SERVICIO GEOLÓGICO COLOMBIANO

PLAN DE TRATAMIENTO DE RIESGOS DESEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

2022

TABLA DE CONTENIDO

LISTA DE ILUSTRACIONES

LISTA DE TABLAS

1. INTRODUCCIÓN

La información que se maneja en el Servicio Geológico Colombiano - SGC, es trascendental para el cumplimiento de los 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 en caso de que un incidente se materialice. 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 del fortalecimiento de su misión institucional, realiza actividades enmarcadas en procesos estratégicos, misionales y de apoyo, los cuales puede afectarse por la presencia de riesgos de seguridad y privacidad dela información. El presente documento establece la manera en la que se van a tipificar los riesgos identificados y su tratamiento de acuerdo a la metodología de gestión de riesgos diseñada y ajustada para el SGC, en el marco del cumplimiento de las directrices y/o recomendaciones de la metodología de gestión de riesgos del Departamento Administrativo de la Función Pública – DAFP (versión 5), ISO 31000:2018, del plan estratégico institucional, los lineamientos de la Arquitectura empresarial, el Sistema Integrado de Gestión de la Seguridad de la Información, Protección de Datos Personales y Continuidad del Negocio (SIGSI-PDP-CN) el Modelo de Seguridad y Privacidad de la Información y el cumplimiento de la Política de Gobierno Digital.

2. OBJETIVO DEL DOCUMENTO

Establecer los lineamientos para un proceso adecuado de gestión de riesgos de seguridady privacidad 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 DEL DOCUMENTO

El plan de tratamiento de riesgos contempla la identificación y valoración de activos de información y contenedores en el SGC, teniendo en cuenta aspectos que van desde el manejo de documentos en medio físico como el proceso de almacenaje y recuperación, hasta los sistemas de información con los que cuenta la entidad o sistemas externos a los que esté obligada a reportar información, pasando por aspectos tan importantes como la forma de almacenamiento de los datos digitales, modelos de respaldo de información y

planes de contingencia o de continuidad del negocio, incluyendo además los sistemas físicos de protección y accesibilidad a sitios o áreas restringidas.

