PLAN DE TRATAMIENTO DE RIESGOS DESEGURIDAD DE LA INFORMACIÓN

DIRECCIÓN DE GESTIÓN DE INFORMACIÓN

Bogotá D.C., enero de 2024

TABLA DE CONTENIDO

LITA DE TABLAS

LISTADO DE FIGURAS

1 INTRODUCCIÓN

Este documento es un instrumento orientador metodológico que busca direccionar las actividades y propósitos definidos en la Política para la Gestión Integral del Riesgo y en la Política de Seguridad de la información del Servicio Geológico Colombiano - SGC, con lo cual se pretende definir un lenguaje unificado en la entidad para implementar las mejores prácticas para la administración del riesgo en los procesos y proyectos que ejecute la entidad en cumplimiento de su objeto misional y de los demás requisitos establecidos por el estado colombiano.

La información que se maneja el SGC es fundamental para el cumplimiento de sus objetivos misionales y su relación con el ciudadano, es por ello que resguardar su información de cualquier posibilidad de alteración, mal uso, pérdida, entre otros muchos eventos, permite orientar las inversiones en seguridad hacia las brechas que mayor impacto pueden generar un incidente materializado. El grado de responsabilidad reposa en los sistemas, datos e información encaminados al logro de los objetivos internos, estos se pueden mejorar y mantener teniendo una adecuada sistematización y documentación.

El Servicio Geológico Colombiano – SGC, en pro de garantizar su misión institucional realiza actividades enmarcadas en procesos estratégicos, misionales y de apoyo, los cuales pueden afectarse por la existencia de riesgos de seguridad y privacidad de la información. El presente documento establece la manera en la que se van a tipificar los riesgos identificados y su tratamiento, todo alineado dentro del plan estratégico institucional, los lineamientos de la Arquitectura empresarial, el Modelo de Seguridad y Privacidad de la Información y el cumplimiento de la Política de Gobierno Digital.

2 OBJETIVO

Establecer los lineamientos para un proceso adecuado de gestión de riesgos de seguridad de la información en el SGC, con el fin de prevenir su materialización, y asegurar la información, los recursos tecnológicos y evitando daños reputacionales a la entidad.

Esto mediante la identificación, análisis, valoración de riesgos y el establecimiento de acciones de tratamiento dirigidos a prevenir la ocurrencia o minimizar el impacto de los riesgos de seguridad y privacidad de la información en el SGC.

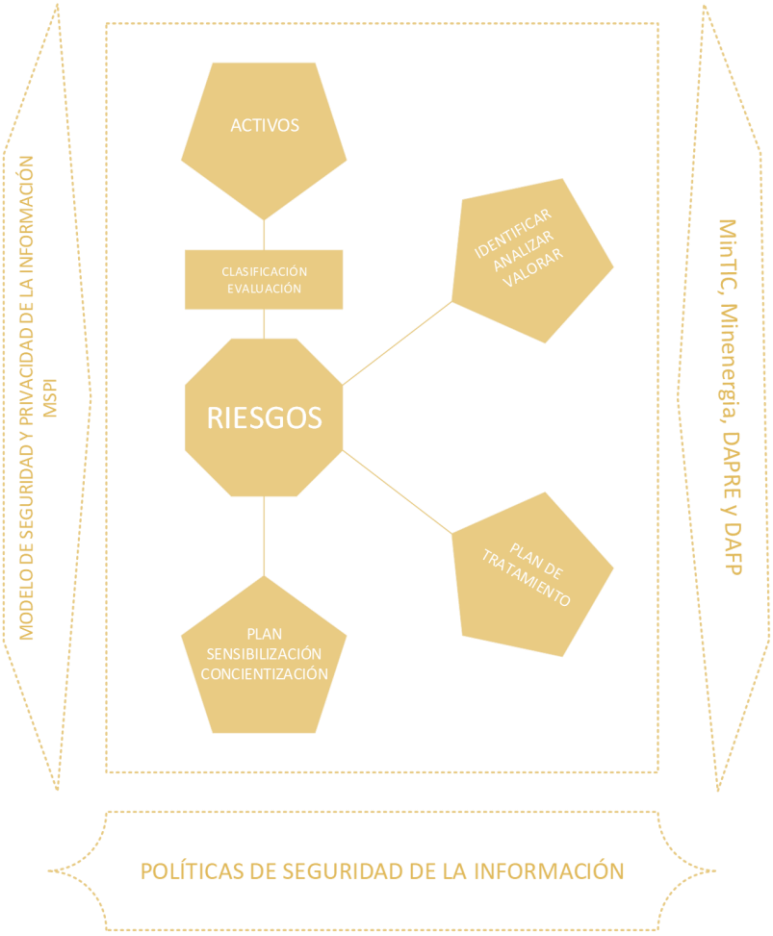
3 ALCANCE

Esta Metodología aplica para la identificación, análisis, valoración, tratamiento, monitoreo, control, comunicación y sensibilización de la gestión de riesgos de seguridad de la información y oportunidades para toda la institución en el desarrollo de los procesos del Sistema de Gestión Institucional y de los propósitos establecidos en su objeto misional para lograr el cumplimiento de los objetivos estratégicos del Servicio Geológico Colombiano.

4 METODOLOGÍA DE GESTIÓN INTEGRADA DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN

La metodología de gestión de riesgos de seguridad de la información del SGC alineada con estándares internacionales como son la familia ISO 27000:2022 y la ISO 31000:2018 como también lineamientos propios del gobierno nacional como son los generados por MINTIC, MINENERGIA, DAPRE Y DAFP.

Figura 1. Alineación de la metodología de gestión de riesgos



Fuente: Propia (2024)

A partir del inventario de activos de información con el que cuenta el SGC; se hace necesario establecer una clasificación de acuerdo con el Manual de Gestión del Riesgo del Departamento Administrativo de la Función Pública que establece tres pilares o principios de la Seguridad de la Información, a continuación, se presentan las definiciones desde los puntos de vista de seguridad de la información y de riesgos, la cual está alineada a la definición de la norma:

- **Confidencialidad**: "Es garantizar el acceso a la información sólo a los usuarios autorizados" (Seguridad de la Información de TGE, 2016). A nivel de riesgos: "La información es accesible solamente a quienes están autorizados para ello. Información cuya divulgación puede

generar desventajas competitivas, pérdidas económicas, afecta la reputación y/o imagen de la compañía" (Seguridad de la Información TGE, 2016).

- **Integridad**: "Evitar que la información sea modificada de manera no autorizada" (Seguridad de la Información de TGE, 2016). A nivel de riesgos: "Protección de la exactitud y estado completo de la información y métodos de procesamiento. Información sin errores ni fraude, la ocurrencia de alguna de estas ocasionará pérdidas significativas" (Seguridad de la Información TGE, 2016).
- **Disponibilidad**: "Garantizar que la información esté disponible cuando se necesite" (Seguridad de la Información de TGE, 2016). "A nivel de riesgos: Seguridad que los usuarios autorizados tienen acceso a la información y a los activos asociados cuando lo requieren. La información debe ser accesible y recuperable fácilmente en caso de suspensión del procesamiento" (Seguridad de la Información TGE, 2016).

El proceso para la gestión del riesgo debe estar adaptado a los procesos de negocio de la organización y comprende las siguientes actividades:

- **Comunicación y consulta.** Las partes involucradas tanto a nivel interno de la compañía como externo deben comunicación eficaz durante todas las etapas del proceso de gestión del riesgo y tener definidos los medios de comunicación, con el fin de garantizar que los responsables del proceso y las partes involucradas entiendan las bases sobre las cuales se toman decisiones (Icontec, 2011).

- **Establecer el Contexto.** Se procede a identificar las características de los factores internos y externo que influyen sobre la gestión del riesgo como por ejemplo la misión, visión, actividades que desarrolla la empresa, los interesados, legislación aplicable y demás factores 20 (Icontec, 2011), esto se analizará a partir del uso del método DOFA – Fortalezas,

Oportunidades, debilidades y Amenazas. El punto de partida de la identificación de riesgos es realizar una identificación y clasificación de activos de información de los procesos.

- **Valoración del Riesgo.** La definición de este término de acuerdo a la Norma ISO 31000, "valoración del riesgo es el proceso total de la identificación del riesgo, análisis del riesgo y evaluación del riesgo" (Icontec, 2011).

- **Identificación de los Riesgos.** "El propósito de la identificación del riesgo es la identificación de lo que puede ocurrir o las situaciones que puedan presentarse que afecten el logro de los objetivos del sistema o de la empresa" (PECB, 2008). El proceso de la identificación del riesgo comprende la identificación de las causas, consecuencias, fuentes generadoras de riesgo que puedan afectar el cumplimiento de los objetivos planteados para los procesos (PECB, 2008).

