E.S.E. HOSPITAL CARISMA

PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

Medellín, Enero de 2024

CONTENIDO

E.S.E. HOSPITAL CARISMA

LISTA DE CUADROS

1. INTRODUCCIÓN

Administración de riesgos es un método lógico y sistemático para establecer el contexto, identificar, analizar, evaluar, tratar, monitorear y comunicar los riesgos asociados con una actividad, función o proceso de tal forma que permita a las entidades minimizar pérdidas y maximizar oportunidades.

Todos los servidores públicos, en cumplimiento de sus funciones, están sometidos a riesgos que pueden hacer fracasar una gestión; por lo tanto, es necesario tomar las medidas, para identificar las causas y consecuencias de la materialización de dichos riesgos. Por esa razón, la presente guía tiene como objetivo orientar y facilitar la implementación y desarrollo de una eficaz, eficiente y efectiva gestión del riesgo, desde la identificación hasta el monitoreo; enfatiza en la importancia de la administración del riesgo, sus fundamentos teóricos y da una orientación para facilitar su identificación, reconocimiento de las causas, efectos, definición de controles y da lineamientos sencillos y claros para su adecuada gestión.

2. OBJETIVOS

2.1 OBJETIVO GENERAL

Realizar el análisis de riesgos de seguridad de la información mediante la metrología MAGERIT, para una adecuada administración de riesgos a partir de su identificación, manejo y seguimiento.

2.2 OBJETIVOS ESPECÍFICOS

- Evaluar los activos informáticos de la entidad, con respecto a los parámetros de disponibilidad, confidencialidad e integridad, para determinar importancia, estado y funcionalidad en la entidad.

- Identificar los factores de amenaza, las vulnerabilidades y riesgos de seguridad informática y de la información que pueden llegar a afectar a la entidad.

- Adaptar las políticas o manuales de seguridad de la información con los que cuenta la entidad, para mejorar la seguridad informática de la ESE.

- Crear o mejorar los controles de seguridad en la entidad, para garantizar la integridad, disponibilidad y confidencialidad de la información.

3. ALCANCE

La ESE Hospital Carisma, es una empresa social del estado de segundo nivel, especializada en el tratamiento de todo tipo de adicciones, actualmente es el único hospital de Colombia, que trabaja esta especialidad. Como toda entidad del sector salud, la información de sus pacientes y de las historias clínicas es el activo más importante de la organización y por tanto es fundamental la protección de los datos[1]; que permita garantizar la privacidad, la confidencialidad y la disponibilidad de los datos de sus usuarios dada la relevancia de este tipo de activo, el sector salud se ha convertido en uno de los principales blancos de ataques informáticos, entre los que se destaca el ramsonwer[2] , donde puede llegar a ser víctima de robo y secuestro de información sensible y ataques de servicios; debido lo sensible de la información que manejan los hospitales, son una víctima perfecta para extorsionar económicamente, a cambio de poder acceder nuevamente a la información.

Garantizar por tanto los 3 pilares fundamentales de la seguridad de la información, se ha convertido en una prioridad para las entidades de salud, que las ha encaminado, al diseño e implementación de sistemas de gestión de la seguridad de la información, que permitan, establecer controles para minimizar riesgos y vulnerabilidades de la información, permite a la ESE Hospital Carisma, fortalecer sus capacidades tecnológicas, acorde también con las necesidades actuales y con tendencia a las proyecciones institucionales, como lo son la interoperabilidad de la historia clínica y la telemedicina, proyectos que requieren mejorar la seguridad de la información de la ESE, ya que al pretender interoperar datos y brindar atención en el área de telemedicina, se puede ver vulnerada la información y la confidencialidad de las historias clínicas, por ser expuestas a canales informáticos externos vía web.

4. ÁMBITO DE APLICACIÓN

Los lineamientos definidos en esta guía, aplica para la gestión de los riesgos de seguridad y privacidad de la información y riesgos asociados al uso de tecnologías de la información.

[1]Doctor, Don. *Protección de datos en hospitales: Políticas de seguridad informática.* s.f. https://dondoctor.com/sector-salud-colombia/proteccion-de-datos-en-hospitales-10-politicas-de-

[2] ESET, Welivesecurity by. *Hospitales: uno de los principales blancos de ciberataques.* 22 de Abril de 2020. https://www.welivesecurity.com/la-es/2020/04/22/por-que-hospitales-blanco-atractivo-cibercriminales/ (último acceso: 13 de Octubre de 2021).