4. METODOLOGÍA DE GESTIÓN INTEGRADA DE RIESGOS DE SEGURIDADY PRIVACIDAD DE LA INFORMACIÓN

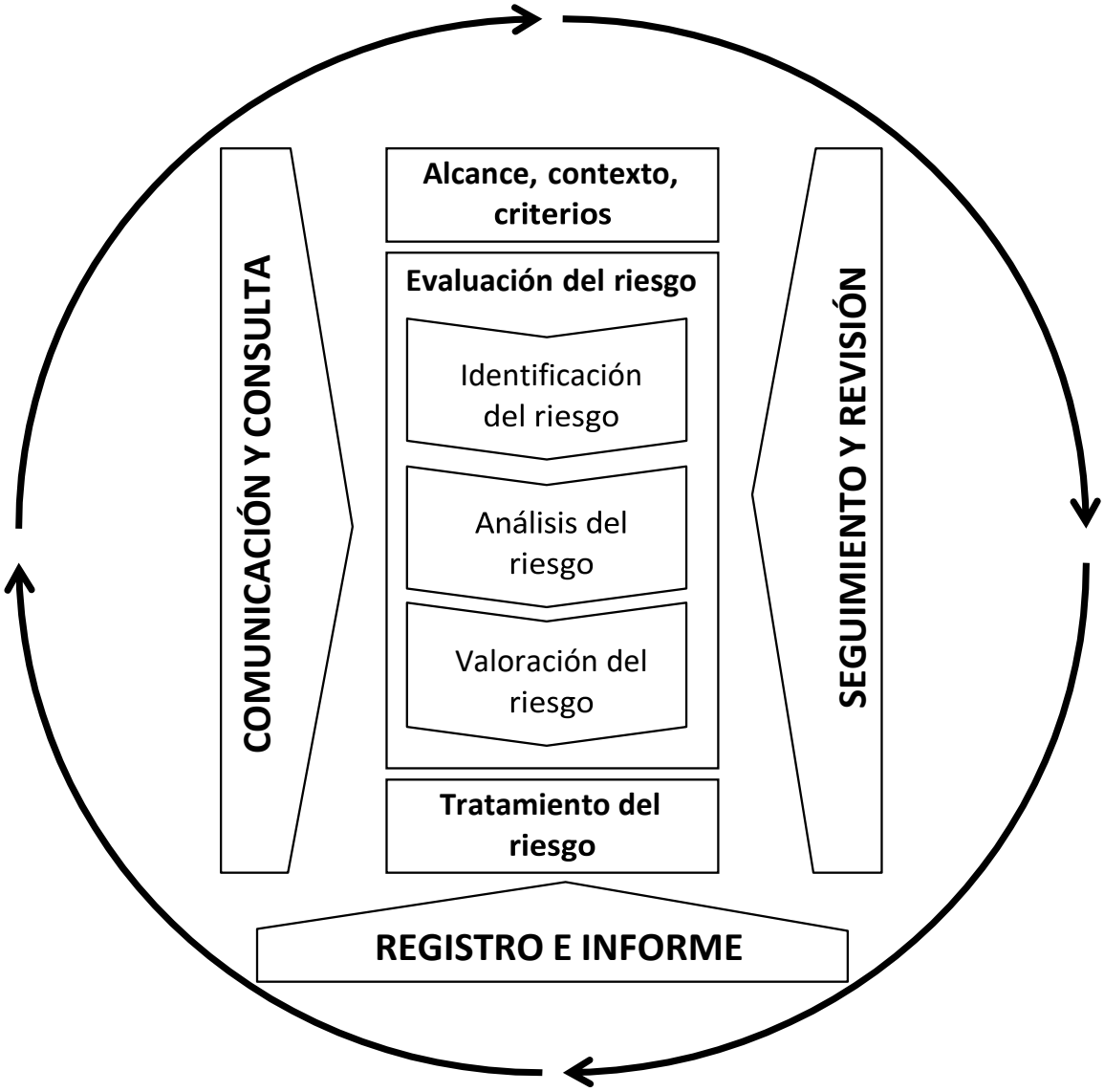
La metodología de gestión integrada es una adaptación y personalización a las necesidades del SGC en la cual se integran las recomendaciones de la metodología de gestión de riesgos del Departamento Administrativo de la Función Pública – DAFP (versión 5) así comotambién lo dispuesto en ISO 31000:2018.

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 y 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 encaso de suspensión del procesamiento” (Seguridad de la Información TGE, 2016).

La Norma ISO 31000 proporciona una serie de recomendaciones planteadas como principios o directrices para la gestión de cualquier tipo de riesgo (Icontec, 2018). El SGC, sigue sus recomendaciones y directrices para realizar una eficaz y eficiente gestión de riesgos de seguridad de la información en los procesos misionales. A continuación, se presenta el proceso para la gestión del riesgo de la norma ISO 31000:2018:

Ilustración 1. Proceso para la Gestión de Riesgos (fuente: ISO 31000:2018)



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:** el propósito de la comunicación y consulta es asistir a las partes interesadas pertinentes a comprender el riesgo, las bases con las que se toman decisiones y las razones por las que son necesarias acciones específicas. La comunicación busca promover la toma de conciencia y la comprensión del riesgo, mientras que la consulta implica obtener retroalimentación e información para apoyar la toma de decisiones (Icontec, 2018)

- **Alcance, contexto y criterios:** como el proceso de la gestión del riesgo puede aplicarse a niveles distintos (por ejemplo: estratégico, operacional, de programa, de proyecto o de otras actividades), es importante tener claro el alcance considerado, los objetivos pertinentes a considerar y su alineamiento con los objetivos de la organización (Icontec, 2018), 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.

- **Evaluación del riesgo:** la evaluación del riesgo es el proceso de identificación del riesgo, análisis del riesgo y valoración del riesgo (Icontec, 2018).

- **Identificación del riesgo** El propósito de la identificación del riesgo es encontrar, reconocer y describir los riesgos que pueden ayudar o impedir a una organización lograr sus objetivos. Para la identificación de los riesgos es importante contar con información pertinente, apropiada y actualizada (Icontec, 2018).

- **Análisis del riesgo:** el propósito del análisis del riesgo es comprender la naturalezadel riesgo y sus características incluyendo, cuando sea apropiado, el nivel de riesgo.El análisis del riesgo implica una consideración detallada de incertidumbres, fuentesde riesgo, consecuencias, probabilidades, eventos, escenarios, controles y sueficacia (Icontec, 2018).