- **Análisis de los Riesgos.** "El análisis de riesgos implica la consideración de las causas y las fuentes de riesgo, sus consecuencias (impacto) y la probabilidad de que estas consecuencias puedan ocurrir" (Icontec, 2011).

- **Evaluación de los Riesgos.** La Norma ISO 31000:2018, establece que la evaluación de la gestión del riesgo debe realizarse: Con base en los resultados del análisis de riesgos, la finalidad de la evaluación del riesgo es ayudar a la toma de decisiones, determinando los riesgos a tratar y la prioridad de implementar el tratamiento de los mismos. La evaluación del riesgo es la comparación de los niveles de riesgo estimados con los criterios de evaluación y los criterios de aceptación del riesgo y los priorizados que se deben establecer cuando se consideró el contexto.

- **Evaluación de los Riesgos.** La Norma ISO 31000:2018 establece que la evaluación de la gestión del riesgo debe realizarse con base en los resultados del análisis de riesgos, la

finalidad de la evaluación del riesgo es ayudar a la toma de decisiones, determinando los riesgos a tratar y la prioridad de implementar el tratamiento de los mismos. La evaluación del riesgo es la comparación de los niveles de riesgo estimados con los criterios de evaluación y los criterios de aceptación del riesgo y los priorizados que se deben establecer cuando se consideró el contexto. La organización debe establecer las prioridades para la aplicación del tratamiento de Riesgos (Icontec, 2011).

- **Tratamiento de Riesgos.** "El tratamiento del riesgo involucra la selección de una o más opciones para modificar los riesgos y la implementación de tales opciones. Una vez implementado, el tratamiento suministra controles o los modifica" (Icontec, 2011).

- **Monitoreo y Revisión.** Como parte del proceso de gestión del riesgo, los riesgos y los controles deberían ser monitoreados y revisados regularmente para comprobar que:
    - La hipótesis acerca de los riesgos sigue siendo válidas
    - La hipótesis en la que está basada la valoración del riesgo, incluyendo el contexto interior y exterior, siguen siendo válidas
    - Se van cumpliendo los resultados esperados
    - La técnica de valoración del riesgo se aplica correctamente
    - Los tratamientos del riesgo son efectivos.

La gestión de riesgos se desarrolla con un ciclo PHVA, (Planear – Hacer – Verificar – Actuar), para alcanzar la mejora continua del sistema de gestión contando con la responsabilidad de conservar y mantener información documentada como respaldo. El ciclo PHVA consta de cuatro fases: En la *Figura 4* se ilustra el Ciclo PHVA.

- **Fase Planificar.** Dentro de esta fase establecen los objetivos y las oportunidades de mejora, igualmente con los indicadores de medición para controlar y cuantificar los objetivos.
- **Fase Hacer:** Se ejecuta el plan establecido que consiste en implementar las acciones para lograr mejoras planteadas.
- **Fase Verificar**: En esta fase del ciclo una vez implementada la mejora, se estipula un periodo de prueba para verificar el perfecto funcionamiento de las acciones implementadas.
- **Fase Actuar:** Se analizan los resultados de las acciones implementadas y si estas por cualquier razón no se cumplen con los objetivos definidos, se analizan las causas de las desviaciones y se generan los respectivos planes de acción.

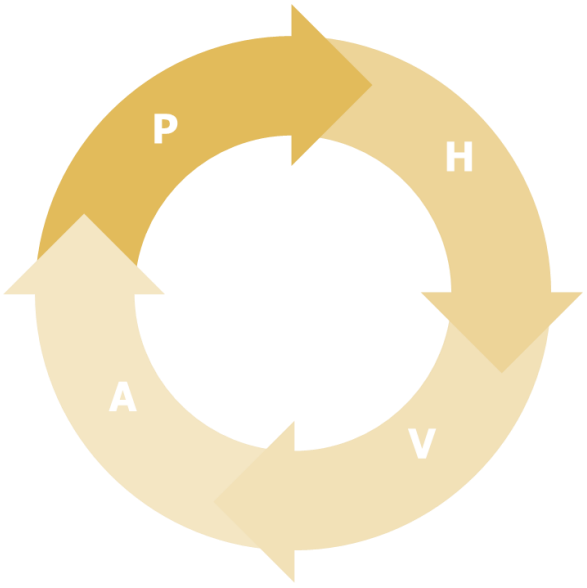


Figura 2. *Ciclo PHVA de la Gestión de Riesgos*

Planear

Analizar el problema para poder definir las actividades En esta fase se realizan análisis cualitativos, reuniones, mesas técnicas para definir actividades, responsables y tiempos

Hacer

Desarrollar cada una de las actividades generadas en la fase de planeación bajo los parámetros establecidos como recursos tiempos, riesgos, etc

Verificar

Se establecen los indicadores y se discuten los resultados de las actividades realizadas verificando que lo ejecutado es igual a lo esperado

Actuar

Se establecen las brechas que se generen en las actividades desarrolladas entre los resultados generados y los resultados deseados

Fuente: Propia (2024)

La planeación de la gestión de riesgos debe ser sistemática y acorde a las necesidades del SGC para que el abordaje sea eficaz y oportuno y a partir de los lineamientos establecidos por los

principios fundamentales que deben ser abordados para realizar el tratamiento de los riesgos esperado por la Entidad.

La gestión del riesgo en la seguridad de la información debe ser un proceso continuo, tal proceso debe establecer el contexto, evaluar los riesgos y tratarlos utilizando un plan de tratamiento para implementar las recomendaciones y decisiones, la gestión del riesgo analiza lo que puede suceder y cuáles pueden ser las posibles consecuencias, antes de decidir lo que se debería hacer y cuándo hacerlo, con el fin de reducir el riesgo hasta un nivel aceptable[1].

Los pasos que comprender las actividades que se deben desarrollar para la gestión de riesgo en seguridad de la información son:

- Identificación del Contexto.
- Activos de la información.
- Riesgo inherente.
- Riesgo residual
- Tratamiento de riesgo.

[1] ICONTEC. Norma Técnica NTC-ISO/IEC 27005, Tecnología de la Información. Técnicas de seguridad. Gestión del riesgo en la seguridad de la información, 2009, p. 4

Figura 3. Paso a paso para llevar a cabo el análisis de riesgos

Fuente: Propia (2024)

4.1 Identificación del Contexto

Para un análisis de riesgos completo y una correcta aplicación de la metodología de gestión, es necesario conocer y entender el contexto general del objeto de evaluación (organización, procesos, subproceso, servicios, etc.); para establecer su entorno interno y externo, complejidad, procesos, planeación institucional, entre otros aspectos.[2]

4.1.1 Contexto externo

Consiste en determinar las características o aspectos esenciales del entorno en el cual opera el SGC, teniendo en cuenta los factores identificados en la siguiente tabla.

[2] Tomando como base la Guía para la gestión del riesgo y diseño de controles, en entidades públicas. DAFP. (2020).

Tabla 1. Factores Externos

Descripción de Factores	
CONTEXTO EXTERNO	• **Sector en el que opera:** Características y deberes del sector de minas y energía. • **Económico:** Patrimonio económico. • **Político:** Aspecto legal y regulatorio**.** • **Social y cultural:** Responsabilidad social. • **Tecnológico:** Avances en tecnología, intercambio de información con otras entidades. • **Medioambientales:** Emisiones y residuos, catástrofes naturales, desarrollo sostenible. • **Comunicación Externa:** Mecanismos utilizados para que los usuarios o ciudadanos entren en contacto con la entidad.

Fuente: Propia (2024)

4.1.2 Contexto interno

Radica en determinar las características o aspectos esenciales del ambiente en el cual la institución busca alcanzar sus objetivos institucionales, teniendo en cuenta los factores descritos en la siguiente tabla.

Tabla 2. Factores Internos

Descripción de Factores	
CONTEXTO INTERNO	• **Direccionamiento estratégico:** misión, visión, objetivos, funciones, organigrama. • **Entes internos de control:** oficina de control interno, sistema de PQRD. • **Financieros: I**nfraestructura. • **Personas:** Competencia del personal, principales contactos. • **Procesos:** Mapa de procesos, tipos de procesos. • **Tecnología:** Conectividad general, gestión de la información geocientífica. • **Comunicación interna:** Canales utilizados para la comunicación interna.

