencia orienta a las empresas o entidades de cualquier tamaño en seguir un técnica organizada para la gestión de los riesgos, pudiendo identifica las vulnerabilidades, amenazas y riesgos , a partir de lo cual se puede comprender el nivel de impacto que puede ocasionar una incidencia sobre las dimensiones de seguridad que se conocen como facetas, a partir de ese reconocimiento es posible trabajar con los controles de la ISO 27001 con la finalidad de eliminar, mitigar las amenazas o riesgos latentes, que puedan perjudicar a la entidad.

Para la infraestructura de telecomunicaciones para este tipo de entidades están en la capacidad de adoptar para sus instalaciones cableadas estructurado las siguientes normas.

Norma TIA/EIA 568 B ó A: Es una especificación de cableado para edificios y sedes que, colaborando en el diseño del área de trabajo, cuartos de equipos, cableado

horizontal, backbone y trabaja en conexidad con la norma ANSI/TIA/EIA 606 dado que es ideal para plantear indicaciones del cómo y dónde se deben nominar todos los elementos que hacen parte de la infraestructura cableada.

Norma TIA/EIA 569 A: Es una especificación tiene como propósito el normalizar o estandarizar las prácticas de diseño e implementación de las vías o canales para el cableado estructurado dentro del diseño de la infraestructura de redes de comunicación.

ANSI/TIA/EIA 606: Es una especificación tiene como propósito plantear indicaciones del cómo y dónde se deben nominar todos los elementos que hacen parte de la infraestructura cableada como por ejemplo áreas de trabajo, cuartos de equipos, cableado horizontal, backbone entre otros.

Norma ANSI-J-STD-607-A: Es una especificación muy importante porque tiene como propósito plantear indicaciones de puesta, uniones y conexión a tierra, para el diseño de la red de datos, o infraestructura de red de comunicación,

5. DISEÑO METODOLÓGICO

Para el desarrollo de este proyecto se trabaja bajo el enfoque basado en la metodología para el análisis y la gestión del riesgo para sistemas de información que se conoce como MAGERIT, en conexidad con las directrices de la gestión que han sido recopiladas en un compendio de buenas prácticas para el análisis y la gestión del riesgo bajo la norma ISO/IEC 31000, junto con el estándar para los sistemas de gestión de seguridad de la información ISO/IEC 27001:2013 , y los controles en el Anexo A de la ISO 27001 bajo un contexto común aplicable a cualquier entidad.

Para una adecuada gestión de riesgos se plantea dos tareas principales:

El análisis de los riesgos y el tratamiento de los riesgos:

- Se debe identificar los activos de información bajo un enfoque de gestión de los riesgos, partiendo de lo cual se logrará identificar las dimensiones de seguridad afectadas con relación a la, o a las amenazas identificadas, dando origen a la identificación de sus salvaguardas.

- En tratamiento de los riesgos, definición de acciones o procesos que permita minimizar los riesgos a un nivel aceptable que debe de ser liderado, aprobado y asumido por la alta gerencia, con proyección de la elaboración de un plan de tratamiento adecuado para los riesgos, acorde a las capacidades técnicas, operativas y financieras en beneficio de la entidad.

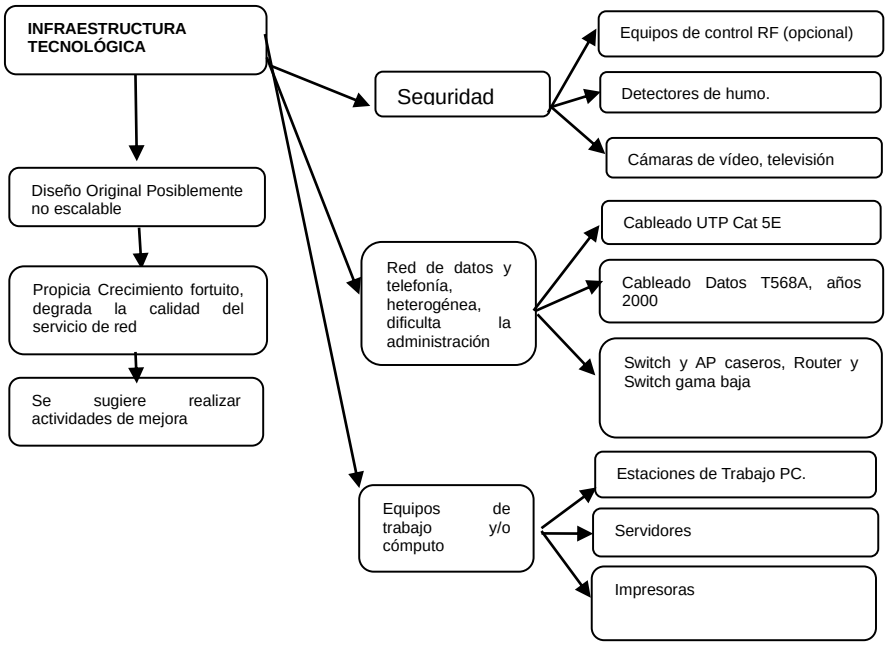
6. ESTADO ACTUAL EN LAS ENTIDADES PÚBLICAS DEDICADAS A PROMOVER LA CIENCIA, CULTURA, TECNOLOGÍA E INNOVACIÓN TECNOLÓGICA

6.1. Infraestructura tecnológica actual

Por lo general el área para la cual se plantea el análisis de seguridad presenta un cableado estructurado mayor parte de cable UTP Categoría 5E: cuenta típicamente de: mesas, equipos de cómputo, equipos de control RF, cámaras de vídeo, televisión, sistema de aire acondicionado, impresoras, detectores de humo, Switch caseros y AP mayormente caseros.

La infraestructura tecnológica de la entidad evidencia características no escalables, que, bajo el crecimiento fortuito, incide en la degradación del servicio y posiblemente afecta la seguridad.

Figura 01: Infraestructura tecnológica.



Autor: Propia.

Nota: Existe una diferencia entre un Switch y Puntos de acceso de tipo casero con Switch y puntos de acceso de gama baja. La diferencia radica en su capacidad de ser administración, el gama baja aún se considera empresarial a modo general tienen un nivel avanzado de administración, permitiendo la capacidad de ser administrables en

todos y cada uno de sus puertos de forma independiente, acciones permitidas entre las cuales están, apagar y poner reglas a puertos específicos, pueden tener presencia de puertos para fibra óptica, mientras que los caseros las configuraciones se limitan a cumplir las veces de conmutación de paquetes de datos.

Por otra parte, este tipo de entidades típicamente adoptaron la norma TIA/EIA-568-B.1-2001 Cableado T568A por lo general son redes que datan de principios de los años 2000. Cabe aclarar que la topología física original para este tipo de entidades con relación la época era buena, al día de hoy soportaría una tasa de transferencia máxima de velocidades de 1 Gbps, sin embargo es posible que el Diseño Original no sea escalable para el común de este tipo de entidades, cuando se realiza un diseño de infraestructura de redes de comunicación y no se prevé un posible crecimiento (escalable), lo anterior posibilita el desarrollo fortuito de los subsistemas que se implementan sin planeación alterando el diseño original, al observar cómo se ejecutó la implementación de los subniveles de acceso, se pueden identificar que se hace uso de Switch y puntos de acceso caseros de diversas marcas como si se tratase de puntos de consolidación, lo que produce un deterioro en la RED y por ende una baja en la calidad de prestación del servicio que depende de la conexión de RED de datos de cualquiera que fuese la entidad.

6.2. Seguridad física

6.2.1. Generalidades sobre la infraestructura

En la mayoría de estas entidades públicas dedicadas a promover la ciencia, cultura, tecnología e innovación tecnológica de la ciudad de Cali, cuando se refiere a las tecnologías de la información y de la comunicación, se presenta un crecimiento fortuito en su infraestructura, que pudo haberse sobrellevado, pero no se hizo.

Lo anterior se hubiese podido controlar un poco mejor con la adquisición de Puntos de Acceso inalámbricos de gama alta, con capacidad de soportar segmentación de red, o adquiriendo un Switch de gama alta por piso y administrables que cumpla con la norma 802.1Q que trabaje como un punto de concentración a nivel de acceso, conectados directamente desde el Switch principal ubicado en el cuarto de equipos preferiblemente con enlace troncal.

Con relación a lo anterior un enlace entre switch de core y de acceso, deben de estar conectados como mínimo con cableado UTP Categoría 6A.

Por otra parte, típicamente las entidades públicas dedicadas a promover la ciencia, cultura, tecnología e innovación tecnológica de la ciudad de Cali, en referencia a las tecnologías de la información y de la comunicación, cada puesto de trabajo cuenta con una salida para voz, salida para datos, con toma regulada y no regulado, cumpliendo con la norma, con excepción de los puntos de red que se instalan de forma no planeada dentro del modelo de red de datos original.

También se puede destacar en estas entidades que adscriptas a la secretaria de Cultura que el cableado horizontal es posible que presente una mezcla de calidades en las canaletas, con canaletas en PVC y las metálicas del cableado vertical, todo debería de la misma calidad.

6.3. Mecanismos actuales de seguridad y su efectividad en las entidades públicas

- En las en entidades públicas dedicadas a promover la ciencia, cultura, tecnología e innovación tecnológica de la ciudad de Cali es posible que esté presente un control Biométrico, pero solo es para registro de control de ingreso de funcionarios, para las áreas críticas como por ejemplo cuarto de equipos y demás áreas críticas donde está presente algún dispositivo de conmutación, routing o servidores no existe control biométrico.

- Los servidores en las entidades públicas dedicadas a promover la ciencia, cultura, tecnología e innovación tecnológica de la ciudad de Cali típicamente son de tipo torre y no cuentan con el adecuado mueble que lo proteja de manipulación inadecuada o accidental como, por ejemplo: durante las actividades de aseo siendo posible tropezar, propiciando perdida de los servicios.

- El cuarto de equipos donde están los servidores y switch de core y de acceso posee aire acondicionado, pero no cuenta con sistema de control de humedad.

- El parque informático cuenta con estaciones de trabajo con sistemas operativos que ya no tienen soporte técnico para recibir actualizaciones.

- La infraestructura dado el crecimiento fortuito y descontrolado, cuenta con una combinación muy variada de switch de tipo caseros lo que propicia tormenta de broadcast perjudicando la adecuada transmisión de información.

6.4. Infraestructura de red de datos

Por lo general las entidades públicas dedicadas a promover la ciencia, cultura, tecnología e innovación tecnológica de la ciudad de Cali hacen uso de un reconocimiento histórico de los componentes plasmados en la memoria de los administradores, posiblemente falta documentación actualizada como, por ejemplo.

1 Plano digital que contenga detalle del diseño del cableado estructurado.
2 Plano impreso que contenga detalle del diseño del cableado estructurado.
3 Plano Digital que contenga detalle de la ruta del enlace de fibra óptica.
4 Plano impreso que contenga detalle de la ruta del enlace de fibra óptica.
5 Plano Digital que contenga detalle de la ruta del enlace con ISP.
6 Plano impreso que contenga detalle de la ruta del enlace con ISP.
7 Plano impreso que contenga detalle del diseño del cableado eléctrico.
8 Plano Digital que contenga detalle del diseño del cableado eléctrico.
9 Planos que contenga detalle tableros de control.
10 Planos de puesta a tierra.
11 Planos eléctricos actualizados de energía regulada y no regulada.
12 Es posible que no se encontré Memoria técnica del proyecto que incluya los estándares o normas que está cumpliendo tales como Norma TIA/EIA 568 B ó A, Norma TIA/EIA 569 A, ANSI/TIA/EIA 606, Norma ANSI-J-STD-607-A, Anexo técnico de cantidad de materiales, Datasheet de los materiales, etc.
13 Es posible que tenga una certificación de puntos de RED, pero dado el posible crecimiento fortuito, esta certificación ya no cumpla.

6.5. Análisis preliminar de seguridad en la infraestructura

El análisis preliminar para reconocimiento del estado actual de la infraestructura de red de comunicaciones, se realiza mediante la combinación de dos formas, mediante la diligencia miento de un cuestionario y observación directa de los componentes del sistema de información.

6.5.1. Controles físicos de acceso.

Controles físicos de acceso, son necesarios como elemento de protección contra personal sin autorización de ingreso a las instalaciones (edificio, cuarto de equipos, etc.) o a los recursos críticos y confidenciales de la entidad, que se encuentran presentes en los sistemas de información e infraestructura.

Los controles, estos deben de ser idóneos para evitar el acceso o sustracción de cualquier tipo de activo de información, de propiedad de la entidad sin una autorización expresa que lo permita.

Al verifican los controles físicos de acceso, se debe de validar su idoneidad y que se cumplan, siempre teniendo en cuenta la capacidad técnica, financiera y operativa de la entidad.

Se sugiere el uso de cuestionarios preliminares y de listas de observaciones que ayuden a documentar un reconocimiento previo y general del estado actual de la infraestructura de comunicación de la entidad.

Tabla No: 1 Cuestionario preliminar.

Descripción	**Análisis**
¿La entidad tiene controles en la seguridad física, que ayuden en la protección de los activos de información en la entidad?	En algunos equipos se presenta controles de seguridad física para proteger los activos, como el uso de guayas de seguridad, en otras puertas con seguro.
¿El cuarto de equipos y telecomunicaciones tiene instalado algún sistema de alarma que ayude en la detección o de informar intrusiones cuarto de equipos y de telecomunicaciones?	El cuarto de equipos y telecomunicaciones no se tiene instalado ningún tipo de sistema de alarma para detectar ni informar de intrusiones
¿La entidad tiene algún tipo de Credencial o medio para identificación de los empleados, los visitantes con sus acompañantes que ayuden a controlar el acceso a zonas restringidas?	No están presente para los visitantes y acompañantes, en la entidad, existe como medio de control el acompañamiento
¿El total de estaciones de trabajo (PC), se encuentra en habitación cerrada con acceso restringido?	El total de estaciones de trabajo (PC) y portátiles no está en habitación cerrada con acceso restringido.

Continuación Tabla No: 1 Cuestionario preliminar.

¿Los equipos de la red de switching, routing y AP se encuentran dentro de armario o gabinete cerrado?	Algunos equipos de red no están protegidos dentro de un armario o gabinete cerrado. (switches caseros, AP).
¿Los servidores se encuentran con acceso restringido, en habitación cerrada y protegida?	Los servidores están en habitación, donde se mezcla cuarto de equipos con oficina de telemática, el único seguro que existe es la puerta con llave, los servidores están parcialmente expuestos.
¿Las estaciones de trabajo están protegidas con cables de seguridad?	Las estaciones de trabajo de la entidad no se encuentran protegidas mediante cables de seguridad.
¿Las estaciones de trabajo del tipo portátil están protegidas con cables de seguridad.	Las estaciones de trabajo del tipo portátil de la entidad, cuentan con protección mediante cables de seguridad.

Fuente: Propia

La tabla 1 refleja un cuestionario preliminar físicos de acceso y seguridad ayudando a validar su idoneidad y que se cumplan, siempre teniendo en cuenta la capacidad técnica, financiera y operativa de la entidad, ayudando a documentar el reconocimiento previo y general del estado actual de la infraestructura de comunicación de la entidad.

presentando el análisis de los subsistemas que componen el cableado estructurado basado en la norma TIA/EIA 568A y las vías de cableado de acuerdo a la norma TIA/EIA 569 A.

6.5.2. Áreas de Trabajo.

Se observa que en apoyo de las tecnologías informáticas de las entidades públicas dedicadas a promover la ciencia, cultura, tecnología e innovación tecnológica de la ciudad de Cali bajo una adecuada dirección y control en la entidad, les permite el cumplimiento de sus actividades a los funcionarios , disponiéndoles a modo general un área de trabajo donde se puede observar que establecieron dos puntos de salida, uno para voz y otro para datos cable UTP Categoría 5E, típicamente se dispone de una toma regulada y no regulada por cada punto de datos en los siguientes cuadros se evidencia las observaciones físicas.

La tabla 2, Se relacionan datos generales pero suficientes de la entidad que se observaron en la en el área de trabajo donde puede haber una debilidad y se encuentra una oportunidad de mejora.

Tabla No: 2 Observación preliminar área de trabajo.

Descripción	**Análisis**
Instalación Área de Trabajo.	Se observa combinación de calidades de canaletas, se identifican subsistemas con switch caseros como si fueran puntos de consolidación, en general organizar y documentar de nuevo.
	Se sugiere implementar cambio de canaletas de PVC por metálicas con su puesta a tierra, dado que el diseño original es canaletas metálicas.
Observación Negativa: Punto Consolidación sin terminar auditorio.	Se observa presencia de punto de Consolidación sin terminar tiene dos plaquetas para terminales. Como medio de consolidación se hace uso de un switch casero, no tiene ningún tipo de identificación ni distancia hasta el armario principal.
	Para puntos de consolidación siempre se debe de respetar 90 mt de cable UTP, partiendo del cuarto de equipos hasta el área de trabajo.
Ejemplo: de Punto Consolidación Adecuado.	Los puntos de Consolidación típicamente en redes se diseñan con el fin de tener un punto pasivo intermedio, que permita la re-ubicación de oficinas.
	Permitiendo re-cablear tramos más cortos del cableado horizontal, en lugar de tenderlos hasta el armario de telecomunicaciones en el ER, su finalidad tener un poco de flexibilidad en las reconexiones de las áreas de trabajo, cabe aclarar que del armario del ER al área de trabajo el cable no debe de superar los 90 mt.

Fuente: Propia

Las entidades públicas dedicadas a promover la ciencia, cultura, tecnología e innovación tecnológica de la ciudad de Cali, es posible que estas cuenten con unos equipos de switching principales en el cuarto de equipos (ER), donde se despliegan los puntos de RED a todos los pisos del edificio o sede dando cumplimiento con la norma de distancia máxima soportada para cable UTP Categoría 5E, lo anterior solo aplica a los puntos que pertenecen a los diseños de infraestructura de red originales.

Acorde a la observación en varias entidades públicas dedicadas a promover la ciencia, cultura, tecnología e innovación tecnológica de la ciudad de Cali, se identifica que el cuarto de equipos (ER) está en proximidades de zonas húmedas como los baños públicos, tanques de agua y tuberías hidráulicas, también de estar en un pasillo de tránsito público externo y que a su vez cumple las funciones de salida de emergencia, como evidencia se deja el siguiente cuadro donde se manifiesta de forma puntual las observaciones.

La tabla 3, Se relacionan datos generales que pueden ser críticos, que posiblemente es un riesgo latente incumpliendo con estándares con relación a rutas y espacios, presentando las actividades de análisis descriptivo a partir de la observación del Cuarto de equipos (ER) tratando de denotar lo que posiblemente se puede presentar en algunas entidades, y que poseen características similares.

Tabla No: 3 Observación preliminar Cuarto de equipos (ER)

Descripción	**Análisis**
Cuarto de equipos (ER)	Lo siguiente se observa en varias entidades, el Pasillo público y salida de emergencia al lado del cuarto de equipos (ER), el (ER) no debería de estar en esta zona, en caso de disturbios asonadas el cuarto de equipos es vulnerable, las puertas son en madera y abre para adentro, seguramente en el diseño original no había un mejor espacio.
	Los baños se encuentran en diagonal, en algunas entidades la oficina comparte el mismo espacio de ER, y posiblemente tengan un baño en su interior como se observó en algunas entidades, no cumple con el estándar 569 que refiere a las rutas y espacios de telecomunicaciones.
	Los equipos críticos tienen libre acceso oficina telemática (cuarto de equipos).
	No se hace uso de piso falso para protección de estática y la adecuación de cableado.

Fuente: Propia

La siguiente tabla, presenta un cuadro donde se puede detallar a modo general las posibles fallas que se pueden presentar en las entidades públicas dedicadas a promover la ciencia, cultura, tecnología e innovación tecnológica de la ciudad de Cali.

La tabla 4, Se relacionan datos generales del cuarto de equipos que pueden ser críticos, que posiblemente es un riesgo latente, reflejando una oportunidad de mejora.

Tabla No: 4 Observación preliminar Rack principal en el Cuarto de equipos (ER).

Descripción	**Análisis**
Rack principal en el Cuarto de equipos (ER).	No tiene puesta a tierra el rack que está en frente este resguarda la mayoría de los Switch de acceso.
	Al observar los puntos en las entidades adscriptas a la secretaria de Cultura se evidencia la calidad de los puntos de RED se nota que ha sido afectada por las constantes manipulaciones en el transcurso de los años
	Datos un procedimiento indica que los impares son Voz y los pares Datos es decir este Rack administraría los puntos de red para los usuarios.
	El mismo mal aspecto tiene el RACK de Archivo general y el gabinete de procesos

Fuente: Propia

6.5.3. Switches principales (Core).

Las entidades públicas dedicadas a promover la ciencia, cultura, tecnología e innovación tecnológica según se observa cuenta con unos equipos de switching obsoletos bajo un esquema heterogéneo dado que no todos son administrables y su tasa de transferencia máxima es de 10/100 Mbp/s y además son de diversas marcas.

Tabla No: 5, A nivel general se observa que los switches no son administrables, cumplen con la norma 802.1Q lo que implica que no se puede segmentar la red, lo que implica que a nivel de red no se puede clasificar los recursos de red, lo que posiblemente puede evolucionar en un riesgo.

Tabla No: 5 Observación preliminar Switches de core.

Descripción	Análisis
Switches de core.	Son obsoletos no son administrables y su tasa de transferencia máxima es de 10/100 Mbp/s
	Aplica tanto para los switches de core como de acceso: Se sugiere reemplazar implementando Switch de gama alta, de igual forma adicionar uno en cada piso, este switch se sugiere que contenga como mínimo 4 puertos de 100/1000/10000 10BASE-T y 48 puertos 10/100/1000
	Aplica tanto para los switches de core como de acceso: Se sugiere para conectar las troncales de los demás Switchd de acceso. Para todos: deben de cumplir con la norma 802.1Q (VLAN) ideal para segmentar la red, etherchanel (suma capacidad de varias interfaces de red) con un mínimo de 4 FSP
	Aplica tanto para los switches de core como de acceso: Se sugiere para mayor alcance de compatibilidad que se adquieran Switch de la misma marca que garantice la homogeneidad de la red garantizando mayor agilidad en las actividades de conmutación de datos y de la seguridad en su transmisión.

Fuente: Propia

6.5.4. Switches secundarios (acceso).

La entidades públicas dedicadas a promover la ciencia, cultura, tecnología e innovación tecnológica según se observa cuenta con unos equipos de switching una parte son obsoletos o de tipo caseros, es de aclarar que un switch empresarial de gama baja es superior a un switch casero aunque ambos para este caso, no son administrables y su tasa de transferencia máxima es de 10/100 Mbp/s, entonces en este caso la diferencia entre el switch casero y el gama baja radica en la capacidad de trabajo intensivo 7/24.

La Tabla No: 6 A nivel general se observa que los switches no son administrables, cumplen con la norma 802.1Q lo que implica que no se puede segmentar la red, lo que implica que a nivel de red no se puede clasificar los recursos de red, lo que posiblemente puede evolucionar en un riesgo.

Tabla No: 6 Observación preliminar Switches de acceso.

Descripción	Análisis
Switches de acceso.	Una parte son obsoletos no son administrables y su tasa de transferencia máxima es de 10/100 Mbp/s.
	Una parte son caseros no son administrables y su tasa de transferencia máxima es de 10/100 Mbp/s.
	Se sugiere para todos: deben de cumplir con la norma 802.1Q (VLAN) ideal para segmentar la red, etherchanel (suma capacidad de varias interfaces de red) con un mínimo de 4 FSP
	Se sugiere para mayor alcance de compatibilidad, que se adquieran Switch de la misma marca que garantice la homogeneidad de la red lo que a su vez contribuye con mayor agilidad en las actividades de conmutación de datos y de la seguridad en su transmisión.

Fuente: Propia

6.5.5. Aire acondicionado.

Las entidades públicas dedicadas a promover la ciencia, cultura, tecnología e innovación tecnológica, típicamente en las entidades pequeñas según se observa, cuenta con unos equipos de acondicionamiento para el ambiente de zonas críticas donde se alojan equipos de conmutación, enrutamiento, almacenamiento, procesamiento de información. No obstante, se requiere un aire de precisión que ayude a conservar en buen estado los componentes electrónicos.

La Tabla No: 7, A nivel general se evidencia que en este tipo de entidades no se usa aire acondicionado de precisión, lo cual puede generar humedad y para algunos equipos puede ser perjudicial a largo plazo.

Tabla No: 7 Observación preliminar aire acondicionado.

Descripción	Análisis
Aire Acondicionado.	Se logra evidenciar que para las distintas áreas críticas entre las que se incluyen algunos procesos de la entidad y el cuarto de equipos (ER) el aire acondicionado que está instalado en el área de telemática y demás zonas críticas no es un aire de precisión.
	Se sugiere Solo para la sala de equipos (ER) Se sugiere un Aire de precisión, tiene un termostato que regula la temperatura, además regula la húmeda, debe de ser calculado según el área por personal idóneo en la materia.

	Continuación Tabla 7
	En caso de no adquirir aire de precisión se sugiere además del aire acondicionado tener un des humificador, aunque lo ideal es tener un aire acondicionado de precisión en la sala de equipos (ER), dicho aire también puede ser implementado de forma focalizada directamente a un RACK de switch, routing o de servidores lo que puede salir más económico a la entidad.

Fuente: Propia

6.5.6. Hardware servidores.

Las entidades públicas dedicadas a promover la ciencia, cultura, tecnología e innovación tecnológica según se observa que cuenta con unos servidores físicos que de forma paulatina están migrando sus servicios a entornos virtuales, lo cual brinda la posibilidad de independizar servicios en un mismo espacio físico permitiendo optimizar el uso del espacio, pero con distinto espacio virtual, también ayuda en reducción de gastos en consumo de energía y mantenimiento, facilita las operaciones de backup.

La Tabla No: 8, A nivel general el cuadro demuestra que los servidores presentan una combinación de equipos modernos y obsoletos, sin embargo, están acogiendo tecnologías como la virtualización, y se evidencia oportunidad de mejora.

Tabla No: 8 Observación preliminar de servidores.

Descripción	**Análisis**
Servidores	Se logra evidenciar para estas entidades los servidores Físicos hay una combinación entre equipos obsoletos, modernos y además se encuentra iniciativas migrar a tecnología virtual.
	Servicios presentes para los servidores virtuales como: Directorio Activo, Servidor DHCP, Servidor de Almacenamiento, Servidor web, servidor bases de datos PostgreSQL y Oracle 12, UTM, servidor de repositorio legal con apache y MySQL.
	Los servidores físicos su ubicación debe mejorar
	Se sugiere la adquisición de software especializado de copias de seguridad se realiza sugerencia de adquisición de servidores con más prestaciones, para agilizar la puesta en marcha al levantar un respaldo total.
	Al realizar actividades de adquisición de nuevos servidores, se sugiere que tengan características sobredimensionadas dejando la probabilidad de implementar más servicios a nivel virtual.

Fuente: Propia

6.5.7. Estaciones de trabajo (Computadores).

Las entidades públicas dedicadas a promover la ciencia, cultura, tecnología e innovación tecnológica según se observa dentro de su infraestructura cuenta con un parque informático que trabaja con una mezcla de tecnología obsoletas y modernas lo que propicia que las estaciones de trabajo sean un punto débil por su incapacidad de poder ser actualizadas.

La Tabla No: 9, Se logra observar que existe una convivencia de sistemas operativos obsoletos sin soporte que toman servicios como DHCP entre otros lo que propicia un riego que se puede tomar como una oportunidad de mejora.

Tabla No: 9 Observación preliminar **estaciones de trabajo**.

Descripción	**Análisis**
Estaciones de trabajo	Se logra evidenciar para estas entidades cuentan con estaciones de trabajo que cuentan con sistemas operativo Windows XP, Windows Vista, Windows 7 sistemas que a la fecha ya no cuentan con soporte técnico para recibir actualizaciones de seguridad, lo que propicia un riesgo latente pudiendo ser aprovechado por virus, y todo tipo de Malware.
	Servicios presentes para los servidores virtuales como: Directorio Activo, Servidor DHCP, Servidor de Almacenamiento, Servidor web, servidor bases de datos PostgreSQL y Oracle 12, UTM, servidor de repositorio legal con apache y MySQL.

Fuente: Propia

7. RIESGOS LATENTES POR EL USO DEL TIC EN ENTIDADES PÚBLICAS

A partir del ESTADO ACTUAL y con los insumos de información que se puede proyectar, se realizara actividades de reconocimiento de impacto de los riesgos latentes, mediante la identificación de las amenazas vs las dimensiones de seguridad, apoyado en Magerit que a su vez se apoya en la normativa ISO 31000 en respuesta a la gestión del riesgo, (magerit libro 1, pag 7)

Por lo anterior un activo puede ser afectado en uno o varias facetas, indispensables para lograr identificar las consecuencias en caso tal que una amenaza se materialice estas dimensiones son:

- Disponibilidad (D).
- Integridad (I).
- Confidencialidad (C).
- Autenticidad (A).
- Trazabilidad (T).

Reconociendo las dimensiones de seguridad que pueden ser afectadas se procede a identificar de forma pormenorizada los activos de información para establecer el estado actual con enfoque de gestión del riesgo.

Los datos contienen información valiosa que pueden o no ser almacenados en equipos informáticos típicamente se encuentra en bases de datos o archivos electrónicos.

7.1. Identificación general de los activos de información

A partir de esta instancia se realizará actividades de identificación de los activos de información se propone trabajar bajo la influencia de la metodología MAGERIT dado que permite una adecuada y sistemática gestión del riesgo, que bajo observación y cuestionarios previos se identificaron para este tipo de entidades públicas, en consecuencia, se sugiere trabajar en conexidad con la ISO 27001 Anexo A.

En la tabla 10 se evidencian activos de información de la categoría DATOS. [11]
Se identifican los activos de información correspondientes a los servicios que satisfacen las necesidades de los funcionarios.

Tabla No: 10 Identificación de [D] DATOS. / Información

ID-Activo	Categoría Activo		Subcategoría	Servicio o descripción del Activo
1	[D] DATOS.	[Files]	Archivos	Repositorio de archivos de apoyo y misionales.
2	[D] DATOS.	[backup].	Copias para respaldo.	Copias para respaldo de configuración de SW, Router.
3	[D] DATOS.	[backup].	Copias para respaldo.	Copias para respaldo de configuración de máquinas, virtuales, bases de datos e información.
4	[D] DATOS.	[backup].	Copias para respaldo.	Copias para respaldo de bases de datos y de información.
5	[D] DATOS.	[Int].	Datos para la gestión interna	Bases de datos de apoyo y misionales.

Fuente: Propia

[11] MAGERIT versión 3 Libro II Catálogo de elementos (versión español): Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Ministerio de Hacienda y Administraciones Públicas. España 2012. [En Línea]. 75 p. Disponible en: https://administracionelectronica.gob.es/pae_Home/dam/jcr:5fbe15c3-c797-46a6-acd8-51311f4c2d29/2012_Magerit_v3_libro2_catalogo-de-elementos_es_NIPO_630-12-171-8.pdf. P.8

La tabla 11 Identificación se evidencian activos de información de la categoría servicios[12].
En la tabla se logra identificar activos de información que están en la categoría servicios para la entidad.

Tabla No: 11 Identificación de [S] Servicios.

ID-Activo	Categoría Activo		Subcategoría	Servicio o descripción del Activo
6	[S] Servicios	[www].	[www]World wide web.	Servicios de publicación del sitio web.
7	[S] Servicios	[email].	[email].Correo electrónico.	Servicios de publicación correo electrónico
8	[S] Servicios	[Int].	[Int].Interno.	Servicios de impresión
9	[S] Servicios	[Int].	[Int].Interno.	Servicios de soporte técnico
10	[S] Servicios	[Int].	[Int].Interno.	Servicios IDS/IPS
11	[S] Servicios	[Int].	[Int].Interno.	Servicios HITS
12	[S] Servicios	[ftp].	[ftp].Transferencia de ficheros.	Protocolo de transferencia de archivos
13	[S] Servicios	[file].	[file].Almacenamiento de archivos.	Soporte en almacenamiento de archivos misionales y de apoyo.
14	[S] Servicios	[idm].	[idm]. Gestión de identidades.	Soporte a gestión de usuarios y contraseñas.

Fuente: Propia

[12] MAGERIT versión 3 Libro II Catálogo de elementos (versión español): Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Ministerio de Hacienda y Administraciones Públicas. España 2012. [En Línea]. 75 p. Disponible en: https://administracionelectronica.gob.es/pae_Home/dam/jcr:5fbe15c3-c797-46a6-acd8-51311f4c2d29/2012_Magerit_v3_libro2_catalogo-de-elementos_es_NIPO_630-12-171-8.pdf. P.8

El [SW] Software - Aplicaciones informáticas son activos de información que corresponden a programas, desarrollos entre otras, que sirven para el ejercicio de labores mediante la elaboración de tareas ejecutadas por medio de un equipo informático. [13]

En la tabla 12 se logra identificar activos de información que están en la categoría Software Aplicaciones informáticas para la entidad.