- **Valoración del riesgo:** el propósito de la valoración de riesgo es apoyar la toma de decisiones. La valoración del riesgo implica comparar los resultados del análisis del riesgo con los criterios del riesgo establecidos para determinar cuándo se requiere una acción adicional (Icontec, 2018).

- **Tratamiento de Riesgos:** el propósito del tratamiento del riesgo es seleccionar e implementar opciones para abordar el riesgo (Icontec, 2018).

- **Seguimiento y Revisión:** el propósito del seguimiento y la revisión es asegurar y mejorar la calidad y la eficacia del diseño, la implementación y los resultados del proceso (Icontec, 2018).

- **Registro e informe:** el proceso de la gestión del riesgo y sus resultados se deberían documentar e informar a través de los mecanismos apropiados. El registro e informe pretenden:
    - Comunicar las actividades de la gestión del riesgo y sus resultados a lo largo del SGC.
    - Proporcionar información para la toma de decisiones

- Mejorar las actividades de la gestión del riesgo
- Asistir la interacción con las partes interesadas, incluyendo a las personas que tienen la responsabilidad y la obligación de rendir cuentas de las actividades de la gestión del riesgo.

Para el tratamiento de riesgo de seguridad y privacidad de la información el SGC, definió las siguientes fases, con sus actividades:

Ilustración 2. Ciclo PHVA de la gestión de riesgos (fuente: elaboración propia)

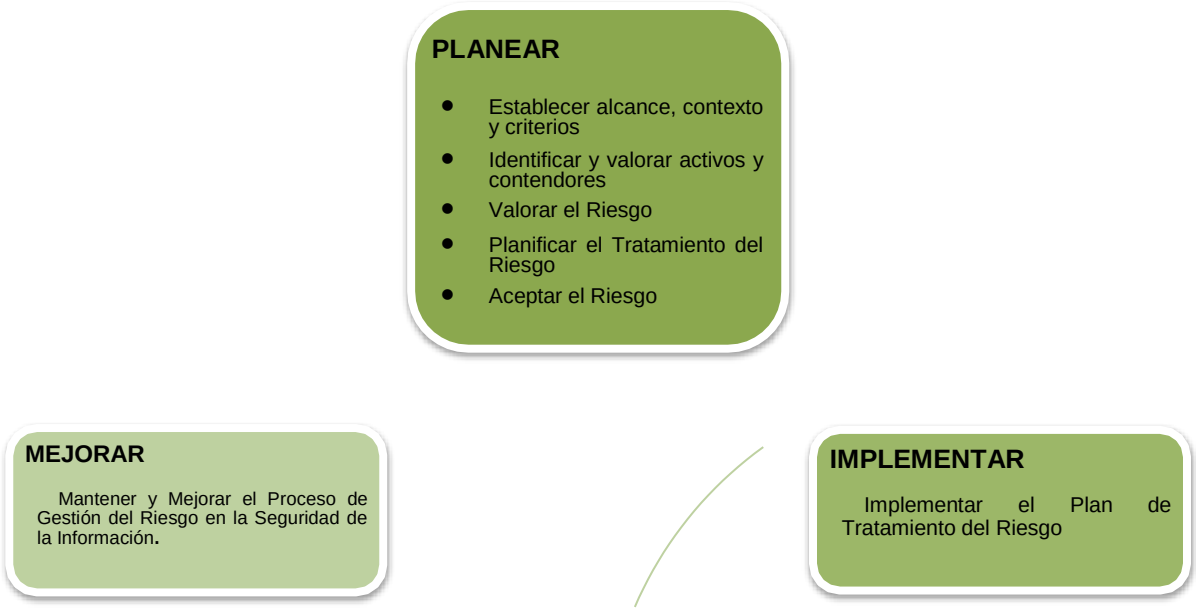


Ilustración 3. Pasó a [illegible]álisis de riesgos (fuente: elaboración propia)

El paso a paso para llevar a cabo el análisis de riesgos de seguridad de la información sepresenta a continuación:

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.

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 siguientes factores:

Tabla 1. Factores Externos (fuente: elaboración propia)

DESCRIPCIÓN DE FACTORES	
CONTEXTO EXTERNO	• **Sector en el que opera:** Características, lineamientos y directrices delsector minas y energía. • **Político:** Cambios de gobierno, legislación, políticas públicas,regulación. • **Económico:** Patrimonio económico.