Fuente: Propia (2024)

4.1.3 Contexto del proceso

Consiste en determinar las características o aspectos esenciales de cada proceso y sus interrelaciones, teniendo en cuenta factores como:

Tabla 3. Factores del proceso

Descripción de Factores	
CONTEXTO DEL PROCESO	• **Diseño del proceso:** Descripción detallada del proceso. • **Transversalidad:** Procesos que determinan lineamientos necesarios para el desarrollo de todos los procesos de la institución. • **Procedimientos y formatos asociados:** Pertinencia de los procedimientos y formatos establecidos en los procesos y su ejecución en términos de tiempo y ubicación. • **Responsables del proceso:** Autoridad y responsabilidad de los empleados frente al proceso.

Fuente: Propia (2024)

Para su desarrollo se deben tener en cuenta los siguientes requisitos:

- Deben participar todas aquellas personas que intervienen en el proceso.
- Los resultados deben ser aprobados por los dueños de los procesos.

4.2 Identificación de los activos de seguridad de la información

Toda organización posee información importante que desea proteger frente a cualquier situación que suponga un riesgo o amenaza, dicha información que resulta fundamental para la organización es lo que se denomina activo de información.

Los activos de información pueden ser archivos, productos geocientíficos, bases de datos, contratos, acuerdos, documentación del sistema, manuales de los usuarios, informes, etc; que pueden estar contenidos en aplicaciones, servidores, medios físicos, archivadores, personas. Dichos contenedores son susceptibles de accesos no autorizados, así como de ataques que ocasionen la pérdida de la información que contienen.

De aquí la importancia de la identificación y valoración de los activos de información, ya que el contenedor heredará la valoración de los impactos más altos de los activos que contiene, y los riesgos de seguridad de la información estarán asociados a dichos contenedores.

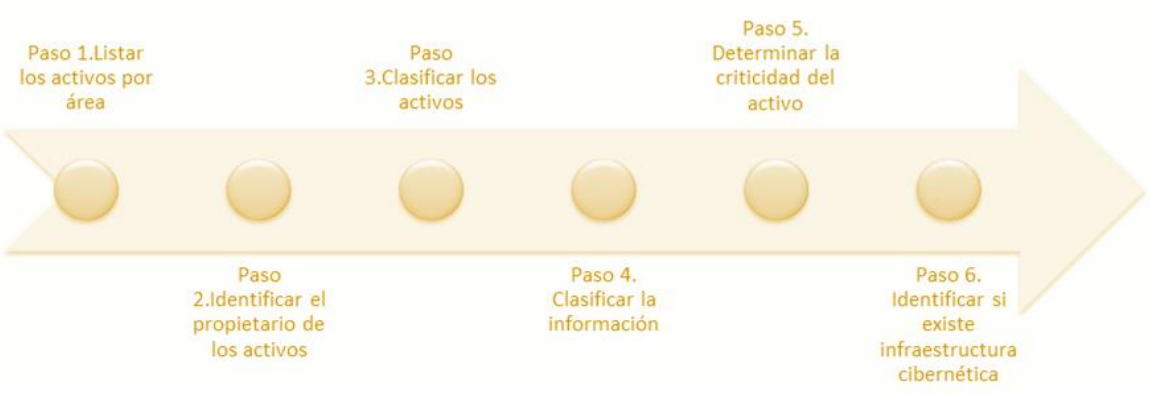
Tabla 4. Conceptualización activos de información

¿Qué son los activos?	¿Por qué identificar los activos?
Un activo es cualquier elemento que tenga valor para la organización, sin embargo, en el contexto de seguridad digital, son activos elementos tales como: -Aplicaciones de la organización	Permite determinar qué es lo más importante que cada entidad y sus procesos poseen (sean bases de datos, archivos, servidores web o aplicaciones clave para que la entidad pueda prestar sus servicios).
-Servicios web -Redes -Información física o digital -Tecnologías de información TI -Tecnologías de operación TO que utiliza la organización para funcionar en el entorno digital	La Entidad puede saber qué es lo que debe proteger para garantizar tanto su funcionamiento interno como su funcionamiento de cara al ciudadano, aumentando así su confianza en el uso del entorno digital.

Fuente: Actualizado por la Dirección de Gestión y Desempeño Institucional de Función Pública y Ministerio TIC, 2020

A continuación, se presentan los pasos necesarios para identificar los activos de información.

Figura 4. Pasos para la identificación de activos



Fuente: Elaboración conjunta entre la Dirección de Gestión y Desempeño Institucional de Función Pública y el Ministerio TIC, 2018.

Dentro de las fuentes de información para identificar activos de información, se encuentran: La documentación y registros de cada proceso y/o subproceso, descritos en el sistema de gestión de

calidad, los inventarios de la plataforma tecnológica, además del estudio de campo que se lleve a cabo en cada proceso o áreas.

A continuación, se realizan algunas aclaraciones sobre los campos que componen el proceso de identificación de activos de información:

- **Id del activo:** Es el identificador único de cada activo. Inicia con la codificación establecida en el SGC para cada proceso, ej: CI-GM-01.

- **Nombre del activo de información:** La orientación para identificar los activos de información, siempre debe ser: cualquier archivo (físico o digital), bases de datos, informe, acuerdo, manual que genere valor para la organización.

- **Descripción del activo de información:** Descripción detallada del activo con el fin de que sea clara la importancia de dicha información para la institución.

- **Tipo de activo:** Los tipos de activos pueden ser: Acta, Base de datos, Base de datos personales, Columnas estratigráficas, Contrato / Convenio, Documentos, Expediente, Fichas técnicas, Formato / Registro, Informe, Libro, Manual, Mapas geológicos, Matriz, Modelos, Muestra, Política, Presentación, Procedimiento, Publicaciones.
- **Formato:** El formato del activo puede ser: Electrónico, Archivo físico, Electrónico / Físico, Información no representada.

- **Clasificación:** La clasificación del activo debe realizarse de acuerdo a la Ley 1712 de 2014 y la Ley 1581 de 2012, en información reservada o información clasificada o información pública como también si contiene o no datos personales.

- **Proceso:** Se debe establecer a qué proceso del SGC y a qué área, pertenece el activo de información.

- **Responsable o Propietario:** Líder de proceso, cargo responsable de la ejecución del proceso, o persona designada por el líder de proceso que tiene bajo su cargo:

    - Evaluar y asignar una clasificación a la información que contiene el activo de información (confidencial, uso interno, y pública).
    - Verificar que se implementen los controles de acuerdo al nivel de clasificación de la información.
    - Establecer los privilegios de acceso asociados con los activos de información de los que es responsable.
    - Determinar los requerimientos de seguridad, criterios de acceso y criterios de copias de respaldo para los activos de información de los que es responsable.
    - Autorizar y revocar el acceso a aquellas personas que tengan necesidad de utilizar sus activos de información.
    - Establecer las actividades de preservación y restauración de información.
    - Aprobar la divulgación de información que esté bajo su cargo.

- **Custodio:** Es el proceso, equipo de trabajo, o cargo, designado por los propietarios o por la institución, encargado de mantener las medidas de protección establecidas sobre los activos de información confiados. Sus responsabilidades son:

    - Proteger la información que le ha sido confiada para efectos de distribución, acceso, modificaciones, destrucción o usos no autorizados.
    - Garantizar la Confidencialidad, Integridad y Disponibilidad de la información que le ha sido confiada.
    - Asegurar que los requerimientos de retención de registros sean basados en los análisis realizados por el propietario de la información.
    - Suministrar los servicios de sistemas informáticos de acuerdo con las instrucciones de los propietarios de la información, cuando sea pertinente.
    - Suministrar y administrar los respaldos y sistemas de recuperación de la información.

- **Usuario:** Cualquier persona, entidad, cargo, proceso, sistema automatizado o grupo de trabajo, que genere, obtenga, transforme, conserve o utilice información en papel o en medio digital, físicamente o a través de las redes de datos y los sistemas de información del SGC, para propósitos propios de su labor.

4.2.1 Valoración de los activos de información

Los activos de información identificados deberán ser valorados según los principios básicos de la seguridad de la información:

- **Confidencialidad**: Violación a la propiedad de la información que permite su divulgación a individuos, entidades o procesos no autorizados.
- **Integridad:** Propiedad de mantener con exactitud la información tal cual fue generada, siendo manipulada o alterada por personas o procesos no autorizados.
- **Disponibilidad**: Condición de la información de encontrarse a disposición de quienes deben acceder a ella, ya sean personas, procesos o aplicaciones.