5. DEFINICIONES

Para la administración del riesgo, se tendrán en cuenta los siguientes términos y definiciones:

- **Acciones asociadas**: son las acciones que se deben tomar posterior a determinar las opciones de manejo del riesgo (asumir, reducir, evitar compartir o transferir), dependiendo de la evaluación del riesgo residual, orientadas a fortalecer los controles identificados.

- **Activos informáticos:** Son aquellos recursos que utiliza un Sistema de Gestión de Seguridad de la Información para que las organizaciones funcionen y consigan los objetivos que se han propuesto por la alta dirección. Existen diferentes tipos de activos, entre ellos, los activos digitales, los tangibles, los intangibles, los de software, los activos de sistemas operativos, los de infraestructura, entre otros. [3]

- **Administración de riesgos**: conjunto de etapas secuenciales que se deben desarrollar para el adecuado tratamiento de los riesgos.

- **Amenaza**: Es una acción que se vale la existencia de una vulnerabilidad, para quebrantar la seguridad de un sistema de información y efectuar ataque provocando un posible daño sobre el sistema, las amenazas pueden proceder de eventos físicos, ataques o negligencia.[4]

- **Análisis del riesgo**: etapa de la administración del riesgo, donde se establece la probabilidad de ocurrencia y el impacto del riesgo antes de determinar los controles (análisis del riesgo inherente).

- **Asumir el riesgo**: opción de manejo donde se acepta la pérdida residual probable, si el riesgo se materializa.

- **Causa**: medios, circunstancias y/o agentes que generan riesgos.

- **Calificación del riesgo**: estimación de la probabilidad de ocurrencia del riesgo y el impacto que puede causar su materialización.

[3] **SGSI**, Blog especializado en Sistemas de Gestión de Seguridad de la Información. ¿Cómo realizar un inventario de activos de información? [En línea] [Consultado: 25 de Octubre de 2021] Disponible en: https://www.pmg-ssi.com/2017/02/realizar-inventario-activos-de-informacion/ .

[4] **INCIBE, INSTITUTO NACIONAL DE CIBERSEGURIDAD.** Amenaza vs Vulnerabilidad, ¿sabes en qué se diferencian? [En línea] [Consultado: 25 de Octubre de 2021] Disponible en: https://www.incibe.es/protege-tu-empresa/blog/amenaza-vs-vulnerabilidad-sabes-se-diferencian

- **Compartir o transferir el riesgo**: opción de manejo que determina traspasar o compartir las pérdidas producto de la materialización de un riesgo con otras organizaciones mediante figuras como outsourcing, seguros, sitios alternos.

- **Consecuencia**: efectos que se pueden presentar cuando un riesgo se materializa.

- **Contexto estratégico**: son las condiciones internas y del entorno, que pueden generar eventos que originan oportunidades o afectan negativamente el cumplimiento de la misión y objetivos de una institución.
- **Control**: acción o conjunto de acciones que minimiza la probabilidad de ocurrencia de un riesgo o el impacto producido ante su materialización.

- **Control preventivo**: acción o conjunto de acciones que eliminan o mitigan las causas del riesgo; está orientado a disminuir la probabilidad de ocurrencia del riesgo.

- **Control correctivo**: acción o conjunto de acciones que eliminan o mitigan las consecuencias del riesgo; está orientado a disminuir el nivel de impacto del riesgo.

- **Debilidad**: situación interna que la entidad puede controlar y que puede afectar su operación.

- **Evaluación del riesgo**: resultado del cruce cuantitativo de las calificaciones de probabilidad e impacto, para establecer la zona donde se ubicará el riesgo.

- **Evitar el riesgo**: opción de manejo que determina la formulación de acciones donde se prevenga la materialización del riesgo mediante el fortalecimiento de controles identificado.

- **Frecuencia**: ocurrencia de un evento expresado como la cantidad de veces que ha ocurrido un evento en un tiempo dado.

- **Identificación del riesgo**: etapa de la administración del riesgo donde se establece el riesgo con sus causas (asociadas a factores externos e internos de riesgo), consecuencias y se clasifica de acuerdo con los tipos de riesgo definidos.

- **Impacto**: medida para estimar cuantitativa y cualitativamente el posible efecto de la materialización del riesgo.