DESCRIPCIÓN DE FACTORES	
	• **Social y cultural:** Responsabilidad social. • **Tecnológico:** Avances en tecnología, acceso a sistemas de informaciónexternos, intercambio de información con otras entidades. • **Ambiental:** Emisiones y residuos, catástrofes naturales, desarrollosostenible. • **Comunicación Externa:** Mecanismos utilizados para que los usuarios o ciudadanos entren en contacto con la entidad.

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 siguientes factores:

Tabla 2. Factores Internos (fuente: elaboración propia)

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 informacióngeocientífica. • **Comunicación interna:** Canales utilizados para la comunicación interna.

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 (fuente: elaboración propia)

DESCRIPCIÓN DE FACTORES	
CONTEXTO DEL PROCESO	• **Diseño del proceso:** Descripción de detallada de procesos. • **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.

4.2. ACTIVOS DE 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 perdida de la información que contienen.

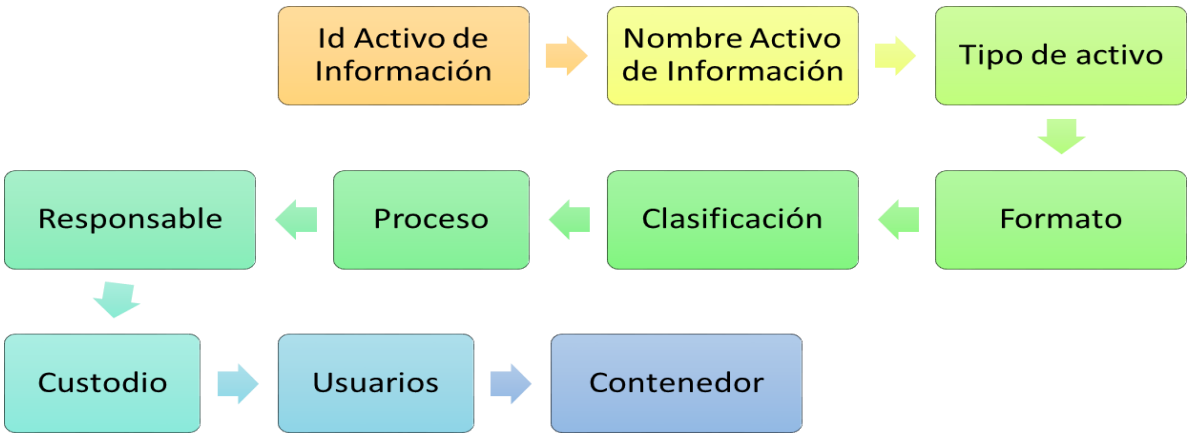
De aquí la importancia de la identificación y valoración de los activos de información, ya que el contenedor heredara la valoración de los impactos más altos de los activos que contiene, y los riesgos de seguridad de la información estarán asociados a dichos contenedores.

4.2.1. Identificación de activos de información

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 de la información levantada en las entrevistas con cada proceso o áreas.

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

Ilustración 4. Proceso de identificación de activos de información y contenedores (fuente: elaboraciónpropia)



Notas:

- Para la valoración de los activos de información se debe tener en cuenta los siguientes requisitos:
  - Deben participar los dueños de los activos de información.
  - Las escalas para valorar los impactos sobre cada principio se están definiendo en conjunto entre el Servicio Geológico Colombiano.
  - Los resultados deben ser aprobados por los dueños 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 presentados 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.

Nota:

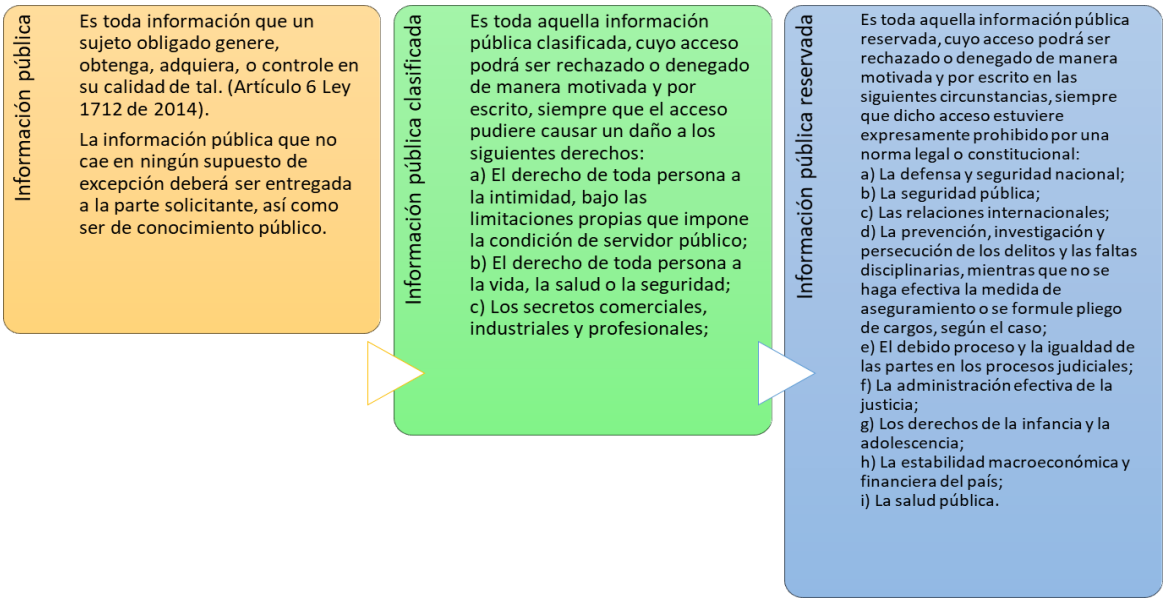
A continuación, se realizan algunas aclaraciones sobre los campos que componen el proceso de identificación de activos de información y contenedores:

- **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 finde 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 con la Ley 1712 de 2014 y la Ley 1581 de 2012.
- **Proceso:** Se debe establecer a que proceso del SGC, pertenece el activo de información.

- **Responsable:** 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 publica).
  - Verificar que se implementen los controles de acuerdo con el 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 este bajo su cargo.
- **Custodio:** Es el proceso, equipo de trabajo, o cargo, designado por los propietarioso 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.
- **Contenedor:** Cualquier medio por el que se reciba, almacene, procese o transmita dicho activo de información, como: Computadores de escritorio, portátiles, USB, Discos Duros, Correo electrónico, Dropbox, Google Drive, One Drive, Aplicación, Smartphone, Personas, Contratistas, carpetas físicas, archivo físico.

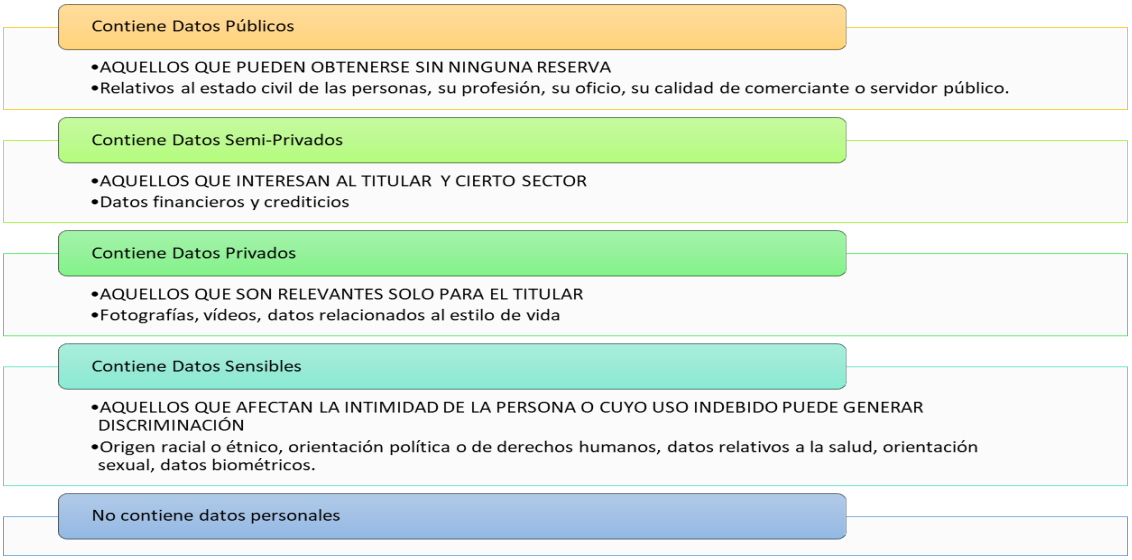
Ley 1712 de 2014

Ilustración 5. Clasificación según Ley 1712 (fuente: elaboración propia)



Ley 1581 de 2012

Ilustración 6. Clasificación según Ley 1581 (fuente: elaboración propia)



4.2.2. Valoración de los activos de información

Los activos de información identificados deben ser valorados según los principios básicos de la seguridad de la información: confidencialidad, integridad y disponibilidad.