Tabla No: 12 Identificación de [SW] Software - Aplicaciones informáticas

ID-Activo	Categoría Activo		Subcategoría	Servicio o descripción del Activo
1	[SW] SOFTWARE	[dbms].	Sistema de administración de bases de datos.	Motor de bases de datos Mysql
2	[SW] SOFTWARE	[dbms].	Sistema de administración de bases de datos.	Motor de bases de datos PostgreSQL
3	[SW] SOFTWARE	[dbms].	Sistema de administración de bases de datos.	Motor de bases de datos Oracle12
4	[SW] SOFTWARE	[os].	Sistema Operativo.	S.O Microsoft Windos 10
5	[SW] SOFTWARE	[os].	Sistema Operativo.	S.O Microsoft Windos 7
6	[SW] SOFTWARE	[os].	Sistema Operativo.	S.O Microsoft Windos Vista
7	[SW] SOFTWARE	[os].	Sistema Operativo.	S.O Microsoft Windos XP
8	[SW] SOFTWARE	[os].	Sistema Operativo.	S.O Microsoft Windos server 2008
9	[SW] SOFTWARE	[os].	Sistema Operativo.	S.O Microsoft Windos server 2012
10	[SW] SOFTWARE	[os].	Sistema Operativo.	Linux Centos 7
11	[SW] SOFTWARE	[os].	Sistema Operativo.	S.O UTM
12	[SW] SOFTWARE	[os].	Sistema Operativo.	Hypervisor de Máquinas virtuales
13	[SW] SOFTWARE	[std].	Estándar.	Apache.
14	[SW] SOFTWARE	[std].	Estándar.	IIS.
15	[SW] SOFTWARE	[std].	Estándar.	CMS Joomla.
16	[SW] SOFTWARE	[std].	Estándar.	CMS WordPress.
17	[SW] SOFTWARE	[std].	Estándar.	GLPI Inventario mesa de ayuda
18	[SW] SOFTWARE	[std].	Estándar.	PHP 5.6.30 – 7.1.1 >

Fuente: Propia

[13] MAGERIT versión 3 Libro II Catálogo de elementos (versión español): Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Ministerio de Hacienda y Administraciones Públicas. España 2012. [En Línea]. 75 p. Disponible en: https://administracionelectronica.gob.es/pae_Home/dam/jcr:5fbe15c3-c797-46a6-acd8-51311f4c2d29/2012_Magerit_v3_libro2_catalogo-de-elementos_es_NIPO_630-12-171-8.pdf.

El [HW] Equipamiento informático (hardware) son activos de información que Soportan de forma directa o indirectamente los servicios de la entidad, que sirven para el ejercicio de labores mediante el procesamiento de tareas siendo capaces de transferir y/o almacenar de forma temporal o permanente los datos. [14]

En la tabla 13 se logra identificar activos de información que están en la categoría hardware equipamiento informático para la entidad.

Tabla No: 13 Identificación de [HW] Equipamiento informático.

ID-Activo	Categoría Activo		Subcategoría	Servicio o descripción del Activo
33	[HW] Equipamiento informático.	[print].	Medios de impresión (6)	Impresora en RED Laser. (Cantidad: X)
34	[HW] Equipamiento informático.	[host].	Grandes quipos	Servidor Hypervisor
35	[HW] Equipamiento informático.	[vhost].	Equipo virtual.	Servidor GLPI de soporte técnico
36	[HW] Equipamiento informático.	[vhost].	Equipo virtual.	Servidor UTM IDS/IPS
37	[HW] Equipamiento informático.	[vhost].	Equipo virtual.	Servidor HITS
38	[HW] Equipamiento informático.	[vhost].	Equipo virtual.	Servidor Protocolo de transferencia de archivos
39	[HW] Equipamiento informático.	[vhost].	Equipo virtual.	Servidor Soporte en almacenamiento de Archivos misionales y de apoyo.
40	[HW] Equipamiento informático.	[vhost].	Equipo virtual.	Servidor gestión de usuarios y contraseñas.

Fuente: Propia

[14] MAGERIT versión 3 Libro II Catálogo de elementos (versión español): Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Ministerio de Hacienda y Administraciones Públicas. España 2012. [En Línea]. 75 p. Disponible en: https://administracionelectronica.gob.es/pae_Home/dam/jcr:5fbe15c3-c797-46a6-acd8-51311f4c2d29/2012_Magerit_v3_libro2_catalogo-de-elementos_es_NIPO_630-12-171-8.pdf.

El [COM] Redes de comunicaciones son activos de información que Soportan los servicios de comunicación para la transferencia de datos o para compartir recursos en red puede incluir servicios contratados por terceros. [15]

En la Tabla No: 14, se logra identificar activos de información que están en la categoría elementos de comunicación redes de comunicación equipamiento y servicios informático para la entidad.

Tabla No: 14 Identificación de [COM] Redes de comunicaciones.

ID-Activo	Categoría Activo		Subcategoría	Servicio o descripción del Activo
41	[COM] Redes de comunicaciones	[PSTN].	Red telefónica	Servicio de telefonía para la organización
41	[COM] Redes de comunicaciones	[Internet].	Internet.	Servicio de internet dedicado para la organización
42	[COM] Redes de comunicaciones	[wifi].	Red inalámbrica.	Radio enlaces local (WI-FI).
43	[COM] Redes de comunicaciones	[LAN].	Red local.	Red de área local

Fuente: Propia

[15] MAGERIT versión 3 Libro II Catálogo de elementos (versión español): Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Ministerio de Hacienda y Administraciones Públicas. España 2012. [En Línea]. 75 p. Disponible en: https://administracionelectronica.gob.es/pae_Home/dam/jcr:5fbe15c3-c797-46a6-acd8-51311f4c2d29/2012_Magerit_v3_libro2_catalogo-de-elementos_es_NIPO_630-12-171-8.pdf. P.12

El [AUX] Equipamiento auxiliar son activos de información que Soportan los servicios de información pero que no se encuentra relacionados con los datos.

En la Tabla No: 15, se logra identificar activos de información que están en la categoría elementos auxiliares típicamente brindan equipos de protección informático o el medio físico por donde se transporta los servicios que se comparten en un medio de comunicación para la entidad.

Tabla No: 15 Identificación de [AUX] Equipamiento auxiliar

ID-Activo	Categoría Activo		Subcategoría	Servicio o descripción del Activo
44	[AUX] Equipamiento auxiliar.	[ups].	Sistemas de alimentación ininterrumpida	UPS dedicado para los servidores.
45	[AUX] Equipamiento auxiliar.	[ac].	Equipos de climatización	Aire acondicionado dedicado para los servidores.
46	[AUX] Equipamiento auxiliar.	[cabling], [wire].	Cableado	Cableado eléctrico.

Fuente: Propia

Las [L] Instalaciones son activos de información necesarios para hospedar los servicios de información y de comunicación.[16]

En la Tabla No: 16, se identifica el activo de información que están en la categoría instalaciones, es decir la localidad o el edificio donde esta presenta la infraestructura de red de telecomunicaciones para la entidad

Tabla No: 16 Identificación de [L] Instalaciones

ID-Activo	Categoría Activo		Subcategoría	Servicio o descripción del Activo
47	[L] Instalaciones.	[building].	Edificio.	Edificio Infraestructura de la organización

Fuente: Propia

[16] MAGERIT versión 3 Libro II Catálogo de elementos (versión español): Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Ministerio de Hacienda y Administraciones Públicas. España 2012. [En Línea]. 75 p. Disponible en: https://administracionelectronica.gob.es/pae_Home/dam/jcr:5fbe15c3-c797-46a6-acd8-51311f4c2d29/2012_Magerit_v3_libro2_catalogo-de-elementos_es_NIPO_630-12-171-8.pdf. P.12-13

Las [P] Personal son activos de información identifica las personas que se encuentran relacionadas con el sistema de información.[17]

En la Tabla No: 17, identifica el activo de información que están en la categoría personal, es decir el recurso humano que va interactuar cumplir roles y funciones con la infraestructura de red de telecomunicaciones para la entidad.

Tabla No: 17 Identificación de [P] Personal

ID-Activo	Categoría Activo		Subcategoría	Servicio o descripción del Activo
48	[P] Personal.	[ui].	Usuarios internos	Usuario interno (Cantidad:2)
48	[P] Personal.	[adm].	Administradores de sistemas	Técnicos para administración y mantenimiento (Cantidad:2)
48	[P] Personal.	[sub].	subcontrata	Contratista de apoyo (Cantidad:1)

Fuente: Propia

Las tablas están basadas en las descripciones de las facetas de seguridad de la información. Establecida en la metodología de análisis y gestión de riesgos de los sistemas de información. Ministerio de Hacienda y Administraciones Públicas, España, 2012

7.2. Determinar amenazas vs las dimensiones de seguridad afectadas

Ahora basado en Magerit y la forma en que se discriminan las amenazas, al mismo tiempo se apoya en la normativa ISO 31000 en respuesta a la gestión del riesgo, establece unas dimensiones derivados del uso de las tecnologías de la información[18]

[17] MAGERIT versión 3 Libro II Catálogo de elementos (versión español): Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Ministerio de Hacienda y Administraciones Públicas. España 2012. [En Línea]. 75 p. Disponible en: https://administracionelectronica.gob.es/pae_Home/dam/jcr:5fbe15c3-c797-46a6-acd8-51311f4c2d29/2012_Magerit_v3_libro2_catalogo-de-elementos_es_NIPO_630-12-171-8.pdf.

[18]

que sirve para identificar el impacto de una amenaza con relación al activo de información puede ser afectado en uno o varias facetas, dichas facetas se distinguen como dimensiones de seguridad, dato indispensables para lograr identificar las consecuencias o impacto en caso tal que una amenaza se materialice
En el siguiente cuadro se enumera las dimensiones de seguridad:

La Tabla No: 18, se identifica las dimensiones de seguridad con las que se va a identificar el impacto de una amenaza para la entidad

Tabla No: 18 Dimensiones de seguridad.

Dimensión	Faceta
Dimensiones de seguridad que pueden ser afectadas.	[D] Disponibilidad.
	[I] Integridad.
	[C] Confidencialidad.
	[A] Autenticidad.
	[T] Trazabilidad.

Fuente: Propia.

Para este momento se ha identificado los activos de información, se han identificado las dimensiones, bajo este punto es la información con la que se cuenta para identificar el impacto de una amenaza.

Se deben identificar las posibles amenazas del activo de información, relacionando las facetas en las cuales son afectadas como por ejemplo [D] Disponibilidad, [I] integridad, [C] confidencialidad, [A] autenticidad y [T] Trazabilidad, pudiendo ser solo una o todas, sin que una faceta intervenga con las demás facetas, para tal fin se realiza las siguientes tablas de amenazas vs dimensiones con relación a los activos de información.

Tabla No: 19, se identifica las Amenazas vs dimensiones el los [D] DATOS logrando identificar la amenaza y el posible impacto sobre el activo de información para la entidad.

Tabla No: 19 Identificación Amenazas vs dimensiones [D] DATOS.

Tabla relacionada	Tipo de Activo	ID-Activo	Activo	Amenaza	Dimensión afectada
Tabla N11	[D] DATOS.	1	[FILES]Archivos de apoyo y misionales.	[E,1]Error de usuario.	[I], [C], [D].
				[E,2]Error de administrador.	[D], [I], [C].
				[A,15]Modificación deliberada de la información.	[I].
				[A,18]Destrucción de información.	[D].
Tabla N11	[D] DATOS.	2	[backup].Copias para respaldo de configuración de SW , Router.	[E,1]Error de usuario.	[I], [C], [D].
				[E,2]Error de administrador.	[D], [I], [C].
				[A,11]Acceso no autorizado.	[C], [I].
Tabla N11	[D] DATOS.	3	[backup].Copia de respaldo estado MV.	[E,1]Error de usuario.	[I], [C], [D].
				[E,2]Error de administrador.	[D], [I], [C].
				[A,11]Acceso no autorizado.	[C], [I].
Tabla N11	[D] DATOS.	4	[backup].Copia de respaldo BD.	[E,1]Error de usuario.	[I], [C], [D].
				[E,2]Error de administrador.	[D], [I], [C].
				[A,11]Acceso no autorizado.	[C], [I].
Tabla N11	[D] DATOS.	5	Bases de datos de apoyo y misionales.	[E,1]Error de usuario.	[I], [C], [D].
				[E,2]Error de administrador.	[D], [I], [C].
				[A,15]Modificación deliberada de la información.	[I].
				[A,18]Destrucción de información.	[D].

Fuente: Propia

Tabla No: 20, se identifica las Amenazas vs dimensiones el los [S] Servicios logrando identificar la amenaza y el posible impacto sobre el activo de información para la entidad.

Tabla No: 20 Identificación Amenazas vs dimensiones [S] Servicios part No 1.

Tabla Rel	Tipo de Activo	ID-Activo	Activo	Amenaza	Dimensión afectada
Tabla N12	[S] Servicios	6	[www].Servicios de publicación del sitio web.	[E,2]Error de administrador.	[D], [I], [C].
				[A.,11]Acceso no autorizado.	[C], [I].
				[A,18]Destrucción de información.	[D].
				[A,24]Denegación de servicio.	[D].
Tabla N12	[S] Servicios	7	[email].Servicios de publicación correo electrónico	[E,2]Error de administrador.	[D], [I], [C].
				[A,5]Suplantación de la identidad del usuario.	[C], [A], [I].
Tabla N12	[S] Servicios	8	[Int].Servicios de impresión	[E,1]Errores de los usuarios.	[I], [C], [D].
				[E,2]Error de administrador.	[D], [I], [C].
				[E,14]Escapes de información.	[C].

Fuente: Propia

Las tablas 19 a 36 donde se logra evidenciar amenazas vs dimensiones de seguridad por categorías.[19]

[19] MAGERIT versión 3 Libro II Catálogo de elementos (versión español): Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Ministerio de Hacienda y Administraciones Públicas. España 2012. [En Línea]. 75 p. Disponible en: https://administracionelectronica.gob.es/pae_Home/dam/jcr:5fbe15c3-c797-46a6-acd8-51311f4c2d29/2012_Magerit_v3_libro2_catalogo-de-elementos_es_NIPO_630-12-171-8.pdf. P.25-57

La Tabla No: 21, se identifica las Amenazas vs dimensiones el los [S] Servicios logrando identificar la amenaza y el posible impacto sobre el activo de información para la entidad.

Tabla No: 21 Identificación Amenazas vs dimensiones [S] Servicios part No 2.

Tabla Rel	Tipo de Activo	ID-Activo	Activo	Amenaza	Dimensión afectada
Tabla N12	[S] Servicios	9	[Int]. Soporte técnico (R.H).	[E,24]Caída del sistema por agotamiento de recursos.	[D].
Tabla N12	[S] Servicios	10	[Int]. Servicios IDS/IPS	[E,2]Error de administrador.	[D], [I], [C].
				[E,24]Caída del sistema por agotamiento de recursos.	[D].
				[A,24]Denegación de servicio.	[D].
Tabla N12	[S] Servicios	11	[Int]. Servicios HITS	[E,2]Error de administrador.	[D], [I], [C].
				[E,24]Caída del sistema por agotamiento de recursos.	[D].
				[A,24]Denegación de servicio.	[D].
Tabla N12	[S] Servicios	12	[ftp]. Protocolo de transferencia de archivos	[E,2]Error de administrador.	[D], [I], [C].
				[E,24]Caída del sistema por agotamiento de recursos.	[D].
				[A,24]Denegación de servicio.	[D].
Tabla N12	[S] Servicios	13	[file]. Soporte en almacenamiento de archivos misionales y de apoyo.	[E,2]Error de administrador.	[D], [I], [C].
				[E,24]Caída del sistema por agotamiento de recursos.	[D].
				[A,24]Denegación de servicio.	[D].
Tabla N12	[S] Servicios	14	[IDM]Soporte a gestión de usuarios y contraseñas.	[E,2]Error de administrador.	[D], [I], [C].
				[E,24]Caída del sistema por agotamiento de recursos.	[D].
				[A,24]Denegación de servicio.	[D].

Fuente: Propia

La Tabla No: 22, se identifica las Amenazas vs dimensiones el [SW] Software logrando identificar la amenaza y el posible impacto sobre el activo de información para la entidad.

Tabla No: 22 Identificación Amenazas vs dimensiones [SW] Software Part No 1.

Tabla Rel	Tipo de Activo	ID-Activo	Activo	Amenaza	Dimensión afectada
Tabla N13	[SW] Software.	15	[dbms]._Bases de datos Mysql	[E,2]Error de administrador.	[D], [I], [C].
				[E,20]Vulnerabilidades en los programas.	[I], [D], [C].
				[E,21]Error de mantenimiento - actualización de programas.	[I], [D].
Tabla N13	[SW] Software.	16	[dbms]._Bases de datos PostgreSQL	[E,2]Error de administrador.	[D], [I], [C].
				[E,20]Vulnerabilidades en los programas.	[I], [D], [C].
				[E,21]Error de mantenimiento - actualización de programas.	[I], [D].
Tabla N13	[SW] Software.	17	[dbms]._Bases de datos Oracle12	[E,2]Error de administrador.	[D], [I], [C].
				[E,20]Vulnerabilidades en los programas.	[I], [D], [C].
				[E,21]Error de mantenimiento - actualización de programas.	[I], [D].
Tabla N13	[SW] Software.	18	[os]._S.O Microsoft Windows 10	[E,1]Error del usuario.	[I], [C], [D].
				[E,20]Vulnerabilidades en los programas.	[I], [D], [C].
				[E,21]Error de mantenimiento - actualización de programas.	[I], [D].
				[A.6]. Abuso de privilegios de acceso.	[C], [I], [D].
				[A,7]Uso no previsto.	[D], [C], [I].
				[A,8]Difusión de software dañino.	[D], [I], [C].

Fuente: Propia

La Tabla No: 23, se identifica las Amenazas vs dimensiones el [SW] Software logrando identificar la amenaza y el posible impacto sobre el activo de información para la entidad.

Tabla No: 23 Identificación Amenazas vs dimensiones [SW] Software Part No 2.

Tabla Rel	Tipo de Activo	ID-Activo	Activo	Amenaza	Dimensión afectada
Tabla N13	[SW] Software.	19	[os]._S.O Microsoft Windows 7	[E,1]Error del usuario.	[I], [C], [D].
				[E,20]Vulnerabilidades en los programas.	[I], [D], [C].
				[E,21]Error de mantenimiento - actualización de programas.	[I], [D].
				[A.6]. Abuso de privilegios de acceso.	[C], [I], [D].
				[A,7]Uso no previsto.	[D], [C], [I].
				[A,8]Difusión de software dañino.	[D], [I], [C].
Tabla N13	[SW] Software.	20	[os]._S.O Microsoft Windows Vista	[E,1]Error del usuario.	[I], [C], [D].
				[E,20]Vulnerabilidades en los programas.	[I], [D], [C].
				[E,21]Error de mantenimiento - actualización de programas.	[I], [D].
				[A.6]. Abuso de privilegios de acceso.	[C], [I], [D].
				[A,7]Uso no previsto.	[D], [C], [I].
				[A,8]Difusión de software dañino.	[D], [I], [C].
Tabla N13	[SW] Software.	21	[os]. _S. O Microsoft Windows XP	[E,1]Error del usuario.	[I], [C], [D].
				[E,20]Vulnerabilidades en los programas.	[I], [D], [C].
				[E,21]Error de mantenimiento - actualización de programas.	[I], [D].

Fuente: Propia

La Tabla No: 24, se identifica las Amenazas vs dimensiones el [SW] Software logrando identificar la amenaza y el posible impacto sobre el activo de información para la entidad.

Tabla No: 24 Identificación Amenazas vs dimensiones [SW] Software Part No 3.

Tabla Rel	Tipo de Activo	ID-Activo	Activo	Amenaza	Dimensión afectada
Tabla N13	[SW] Software.	21	[os]._S.O Microsoft Windows XP	[A.6]. Abuso de privilegios de acceso.	[C], [I], [D].
				[A,7]Uso no previsto.	[D], [C], [I].
				[A,8]Difusión de software dañino.	[D], [I], [C].
Tabla N13	[SW] Software.	22	[os]._S.O Microsoft Windows server 2008	[E,2]Error de administrador.	[D], [I], [C].
				[E,20]Vulnerabilidades en los programas.	[I], [D], [C].
				[E,21]Error de mantenimiento - actualización de programas.	[I], [D].
				[E,24]Caída del sistema por agotamiento de recursos.	[D].
Tabla N13	[SW] Software.	23	[os]._S.O Microsoft Windows server 2012	[E,2]Error de administrador.	[D], [I], [C].
				[E,20]Vulnerabilidades en los programas.	[I], [D], [C].
				[E,21]Error de mantenimiento - actualización de programas.	[I], [D].
				[E,24]Caída del sistema por agotamiento de recursos.	[D].
Tabla N13	[SW] Software.	24	[os]._Linux Centos 7	[E,2]Error de administrador.	[D], [I], [C].
				[E,20]Vulnerabilidades en los programas.	[I], [D], [C].
				[E,21]Error de mantenimiento - actualización de programas.	[I], [D].
				[E,24]Caída del sistema por agotamiento de recursos.	[D].

Fuente: Propia

La Tabla No: 25, se identifica las Amenazas vs dimensiones el [SW] Software logrando identificar la amenaza y el posible impacto sobre el activo de información para la entidad.

Tabla No: 25 Identificación Amenazas vs dimensiones [SW] Software Part No 4.

Tabla Rel	Tipo de Activo	ID-Activo	Activo	Amenaza	Dimensión afectada
Tabla N13	[SW] Software.	25	[os]._S.O UTM	[E,2]Error de administrador.	[D], [I], [C].
				[E,20]Vulnerabilidades en los programas.	[I], [D], [C].
				[E,21]Error de mantenimiento - actualización de programas.	[I], [D].
				[E,24]Caída del sistema por agotamiento de recursos.	[D].
Tabla N13	[SW] Software.	26	[os]._Hypervisor de Máquinas virtuales	[E,2]Error de administrador.	[D], [I], [C].
				[E,20]Vulnerabilidades en los programas.	[I], [D], [C].
				[E,21]Error de mantenimiento - actualización de programas.	[I], [D].
				[E,24]Caída del sistema por agotamiento de recursos.	[D].
Tabla N13	[SW] Software.	27	[std]._Apache.	[E,2]Error de administrador.	[D], [I], [C].
				[E,20]Vulnerabilidades en los programas.	[I], [D], [C].
				[E,21]Error de mantenimiento - actualización de programas.	[I], [D].
				[E,24]Caída del sistema por agotamiento de recursos.	[D].
Tabla N13	[SW] Software.	28	[std]._IIS.	[E,2]Error de administrador.	[D], [I], [C].
				[E,20]Vulnerabilidades en los programas.	[I], [D], [C].

Fuente: Propia

La Tabla No: 26, se identifica las Amenazas vs dimensiones el [SW] Software logrando identificar la amenaza y el posible impacto sobre el activo de información para la entidad.

Tabla No: 26 Identificación Amenazas vs dimensiones [SW] Software Part No 5.

Tabla Rel	Tipo de Activo	ID-Activo	Activo	Amenaza	Dimensión afectada
Tabla N13	[SW] Software.	28	[std]._IIS.	[E,21]Error de mantenimiento - actualización de programas.	[I], [D].
				[E,24]Caída del sistema por agotamiento de recursos.	[D].
Tabla N13	[SW] Software.	29	[std]._CMS Joomla.	[E,2]Error de administrador.	[D], [I], [C].
				[E,20]Vulnerabilidades en los programas.	[I], [D], [C].
				[E,21]Error de mantenimiento - actualización de programas.	[I], [D].
Tabla N13	[SW] Software.	30	[std]._CMS WordPress.	[E,2]Error de administrador.	[D], [I], [C].
				[E,20]Vulnerabilidades en los programas.	[I], [D], [C].
				[E,21]Error de mantenimiento - actualización de programas.	[I], [D].
Tabla N13	[SW] Software.	31	[std]._GLPI Inventario mesa de ayuda	[E,2]Error de administrador.	[D], [I], [C].
				[E,20]Vulnerabilidades en los programas.	[I], [D], [C].
				[E,21]Error de mantenimiento - actualización de programas.	[I], [D].
Tabla N13	[SW] Software.	32	[std]._PHP 5.6.30 >	[E,2]Error de administrador.	[D], [I], [C].
				[E,20]Vulnerabilidades en los programas.	[I], [D], [C].
				[E,21]Error de mantenimiento - actualización de programas.	[I], [D].

Fuente: Propia

La Tabla No: 27, se identifica las Amenazas vs dimensiones el [HW] Equipamiento informático (hardware) logrando identificar la amenaza y el posible impacto sobre el activo de información para la entidad.

Tabla No: 27 Identificación Amenazas vs dimensiones [HW] Equipamiento informático (hardware) Part 1.

Tabla Rel	Tipo de Activo	ID-Activo	Activo	Amenaza	Dimensión afectada
Tabla N14	[HW] Equipamiento informático.	33	[print]._Impresora en RED Laser.(Cantidad: X)	[E,23]Errores de mantenimiento - actualización de equipos.	[D].
				[I,3]Contaminación mecánica.	[D].
				[I,5]Avería de origen físico o lógico.	[D].
				[I,6]Corte suministro eléctrico.	[D].
Tabla N14	[HW] Equipamiento informático.	34	[host]._Servidor Hypervisor	[E,23]Errores de mantenimiento - actualización de equipos.	[D].
				[A,23]Manipulación de equipos.	[C], [D].
				[A,25]Robo.	[D], [C].
				[A,26]Ataque destructivo	[D].
				[I,3]Contaminación mecánica.	[D].
				[I,5]Avería de origen físico o lógico.	[D].
				[I,7]Condiciones inadecuadas de temperatura y/o humedad.	[D].
				[N*]Desastres naturales.	[D].
Tabla N14	[HW] Equipamiento informático.	35	[vhost]._Servidor GLPI de soporte técnico	[E,2]Error de administrador.	[D], [I], [C].
				[E,21]Error de mantenimiento - actualización de programas.	[I], [D].
				[E,24]Caída del sistema por agotamiento de recursos.	[D].
				[A,24]Denegación de servicio.	[D].

Fuente: Propia

La Tabla No: 28, se identifica las Amenazas vs dimensiones el [HW] Equipamiento informático (hardware) logrando identificar la amenaza y el posible impacto sobre el activo de información para la entidad.

Tabla No: 28 Identificación Amenazas vs dimensiones [HW] Equipamiento informático (hardware) Part 2.

Tabla Rel	Tipo de Activo	ID-Activo	Activo	Amenaza	Dimensión afectada
Tabla N14	[HW] Equipamiento informático.	36	[vhost]._Servidor UTM IDS/IPS	[E,2]Error de administrador.	[D], [I], [C].
				[E,21]Error de mantenimiento - actualización de programas.	[I], [D].
				[E,24]Caída del sistema por agotamiento de recursos.	[D].
				[A,24]Denegación de servicio.	[D].
Tabla N14	[HW] Equipamiento informático.	37	[vhost]._Servidor HITS	[E,2]Error de administrador.	[D], [I], [C].
				[E,21]Error de mantenimiento - actualización de programas.	[I], [D].
				[E,24]Caída del sistema por agotamiento de recursos.	[D].
				[A,24]Denegación de servicio.	[D].
Tabla N14	[HW] Equipamiento informático.	38	[vhost]._Servidor Protocolo de transferencia de archivos	[E,2]Error de administrador.	[D], [I], [C].
				[E,21]Error de mantenimiento - actualización de programas.	[I], [D].
				[E,24]Caída del sistema por agotamiento de recursos.	[D].
				[A,24]Denegación de servicio.	[D].

Fuente: Propia

La Tabla No: 29, se identifica las Amenazas vs dimensiones el [HW] Equipamiento informático (hardware) logrando identificar la amenaza y el posible impacto sobre el activo de información para la entidad.

Tabla No: 29 Identificación Amenazas vs dimensiones [HW] Equipamiento informático (hardware) Part 3.

Tabla Rel	Tipo de Activo	ID-Activo	Activo	Amenaza	Dimensión afectada
Tabla N14	[HW] Equipamiento informático.	39	[vhost]._Servidor Soporte en almacenamiento de archivos misionales y de apoyo.	[E,2]Error de administrador.	[D], [I], [C].
				[E,21]Error de mantenimiento - actualización de programas.	[I], [D].
				[E,24]Caída del sistema por agotamiento de recursos.	[D].
				[A,24]Denegación de servicio.	[D].
Tabla N14	[HW] Equipamiento informático.	40	[vhost]._Servidor gestión de usuarios y contraseñas.	[E,2]Error de administrador.	[D], [I], [C].
				[E,21]Error de mantenimiento - actualización de programas.	[I], [D].
				[E,24]Caída del sistema por agotamiento de recursos.	[D].
				[A,24]Denegación de servicio.	[D].
Tabla N14	[HW] Equipamiento informático.	41	[vhost]._Servidor DHCP.	[E,2]Error de administrador.	[D], [I], [C].
				[E,21]Error de mantenimiento - actualización de programas.	[I], [D].
				[E,24]Caída del sistema por agotamiento de recursos.	[D].
				[A,24]Denegación de servicio.	[D].

Fuente: Propia

La Tabla No: 30, se identifica las Amenazas vs dimensiones el [HW] Equipamiento informático (hardware) logrando identificar la amenaza y el posible impacto sobre el activo de información para la entidad.

Tabla No: 30 Identificación Amenazas vs dimensiones [HW] Equipamiento informático (hardware) Part 4.

Tabla Rel	Tipo de Activo	ID-Activo	Activo	Amenaza	Dimensión afectada
Tabla N14	[HW] Equipamiento informático.	42	[host]._Estaciones de trabajo.	[E,23]Errores de mantenimiento - actualización de equipos.	[D].
				[A,23]Manipulación de equipos.	[C], [D].
				[A,25]Robo.	[D], [C].
				[A,26]Ataque destructivo	[D].
				[I,3]Contaminación mecánica.	[D].
				[I,5]Avería de origen físico o lógico.	[D].
Tabla N14	[HW] Equipamiento informático.	43	[phone]_Telefonos.	[I,5]Avería de origen físico o lógico.	[D].
				[N*]Desastres naturales.	[D].
Tabla N14	[HW] Equipamiento informático.	44	[pabx]_Servidor [PSTN]..	[E,2]Error de administrador.	[D], [I], [C].
				[E,23]Errores de mantenimiento - actualización de equipos.	[D].
				[A,26]Ataque destructivo.	[D].
				[I,3]Contaminación mecánica.	[D].
				[I,5]Avería de origen físico o lógico.	[D].
				[I,7]Condiciones inadecuadas de temperatura y/o humedad.	[D].
				[N*]Desastres naturales.	[D].

Fuente: Propia

La Tabla No: 31, se identifica las Amenazas vs dimensiones el [HW] Equipamiento informático (hardware) logrando identificar la amenaza y el posible impacto sobre el activo de información para la entidad.

Tabla No: 31 Identificación Amenazas vs dimensiones [HW] Equipamiento informático (hardware) Part 5.

Tabla Rel	Tipo de Activo	ID-Activo	Activo	Amenaza	Dimensión afectada
Tabla N14	[HW] Equipamiento informático.	45	[network] _Router	[E,2]Error de administrador.	[D], [I], [C].
				[E,23]Errores de mantenimiento - actualización de equipos.	[D].
				[A,26]Ataque destructivo.	[D].
				[I,3]Contaminación mecánica.	[D].
				[I,5]Avería de origen físico o lógico.	[D].
				[I,7]Condiciones inadecuadas de temperatura y/o humedad.	[D].
				[N*]Desastres naturales.	[D].
Tabla N14	[HW] Equipamiento informático.	46	[network] _Switches Core.	[E,2]Error de administrador.	[D], [I], [C].
				[E,23]Errores de mantenimiento - actualización de equipos.	[D].
				[A,26]Ataque destructivo.	[D].
				[I,3]Contaminación mecánica.	[D].
				[I,5]Avería de origen físico o lógico.	[D].
				[I,7]Condiciones inadecuadas de temperatura y/o humedad.	[D].
				[N*]Desastres naturales.	[D].

Fuente: Propia

La Tabla No: 32, se identifica las Amenazas vs dimensiones el [HW] Equipamiento informático (hardware) logrando identificar la amenaza y el posible impacto sobre el activo de información para la entidad.

Tabla No: 32 Identificación Amenazas vs dimensiones [HW] Equipamiento informático (hardware) Part 6.

Tabla Rel	Tipo de Activo	ID-Activo	Activo	Amenaza	Dimensión afectada
Tabla N14	[HW] Equipamiento informático.	47	[network] _Switches Acceso.	[E,2]Error de administrador.	[D], [I], [C].
				[E,23]Errores de mantenimiento - actualización de equipos.	[D].
				[A,26]Ataque destructivo.	[D].
				[I,3]Contaminación mecánica.	[D].
				[I,5]Avería de origen físico o lógico.	[D].
				[I,7]Condiciones inadecuadas de temperatura y/o humedad.	[D].
				[N*]Desastres naturales.	[D].
Tabla N14	[HW] Equipamiento informático.	48	[network] _Switches Caseros.	[E,23]Errores de mantenimiento - actualización de equipos.	[D].
				[A,26]Ataque destructivo.	[D].
				[I,7]Condiciones inadecuadas de temperatura y/o humedad.	[D].
Tabla N14	[HW] Equipamiento informático.	49	[network] _Puntos de acceso inalambrico.	[E,23]Errores de mantenimiento - actualización de equipos.	[D].
				[A,26]Ataque destructivo.	[D].
				[I,7]Condiciones inadecuadas de temperatura y/o humedad.	[D].

Fuente: Propia.

La Tabla No: 33, se identifica las Amenazas vs dimensiones de los [COM] Equipamiento informático de comunicación logrando identificar la amenaza y el posible impacto sobre el activo de información para la entidad.

Tabla No: 33 Identificación Amenazas vs dimensiones [COM] Redes de comunicaciones.

Tabla Rel	Tipo de Activo	ID-Activo	Activo	Amenaza	Dimensión afectada
Tabla N15	[COM] Redes de comunicaciones	50	[PSTN]. _Servicio de telefonía análoga.	[I,8]Fallo de servicios de comunicaciones.	[D].
				[A,6]Abuso de privilegios de acceso.	[C], [I], [D].
				[A,7]Uso no previsto.	[D], [C], [I].
Tabla N15	[COM] Redes de comunicaciones	51	[Internet]._Servicio de internet dedicado para la organización	[A,6]Abuso de privilegios de acceso.	[C], [I], [D].
				[A.7] Uso no previsto.	[D], [C], [I].
				[I,8]Fallo de servicios de comunicaciones.	[D].
Tabla N15	[COM] Redes de comunicaciones	52	[wifi]._Radio enlace local (WI-FI).	[I,8]Fallo de servicios de comunicaciones.	[D].
				[E,19]Fugas de información	[C].
				[E,23]Errores de mantenimiento - actualización de equipos.	[D].
				[E,24]Caída del sistema por agotamiento de recursos.	[D].
				[A,6]Abuso de privilegios de acceso.	[C], [I], [D].
				[A,11]Acceso no autorizado.	[C], [I].
				[A,12]Análisis de tráfico.	[C].
				[A,14]Interceptación de información (escucha).	[C].
Tabla N15	[COM] Redes de comunicaciones	53	[LAN]._Red de área local	[I,8]Fallo de servicios de comunicaciones.	[D].
				[E,19]Fugas de información	[C].
				[E,23]Errores de mantenimiento - actualización de equipos.	[D].
				[E,24]Caída del sistema por agotamiento de recursos.	[D].
				[A,6]Abuso de privilegios de acceso.	[C], [I], [D].
				[A,11]Acceso no autorizado.	[C], [I].
				[A,12]Análisis de tráfico.	[C].
				[A,14]Interceptación de información (escucha).	[C].