Para valor el activo de información cada principio se tendrá en cuenta los siguientes criterios:

- Social
- Legal
- Reputacional
- Conocimiento o Investigación

Notas:

- Para la valoración de los activos de información se deben tener en cuenta los siguientes requisitos:
  a. Deben participar los responsables o propietarios de los activos de información.
  b. Las escalas para valorar los impactos sobre cada principio se definieron por el SGC.
  c. Los resultados deben ser aprobados por los líderes de los procesos.
- El impacto total por principio de seguridad de la información será el mayor de los impactos analizados.

- La valoración se realiza únicamente cuando se hayan presentado cambios significativos en los procesos de la institución o se generen nuevos activos de información o simplemente dichos activos ya no sean necesarios para el proceso.

A continuación, se presentan las escalas que se deben tener en cuenta para determinar el nivel del impacto de la pérdida de confidencialidad, integridad o disponibilidad de la información.

4.3 Riesgo Inherente

Es el riesgo intrínseco de cada proceso o actividad, sin tener en cuenta los controles que de éste se tengan. Es propio del trabajo o proceso, que no puede ser eliminado del sistema; es decir, en todo trabajo o proceso se encontrarán riesgos para las personas o para la ejecución de la actividad en sí misma.

4.3.1 Identificación del riesgo

La identificación del riesgo consiste en establecer las fuentes de riesgo, los eventos, sus causas y sus consecuencias. Para el análisis se pueden involucrar datos históricos, análisis teóricos, opiniones informadas y expertas y las necesidades de las partes involucradas. (NTC ISO 31000, Numeral 2.15). Durante la identificación del riesgo se debe tener en cuenta el contexto organizacional, según lo establecido en el numeral 7.1 Identificación del Contexto: Contexto externo, contexto interno y el contexto del proceso.

Adicionalmente se recomienda tener en cuenta todas aquellas situaciones que pueden entorpecer el normal desarrollo o impedir el logro de los objetivos y metas de la institución, de sus procesos, subprocesos o actividades o de las disposiciones a las que está obligada y comprometida a cumplir. Los riesgos se identifican mediante la presentación del escenario de afectación de los pilares de seguridad de la información los cuales serían:

- Pérdida de la confidencialidad
- Pérdida de la integridad
- Pérdida de la disponibilidad

Cada riesgo identificado debe contener inicialmente la siguiente información:

- **Id del riesgo:** Es el código en secuencia con el cual va a ir identificado el riesgo, ej: RSEG1: Riesgo de seguridad de la información.

- **Descripción del Riesgo:** Con el fin de prevenir la confusión entre causas de riesgos, riesgos verdaderos y efectos o consecuencias del riesgo, se recomienda usar una descripción formal de los elementos requeridos del riesgo (Metalenguaje de riesgo) es decir una declaración estructurada del riesgo en tres partes, como se muestra a continuación: ***Se produce <Amenaza>, debido a <Vulnerabilidad>, ocasionando <Consecuencia>.***

Figura 5. Estructura propuesta para la redacción del riesgo

Fuente: Adaptado del Curso Riesgo Operativo de la Universidad del Rosario por la Dirección de Gestión y Desempeño Institucional de Función Pública, 2020

Ejemplos:

a) Se produce un incendio en el Centro de Cómputo <*Amenaza*> debido a la ausencia de mantenimiento del sistema contraincendios <*Vulnerabilidad*>, ocasionando daños a la infraestructura y a los recursos tecnológicos <*Consecuencia*>.
b) Se genera un ataque cibernético <*Amenaza*> debido a la ausencia de controles fuertes de acceso a la red informática <*Vulnerabilidad*>, que ocasiona la no disponibilidad de información crítica para los procesos que se soportan en dicha información <*Consecuencia*>.
c) Se produce un acceso no autorizado de personal ajeno a la institución <*Amenaza*> debido a la ausencia de controles de acceso que restrinjan el acceso adecuadamente a las instalaciones

<Vulnerabilidad>, ocasionando el robo de activos y contenedores de información críticos para la institución *<Consecuencia>*.

4.3.1.1 Identificación de Amenazas

Las amenazas son aquellas fuentes que pueden explotar exitosamente una vulnerabilidad en particular. Una vulnerabilidad es una debilidad (vacío) que se puede activar accidentalmente o explotar intencionalmente. Una fuente de amenaza no representa un riesgo cuando no existe una vulnerabilidad que pueda ser explotada. Las amenazas se pueden clasificar en:

- Amenazas naturales: Inundaciones, terremotos, tornados, deslizamientos de tierra, avalanchas, tormentas eléctricas y otros eventos similares.
- Amenazas humanas: Eventos activados o causados por las personas, tales como actos no intencionados (errores en la entrada de datos) o malintencionados (ataques a la red, activación de software malicioso, acceso no autorizado a información confidencial).
- Amenazas ambientales: Faltas prolongadas de energía eléctrica, polución, químicos, dispersión de líquidos.

Durante la identificación de las amenazas, es importante considerar todas las fuentes potenciales que podrían afectar a la institución.

4.3.1.2 Identificación de Vulnerabilidades

Se definen como el defecto o debilidad en los procedimientos, diseño, implementación o en los controles internos de los procesos y los sistemas que podrían ser explotadas (activadas accidentalmente o explotadas intencionalmente) y que resulta en una brecha de seguridad o violación de las políticas de seguridad.

El análisis de las amenazas de un proceso incluye el análisis de las vulnerabilidades asociadas al ambiente donde opera. La meta de este paso es desarrollar una lista de vulnerabilidades del proceso (defectos o debilidades) que podrían ser explotadas por fuentes de amenazas potenciales.

Los métodos para la identificación de vulnerabilidades comprenden el uso de fuentes de vulnerabilidades, la realización de pruebas a la seguridad de los procesos, pruebas a la seguridad de los sistemas y evaluaciones de control interno.

Tabla 5. Tabla de amenazas y vulnerabilidades de acuerdo con el tipo de activo

Tipo de activo	Ejemplos de vulnerabilidades	Ejemplos de amenazas
Hardware	Almacenamiento de medios sin protección	Hurto de medios o documentos
Software	Ausencia de parches de seguridad	Abuso de los derechos
Red	Líneas de comunicación sin protección	Escucha encubierta
Información	Falta de controles de acceso físico	Hurto de información
Personal	Falta de capacitación en las herramientas	Error en el uso
Organización	Ausencia de políticas de seguridad	Abuso de los derechos

Fuente: Ministerio de Tecnologías de la Información y Comunicaciones MinTIC, 2018.

Puntos a tener en cuenta para la identificación de riesgos:

- El proceso de identificación de riesgos debe ser llevado a cabo por personal capacitado en riesgos de cada sistema de gestión, en acompañamiento de los funcionarios que hacen parte de cada proceso.
- Tener claro el contexto del proceso, sus objetivos, metas, obligaciones, compromisos.
- Centrarse en riesgos más significativos para la institución o el proceso, y que estén relacionados con los objetivos, metas y obligaciones.
- Tener en cuenta causas internas y externas.
- Al final los riesgos deberán ser presentados a los dueños de los procesos, quienes deberán aceptarlos y tomar las medidas necesarias para reducirlos a niveles aceptables para la institución.
- Los riesgos también pueden ser identificados mediante el acompañamiento de expertos externos, así como teniendo en cuenta la experiencia de otras entidades del sector.
- Algunas técnicas que se pueden utilizar para identificar riesgos son:

    - Tormenta de Ideas
    - Técnica Delphi
    - Entrevistas
    - Taller práctico

- Juicio de expertos

Nota: El método más efectivo para valorar activos de información, así como identificar posibles riesgos en materia de seguridad de la información es la de entrevistar a cada uno de los líderes de los procesos para realizar dicho análisis para cada activo de información identificado.

4.3.2 Clasificación del riesgo

Permite agrupar los riesgos identificados, se clasifica cada uno de los riesgos en las siguientes categorías.

Tabla 6. Clasificación de riesgos

Ejecución y administración de procesos	Pérdidas derivadas de errores en la ejecución y administración de procesos.
Fraude externo	Pérdida derivada de actos de fraude por personas ajenas a la organización (no participa personal de la entidad).
Fraude interno	Pérdida debido a actos de fraude, actuaciones irregulares, comisión de hechos delictivos abuso de confianza, apropiación indebida, incumplimiento de regulaciones legales o internas de la entidad en las cuales está involucrado por lo menos 1 participante interno de la organización, son realizadas de forma intencional y/o con ánimo de lucro para sí mismo o para terceros.
Fallas tecnológicas	Errores en hardware, software, telecomunicaciones, interrupción de servicios básicos.
Relaciones laborales	Pérdidas que surgen de acciones contrarias a las leyes o acuerdos de empleo, salud o seguridad, del pago de demandas por daños personales o de discriminación.
Usuarios, productos y prácticas	Fallas negligentes o involuntarias de las obligaciones frente a los usuarios y que impiden satisfacer una obligación profesional frente a éstos.
Daños a activos fijos/ eventos externos	Pérdida por daños o extravíos de los activos fijos por desastres naturales u otros riesgos/eventos externos como atentados, vandalismo, orden público.