- **MAGERIT:** Metodología de Análisis y Gestión de Riesgos, fue creada por Consejo Superior de Informática, trabaja bajo un método sistémico, que permite

la mitigación de los riesgos de la información, derivados del uso de la tecnología y las comunicaciones, ayuda a determinar el impacto que puede llegar a tener una empresa en caso de vulneración de la seguridad informática[5]. Esta metodología está basada en cuatro etapas: Planeación, análisis de riesgos, gestión de riesgos y seleccionar las salvaguardas. Sirve además para la valoración de los activos, según el impacto que pueda ocasionar para la empresa su daño o perdida.

- **Mapa de riesgos**: documento que de manera sistemática, muestra el desarrollo de las etapas de la administración del riesgo.

- **Materialización del riesgo**: ocurrencia del riesgo identificado.

- **Modelo de seguridad y privacidad de la información:** "Conduce a la preservación de la confidencialidad, integridad, disponibilidad de la información, permitiendo garantizar la privacidad de los datos, mediante la aplicación de un proceso de gestión del riesgo, brindando confianza a las partes interesadas acerca de la adecuada gestión de riesgos" [6]. Es una herramienta del Ministerio de las TIC's de Colombia, que está alineada con el MIPG y permite por medio de una serie de guías identificar el estado de madurez de una entidad en términos de seguridad y privacidad de la información, buscando además la implementación de buenas prácticas con el objetivo de garantizar la seguridad, confidencialidad, integridad y disponibilidad de la información.[7]

- **Opciones de manejo**: posibilidades disponibles para administrar el riesgo posterior a la valoración de los controles definidos (asumir, reducir, evitar compartir o transferir el riesgo residual).

- **Plan de contingencia**: conjunto de acciones inmediatas, recursos, responsables y tiempos establecidos para hacer frente a la materialización del riesgo y garantizar la continuidad del servicio.

---

[5] **ESET**, Welivesecurity by. MAGERIT: metodología práctica para gestionar riesgos. [Sitio web] 14 de Mayo de 2013. [En línea] [Consultado: 13 de Octubre de 2021] Disponible en: https://www.welivesecurity.com/la-es/2013/05/14/magerit-metodologia-practica-para-gestionar-riesgos/

[6] **COLOMBIA, MINISTERIO DE LAS TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES MINTIC.** Modelo de Seguridad y Privacidad de la información . [En línea] [Consultado: 15 de Octubre de 2021] Disponible en: https://mintic.gov.co/gestionti/615/articles-5482_Modelo_de_Seguridad_Privacidad.pdf

[7] **COLOMBIA, MINISTERIO DE LAS TECNOLOGIAS DE LA INFORMACIÓN Y LAS COMUNICACIONES MMINTIC** Modelo de Seguridad - Fortalecimiento de la gestión en el Estado. [En línea] [Consultado: 18 de Octubre de 2021] Disponible en: https://mintic.gov.co/gestion-ti/Seguridad-TI/Modelo-de-Seguridad/

- **Probabilidad**: medida para estimar cuantitativa y cualitativamente la posibilidad de ocurrencia del riesgo.

- **Procedimiento**: conjunto de especificaciones, relaciones, responsabilidades, controles y ordenamiento de las actividades y tareas requeridas para cumplir con el proceso.

- **Proceso**: conjunto de entradas tangibles o intangibles, suministradas por un proveedor, a estas entradas se les asigna recursos y se aplican controles, obteniendo salidas tangibles o intangibles, destinadas a un usuario, generando un impacto en estos. Se clasifican en estratégicos, misionales, de apoyo y de evaluación.

- **Riesgo**: Se podría definir como la probabilidad de ocurrencia de un ataque o vulneración de seguridad, este es un factor muy importante, ya que una vez se identifique el riesgo, se debe hacer un análisis y tratamiento del mismo, una valoración del riesgo y posteriormente se hace una gestión del riesgo, con la intensión de disminuir la posibilidad de ocurrencia de una determinada amenaza[8].

- **Riesgo de corrupción**: posibilidad de que por acción u omisión, mediante el uso indebido del poder, de los recursos o de la información, se lesionen los intereses de una entidad y en consecuencia del Estado, para la obtención de un beneficio particular.

- **Riesgo inherente**: es aquel al que se enfrenta una entidad o proceso en ausencia de controles y/o acciones para modificar su probabilidad o impacto.