Fuente: Propia

La Tabla No: 34, se identifica las Amenazas vs dimensiones del equipamiento [AUX] Equipamiento auxiliar informático de comunicación logrando identificar la amenaza y el posible impacto sobre el activo de información para la entidad.

Tabla No: 34 Identificación Amenazas vs dimensiones [AUX] Equipamiento auxiliar.

Tabla Rel	Tipo de Activo	ID-Activo	Activo	Amenaza	Dimensión afectada
Tabla N16	[AUX] Equipamiento auxiliar.	54	[ups]._UPS dedicado para los servidores.	[N,2]Daños por agua.	[D].
				[I.3] Contaminación mecánica.	[D].
				[E,23]Errores de mantenimiento - actualización de equipos.	[D].
Tabla N16	[AUX] Equipamiento auxiliar.	55	[ac]._Aire acondicionado dedicado para los servidores.	[I.3] Contaminación mecánica.	[D].
				[E,23]Errores de mantenimiento - actualización de equipos.	[D].
Tabla N16	[AUX] Equipamiento auxiliar.	56	[cabling][wire]_ Cableado electrico.	[E,23]Errores de mantenimiento - actualización de equipos.	[D].

Fuente: Propia

La Tabla No: 35, se identifica las Amenazas vs dimensiones de las instalaciones [L] logrando identificar las amenazas y el posible impacto sobre el activo de información para la entidad.

Tabla No: 35 Identificación Amenazas vs dimensiones [L] Instalaciones.

Tabla Rel	Tipo de Activo	ID-Activo	Activo	Amenaza	Dimensión afectada
Tabla N17	[L] Instalaciones.	57	[building] _Sede principal (Edificio).	[N,*]Desastres naturales.	[D].
				[I,*]Desastres industriales.	[D].
				[A,11]Acceso no autorizado.	[C], [I].
				[A,26]Ataque destructivo.	[D].

Fuente: Propia

La Tabla No: 36, se identifica las Amenazas vs dimensiones del personal [P] logrando identificar las amenazas y el posible impacto sobre el activo de información para la entidad.

Tabla No: 36 Identificación Amenazas vs dimensiones [P] Personal.

Tabla Rel	Tipo de Activo	ID-Activo	Activo	Amenaza	Dimensión afectada
Tabla N18	[P] Personal.	58	[ui]_Usuario interno (Cantidad:2)	[E.7]Deficiencias en la organización.	[D].
				[E,19]Fuga información.	[C].
				[E,28]Indisponibilidad del personal.	[D].
				[A,28]Indisponibilidad del personal.	[D].
				[A,29]Extorsión.	[C], [I], [D].
Tabla N18	[P] Personal.	59	[adm]_Técnicos para administración y mantenimiento (Cantidad:2)	[E.7]Deficiencias en la organización.	[D].
				[E,19]Fuga información.	[C].
				[E,28]Indisponibilidad del personal.	[D].
				[A,28]Indisponibilidad del personal.	[D].
				[A,29]Extorsión.	[C], [I], [D].
Tabla N18	[P] Personal.	60	[sub]_Contratista de apoyo (Cantidad:1)	[E.7]Deficiencias en la organización.	[D].
				[E,19]Fuga información.	[C].
				[E,28]Indisponibilidad del personal.	[D].
				[A,28]Indisponibilidad del personal.	[D].
				[A,29]Extorsión.	[C], [I], [D].

Fuente: Propia

Adicionalmente, se identifica un análisis del riesgo latente con relación a las dimensiones de seguridad. Determinado por la posición de cada una de las facetas lo que define el nivel de criticidad que se tiene con la amenaza, de cada uno de los activos de información, lo que facilita una visión amplia y sencilla para identificar los riesgos, facilitando la decisión de cuales riesgos se van a priorizar o en qué orden se van a abordar:

La Tabla No: 37, se identifica un resumen del riesgo latente identificados con relación a las Amenazas vs dimensiones de seguridad que afectan los activos de información para la entidad.

Tabla No: 37 Resumen del riesgo latente con relación a las dimensiones de seguridad.

Contador	Dimensión afectada	Cant Dimensiones vs tipo de amenaza	Riesgos
1	[C], [A], [I].	1	1
2	[C], [D].	1	2
3	[C], [I], [D].	3	11
4	[C], [I].	1	7
5	[C].	4	10
6	[D], [C], [I].	1	6
7	[D], [C].	1	2
8	[D], [I], [C].	2	42
9	[D].	17	108
10	[I], [C], [D].	1	10
11	[I], [D], [C].	1	18
12	[I], [D].	1	25
13	[I].	1	2
Total		35	244

Disponibilidad (D). Integridad (I). Confidencialidad (C). Autenticidad (A). Trazabilidad (T).

Fuente: Propia

En esta tabla anterior, se puede identificar que la faceta con mayor índice de afectación es la de Disponibilidad [D] un total de 17 tipos de amenazas para un total de 108 riesgos que podrían afectar la entidad, le sigue Confidencialidad [C] con 4 tipos de

amenazas con un total de 10 riesgos y en tercer lugar [C], [I], [D] con 3 tipos de amenazas con un total de 11 riesgos. Lo que evidencia que la afectación más relevante hasta este punto es la disponibilidad.

8. METODOLOGÍA PARA EL ANÁLISIS DE RIESGOS, PARA ENTIDADES PÚBLICAS DEDICADAS A PROMOVER LA CIENCIA, TECNOLOGÍA E INNOVACIÓN TECNOLÓGICA DE LA CIUDAD DE CALI

En las entidades públicas dedicadas a promover la ciencia, tecnología e innovación tecnológica de la ciudad de Cali. Se sugiere implementar una metodología para el análisis de riesgos que contribuya a la aplicación de medidas de prevención para evitar peligros potenciales o reducir su impacto en la infraestructura TI de las entidades, que sea simple sin perder el nivel de importancia.

8.1. Metodologías existentes

A partir del estado actual a modo general es posible encontrar en las entidades públicas dedicadas a promover la ciencia, tecnología e innovación tecnológica en la ciudad de Cali, se hace necesario identificar algunos modelos ya existentes para la gestión de riesgos en TI como por ejemplo: CRAMM, COBIT 5, ITIL, ISO/IEC 31000:2018, MAGERIT, OCTAVE de los cuales se identificara el que se perciba como el más idóneo con relación a la capacidad operativa de este tipo de entidades, que típicamente cuenta con un técnico o ingeniero de infraestructura de tecnologías de información o afines, más un auxiliar o contratista para actividades de apoyo, lo que implica que el modelo debe de ser lo más intuitivo , simple y que se pueda alinear con los controles que propone al ISO/IEC 27001 en su Anexo A, dado que el estado en la actualidad apunta a establecer garantías de seguridad y privacidad de la información basados en la ISO 27001.

CRAMM: "El método CRAMM (Método de análisis y gestión de riesgos CCTA) es una metodología destinada a la gestión de riesgos. CRAMM, que hoy pertenece a las metodologías con mayor aplicación en el análisis y gestión de riesgos, fue desarrollado en base a las necesidades de la agencia gubernamental británica CCTA en 1985."[20]

[20]Management Mania. (s. f.). *CRAMM (CCTA Risk Analysis and Management Method)*. ManagementMania.com. Recuperado, de https://managementmania.com/en/cramm-ccta-risk-analysis-and-management-method

CRAMM, la versión que se encuentra vigente en la actualidad es la 5.2, se define como una metodología enfocada para el análisis y de la gestión de los riesgos, siendo aplicable a todas las etapas presentes en el ciclo de vida de los sistemas de información.

CRAMM es apoya por una aplicación que se denomina con el mismo nombre, ayudando a recopilar información para generar informes que se basan en evaluaciones cualitativas y cuantitativas logrando identificar los riesgos, pudiendo aplicar los distintos conceptos formales , sistemáticos, disciplinados , estructurados y reproducibles con el objeto de proteger los tres principios de la seguridad y privacidad de la información como lo son, la confidencialidad, integridad y la disponibilidad de un sistema con sus activos, logrando ser implementado en todos los tipos de sistemas de información, lo que incluye las redes de datos durante la etapa del análisis de factibilidad, es decir, incluye la capacidad técnica, operativa y financiera, en donde se enmarque los altos riesgos de seguridad, sirviendo para la identificación de los requisitos generales enfocados en la seguridad, el plan de contingencia , garantías de continuidad, plan de negocio y de continuidad con sus respectivos costos asociados a cada una de las distintas opciones sugeridas, entonces CRAMM puede ayudar a demostrar la efectividad de los costos asociados para la implementación de la gestión de los riesgos y de la planificación de las contingencias en caso de emergencia, lo que lo hace idóneo para trabajar con profesionales relacionados a directores de riesgo y los administradores de riesgos, en consecuencia es ideal para trabajar en el campo de la gestión de los riesgos como en la gestión de la seguridad,

Para lograr un resultado idóneo con el objeto de segurizar la continuidad del negocio se puede incluir elementos que van desde la identificación de activos de información, sus riesgos, amenazas, vulnerabilidades con sus salvaguardas relacionadas, su implementación y auditoria,

Lo anterior implica que CRAMM es posible relacionarlo con los métodos y términos como: la gestión en la continuidad del negocio, plan de negocio de continuidad, contramedidas, controles o salvaguardas, plan de emergencia o contingencia, SGSI, la ISO 27001, Los riesgos, las amenazas y las vulnerabilidades, aunque para CRAMM “a su vez, tiene un enfoque más práctico, pues su base de referencia es la ISO 27002, y contempla además los fundamentos de la ISO 27005 e ISO 31000”[21]

[21]Gestión de riesgo tecnológico de las MPYMES ecuatorianas 45 (s. f.). Recuperado 5, de https://1library.co/article/gesti%C3%B3n-riesgo-tecnol%C3%B3gico-mpymes-ecuatorianas.zgg0jwnz

MAGERIT: Es un método creada y coordinación de contenidos por "Dirección General de Modernización Administrativa, Procedimientos e Impulso de la Administración Electrónica"[22] en Madrid, octubre del 2012 en su versión 3, en donde se considera la gestión del riesgo como el punto focal para la elaboración de guías de buen gobierno, con el objeto de mitigar los riesgos en la implementación y del buen uso de las tecnologías de la Información dirigido especialmente al sector público , adicionalmente es de reconocer que es una metodología de uso libre conocida como MAGERIT que viene del acrónimo Metodología de Análisis y Gestión de Riesgos de la Información , apoya la necesidad de evidenciar el nivel de seguridad o inseguridad que tenga un sistema de información, es decir, es el método formal documental que sirve para investigar los riesgos a los que está asociado un sistema, dichos riesgos sirven como insumo para poder sugerir las medidas de control que se deberían de adoptar para poder controlar los riesgos, lo que incide en la gestión de la seguridad.

Ahora con MAGERIT "Si hablamos de Gestión global de la Seguridad de un Sistema de Seguridad de la Información basado en ISO 27001, MAGERIT, es el núcleo de toda actuación organizada en dicha materia, ya que influye en todas las fases que sean de tipo estratégico y se condiciona la profundidad de las fases de tipo logístico"[23]

Además, MAGERIT considera en toda instancia el hardware, el software, la data como por ejemplo toda información electrónica, el recurso humano, entre otros, como actores activos en el sistema que generan, producen, emiten y consumen información, bajo la primicia que para cualquier entidad tanto en el ámbito privado, como en el ámbito del sector público, la información tiene un valor económico. Como por ejemplo en la Unidad Administrativa de Impuestos y Rentas, es vital la base de datos de los contribuyentes.

En relación a lo anterior, propiciando que magerit sea un instrumento idóneo que facilita la aplicación e implementación de medidas de seguridad, sugiriendo los principios básicos y de los requisitos mínimos para proteger de forma más acertada de proteger la información, con el objeto de concientizar a los responsables de los sistemas de información , sobre la existencia de riesgos y de la necesidad de mitigarlos hasta obtener un nivel aceptable y asumible de los riesgos, Ofrecer una metodología sistemática para lograr ejecutar un adecuado analices del riesgo en la entidad el cual parte de la necesidad de proteger la misión con relación a las dimensiones de seguridad, Identificar y planificar los controles en forma oportuna

[22]Administracionelectronica.gob.es. (2012). *MAGERIT versión 3 Libro I Método (versión española): Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. (10.)*. https://administracionelectronica.gob.es/pae_Home/dam/jcr:fb373672-f804-4d05-8567-2d44b3020387/2012_Magerit_v3_libro1_metodo_es_NIPO_630-12-171-8.pdf , p.2

[23]Pineda, N., & Orlando, E. (s. f.). Análisis de riesgos: proceso, regulaciones y metodologías. 12.p.7

para lograr controlar los riesgos, preparar a la entidad para actividades de evaluación , auditoria y una posterior certificación o de una acreditación en dependencia de la necesidad de la entidad, todo lo anterior mencionado con la necesidad de proteger los tres principios de la seguridad en la información como lo es la Disponibilidad, dado que la falta de esta dimensión reflejaría la carencia del servicio, lo que incide directamente en la productividad lo que limita el cumplimiento de su misión y por ende cumplir con su objeto social, Integridad la ausencia de esta dimensión reflejaría la falta de completitud y adecuada actualización de la información, es decir; indicaría que la información ha sido alterada o eliminada, afectando el correcto desempeño de la entidad, Confidencialidad la carencia de esta dimensión de seguridad indicaría que se está presentado posiblemente fugas y/o accesos no autorizados de la información, es de comprender que esta dimensión es un cualidad que afecta la reputación de la entidad, por tanto es muy difícil de recuperar, dado que afecta la confianza que refleja a nivel externo , indicando que no es diligente en cuanto al manejo de la confidencialidad lo que implica posiblemente el incumplimiento de algunas leyes y de compromisos contractuales entre las partes interesadas con relación a la custodia de la información o datos.

De modo que, MAGERIT es posible relacionarlo con los métodos y términos como: Buen Gobierno, confianza, análisis y gestión del riesgo, tratamiento del riesgo, concientización, formación, incidencias, recuperación, orden de las guías, evaluación, certificación, auditoria, acreditación, identificación de activos, identificación de amenazas, impacto potencial, riesgo potencial, salvaguardas, impacto residual, riesgo residual, entre otros.

MAGERIT también se basa en la ISO 27005 también se basa en la ISO 31000, dado que administra y trata los riesgos aplicando salvaguardas y controles para la protección de claves, el software, el hardware, las comunicaciones y los servicios.

COBIT 5: es utilizado para “optimizar el costo de los servicios de TI y la tecnología, a través de la integración de un sistema operativo mejorado de TI. Proporcionando una visión clara de los roles y responsabilidades internas dando así a una organización una ventaja competitiva”[24].

Entonces COBIT 5 es un marco de trabajo que fue desarrollado para ayudar a las entidades en ganar un valor idóneo de TI en conexidad con los beneficios, bajo el uso

[24]Pineda, N., & Orlando, E. (s. f.). Análisis de riesgos: proceso, regulaciones y metodologías. 12.P.7

de los recursos y de los niveles de riesgo aceptables y asumibles por la alta gerencia en representación de los beneficios de la entidad, tomando en consideración el objeto social del negocio y todas las áreas funcionales como los interesados internos y externos. Algunas guías del estado nacional colombiano bajo el MINTIC principalmente la del desarrollo del PETI plan estratégico de tecnologías de la información obedecen al reconocimiento de los datos antes mencionados, lo que hace que COBIT 5, sea considerado como una opción para enmarcar la forma de trabajar la gestión de tecnologías de la información, con el objeto de lograr evaluar el estado actual de las tecnologías de la información TI en la entidad.

Con relación a lo anterior bajo el marco de COBIT 5 la entidad debería de seguir los cinco principios en adopción de la gestión de TI:

Persecución de valor basado en las necesidades de los accionistas: es necesario alinear las necesidades de los accionistas con la necesidad del cumplimiento del objeto social de la entidad.

Orientado al negocio de la entidad: se debe asumir desde un punto de vista global la gestión de TI y el Gobierno de TI, para que de alcance a todas las necesidades corporativas.

Aplicar modelo de referencia considerando la integración con los mejores marcos de sistemas de auditoría de información y asociación de controles como Val IT para trabajar con los procesos de COBIT y para dar un valor agregado se trabajaría con Risk IT desarrollado por la ISACA logrando un balance con relación a los riesgos vs beneficios, de la misma forma puede considerar el uso de BMISS modelo de negocio para la seguridad de la información, por otra parte también permite una adecuada alineación con los principales marcos de trabajo como ITIL, TOGAF, PMBOK, PRINCE2, COSO y estándares ISO.

Interrelación bajo enfoque holístico: desde un punto de vista global la gestión de TI y el Gobierno de TI es necesario que trabajen en función del objeto social del negocio, es decir la misión.

Separar pero interrelacionar el gobierno de la gestión de TI: debe de haber una distinción entre la gestión de TI y el Gobierno de TI y sus funciones relacionadas con la dirección , evaluación, auditoria y el monitoreo de las tecnologías de la información (TI), para asegurar el alcance de los objetivos alineados con las necesidades de los socios,

así como las condiciones y las opciones inherentes a TI, lo que puede influir en la priorización incidiendo en la toma de decisiones, en contraparte el monitoreo evalúa el cumplimiento mediante el nivel de desempeño en función de los objetivos corporativos acordados, bajo un enfoque de gestión lo que está relacionado con la ejecución, construcción y el monitoreo de las actividades pactadas con la entidad.[25]

ITIL:" Es un marco de mejores prácticas para la prestación de servicios de TI. El enfoque sistemático de ITIL para la gestión de servicios de TI puede ayudar a las empresas a gestionar el riesgo, fortalecer las relaciones con los clientes, establecer prácticas rentables y construir un entorno de TI estable que permita el crecimiento, la escala y el cambio."[26]

En la actualidad ITIL llega del acrónimo Information Tecnology Infraestructure Library, es decir Biblioteca de infraestructura de tecnologías de la información, Entonces a nivel general ITIL es el marco de referencia o de buenas prácticas que es más usado en la actualidad a nivel mundial y es certificable, donde se certifican a las personas mas no las empresas.

ITIL surge en los años 80´S en el reino unido gracias al trabajo de la Agencia central de Comunicaciones que se conoce con el Acrónimo CTTA, quien se llevaron a la tarea de crear e implementar un servicio de para los equipos de TI, para los años 80´s no había ninguna referencia, solamente podían referirse en cuanto al desempeño, pero también se requería que relacionara lo financiero.

En relación a lo anterior ITIL necesito evolucionar, por eso en 1989 lanzó sus primeros libros y estos fueron conocidos como British Standards, luego entre 1990 a 1999 ITIL público su primera (1) versión , en donde se lograba establecer estándares más amplios donde acogía las mejores prácticas en IT para la época, {después entre los años 2000 a 2007 publica su versión dos (2) se convierte en un estándar más accesible, luego entre los años 2007 a 2018 lanza la versión tres (3) en donde ITIL asume un enfoque basado en el ciclo de Vida lo cual es ideal para la integración empresarial en TI, en donde se proponen cinco (5) etapas para el ciclo de vida de los sistemas de TI para el servicio, lo que cubre, Etapa de estrategia del servicio, Etapa de Diseño del servicio,

[25]¿Qué es COBIT 5? Entendiendo el Gobierno de TI ó IT Governance. (2018, enero 24). *Genius IT Training*. https://geniusitt.com/blog/que-es-cobit-5/

[26]Greiner, S. K. W. and L. (2019, enero 18). *What is ITIL? Your guide to the IT Infrastructure Library*. CIO. https://www.cio.com/article/2439501/infrastructure-it-infrastructure-library-itil-definition-and-solutions.html

Etapa de Transición del servicio, Etapa de Operación del servicio y por último la Etapa de Mejora continua para el servicio, Por ultimo entre los años 2019 hasta el día de hoy llega ITIL en su versión cuatro (4), en donde se acogen las complejas demandas modernas propiciadas a partir del internet de las cosas, en donde se interconectan de manera compleja los negocios que hoy en día están globalizados, una de sus ventajas es que no requiere de profesionales dentro de las organizaciones en su transición digital, dato a tener en cuenta , los procesos que se aplicaban hasta la versión tres (3) de ITIL , en su versión cuatro (4) cambiaron de la definición de ser procesos a ser prácticas.

Ahora dentro de ITIL en su versión cuatro (4), afloran nuevos conceptos como:

Valor del servicio: se plasma en conjunto las actividades y los componentes que posiblemente se tengan en una entidad, los cuales participan en la creación del valor agregado por medio de los servicios que se ofrecen por el departamento de TI, en donde se siguen los principios guía, los cuales contienen las recomendaciones que posiblemente guían a la entidad en un abanico de circunstancias sin importar si las metas enfrentaron cambios relacionados con la estrategia, estructura de la estrategia o en el tipo de trabajo para el análisis de un trabajo o lograr el alcance de uno o los objetivos

Gobierno o Gobernanza: es el medio por el cual la entidad se encuentra dirigida y controlada.

Prácticas de ITIL: hace referencia a un conjunto de recursos corporativos y organizativos que fueron diseñados.

Mejora Continua: Es una actividad de tipo organizativa y recurrente que es ejecutada en todos los niveles de la entidad lo que propicia que el rendimiento logre satisfacer de las partes interesadas,

Entonces ITIL opera bajo cuatro (4) Dimensiones con enfoque Heolistico lo cual es requerido para cualquier tipo de entidad, con el objeto de ofrecer un servicio de forma sistemática, entonces estas dimensiones son:

Dimensión Organizaciones y personas:

Dimensión Información y tecnología.

Dimensión Socios y proveedores.

Dimensión Flujos de Valor y procesos.

Las anteriores dimensiones son influenciadas por diversos factores tipo político, económico, tecnológico y legislativo.

Con relación a lo anterior la cadena de valor propicia en tener una consideración con relación a tener lo necesario para una correlación de servicios, donde cada una de las actividades operan en conexidad en la entidad para la entrega de un producto que también puede ser un servicio dirigido hacia su público objetivo o consumidor final lo que facilita la creación de un mayor valor Partiendo de las siguientes actividades Planificar, a partir de comprender la visión, la dirección de las dimensiones y el estado actual, Mejorar a partir del ejercicio de la mejora continua de los productos teniendo en cuanta que el servicio también es un producto, Involucrar actividades que ayudan a comprender las necesidades requeridas de las partes interesadas propiciando transparencia y buenas relaciones entre las partes, lo que ayuda a convertir los requisitos en diseños de transición, Diseñar ejecuta actividades de diseño de transición propiciando que los productos incluyendo los servicios den cumplimiento con las expectativas de las partes interesadas, siempre teniendo en cuanta la calidad , el costo con relación al tiempo de comercialización, Obtener y construir, a partir de la gestión financiera, gestión de portafolios de servicios, gestión de demanda , con el objeto de poder diseñar el servicio con ITIL y así poder gestionar el catálogo de servicios , establecer y gestionar niveles de servicio (SLA), gestión de capacidad, gestión de disponibilidad, gestión de continuidad, gestión de proveedores hasta llegar a la gestión de la seguridad de la información, y así lograr una adecuada Gestión de cambios, gestión de configuración de activos del servicio, de igual forma gestionar las versiones y despliegues, validación y pruebas de servicio, gestión de problemas, gestión de accesos, entre otros, todos dando cumplimiento al ciclo PHVA el ciclo de mejora continua en los sistemas de información.[27]

ISO/IEC 31000:2018: El comité de la ISO, público en el año 2018 la nueva versión de ISO 31000:2018 la cual “proporciona directrices para gestionar el riesgo al que se

[27]Introducción a ITIL V3 | Definición ITIL. (2016, mayo 24). *ServiceTonic*. https://www.servicetonic.com/es/itil/introduccion-a-itil-v3/

enfrentan las organizaciones. La aplicación de estas directrices puede adaptarse a cualquier organización ya su contexto […] proporciona un enfoque común para gestionar cualquier tipo de riesgo y no es específico de una industria o un sector"[28]

Entonces la adopción de gestión del riesgo se convierte en una decisión en la entidad con el objeto de optimizar el desempeño global bajo la introducción de desarrollo y ejecución de iniciativas, propiciando una serie de posibles beneficios en la entidad en caso de tomar la decisión de implementar la gestión del riesgo tomando como base la norma internacional ISO/IEC 31000:2018, las cuales se enumerarán en forma general a continuación:

La gestión del riesgo es dinámica logrando participar en la implementación de estrategias acordes a las necesidades, para dar cumplimiento a los objetivos trazados por la entidad.

La gestión del Riesgo es necesaria en todos los niveles de la entidad haciendo parte de la gobernanza, y del liderazgo propositivo y participativo que contribuya en el perfeccionamiento de los sistemas de gestión.

La gestión del riesgo comprende la correlación entre las partes interesadas y al mismo tiempo hace parte a todas las actividades asociadas a la misión u objeto social de la entidad.

Lo anterior contempla que es el marco de referencia de la gestión del riesgo bajo el estándar internacional ISO/IEC 31000:2018 logrando englobar Generalidades, liderazgo y compromiso de igual forma se enmarcan actividades de integración, el Diseño, la implementación, la auditoria o evaluación y por último la mejora, lo que implica que es posible trabajar con el ciclo PHVA, propiciando que sea compatible con otros estándares o modelos de gestión del riesgo.

Lo anterior se logra a partir de unos principios globales compatibles para cualquier tipo de entidad como lo es la capacidad de ser integrada, ser personalizada en forma

[28]Rodríguez, M. F. M. (s. f.). *NORMA TÉCNICA NTC-ISO COLOMBIANA 31000 GESTIÓN DEL RIESGO. DIRECTRICES*. Recuperado, de https://www.academia.edu/40418832/NORMA_T%C3%89CNICA_NTC_ISO_COLOMBIANA_31000_GESTI%C3%93N_DEL_RIESGO_DIRECTRICES

estructurada, incluyente, dinámica propiciando la mejor información posible para la toma de decisiones interviniendo de forma armónica en el factor humano, cultural propiciando el mejoramiento continuo en la entidad.

Para lograr lo anterior la gestión del riesgo bajo la ISO/IEC 31000:2018 debe de implementar una serie de actividades como:

- La Comunicación y Consulta.
- Definición de un alcance.
- Establecer el Contexto.
- Establecer Criterios.
- Identificación del o los riesgos.
- Definir la valoración del riesgo.
- Definir el tratamiento del riesgo.
- Definir las actividades de control, monitoreo y revisión.
- Elaboración de Registro.
- Elaboración de Informes.

Estas herramientas son necesarias para lograr diseñar e implementar bajo la perspectiva de prevenir con la gestión del riesgo, aplicable a cualquier tipo de entidad o proyecto, de la misma forma puede servir como apoyo al sistema de gestión que ya tenga establecido, participando de tal forma en la mejora continua.

OCTAVE: llega del acrónimo en inglés **Operationally Critical Threat, Asset and Vulnerability Evaluation, o en español Evaluación de Vulnerabilidades, Activos y Amenazas Operativamente Críticas,** "es un marco de seguridad para identificar, abordar y gestionar evaluaciones de seguridad de la información y planificación basada en riesgos. Consiste en herramientas, tecnologías y procedimientos para ayudar a las organizaciones a identificar y evaluar los riesgos de seguridad que enfrentan. OCTAVE está dirigido principalmente a los riesgos de seguridad relacionados con la organización más que a los riesgos tecnológicos"[29]

[29] *What is an Operationally Critical Threat, Asset and Vulnerability Evaluation (OCTAVE)? - Definition from Techopedia*. (s. f.). Techopedia.com. Recuperado, de http://www.techopedia.com/definition/21133/operationally-critical-threat-asset-and-vulnerability-evaluation-octave

Fue desarrollado por el instituto Ingeniería de Software, Universidad Carnegie Mellon con el objeto de abordar los desafíos de seguridad y riesgos para el departamento de defensa de EE. UU definiendo una metodología para evaluación integral, lo que permite hoy en día a las entidades, en principio identificar los activos de información que están directamente relacionado con el cumplimiento del objeto social de la entidad, es decir con la misión institucional, en consecuencia se logra identificar las amenazas y vulnerabilidades que afectan dichos activos, por tanto la entidad cambia sus estado de conciencia al comprender que información está en riesgo y es relevante para iniciar actividades de diseño de estrategias para proteger dichos activos minimizando la exposición al riesgo, para lograrlo OCTAVE opera en tres fases:

Creación de perfil basado en las amenazas de los activos: En esta fase se trabaja en la identificación de los activos de información que son críticos para el objeto social de la entidad, se establecen sus prerrequisitos de seguridad, lo que sirve para crear un perfil basado en las amenazas, para cada uno de los activos.

Identifica vulnerabilidades en la Infraestructura de red: En esta fase se reconoce rutas para el acceso de la red, se reconocen cada uno de los elementos tecnológicos que se encuentran vinculados a los activos críticos, y se reconoce hasta que puntos esos elementos son seguros contra irrupción no autorizada hacia la red.

Desarrollo de estrategia y plan de seguridad: Tomando como insumo los datos recopilados previamente en las anteriores fases, con el objeto de diseñar un plan formal, donde se evidencian las acciones necesarias para afrontar cada uno de los riesgos que están vinculados a los activos críticos de la entidad.

Este tipo de entidades por lo general conocidas como entes descentralizados , son entidades de tipo públicas que pueden tener dependencia económica por parte del estado, sin embargo también pueden tener aportes o capital de tipo privado sin excluirlos de sus responsabilidades legales y normativas generales y particulares con relación al objeto social, en consecuencia es posible que su presupuesto aun que las tecnologías de la información a pesar que son transversales a todos los procesos o departamentos en las entidades, es probable que su inyección anual de presupuesto sea limitada, por tanto en principio la metodología MAGERIT es un método que podría ser aplicado a este tipo de entidades, dado que MAGERIT es de uso público y puede ser utilizada de forma libre, presenta una serie de ventajas que incluyen lo “que” busca el (Activo de Información) representa el que se quiere securizar o proteger, posteriormente indicar “como” se protege, en consecuencia, a partir del ESTADO ACTUAL y con los insumos de información que se puede proyectar, es posible realizar actividades de reconocimiento de impacto de los riesgos latentes, mediante la

identificación de las amenazas vs la dimensiones de seguridad, apoyado en Magerit que a su vez se apoya en la normativa ISO 31000 en respuesta a la gestión del riesgo[30], logrando plantear contramedidas o pautas a considerar para preservar la seguridad de la información, pudiendo incluso evidenciar la necesidad de introducir nuevas políticas que estén dirigidas a preservar la continuidad del negocio aplicable al ciclo PHVA, por tanto se sugiere considerar el uso de MAGERIT.

8.2. Metodología para el análisis de riesgos

Teniendo en cuenta lo anterior y sabiendo que las entidades públicas dedicadas a promover la ciencia, tecnología e innovación tecnológica de la ciudad de Cali, posiblemente solo cuentan con personal técnico o en su defecto con poco personal del área de Sistemas de información y/o telemática, dicha metodología debe de ser capaz de abstraer de forma simple , respetando su nivel de importancia y orientada al cumplimiento de los procesos de análisis e identificación de los riesgos de TI, en cumplimiento de los requerimientos de seguridad y privacidad de la información , que sirva como insumo para la elaboración del PETI Plan estrategia de Tecnologías de la Información y el PESI Plan Estratégico de seguridad de la información, planes que en la actualidad se les exigen a las entidades públicas en general pero en este caso enfocadas a entidades públicas dedicadas a promover la ciencia, tecnología e innovación tecnológica de la ciudad de Cali que son participes de los denominados entes descentralizados, bajo el uso de la metodología MAGERIT en conexidad con la norma iso/iec 27001:2013 y la gestión del riesgo iso/iec 31000.

Bajo un enfoque de lograr la simplicidad sin perder la importancia que refiere en estos tiempos una adecuada gestión del riesgo, esta se subdivide en dos tareas Importantes: Primero el análisis de los riesgos, y luego el tratamiento de los riesgos. Es decir, el análisis de los riesgos con relación a los activos, amenazas y las salvaguardas.

Lo anterior permite determinar el estado inicial o actual de las entidades públicas dedicadas a promover la ciencia, tecnología e innovación tecnológica de la ciudad de Cali, pudiendo servir como base de conocimiento para estimar lo que podría pasar en caso que un riesgo se materialice.

[30] administracionelectronica.gob.es. (2012). MAGERIT versión 3 Libro I Método (versión española): Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. (10.). https://administracionelectronica.gob.es/pae_Home/dam/jcr:fb373672-f804-4d05-8567-2d44b3020387/2012_Magerit_v3_libro1_metodo_es_NIPO_630-12-171-8.pdf , p.7

Con relación al tratamiento de los riesgos permite minimizar los riesgos hasta un nivel aceptable, asumible, pactado y aprobado por la alta dirección, logrando así, el cumplimiento del objeto social en las entidades públicas dedicadas a promover la ciencia, tecnología e innovación tecnológica de la ciudad de Cali.

8.3. Riesgo por tratar

Cada uno de los riesgos que se identificaran y como consecuencia de su hallazgo, se dará tratamiento también su correspondiente valoración en cuanto a probabilidad de materialización del riesgo y su impacto siendo definido a partir de la metodología MAGERIT, por medio del cual se identifica los niveles de aceptación como lo son: aceptable, moderado e inaceptable.

Lo anterior prospera a partir de una valoración que es subjetiva sin embargo debe de ser una valoración lo más imparcial posible, evitando caer en una actividad de inflar o minimizar cifras a discreción del analista (Auditor) o el entrevistado.

En consecuencia, al identificar el riesgo, se le otorgara un nivel, a su vez identificara su importancia o criticidad frente al sistema de información, por tanto, a nivel cuantitativo se tratarán los riesgos cuyos niveles se encuentren entre 16 a 26 siendo inaceptables:

(I), además que tenga un impacto que esté relacionado como alto o muy alto.