Fuente: Adaptado del Curso Riesgo Operativo Universidad del Rosario por la Dirección de Gestión y Desempeño Institucional de Función Pública, 2020

Teniendo en cuenta que en la anterior se definieron una serie de factores generadores de riesgo, para poder definir la clasificación de riesgos, su interrelación es la siguiente:

Figura 6. Relación entre factores de riesgo y clasificación del riesgo

Fuente: Adaptado del Curso Riesgo Operativo Universidad del Rosario por la Dirección de Gestión y Desempeño Institucional de Función Pública, 2020.

4.3.3 Valoración del riesgo

La valoración del riesgo consiste en valorar la probabilidad y el impacto del riesgo identificado, con el fin de determinar el nivel del riesgo inherente.

Figura 7. Valoración del riesgo inherente

Fuente: Propia (2024)

La probabilidad se define como la posibilidad de ocurrencia del escenario de riesgo inherente.

Tabla 7. Tabla de probabilidad Tabla de probabilidad

	Frecuencia de la Actividad	Probabilidad
Muy Baja	La actividad que conlleva el riesgo se ejecuta como máximos 2 veces por año	20%
Baja	La actividad que conlleva el riesgo se ejecuta de 3 a 24 veces por año	40%
Media	La actividad que conlleva el riesgo se ejecuta de 24 a 500 veces por año	0%
Alta	La actividad que conlleva el riesgo se ejecuta mínimo 500 veces al año y máximo 5000 veces por año	80%
Muy Alta	La actividad que conlleva el riesgo se ejecuta más de 5000 veces por año	100%

Fuente: Propia (2024)

La determinación del impacto se entiende como la consecuencia económica y reputacional que se genera por la materialización del riesgo.

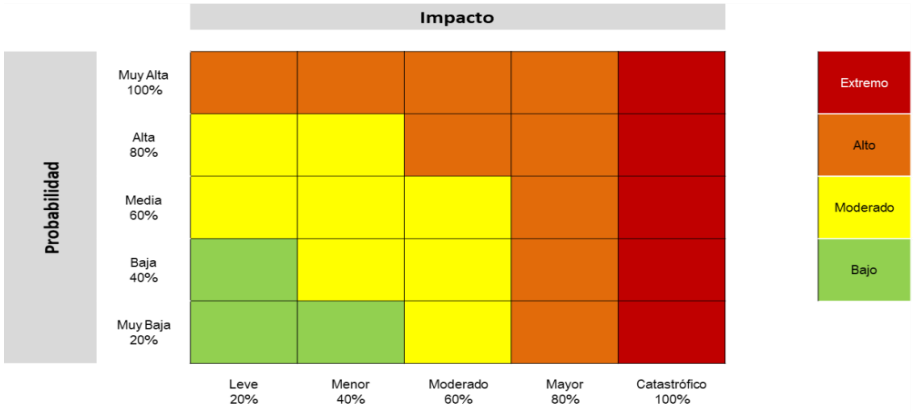
Tabla 8. Tabla de impacto

	Afectación Económica	Reputacional
Leve 20%	Afectación menor a 10 SMLMV .	El riesgo afecta la imagen de algún área de la organización.
Menor 40%	Entre 10 y 50 SMLMV	El riesgo afecta la imagen de la entidad internamente, de conocimiento general nivel interno, de junta directiva y accionistas y/o de proveedores.
Moderado 60%	Entre 50 y 100 SMLMV	El riesgo afecta la imagen de la entidad con algunos usuarios de relevancia frente al logro de los objetivos.
Mayor 80%	Entre 100 y 500 SMLMV	El riesgo afecta la imagen de la entidad con efecto publicitario sostenido a nivel de sector administrativo, nivel departamental o municipal.
Catastrófico 100%	Mayor a 500 SMLMV	El riesgo afecta la imagen de la entidad a nivel nacional, con efecto publicitario sostenido a nivel país

Fuente: Propia (2024)

Para el análisis preliminar (riesgo inherente), en esta etapa se define el nivel de severidad para el riesgo de seguridad de la información identificado, para ello, se aplica la matriz de calor.

Figura 8. Matriz de calor



Fuente: Propia (2024)

En la *Figura 12* se observa un ejemplo aplicando la etapa de valoración del riesgo sobre un activo como es la base de datos de nómina.

4.4 Riesgo Residual

El riesgo residual es aquel riesgo que subsiste, después de haber valorado la efectividad de los controles existentes. Es importante advertir que el nivel de riesgo al que está sometido una organización nunca puede erradicarse totalmente. Por ello, se debe buscar un equilibrio entre el nivel de recursos y mecanismos que es preciso dedicar para minimizar o mitigar estos riesgos y un cierto nivel de confianza que se puede considerar suficiente (riesgo aceptable).

El riesgo residual refleja el riesgo remanente, una vez se han implantado de manera eficaz las acciones planificadas por la institución para mitigar el riesgo inherente. A continuación, se presenta el proceso para la evaluación de los controles:

Figura 9. Proceso de evaluación de los controles

Fuente: Propia (2024)

- **Descripción del control:** Corresponde a la mención precisa de un proceso, política, dispositivo, práctica, u otra acción determinada que está prevista para modificar el riesgo.

- **Tipo de control**: Corresponde a controles tipo: preventivo, correctivo, o preventivo y correctivo.

- **Efectividad del control:** Resultado de la evaluación de los criterios antes mencionados para establecer si el control "es efectivo" o "no es efectivo".

4.4.1 Identificación de los controles existentes

Este paso consiste en identificar los controles actualmente implementados y en funcionamiento para cada uno de los riesgos analizados. Durante esta actividad se debe determinar la naturaleza de cada control. A continuación, se describen los tipos de control a tener en cuenta:

- **Controles Preventivos:** Evitan que un evento suceda. Por ejemplo, el requerimiento de un login y password en un sistema de información es un control preventivo. Éste previene (teóricamente) que personas no autorizadas puedan ingresar al sistema.
- **Controles Correctivos:** Permiten enfrentar la situación una vez se ha presentado. Por ejemplo, en caso de un desastre natural u otra emergencia mediante las pólizas de seguro y otros mecanismos de recuperación de negocio o respaldo, es posible volver a recuperar las operaciones.

- **Controles preventivos – correctivos:** cuando se aplican los dos tipos de controles al mismo tiempo, por ejemplo: Firewall, en el cual se gestionan permiso de acceso (Control preventivo) y bloquea en caso de detectar un intento de acceso no autorizado (Control correctivo).

4.4.2 Evaluación de los controles existentes

Este paso consiste en evaluar si el control es o no es efectivo. Para esto se requiere evaluar cada uno de los siguientes aspectos.

Tabla 9. Criterios de evaluación de los controles

Criterio de evaluación	Respuesta	Peso
1.1. Asignación de responsable	Asignado	15
	No asignado	0
1.2. Segregación y autoridad del responsable	Adecuado	15
	Inadecuado	0
2. Periodicidad	Oportuna	15
	Inoportuna	0
3. Propósito	Preventivo	15
	Detectivo	10
	Correctivo	10
	No es un control	0
4. Como se realiza la actividad del control	Confiable	15
	No confiable	0
5. Qué pasa con las observaciones o desviaciones	Se investigan y resuelven oportunamente	15
	No se investigan ni resuelven oportunamente	0
	Completa	10

Criterio de evaluación	Respuesta	Peso
6. Evidencia de la ejecución del control	Incompleta	5
	No existe	0

Fuente: Propia (2024)

La suma de los puntajes obtenidos para cada criterio será la calificación individual de cada control, según la siguiente tabla.

Tabla 10. Calificación individual del control

Calificación individual del control	Peso de la evaluación individual del diseño del control
Fuerte	Calificación entre 96 y 100
Moderado	Calificación entre 86 y 95
Débil	Calificación entre 0 y 85

Fuente: Propia (2024)

4.4.3 Análisis y valoración del riesgo residual

Una vez los controles han sido evaluados de acuerdo con el proceso descrito anteriormente, se procede a determinar si los controles analizados reducen la probabilidad o el impacto del riesgo. Para este análisis se deben tener en cuenta los siguientes criterios de afectación.