- **Riesgo institucional**: Son los que afectan de manera directa el cumplimiento de los objetivos o la misión institucional. Los riesgos institucionales, son producto del análisis de los riesgos por proceso y son denominados de este tipo cuando cumplen las siguientes características:

- **Los riesgos que han sido clasificados como estratégicos**: en el paso de identificación deben haber sido marcados como de clase estratégica, es decir, se relacionan con el cumplimiento de objetivos institucionales, misión y visión.

- **Los riesgos que se encuentran en zona alta o extrema**: después de valorar

[8] **COLOMBIA, MINISTERIO DE LAS TECNOLOGIAS DE LA INFORMACIÓN Y LAS COMUNICACIONES MMINTIC.** Guía de gestión de riesgos. s.f. https://mintic.gov.co/gestionti/615/articles-5482_G7_Gestion_Riesgos.pdf (último acceso: 15 de Octubre de 2021).

el riesgo (identificación y evaluación de controles), el riesgo residual se ubica en zonas de riesgo alta o extrema, indicando que el grado de exposición a la materialización del riesgo aún se encuentra poco controlado.

- **Los riesgos que tengan incidencia en usuario o destinatario final externo**: en el caso de la materialización del riesgo la afectación del usuario externo se presenta de manera directa.

- **Los riesgos de corrupción**: todos los riesgos identificados que hagan referencia a situaciones de corrupción, serán considerados como riesgos de tipo institucional.

- **Riesgo residual**: nivel de riesgo que permanece luego de determinar y aplicar controles para su administración.

- **Valoración del riesgo**: establece la identificación y evaluación de los controles para prevenir la ocurrencia del riesgo o reducir los efectos de su materialización. En la etapa de valoración del riesgo se determina el riesgo residual, la opción de manejo a seguir, y si es necesita.

- **Vulnerabilidad:** Es una falla o debilidad del sistema de información que puede poner en riesgo la seguridad de la información y garantizar su disponibilidad.[9]

[9] **BST**, Ambit. Qué son las vulnerabilidades y amenazas informáticas [En línea] [Consultado: 20 de Octubre de 2021] Disponible en: https://www.ambit-bst.com/blog/tipos-de-vulnerabilidades-y-amenazas-inform%C3%A1ticas

6. ROLES Y RESPONSABILIDADES FRENTE A LA ADMINISTRACIÓN DEL RIESGO

El éxito de la administración del riesgo depende de la decidida participación de los directivos, servidores públicos y contratistas; por esto, es preciso identificar los actores que intervienen:

- **Alta Dirección**: aprueban las directrices para la administración del riesgo en la Entidad. La Alta Dirección es la responsable del fortalecimiento de la política de administración del riesgo.

- **Proceso Administración del Sistema Integrado de Gestión**: Genera la metodología para la administración del riesgo de la Entidad, coordina, lidera, capacita y asesora en su aplicación.

- **Responsables de los procesos**: Identifican, analizan, evalúan y valoran los riesgos de la entidad (por procesos e institucionales) al menos una vez al año. Si bien los Líderes SIG apoyan la ejecución de las etapas de gestión del riesgo a nivel de los procesos, esto no quiere decir que el proceso de administración de riesgos este solo bajo su responsabilidad. Al contrario, cada responsable de proceso se encarga de garantizar que en el proceso a su cargo se definan los riesgos que le competen, se establezcan las estrategias y responsabilidades para tratarlos y, sobre todo, que se llegue a cada funcionario que trabaja en dicho proceso. No se debe olvidar que son las personas que trabajan en cada uno de los procesos los que mejor conocen los riesgos existentes en el desarrollo de sus actividades.

- **Servidores públicos y contratistas**: ejecutar los controles y acciones definidas para la administración de los riesgos definidos, aportar en la identificación de posibles riesgos que puedan afectar la gestión de los procesos y/o de la entidad.

- **Quien haga las veces de Control Interno**: debe realizar evaluación y seguimiento a la política, los procedimientos y los controles propios de la administración de riesgos.

7. POLÍTICA DEL SISTEMA DE GESTIÓN DE RIESGOS ORGANIZACIONALES (SGRO)

La ESE HOSPITAL CARISMA establece su compromiso con la Gestión de los Riesgos derivados de sus procesos organizacionales, incluyendo dentro de su gestión la metodología, identificación y medidas de intervención para que todos los funcionarios y contratistas identifiquen, coordinen y administren los eventos que pueden impedir el logro de los objetivos de la entidad.