Con relación a lo anterior se sugiere una paramétrica intuitiva, simple sin perder su importancia, rindiendo una clasificación e identificación de los riesgos:

1. **Es necesario identificar o definir la estructura organizacional de la entidad así:**

Identificación de Organigrama: Cada uno de los procesos de la Entidad debe de ser descriptos mediante un mapa jerárquico que indique los distintos procesos (Departamentos) mediante un organigrama de la entidad, para identificar la dependencia de cada Uno y ayudar a esclarecer su nivel de importancia dentro de la Organización.

- **Es necesaria documentar las dependencias de cada área (proceso o Departamento.**

Con relación a la información contenida en el anterior organigrama de la entidad pública dedicada a promover la ciencia, tecnología e innovación tecnológica en la ciudad de Cali es necesario identificar lo siguiente:

NOTA: Algunas entidades clasifican los departamentos operativos de la entidad como procesos, en consecuencia, cuando se habla de procesos de debe de interpretar bajo el contexto que se redacta, pudiendo ser proceso como departamento, o proceso como actividad a desarrollar.

Área Dependencia: Corresponde a la dependencia o subdirección que corresponde el proceso o departamento, Corresponde al proceso o departamento.

Composición: Descripción general de los servicios, equipamiento que componen el departamento y que está relacionado con la infraestructura de TI.

Funciones: La función general y relevante que cumple el departamento y que esté relacionado o necesite apoyo de la infraestructura de TI.

Se sugiere hacer uso del siguiente cuadro, el cual debe de ser avalado para este tipo de entidades por el departamento de planeación, y aprobado por la alta gerencia, de lo contrario preservarlo como documentación de la actividad.

La Tabla N 38, se identifica un resumen con Información General de las dependencias para la entidad, reconocimiento necesario para identificar los procedimientos funcionales que ayudan a cumplir con el objeto social de la entidad.

Tabla N 38 Información General de las dependencias.

Área Dependencia	Composición	Funciones Generales
Junta Directiva	A nivel general puede variar en dependencia de la entidad, se compone en principio por el gerente General en apoyo de los líderes que intervienen en el cumplimiento del objeto social de la entidad, y de los responsables de propender en el Cumplimiento de los requerimientos gubernamentales y particulares propios de la actividad social de la entidad.	Validar, Analizar y Tomar decisiones que propicien el cumplimiento de los requerimientos gubernamentales y particulares en relación al objeto social de la entidad entre los cuales se incluye, negociación de recursos y apoyos necesarios, garantizando la continuidad del negocio en beneficio de la comunidad caleña.
Dirección General	Despacho jurídico, Oréganos de Asesoría y coordinación, control interno, planeación, comunicaciones, mercadeo, Subdirección administrativa (operativa) y financiera, subdirección técnica (misional)	A nivel general se Compone en apoyo de los siguientes comités, Institucional y desempeño, Institucional de control interno, comisión personal
Subdirección técnica (Misional).	Típicamente puede variar en relación a la entidad, se compone de grupos de trabajo que están relacionados directamente con la Misión o el objeto social de la entidad, lo que incluye procesos de servicios, investigación y actos sociales en beneficio de la sociedad	Misionales son los departamentos que trabajan en torno al cumplimiento de las actividades particulares en relación al objeto social de la entidad, en beneficio de la sociedad.
Subdirección Financiera y administrativa (Operativa).	Típicamente puede variar en relación a la entidad, se compone de grupos de trabajo (procesos, departamentos, Talento Humano (RH), Gestión Financiera, Gestión Administrativa, Gestión de TI, es decir todos los equipos que apoyan el cumplimiento de las actividades misionales de la entidad.	Apoya los procesos misionales facilitando el Cumplimiento de las actividades particulares que proponen los grupos misionales, en beneficio de la sociedad.

Fuente: Propia

Al validar la información de la estructura general con sus funciones generales, se logra evidenciar la existencia o no de un departamento de TI en la entidad. De manera general, es posible que no exista un comité de TI en cabeza de la alta gerencia, que actué en el marco de TI para la gestión del riesgo, no obstante, las actividades de mejora y seguridad en TI son incluidas en las sugerencias de los demás comités.

Todo esto, puede generar dificultades en la gestión del Riesgo específicamente para infraestructura de red de telecomunicaciones dentro de la entidad, dado que los demás comités se enfocan en la evaluación de desempeño, control interno y evaluaciones del personal en el marco del cumplimiento de las metas trazadas para cada vigencia con relación a su enfoque, por tanto es posible que se propicie que el apalancamiento de los proyectos de gestión de Riesgo en cuanto a planes de TI, su enfoque sea minimizado al no ser el objeto de trabajo especializado de cada comité, lo que a su vez es posible que genere fallas en la mitigación de riesgos, por tanto es recomendable que en apoyo de las tecnologías informáticas de las entidades públicas dedicadas a promover la ciencia, cultura, tecnología e innovación tecnológica de la ciudad de Cali, es decir el departamento de TI bajo una adecuada dirección y control en la entidad, propicie la creación de un comité de TI, en cualquier caso se cree o no el comité, el área de TI debe apoyar el cumplimiento de las actividades de los funcionarios, en consecuencia a lo anterior se revela la gran importancia que tiene una idónea gestión del riesgo para TI.

- **Es necesaria documentar las dependencias de cada área (proceso o Departamento.**

Con relación a la información contenida en el organigrama de la entidad pública dedicada a promover la ciencia, tecnología e innovación tecnológica en la ciudad de Cali, es necesario presentar de forma general la planta de cargos de la entidad.

Se sugiere hacer uso del siguiente cuadro, el cual debe de ser avalado para este tipo de entidades por el departamento de planeación, y aprobado por la alta gerencia, de lo contrario preservarlo como documentación de la actividad.

Para diligenciar el Siguiente cuadro se sugiere hacer una entrevista con el funcionario a cargo o si no está presente tomar nota a partir del manual de funciones de la entidad.

NOTA: para esta parte de la documentación no se requiere del nombre del responsable del cargo.

Dependencia: Nombre de la dependencia a la que está adscripta el cargo.
Denominación del cargo: Nombre del cargo
Nivel: Facilita la comprensión de la jerarquía del cargo dentro de la entidad.

La siguiente tabla recopila información relevante a la planta de cargos Esta basada en un contexto general para este tipo de entidades.

La Tabla N 39, se identifica a nivel General la planta de cargos de las dependencias para la entidad, reconocimiento necesario para identificar la cantidad de funcionales que ayudan a cumplir con el objeto social de la entidad.

Tabla N 39 Planta de cargos a nivel general

Código	GRADO	Cantidad Cargos.	Dependencia	Denominación del cargo	Nivel
50	1	1	Dirección General	Director General	Directivo
105	1	1	Dirección General	Asesor	Asesor
9	1	3	Dirección General	Director control interno, técnico, Administrativo y Financiero	Directivo
222	3	1	Dirección General	Profesional Especializado	Profesional
319	1	5	Subdirección Financiero y administrativo	Profesional Universitario	Profesional
314	3	3	Subdirección Técnica	Técnico Operativo.	Técnico
314	2	3	Subdirección Técnica	Técnico Operativo.	Técnico
314	1	6	Subdirección Financiero y administrativo	Técnico Operativo.	Técnico
425	6	1	Dirección General	Secretario Ejecutivo	Asistencial
407	4	4	Subdirección Financiero y administrativo	Auxiliar Administrativo	Asistencial
407	3	16	Subdirección Técnica	Auxiliar Administrativo	Asistencial
407	2	6	Subdirección Financiero y administrativo	Auxiliar Administrativo	Asistencial
407	1	9	Subdirección Técnica	Auxiliar Administrativo	Asistencial
Total, funcionarios posiblemente aproximados de planta para entidad pública dedicada a promover la ciencia, tecnología e innovación tecnológica en la ciudad de Cali				**59**	

Fuente: Propia

NOTA: para la anterior tabla se revisaron vía internet organigramas y planta de cargos y se tomó como referencia la entidad que contara con un abanico más amplio de cargos que posiblemente acoja las demás entidades, que posiblemente también encajen dentro del segmento de entes descentralizados.

De la Anterior Tabla se puede profundizar en un contexto general en lo siguiente:

Director (gerente) Directivo:

Representante legal, celebrar contratos, actos y nombramientos, podrá designar apoderados en caso de requerir representante judicial y/o extrajudicial, apoderados en beneficio de la entidad, y guiar la entidad dirigiendo sus políticas institucionales en la adopción de planes, proyectos incluyendo programas.

Subdirector Financiero y administrativo Directivo:

Garantiza la gestión necesaria para tener disponibilidad y obtener los recursos financieros necesarios para Apoyar las áreas misionales de la entidad en el cumplimiento de la misión , visión , administrando los recursos financieros de forma tal que se distribuyan teniendo en cuenta la normativa legal que acoge la entidad , en consecuencia coordinara políticas con sus directrices presupuestales, lo que puede influir en contratos, planta de cargos , recursos físicos y tecnológicos para la prestación de servicios, o créditos o todo aquello que incida en el aspecto económico y financiero de la entidad.

Subdirector Técnico Directivo:

Garantiza el cumplimiento y fortalecimiento basado en Objeto social de la entidad mediante la elaboración, elaboración, gestión, controlar y evaluar los planes, programas o estrategias que impulsen los servicios misionales de la entidad, participando en la elaboración de políticas que se encuentren en conexidad con el plan de desarrollo vigente, participando en investigaciones inherentes a la misión

Control Interno Directivo:

Garantiza el cumplimiento y fortalecimiento a partir del desarrollo de auditorías internas en la entidad, con el objeto de velar en el cumplimiento todos los procedimientos críticos que deben de haber sido identificados previamente en el plan anual, estén debidamente implementados según las normas establecidas con el objeto de implementar una adecuada gestión de calidad, en apoyo para el director general , de igual forma controlar los planes de mejoramiento continua que fueron inscriptos ante entes de control como la contraloría nacional , departamental y municipal, de igual forma emitir un concepto con recomendaciones que ayude en la toma de decisiones. Por otra parte, debe de acompañar a la entidad en todo el proceso de licitación y contrataciones hasta su cierre.

9. MODELO DE GESTIÓN DE RIESGOS TI

Con relación al capítulo anterior, se puede deducir que el personal de TI es definido típicamente para este tipo de entidad pública dedicada a promover la ciencia, tecnología e innovación tecnológica en la ciudad de Cali, como un funcionario técnico de apoyo a la misión, lo que posiblemente quiere implicar que a nivel Directivo Administrativo es posible que no exista personal con capacidad de toma de decisiones, sino un o unos funcionarios técnicos que aunque no pueden decidir, si pueden incidir en evaluar los posibles riesgos que pueden llegar a afectar el normal ejercicio de las operaciones, que inciden en el cumplimiento de su objeto social, en consecuencia para poder ejercer labores de gestión y control de los riesgos depende de Director de control Interno quien es el encargado de realizar auditorías, dichos hallazgos, se toman como insumos para trabajar en la gestión del riesgo institucional, que a su vez se reflejara en el plan de acción de vigencias futuras , y los planes estratégicos de tecnologías de la Información.

En consecuencia el área de TI no puede ser evaluado como se evalúa cualquier otro departamento de la entidad , y más aún cuando es un área que es transversal a todas las demás dependencias, lo que implica que se debe de gestionar el riesgo de forma un poco más específica pero que sea fácil de comprender con la capacidad de indicar cuales riesgos o amenazas se deben priorizar , con el objeto de propiciar el normal ejercicio de las operaciones, que inciden en el cumplimiento de su objeto social para este tipo de entidad pública dedicada a promover la ciencia, tecnología e innovación tecnológica en la ciudad de Cali.

9.1. Activos de información mediante su categorización

La identificación de activos de información se realizará según metodología MAGERIT, dado que cuenta con una serie de puntos esenciales sistemáticos que sirven para realizar un idóneo análisis de riesgo, a las entidades públicas dedicadas a promover la ciencia, tecnología e innovación tecnológica en la ciudad de Cali.

En consecuencia, a lo anterior se sugiere realizar la clasificación que se describe a continuación:

La siguiente tabla recopila información relevante a la categorización de los activos de información necesario para identificar el activo, lo anterior toma como referente las guías de MAGERIT Libro 2 lo que posibilita trabajar de forma sistemática [31]

La Tabla N 40, se identifica la Categorización de Activos modelo Magerit con la cual se sugiere trabajar para este tipo de entidad.

Tabla N 40 Categorización de Activos modelo Magerit.

CATEGORIZACIÓN
[D]DATOS.
[K]CLAVES CRIPTOGRAFICAS.
[S]SERVICIOS.
[SW]SOFTWARE.
[HW]HARDWARE.
[COM]REDES DE COMUNICACIÓN.
[AUX]EQUIPO AUXILIAR.
[L]INSTALACIONES(infraestructura,edificio,CM)
[P]PERSONAL (funcionarios).

Fuente: Propia

[31] Administracionelectronica.gob.es. (2012). *MAGERIT versión 3 Libro II Catálogo de elementos (versión español): Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información.(11.)*. P8-14 https://administracionelectronica.gob.es/pae_Home/dam/jcr:5fbe15c3-c797-46a6-acd8-51311f4c2d29/2012_Magerit_v3_libro2_catalogo-de-elementos_es_NIPO_630-12-171-8.pdf

9.2. Identificación de amenazas con sus vulnerabilidades de los activos de información

A partir de este momento previo reconocimiento de los activos de información y sus facetas con relación a los dominios de seguridad, se identificarán vulnerabilidades que se pudieron identificar en forma general para este tipo de entidades.

La Tabla No: 41, se identifica las amenazas vs vulnerabilidades sobre los activos de información de la categoría DATOS.

Tabla No: 41 Amenazas - vulnerabilidades

Nombre del activo de información	Amenazas Metodología Magerit	Vulnerabilidades
[D] DATOS.[FILES]Archivos de apoyo y misionales.	[E,1]~Errores de usuario.	Uso inadecuado, Desconocimiento de la importancia del buen uso del espacio designado para los archivos.
[D] DATOS.[FILES]Archivos de apoyo y misionales.	[E,2]~Error de administrador.	Deficiente plan de clasificación de los documentos, y adecuado uso de los documentos en el activo relacionado.
[D] DATOS.[FILES]Archivos de apoyo y misionales.	[A,15]~Modificación deliberada de información.	No se evidencia gestión de auditorías y monitoreo periódico para validar el estado de la información, para el activo relacionado.
[D] DATOS.[FILES]Archivos de apoyo y misionales.	[E,18]~Destrucción de información.	Niveles de seguridad inadecuados para proteger la información del activo relacionado.
[D] DATOS.[backup]Copias de respaldo de configuración de SW , Router.	[E,1]~Errores de usuario.	Existe la posibilidad que el usuario no realice el respaldo de la información, no hay un gestor de respaldo profesional.
[D] DATOS.[backup]Copias de respaldo de configuración de SW , Router.	[E,2]~Error de administrador.	No cuenta con respaldo adecuado (backup) debido a que no se genera automáticamente enviándola a un servidor especializado.
[D] DATOS.[backup]Copias de respaldo de configuración de SW , Router.	[A,11]~Acceso no autorizado.	No se evidencia o no se reconoce, gestión adecuada o controles idóneos al servidor que almacena los respaldos del activo relacionado

Fuente: Propia

Continuación Tabla No: 41, se identifica las amenazas vs vulnerabilidades sobre los activos de información de la categoría DATOS.

Tabla No: 41 Amenazas - vulnerabilidades

Nombre del activo de información	Amenazas Metodología Magerit	Vulnerabilidades
[D] DATOS.[backup]Copia de respaldo estado MV.	[E,1]~Errores de usuario.	Existe la posibilidad que el usuario no realice el respaldo de la información, no hay un gestor de respaldo profesional.
[D] DATOS.[backup]Copia de respaldo estado MV.	[E,2]~Error de administrador.	No cuenta con respaldo adecuado (backup) debido a que no se genera automáticamente enviándola a un servidor especializado.
[D] DATOS.[backup]Copia de respaldo estado MV.	[A,11]~Acceso no autorizado.	No se evidencia o no se reconoce, gestión adecuada o controles idóneos al servidor que almacena los respaldos del activo relacionado
[D] DATOS.[backup]Copia de respaldo BD.	[E,1]~Errores de usuario.	Existe la posibilidad que el usuario no realice el respaldo de la información, no hay un gestor de respaldo profesional.
[D] DATOS.[backup]Copia de respaldo BD.	[E,2]~Error de administrador.	No cuenta con respaldo adecuado (backup) debido a que no se genera automáticamente enviándola a un servidor especializado.
[D] DATOS.[backup]Copia de respaldo BD.	[A,11]~Acceso no autorizado.	No se evidencia o no se reconoce, gestión adecuada o controles idóneos al servidor que almacena los respaldos del activo relacionado
[D] DATOS.Bases de datos de apoyo y misionales.	[E,1]~Errores de usuario.	Existe la posibilidad que el usuario no realice el respaldo de la información, no hay un gestor de respaldo profesional.
[D] DATOS.Bases de datos de apoyo y misionales.	[E,2]~Error de administrador.	Deficiente plan de clasificación de los documentos, y adecuado uso de los documentos en el activo relacionado.
[D] DATOS.Bases de datos de apoyo y misionales.	[A,15]~Modificación deliberada de información.	No se evidencia gestión de auditorías y monitoreo periódico para validar el estado de la información, para el activo relacionado.
[D] DATOS.Bases de datos de apoyo y misionales.	[E,18]~Destrucción de información.	Niveles de seguridad inadecuados para proteger la información del activo relacionado.

Fuente: Propia

Continuación Tabla No: 41, se identifica las amenazas vs vulnerabilidades sobre los activos de información de la categoría servicios de la entidad.

Tabla No: 41 Amenazas - vulnerabilidades

Nombre del activo de información	Amenazas Metodología Magerit	Vulnerabilidades
[S] Servicios.[www]Servicios de publicación del sitio web.	[E,2]~Error de administrador.	Escasas configuraciones de seguridad en el servidor. Parametrización de autenticación errónea.
[S] Servicios.[www]Servicios de publicación del sitio web.	[A,11]~Acceso no autorizado.	Gestión de permisos de acceso y autenticación deficiente,
[S] Servicios.[www]Servicios de publicación del sitio web.	[E,18]~Destrucción de información.	Niveles de seguridad inadecuados para proteger la información del activo relacionado.
[S] Servicios.[www]Servicios de publicación del sitio web.	[A,24]~Denegación de servicio.	Servicio de gestión inadecuada de los subdominios, facilitando el índice de trafico alto, posiblemente saturando el servicio.
[S] Servicios.[EMAIL]Servicios de publicación correo electrónico	[E,2]~Error de administrador.	Administración y Gestión inadecuada para las cuentas de usuarios.
[S] Servicios.[EMAIL]Servicios de publicación correo electrónico	[A,5]~Suplantación de identidad del usuario.	No se evidencia capacitación a los funcionarios en temas relacionados con Ingeniería Social, socialización que se incluya en el plan de seguridad para los funcionarios; propiciando seguridad en el buen uso del activo relacionado.
[S] Servicios.[INT]Servicios de impresión	[E,1]~Errores de usuario.	Daño por uso inadecuado
[S] Servicios.[INT]Servicios de impresión	[E,2]~Error de administrador.	Administración y Gestión de configuraciones, suficiencia de acceso al servicio y programación periódica de capacitaciones para el buen uso del activo relacionado.

Fuente: Propia

Continuación Tabla No: 41, se identifica las amenazas vs vulnerabilidades sobre los activos de información de la categoría servicios de la entidad.

Tabla No: 41 Amenazas - vulnerabilidades

Nombre del activo de información	Amenazas Metodología Magerit	Vulnerabilidades
[S] Servicios.[INT]Servicios de impresión	[E,19]~Fuga de información.	Deficiencia en la configuración de seguridad del servicio afectando la adecuada gestión de la seguridad, para el activo relacionado.
[S] Servicios.[INT]Soporte técnico(R.H).	[E,24]~Caída del sistema, causa agotamiento de recursos.	No se posee recurso físico humano suficiente para soportar las incidencias de soporte que requieren los funcionarios
[S] Servicios.[INT]Servicios IDS/IPS	[E,2]~Error de administrador.	No existe un reglamento o regulación para permitir o negar las conexiones o el intercambio de datos. (IDS/IPS,ROUTER,Firewall,HITS).
[S] Servicios.[INT]Servicios IDS/IPS	[E,24]~Caída del sistema, causa agotamiento de recursos.	No se posee recursos suficientes para soportar las necesidades con relación al activo relacionado.
[S] Servicios.[INT]Servicios IDS/IPS	[A,24]~Denegación de servicio.	Deficiencia en la configuración del servicio afectando el adecuado funcionamiento, para el activo relacionado.
[S] Servicios.[INT]Servicios HITS	[E,2]~Error de administrador.	No existe un reglamento o regulación para permitir o negar las conexiones o el intercambio de datos. (IDS/IPS,ROUTER,Firewall,HITS).
[S] Servicios.[INT]Servicios HITS	[E,24]~Caída del sistema, causa agotamiento de recursos.	No se posee recursos suficientes para soportar las necesidades con relación al activo relacionado.
[S] Servicios.[INT]Servicios HITS	[A,24]~Denegación de servicio.	Deficiencia en la configuración del servicio afectando el adecuado funcionamiento, para el activo relacionado.

Fuente: Propia

Continuación Tabla No: 41, se identifica las amenazas vs vulnerabilidades sobre los activos de información de la categoría servicios de la entidad.

Tabla No: 41 Amenazas - vulnerabilidades

Nombre del activo de información	Amenazas Metodología Magerit	Vulnerabilidades
[S] Servicios.[FTP]Protocolo de transferencia de archivos	[E,2]~Error de administrador.	Deficiencia en la configuración del protocolo, para el activo relacionado.
[S] Servicios.[FTP]Protocolo de transferencia de archivos	[E,24]~Caída del sistema, causa agotamiento de recursos.	No se posee recursos suficientes para desoportar las necesidades con relación al activo relacionado.
[S] Servicios.[FTP]Protocolo de transferencia de archivos	[A,24]~Denegación de servicio.	No existe un reglamento o regulación para permitir o negar las conexiones o el intercambio de datos. (IDS/IPS,ROUTER,Firewall).
[S] Servicios.[FILE]Soporte en almacenamiento de archivos misionales y de apoyo.	[E,2]~Error de administrador.	Deficiencia en la configuración del protocolo, para el activo relacionado.
[S] Servicios.[FILE]Soporte en almacenamiento de archivos misionales y de apoyo.	[E,24]~Caída del sistema, causa agotamiento de recursos.	No se posee recursos suficientes para desoportar las necesidades con relación al activo relacionado.
[S] Servicios.[FILE]Soporte en almacenamiento de archivos misionales y de apoyo.	[A,24]~Denegación de servicio.	No existe un reglamento o regulación para permitir o negar las conexiones o el intercambio de datos. (IDS/IPS,ROUTER,Firewall).
[S] Servicios.[IDM]Soporte a gestión de usuarios y contraseñas.	[E,2]~Error de administrador.	Uso de configuraciones por defecto, nativas o genéricas. Deficiente parametrización de usuarios y contraseñas.
[S] Servicios.[IDM]Soporte a gestión de usuarios y contraseñas.	[E,24]~Caída del sistema, causa agotamiento de recursos.	No se posee recurso físico humano desuficiente para soportar las incidencias de soporte que requieren los funcionarios

Fuente: Propia

Continuación Tabla No: 41, se identifica las amenazas vs vulnerabilidades sobre los activos de información de la categoría servicios de la entidad.

Tabla No: 41 Amenazas - vulnerabilidades

Nombre del activo de información	Amenazas Metodología Magerit	Vulnerabilidades
[S] Servicios.[IDM]Soporte a gestión de usuarios y contraseñas.	[A,24]~Denegación de servicio.	No existe un reglamento o regulación para permitir o negar las conexiones o el intercambio de datos. (IDS/IPS,ROUTER,Firewall).
[SW] Software.[dbms] _Bases de datos Mysql	[E,2]~Error de administrador.	Deficiencia en la configuración del servicio afectando el adecuado funcionamiento, para el activo relacionado.
[SW] Software.[dbms] _Bases de datos Mysql	[E,20]~Vulnerabilidades de los programas (software).	Vulnerabilidades conocidas y de día cero presentes en el activo relacionado. Inexistencia de plan de contingencia y/o plan de seguridad.
[SW] Software.[dbms] _Bases de datos Mysql	[E,21]~Error de mantenimiento / actualización de los programas (software).	No existe un adecuado control para las actualizaciones, por tanto el mantenimiento no es eficiente.
[SW] Software.[dbms] _Bases de datos PostgreSQL	[E,2]~Error de administrador.	Deficiencia en la configuración del servicio afectando el adecuado funcionamiento, para el activo relacionado.
[SW] Software.[dbms] _Bases de datos PostgreSQL	[E,20]~Vulnerabilidades de los programas (software).	Vulnerabilidades conocidas y de día cero presentes en el activo relacionado. Inexistencia de plan de contingencia y/o plan de seguridad.
[SW] Software.[dbms] _Bases de datos PostgreSQL	[E,21]~Error de mantenimiento / actualización de los programas (software).	No existe un adecuado control para las actualizaciones, por tanto el mantenimiento no es eficiente.
[SW] Software.[dbms] _Bases de datos Oracle12	[E,2]~Error de administrador.	Deficiencia en la configuración del servicio afectando el adecuado funcionamiento, para el activo relacionado.

Fuente: Propia

Nombre del activo de información	Amenazas Metodología Magerit	Vulnerabilidades
[SW] Software.[dbms]_Bases de datos Oracle12	[E,20]~Vulnerabilidades de los programas (software).	Vulnerabilidades conocidas y de día cero presentes en el activo relacionado. Inexistencia de plan de contingencia y/o plan de seguridad.
[SW] Software.[dbms]_Bases de datos Oracle12	[E,21]~Error de mantenimiento /actualización de los programas (software).	No existe un adecuado control para las actualizaciones, por tanto el mantenimiento no es eficiente.
[SW] Software.[os]_S.O Microsoft Windows 10	[E,1]~Errores de usuario.	Uso inadecuado, Desconocimiento sobre la funcionalidad por tanto del buen uso del Sistema Operativo.
[SW] Software.[os]_S.O Microsoft Windows 10	[E,20]~Vulnerabilidades de los programas (software).	Vulnerabilidades conocidas y de día cero presentes en el activo relacionado. Inexistencia de plan de contingencia y/o plan de seguridad.
[SW] Software.[os]_S.O Microsoft Windows 10	[E,21]~Error de mantenimiento /actualización de los programas (software).	No existe un adecuado control para las actualizaciones, por tanto el mantenimiento no es eficiente.
[SW] Software.[os]_S.O Microsoft Windows 10	[A,6]~Abuso privilegios de acceso.	Gestion de permisos de acceso y autenticación deficiente.
[SW] Software.[os]_S.O Microsoft Windows 10	[A,7]~Uso no previsto.	No existe políticas restrictivas, que eviten el acceso a sitios web maliciosos.
[SW] Software.[os]_S.O Microsoft Windows 10	[A,8]~Difusión de software dañino.	Deficiencia en configuraciión de antivirus.
[SW] Software.[os]_S.O Microsoft Windows 7	[E,1]~Errores de usuario.	Uso inadecuado, Desconocimiento sobre la funcionalidad por tanto del buen uso del Sistema Operativo.

Fuente: Propia

En la tabla se identifica las amenazas vs vulnerabilidades sobre los activos de información de la categoría software de la entidad.

Continuación Tabla No: 41, se identifica las amenazas vs vulnerabilidades sobre los activos de información de la categoría servicios de la entidad.

Tabla No: 41 Amenazas - vulnerabilidades

Nombre del activo de información	Amenazas Metodología Magerit	Vulnerabilidades
[SW] Software.[os]_S.O Microsoft Windows 7	[E,20]~Vulnerabilidades de los programas (software).	Vulnerabilidades conocidas y de día cero presentes en el activo relacionado. Inexistencia de plan de contingencia y/o plan de seguridad.
[SW] Software.[os]_S.O Microsoft Windows 7	[E,21]~Error de mantenimiento / actualización de los programas (software).	No existe un adecuado control para las actualizaciones, por tanto el mantenimiento no es eficiente.
[SW] Software.[os]_S.O Microsoft Windows 7	[A,6]~Abuso privilegios de acceso.	Gestión de permisos de acceso y autenticación deficiente.
[SW] Software.[os]_S.O Microsoft Windows 7	[A,7]~Uso no previsto.	No existen políticas restrictivas, que eviten el acceso a sitios web maliciosos.
[SW] Software.[os]_S.O Microsoft Windows 7	[A,8]~Difusión de software dañino.	Deficiencia en configuración de antivirus.
[SW] Software.[os]_S.O Microsoft Windows Vista	[E,1]~Errores de usuario.	Uso inadecuado, Desconocimiento sobre la funcionalidad por tanto del buen uso del Sistema Operativo.
[SW] Software.[os]_S.O Microsoft Windows Vista	[E,20]~Vulnerabilidades de los programas (software).	Vulnerabilidades conocidas y de día cero presentes en el activo relacionado. Inexistencia de plan de contingencia y/o plan de seguridad.
[SW] Software.[os]_S.O Microsoft Windows Vista	[E,21]~Error de mantenimiento / actualización de los programas (software).	No existe un adecuado control para las actualizaciones, por tanto el mantenimiento no es eficiente.
[SW] Software.[os]_S.O Microsoft Windows Vista	[A,6]~Abuso privilegios de acceso.	Gestión de permisos de acceso y autenticación deficiente.
[SW] Software.[os]_S.O Microsoft Windows Vista	[A,7]~Uso no previsto.	No existen políticas restrictivas, que eviten el acceso a sitios web maliciosos.

Fuente: Propia

Continuación Tabla No: 41, se identifica las amenazas vs vulnerabilidades sobre los activos de información de la categoría servicios de la entidad.

Tabla No: 41 Amenazas - vulnerabilidades

Nombre del activo de información	Amenazas Metodología Magerit	Vulnerabilidades
[SW] Software.[os]_S.O Microsoft Windows Vista	[A,8]~Difusión de software dañino.	Deficiencia en configuración de antivirus.
[SW] Software.[os]_S.O Microsoft Windows XP	[E,1]~Errores de usuario.	Uso inadecuado, Desconocimiento sobre la funcionalidad por tanto del buen uso del Sistema Operativo.
[SW] Software.[os]_S.O Microsoft Windows XP	[E,20]~Vulnerabilidades de los programas (software).	Vulnerabilidades conocidas y de día cero presentes en el activo relacionado. Inexistencia de plan de contingencia y/o plan de seguridad.
[SW] Software.[os]_S.O Microsoft Windows XP	[E,21]~Error de mantenimiento / actualización de los programas (software).	No existe un adecuado control para las actualizaciones, por tanto el mantenimiento no es eficiente.
[SW] Software.[os]_S.O Microsoft Windows XP	[A,6]~Abuso privilegios de acceso.	Gestión de permisos de acceso y autenticación deficiente.
[SW] Software.[os]_S.O Microsoft Windows XP	[A,7]~Uso no previsto.	No existen políticas restrictivas, que eviten el acceso a sitios web maliciosos.
[SW] Software.[os]_S.O Microsoft Windows XP	[A,8]~Difusión de software dañino.	Deficiencia en configuración de antivirus.
[SW] Software.[os]_S.O Microsoft Windows server 2008	[E,2]~Error de administrador.	Administración y Gestión inadecuada para las cuentas de usuarios.
[SW] Software.[os]_S.O Microsoft Windows server 2008	[E,20]~Vulnerabilidades de los programas (software).	Vulnerabilidades conocidas y de día cero presentes en el activo relacionado. Inexistencia de plan de contingencia y/o plan de seguridad.
[SW] Software.[os]_S.O Microsoft Windows server 2008	[E,21]~Error de mantenimiento / actualización de los programas (software).	No existe un adecuado control para las actualizaciones, por tanto el mantenimiento no es eficiente.

Fuente: Propia

Continuación Tabla No: 41, se identifica las amenazas vs vulnerabilidades sobre los activos de información de la categoría servicios de la entidad.

Tabla No: 41 Amenazas - vulnerabilidades

Nombre del activo de información	Amenazas Metodología Magerit	Vulnerabilidades
[SW] Software.[os]_S.O Microsoft Windows server 2008	[E,24]~Caída del sistema, causa agotamiento de recursos.	La demanda de recursos de la entidad supera los recursos físicos, técnicos con los que se cuenta, propiciando pérdida de disponibilidad, intermitencia, interferencia, interferencia de los recursos, para el activo relacionado.
[SW] Software.[os]_S.O Microsoft Windows server 2012	[E,2]~Error de administrador.	Administración y Gestión inadecuada para las cuentas de usuarios.
[SW] Software.[os]_S.O Microsoft Windows server 2012	[E,20]~Vulnerabilidades de los programas (software).	Vulnerabilidades conocidas y de día cero presentes en el activo relacionado. Inexistencia de plan de contingencia y/o plan de seguridad.
[SW] Software.[os]_S.O Microsoft Windows server 2012	[E,21]~Error de mantenimiento /actualización de los programas (software).	No existe un adecuado control para las actualizaciones, por tanto el mantenimiento no es eficiente.
[SW] Software.[os]_S.O Microsoft Windows server 2012	[E,24]~Caída del sistema, causa agotamiento de recursos.	La demanda de recursos de la entidad supera los recursos físicos, técnicos con los que se cuenta, propiciando pérdida de disponibilidad, intermitencia, interferencia, interferencia de los recursos, para el activo relacionado.
[SW] Software.[os]_Linux Centos 7	[E,2]~Error de administrador.	Administración y Gestión inadecuada para las cuentas de usuarios.
[SW] Software.[os]_Linux Centos 7	[E,20]~Vulnerabilidades de los programas (software).	Vulnerabilidades conocidas y de día cero presentes en el activo relacionado. Inexistencia de plan de contingencia y/o plan de seguridad.

Fuente: Propia

Continuación Tabla No: 41, se identifica las amenazas vs vulnerabilidades sobre los activos de información de la categoría servicios de la entidad.