Tabla 11. Criterios de Afectación del Control

Afectación	Naturaleza del Control
Probabilidad	Controles preventivos
Impacto	Controles correctivos y detectivos

Fuente: Propia (2024)

El promedio de los controles que afectan la probabilidad o el impacto determinarán el nivel de solidez del conjunto de controles, de acuerdo con la siguiente tabla.

Tabla 12. Solidez del conjunto de controles

Solidez del conjunto de controles	
Fuerte	El promedio de la solidez individual de cada control al sumarlos y ponderarlos es igual a 100.
Moderado	El promedio de la solidez individual de cada control al sumarlos y ponderarlos está entre 50 y 99.
Débil	El promedio de la solidez individual de cada control al sumarlos y ponderarlos es menor a 50.

Fuente: Propia (2024)

Resultado del análisis del control:

Únicamente los controles fuertes o moderados reducirán el nivel de la probabilidad o el impacto del riesgo analizado. Esto significa que se realiza un desplazamiento en el mapa de riesgos como se representa en la siguiente tabla.

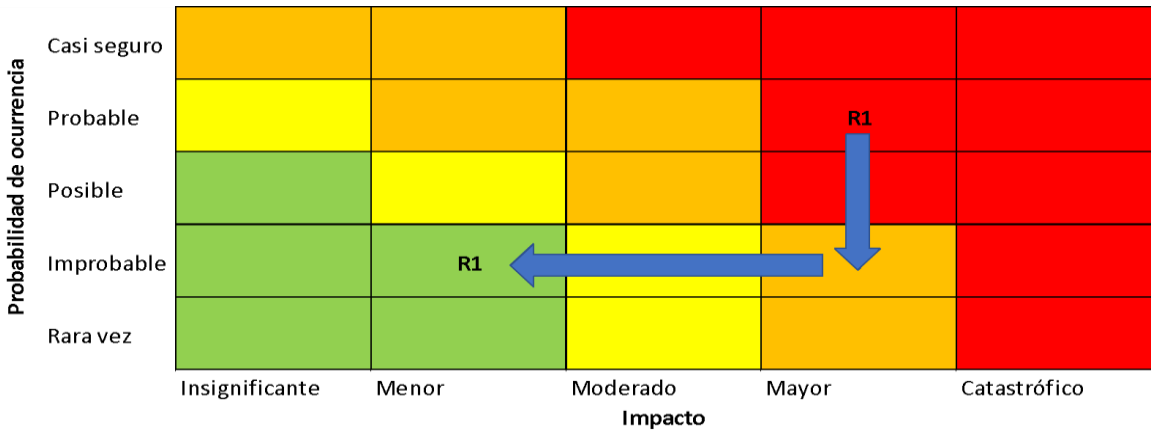
Tabla 13. Solidez del conjunto de controles

Solidez del conjunto de controles	
Fuerte	Reduce en 2 niveles la probabilidad o el impacto según el tipo de control.
Moderado	Reduce en 1 nivel la probabilidad o el impacto según el tipo de control.
Débil	Sin afectación de la probabilidad o el impacto.

Fuente: Propia (2024)

Los lineamientos anteriores hacen que se presenten movimientos del riesgo en el mapa de riesgos, trasladándose el riesgo a un nuevo campo que denota que se ha reducido su probabilidad (hacia abajo) o su impacto (hacia la izquierda), como se muestra a continuación:

Figura 10. Movimiento del riesgo según la efectividad de los controles



Fuente: Propia (2024)

4.4.4 Criterios de aceptación del riesgo

La siguiente tabla define la tolerancia al riesgo en la institución, así como la prioridad de mitigación según el nivel del riesgo.

Tabla 14. Criterios de aceptación del riesgo

Criterios de aceptación del riesgo	
B: Zona de riesgo baja	Riesgo aceptable. Deben ser monitoreados mínimo dos veces al año.
M: Zona de riesgo moderada	Requiere planes de tratamiento a largo plazo. (En un término de 3 a 6 meses).
A: Zona de riesgo Alta	Requiere planes de tratamiento a corto plazo (En un término de 1 a 3 meses).
E: Zona de riesgo extrema	Requiere planes de tratamiento con urgencia. (En un término máximo de 30 días).

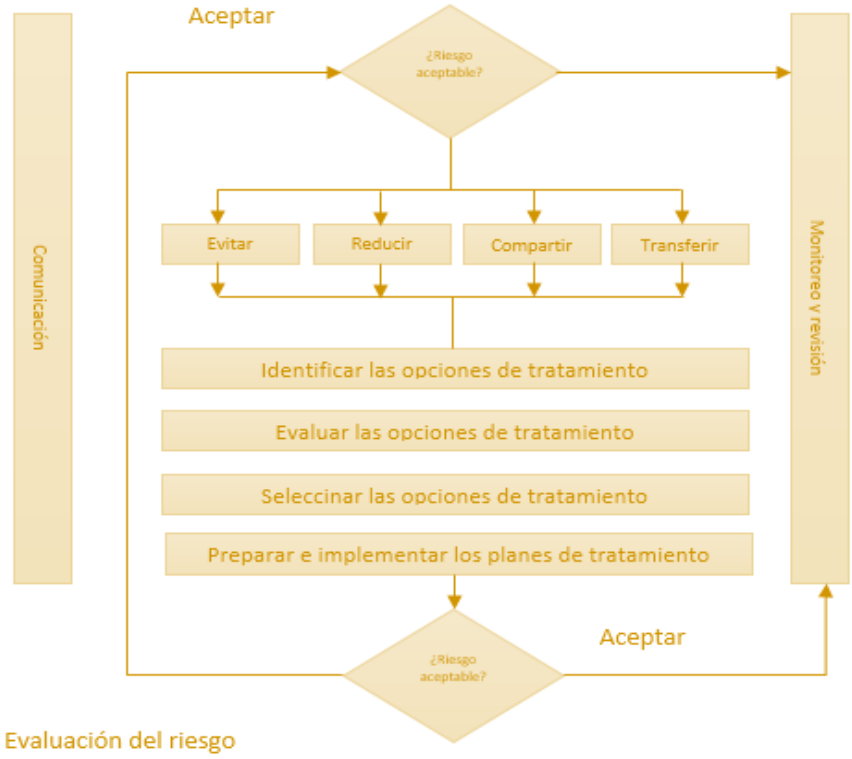
Fuente: Propia (2024)

4.5 Tratamiento de datos

El riesgo deseado es el nivel del riesgo que la institución espera alcanzar, a través de la implementación de planes de tratamiento que mitiguen el riesgo residual valorado. El proceso para el tratamiento del riesgo incluye las siguientes etapas:

- Identificar las opciones de tratamiento.
- Evaluar las opciones de tratamiento.
- Seleccionar las opciones de tratamiento.
- Preparar e implementar los planes de tratamiento.

Figura 11. Proceso del tratamiento del riesgo



Fuente: Propia (2024)

4.5.1 Identificación de las opciones de tratamiento

Este paso consiste en identificar los planes de tratamiento más adecuados para la institución. Esto implica equilibrar los costos y los esfuerzos para su implementación, así como los beneficios finales.

Los planes de tratamiento tienen como fin la mitigación de los riesgos enfocándose bien sea en la reducción de la probabilidad o del impacto. Las siguientes son las descripciones de las opciones de tratamiento del riesgo:

- Evitar el riesgo, tomar las medidas encaminadas a prevenir su materialización. Es siempre la primera alternativa a considerar, se logra cuando al interior de los procesos se generan cambios sustanciales por mejoramiento, rediseño o eliminación, resultado de unos adecuados controles y acciones emprendidas.

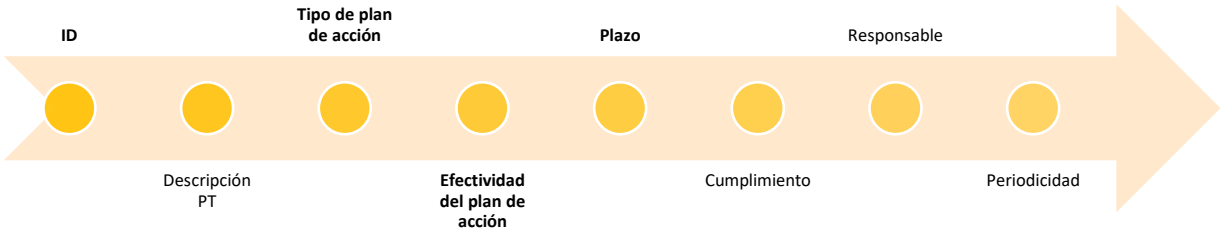
- Reducir el riesgo, implica tomar medidas encaminadas a disminuir tanto la probabilidad (medidas de prevención), como el impacto (medidas de protección). La reducción del riesgo es probablemente el método más sencillo y económico para superar las debilidades antes de aplicar medidas más costosas y difíciles.