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

Ilustración 7. Valoración de activos de información (fuente: elaboración propia)

Para cada principio se tendrá en cuenta los siguientes impactos:

- Impacto Social
- Impacto Legal
- Impacto Reputacional
- Impacto Conocimiento o Investigación

Los cuales se puedan llegar a presentar en el SGC, por la ausencia de dicho principioen cada activo de información valorado, como se muestra a continuación:

Ilustración 8. Evaluación de principios de seguridad de la información (fuente: elaboración propia)

Confidencialidad				
Social	Legal	Reputacional	Conocimiento o Investigación	**Impacto mayor**

Integridad				
Social	Legal	Reputacional	Conocimiento o Investigación	**Impacto mayor**

Disponibilidad				
Social	Legal	Reputacional	Conocimiento o Investigación	**Impacto mayor**

Impacto Social

Nivel de afectación en la toma de decisiones de carácter social, es decir aquella información que pueda afectar la toma de decisiones por la pérdida de confidencialidad, integridad o disponibilidad.

Tabla 4. Escala de Impacto Social (fuente: elaboración propia)

Impacto	Impacto Social	Nivel
Insignificante	La información no afecta la toma de decisiones.	1
Menor	La información es deseable tenerla para la toma de decisiones, perono es fundamental en dicha actividad.	2
Moderado	La información hace parte de la toma de decisiones, pero se puedetomar la decisión sin dicha información.	3
Mayor	La información es necesaria para la toma de decisiones.	4
Catastrófico	La información es fundamental para la toma de decisiones.	5

Impacto Legal

Afectación legal o jurídica causada por una pérdida de confidencialidad, integridad o

disponibilidad de un activo de información.

Tabla 5. Escala de Impacto Legal (fuente: elaboración propia)

Impacto	Impacto Legal	Nivel
Insignificante	No tiene ningún tipo de impacto legal.	1
Menor	Conduciría a una falta disciplinaria leve sobre algún funcionario, pero no segeneran consecuencias para el SGC.	2
Moderado	Conduciría a una falta disciplinaria de tipo grave o gravísima sobre algúnfuncionario, pero no se generan consecuencias para el SGC.	3
Mayor	Genera consecuencias de carácter penal sobre algún funcionario, pero nose generan consecuencias para el SGC.	4
Catastrófico	Eventualmente tiene consecuencias económicas o fiscales para el SGC,derivadas de reparaciones económicas.	5

Impacto Reputacional

Afectación del buen nombre que puede experimentar el SGC ante una pérdida de confidencialidad, integridad o disponibilidad de un activo de información.

Tabla 6. Escala de Impacto Reputacional (fuente: elaboración propia)

Impacto	Impacto Reputacional	Nivel
Insignificante	El incidente de seguridad no genera ninguna afectación a la reputación delSGC.	1
Menor	El incidente de seguridad es conocido a nivel interno, en un área del SGC.	2
Moderado	El incidente de seguridad es conocido a nivel interno, en todo el SGC.	3
Mayor	El incidente de seguridad es conocido a nivel nacional.	4
Catastrófico	El incidente de seguridad es conocido a nivel nacional e internacional.	5

Impacto de Conocimiento o Investigación

Afectación que puede experimentar el SGC ante una pérdida de confidencialidad, integridad o disponibilidad de un activo de información del SGC.

Tabla 7. Escala de Impacto de Conocimiento o investigación (fuente: elaboración propia)

Impacto	Conocimiento o investigación	Nivel
Insignificante	Pérdida o revelación de información que no afecta el conocimiento oinvestigación.	1
Menor	• La información se puede recuperar muy fácilmente o, • Se afecta una investigación científica en caso de revelación noautorizada.	2
Moderado	• La mayor parte de la información se puede reconstruir fácilmente o, • Se genera un conflicto con otro instituto o universidad, por unainvestigación científica en caso de revelación no autorizada.	3
Mayor	• La información es de difícil recuperación o reconstrucción o, • Se genera falsa alarma por interpretación errada de la informaciónen caso de revelación no autorizada.	4
Catastrófico	• La información no se puede recuperar ni reconstruir o, • Se favorece artificialmente un proveedor en licitaciones o endecisiones de inversión en caso de revelación no autorizada.	5