Tabla No: 41 Amenazas - vulnerabilidades

Nombre del activo de información	Amenazas Metodología Magerit	Vulnerabilidades
[HW] Equipamiento informático.[vhost]_[vhost] _Servidor Soporte en almacenamiento de archivos misionales y de apoyo.	[E,21]~Error de mantenimiento / actualización de los programas (software).	No existe un adecuado control para las actualizaciones, por tanto el mantenimiento no es eficiente.
[HW] Equipamiento informático.[vhost]_[vhost] _Servidor Soporte en almacenamiento de archivos misionales y de apoyo.	[E,24]~Caída del sistema, causa agotamiento de recursos.	La demanda de recursos de la entidad supera los recursos físicos, técnicos con los que se cuenta, propiciando pérdida de disponibilidad, intermitencia, interferencia, interferencia de los recursos, para el activo relacionado.
[HW] Equipamiento informático.[vhost]_[vhost] _Servidor Soporte en almacenamiento de archivos misionales y de apoyo.	[A,24]~Denegación de servicio.	No existe un reglamento o regulación para permitir o negar las conexiones o el intercambio de datos. (IDS/IPS,ROUTER,Firewall).
[HW] Equipamiento informático.[vhost]_[vhost] _Servidor gestión de usuarios y contraseñas.	[E,2]~Error de administrador.	Deficiencia en la configuración en el volumen de almacenamiento puede afectar el adecuado funcionamiento, para el activo relacionado.
[HW] Equipamiento informático.[vhost]_[vhost] _Servidor gestión de usuarios y contraseñas.	[E,21]~Error de mantenimiento / actualización de los programas (software).	No existe un adecuado control para las actualizaciones, por tanto el mantenimiento no es eficiente.
[HW] Equipamiento informático.[vhost]_[vhost] _Servidor gestión de usuarios y contraseñas.	[E,24]~Caída del sistema, causa agotamiento de recursos.	La demanda de recursos de la entidad supera los recursos físicos, técnicos con los que se cuenta, propiciando pérdida de disponibilidad, intermitencia, interferencia, interferencia de los recursos, para el activo relacionado.

Fuente: Propia

Continuación Tabla No: 41, se identifica las amenazas vs vulnerabilidades sobre los activos de información de la categoría servicios de la entidad.

Tabla No: 41 Amenazas - vulnerabilidades

Nombre del activo de información	Amenazas Metodología Magerit	Vulnerabilidades
[SW] Software.[os]_Linux CentOS 7	[E,21]~Error de mantenimiento / actualización de los programas (software).	No existe un adecuado control para las actualizaciones, por tanto el mantenimiento no es eficiente.
[SW] Software.[os]_Linux CentOS 7	[E,24]~Caída del sistema, causa agotamiento de recursos.	La demanda de recursos de la entidad supera los recursos físicos, técnicos con los que se cuenta, propiciando pérdida de disponibilidad, intermitencia, interferencia, interferencia de los recursos, para el activo relacionado.
[SW] Software.[os]_S.O UTM	[E,2]~Error de administrador.	Administración y Gestión inadecuada para las cuentas de usuarios.
[SW] Software.[os]_S.O UTM	[E,20]~Vulnerabilidades de los programas (software).	Vulnerabilidades conocidas y de día cero presentes en el activo relacionado. Inexistencia de plan de contingencia y/o plan de seguridad.
[SW] Software.[os]_S.O UTM	[E,21]~Error de mantenimiento / actualización de los programas (software).	No existe un adecuado control para las actualizaciones, por tanto el mantenimiento no es eficiente.
[SW] Software.[os]_S.O UTM	[E,24]~Caída del sistema, causa agotamiento de recursos.	La demanda de recursos de la entidad supera los recursos físicos, técnicos con los que se cuenta, propiciando pérdida de disponibilidad, intermitencia, interferencia, interferencia de los recursos, para el activo relacionado.
[SW] Software.[os]_Hypervisor de Máquinas virtuales	[E,2]~Error de administrador.	Administración y Gestión inadecuada para las cuentas de usuarios.

Fuente: Propia

Continuación Tabla No: 41, se identifica las amenazas vs vulnerabilidades sobre los activos de información de la categoría servicios de la entidad.

Tabla No: 41 Amenazas - vulnerabilidades

Nombre del activo de información	Amenazas Metodología Magerit	Vulnerabilidades
[SW] Software.[os]_Hypervisor de Máquinas virtuales	[E,20]~Vulnerabilidades de los programas (software).	Vulnerabilidades conocidas y de día cero presentes en el activo relacionado. Inexistencia de plan de contingencia y/o plan de seguridad.
[SW] Software.[os]_Hypervisor de Máquinas virtuales	[E,21]~Error de mantenimiento /actualización de los programas (software).	No existe un adecuado control para las actualizaciones, por tanto, el mantenimiento no es eficiente.
[SW] Software.[os]_Hypervisor de Máquinas virtuales	[E,24]~Caída del sistema, causa agotamiento de recursos.	La demanda de recursos de la entidad supera los recursos físicos, técnicos con los que se cuenta, propiciando pérdida de disponibilidad, intermitencia, interferencia, interferencia de los recursos, para el activo relacionado.
[SW] Software.[std]_Apache.	[E,2]~Error de administrador.	Deficiencia en la configuración del servicio afectando el adecuado funcionamiento, para el activo relacionado.
[SW] Software.[std]_Apache.	[E,20]~Vulnerabilidades de los programas (software).	Vulnerabilidades conocidas y de día cero presentes en el activo relacionado. Inexistencia de plan de contingencia y/o plan de seguridad.
[SW] Software.[std]_Apache.	[E,21]~Error de mantenimiento /actualización de los programas (software).	No existe un adecuado control para las actualizaciones, por tanto el mantenimiento no es eficiente.
[SW] Software.[std]_Apache.	[E,24]~Caída del sistema, causa agotamiento de recursos.	La demanda de recursos de la entidad supera los recursos físicos, técnicos con los que se cuenta, propiciando pérdida de disponibilidad, intermitencia, interferencia, interferencia de los recursos, para el activo relacionado.

Fuente: Propia

Continuación Tabla No: 41, se identifica las amenazas vs vulnerabilidades sobre los activos de información de la categoría servicios de la entidad.

Tabla No: 41 Amenazas - vulnerabilidades

Nombre del activo de información	Amenazas Metodología Magerit	Vulnerabilidades
[SW] Software.[std]_IIS.	[E,2]~Error de administrador.	Deficiencia en la configuración del servicio afectando el adecuado funcionamiento, para el activo relacionado.
[SW] Software.[std]_IIS.	[E,20]~Vulnerabilidades de los programas (software).	Vulnerabilidades conocidas y de día cero presentes en el activo relacionado. Inexistencia de plan de contingencia y/o plan de seguridad.
[SW] Software.[std]_IIS.	[E,21]~Error de mantenimiento / actualización de los programas (software).	No existe un adecuado control para las actualizaciones, por tanto el mantenimiento no es eficiente.
[SW] Software.[std]_IIS.	[E,24]~Caída del sistema, causa agotamiento de recursos.	La demanda de recursos de la entidad supera los recursos físicos, técnicos con los que se cuenta, propiciando pérdida de disponibilidad, intermitencia, interferencia, interferencia de los recursos, para el activo relacionado.
[SW] Software.[std]_CMS Joomla.	[E,2]~Error de administrador.	Deficiencia en la configuración del servicio afectando el adecuado funcionamiento, para el activo relacionado.
[SW] Software.[std]_CMS Joomla.	[E,20]~Vulnerabilidades de los programas (software).	Vulnerabilidades conocidas y de día cero presentes en el activo relacionado. Inexistencia de plan de contingencia y/o plan de seguridad.
[SW] Software.[std]_CMS Joomla.	[E,21]~Error de mantenimiento / actualización de los programas (software).	No existe un adecuado control para las actualizaciones, por tanto el mantenimiento no es eficiente.

Fuente: Propia

Continuación Tabla No: 41, se identifica las amenazas vs vulnerabilidades sobre los activos de información de la categoría servicios de la entidad.

Tabla No: 41 Amenazas - vulnerabilidades

Nombre del activo de información	Amenazas Metodología Magerit	Vulnerabilidades
[SW] Software.[std]_CMS WordPress.	[E,2]~Error de administrador.	Deficiencia en la configuración del servicio afectando el adecuado funcionamiento, para el activo relacionado.
[SW] Software.[std]_CMS WordPress.	[E,20]~Vulnerabilidades de los programas (software).	Vulnerabilidades conocidas y de día cero presentes en el activo relacionado. Inexistencia de plan de contingencia y/o plan de seguridad.
[SW] Software.[std]_CMS WordPress.	[E,21]~Error de mantenimiento / actualización de los programas (software).	No existe un adecuado control para las actualizaciones, por tanto, el mantenimiento no es eficiente.
[SW] Software.[std]_GLPI Inventario mesa de ayuda	[E,2]~Error de administrador.	Parametrización de usuarios y contraseñas está en dependencia del Directorio Activo.
[SW] Software.[std]_GLPI Inventario mesa de ayuda	[E,20]~Vulnerabilidades de los programas (software).	Vulnerabilidades conocidas y de día cero presentes en el activo relacionado. Inexistencia de plan de contingencia y/o plan de seguridad.
[SW] Software.[std]_GLPI Inventario mesa de ayuda	[E,21]~Error de mantenimiento / actualización de los programas (software).	No existe un adecuado control para las actualizaciones, por tanto el mantenimiento no es eficiente.
[SW] Software.[std]_PHP 5.6.30 >	[E,2]~Error de administrador.	Deficiencia en la configuración del servicio afectando el adecuado funcionamiento, para el activo relacionado.
[SW] Software.[std]_PHP 5.6.30 >	[E,20]~Vulnerabilidades de los programas (software).	Vulnerabilidades conocidas y de día cero presentes en el activo relacionado. Inexistencia de plan de contingencia y/o plan de seguridad.

Fuente: Propia

Continuación Tabla No: 41, se identifica las amenazas vs vulnerabilidades sobre los activos de información de la categoría Hardware de la entidad.

Tabla No: 41 Amenazas - vulnerabilidades

Nombre del activo de información	Amenazas Metodología Magerit	Vulnerabilidades
[SW] Software.[std]_PHP 5.6.30 >	[E,21]~Error de mantenimiento / actualización de los programas (software).	No existe un adecuado control para las actualizaciones, por tanto, el mantenimiento no es eficiente.
[HW] Equipamiento informático.[print]_[print]_Impresora en RED Laser.(Cantidad: X)	[E,23]~Error de mantenimiento / actualización de los equipos (hardware).	Deficiente cumplimiento del plan de mantenimiento e instalación ineficiente para hardware posiblemente no hay repuestos.
[HW] Equipamiento informático.[print]_[print]_Impresora en RED Laser.(Cantidad: X)	[I,3]~Contaminación mecánica.	El activo de Información es susceptible a accidentes o daños deliberados.
[HW] Equipamiento informático.[print]_[print]_Impresora en RED Laser.(Cantidad: X)	[I,5]~Avería de origen físico o lógico.	Averías propias del dispositivo que pueden ser tanto de tipo lógico como físico.
[HW] Equipamiento informático.[print]_[print]_Impresora en RED Laser.(Cantidad: X)	[I,6]~Corte del suministro eléctrico.	Deficiencia en el sistema de respaldo de energía para el activo de información relacionado.
[HW] Equipamiento informático.[host]_[host]_Servidor Hypervisor	[E,23]~Error de mantenimiento / actualización de los equipos (hardware).	Deficiente cumplimiento del plan de mantenimiento e instalación ineficiente para hardware posiblemente no hay repuestos.
[HW] Equipamiento informático.[host]_[host]_Servidor Hypervisor	[A,24]~Denegación de servicio.	No existe un reglamento o regulación para permitir o negar las conexiones o el intercambio de datos. (IDS/IPS,ROUTER,Firewall).
[HW] Equipamiento informático.[host]_[host]_Servidor Hypervisor	[A,25]~Robo.	Deficiencia en el control de acceso al servidor a través de estaciones de trabajo, dedicadas en la gestión de Máquinas virtuales.

Fuente: Propia

Continuación Tabla No: 41, se identifica las amenazas vs vulnerabilidades sobre los activos de información de la categoría Hardware de la entidad.

Tabla No: 41 Amenazas - vulnerabilidades

Nombre del activo de información	Amenazas Metodología Magerit	Vulnerabilidades
[HW] Equipamiento informático.[host]_[host]_Servidor Hypervisor	[A,26]~Ataque destructivo.	Es posible daños a consecuencia del ejercicio de paro social del orden Nacional/Departamental/Municipal bajo actividades de actos vandálicos.
[HW] Equipamiento informático.[host]_[host]_Servidor Hypervisor	[I,3]~Contaminación mecánica.	El activo de Información es susceptible a accidentes o daños deliberados.
[HW] Equipamiento informático.[host]_[host]_Servidor Hypervisor	[I,5]~Avería de origen físico o lógico.	Averías propias del dispositivo que pueden ser tanto de tipo lógico como físico.
[HW] Equipamiento informático.[host]_[host]_Servidor Hypervisor	[I,7]~Condiciones inadecuadas de temperatura o humedad.	El hardware es usado en espacios físicos que no cumplen los requerimientos de temperatura y humedad que exige el fabricante, no hay forma de evaluar su cumplimiento, para el activo de información relacionado.
[HW] Equipamiento informático.[host]_[host]_Servidor Hypervisor	[N,*]~Desastres naturales.	Deficiente plan de prevención contra desastres naturales, que incluyan rayos, tormentas, eléctricas, inundación.
[HW] Equipamiento informático.[vhost]_[vhost]_Servidor GLPI de soporte técnico	[E,2]~Error de administrador.	Deficiencia en la configuración en el volumen de almacenamiento puede afectar el adecuado funcionamiento, para el activo relacionado.
[HW] Equipamiento informático.[vhost]_[vhost]_Servidor GLPI de soporte técnico	[E,21]~Error de mantenimiento / actualización de los programas (software).	No existe un adecuado control para las actualizaciones, por tanto el mantenimiento no es eficiente.
[HW] Equipamiento informático.[vhost]_[vhost]_Servidor GLPI de soporte técnico	[E,24]~Caída del sistema, causa agotamiento de recursos.	La demanda de recursos de la entidad supera los recursos físicos, técnicos con los que se cuenta, propiciando pérdida de disponibilidad, intermitencia, interferencia, interferencia de los recursos, para el activo relacionado.

Fuente: Propia

Continuación Tabla No: 41, se identifica las amenazas vs vulnerabilidades sobre los activos de información de la categoría Hardware de la entidad.

Tabla No: 41 Amenazas - vulnerabilidades

Nombre del activo de información	Amenazas Metodología Magerit	Vulnerabilidades
[HW] Equipamiento informático.[vhost]_[vhost]_ Servidor GLPI de soporte técnico	[A,24]~Denegación de servicio.	No existe un reglamento o regulación para permitir o negar las conexiones o el intercambio de datos. (IDS/IPS,ROUTER,Firewall).
[HW] Equipamiento informático.[vhost]_[vhost]_ Servidor UTM IDS/IPS	[E,2]~Error de administrador.	No existe un reglamento o regulación para permitir o negar las conexiones o el intercambio de datos. (IDS/IPS,ROUTER,Firewall).
[HW] Equipamiento informático.[vhost]_[vhost]_ Servidor UTM IDS/IPS	[E,21]~Error de mantenimiento / actualización de los programas (software).	No existe un adecuado control para las actualizaciones, por tanto el mantenimiento no es eficiente.
[HW] Equipamiento informático.[vhost]_[vhost]_ Servidor UTM IDS/IPS	[E,24]~Caída del sistema, causa agotamiento de recursos.	La demanda de recursos de la entidad supera los recursos físicos, técnicos con los que se cuenta, propiciando pérdida de disponibilidad, intermitencia, interferencia, interferencia de los recursos, para el activo relacionado.
[HW] Equipamiento informático.[vhost]_[vhost]_ Servidor UTM IDS/IPS	[A,24]~Denegación de servicio.	No existe un reglamento o regulación para permitir o negar las conexiones o el intercambio de datos. (IDS/IPS,ROUTER,Firewall).
[HW] Equipamiento informático.[vhost]_[vhost]_ Servidor HITS	[E,2]~Error de administrador.	Deficiencia en la configuración en el volumen de almacenamiento puede afectar el adecuado funcionamiento, para el activo relacionado.
[HW] Equipamiento informático.[vhost]_[vhost]_ Servidor HITS	[E,21]~Error de mantenimiento / actualización de los programas (software).	No existe un adecuado control para las actualizaciones, por tanto, el mantenimiento no es eficiente.

Fuente: Propia

Continuación Tabla No: 41, se identifica las amenazas vs vulnerabilidades sobre los activos de información de la categoría Hardware de la entidad.

Tabla No: 41 Amenazas - vulnerabilidades

Nombre del activo de información	Amenazas Metodología Magerit	Vulnerabilidades
[HW] Equipamiento informático.[vhost]_[vhost]_ Servidor HITS	[E,24]~Caída del sistema, causa agotamiento de recursos.	La demanda de recursos de la entidad supera los recursos físicos, técnicos con los que se cuenta, propiciando pérdida de disponibilidad, intermitencia, interferencia, interferencia de los recursos, para el activo relacionado.
[HW] Equipamiento informático.[vhost]_[vhost]_ Servidor HITS	[A,24]~Denegación de servicio.	No existe un reglamento o regulación para permitir o negar las conexiones o el intercambio de datos. (IDS/IPS,ROUTER,Firewall).
[HW] Equipamiento informático.[vhost]_[vhost]_ Servidor Protocolo de transferencia de archivos	[E,2]~Error de administrador.	Deficiencia en la configuración en el volumen de almacenamiento puede afectar el adecuado funcionamiento, para el activo relacionado.
[HW] Equipamiento informático.[vhost]_[vhost]_ Servidor Protocolo de transferencia de archivos	[E,21]~Error de mantenimiento / actualización de los programas (software).	No existe un adecuado control para las actualizaciones, por tanto, el mantenimiento no es eficiente.
[HW] Equipamiento informático.[vhost]_[vhost]_ Servidor Protocolo de transferencia de archivos	[E,24]~Caída del sistema, causa agotamiento de recursos.	La demanda de recursos de la entidad supera los recursos físicos, técnicos con los que se cuenta, propiciando pérdida de disponibilidad, intermitencia, interferencia, interferencia de los recursos, para el activo relacionado.
[HW] Equipamiento informático.[vhost]_[vhost]_ Servidor Protocolo de transferencia de archivos	[A,24]~Denegación de servicio.	No existe un reglamento o regulación para permitir o negar las conexiones o el intercambio de datos. (IDS/IPS,ROUTER,Firewall).
[HW] Equipamiento informático.[vhost]_[vhost]_ Servidor Soporte en almacenamiento de archivos misionales y de apoyo.	[E,2]~Error de administrador.	Deficiencia en la configuración en el volumen de almacenamiento puede afectar el adecuado funcionamiento, para el activo relacionado.

Fuente: Propia

Continuación Tabla No: 41, se identifica las amenazas vs vulnerabilidades sobre los activos de información de la categoría Hardware de la entidad.

Tabla No: 41 Amenazas - vulnerabilidades

Nombre del activo de información	Amenazas Metodología Magerit	Vulnerabilidades
[HW] Equipamiento informático.[vhost]_[vhost] _Servidor Soporte en almacenamiento de archivos misionales y de apoyo.	[E,21]~Error de mantenimiento / actualización de los programas (software).	No existe un adecuado control para las actualizaciones, por tanto, el mantenimiento no es eficiente.
[HW] Equipamiento informático.[vhost]_[vhost] _Servidor Soporte en almacenamiento de archivos misionales y de apoyo.	[E,24]~Caída del sistema, causa agotamiento de recursos.	La demanda de recursos de la entidad supera los recursos físicos, técnicos con los que se cuenta, propiciando pérdida de disponibilidad, intermitencia, interferencia, interferencia de los recursos, para el activo relacionado.
[HW] Equipamiento informático.[vhost]_[vhost] _Servidor Soporte en almacenamiento de archivos misionales y de apoyo.	[A,24]~Denegación de servicio.	No existe un reglamento o regulación para permitir o negar las conexiones o el intercambio de datos. (IDS/IPS,ROUTER,Firewall).
[HW] Equipamiento informático.[vhost]_[vhost] _Servidor gestión de usuarios y contraseñas.	[E,2]~Error de administrador.	Deficiencia en la configuración en el volumen de almacenamiento puede afectar el adecuado funcionamiento, para el activo relacionado.
[HW] Equipamiento informático.[vhost]_[vhost] _Servidor gestión de usuarios y contraseñas.	[E,21]~Error de mantenimiento / actualización de los programas (software).	No existe un adecuado control para las actualizaciones, por tanto, el mantenimiento no es eficiente.

Fuente: Propia

Continuación Tabla No: 41, se identifica las amenazas vs vulnerabilidades sobre los activos de información de la categoría Hardware de la entidad.

Tabla No: 41 Amenazas - vulnerabilidades

Nombre del activo de información	Amenazas Metodología Magerit	Vulnerabilidades
[HW] Equipamiento informático.[vhost]_[vhost] _Servidor gestión de usuarios y contraseñas.	[E,24]~Caída del sistema, causa agotamiento de recursos.	La demanda de recursos de la entidad supera los recursos físicos, técnicos con los que se cuenta, propiciando pérdida de disponibilidad, intermitencia, interferencia, interferencia de los recursos, para el activo relacionado.
[HW] Equipamiento informático.[vhost]_[vhost] _Servidor gestión de usuarios y contraseñas.	[A,24]~Denegación de servicio.	No existe un reglamento o regulación para permitir o negar las conexiones o el intercambio de datos. (IDS/IPS,ROUTER,Firewall).
[HW] Equipamiento informático.[vhost]_[vhost] _Servidor DHCP.	[E,2]~Error de administrador.	Deficiencia en la configuración en el volumen de almacenamiento puede afectar el adecuado funcionamiento, para el activo relacionado.
[HW] Equipamiento informático.[vhost]_[vhost] _Servidor DHCP.	[E,21]~Error de mantenimiento / actualización de los programas (software).	No existe un adecuado control para las actualizaciones, por tanto el mantenimiento no es eficiente.
[HW] Equipamiento informático.[vhost]_[vhost] _Servidor DHCP.	[E,24]~Caída del sistema, causa agotamiento de recursos.	La demanda de recursos de la entidad supera los recursos físicos, técnicos con los que se cuenta, propiciando pérdida de disponibilidad, intermitencia, interferencia, interferencia de los recursos, para el activo relacionado.
[HW] Equipamiento informático.[vhost]_[vhost] _Servidor DHCP.	[A,24]~Denegación de servicio.	No existe un reglamento o regulación para permitir o negar las conexiones o el intercambio de datos. (IDS/IPS,ROUTER,Firewall).
[HW] Equipamiento informático.[host]_[host]_E staciones de trabajo.	[E,23]~Error de mantenimiento / actualización de los equipos (hardware).	Deficiente cumplimiento del plan de mantenimiento e instalación ineficiente para hardware posiblemente no hay repuestos.

Fuente: Propia

Continuación Tabla No: 41, se identifica las amenazas vs vulnerabilidades sobre los activos de información de la categoría Hardware de la entidad.

Tabla No: 41 Amenazas - vulnerabilidades

Nombre del activo de información	Amenazas Metodología Magerit	Vulnerabilidades
[HW] Equipamiento informático.[host]_[host]_Estaciones de trabajo.	[A,23]~Manipulación de equipos.	Deficiencia en los controles para acceder a las estaciones de trabajo de la entidad.
[HW] Equipamiento informático.[host]_[host]_Estaciones de trabajo.	[A,25]~Robo.	Deficiencia en los controles para acceder a las estaciones de trabajo de la entidad.
[HW] Equipamiento informático.[host]_[host]_Estaciones de trabajo.	[A,26]~Ataque destructivo.	Es posible daños a consecuencia del ejercicio de paro social del orden Nacional/Departamental/Municipal bajo actividades de actos vandálicos.
[HW] Equipamiento informático.[host]_[host]_Estaciones de trabajo.	[I,3]~Contaminación mecánica.	El activo de Información es susceptible a accidentes o daños deliberados.
[HW] Equipamiento informático.[host]_[host]_Estaciones de trabajo.	[I,5]~Avería de origen físico o lógico.	Averías propias del dispositivo que pueden ser tanto de tipo lógico como físico.
[HW] Equipamiento informático.[phone]_[phone]_Telefonos.	[I,5]~Avería de origen físico o lógico.	Averías propias del dispositivo que pueden ser tanto de tipo lógico como físico.
[HW] Equipamiento informático.[phone]_[phone]_Telefonos.	[N,*]~Desastres naturales.	Deficiente plan de prevención contra desastres naturales, que incluyan rayos, tormentas, eléctricas, inundación.
[HW] Equipamiento informático.[pabx]_[pabx]_Servidor [PSTN].	[E,2]~Error de administrador.	Deficiencia en la configuración en el volumen de almacenamiento puede afectar el adecuado funcionamiento, para el activo relacionado.
[HW] Equipamiento informático.[pabx]_[pabx]_Servidor [PSTN].	[E,23]~Error de mantenimiento / actualización de los equipos (hardware).	Deficiente cumplimiento del plan de mantenimiento e instalación ineficiente para hardware posiblemente no hay repuestos.

Fuente: Propia

Continuación Tabla No: 41, se identifica las amenazas vs vulnerabilidades sobre los activos de información de la categoría Hardware de la entidad.

Tabla No: 41 Amenazas - vulnerabilidades

Nombre del activo de información	Amenazas Metodología Magerit	Vulnerabilidades
[HW] Equipamiento informático.[pabx]_[pabx]_ Servidor [PSTN].	[A,26]~Ataque destructivo.	Es posible daños a consecuencia del ejercicio de paro social del orden Nacional/Departamental/Municipal bajo actividades de actos vandálicos.
[HW] Equipamiento informático.[pabx]_[pabx]_ Servidor [PSTN].	[I,3]~Contaminación mecánica.	El activo de Información es susceptible a accidentes o daños deliberados.
[HW] Equipamiento informático.[pabx]_[pabx]_ Servidor [PSTN].	[I,5]~Avería de origen físico o lógico.	Averías propias del dispositivo que pueden ser tanto de tipo lógico como físico.
[HW] Equipamiento informático.[pabx]_[pabx]_ Servidor [PSTN].	[I,7]~Condiciones inadecuadas de temperatura o humedad.	El hardware es usado en espacios físicos que no cumplen los requerimientos de temperatura y humedad que exige el fabricante, no hay forma de evaluar su cumplimiento, para el activo de información relacionado.
[HW] Equipamiento informático.[pabx]_[pabx]_ Servidor [PSTN].	[N,*]~Desastres naturales.	Deficiente plan de prevención contra desastres naturales, que incluyan rayos, tormentas, eléctricas, inundación.
[HW] Equipamiento informático.[network] _[network] _Router	[E,2]~Error de administrador.	Deficiencia en la configuración en el volumen de almacenamiento puede afectar el adecuado funcionamiento, para el activo relacionado.
[HW] Equipamiento informático.[network] _[network] _Router	[E,23]~Error de mantenimiento / actualización de los equipos (hardware).	Deficiente cumplimiento del plan de mantenimiento e instalación ineficiente para hardware posiblemente no hay repuestos.
[HW] Equipamiento informático.[network] _[network] _Router	[A,26]~Ataque destructivo.	Es posible daños a consecuencia del ejercicio de paro social del orden Nacional/Departamental/Municipal bajo actividades de actos vandálicos.

Fuente: Propia

Continuación Tabla No: 41, se identifica las amenazas vs vulnerabilidades sobre los activos de información de la categoría Hardware de la entidad.

Tabla No: 41 Amenazas - vulnerabilidades

Nombre del activo de información	Amenazas Metodología Magerit	Vulnerabilidades
[HW] Equipamiento informático.[network] _[network] _Router	[I,3]~Contaminación mecánica.	El activo de Información es susceptible a accidentes o daños deliberados.
[HW] Equipamiento informático.[network] _[network] _Router	[I,5]~Avería de origen físico o lógico.	Averías propias del dispositivo que pueden ser tanto de tipo lógico como físico.
[HW] Equipamiento informático.[network] _[network] _Router	[I,7]~Condiciones inadecuadas de temperatura o humedad.	El hardware es usado en espacios físicos que no cumplen los requerimientos de temperatura y humedad que exige el fabricante, no hay forma de evaluar su cumplimiento, para el activo de información relacionado.
[HW] Equipamiento informático.[network] _[network] _Router	[N,*]~Desastres naturales.	Deficiente plan de prevención contra desastres naturales, que incluyan rayos, tormentas, eléctricas, inundación.
[HW] Equipamiento informático.[network] _[network] _Switches Core.	[E,2]~Error de administrador.	Deficiencia en la configuración en el volumen de almacenamiento puede afectar el adecuado funcionamiento, para el activo relacionado.
[HW] Equipamiento informático.[network] _[network] _Switches Core.	[E,23]~Error de mantenimiento / actualización de los equipos (hardware).	Deficiente cumplimiento del plan de mantenimiento e instalación ineficiente para hardware posiblemente no hay repuestos.
[HW] Equipamiento informático.[network] _[network] _Switches Core.	[A,26]~Ataque destructivo.	Es posible daños a consecuencia del ejercicio de paro social del orden Nacional/Departamental/Municipal bajo actividades de actos vandálicos.
[HW] Equipamiento informático.[network] _[network] _Switches Core.	[I,3]~Contaminación mecánica.	El activo de Información es susceptible a accidentes o daños deliberados.

Fuente: Propia

Continuación Tabla No: 41, se identifica las amenazas vs vulnerabilidades sobre los activos de información de la categoría Hardware de la entidad.

Tabla No: 41 Amenazas - vulnerabilidades

Nombre del activo de información	Amenazas Metodología Magerit	Vulnerabilidades
[HW] Equipamiento informático.[network] _[network] _Switches Core.	[I,5]~Avería de origen físico o lógico.	Averías propias del dispositivo que pueden ser tanto de tipo lógico como físico.
[HW] Equipamiento informático.[network] _[network] _Switches Core.	[I,7]~Condiciones inadecuadas de temperatura o humedad.	El hardware es usado en espacios físicos que no cumplen los requerimientos de temperatura y humedad que exige el fabricante, no hay forma de evaluar su cumplimiento, para el activo de información relacionado.
[HW] Equipamiento informático.[network] _[network] _Switches Core.	[N,*]~Desastres naturales.	Deficiente plan de prevención contra desastres naturales, que incluyan rayos, tormentas, eléctricas, inundación.
[HW] Equipamiento informático.[network] _[network] _Switches Acceso.	[E,2]~Error de administrador.	Deficiencia en la configuración en el volumen de almacenamiento puede afectar el adecuado funcionamiento, para el activo relacionado.
[HW] Equipamiento informático.[network] _[network] _Switches Acceso.	[E,23]~Error de mantenimiento / actualización de los equipos (hardware).	Deficiente cumplimiento del plan de mantenimiento e instalación ineficiente para hardware posiblemente no hay repuestos.
[HW] Equipamiento informático.[network] _[network] _Switches Acceso.	[A,26]~Ataque destructivo.	Es posible daños a consecuencia del ejercicio de paro social del orden Nacional/Departamental/Municipal bajo actividades de actos vandálicos.
[HW] Equipamiento informático.[network] _[network] _Switches Acceso.	[I,3]~Contaminación mecánica.	El activo de Información es susceptible a accidentes o daños deliberados.
[HW] Equipamiento informático.[network] _[network] _Switches Acceso.	[I,5]~Avería de origen físico o lógico.	Averías propias del dispositivo que pueden ser tanto de tipo lógico como físico.

Fuente: Propia

Continuación Tabla No: 41, se identifica las amenazas vs vulnerabilidades sobre los activos de información de la categoría Hardware de la entidad.

Tabla No: 41 Amenazas - vulnerabilidades

Nombre del activo de información	Amenazas Metodología Magerit	Vulnerabilidades
[HW] Equipamiento informático.[network] _[network] _Switches Acceso.	[I,7]~Condiciones inadecuadas de temperatura o humedad.	El hardware es usado en espacios físicos que no cumplen los requerimientos de temperatura y humedad que exige el fabricante, no hay forma de evaluar su cumplimiento, para el activo de información relacionado.
[HW] Equipamiento informático.[network] _[network] _Switches Acceso.	[N,*]~Desastres naturales.	Deficiente plan de prevención contra desastres naturales, que incluyan rayos, tormentas, eléctricas, inundación.
[HW] Equipamiento informático.[network] _[network] _Switches Caseros.	[E,23]~Error de mantenimiento / actualización de los equipos (hardware).	Deficiente cumplimiento del plan de mantenimiento e instalación ineficiente para hardware posiblemente no hay repuestos.
[HW] Equipamiento informático.[network] _[network] _Switches Caseros.	[A,26]~Ataque destructivo.	Es posible daños a consecuencia del ejercicio de paro social del orden Nacional/Departamental/Municipal bajo actividades de actos vandálicos.
[HW] Equipamiento informático.[network] _[network] _Switches Caseros.	[I,7]~Condiciones inadecuadas de temperatura o humedad.	El hardware es usado en espacios físicos que no cumplen los requerimientos de temperatura y humedad que exige el fabricante, no hay forma de evaluar su cumplimiento, para el activo de información relacionado.
[HW] Equipamiento informático.[network] _[network] _Puntos de acceso inalambrico.	[E,23]~Error de mantenimiento / actualización de los equipos (hardware).	Deficiente cumplimiento del plan de mantenimiento e instalación ineficiente para hardware posiblemente no hay repuestos.
[HW] Equipamiento informático.[network] _[network] _Puntos de acceso inalambrico.	[A,26]~Ataque destructivo.	Es posible daños a consecuencia del ejercicio de paro social del orden Nacional/Departamental/Municipal bajo actividades de actos vandálicos.

Fuente: Propia

Continuación Tabla No: 41, se identifica las amenazas vs vulnerabilidades sobre los activos de información de la categoría Hardware de la entidad.