- Compartir o transferir el riesgo, reduce su efecto a través del traspaso de las pérdidas a otras organizaciones, como en el caso de los contratos de seguros o a través de otros medios que permiten distribuir una porción del riesgo con otra entidad, como en los contratos a riesgo compartido.

- Aceptar un riesgo, luego de que el riesgo ha sido reducido o transferido puede quedar un riesgo residual que se mantiene, en este caso, el gerente del proceso simplemente acepta la pérdida residual probable y elabora planes de contingencia para su manejo (DAFP, 2011).

A continuación, se presentan los pasos para definir los planes de tratamiento:

Figura 12. Elementos de definición de planes de tratamiento



Fuente: Propia (2024)

- **ID del plan de tratamiento:** Es un identificador único del plan de tratamiento, ej: PT001
- **Descripción PT:** Descripción del plan de tratamiento o las actividades que se van a realizar para mitigar el riesgo.
- **Tipo:** Se debe indicar si es un plan correctivo, preventivo o ambos.
- **Efectividad del plan de acción:** Que tan efectivo es el control si es fuerte, muy alta, alta.
- **Plazo:** Se debe indicar si es un plan a corto, mediano o largo plazo.
- **Cumplimiento:** Se debe justificar por qué no se ha dado cumplimiento.
- **Responsable:** Cargo responsable de llevar a cabo el plan de tratamiento.
- **Periodicidad**: Cada cuanto se ejecuta el control.

Los Planes de Tratamiento de Riesgos de seguridad se deben plantear en términos de los controles de la Norma ISO/IEC 27001 y del manual de buenas prácticas de la norma ISO/IEC 27002.

4.5.2 Evaluación de los planes de tratamiento

Como se mencionó anteriormente la evaluación de los planes de tratamiento debe ser consistente con el proceso contemplado en el numeral "5.4.2. Evaluación de los controles existentes". Durante la evaluación de los planes de tratamiento, también se recomienda tener en cuenta otros aspectos importantes, como:

- **Viabilidad Jurídica:** Velar por que los controles que se van a implantar no están en contra de la normatividad vigente.
- **Viabilidad Técnica e Institucional**: Establecer claramente si la institución está en capacidad de implantar y sostener a largo plazo nuevas tecnologías u otros mecanismos necesarios para ejecutar el control.
- **Análisis de costo/beneficio:** Esto implica sopesar el costo directo o indirecto con el beneficio que genera el plan de tratamiento analizado. Se ha de considerar el costo inicial del diseño e implementación del plan de tratamiento (procesos, personal, tecnología), así como el costo de mantenerlo de forma continua.

4.5.3 Selección de las opciones de tratamiento

La selección de las opciones más adecuadas para el tratamiento del riesgo implica equilibrar los costos y los esfuerzos de la implementación frente a los beneficios derivados con respecto a los requisitos legales y reglamentarios. En las decisiones también se deberían considerar los riesgos que pueden ameritar el tratamiento que no es justificable en términos económicos, por ejemplo, los riesgos graves (consecuencia negativa alta) pero raros (baja probabilidad).

Al seleccionar las opciones para tratar el riesgo, la organización debería considerar las percepciones de las partes involucradas, y las vías más adecuadas para comunicarse con ellos. Cuando las opciones para tratar el riesgo puedan tener impacto en otras partes de la organización u otras partes involucradas, estas observaciones se deberían incluir en la decisión.

El plan de tratamiento debería identificar claramente el orden de prioridad en el cual se deberían implementar los tratamientos individuales para el riesgo. El tratamiento también puede introducir riesgos secundarios que es necesario valorar, tratar, monitorear y revisar. Estos riesgos secundarios se deberían incorporar en el mismo plan de tratamiento definido para el riesgo original y no se deberían tratar como riesgos nuevos.

4.5.4 Implementación de los planes de tratamiento

El propósito de los planes para el tratamiento del riesgo es documentar la forma en que se van a implementar las opciones de tratamiento seleccionadas. La información suministrada en los planes de tratamiento debería incluir:

- Razones para la selección de las opciones de tratamiento, que incluyan los beneficios que se espera obtener.
- Los responsables de aprobar el plan y los responsables de implementarlo.
- Acciones propuestas.
- Requisitos de recursos, incluyendo las contingencias.
- Medidas y restricciones de desempeño.
- Requisitos de monitoreo y reporte.
- Tiempo y cronograma.

Los planes de tratamiento se deberían integrar con los procesos de gestión de la organización y se deberían discutir con las partes involucradas pertinentes.

Los encargados de tomar las decisiones y otras partes involucradas deberían conocer la naturaleza y la extensión del riesgo residual después del tratamiento del riesgo.

4.5.5 Análisis y valoración del riesgo deseado

En este punto es necesario estimar si los planes de tratamiento o controles propuestos reducen la probabilidad o el impacto del riesgo residual para alcanzar el riesgo deseado, se deben tener en cuenta los criterios de la tabla de afectación del control.

4.6 Monitoreo y Revisión

El monitoreo y revisión debe asegurar que los planes de tratamiento establecidos se estén llevando a cabo. Adicionalmente se debe evaluar la eficiencia en su implementación, y efectuar revisiones sobre la marcha para evidenciar todas aquellas situaciones o factores que pueden estar influyendo en la aplicación de las acciones preventivas.

El monitoreo debe ser continuo y periódico; sin embargo, se debe realizar también cuando ocurren cambios en los procesos del SGC o cambios en los activos de información que apoyan estos procesos.

El monitoreo pretende:

- Revisar el análisis, evaluación y tratamiento del riesgo para determinar cambios en los niveles de riesgo o en la eficacia de los controles establecidos.
- Realizar el análisis, evaluación y tratamiento del riesgo en el momento de identificar nuevos activos de información asociados a los procesos de la institución.

El monitoreo debe estar a cargo de:

- Los responsables de los procesos: Encargados de realizar las acciones asociadas a los controles establecidos para cada uno de los riesgos identificados para su proceso.
- El líder del proceso de Gestión de mejora, debe ser el encargado de:

    - Realizar el seguimiento a los riesgos que a nivel institucional han sido consolidados.
    - Analizar el diseño e idoneidad de los controles, determinando si son o no adecuados para prevenir o mitigar los riesgos en los procesos.
    - Comunicar y presentar luego del seguimiento y evaluación sus resultados y propuestas de mejoramiento y tratamiento a las situaciones detectadas.

5 PLANES DE TRATAMIENTO DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN

Tabla 15. Planes de tratamiento de riesgos de seguridad y de la información

ID	Planes de tratamiento	Tipo de plan de acción	Efectividad del plan de acción	Plazo	Cumplimiento	Responsable	Periodicidad
PT001	Realizar la verificación de cumplimiento de la política para la conservación de registros de auditoría de los usuarios con perfil de administrador en sistemas de información y plataformas tecnológicas críticas del SGC	Preventivo / Detectivo /Correctivo	Fuerte	Mediano plazo	No se ha contratado un auditor externo ya que se utiliza la herramienta SIEM como herramienta de recolección, normalización, correlación y alertamiento de registros (logs) de auditoría en diferentes fuentes de información. Se tienen actualmente 55 casos de uso que no solo validan el comportamiento de usuarios administradores sino también otro tipo de comportamiento asociado a las diferentes fuentes de información.	Coordinador de sistemas de Información Líder de plataforma Tecnológica	Anual
PT002	Realizar un muestreo para verificar que se esté aplicando la política de bloqueo de pantalla después de los 5 minutos de inactividad.	Detectivo	Fuerte	Corto plazo	A través de la validación de la GPO respectiva se puede comprobar que dicha política se encuentra desplegada.	Administrador de servidores y directorio activo	Anual
PT003	Actualizar una política de acceso remoto y un procedimiento mediante el cual se autorice o se niegue la solicitud de acceso remoto por parte de funcionarios a sistemas de información o plataformas tecnológicas del SGC	Preventivo	Fuerte	Corto plazo	Se está trabajando en el diseño del procedimiento y la política	Coordinador de sistemas de Información Administrador de servidores y directorio activo	Anual
PT004	Actualizar políticas de backups para sistemas de información y plataformas críticas del SGC, que incluyan backups completos e incrementales.	Correctivo	Fuerte	Corto plazo	Las políticas en Networker se trabajan con full e incremental	Líder de plataforma Tecnológica Administrador de backup	Anual
PT005	Actualizar políticas de restauración periódica de backups aleatorios para garantizar que los backups se están haciendo correctamente.	Preventivo	Fuerte	Corto plazo	Se realizan periódicamente pruebas de restauración tanto de NAS como SAN.	Líder de plataforma Tecnológica Administrador de backup	Anual