De acuerdo a lo anterior, la organización ha definido los siguientes pilares para tratar y manejar los riesgos con base en su valoración, permitiendo tomar decisiones adecuadas para evitar, reducir, compartir, transferir, y asumir el riesgo:

- **Identificar el riesgo:** La organización debe identificar el riesgo en sus procesos, el impacto que este genera, como sus causas y consecuencias con el fin de generar el tratamiento del mismo.
- **Evitar el riesgo:** Medidas encaminadas a prevenir su materialización, generando cambios sustanciales al interior de los procesos por mejoramiento, rediseño o eliminación, resultado de unos adecuados controles y acciones emprendidas.
- **Reducir el riesgo:** Medidas encaminadas a disminuir tanto la probabilidad como el impacto del riesgo, adoptando actividades de prevención y de protección al interior de la entidad, optimizando los procedimientos y la implementación de los controles.
- **Compartir o Transferir el riesgo:** Medidas encaminadas a reducir los efectos de los riesgos a través del traspaso de estos a otras áreas.
- **Asumir un riesgo:** Los riesgos residuales se aceptan como pérdida y se elaboran planes de contingencia para su manejo.
- **Mapa de riesgos:** La herramienta conceptual y metodológica para la valoración de los riesgos en la ESE Hospital Carisma.

Tomado de la política institucional del sistema de gestión de riesgos organizacionales de la ESE Hospital Carisma.

8. METODOLOGÍA MAGERIT PARA LA IDENTIFICACIÓN Y ANÁLISIS DE RIEGOS DE LAS TECNOLOGIAS DE LA INFORMACIÓN

En la metodóloga MAGERIT, se parte de la identifican todos los activos informáticos de la ESE, realizando un inventario de los activos que tienen un valor para la entidad y requieren protección, diferenciándolos entre los siguientes tipos de activos (activos de Software, hardware, información, intangibles, servicios, componentes de red, talento humano infraestructura física).

Una vez realizada la identificación e inventario de activos, se procede a hacer una valoración de cada activo, de acuerdo a los criterios de disponibilidad, confidencialidad e integridad.

En cuanto a la identificación de las amenazas, así como de su valoración, se implementará como modelo de aplicación la "Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información MAGERIT"[10], por medio de la cual se puede realizar también la gestión y administración de los riesgos[11] y está alineada con los estándares de seguridad más relevantes de la ISO y el Modelo de seguridad y privacidad de la información del Ministerio de las Tecnologías De La Información Y Las Comunicaciones MINTIC

Posteriormente se hace una valoración de los activos teniendo en cuenta los criterios de autenticidad, trazabilidad, confidencialidad, integridad y disponibilidad, planteados en la metodología MAGERIT para el análisis y gestión de riesgos de la información

Para la valoración de cada uno de los activos identificados, se realiza una valoración cualitativa donde se mide el impacto del riesgo (ver tabla 1) y una y una cuantitativa con escalas que van desde 1 a 25 (ver tabla 2).

[10] **MAGERIT**. Versión 3.0. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Libro I – Método, 2012. [En línea] [Consultado: 21 de octubre de 2021]. Disponible en: https://www.ccn-cert.cni.es/documentos-publicos/1789-magerit-libro-i-metodo/file.html

[11] **ESET**, Welivesecurity by. MAGERIT: metodología práctica para gestionar riesgos. [Sitio web] 14 de Mayo de 2013. [En línea] [Consultado: 13 de Octubre de 2021] Disponible en: https://www.welivesecurity.com/la-es/2013/05/14/magerit-metodologia-practica-para-gestionar-riesgos/

Cuadro 1: Criterios para valoración de activos

IMPACTO DEL RIESGO			
	Nomenclatura	Categoría	Valoración
Impacto	MA	Muy Alto	5
	A	Alto	4
	M	Medio	3
	B	Bajo	2
	MB	Muy Bajo	1

Fuente: Matriz de análisis de riesgos.

Cuadro 2: Criterios cuantitativos para valoración de activos

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: Matriz de análisis de riesgos.

La aplicación de las tablas con las escalas de valoración, tal y como lo plantea la metodología MAGERIT[12], facilita la valoración de los activos, ayudando a determinar el impacto del riesgo y la valoración del riesgo, con el fin de poder definir posteriormente controles para los activos que son más críticos para la entidad.