4.3. EVALUACIÓN DEL 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

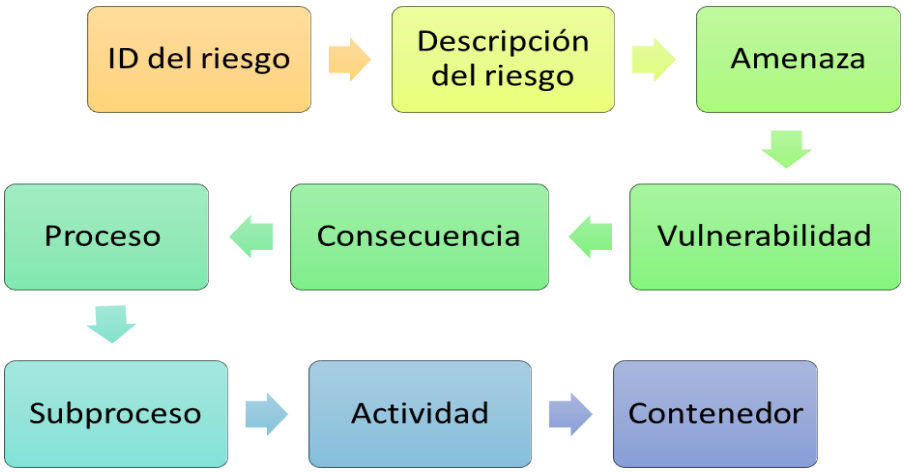
La identificación del riesgo consiste en establecer las fuentes de riesgo, los eventos, sus causas y sus consecuencias. Para el análisis se pueden involucrar datos históricos, análisis teóricos, opiniones informadas y expertas y las necesidades de las partes involucradas. (NTC ISO31000, Numeral 2.15).

Durante la identificación del riesgo se debe tener en cuenta el contexto organizacional, según lo establecido en el numeral 3.1 Identificación del Contexto: Contexto externo, contexto interno y el contexto del proceso.

Adicionalmente, se recomienda tener en cuenta durante el análisis 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 disposicionesa las que está obligada y comprometida a cumplir.

A continuación, se presenta el proceso a seguir:

Ilustración 9. Proceso de identificación del riesgo (fuente: elaboración propia)



4.3.2. Análisis del riesgo

Este paso tiene como fin establecer la probabilidad de ocurrencia y el nivel de impacto, con el fin de estimar el nivel del riesgo inherente.

Determinar la probabilidad

Es la posibilidad de ocurrencia del riesgo. A continuación, se relacionan los criterios para evaluar las probabilidades de ocurrencia de los riesgos identificados.

Tabla 9. Escala de probabilidad (fuente: elaboración propia)

TABLA DE PROBABILIDAD			
NIVEL	**DESCRIPTOR**	**DESCRIPCIÓN**	**FRECUENCIA**
1	Raro	El evento puede ocurrir sólo encircunstancias excepcionales	No se ha presentado en losúltimos 5 años
2	Improbable	El evento puede ocurrir en cualquier momento	Al menos una vez en los últimos 2 años
3	Posible	El evento podría ocurrir en algúnmomento	Al menos una vez en el últimoaño
4	Probable	El evento probablemente ocurrirá en la mayoría de las circunstancias	Al menos una vez en el últimosemestre
5	Casi seguro	Se espera que el evento ocurra en la mayoría de las circunstancias	El evento se presentó en elúltimo mes

Determinar el nivel de impacto

El impacto son las consecuencias que puede ocasionar la materialización del riesgo a la institución. Los impactos que se pretenden analizar son los que puedan causar afectaciones de tipo social, legal, reputacional, y de conocimiento o investigación.

En todo caso, teniendo en cuenta la incertidumbre que representan los riesgos, el análisis del impacto debe considerar las situaciones de mayor afectación que pueda tener la entidad.

Las escalas de los impactos contemplados para el análisis de riesgos son los mismos descritos en el numeral 4.2.2. Valoración de los activos de información.

4.3.3. Valoración del riesgo inherente

Consiste en valorar la probabilidad y el impacto del riesgo analizado, con el fin de determinar el nivel del riesgo inherente.