ID	Planes de tratamiento	Tipo de plan de acción	Efectividad del plan de acción	Plazo	Cumplimiento	Responsable	Periodicidad
PT006	Verificar que los centros de cómputo del SGC cumplen con las mejores prácticas en cuanto al mantenimiento y administración de este tipo de instalaciones	Preventivo / Detectivo / Correctivo	Fuerte	Corto plazo	Depende el presupuesto del año 2024	Líder de plataforma Tecnológica	Anual
PT007	Adquisición de una solución tipo DLP para gestionar medios removibles de acuerdo al esquema de clasificación de la información.	Preventivo	Fuerte	Mediano plazo	Depende el presupuesto del año 2024	Líder de seguridad Coordinadora de plataforma Tecnológica	2024
PT008	Actualizar procedimientos operativos para la administración adecuada de la red	Preventivo	Fuerte	Corto plazo	Se tienen topologías de la red y plan de direccionamiento ipv4	Administrador redes	Anual
PT009	Crear y oficializar el procedimiento de gestión de incidentes por parte de la DGI	Preventivo	Fuerte	Corto plazo	Se encuentra en revisión el procedimiento de gestión de incidentes	Líder de seguridad	2024
PT010	Actualizar la política para el acceso de dispositivos móviles en redes externas (antivirus, sistema operativo y navegadores actualizados)	Preventivo	Fuerte	Corto plazo	Se está en proceso de implementación de NAC en toda la entidad para implementar, entre otras cosas, las políticas BYOD y de control de acceso (LAN y remoto)	Líder de seguridad	Anual
PT011	Actualizar la política de uso aceptable de activos de información.	Preventivo	Fuerte	Corto plazo	Está en proceso de oficialización	Líder de seguridad	Anual
PT012	Cifrar bases de datos y carpetas compartidas a nivel institucional	Preventivo	Fuerte	Mediano plazo	Depende el presupuesto del año 2024	Líder de plataforma Tecnológica Líder de seguridad Coordinadora de plataforma Tecnológica	2024

ID	Planes de tratamiento	Tipo de plan de acción	Efectividad del plan de acción	Plazo	Cumplimiento	Responsable	Periodicidad
PT013	Actualizar un plan para implementar las políticas de escritorio limpio y pantalla limpia	Preventivo	Fuerte	Corto plazo	En desarrollo	Administrador de servidores y directorio activo	Anual
PT014	Sincronizar toda la plataforma tecnológica con el servidor NTP de la red sismológica, que es un servidor especializado de hora	Preventivo	Fuerte	Corto plazo	Todos los productos/servicios que administra y/o controla el equipo de seguridad de la información se encuentran sincronizados con los servidores NTP del SGC	Administrador de servidores y directorio activo	Anual
PT015	Adquirir e implementar una solución que permita hacer el monitoreo de disponibilidad de los servicios internos	Preventivo / Detectivo / Correctivo	Fuerte	Largo plazo	Depende el presupuesto del año 2024	Líder de plataforma Tecnológica	2024
PT016	Actualizar políticas de seguridad de la información para la relación con proveedores o terceros	Preventivo	Fuerte	Corto plazo	Está en proceso de oficialización	Líder de plataforma Tecnológica	Anual
PT017	Se tiene un proyecto para llevar a cabo la actualización del plan de recuperación de desastres tecnológicos, el cual incluirá el diseño y la ejecución de las pruebas ante la falla de la plataforma tecnológica.	Preventivo	Fuerte	Mediano plazo	Se desarrolló un plan de pruebas con algunos sistemas de apoyo	Líder de seguridad Líder de plataforma Tecnológica	Anual
PT018	El proyecto de hiperconvergencia permitirá tener contingencia de la plataforma critica en el Datacenter Alterno a nivel procesamiento, y contingencia de la red sismológica en el centro alterno de monitoreo ubicado en pasto.	Preventivo	Fuerte	Mediano plazo	Mantener el Data center alterno en Pasto	Líder de plataforma Tecnológica	Anual
PT019	Garantizar la revisión del SGSI por la dirección a través de la revisión y aprobación de los planes anuales.	Preventivo	Fuerte	Corto plazo	Planes anuales de seguridad de la información y plan de tratamiento de riesgos	Líder de seguridad	Anual
PT020	Garantizar el cumplimiento de la política para la conservación de registros de auditoría de usuarios	Preventivo / Detectivo	Fuerte	Mediano plazo	Realizar una auditoría interna para verificar el cumplimiento de la política de conservación de registros de auditoría de administradores en	Líder de Seguridad	Anual

ID	Planes de tratamiento	Tipo de plan de acción	Efectividad del plan de acción	Plazo	Cumplimiento	Responsable	Periodicidad
	con perfil de administrador en sistemas críticos mediante la implementación y monitoreo efectivo de casos de uso en el SIEM.	/ Correctivo			sistemas críticos del Sistema de Gestión de la Seguridad de la Información (SGC). Utilizar la herramienta SIEM para: Recolectar, normalizar y correlacionar registros (logs) de auditoría de diversas fuentes de información. Desarrollar casos de uso en el SIEM para validar comportamientos de usuarios administradores y otros tipos de comportamientos asociados a diferentes fuentes de información.		
PT021	Actualizar y mantener un sistema eficaz de Prevención de Intrusiones (IPS) utilizando McAfee para detectar y prevenir actividades maliciosas en la red y sistemas críticos del entorno de tecnología de la información.	Preventivo / Detectivo	Alta	Corto plazo y Continuo	Actualizar el IPS McAfee para monitorear el tráfico de red y prevenir intrusiones, ataques y comportamientos maliciosos en tiempo real. Configurar las reglas de detección y respuesta para identificar patrones de amenazas conocidas y desconocidas. Realizar actualizaciones periódicas de firmas y parches para mantener el IPS actualizado contra las últimas amenazas. Supervisar de manera continua la efectividad del IPS y ajustar las reglas de detección según sea necesario para mejorar la precisión y eficacia.	Equipo de Plataforma Tecnológica	Mensual
PT022	Actualizar y operar eficazmente la solución de antivirus para mejorar la detección, investigación y respuesta a amenazas avanzadas en el entorno de seguridad	Detectivo / Correctivo	Muy alta	Corto plazo	Configurar y personalizar las reglas y políticas de detección para alinearlas con las necesidades específicas de seguridad y los indicadores de compromiso (IOC) relevantes.	Equipo de Plataforma Tecnológica	Continuo
PT023	Desarrollar actividades de gestión de vulnerabilidades para identificar, evaluar y mitigar las vulnerabilidades en los sistemas y activos del SGC.	Preventivo / Correctivo	Alta	Mediano plazo	Utilizar herramientas de escaneo de vulnerabilidades para identificar y catalogar las vulnerabilidades en la red, aplicaciones y sistemas.	Equipo de Plataforma Tecnológica	Continuo

ID	Planes de tratamiento	Tipo de plan de acción	Efectividad del plan de acción	Plazo	Cumplimiento	Responsable	Periodicidad
					Establecer un proceso de evaluación de riesgos para priorizar las vulnerabilidades en función de su gravedad, impacto potencial y exposición. Implementar parches y soluciones temporales para mitigar las vulnerabilidades críticas de forma proactiva. Realizar análisis de causa raíz para abordar problemas subyacentes que puedan dar lugar a vulnerabilidades recurrentes.		

Fuente: Propia (2024)

6 MEDICIÓN

Se han ejecutado 32 de los 55 planes de tratamiento de riesgos en las vigencias pasadas, que equivale al 58,18% de los planes de tratamiento de riesgos, esto quiere decir que se ha realizado un importante progreso en temas de mitigación de riesgos en seguridad digital, sin embargo, hay que tener en cuenta que los controles implementados requieren de un afinamiento que toma más tiempo en su implementación y adicionalmente, los controles no implementados o sin actualizar requieren de presupuesto para su ejecución y mantenimiento.

7 SEGUIMIENTO Y CONTROL

El seguimiento y monitoreo a la ejecución de las actividades establecidas para los planes/proyectos del Plan de Tratamiento de Riesgos Seguridad y Privacidad de la Información, se realizará a través del Plan de Acción y de las herramientas definidas en el Sistema de Gestión Institucional del SGC, se determinará la periodicidad en Cronograma deSeguimiento a los Planes definidos en el Decreto 612 de 2018.