[12] **MAGERIT**. Versión 3.0. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Libro I – Método, 2012. [En línea] [Consultado: 21 de octubre de 2021]. Disponible en: https://www.ccn-cert.cni.es/documentos-publicos/1789-magerit-libro-i-metodo/file.html

8.1. IDENTIFICACIÓN DE ACTIVOS

Se identifican todos los activos informáticos de la ESE, realizando un inventario de los activos que tienen un valor para la entidad y requieren protección, diferenciándolos entre los siguientes tipos de activos:

- Activos de Software: programas, sistemas operativos, herramientas ofimáticas
- Activos de hardware: equipos de cómputo, servidores, dispositivos de red, biométricos, entre otros.
- Activos de información: información importante para la entidad almacenada en medio físico o digital, como la historia clínica, contratos, acuerdos, planes, procedimientos, etc.
- Activos intangibles: hace referencia, a esas características que hacen único el producto o servicio que ofrece la empresa y representan una ventaja competitiva, como el Good Will, la reputación o la imagen corporativa.
- Servicios: Tales como; página web, intranet, ERP, CMR, portal de gestión documental, aplicaciones, entre otros.
- Componentes de red: en este tipo de activos, se tienen en cuenta todos los elementos necesarios para lograr las interconexiones, como lo son el cableado estructurado, los switches, routers, access point, entre otros.
- Talento Humano: son aquellas personas que por su rol, experiencia y labor que desempeñan en la institución, desempeñan un papel fundamental para realizar una tarea especifica.
- Instalaciones físicas: Son los espacios físicos de la entidad; los lugares donde se alojan los activos que son considerados como críticos para la empresa.

Para la identificación de activos, se tienen en cuenta todos los activos informáticos que tienen valor para la entidad, se agrupan por tipo de activos, se les asigna un código de identificación, de acuerdo con el tipo de activo, según la clasificación de activos que ofrece la metodología MAGERIT donde [SW] es Software, [HW] es Hardware, [S] son servicios y [D] Datos, el nombre del activo, el tipo de activo, su ubicación, descripción de funcionalidades principales y la cantidad. Se relaciona a continuación el inventario de activos de la ESE Hospital Carisma.

Cuadro 3: Matriz para la identificación de activos

N°	Código Activo	Nombre del activo	Descripción	Tipo de Activo	Ubicación	Funciones Principales	Cantidad

8.2. VALORACIÓN DE ACTIVOS

Una vez realizada la identificación e inventario de activos, se procede a hacer una valoración de cada activo, de acuerdo a los criterios de disponibilidad, confidencialidad e integridad. Se definen dichos criterios así:

- Disponibilidad: Hace alusión a que la información sea accesible, que se garantice su uso cuando sea requerida.
- Confidencialidad: Define criterios de acceso a la información, es decir, solo quien este autorizado a acceder a cierto tipo de información, contará con los permisos necesarios para hacerlo.

La para la valoración de los activos, se tiene en cuenta los criterios de autenticidad, trazabilidad, confidencialidad, integridad y disponibilidad, se asigna una valoración cualitativa, donde MA= Muy alto, A= Alto, M= Medio, B= Bajo y MB= Muy bajo, siendo MB un criterio donde se define que no afectaría el normal funcionamiento de la entidad y MA el máximo, donde se considera que la pérdida de la seguridad en la dimensión evaluada afectaría gravemente el normal funcionamiento de la entidad, como se explica en la *Tabla1: "Criterios para valoración de activos"*. Finalmente se realiza una valoración cuantitativa, donde cada una de las variables tiene un valor definido en una escala de 1 a 25 como se explica en la *Tabla2: "Criterios cuantitativos para valoración de activos"* para determinar una valoración general.

Cuadro 4: Valoración de activos cualitativa

DATOS DEL ACTIVO DE INFORMACION		DIMENSION				
Nombre del activo de información	Tipo de Activo	Autenticidad	Trazabilidad	Confidencialidad	Integridad	Disponibilidad

Cuadro 5: Valoración cuantitativa de activos

N°	NOMBRE	RIESGO	AUTENTICIDAD	TRAZABILIDAD	CONFIDENCIALIDAD	INTEGRIDAD	DISPONIBILIDAD	VALOR

8.3. IDENTIFICACIÓN DE LAS AMENAZAS

Para la identificación de las amenazas, así como de su valoración se implementará como modelo de aplicación la "Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información MAGERIT"[13], por medio de la cual se puede realizar la gestión y administración de los riesgos[14] y esta alineada con los estándares de seguridad más relevantes de la ISO.