Tabla No: 41 Amenazas - vulnerabilidades

Nombre del activo de información	Amenazas Metodología Magerit	Vulnerabilidades
[HW] Equipamiento informático.[network] _[network] _Puntos de acceso inalambrico.	[I,7]~Condiciones inadecuadas de temperatura o humedad.	El hardware es usado en espacios físicos que no cumplen los requerimientos de temperatura y humedad que exige el fabricante, no hay forma de evaluar su cumplimiento, para el activo de información relacionado.
[COM] Redes de comunicaciones [PSTN] _Servicio de de telefonia analoga.	[I,8]~Fallo de servicios de comunicaciones.	Deficiencia relacionada con la infraestructura de redes de voz y datos de la entidad.
[COM] Redes de comunicaciones [PSTN] _Servicio de de telefonia analoga.	[A,6]~Abuso privilegios de acceso.	Deficiente estrategia de segmentación de red, facilitando el acceso no autorizado.
[COM] Redes de comunicaciones [PSTN] _Servicio de de telefonia analoga.	[A,7]~Uso no previsto.	Ineficientes políticas restrictivas, que eviten el uso personal del activo relacionado.
[COM] Redes de comunicaciones[Internet]_ Servicio de internet dedicado para la organización	[A,6]~Abuso privilegios de acceso.	Deficiente estrategia de segmentación de red, facilitando el acceso no autorizado.
[COM] Redes de comunicaciones[Internet]_ Servicio de internet dedicado para la organización	[A,7]~Uso no previsto.	No existen políticas restrictivas, que eviten el acceso a sitios web maliciosos.
[COM] Redes de comunicaciones[Internet]_ Servicio de internet dedicado para la organización	[I,8]~Fallo de servicios de comunicaciones.	Deficiencia relacionada con la infraestructura de redes de voz y datos de la entidad.

Fuente: Propia

Continuación Tabla No: 41, se identifica las amenazas vs vulnerabilidades sobre los activos de información de la categoría [COM] comunicación de la entidad

Tabla No: 41 Amenazas - vulnerabilidades

Nombre del activo de información	Amenazas Metodología Magerit	Vulnerabilidades
[COM] Redes de comunicaciones[wifi]_Radio enlace local (WI-FI).	[I,8]~Fallo de servicios de comunicaciones.	Deficiencia relacionada con la infraestructura de redes de voz y datos de la entidad.
[COM] Redes de comunicaciones[wifi]_Radio enlace local (WI-FI).	[E,19]~Fuga de información.	Deficiencia en la configuración de seguridad del servicio afectando la adecuada gestión de la seguridad, para el activo relacionado.
[COM] Redes de comunicaciones[wifi]_Radio enlace local (WI-FI).	[E,23]~Error de mantenimiento / actualización de los equipos (hardware).	Deficiente cumplimiento del plan de mantenimiento e instalación ineficiente para hardware posiblemente no hay repuestos.
[COM] Redes de comunicaciones[wifi]_Radio enlace local (WI-FI).	[E,24]~Caída del sistema, causa agotamiento de recursos.	La demanda de recursos de la entidad supera los recursos físicos, técnicos con los que se cuenta, propiciando pérdida de disponibilidad, intermitencia, interferencia, interferencia de los recursos, para el activo relacionado.
[COM] Redes de comunicaciones[wifi]_Radio enlace local (WI-FI).	[A,6]~Abuso privilegios de acceso.	Deficiente estrategia de segmentación de red, facilitando el acceso no autorizado.
[COM] Redes de comunicaciones[wifi]_Radio enlace local (WI-FI).	[A,11]~Acceso no autorizado.	Deficiente estrategia de segmentación de red, facilitando el acceso no autorizado.
[COM] Redes de comunicaciones[wifi]_Radio enlace local (WI-FI).	[A,12]~Análisis de tráfico.	Deficiencia en el análisis de logs de tráfico, no hay sistemas especializados de lectura de log , que faciliten la gestión del tráfico, los log se leen de forma nativa.

Fuente: Propia

Continuación Tabla No: 41, se identifica las amenazas vs vulnerabilidades sobre los activos de información de la categoría [COM] comunicación de la entidad

Tabla No: 41 Amenazas - vulnerabilidades

Nombre del activo de información	Amenazas Metodología Magerit	Vulnerabilidades
[COM] Redes de comunicaciones[wifi]_Radio enlace local (WI-FI).	[A,14]~Interceptación de información (escucha).	Deficiencia en la configuración y parametrización de protocolos de seguridad, que permita la creación de ACL y asignación de IP para establecer directrices de aceptación o negación de conexión a la red de Voz y Datos.
[COM] Redes de comunicaciones[LAN]_Red de área local	[I,8]~Fallo de servicios de comunicaciones.	Deficiencia relacionada con la infraestructura de redes de voz y datos de la entidad.
[COM] Redes de comunicaciones[LAN]_Red de área local	[E,19]~Fuga de información.	Deficiencia en la configuración de seguridad del servicio afectando la adecuada gestión de la seguridad, para el activo relacionado.
[COM] Redes de comunicaciones[LAN]_Red de área local	[E,23]~Error de mantenimiento / actualización de los equipos (hardware).	Deficiente cumplimiento del plan de mantenimiento e instalación ineficiente para hardware posiblemente no hay repuestos.
[COM] Redes de comunicaciones[LAN]_Red de área local	[E,24]~Caída del sistema, causa agotamiento de recursos.	La demanda de recursos de la entidad supera los recursos físicos, técnicos con los que se cuenta, propiciando pérdida de disponibilidad, intermitencia, interferencia, interferencia de los recursos, para el activo relacionado.
[COM] Redes de comunicaciones[LAN]_Red de área local	[A,6]~Abuso privilegios de acceso.	Deficiente estrategia de segmentación de red, facilitando el acceso no autorizado.
[COM] Redes de comunicaciones[LAN]_Red de área local	[A,11]~Acceso no autorizado.	Deficiente estrategia de segmentación de red, facilitando el acceso no autorizado.

Fuente: Propia

Continuación Tabla No: 41, se identifica las amenazas vs vulnerabilidades sobre los activos de información de la categoría [COM] comunicación de la entidad.

Tabla No: 41 Amenazas - vulnerabilidades

Nombre del activo de información	Amenazas Metodología Magerit	Vulnerabilidades
[COM] Redes de comunicaciones[LAN]_Red de área local	[A,12]~Análisis de tráfico.	Deficiencia en el análisis de logs de tráfico, no hay sistemas especializados de lectura de logs, que faciliten la gestión del tráfico, los logs se leen de forma nativa.
[COM] Redes de comunicaciones[LAN]_Red de área local	[A,14]~Interceptación de información (escucha).	Deficiencia en la configuración y parametrización de protocolos de seguridad, que permita la creación de ACL y asignación de IP para establecer directrices de aceptación o negación de conexión a la red de Voz y Datos.
[AUX] Equipamiento auxiliar.[ups]_UPS dedicado para los servidores.	[N,2]~Daños por agua.	Ubicación de las UPS en espacio muy próximo a fuentes de agua.
[AUX] Equipamiento auxiliar.[ups]_UPS dedicado para los servidores.	[I,3]~Contaminación mecánica.	El activo de Información es susceptible a accidentes o daños deliberados.
[AUX] Equipamiento auxiliar.[ups]_UPS dedicado para los servidores.	[E,23]~Error de mantenimiento / actualización de los equipos (hardware).	Deficiente cumplimiento del plan de mantenimiento e instalación ineficiente para hardware posiblemente no hay repuestos.
[AUX] Equipamiento auxiliar.[ac]_Aire acondicionado dedicado para los servidores.	[I,3]~Contaminación mecánica.	El activo de Información es susceptible a accidentes o daños deliberados.
[AUX] Equipamiento auxiliar.[ac]_Aire acondicionado dedicado para los servidores.	[E,23]~Error de mantenimiento / actualización de los equipos (hardware).	Deficiente cumplimiento del plan de mantenimiento e instalación ineficiente para hardware posiblemente no hay repuestos.

Fuente: Propia

Continuación Tabla No: 41, se identifica las amenazas vs vulnerabilidades sobre los activos de información de la categoría [AUX] Equipamiento auxiliar de comunicación de la entidad.

Tabla No: 41 Amenazas – vulnerabilidades

Nombre del activo de información	Amenazas Metodología Magerit	Vulnerabilidades
[AUX] Equipamiento auxiliar.[cabling][wire]_Cableado electrico.	[E,23]~Error de mantenimiento / actualización de los equipos (hardware).	Deficiente cumplimiento del plan de mantenimiento e instalación ineficiente para hardware posiblemente no hay repuestos.
[L] Instalaciones.Sede principal (Edificio).	[N,*]~Desastres naturales.	Deficiente plan de prevención contra desastres naturales, que incluyan rayos, tormentas, eléctricas, inundación.
[L] Instalaciones.Sede principal (Edificio).	[I,*]~Desastres industriales.	Deficiente plan de prevención contra desastres industriales.
[L] Instalaciones.Sede principal (Edificio).	[A,11]~Acceso no autorizado.	Pendiente aumentar los niveles de Gestión Biométrica o monitoreo que limiten el acceso a las instalaciones de la entidad.
[L] Instalaciones.Sede principal (Edificio).	[A,26]~Ataque destructivo.	Es posible daños a consecuencia del ejercicio de paro social del orden Nacional/Departamental/Municipal bajo actividades de actos vandálicos.
[P] Personal.[ui]_Usuario interno (Cantidad:2)	[E,7]~Deficiencia en la organización.	Existe una jerarquía de roles y responsabilidades, pero los sistemas presentan falencias en su implementación.
[P] Personal.[ui]_Usuario interno (Cantidad:2)	[E,19]~Fuga de información.	Inexistencia de monitoreo, logs para la auditoría con el objeto de validar el uso y acceso a los datos.
[P] Personal.[ui]_Usuario interno (Cantidad:2)	[E,28]~Indisponibilidad de personal.	Ausencia de RH por motivos médicos, incertidumbre relacionada con incidencias de tipo público o privada, entre otros.
[P] Personal.[ui]_Usuario interno (Cantidad:2)	[A,28]~Indisponibilidad del personal.	Ausencia de RH por motivos médicos, incertidumbre relacionada con incidencias de tipo público o privada, entre otros.

Fuente: Propia

Continuación Tabla No: 41, se identifica las amenazas vs vulnerabilidades sobre los activos de información de la categoría Personal [P] de la entidad.

Tabla No: 41 Amenazas – vulnerabilidades

Nombre del activo de información	Amenazas Metodología Magerit	Vulnerabilidades
[P] Personal.[ui]_Usuario interno (Cantidad:2)	[A,29]~Extorsión.	Obligar al funcionario por medio de algún tipo de intimidación, para ejecutar acciones ilícitas que pueden perjudicar de forma parcial o total a la entidad.
[P] Personal.[adm]_Técnicos para administración y mantenimiento (Cantidad:2)	[E,7]~Deficiencia en la organización.	Existe una jerarquía de roles y responsabilidades, pero los sistemas presentan falencias en su implementación.
[P] Personal.[adm]_Técnicos para administración y mantenimiento (Cantidad:2)	[E,19]~Fuga de información.	Inexistencia de monitoreo, logs para la auditoría con el objeto de validar el uso y acceso a los datos.
[P] Personal.[adm]_Técnicos para administración y mantenimiento (Cantidad:2)	[E,28]~Indisponibilidad de personal.	Ausencia de RH por motivos médicos, incertidumbre relacionada con incidencias de tipo público o privada, entre otros.
[P] Personal.[adm]_Técnicos para administración y mantenimiento (Cantidad:2)	[A,28]~Indisponibilidad del personal.	Ausencia de RH por motivos médicos, incertidumbre relacionada con incidencias de tipo público o privada, entre otros.
[P] Personal.[adm]_Técnicos para administración y mantenimiento (Cantidad:2)	[A,29]~Extorsión.	Obligar al funcionario por medio de algún tipo de intimidación, para ejecutar acciones ilícitas que pueden perjudicar de forma parcial o total a la entidad.
[P] Personal.[sub]_Contratista de apoyo (Cantidad:1)	[E,7]~Deficiencia en la organización.	Existe una jerarquía de roles y responsabilidades, pero los sistemas presentan falencias en su implementación.
[P] Personal.[sub]_Contratista de apoyo (Cantidad:1)	[E,19]~Fuga de información.	Inexistencia de monitoreo, logs para la auditoría con el objeto de validar el uso y acceso a los datos.

Fuente: Propia

Continuación Tabla No: 41, se identifica las amenazas vs vulnerabilidades sobre los activos de información de la categoría Personal [P] de la entidad.

Tabla No: 41 Amenazas – vulnerabilidades

Nombre del activo de información	Amenazas Metodología Magerit	Vulnerabilidades
[P] Personal.[sub]_Contratista de apoyo (Cantidad:1)	[E,28]~Indisponibilidad de personal.	Ausencia de RH por motivos médicos, incertidumbre relacionada con incidencias de tipo público o privada, entre otros.
[P] Personal.[sub]_Contratista de apoyo (Cantidad:1)	[A,28]~Indisponibilidad del personal.	Ausencia de RH por motivos médicos, incertidumbre relacionada con incidencias de tipo público o privada, entre otros.
[P] Personal.[sub]_Contratista de apoyo (Cantidad:1)	[A,29]~Extorsión.	Obligar al funcionario por medio de algún tipo de intimidación, para ejecutar acciones ilícitas que pueden perjudicar de forma parcial o total a la entidad.

Fuente: Propia

9.3. Valorización de amenazas

Es necesario establecer un valor a las amenazas relacionadas a los activos de información, teniendo como referente el modelo MAGERIT, para lo cual según el modelo es necesario reconocer el impacto y probabilidad del riesgo lo cual se estimará a continuación.

9.3.1. Probabilidad de ocurrencia del riesgo.

Se define la probabilidad, como la posibilidad que se materialice un riesgo, se sugiere para esta actividad medirlo con el criterio de la frecuencia en el tiempo, es decir un número de veces en el que un riesgo se materializa en un rango de tiempo establecido, o la estimación de la posibilidad que se materialice por circunstancias que pueden ser de tipo interno o externo.

El Cuadro No 1, se identifica Metodología Magerit probabilidad del riesgo para los activos de información de la entidad.

cuadro No 1 Metodología Magerit probabilidad del riesgo –

PROBABILIDAD DEL RIESGO					
	Nomenclatura	**Categoría**	**Descripción**	**Frecuencia de suceso.**	**Nivel**
Probabilidad	MA	**Aproximadamente seguro.**	**Incidencia que se espera que suceda en la mayoría de las condiciones.**	**Ocurrió más de una (1) vez en lo que va del año.**	5
	A	**Probable.**	**Incidencia probablemente suceda en la mayoría de las condiciones.**	**Por lo menos ocurrió una (1) vez en lo que va del año.**	4
	M	**Posible.**	**Incidencia es posible que suceda en algún momento**	**Por lo menos ocurrió una (1) vez en los últimos dos (2) años.**	3
	B	**Escaso Probable.**	**Incidencia escasamente sucede en algún momento.**	**Por lo menos ocurrió una vez en los últimos cuatro (4) años.**	2
	MB	**Raro.**	**Incidencia solo sucede en algún momento extraordinario.**	**No ha ocurrido en los últimos cuatro (4) años.**	1
Fuente: Propia					

Para identificar la probabilidad que un riesgo se materialice se hace mediante entrevista frente a un enfoque de reconocer la posibilidad que se materialice un riesgo, midiendo con el criterio de la frecuencia, es decir identificando el número de veces que un riesgo se materializa en un rango de tiempo establecido, o de la posibilidad que se materialice por circunstancias que pueden ser de tipo interno o externo.

Con relación a lo anterior se reconoce que este tipo de entidades lleva muy poco tiempo trabajando con un sistema de gestión de incidencias de mesas de ayuda HELP DESK por lo que no es posible determinar una estadística de ocurrencia de los riesgos, por tanto, a partir del reconocimiento se lleva a determinar la probabilidad mediante una percepción netamente subjetiva durante el levantamiento de la información, por lo que se documenta un estimado de probabilidad.

9.3.2. Impacto en Caso de la Ocurrencia del Riesgo.

Ahora teniendo en cuenta, típicamente el área de sistemas y/o telemática es la encargada de la infraestructura de red de telecomunicaciones en las entidades públicas dedicadas a promover la ciencia, tecnología e innovación tecnológica de la ciudad de Cali, siendo transversal a los demás procesos (departamentos), de esta manera, será la encargada de tener en cuenta las características, servicios necesarios para definir la escala para darle valor al impacto.

Entonces: Impacto se debe de comprender para el contexto de infraestructura de TI, como el resultado negativo que produce una incidencia a la entidad en el momento de materializarse un riesgo, lo siguiente se basa en el manual de la administración del riesgo y MAGERIT.

El cuadro No 2, se identifica Metodología Magerit Impacto del riesgo para los activos de información de la entidad.

Cuadro No 2 Metodología Magerit Impacto del Riesgo

IMPACTO DEL RIESGO				
	Nomenclatura	**Categoría**	**Descripción**	**Valoración**
Impacto	MA	**Muy Alto.**	**Incidencia afecta a toda la entidad y a su vez afecta a terceros o a otra entidad.**	5
	A	**Alto.**	**Incidencia afecta a toda la entidad.**	4
	M	**Medio.**	**Incidencia afecta a más un proceso (Departamento) de la entidad.**	3
	B	**Bajo.**	**Incidencia afecta a un proceso (Departamento) de la entidad.**	2
	MB	**Muy Bajo.**	**Incidencia solo afecta a un funcionario, y este no es de alta gerencia.**	1
Fuente: Propia				

9.3.3. Valoración del riesgo.

Para identificar la valoración de cada riesgo mediante la matriz de **VALORACIÓN DEL RIESGO** se debe de asignar una ubicación mediante la intercepción de la probabilidad vs Impacto basada en la guía de la DAFP pagina 42 y Manual de administración del Riesgo.

En el cuadro No 3, se identifica Metodología Magerit valoración del riesgo para los activos de información de la entidad.

Tabla No 3 Metodología Magerit Valoración del Riesgo

VALORACIÓN DEL RIESGO						
IMPACTO	MA					
	A					
	M					
	B					
	MB					
RIESGO		MB	B	M	A	MA
		PROBABILIDAD				

VALORACIÓN DEL RIESGO			
	Nomenclatura	Categoría	Valoración
Valoracion del riesgo	MA	**Critico**	21 a 25
	A	**Importante**	16 a 20
	M	**Apreciable**	10 a 15
	B	**Bajo**	5 a 9
	MB	**Despreciable**	1 a 4

Fuente: Propia

Blanco: Zona que indica riesgo Muy bajo, se debe de asumir el riesgo.
Verde: Zona que indica riesgo bajo, se debe de asumir el riesgo.
Amarillo: Zona que indica riesgo Moderado, se debe de asumir el riesgo.
Naranja: Zona que indica riesgo alto, se debe de minimizar el riesgo por tanto se debe evitar, compartir o transferir.
Rojo: Zona que indica riesgo Muy alto, se debe de minimizar el riesgo por tanto se debe evitar, compartir o transferir.

La matriz de valoración del Riego se estima con cinco (5) niveles, Muy bajo despreciable, bajo, apreciable, pero se asume, importante y crítico.

9.3.4. Prioridades de los riesgos para su manejo y para su posible adición a las políticas.

En este aparte es donde se define el nivel de aceptación del riesgo, por ello, se debe de evitar resultados subjetivos a los controles, dado que puede ser posible que un riesgo posea varios controles, o no se haya aplicado ninguno al momento del análisis y por esto, hay que tener en cuenta para poder dar prioridad a los riesgos los siguientes datos.

Calculo Riesgo Neto: Valoración del Riesgo X Probabilidad del riesgo.

Criticidad: Si Calculo Riesgo Neto <= 4 Despreciable,
Si Calculo Riesgo Neto <= 9 Bajo,
Si Calculo Riesgo Neto <= 15 Apreciable,
Si Calculo Riesgo Neto <= 20 Importante,
Si Calculo Riesgo Neto <= 25 Critico

En el cuadro No: 4 se identifica Metodología Magerit escala de valoración del riesgo para los activos de información de la entidad.

Cuadro No: 4 Valoración Criticidad Neta

Nivel	**Escala Valoración de criticidad.**
Despreciable	1 a 4
Bajo	5 a 9
Apreciable	10 a 15
Importante	16 a 20
Critico	21 a 25

Fuente: Propia

Con esta escala de valoración, es posible presentar un análisis resumido con relación a la escala de criticidad de las amenazas identificadas:

Se tomó 244 amenazas, que están relacionados a los activos de información que se reconocieron previamente para este tipo de entidad.

Se logra determinar que este tipo de entidad presenta un abanico amplio de amenazas, que quizás debido a su falta de capacidad adquisitiva con el correr de los tiempos, propicia el incremento de amenazas, particularmente se puede notar dado que aún existe presencia de sistemas operativos como Windows XP, Vista, Seven, implícitamente sugiere una ausencia de salvaguardas, en el siguiente cuadro se mostrara una relación de criticidad para la entidad.

En el cuadro 5 se identifica Metodología Magerit cantidad de amenazas identificadas para los activos de información de la entidad.

Cuadro No: 5 Valoración Criticidad, Cantidad de amenazas identificadas

Nivel	**Cantidad de amenazas identificadas**
Despreciable	
Bajo	14
Apreciable	5
Importante	11
Critico	212
TOTAL	**244**

Fuente: Propia

Por otra parte, es posible analizar los niveles de gestión que pueden presentar los activos de información con relación a las amenazas identificadas

Gestión: Si tiene Gestión = 1,
Si tiene Gestión, pero no es efectivo = 2,
Si tiene Gestión, es efectivo, pero no está documentado = 3,
Si tiene Gestión, es efectivo, y está documentado = 4.

En la tabla 42 se identifica Metodología Magerit Valoración niveles de gestión para las amenazas identificadas para los activos de información de la entidad.

Tabla No: 42 Valoración niveles de gestión.

Nivel	Escala niveles de gestión.
Si tiene Gestión, es efectivo, y está documentado	4
Si tiene Gestión, es efectivo, pero no está documentado	3
Si tiene Gestión, pero no es efectivo	2
Si tiene Gestión	1

Fuente: Propia

Se logra determinar que este tipo de entidad sus niveles de gestión son bajos lo cual se detallara en el siguiente cuadro:

En la tabla 43 se identifica Metodología Magerit Valoración Criticidad Neta vs niveles de gestión para las amenazas identificadas para los activos de información de la entidad.

Tabla No: 48 Valoración Criticidad Neta

Nivel	Escala niveles de gestión.
Si tiene Gestión, es efectivo, y está documentado	0
Si tiene Gestión, es efectivo, pero no está documentado	33
Si tiene Gestión, pero no es efectivo	42
No tiene Gestión	169
TOTAL	**244**

Fuente: Propia

9.3.5. Identificación de controles.

Con relación a lo anterior para los activos de información se logra comprender que hay una correlación entre los niveles de gestión y el personal de soporte técnico, se logra entender que este tipo de entidades, cuenta con poco personal de soporte

técnico, lo que influye en la capacidad de gestionar salvaguardas, necesarias para proteger los activos de información.

Posible estrategia seria, transferir responsabilidades a terceros o ejecutar procesos de contratación de contratistas para soporte en sitio, con el objeto de apoyar las actividades necesarias para asegurar los activos de información en la entidad.

Teniendo en cuenta el anterior capitulo se evidenciaron fallos, relacionados con configuraciones, entre otras vulnerabilidades; vulnerabilidades que tienen que ser subsanadas y evaluar la posibilidad de establecer nuevos controles, que implican el ejercicio de establecer salvaguardas.

Ahora se presentará los controles identificados, tomando como base de conocimiento el Anexo A de la ISO 27001:

Por lo cual se ejecuta evaluación de riesgos con respeto a los activos de información, partiendo de lo cual se establecerán unos controles con el objeto de reducir la criticidad relacionados con la siguiente tabla:

Riesgo Residual: Calculo Riesgo Neto / Gestión

En la tabla 44 se identifica Metodología Magerit Valoración residual de las amenazas por las amenazas identificadas para los activos de información de la entidad.

Tabla No: 44 Valoración residual de las amenazas.

Nivel	Cantidad de amenazas por categoría
Despreciable	2
Bajo	14
Apreciable	5
Importante	11
Critico	212
TOTAL	244

Fuente: Propia

La siguiente actividad permite evaluar los niveles de aceptación de los riesgos, teniendo en cuenta el apetito de riesgo en donde se toma en consideración los niveles de riesgos qué serán asumibles, donde cabe riesgo moderado y/o aceptable, con la claridad que se deben de tratar toda amenaza que encuadren enmarcadas como inaceptables.

Teniendo en cuenta la escala de valoración del riego, se va tomar la siguiente escala de valores, con lo cual podremos determinar la prioridad de los riesgos a tratar así:

Niveles de aceptación del riesgo.

Teniendo en cuenta el riesgo Residual con relación al nivel de gestión así:

Riesgo Residual = Calculo del riesgo neto / Calificación de Gestión

Nivel Aceptación Riesgo = Riesgo Residual

Donde el nivel de Aceptación del Riesgo se tomaría los siguientes Rangos.

Entre 1 a 5 aceptable (A).
Entre 6 a 15 moderado (M).
Entre 16 a 25 inaceptable (I).

Con relación a lo anterior se sugiere una paramétrica intuitiva, simple sin perder su importancia, rindiendo una clasificación e identificación de los riesgos lo cual al final del ejercicio se trata de obtener un nivel de riesgo aceptable y aprobado por la alta gerencia de la entidad. [32]

A continuación, en la siguiente tabla se establecerá un resumen donde se relaciona los niveles de aceptación:

[32]Administracionelectronica.gob.es. (2012). *MAGERIT versión 3 Libro II Catálogo de elementos (versión española): Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. (11.)*. P7-14 https://administracionelectronica.gob.es/pae_Home/dam/jcr:5fbe15c3-c797-46a6-acd8-51311f4c2d29/2012_Magerit_v3_libro2_catalogo-de-elementos_es_NIPO_630-12-171-8.pdf

En la tabla 50 se logra identifica a partir de la Metodología Magerit Niveles de aceptación del Riesgo - Cantidad de amenazas por nivel para los activos de información de la entidad.

Se logra evidenciar que en la entidad existe un elevado número (223) de amenazas que se identificaron como Inaceptable, de esta manera, se deben de ser tratadas, se enunciaran a continuación.

Tabla No: 45 Niveles de aceptación del Riesgo - Cantidad de amenazas por nivel

Niveles	Cantidad de amenazas por nivel
Aceptable	2
Moderado	19
Inaceptable	223
TOTAL	**244**

Fuente: Propia

En la tabla 46, se logra identifica a partir de la Metodología Magerit Evaluación de controles para amenazas por tratar. para los activos de información de la entidad.

Tabla No:46 Evaluación de controles para amenazas por tratar

Nombre del activo de información	Amenazas Metodologia Magerit		Control ISO 27001 Anexo A
[D] DATOS.[FILES]Archivos de apoyo y misionales.	[E,1]~Errores de usuario.	A5.1.1	Políticas de seguridad para la información
[D] DATOS.[FILES]Archivos de apoyo y misionales.	[E,2]~Error de administrador.	A8.2.1	Clasificación de la información
[D] DATOS.[FILES]Archivos de apoyo y misionales.	[A,15]~Modificación deliberada de información.	A8.2.3	Manejo de activos
[D] DATOS.[FILES]Archivos de apoyo y misionales.	[E,18]~Destrucción de información.	A9.2.3	Gestión derechos de acceso privilegiado
[D] DATOS.[backup]Copias de respaldo de configuracion de SW , Router.	[E,1]~Errores de usuario.	A12.1.1	Procedimientos de operación documentados.
[D] DATOS.[backup]Copias de respaldo de configuracion de SW , Router.	[E,2]~Error de administrador.	A12.4.3	Registro de administrador y de operador.
[D] DATOS.[backup]Copias de respaldo de configuracion de SW , Router.	[A,11]~Acceso no autorizado.	A9.2.3	Gestión derechos de acceso privilegiado.
[D] DATOS.[backup]Copia de respaldo estado MV.	[E,1]~Errores de usuario.	A12.1.1	Procedimientos de operación documentados.
[D] DATOS.[backup]Copia de respaldo estado MV.	[E,2]~Error de administrador.	A12.4.3	Registro de administrador y de operador.
[D] DATOS.[backup]Copia de respaldo estado MV.	[A,11]~Acceso no autorizado.	A9.2.3	Gestión derechos de acceso privilegiado.
[D] DATOS.[backup]Copia de respaldo BD.	[E,1]~Errores de usuario.	A12.1.1	Procedimientos de operación documentados.

Fuente: Propia

En la tabla 46 se logra identifica a partir de la Metodología Magerit Evaluación de controles para amenazas por tratar. para los activos de información de la entidad.

Continuación Tabla No: 46 Evaluación de controles para amenazas por tratar.

Nombre del activo de información	**Amenazas Metodologia Magerit**	**Control ISO 27001 Anexo A**	
[D] DATOS.[backup]Copia de respaldo BD.	[E,2]~Error de administrador.	A12.4.3	Registro de administrador y de operador.
[D] DATOS.[backup]Copia de respaldo BD.	[A,11]~Acceso no autorizado.	A9.2.3	Gestión derechos de acceso privilegiado.
[D] DATOS.Bases de datos de apoyo y misionales.	[E,1]~Errores de usuario.	A5.1.1	Políticas de seguridad para la información
[D] DATOS.Bases de datos de apoyo y misionales.	[E,2]~Error de administrador.	A8.2.1	Clasificación de la información
[D] DATOS.Bases de datos de apoyo y misionales.	[A,15]~Modificación deliberada de información.	A8.2.3	Manejo de activos
[D] DATOS.Bases de datos de apoyo y misionales.	[E,18]~Destrucción de información.	A9.2.3	Gestión derechos de acceso privilegiado
[S] Servicios.[www]Servicios de publicación del sitio web.	[E,2]~Error de administrador.	A15.1.3	Cadena suministro tecnología de información y comunicación
[S] Servicios.[www]Servicios de publicación del sitio web.	[A,11]~Acceso no autorizado.	A9.2.3	Gestión derechos de acceso privilegiado.
[S] Servicios.[www]Servicios de publicación del sitio web.	[E,18]~Destrucción de información.	A9.2.3	Gestión derechos de acceso privilegiado
[S] Servicios.[www]Servicios de publicación del sitio web.	[A,24]~Denegación de servicio.	A15.1.3	Suministro tecnología de información y comunicación
[S] Servicios.[EMAIL]Servicios de publicación correo electrónico	[E,2]~Error de administrador.	A9.2.1	Registro y cancelación registro usuarios
[S] Servicios.[EMAIL]Servicios de publicación correo electrónico	[A,5]~Suplantación de identidad del usuario.	A12.2.1	Controles contra código malicioso.
[S] Servicios.[INT]Servicios de impresión	[E,1]~Errores de usuario.	A12.1.1	Procedimientos de operación documentados.
[S] Servicios.[INT]Servicios de impresión	[E,2]~Error de administrador.	A7.2.2	Toma de conciencia, educación, formación de seguridad de información.
[S] Servicios.[INT]Servicios de impresión	[E,19]~Fuga de información.	A9.2.3	Gestión derechos de acceso privilegiado

Fuente: Propia

En la tabla 46 se logra identifica a partir de la Metodología Magerit Evaluación de controles para amenazas por tratar. para los activos de información de la entidad.

Continuación Tabla No: 46 Evaluación de controles para amenazas por tratar.

Nombre del activo de información	Amenazas Metodologia Magerit	Control ISO 27001 Anexo A	
[S] Servicios.[INT]Soporte técnico(R.H).	[E,24]~Caída del sistema, causa agotamiento de recursos.	A12.1.3	Gestión de capacidad.
[S] Servicios.[INT]Servicios IDS/IPS	[E,2]~Error de administrador.	A11.2.4	Mantenimiento de equipos.
[S] Servicios.[INT]Servicios IDS/IPS	[E,24]~Caída del sistema, causa agotamiento de recursos.	A12.1.3	Gestión de capacidad.
[S] Servicios.[INT]Servicios IDS/IPS	[A,24]~Denegación de servicio.	A13.1.2	Seguridad servicios de red
[S] Servicios.[INT]Servicios HITS	[E,2]~Error de administrador.	A11.2.4	Mantenimiento de equipos.
[S] Servicios.[INT]Servicios HITS	[E,24]~Caída del sistema, causa agotamiento de recursos.	A12.1.3	Gestión de capacidad.
[S] Servicios.[INT]Servicios HITS	[A,24]~Denegación de servicio.	A13.1.2	Seguridad servicios de red
[S] Servicios.[FTP]Protocolo de transferencia de archivos	[E,2]~Error de administrador.	A7.2.2	Toma de conciencia, educación, formación de seguridad de información.
[S] Servicios.[FTP]Protocolo de transferencia de archivos	[E,24]~Caída del sistema, causa agotamiento de recursos.	A12.1.3	Gestión de capacidad.
[S] Servicios.[FTP]Protocolo de transferencia de archivos	[A,24]~Denegación de servicio.	A13.1.2	Seguridad servicios de red
[S] Servicios.[FILE]Soporte en almacenamiento de archivos misionales y de apoyo.	[E,2]~Error de administrador.	A7.2.2	Toma de conciencia, educación, formación de seguridad de información.
[S] Servicios.[FILE]Soporte en almacenamiento de archivos misionales y de apoyo.	[E,24]~Caída del sistema, causa agotamiento de recursos.	A12.1.3	Gestión de capacidad.

Fuente: Propia

En la tabla 46 se logra identifica a partir de la Metodología Magerit Evaluación de controles para amenazas por tratar. para los activos de información de la entidad.

Continuación Tabla No: 46 Evaluación de controles para amenazas por tratar.