La identificación de los activos de información y tecnológicos permiten definir su valor e importancia dentro de la ESE, una vez se define esto, se deben establecer cuáles son las amenazas a los que se encuentra expuesta la institución y que repercusión tienen si se llegara presentar un incidente con estos.

Una vez determinadas las posibles amenazas, se realiza la valoración cualitativa, para determina la posibilidad de ocurrencia, para definir dicha probabilidad se tendrá en cuenta la siguiente tabla:

Cuadro 6: Probabilidad de ocurrencia de amenazas

PROBABILIDAD DEL RIESGO			
	Nomenclatura	Categoría	Valoración
Probabilidad	MA	Prácticamente seguro	5
	A	Probable	4
	M	Posible	3
	B	Poco probable	2
	MB	muy raro	1

Fuente: Matriz de análisis de riesgos.

[13] **MAGERIT**. Versión 3.0. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Libro I – Método, 2012. [En línea] [Consultado: 21 de octubre de 2021]. Disponible en: https://www.ccn-cert.cni.es/documentos-publicos/1789-magerit-libro-i-metodo/file.html

[14] **ESET**, Welivesecurity by. MAGERIT: metodología práctica para gestionar riesgos. [Sitio web] 14 de Mayo de 2013. [En línea] [Consultado: 13 de Octubre de 2021] Disponible en: https://www.welivesecurity.com/la-es/2013/05/14/magerit-metodologia-practica-para-gestionar-riesgos/

Para la identificación de amenazas, y evaluar su posibilidad de ocurrencia, se trabaja con base al catálogo de amenazas que sugiere la metodología MAGERIT la cual define en 4 grandes grupos amenazas de tipo:

- [N] Desastres Naturales
- [I] De origen industrial
- [E] Errores de los usuarios
- [A] Ataques intencionados

Cuadro 7: Identificación de amenazas

IDENTIFICACIÓN DE AMENAZAS				
Tipo	**Amenaza**	**Descripción**	**Probabilidad**	
[L] Instalaciones: Infraestructura Física	[N.1] Fuego	Posibilidad de que las instalaciones de la ESE, se puedan ver afectadas por el fuego y se queme la infraestructura tecnológica	POCO PROBABLE	B

8.4. IDENTIFICACIÓN DE VULNERABILIDADES Y RIESGOS DE SEGURIDAD

Cuando hablamos en términos de seguridad de la información, podemos definir una vulnerabilidad como una debilidad que se encuentra en un activo y que puede llegar a ser materializada o explotada por una o más amenazas y que se convierte en un riesgo de seguridad. Es indispensable, por tanto, para poder proteger la información partir de la identificación de las vulnerabilidades que tenga los activos.

El análisis de vulnerabilidades se realizará por categoría de activo, ya que esta agrupación permite analizar activos de un mismo tipo, que poseen características muy similares.

Cuadro 8: Identificación de vulnerabilidades y riesgos

TIPO	VULNERABILIDAD
[HW] HARDWARE	•
[SW] SOFTWARE	•
[COM] RED	•
[P] PERSONAL	•
[L] INFRAESTRUCTURA FÍSICA	•
ORGANIZACIÓN	•

Fuente: Propia, realizada por el autor del plan.

8.5. IDENTIFICACIÓN DE CONTROLES

Los controles son las acciones orientadas a minimizar la probabilidad de ocurrencia o el impacto del riesgo; estos, deben estar directamente relacionados con las causas o las consecuencias identificadas para el riesgo y eliminarlas o mitigarlas. La administración del riesgo contribuirá a la gestión de la entidad, en la medida en que los controles se identifiquen, documenten, apliquen y sean efectivos para prevenir o mitigar los riesgos.

A continuación, se presentan las características mínimas que se deben tener en cuenta para la definición de los controles:

Cuadro 9: Características para la definición de controles

Característica	Descripción
Objetivos	No dependen del criterio de quien lo define y/o ejecute, sino de los resultados que se esperan obtener
Pertinentes	Están directamente orientados a atacar las causas o consecuencias del riesgo
Realizables	Se deben definir controles que la entidad o el proceso esté en capacidad de llevar a cabo
Medibles	Permiten el establecimiento de indicadores para verificar el cumplimiento de su aplicación y/o efectividad
Periódicos	Tienen frecuencia de aplicación en el tiempo
Efectivos	Eliminan o mitigan las causas o consecuencias y evitan la materialización del riesgo
Asignables	tienen responsables definidos para su ejecución

En el siguiente ejemplo se presenta una forma de redacción de un control.

Cuadro 10: Ejemplo de definición de control

Causa	Riesgo	Efecto/Consecuencia	Control
Uso de un calendario tributario obsoleto	Declaración de impuestos extemporánea	Sanciones pecuniarias para la entidad o disciplinaria para un(os) funcionario(s)	El contador y/o el Subdirector Administrativo y Financiero debe realizar la actualización u divulgación, en enero de cada año, de los calendarios tributarios nacionales y departamentales, en la página web, intranet, físicos, etc.

En esta etapa se deben describir todos los controles, existentes y por definir, deben estar orientados a atacar las causas y/o consecuencias (mitigar y/o eliminar) del riesgo. Una vez se hayan identificado y descrito los controles se debe determinar la clase del control; un control puede ser de tipo preventivo o correctivo como se presenta a continuación:

Cuadro 11: Descripción de las clases de controles

Clases de controles	
PREVENTIVO	CORRECTIVO
Acción o Conjunto de acciones que elimina o mitiga las causas del riesgo	Acción o conjunto de acciones que eliminan o mitigan las consecuencias
Orientación a disminuir la probabilidad de ocurrencia del riesgo	**Orienta a disminuir el nivel de impacto del Riesgo**

8.6. EVALUACIÓN DE LOS CONTROLES

Permite determinar en qué medida los controles identificados están aportando para disminuir los niveles de probabilidad e impacto del riesgo. Se evalúan verificando su documentación, aplicación y efectividad de la siguiente manera:

¿El control está documentado, incluye el responsable y la frecuencia de aplicación?	¿El control se está aplicando?	¿El control es efectivo (sirve o cumple su función?

- Si la pregunta relacionada con documentación se está cumpliendo, se deben asignar 25 puntos; en caso contrario marque 0.

- Si la pregunta relacionada con aplicación se está cumpliendo, se deben asignar 25 puntos; en caso contrario marque 0.

- Si la pregunta relacionada con efectividad se está cumpliendo, se deben asignar 50 puntos; en caso contrario marque 0.

La evaluación se debe aplicar a cada control definido para el riesgo, determinando si se cumple o no el factor, según corresponda.

9. MANEJO DE RIESGOS

Una vez determinada la zona donde está ubicado el riesgo, y dependiendo de las opciones de manejo, se deben formular las acciones orientadas al mejoramiento y fortalecimiento de los controles identificados. Las acciones que se definan para el manejo del riesgo deben contemplar:

- Corregir las fallas identificadas en los controles según la evaluación realizada a cada uno.
- Reforzar o fortalecer los controles existentes.

Acción a Desarrollar	**+**	**Definición de responsables**	**+**	Definición de Plazo	**=**	Definición Adecuada de Acciones
Resolución adecuada de los Riesgos						Resultado esperado

Definición adecuada de las acciones

Si la evaluación del riesgo residual, lo ubica en la zona baja no se deben formular acciones de manejo, el manejo estará únicamente enfocado en garantizar que los controles previamente establecidos operan de manera adecuada. Los riesgos ubicados en las zonas moderada, alta o extrema, exigen realizar acciones que fortalezcan los puntos débiles identificados en la evaluación de los controles.

10. SEGUIMIENTO DE RIESGOS

Cada cuatro meses Control Interno realizará seguimiento a todo el componente de administración de riesgos y verificará aspectos como:

- Cumplimiento de las políticas y directrices para la administración del riesgo: metodología de Administración del Riesgo (diseño y funcionamiento).
- Administración de los riesgos por proceso e institucionales: calificación y evaluación, efectividad de los controles y cumplimiento de las acciones.

Los resultados de la evaluación y las observaciones de la persona que haga las veces de Control Interno deben ser presentados a la Alta Dirección, para que se tomen las decisiones pertinentes que garanticen la sostenibilidad de la Administración del Riesgo en la organización.

11. MAPA DE RIESGOS

Una vez se tenga toda la información relacionada en los numerales anteriores, se documentará la información en el formato Mapa de riesgos de la Institucional y se articulará al resto de los riesgos identificados en los demás procesos.

12. ACTIVIDADES

Las siguientes actividades que se plantean son de ejecución anual

- Actualización del inventario de activos informáticos
- Valoración de activos informáticos según metodología MAGERIT.
- Identificación de amenazas, riesgos y vulnerabilidades.
- Identificación y definición de controles.