Nombre del activo de información	Amenazas Metodología Magerit	Control ISO 27001 Anexo A	
[S] Servicios.[FILE]Soporte en almacenamiento de archivos misionales y de apoyo.	[A,24]~Denegación de servicio.	A13.1.2	Seguridad servicios de red
[S] Servicios.[IDM]Soporte a gestión de usuarios y contraseñas.	[E,2]~Error de administrador.	A9.4.3	Sistema gestión de contraseñas
[S] Servicios.[IDM]Soporte a gestión de usuarios y contraseñas.	[E,24]~Caída del sistema, causa agotamiento de recursos.	A12.1.3	Gestión de capacidad.
[S] Servicios.[IDM]Soporte a gestión de usuarios y contraseñas.	[A,24]~Denegación de servicio.	A13.1.2	Seguridad servicios de red
[SW] Software.[dbms] _Bases de datos Mysql	[E,2]~Error de administrador.	A.14.2.3	Revisión técnica de aplicaciones después de cambios en la plataforma de operación
[SW] Software.[dbms] _Bases de datos Mysql	[E,20]~Vulnerabilidades de los programas (software).	A12.6.1	Gestión de las vulnerabilidades técnicas
[SW] Software.[dbms] _Bases de datos Mysql	[E,21]~Error de mantenimiento / actualización de los programas (software).	A18.2.3	Revisión del cumplimiento técnico
[SW] Software.[dbms] _Bases de datos PostgreSQL	[E,2]~Error de administrador.	A.14.2.3	Revisión técnica de aplicaciones después de cambios en la plataforma de operación
[SW] Software.[dbms] _Bases de datos PostgreSQL	[E,20]~Vulnerabilidades de los programas (software).	A12.6.1	Gestión de las vulnerabilidades técnicas
[SW] Software.[dbms] _Bases de datos PostgreSQL	[E,21]~Error de mantenimiento / actualización de los programas (software).	A18.2.3	Revisión del cumplimiento técnico
[SW] Software.[dbms] _Bases de datos Oracle12	[E,2]~Error de administrador.	A.14.2.3	Revisión técnica de aplicaciones después de cambios en la plataforma de operación
[SW] Software.[dbms] _Bases de datos Oracle12	[E,20]~Vulnerabilidades de los programas (software).	A12.6.1	Gestión de las vulnerabilidades técnicas

Fuente: Propia

En la tabla 46 se logra identifica a partir de la Metodología Magerit Evaluación de controles para amenazas por tratar. para los activos de información de la entidad.

Continuación Tabla No: 46 Evaluación de controles para amenazas por tratar.

Nombre del activo de información	**Amenazas Metodología Magerit**	**Control ISO 27001 Anexo A**	
[SW] Software.[dbms] _Bases de datos Oracle12	[E,21]~Error de mantenimiento / actualización de los programas (software).	A18.2.3	[SW] Software.[dbms] _Bases de datos Oracle12
[SW] Software.[os]_S.O Microsoft Windows 10	[E,1]~Errores de usuario.	A12.1.1	[SW] Software.[os]_S.O Microsoft Windows 10
[SW] Software.[os]_S.O Microsoft Windows 10	[E,20]~Vulnerabilidades de los programas (software).	A12.6.1	[SW] Software.[os]_S.O Microsoft Windows 10
[SW] Software.[os]_S.O Microsoft Windows 10	[E,21]~Error de mantenimiento / actualización de los programas (software).	A12.5.1	[SW] Software.[os]_S.O Microsoft Windows 10
[SW] Software.[os]_S.O Microsoft Windows 10	[A,6]~Abuso privilegios de acceso.	A9.2.3	[SW] Software.[os]_S.O Microsoft Windows 10
[SW] Software.[os]_S.O Microsoft Windows 10	[A,7]~Uso no previsto.	A16.1.1	[SW] Software.[os]_S.O Microsoft Windows 10
[SW] Software.[os]_S.O Microsoft Windows 7	[E,1]~Errores de usuario.	A12.1.1	[SW] Software.[os]_S.O Microsoft Windows 7
[SW] Software.[os]_S.O Microsoft Windows 7	[E,20]~Vulnerabilidades de los programas (software).	A12.6.1	[SW] Software.[os]_S.O Microsoft Windows 7
[SW] Software.[os]_S.O Microsoft Windows 7	[E,21]~Error de mantenimiento / actualización de los programas (software).	A12.5.1	[SW] Software.[os]_S.O Microsoft Windows 7
[SW] Software.[os]_S.O Microsoft Windows 7	[A,6]~Abuso privilegios de acceso.	A9.2.3	[SW] Software.[os]_S.O Microsoft Windows 7
[SW] Software.[os]_S.O Microsoft Windows 7	[A,7]~Uso no previsto.	A16.1.1	[SW] Software.[os]_S.O Microsoft Windows 7
[SW] Software.[os]_S.O Microsoft Windows Vista	[E,1]~Errores de usuario.	A12.1.1	[SW] Software.[os]_S.O Microsoft Windows Vista
[SW] Software.[os]_S.O Microsoft Windows Vista	[E,20]~Vulnerabilidades de los programas (software).	A12.6.1	[SW] Software.[os]_S.O Microsoft Windows Vista
[SW] Software.[os]_S.O Microsoft Windows Vista	[E,21]~Error de mantenimiento / actualización de los programas (software).	A12.5.1	[SW] Software.[os]_S.O Microsoft Windows Vista
[SW] Software.[os]_S.O Microsoft Windows Vista	[A,6]~Abuso privilegios de acceso.	A9.2.3	[SW] Software.[os]_S.O Microsoft Windows Vista

Fuente: Propia

En la tabla 46 se logra identifica a partir de la Metodología Magerit Evaluación de controles para amenazas por tratar. para los activos de información de la entidad.

Continuación Tabla No: 46 Evaluación de controles para amenazas por tratar.

Nombre del activo de información	**Amenazas Metodologia Magerit**	**Control ISO 27001 Anexo A**	
[SW] Software.[os]_S.O Microsoft Windows Vista	[A,7]~Uso no previsto.	A16.1.1	[SW] Software.[os]_S.O Microsoft Windows Vista
[SW] Software.[os]_S.O Microsoft Windows XP	[E,1]~Errores de usuario.	A12.1.1	[SW] Software.[os]_S.O Microsoft Windows XP
[SW] Software.[os]_S.O Microsoft Windows XP	[E,20]~Vulnerabilidades de los programas (software).	A12.6.1	[SW] Software.[os]_S.O Microsoft Windows XP
[SW] Software.[os]_S.O Microsoft Windows XP	[E,21]~Error de mantenimiento / actualización de los programas (software).	A12.5.1	[SW] Software.[os]_S.O Microsoft Windows XP
[SW] Software.[os]_S.O Microsoft Windows XP	[A,6]~Abuso privilegios de acceso.	A9.2.3	[SW] Software.[os]_S.O Microsoft Windows XP
[SW] Software.[os]_S.O Microsoft Windows XP	[A,7]~Uso no previsto.	A16.1.1	[SW] Software.[os]_S.O Microsoft Windows XP
[SW] Software.[os]_S.O Microsoft Windows server 2008	[E,2]~Error de administrador.	A.14.2.3	[SW] Software.[os]_S.O Microsoft Windows server 2008
[SW] Software.[os]_S.O Microsoft Windows server 2008	[E,20]~Vulnerabilidades de los programas (software).	A12.6.1	[SW] Software.[os]_S.O Microsoft Windows server 2008
[SW] Software.[os]_S.O Microsoft Windows server 2008	[E,21]~Error de mantenimiento / actualización de los programas (software).	A12.5.1	[SW] Software.[os]_S.O Microsoft Windows server 2008
[SW] Software.[os]_S.O Microsoft Windows server 2008	[E,24]~Caída del sistema, causa agotamiento de recursos.	A12.1.3	[SW] Software.[os]_S.O Microsoft Windows server 2008
[SW] Software.[os]_S.O Microsoft Windows server 2012	[E,2]~Error de administrador.	A.14.2.3	[SW] Software.[os]_S.O Microsoft Windows server 2012
[SW] Software.[os]_S.O Microsoft Windows server 2012	[E,20]~Vulnerabilidades de los programas (software).	A12.6.1	[SW] Software.[os]_S.O Microsoft Windows server 2012
[SW] Software.[os]_S.O Microsoft Windows server 2012	[E,21]~Error de mantenimiento / actualización de los programas (software).	A12.5.1	[SW] Software.[os]_S.O Microsoft Windows server 2012

Fuente: Propia

En la tabla 46 se logra identifica a partir de la Metodología Magerit Evaluación de controles para amenazas por tratar. para los activos de información de la entidad.

Continuación de la Tabla No: 46 Evaluación de controles para amenazas por tratar.

Nombre del activo de información	**Amenazas Metodologia Magerit**	**Control ISO 27001 Anexo A**	
[SW] Software.[os]_S.O Microsoft Windows server 2012	[E,24]~Caída del sistema, causa agotamiento de recursos.	A12.1.3	[SW] Software.[os]_S.O Microsoft Windows server 2012
[SW] Software.[os]_Linux Centos 7	[E,2]~Error de administrador.	A.14.2.3	[SW] Software.[os]_Linux Centos 7
[SW] Software.[os]_Linux Centos 7	[E,20]~Vulnerabilidades de los programas (software).	A12.6.1	[SW] Software.[os]_Linux Centos 7
[SW] Software.[os]_Linux Centos 7	[E,21]~Error de mantenimiento / actualización de los programas (software).	A12.5.1	[SW] Software.[os]_Linux Centos 7
[SW] Software.[os]_Linux Centos 7	[E,24]~Caída del sistema, causa agotamiento de recursos.	A12.1.3	[SW] Software.[os]_Linux Centos 7
[SW] Software.[os]_S.O UTM	[E,2]~Error de administrador.	A.14.2.3	[SW] Software.[os]_S.O UTM
[SW] Software.[os]_S.O UTM	[E,20]~Vulnerabilidades de los programas (software).	A12.6.1	[SW] Software.[os]_S.O UTM
[SW] Software.[os]_S.O UTM	[E,21]~Error de mantenimiento / actualización de los programas (software).	A12.5.1	[SW] Software.[os]_S.O UTM
[SW] Software.[os]_S.O UTM	[E,24]~Caída del sistema, causa agotamiento de recursos.	A12.1.3	[SW] Software.[os]_S.O UTM
[SW] Software.[os]_Hypervisor de Maquinas virtuales	[E,2]~Error de administrador.	A.14.2.3	[SW] Software.[os]_Hypervisor de Maquinas virtuales
[SW] Software.[os]_Hypervisor de Maquinas virtuales	[E,20]~Vulnerabilidades de los programas (software).	A12.6.1	[SW] Software.[os]_Hypervisor de Maquinas virtuales
[SW] Software.[os]_Hypervisor de Maquinas virtuales	[E,21]~Error de mantenimiento / actualización de los programas (software).	A12.5.1	[SW] Software.[os]_Hypervisor de Maquinas virtuales
[SW] Software.[os]_Hypervisor de Maquinas virtuales	[E,24]~Caída del sistema, causa agotamiento de recursos.	A12.1.3	[SW] Software.[os]_Hypervisor de Maquinas virtuales

Fuente: Propia

En la tabla 46 se logra identifica a partir de la Metodología Magerit Evaluación de controles para amenazas por tratar. para los activos de información de la entidad.

Continuación de la Tabla No: 46 Evaluación de controles para amenazas por tratar.

Nombre del activo de información	**Amenazas Metodologia Magerit**	**Control ISO 27001 Anexo A**	
[SW] Software.[std]_Apache.	[E,2]~Error de administrador.	A.14.2.3	[SW] Software.[std]_Apache.
[SW] Software.[std]_Apache.	[E,20]~Vulnerabilidades de los programas (software).	A12.6.1	[SW] Software.[std]_Apache.
[SW] Software.[std]_Apache.	[E,21]~Error de mantenimiento / actualización de los programas (software).	A18.2.3	[SW] Software.[std]_Apache.
[SW] Software.[std]_Apache.	[E,24]~Caída del sistema, causa agotamiento de recursos.	A12.1.3	[SW] Software.[std]_Apache.
[SW] Software.[std]_IIS.	[E,2]~Error de administrador.	A.14.2.3	[SW] Software.[std]_IIS.
[SW] Software.[std]_IIS.	[E,20]~Vulnerabilidades de los programas (software).	A12.6.1	[SW] Software.[std]_IIS.
[SW] Software.[std]_IIS.	[E,21]~Error de mantenimiento / actualización de los programas (software).	A18.2.3	[SW] Software.[std]_IIS.
[SW] Software.[std]_IIS.	[E,24]~Caída del sistema, causa agotamiento de recursos.	A12.1.3	[SW] Software.[std]_IIS.
[SW] Software.[std]_CMS Joomla.	[E,2]~Error de administrador.	A.14.2.3	[SW] Software.[std]_CMS Joomla.
[SW] Software.[std]_CMS Joomla.	[E,20]~Vulnerabilidades de los programas (software).	A12.6.1	[SW] Software.[std]_CMS Joomla.
[SW] Software.[std]_CMS Joomla.	[E,21]~Error de mantenimiento / actualización de los programas (software).	A18.2.3	[SW] Software.[std]_CMS Joomla.
[SW] Software.[std]_CMS WordPress.	[E,2]~Error de administrador.	A.14.2.3	[SW] Software.[std]_CMS WordPress.
[SW] Software.[std]_CMS WordPress.	[E,20]~Vulnerabilidades de los programas (software).	A12.6.1	[SW] Software.[std]_CMS WordPress.

Fuente: Propia

En la tabla 46, se logra identifica a partir de la Metodología Magerit Evaluación de controles para amenazas por tratar. para los activos de información de la entidad.

Continuación de la Tabla No: 46 Evaluación de controles para amenazas por tratar.

Nombre del activo de información	**Amenazas Metodologia Magerit**	**Control ISO 27001 Anexo A**	
[SW] Software.[std]_CMS WordPress.	[E,21]~Error de mantenimiento / actualización de los programas (software).	A18.2.3	[SW] Software.[std]_CMS WordPress.
[SW] Software.[std]_GLPI Inventario mesa de ayuda	[E,2]~Error de administrador.	A9.4.3	[SW] Software.[std]_GLPI Inventario mesa de ayuda
[SW] Software.[std]_GLPI Inventario mesa de ayuda	[E,21]~Error de mantenimiento / actualización de los programas (software).	A18.2.3	[SW] Software.[std]_GLPI Inventario mesa de ayuda
[SW] Software.[std]_PHP 5.6.30 >	[E,2]~Error de administrador.	A.14.2.3	[SW] Software.[std]_PHP 5.6.30 >
[SW] Software.[std]_PHP 5.6.30 >	[E,20]~Vulnerabilidades de los programas (software).	A12.6.1	[SW] Software.[std]_PHP 5.6.30 >
[SW] Software.[std]_PHP 5.6.30 >	[E,21]~Error de mantenimiento / actualización de los programas (software).	A18.2.3	[SW] Software.[std]_PHP 5.6.30 >
[HW] Equipamiento informático.[print]_[print]_Impresora en RED Laser.(Cantidad: X)	[I,3]~Contaminación mecánica.	A11.1.2	[HW] Equipamiento informático.[print]_[print]_Impresora en RED Laser.(Cantidad: X)
[HW] Equipamiento informático.[print]_[print]_Impresora en RED Laser.(Cantidad: X)	[I,5]~Avería de origen físico o lógico.	A.14.2.3	[HW] Equipamiento informático.[print]_[print]_Impresora en RED Laser.(Cantidad: X)
[HW] Equipamiento informático.[host]_[host]_Servidor Hypervisor	[E,23]~Error de mantenimiento / actualización de los equipos (hardware).	A11.2.4	[HW] Equipamiento informático.[host]_[host]_Servidor Hypervisor
[HW] Equipamiento informático.[host]_[host]_Servidor Hypervisor	[A,24]~Denegación de servicio.	A13.1.2	[HW] Equipamiento informático.[host]_[host]_Servidor Hypervisor
[HW] Equipamiento informático.[host]_[host]_Servidor Hypervisor	[A,25]~Robo.	A11.1.2	[HW] Equipamiento informático.[host]_[host]_Servidor Hypervisor
[HW] Equipamiento informático.[host]_[host]_Servidor Hypervisor	[I,3]~Contaminación mecánica.	A11.1.2	[HW] Equipamiento informático.[host]_[host]_Servidor Hypervisor

Fuente: Propia

En la tabla 46 se logra identifica a partir de la Metodología Magerit Evaluación de controles para amenazas por tratar. para los activos de información de la entidad.

Continuación de la Tabla No: 46 Evaluación de controles para amenazas por tratar.

Nombre del activo de información	**Amenazas Metodologia Magerit**	**Control ISO 27001 Anexo A**	
[HW] Equipamiento informático.[host]_[host]_Servidor Hypervisor	[I,5]~Avería de origen físico o lógico.	A.14.2.3	[HW] Equipamiento informático.[host]_[host]_Servidor Hypervisor
[HW] Equipamiento informático.[host]_[host]_Servidor Hypervisor	[I,7]~Condiciones inadecuadas de temperatura o humedad.	A11.2.1	[HW] Equipamiento informático.[host]_[host]_Servidor Hypervisor
[HW] Equipamiento informático.[host]_[host]_Servidor Hypervisor	[N,*]~Desastres naturales.	A15.1.2	[HW] Equipamiento informático.[host]_[host]_Servidor Hypervisor
[HW] Equipamiento informático.[vhost]_[vhost]_Servidor GLPI de soporte técnico	[E,2]~Error de administrador.	A11.2.4	[HW] Equipamiento informático.[vhost]_[vhost]_Servidor GLPI de soporte técnico
[HW] Equipamiento informático.[vhost]_[vhost]_Servidor GLPI de soporte técnico	[E,21]~Error de mantenimiento / actualización de los programas (software).	A18.2.3	[HW] Equipamiento informático.[vhost]_[vhost]_Servidor GLPI de soporte técnico
[HW] Equipamiento informático.[vhost]_[vhost]_Servidor GLPI de soporte técnico	[E,24]~Caída del sistema, causa agotamiento de recursos.	A12.1.3	[HW] Equipamiento informático.[vhost]_[vhost]_Servidor GLPI de soporte técnico
[HW] Equipamiento informático.[vhost]_[vhost]_Servidor GLPI de soporte técnico	[A,24]~Denegación de servicio.	A13.1.2	[HW] Equipamiento informático.[vhost]_[vhost]_Servidor GLPI de soporte técnico
[HW] Equipamiento informático.[vhost]_[vhost]_Servidor UTM IDS/IPS	[E,2]~Error de administrador.	A11.2.4	[HW] Equipamiento informático.[vhost]_[vhost]_Servidor UTM IDS/IPS
[HW] Equipamiento informático.[vhost]_[vhost]_Servidor UTM IDS/IPS	[E,21]~Error de mantenimiento / actualización de los programas (software).	A18.2.3	[HW] Equipamiento informático.[vhost]_[vhost]_Servidor UTM IDS/IPS

Fuente: Propia

En la tabla 46 se logra identifica a partir de la Metodología Magerit Evaluación de controles para amenazas por tratar. para los activos de información de la entidad.

Continuación de la Tabla No: 46 Evaluación de controles para amenazas por tratar

Nombre del activo de información	**Amenazas Metodologia Magerit**	**Control ISO 27001 Anexo A**	
[HW] Equipamiento informático.[vhost]_[vhost]_Servidor UTM IDS/IPS	[E,24]~Caída del sistema, causa agotamiento de recursos.	A12.1.3	[HW] Equipamiento informático.[vhost]_[vhost]_Servidor UTM IDS/IPS
[HW] Equipamiento informático.[vhost]_[vhost]_Servidor UTM IDS/IPS	[A,24]~Denegación de servicio.	A13.1.2	[HW] Equipamiento informático.[vhost]_[vhost]_Servidor UTM IDS/IPS
[HW] Equipamiento informático.[vhost]_[vhost]_Servidor HITS	[E,2]~Error de administrador.	A11.2.4	[HW] Equipamiento informático.[vhost]_[vhost]_Servidor HITS
[HW] Equipamiento informático.[vhost]_[vhost]_Servidor HITS	[E,21]~Error de mantenimiento / actualización de los programas (software).	A18.2.3	[HW] Equipamiento informático.[vhost]_[vhost]_Servidor HITS
[HW] Equipamiento informático.[vhost]_[vhost]_Servidor HITS	[E,24]~Caída del sistema, causa agotamiento de recursos.	A12.1.3	[HW] Equipamiento informático.[vhost]_[vhost]_Servidor HITS
[HW] Equipamiento informático.[vhost]_[vhost]_Servidor HITS	[A,24]~Denegación de servicio.	A13.1.2	[HW] Equipamiento informático.[vhost]_[vhost]_Servidor HITS
[HW] Equipamiento informático.[vhost]_[vhost]_Servidor Protocolo de transferencia de archivos	[E,2]~Error de administrador.	A11.2.4	[HW] Equipamiento informático.[vhost]_[vhost]_Servidor Protocolo de transferencia de archivos
[HW] Equipamiento informático.[vhost]_[vhost]_Servidor Protocolo de transferencia de archivos	[E,21]~Error de mantenimiento / actualización de los programas (software).	A18.2.3	[HW] Equipamiento informático.[vhost]_[vhost]_Servidor Protocolo de transferencia de archivos
[HW] Equipamiento informático.[vhost]_[vhost]_Servidor Protocolo de transferencia de archivos	[E,24]~Caída del sistema, causa agotamiento de recursos.	A12.1.3	[HW] Equipamiento informático.[vhost]_[vhost]_Servidor Protocolo de transferencia de archivos

Fuente: Propia

En la tabla 46 se logra identifica a partir de la Metodología Magerit Evaluación de controles para amenazas por tratar. para los activos de información de la entidad.

Continuación Tabla No: 46 Evaluación de controles para amenazas por tratar.

Nombre del activo de información	**Amenazas Metodologia Magerit**	**Control ISO 27001 Anexo A**	
[HW] Equipamiento informático.[vhost]_[vhost]_Servidor Protocolo de transferencia de archivos	[A,24]~Denegación de servicio.	A13.1.2	Seguridad servicios de red
[HW] Equipamiento informático.[vhost]_[vhost]_Servidor Soporte en almacenamiento de archivos misionales y de apoyo.	[E,2]~Error de administrador.	A11.2.4	Mantenimiento de equipos.
[HW] Equipamiento informático.[vhost]_[vhost]_Servidor Soporte en almacenamiento de archivos misionales y de apoyo.	[E,21]~Error de mantenimiento / actualización de los programas (software).	A18.2.3	Revisión del cumplimiento técnico
[HW] Equipamiento informático.[vhost]_[vhost]_Servidor Soporte en almacenamiento de archivos misionales y de apoyo.	[E,24]~Caída del sistema, causa agotamiento de recursos.	A12.1.3	Gestión de capacidad.
[HW] Equipamiento informático.[vhost]_[vhost]_Servidor Soporte en almacenamiento de archivos misionales y de apoyo.	[A,24]~Denegación de servicio.	A13.1.2	Seguridad servicios de red
[HW] Equipamiento informático.[vhost]_[vhost]_Servidor gestión de usuarios y contraseñas.	[E,2]~Error de administrador.	A11.2.4	Mantenimiento de equipos.
[HW] Equipamiento informático.[vhost]_[vhost]_Servidor gestión de usuarios y contraseñas.	[E,21]~Error de mantenimiento / actualización de los programas (software).	A18.2.3	Revisión del cumplimiento técnico
[HW] Equipamiento informático.[vhost]_[vhost]_Servidor gestión de usuarios y contraseñas.	[E,24]~Caída del sistema, causa agotamiento de recursos.	A12.1.3	Gestión de capacidad.

Fuente: Propia

En la tabla 46, se logra identifica a partir de la Metodología Magerit Evaluación de controles para amenazas por tratar. para los activos de información de la entidad.

Continuación Tabla No: 46 Evaluación de controles para amenazas por tratar.

Nombre del activo de información	**Amenazas Metodologia Magerit**	**Control ISO 27001 Anexo A**	
[HW] Equipamiento informático.[vhost]_[vhost]_Servidor gestión de usuarios y contraseñas.	[A,24]~Denegación de servicio.	A13.1.2	[HW] Equipamiento informático.[vhost]_[vhost]_Servidor gestión de usuarios y contraseñas.
[HW] Equipamiento informático.[vhost]_[vhost]_Servidor DHCP.	[E,2]~Error de administrador.	A11.2.4	[HW] Equipamiento informático.[vhost]_[vhost]_Servidor DHCP.
[HW] Equipamiento informático.[vhost]_[vhost]_Servidor DHCP.	[E,21]~Error de mantenimiento / actualización de los programas (software).	A18.2.3	[HW] Equipamiento informático.[vhost]_[vhost]_Servidor DHCP.
[HW] Equipamiento informático.[vhost]_[vhost]_Servidor DHCP.	[E,24]~Caída del sistema, causa agotamiento de recursos.	A12.1.3	[HW] Equipamiento informático.[vhost]_[vhost]_Servidor DHCP.
[HW] Equipamiento informático.[vhost]_[vhost]_Servidor DHCP.	[A,24]~Denegación de servicio.	A13.1.2	[HW] Equipamiento informático.[vhost]_[vhost]_Servidor DHCP.
[HW] Equipamiento informático.[host]_[host]_Estaciones de trabajo.	[E,23]~Error de mantenimiento / actualización de los equipos (hardware).	A11.2.4	[HW] Equipamiento informático.[host]_[host]_Estaciones de trabajo.
[HW] Equipamiento informático.[host]_[host]_Estaciones de trabajo.	[A,23]~Manipulación de equipos.	A11.1.2	[HW] Equipamiento informático.[host]_[host]_Estaciones de trabajo.
[HW] Equipamiento informático.[host]_[host]_Estaciones de trabajo.	[A,25]~Robo.	A11.1.2	[HW] Equipamiento informático.[host]_[host]_Estaciones de trabajo.
[HW] Equipamiento informático.[host]_[host]_Estaciones de trabajo.	[I,3]~Contaminación mecánica.	A11.1.2	[HW] Equipamiento informático.[host]_[host]_Estaciones de trabajo.
[HW] Equipamiento informático.[host]_[host]_Estaciones de trabajo.	[I,5]~Avería de origen físico o lógico.	A.14.2.3	[HW] Equipamiento informático.[host]_[host]_Estaciones de trabajo.
[HW] Equipamiento informático.[phone]_[phone]_Telefonos.	[I,5]~Avería de origen físico o lógico.	A.14.2.3	[HW] Equipamiento informático.[phone]_[phone]_Telefonos.

Fuente: Propia

En la tabla 46.se logra identifica a partir de la Metodología Magerit Evaluación de controles para amenazas por tratar. para los activos de información de la entidad.

Continuación Tabla No: 46 Evaluación de controles para amenazas por tratar.

Nombre del activo de información	**Amenazas Metodologia Magerit**	**Control ISO 27001 Anexo A**	
[HW] Equipamiento informático.[phone]_[phone]_Telefonos.	[N,*]~Desastres naturales.	A15.1.2	[HW] Equipamiento informático.[phone]_[phone]_Telefonos.
[HW] Equipamiento informático.[pabx]_[pabx]_Servidor [PSTN].	[I,3]~Contaminación mecánica.	A11.1.2	[HW] Equipamiento informático.[pabx]_[pabx]_Servidor [PSTN].
[HW] Equipamiento informático.[pabx]_[pabx]_Servidor [PSTN].	[I,5]~Avería de origen físico o lógico.	A.14.2.3	[HW] Equipamiento informático.[pabx]_[pabx]_Servidor [PSTN].
[HW] Equipamiento informático.[pabx]_[pabx]_Servidor [PSTN].	[I,7]~Condiciones inadecuadas de temperatura o humedad.	A11.2.1	[HW] Equipamiento informático.[pabx]_[pabx]_Servidor [PSTN].
[HW] Equipamiento informático.[network]_[network]_Router	[E,2]~Error de administrador.	A11.2.4	[HW] Equipamiento informático.[network]_[network]_Router
[HW] Equipamiento informático.[network]_[network]_Router	[E,23]~Error de mantenimiento / actualización de los equipos (hardware).	A11.2.4	[HW] Equipamiento informático.[network]_[network]_Router
[HW] Equipamiento informático.[network]_[network]_Router	[I,3]~Contaminación mecánica.	A11.1.2	[HW] Equipamiento informático.[network]_[network]_Router
[HW] Equipamiento informático.[network]_[network]_Router	[I,5]~Avería de origen físico o lógico.	A.14.2.3	[HW] Equipamiento informático.[network]_[network]_Router
[HW] Equipamiento informático.[network]_[network]_Router	[I,7]~Condiciones inadecuadas de temperatura o humedad.	A11.2.1	[HW] Equipamiento informático.[network]_[network]_Router
[HW] Equipamiento informático.[network]_[network]_Router	[N,*]~Desastres naturales.	A15.1.2	[HW] Equipamiento informático.[network]_[network]_Router
[HW] Equipamiento informático.[network]_[network]_Switches Core.	[E,2]~Error de administrador.	A11.2.4	[HW] Equipamiento informático.[network]_[network]_Switches Core.

Fuente: Propia

En la tabla 46, se logra identifica a partir de la Metodología Magerit Evaluación de controles para amenazas por tratar. para los activos de información de la entidad.

Continuación Tabla No: 46 Evaluación de controles para amenazas por tratar.

Nombre del activo de información	**Amenazas Metodologia Magerit**	**Control ISO 27001 Anexo A**	
[HW] Equipamiento informático.[network] _[network] _Switches Core.	[E,23]~Error de mantenimiento / actualización de los equipos (hardware).	A11.2.4	Mantenimiento de equipos.
[HW] Equipamiento informático.[network] _[network] _Switches Core.	[I,3]~Contaminación mecánica.	A11.1.2	Control acceso físicos
[HW] Equipamiento informático.[network] _[network] _Switches Core.	[I,5]~Avería de origen físico o lógico.	A.14.2.3	Revisión técnica de las aplicaciones después de cambios en la plataforma de operación
[HW] Equipamiento informático.[network] _[network] _Switches Core.	[I,7]~Condiciones inadecuadas de temperatura o humedad.	A11.2.1	Ubicación y protección de los equipos
[HW] Equipamiento informático.[network] _[network] _Switches Core.	[N,*]~Desastres naturales.	A15.1.2	Tratamiento de la seguridad dentro de los acuerdos con proveedores
[HW] Equipamiento informático.[network] _[network] _Switches Acceso.	[E,2]~Error de administrador.	A11.2.4	Mantenimiento de equipos.
[HW] Equipamiento informático.[network] _[network] _Switches Acceso.	[E,23]~Error de mantenimiento / actualización de los equipos (hardware).	A11.2.4	Mantenimiento de equipos.
[HW] Equipamiento informático.[network] _[network] _Switches Acceso.	[I,3]~Contaminación mecánica.	A11.1.2	Control acceso físicos
[HW] Equipamiento informático.[network] _[network] _Switches Acceso.	[I,5]~Avería de origen físico o lógico.	A.14.2.3	Revisión técnica de las aplicaciones después de cambios en la plataforma de operación
[HW] Equipamiento informático.[network] _[network] _Switches Acceso.	[I,7]~Condiciones inadecuadas de temperatura o humedad.	A11.2.1	Ubicación y protección de los equipos
[HW] Equipamiento informático.[network] _[network] _Switches Acceso.	[N,*]~Desastres naturales.	A15.1.2	Tratamiento de la seguridad dentro de los acuerdos con proveedores

Fuente: Propia

En la tabla 46, se logra identifica a partir de la Metodología Magerit Evaluación de controles para amenazas por tratar. para los activos de información de la entidad.

Continuación Tabla No: 46 Evaluación de controles para amenazas por tratar.

Nombre del activo de información	**Amenazas Metodologia Magerit**	**Control ISO 27001 Anexo A**	
[HW] Equipamiento informático.[network] _[network] _Switches Caseros.	[E,23]~Error de mantenimiento / actualización de los equipos (hardware).	A11.2.4	[HW] Equipamiento informático.[network] _[network] _Switches Caseros.
[HW] Equipamiento informático.[network] _[network] _Switches Caseros.	[I,7]~Condiciones inadecuadas de temperatura o humedad.	A11.2.1	[HW] Equipamiento informático.[network] _[network] _Switches Caseros.
[HW] Equipamiento informático.[network] _[network] _Puntos de acceso inalambrico.	[E,23]~Error de mantenimiento / actualización de los equipos (hardware).	A11.2.4	[HW] Equipamiento informático.[network] _[network] _Puntos de acceso inalambrico.
[HW] Equipamiento informático.[network] _[network] _Puntos de acceso inalambrico.	[I,7]~Condiciones inadecuadas de temperatura o humedad.	A11.2.1	[HW] Equipamiento informático.[network] _[network] _Puntos de acceso inalambrico.
[COM] Redes de comunicaciones [PSTN] _Servicio de de telefonia analoga.	[I,8]~Fallo de servicios de comunicaciones.	A15.1.2	[COM] Redes de comunicaciones [PSTN] _Servicio de de telefonia analoga.
[COM] Redes de comunicaciones [PSTN] _Servicio de de telefonia analoga.	[A,6]~Abuso privilegios de acceso.	A9.2.3	[COM] Redes de comunicaciones [PSTN] _Servicio de de telefonia analoga.
[COM] Redes de comunicaciones [PSTN] _Servicio de de telefonia analoga.	[A,7]~Uso no previsto.	A16.1.1	[COM] Redes de comunicaciones [PSTN] _Servicio de de telefonia analoga.
[COM] Redes de comunicaciones[Internet]_Servicio de internet dedicado para la organización	[A,6]~Abuso privilegios de acceso.	A9.2.3	[COM] Redes de comunicaciones[Internet]_Servicio de internet dedicado para la organización
[COM] Redes de comunicaciones[Internet]_Servicio de internet dedicado para la organización	[A,7]~Uso no previsto.	A16.1.1	[COM] Redes de comunicaciones[Internet]_Servicio de internet dedicado para la organización
[COM] Redes de comunicaciones[Internet]_Servicio de internet dedicado para la organización	[I,8]~Fallo de servicios de comunicaciones.	A15.1.2	[COM] Redes de comunicaciones[Internet]_Servicio de internet dedicado para la organización

Fuente: Propia

En la tabla 46, se logra identifica a partir de la Metodología Magerit Evaluación de controles para amenazas por tratar. para los activos de información de la entidad.

Continuación Tabla No: 46 Evaluación de controles para amenazas por tratar.

Nombre del activo de información	**Amenazas Metodologia Magerit**	**Control ISO 27001 Anexo A**	
[COM] Redes de comunicaciones[wifi]_Radio enlace local (WI-FI).	[I,8]~Fallo de servicios de comunicaciones.	A15.1.2	[COM] Redes de comunicaciones[wifi]_Radio enlace local (WI-FI).
[COM] Redes de comunicaciones[wifi]_Radio enlace local (WI-FI).	[E,19]~Fuga de información.	A9.2.3	[COM] Redes de comunicaciones[wifi]_Radio enlace local (WI-FI).
[COM] Redes de comunicaciones[wifi]_Radio enlace local (WI-FI).	[E,23]~Error de mantenimiento / actualización de los equipos (hardware).	A11.2.4	[COM] Redes de comunicaciones[wifi]_Radio enlace local (WI-FI).
[COM] Redes de comunicaciones[wifi]_Radio enlace local (WI-FI).	[E,24]~Caída del sistema, causa agotamiento de recursos.	A12.1.3	[COM] Redes de comunicaciones[wifi]_Radio enlace local (WI-FI).
[COM] Redes de comunicaciones[wifi]_Radio enlace local (WI-FI).	[A,6]~Abuso privilegios de acceso.	A9.2.3	[COM] Redes de comunicaciones[wifi]_Radio enlace local (WI-FI).
[COM] Redes de comunicaciones[wifi]_Radio enlace local (WI-FI).	[A,11]~Acceso no autorizado.	A9.2.3	[COM] Redes de comunicaciones[wifi]_Radio enlace local (WI-FI).
[COM] Redes de comunicaciones[wifi]_Radio enlace local (WI-FI).	[A,12]~Análisis de tráfico.	A12.7.1	[COM] Redes de comunicaciones[wifi]_Radio enlace local (WI-FI).
[COM] Redes de comunicaciones[wifi]_Radio enlace local (WI-FI).	[A,14]~Interceptación de información (escucha).	A12.7.1	[COM] Redes de comunicaciones[wifi]_Radio enlace local (WI-FI).
[COM] Redes de comunicaciones[LAN]_Red de área local	[I,8]~Fallo de servicios de comunicaciones.	A15.1.2	[COM] Redes de comunicaciones[LAN]_Red de área local
[COM] Redes de comunicaciones[LAN]_Red de área local	[E,19]~Fuga de información.	A9.2.3	[COM] Redes de comunicaciones[LAN]_Red de área local
[COM] Redes de comunicaciones[LAN]_Red de área local	[E,23]~Error de mantenimiento / actualización de los equipos (hardware).	A11.2.4	[COM] Redes de comunicaciones[LAN]_Red de área local
[COM] Redes de comunicaciones[LAN]_Red de área local	[E,24]~Caída del sistema, causa agotamiento de recursos.	A12.1.3	[COM] Redes de comunicaciones[LAN]_Red de área local

Fuente: Propia

En la tabla 46, se logra identifica a partir de la Metodología Magerit Evaluación de controles para amenazas por tratar. para los activos de información de la entidad.

Continuación Tabla No: 46 Evaluación de controles para amenazas por tratar.

Nombre del activo de información	**Amenazas Metodologia Magerit**	**Control ISO 27001 Anexo A**	
[COM] Redes de comunicaciones[LAN]_Red de área local	[A,6]~Abuso privilegios de acceso.	A9.2.3	[COM] Redes de comunicaciones[LAN]_Red de área local
[COM] Redes de comunicaciones[LAN]_Red de área local	[A,11]~Acceso no autorizado.	A9.2.3	[COM] Redes de comunicaciones[LAN]_Red de área local
[COM] Redes de comunicaciones[LAN]_Red de área local	[A,12]~Análisis de tráfico.	A12.7.1	[COM] Redes de comunicaciones[LAN]_Red de área local
[COM] Redes de comunicaciones[LAN]_Red de área local	[A,14]~Interceptación de información (escucha).	A12.7.1	[COM] Redes de comunicaciones[LAN]_Red de área local
[AUX] Equipamiento auxiliar.[ups]_UPS dedicado para los servidores.	[I,3]~Contaminación mecánica.	A11.1.2	[AUX] Equipamiento auxiliar.[ups]_UPS dedicado para los servidores.
[AUX] Equipamiento auxiliar.[ups]_UPS dedicado para los servidores.	[E,23]~Error de mantenimiento / actualización de los equipos (hardware).	A11.2.4	[AUX] Equipamiento auxiliar.[ups]_UPS dedicado para los servidores.
[AUX] Equipamiento auxiliar.[ac]_Aire acondicionado dedicado para los servidores.	[I,3]~Contaminación mecánica.	A11.1.2	[AUX] Equipamiento auxiliar.[ac]_Aire acondicionado dedicado para los servidores.
[AUX] Equipamiento auxiliar.[ac]_Aire acondicionado dedicado para los servidores.	[E,23]~Error de mantenimiento / actualización de los equipos (hardware).	A11.2.4	[AUX] Equipamiento auxiliar.[ac]_Aire acondicionado dedicado para los servidores.
[L] Instalaciones.Sede principal (Edificio).	[N,*]~Desastres naturales.	A15.1.2	[L] Instalaciones.Sede principal (Edificio).
[L] Instalaciones.Sede principal (Edificio).	[I,*]~Desastres industriales.	A15.1.2	[L] Instalaciones.Sede principal (Edificio).
[L] Instalaciones.Sede principal (Edificio).	[A,11]~Acceso no autorizado.	A11.1.2	[L] Instalaciones.Sede principal (Edificio).

Fuente: Propia

En la tabla 46, se logra identifica a partir de la Metodología Magerit Evaluación de controles para amenazas por tratar. para los activos de información de la entidad.

Continuación Tabla No: 46 Evaluación de controles para amenazas por tratar.

Nombre del activo de información	**Amenazas Metodologia Magerit**	**Control ISO 27001 Anexo A**	
[P] Personal.[ui]_Usuario interno (Cantidad:2)	[E,7]~Deficiencia en la organización.	A6.1.2	[P] Personal.[ui]_Usuario interno (Cantidad:2)
[P] Personal.[ui]_Usuario interno (Cantidad:2)	[E,19]~Fuga de información.	A5.1.2	[P] Personal.[ui]_Usuario interno (Cantidad:2)
[P] Personal.[ui]_Usuario interno (Cantidad:2)	[E,28]~Indisponibilidad de personal.		[P] Personal.[ui]_Usuario interno (Cantidad:2)
[P] Personal.[ui]_Usuario interno (Cantidad:2)	[A,28]~Indisponibilidad del personal.		[P] Personal.[ui]_Usuario interno (Cantidad:2)
[P] Personal.[ui]_Usuario interno (Cantidad:2)	[A,29]~Extorsión.	A7.2.3	[P] Personal.[ui]_Usuario interno (Cantidad:2)
[P] Personal.[adm]_Técnicos para administración y mantenimiento (Cantidad:2)	[E,7]~Deficiencia en la organización.	A6.1.2	[P] Personal.[adm]_Técnicos para administración y mantenimiento (Cantidad:2)
[P] Personal.[adm]_Técnicos para administración y mantenimiento (Cantidad:2)	[E,19]~Fuga de información.	A5.1.2	[P] Personal.[adm]_Técnicos para administración y mantenimiento (Cantidad:2)
[P] Personal.[adm]_Técnicos para administración y mantenimiento (Cantidad:2)	[E,28]~Indisponibilidad de personal.		[P] Personal.[adm]_Técnicos para administración y mantenimiento (Cantidad:2)
[P] Personal.[adm]_Técnicos para administración y mantenimiento (Cantidad:2)	[A,28]~Indisponibilidad del personal.		[P] Personal.[adm]_Técnicos para administración y mantenimiento (Cantidad:2)
[P] Personal.[adm]_Técnicos para administración y mantenimiento (Cantidad:2)	[A,29]~Extorsión.	A7.2.3	[P] Personal.[adm]_Técnicos para administración y mantenimiento (Cantidad:2)
[P] Personal.[sub]_Contratista de apoyo (Cantidad:1)	[E,7]~Deficiencia en la organización.	A6.1.2	[P] Personal.[sub]_Contratista de apoyo (Cantidad:1)
[P] Personal.[sub]_Contratista de apoyo (Cantidad:1)	[E,19]~Fuga de información.	A5.1.2	[P] Personal.[sub]_Contratista de apoyo (Cantidad:1)
[P] Personal.[sub]_Contratista de apoyo (Cantidad:1)	[E,28]~Indisponibilidad de personal.		[P] Personal.[sub]_Contratista de apoyo (Cantidad:1)
[P] Personal.[sub]_Contratista de apoyo (Cantidad:1)	[A,28]~Indisponibilidad del personal.		[P] Personal.[sub]_Contratista de apoyo (Cantidad:1)
[P] Personal.[sub]_Contratista de apoyo (Cantidad:1)	[A,29]~Extorsión.	A7.2.3	[P] Personal.[sub]_Contratista de apoyo (Cantidad:1)

Fuente: Propia

9.4. Aprobación

Teniendo en cuenta que el análisis de GESTIÓN DEL RIESGOS EN TI es transversal a todos los procesos (Departamentos) de la entidad, dichas acciones deben de ser firmado por el responsable (Líder, supervisor) del proceso (Departamento) y de su correspondiente director.

Es de recalcar que el plan de tratamiento se puede realizar de forma periódica cada año, por tanto, su cumplimiento debe de ser medible y alcanzable teniendo en cuenta la capacidad técnica, operativa y financiera de la entidad.

Bajo consenso institucional, se leen las acciones como plan de tratamiento de los riesgos inaceptables en la entidad, para ser aprobado y firmado por las partes interesadas.

9.5. Socialización

Típicamente el proceso de sistemas o telemática es reconocido como un departamento de apoyo, no misional, para este tipo de entidades. En cuanto a Gestión del Riesgo en TI, se sugiere socializar con el Departamento de planeación y este dará a conocer las acciones a tomar como parte de las estrategias para la Gestión del Riesgo, se sugiere actualizar cada año y tomarlo como insumo para el PESI y el PETI, se sugiere crearlo con un alcance a cuatro (4) años, a menos que exista algún cambio considerable dentro de la infraestructura de TI.

10.CONCLUSIONES

Con el presente trabajo se logró identificar el estado actual en forma general en las entidades públicas dedicadas a promover la ciencia, cultura, tecnología e innovación tecnológica de la ciudad de Cali en referencia a las tecnologías de la información y de la comunicación bajo el enfoque de la gestión del riesgo, evidenciando cuando se refiere a las tecnologías de la información y de la comunicación, se presenta un crecimiento fortuito en su infraestructura, que pudo haberse sobrellevado pero regularmente no se hace, de igual forma se identifica que la infraestructura, con sus características físicas generales de la infraestructura de TI, lo que sirvió como insumo para la actividad de la gestión de los riesgos , propició la necesidad de identificar los activos de información que pudiesen interactuar con la infraestructura de red de comunicación de la entidad, donde a nivel de tecnologías de conmutación por lo general presentan componentes de swching, routing, cableado estructurado , estaciones de trabajo, servidores, sistemas de refrigeración y sistemas operativos, que son heterogéneos donde se evidencia un abanico amplio de marcas y tecnologías lo que dificulta una adecuada gestión, y por ende dificulta la capacidad de endurecimiento de los sistemas .

En el desarrollo de este documento se reconoció e identificó el impacto de los riesgos latentes por el uso de las tecnologías de la información que pueden afectar la operación y cumplimiento misional de las entidades, mediante la identificación de las amenazas vs la dimensiones de seguridad, apoyado en Magerit que a su vez se apoya en la normativa ISO 31000 en respuesta a la gestión del riesgo, reconociendo que un activo de información puede ser afectado en una o varias facetas entre las cuales se reconoce la Disponibilidad, la integridad, la confidencialidad , la autenticidad y la trazabilidad datos necesarios para reconocer las posibles consecuencias en caso de que un riesgo se materialice, con lo anterior se logró reconocer de forma pormenorizada los activos de información críticos para establecer el estado actual con enfoque de gestión del riesgo para este tipo de entidades.

Con relación a todo lo anterior se estableció una metodología para el análisis de riesgos que contribuya a la aplicación de medidas de prevención para evitar peligros potenciales o reducir su impacto en la infraestructura TI de las entidades públicas dedicadas a promover la ciencia, cultura, tecnología e innovación tecnológica de la ciudad de Cali, ayudando a dar cumplimiento con los requerimientos de seguridad y privacidad de la información , que sirva como insumo para la elaboración del PETI Plan estrategia de Tecnologías de la Información y el PESI Plan Estratégico de seguridad de la información que en la actualidad se les exigen a las entidades públicas en Colombia.

Al final en este documento se plantea un análisis de varias metodologías y algún estándar dedicados a tareas de gestión del riesgo, con lo que se logró sugerir un modelo idóneo para la gestión de riesgos TI como aporte de seguridad de la información para las entidades públicas dedicadas a promover la ciencia, tecnología e innovación tecnológica de la ciudad de Cali, apoyando la necesidad de evidenciar el nivel de seguridad o inseguridad que tenga un sistema de información, es decir, sugiriendo un método formal documental que sirve para investigar los riesgos a los que está asociado un sistema, dichos riesgos a su vez sirven como insumo para sugerir las medidas de control que se deberían de adoptar con el objeto de controlar los riesgos, lo que incide en la gestión de la seguridad y ayuda en el cumplimiento de su objeto social para la entidad.

11. RECOMENDACIONES

Se sugiere adquirir o implementar un modelo de gestión del riesgo específico para evaluar la infraestructura de red de comunicación con sus diversos componentes , lo cuales será reconocidos como los activos de información, para tal actividad se sugiere ser prudentes con relación a la parte operativa dado que es muy probable que para el departamento o proceso de telemática no cuenten con el suficiente personal para responder por una eventual sobrecarga de trabajo en relación a los controles que se puedan generar a partir de un análisis de riesgos, de igual forma se debe de tener en cuenta la capacidad técnica, si el personal cuenta con la experticia necesaria para poder implementar dichos controles, por último la capacidad financiera, la solución o control establecido debe ser coherente con la capacidad adquisitiva de la entidad.

12. BIBLIOGRAFÍA.

AGUDELO, Jorge. Diseño de un plan de gestión de riesgos y vulnerabilidades del caso de estudio de la empresa QWERTY S.A., basados en los estándar NTC-ISO/IEC 27001 y NTC-ISO/IEC 27032. UNAD Tunja 2020. [En Línea]. 156 p. Disponible en: http://repository.unad.edu.co/handle/10596/36866

BARRETO, Carlos Y RODRÍGUEZ, Jaime. Diseño de un plan de gestión de riesgos de la información en el instituto nacional de estudios sociales, ines de Colombia. Bogotá 2018. . [En Línea]. 217 p. Disponible en: http://repository.unipiloto.edu.co/bitstream/handle/20.500.12277/6149/00005166%20-%20ANEXO%201.pdf?sequence=2&isAllowed=y

CANO, Jeimy. Inseguridad informática: Un concepto dual en seguridad informática. 2004. [En Línea]. 5 p. Disponible en: https://pdfs.semanticscholar.org/bcb5/12fa66710b3662e50b07029a3f7a43c0bfc3.pdf

Certificación ISO 27001 acreditada vs no acreditada. 2019. [En Línea]. Disponible en: https://www.escuelaeuropeaexcelencia.com/2019/12/certificacion-iso-27001-acreditada-vs-no-acreditada/

CertiProf. 3. Términos y Definiciones. 2018. 18 p.

CertiProf. CERTIPROF CERTIFIED ISO 27001 AUDITOR / LEAD AUDITOR (I27001A/LA). Versión 07218. 2018. 115 p.

CertiProf. ISO/IEC 27000-series. 2018. 2 p.

Documento de clasificación de entidades del sector público colombiano Versión 2. 2018. [En Línea]. 84 p. Disponible en: http://www.urf.gov.co/webcenter/ShowProperty?nodeId=/ConexionContent/WCC_CLUSTER-070104

GARCÍA, Paloma. UNE-ISO/IEC 27002, La guía en la era de la ciberseguridad [En Línea]. Disponible en: https://portal.aenormas.aenor.com/revista/309/27002-309.html

Guía de gestión de riesgos. 2016. [En Línea]. 39 p. Disponible en: https://www.mintic.gov.co/gestionti/615/articles-5482_G7_Gestion_Riesgos.pdf

Guía para la Gestión y Clasificación de Activos de Información. 2016. [En Línea]. 18 p. Disponible en: https://www.mintic.gov.co/gestionti/615/articles-5482_G5_Gestion_Clasificacion.pdf

Introducción a ITIL V3 | Definición ITIL. (2016, mayo 24). ServiceTonic. https://www.servicetonic.com/es/itil/introduccion-a-itil-v3/

ISO 27001—Certificado ISO 27001 punto por punto—Presupuesto Online. 2021. [En Línea]. Disponible en: https://normaiso27001.es/

MAFLA, Samanta y ESQUIVEL, Arley. Análisis y plan de tratamiento de riesgos para los activos de la información del cuerpo de bomberos voluntarios de tunja. Tunja 2019. [En Línea]. 208 p. Disponible en: https://repository.usta.edu.co/bitstream/handle/11634/21200/2019Samanthasierra?sequence=1&isAllowed=y

MAGERIT versión 3 Libro I Método (versión español): Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Ministerio de Hacienda y Administraciones Públicas. España 2012. [En Línea]. 127 p. Disponible en: https://administracionelectronica.gob.es/pae_Home/dam/jcr:fb373672-f804-4d05-8567-2d44b3020387/2012_Magerit_v3_libro1_metodo_es_NIPO_630-12-171-8.pdf

MAGERIT versión 3 Libro II Catálogo de elementos (versión español): Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Ministerio de Hacienda y Administraciones Públicas. España 2012. [En Línea]. 75 p. Disponible en: https://administracionelectronica.gob.es/pae_Home/dam/jcr:5fbe15c3-c797-46a6-acd8-51311f4c2d29/2012_Magerit_v3_libro2_catalogo-de-elementos_es_NIPO_630-12-171-8.pdf

MAGERIT versión 3 Libro III: Guía de Técnicas (versión español): Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Ministerio de Hacienda y Administraciones Públicas. España 2012. [En Línea]. 42 p. Disponible en: https://administracionelectronica.gob.es/pae_Home/dam/jcr:130c633a-ee11-4e17-9cec-1082ceeac38c/2012_Magerit_v3_libro3_guia-de-tecnicas_es_NIPO_630-12-171-8.pdf

MARTÍNEZ, Christian. Diseño de un modelo de gestión de riesgos aplicable a proyectos de naturaleza ti de la alcaldía distrital de Cartagena de indias. Cartagena 2020. [En Línea]. 175 p. Disponible en: https://biblioteca.utb.edu.co/notas/tesis/0074654.pdf

Modelo de seguridad—fortalecimiento ti. 2020. [En Línea]. Disponible en: https://www.mintic.gov.co/gestion-ti/seguridad-ti/modelo-de-seguridad/

Niveles de seguridad: Qué son y su importancia en la empresa. 2018. [En Línea]. 394 p. Disponible en: https://blog.mdcloud.es/niveles-de-seguridad-que-son-y-su-importancia-en-la-empresa/

OSORIO, Mónica; HERRERA, Darwin y HENAO, Andrés. Diseño del sistema de gestión de seguridad de la información para una agencia de viajes y turismo. Bogotá 2017. [En

Línea]. 34 p. Disponible en: https://alejandria.poligran.edu.co/bitstream/handle/10823/999/EntregaFinal.pdf?sequence=1

OSPINA, Julián. PLAN DE TRATAMIENTOS DE RIESGOS DE SEGURIDADY PRIVACIDADDE LA INFORMACION. Cali 2019. [En Línea]. 15 p. Disponible en: 61747-plan de tratamiento de riesgos de seguridad y privacidad de la informacion ver.00.pdf (inciva.gov.co)

Plan de Seguridad y Privacidad de la Información 2019. Cali 2019. [En Línea]. 15 p. Disponible en: https://www.bibliovalle.gov.co/portal/component/phocadownload/category/19-planes-estrategicos?download=932:plan-seguridad-privacidad-info-2019

Plan Estratégico de las Tecnologías de la información 2019. Cali 2019. [En Línea]. 60 p. Disponible en: file:///tmp/mozilla_toor0/19-planes-estrategicos?download=926:plan-tecnologias-informacion-2019

POLÍTICA DE OPERACIÓN ADMINISTRACIÓN DEL RIESGO. [En Línea]. 60 p. Disponible en: file:///tmp/mozilla_toor0/M04-PMC-POLITICA%20-ADMON-RIESGO-2019.pdf

Revisión del marco regulatorio para la gestión de riesgos de seguridad digital. Cali 2017. [En Línea]. 60 p. Disponible en: https://www.crcom.gov.co/recursos_user/2017/actividades_regulatorias/ciberseguridad/Documento_CRC_Seguridad_Digital_Vpublicar.pdf

Qué es COBIT 5? Entendiendo el Gobierno de TI ó IT Governance. (2018, enero 24). Genius IT Training. https://geniusitt.com/blog/que-es-cobit-5/

SARMIENTO, Angie. Norma Icontec 6166. Colombia 2021. [En Línea]. Disponible en: https://www.youtube.com/watch?v=GAiQVceX_Q4

VIECCO, Luis y PINEDO, Víctor. Modelo de gobierno de tecnología de la información, basado en gestión del riesgo y seguridad de la información para las universidades públicas: caso de estudio universidad de la guajira. Guajira 2018. [En Línea]. 148 p. Disponible en: https://manglar.uninorte.edu.co/bitstream/handle/10584/8330/133663.pdf?sequence=1&isAllowed=y

What is an Operationally Critical Threat, Asset and Vulnerability Evaluation (OCTAVE)? - Definition from Techopedia. (s. f.). Techopedia.com. Recuperado, de http://www.techopedia.com/definition/21133/operationally-critical-threat-asset-and-vulnerability-evaluation-octave

13. ANEXOS

Anexo 1 Tipo de activo de información

Teniendo en cuenta la anterior Clasificación se debe de otorgar un tipo de activo de información tomando como base el modelo MAGERIT como se observa a en el capítulo 7.1 7.1 IDENTIFICACIÓN GENERAL DE LOS ACTIVOS DE INFORMACIÓN, que se basa en la guía 2 de MAGERIT

ID de Activo: Identificador del activo de información se recomienda crear en principio un valor numérico incremental 1, 2,3 etc.

Categoría Activo: Se indica a que categoría general pertenece el activo basado en la tabla anterior.

Sufijo Activo: Un identificador general del activo que logra particularizar el servicio del activo de información se base en Magerit libro 2, pag 7 -14.

Nombre Activo: Nombre distintivo del Activo, se sugiere complementar el nombre Distintivo más Numero de Inventario propio de la Entidad si lo tiene.

Servicio o descripción del Activo: Descripción general del activo.

Cuadro Clasificación por Tipo de Activo.

Categoría				
ID-Activo	**Categoría Activo**	**Sufijo Activo**	**Nombre Activo**	**Servicio o descripción del Activo**
Fuente: Propia.				

La tabla Clasificación por Tipo de Activo., como herramienta para ayudar a documentar los tipos de activos en la entidad.

Anexo 2 Amenazas y las dimensiones de seguridad que fueron afectadas

Teniendo en cuenta la anterior enumeración de activos de la entidad se deben definir **las amenazas y las dimensiones de seguridad que fueron o pueden ser afectadas**, es decir las dimensiones están estrechamente relacionadas con la probabilidad de que un riesgo se materialice**.**

Para las dimensiones de seguridad se basara en MAGERIT y el cómo logra clasificar las amenazas como se observa a en el capítulo 7.2 **Determinar AMENAZAS VS las DIMENSIONES DE SEGURIDAD AFECTADAS,** en apoyo de la ISO 31000 como mecanismo de gestión del Riesgo, coadyuvando en definir unas dimensiones derivas de utilizar tecnologías de la información (magerit libro 1, pag 7), ayudando a definir el impacto de una amenaza sobre el activo de información de la entidad, pudiendo afectar una o varias facetas de las dimensiones de seguridad:

En principio se deben de documentar los activos, proceso o departamento a que corresponde y el responsable, con ayuda de la siguiente tabla así:

Cuadro DATOS DEL ACTIVO DE INFORMACIÓN

Amenazas y dimensiones de seguridad afectadas.				
DATOS DEL ACTIVO DE INFORMACIÓN				
ID-Activo	**Nombre del activo de información**	**Proceso propietario del activo**	**Responsable**	**Tipo Activo**
Fuente: Propia.				

La Tabla DATOS DEL ACTIVO DE INFORMACIÓN, ayuda a documentar la propiedad del activo identificado como proceso y el responsable.

Ahora con relación a los activos que fueron enumerados, se debe de definir **las amenazas y las dimensiones de seguridad que fueron o pueden ser afectadas** así:

Cuadro Amenazas afectadas vs Dimensión.

Amenazas y dimensiones de seguridad afectadas.									
DATOS DEL ACTIVO DE INFORMACIÓN					**DIMENSIÓN**				
ID-Activo	**Nombre del activo de información**	**Tipo Activo**	**Tipo Amenazas**	**Amenazas**	**(D) Disponibilidad(B / M /A / MA/ MB)**	**(I) Integridad (B / M /A / MA/ MB)**	**(C) Confidencialidad (B / M /A / MA/ MB)c**	**(A) Autenticidad (B / M /A / MA/ MB**	**(T) Trazabilidad (B / M /A / MA/ MB)**
Nivel de ocurrencia que impacte una o varias facetas de la dimensión de seguridad de la información: MA : Aproximadamente seguro, nivel 25, afecto mas de una(1) vez en lo que va del año. A : Probable, nivel 20, Por lo menos afecto una(1) vez en lo que va del año. M : posible, nivel 15, Por lo menos afecto una(1) vez en los últimos dos(2) años. B : Escaso Probable, nivel 9, Por lo menos afecto una vez en los últimos cuatro años. MB : Raro, nivel 4, No ha sido afectado en los últimos cuatro(4) años.									
Fuente: Propia.									

La Tabla Amenazas afectadas vs Dimensión, herramienta que ayuda a documentar los activos sus amenazas y las dimensiones que puede afectar.

La anterior tabla ayuda a enumerar las amenazas que han o pueden llegar a afectar el activo de información con relación al tipo de activo, tomando como referencia las guías de Magerit libro 2 páginas 8 a 14, y las dimensiones de seguridad con Magerit libro 1 páginas 7 a 14.

Como resultado se obtendrá una valoración del riesgo a partir de la recopilación valores cualitativos con relación a las distintas facetas de seguridad, como se evidencia en la tabla 46, y que posteriormente se evaluará mediante mapas de calor, brindando una valoración del riesgo de forma cuantitativa, facilitando tener un cambio de estado de conciencia de la exposición de riesgos a la que está expuesta la entidad con relación a TI.

Anexo 3 Vulnerabilidades y riesgos

Teniendo en cuenta la anterior identificación de amenazas, es necesario identificar las vulnerabilidades y riesgos **que se encuentran asociados a los activos de información y se deben de enumerar en la siguiente tabla así:**

Cuadro Vulnerabilidades y riesgos asociados a los Activos

VULNERABILIDADES Y RIESGOS DE LOS ACTIVOS DE INFORMACIÓN						
ID-Activo	**Nombre del activo de información**	**Tipo Activo**	**Tipo Amenazas**	**Amenazas**	**Vulnerabilidad(s).**	**Riesgo(s).**
Fuente: Propia.						

La Tabla Vulnerabilidades y riesgos asociados a los Activos, herramienta de documentación para poder identificar las vulnerabilidades y riesgos inherentes a cada tipo de activo de información.

Anexo 4 Probabilidad e impacto de los riesgos asociados a los activos así

Nivel de probabilidad e impacto que está asociado a un riesgo de la entidad, para tal fin se debe de diligenciar la siguiente tabla.

La siguiente tabla recopila información relevante para identificar la probabilidad e impacto de riesgo asociado al activo, lo anterior toma como referente las guías de MAGERIT Libro 2 lo que posibilita trabajar de forma sistemática [33]

Cuadro Probabilidad e impacto de los riesgos asociados a los Activos

Probabilidad e impacto de los riesgos asociados a los Activos					
ID-Activo	**Nombre del activo de información**	**Tipo Activo**	**Riesgo(s).**	**Probabilidad (B / M /A / MA/ MB)**	**Impacto (B / M /A / MA/ MB)**
Fuente: Propia.					

La Tabla Probabilidad e impacto de los riesgos asociados a los Activos, herramienta que ayuda a documentar la probabilidad de ocurrencia y el impacto en caso que un riesgo se materialice.

[33]Administracionelectronica.gob.es. (2012). *MAGERIT versión 3 Libro II Catálogo de elementos (versión española): Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. (11.)*. P7-14 https://administracionelectronica.gob.es/pae_Home/dam/jcr:5fbe15c3-c797-46a6-acd8-51311f4c2d29/2012_Magerit_v3_libro2_catalogo-de-elementos_es_NIPO_630-12-171-8.pdf

Anexo 5 Prioridades de los riesgos para su manejo y para su posible adición a las políticas

En este aparte es donde se define el nivel de aceptación del riesgo.

Se debe de evitar resultados subjetivos a los controles dado que puede ser posible que un riesgo posea varios controles, o no se haya aplicado ninguno al momento del análisis, por ende, se debe de tener en cuenta para poder dar prioridad a los riesgos los siguientes datos.

Calculo Riesgo Neto: Valoración del Riesgo X Probabilidad del riesgo.

Criticidad: Si Calculo Riesgo Neto <= 4 Despreciable,
Si Calculo Riesgo Neto <= 9 Bajo,
Si Calculo Riesgo Neto <= 15 Apreciable,
Si Calculo Riesgo Neto <= 25 Critico.

Gestión: Si tiene Gestión = 1,
Si tiene Gestión, pero no es efectivo = 2,
Si tiene Gestión, es efectivo, pero no está documentado = 3,
Si tiene Gestión, es efectivo, y está documentado = 4.

Riesgo Residual: Calculo Riesgo Neto / Gestión

Teniendo en cuenta la escala de valoración del riego se va tomar la siguiente escala de valores, con lo cual podremos determinar la prioridad de los riesgos a tratar así:

Anexo 6 Niveles de aceptación del riesgo

Teniendo en cuenta el riesgo Residual con relación al nivel de gestión así:

Riesgo Residual = Calculo del riesgo neto / Calificación de Gestión

Nivel Aceptación Riesgo = Riesgo Residual

Donde el nivel de Aceptación del Riesgo se tomaría los siguientes Rangos.

Entre 1 a 5 aceptable (A).
Entre 6 a 15 moderado (M).
Entre 16 a 25 inaceptable (I).

Esto permite al identificar el riesgo, se le otorgara un nivel, a su vez identificara su importancia o criticidad frente al sistema de información, por tanto, a nivel cuantitativo se tratarán los riesgos cuyos niveles se encuentren entre 16 a 25 siendo inaceptables (I), además que tenga un impacto que esté relacionado como alto o muy alto. Asimismo, se sugiere una paramétrica intuitiva, simple sin perder su importancia, rindiendo una clasificación e identificación de los riesgos lo cual al final del ejercicio se trata de obtener un nivel de riesgo aceptable y aprobado por la alta gerencia de la entidad. [34]

Cuadro Nivel Aceptación Riesgo.

Nivel Aceptación Riesgo.							
ID-Activo	**Nombre del activo de información**	**AMENAZA**	**Riesgo Neto**	**Criticidad**	**Gestión**	**Riesgo Residual**	**Nivel Aceptación Riesgo**
Fuente: “elaboración propia”.							

[34]Administracionelectronica.gob.es. (2012). *MAGERIT versión 3 Libro II Catálogo de elementos (versión española): Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. (11.)*. P7-14 https://administracionelectronica.gob.es/pae_Home/dam/jcr:5fbe15c3-c797-46a6-acd8-51311f4c2d29/2012_Magerit_v3_libro2_catalogo-de-elementos_es_NIPO_630-12-171-8.pdf

La Tabla Nivel Aceptación Riesgo, es una herramienta que ayuda a documentar el nivel de riesgo asumible sobre un riesgo.

Todo riesgo que nivel de aceptación sea superior a 15 será tratado dado que se considera inaceptable. De la misma forma, en que se identifica el nivel aceptable del riesgo, de la misma forma debe de ser identificado los niveles de riesgo inaceptables, lo que implica que debes de recibir un trato para minimizar el riesgo. [35]

Cuadro Riesgos Inaceptables por tratar

Riesgos Inaceptables por tratar				
ID-Activo	**Nombre del activo de información**	**AMENAZA**	**VULNERABILIDAD**	**Cantidad Riesgos por tratar**
Fuente: “elaboración propia”.				

La Riesgos Inaceptables por tratar, es una herramienta que ayuda a priorizar los riesgos inaceptables y que por tal motivo deben de ser tratados.

[35]Administracionelectronica.gob.es. (2012). *MAGERIT versión 3 Libro II Catálogo de elementos (versión española): Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. (11.)*. P7-14 https://administracionelectronica.gob.es/pae_Home/dam/jcr:5fbe15c3-c797-46a6-acd8-51311f4c2d29/2012_Magerit_v3_libro2_catalogo-de-elementos_es_NIPO_630-12-171-8.pdf

Anexo 7 Acciones a cada uno de los riesgos para su manejo basado la norma iso/iec 27001:2013 anexo a y para su posible adición a las políticas

Basado en la definición de priorización de los riesgos se establecen controles basado LA NORMA ISO/IEC 27001:2013 Anexo A, se deben abordar acciones correctivas dirigidas a evitar la materialización de un riesgo , reducir el riesgo, compartir o transferir el riesgo hasta lograr un nivel aceptable concertado , firmado y aprobado por las partes interesadas teniendo en cuenta factibilidad Jurídica, Técnica, financiera teniendo en cuenta una relación costo beneficio para la entidad, insumo que sirve para establecer compromisos de acciones a tomar que deben ser acorde a su capacidad técnica , operativa y financiera.

Cuadro Plan de Tratamiento

Plan de Tratamiento							
ID Activos.	**Tipo activo de Información**	**Nombre del activo de información**	**Tratamiento. (transferir, Aceptar, Mitigar)**	**Clausula Anexo A Iso 27001**	**Descripción Clausula**	**Control**	**Aplicación Control.**
Fuente: Propia.							

La Plan de Tratamiento es una herramienta de control con la cual se ayuda a documentar el tratamiento que se le va a dar a cada riesgo y los controles que se establecen a dicho tratamiento, con el objeto de realizar seguimiento para minimizar o eliminar un riesgo.