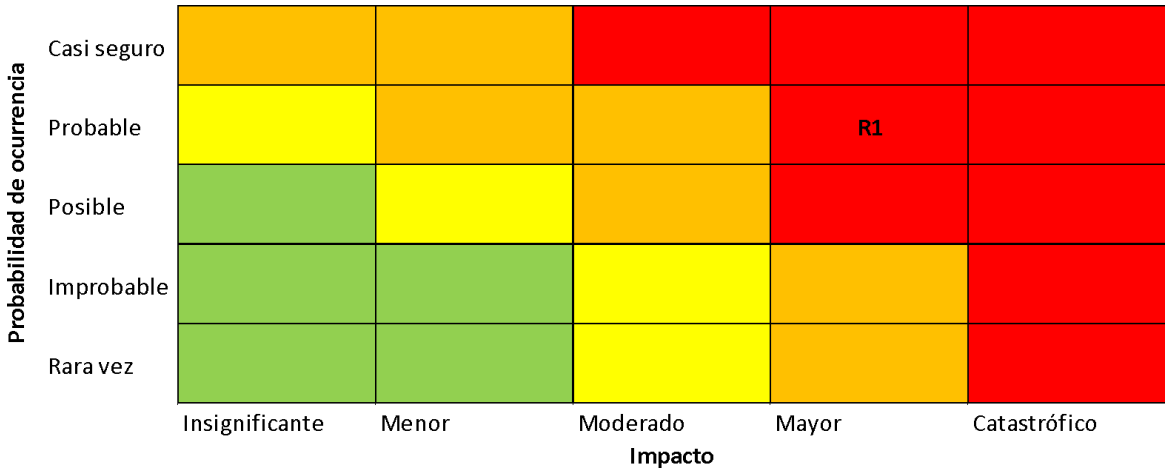
Ilustración 10. Proceso de valoración del riesgo inherente (fuente: elaboración propia)

Nota:

El impacto del riesgo inherente será el impacto mayor de los tres principios analizados (Confidencialidad, Integridad y Disponibilidad).

El nivel del riesgo resulta de cruzar la probabilidad y el impacto en el siguiente mapa.

Ilustración 11. Mapa de probabilidad por impacto (fuente: elaboración propia)



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. Por ello, se debe buscar un equilibrioentre 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).

1. PLANES DE TRATAMIENTO DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN

ID	Planes de tratamiento	Tipo de plan de acción	Peso de evaluación del plan de acción	Efectividad del plan de acción	Plazo	Cumplimiento	Responsable	Fecha en la que se ejecutó el plan
PT001	Verificar que la solución de File Activity Monitoring (FAM) con que cuenta actualmente el SGC permita el monitoreo de cualquier modificación no autorizada en activos de información críticos, de lo contrario se recomienda adquirir una solución de File Integrity Monitoring(FIM) o contratarlo como servicio.	Detectivo	100	Fuerte	Mediano plazo	La solución FAM se encuentra en proceso de renovación a través de la plataforma SECOP II (https://community.secop.gov.co/Public/Tendering/ContractNoticePhases/View?PPI=CO1.PPI.15167322&isFromPublicArea=True&isModal=False)	Andrés Oliva	Dic- 2022
PT002	Contratar una auditoria externa que realice la verificación de cumplimiento de la política para la conservación de registros de auditoria de los usuarios con perfil de administrador en sistemas de información y plataformas tecnológicas criticas del SGC	Preventivo / Detectivo / Correctivo	100	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.	Andrés Oliva - Sofsecurity - CSVD	Dic- 2022
PT003	Realizar un muestreo para verificar que se esté aplicando la política de bloqueo de pantalla después de los 5 minutos de inactividad.	Detectivo	100	Fuerte	Corto plazo	A través de la validación de la GPO respectiva se puede comprobar que dicha política se encuentra desplegada. (validar con pchamorro)	Pablo Chamorro	Continuo
PT004	Contratar el diseño de una red segura y su respectivo acompañamiento en la implementación de dicho diseño.	Preventivo	100	Fuerte	Mediano plazo	No se ha realizado dicha contratación, sin embargo, se está trabajando a nivel interno esta arquitectura	Andrés Oliva - Darío Agudelo	Dic- 2022

ID	Planes de tratamiento	Tipo de plan de acción	Peso de evaluación del plan de acción	Efectividad del plan de acción	Plazo	Cumplimiento	Responsable	Fecha en la que se ejecutó el plan
PT005	Adquirir una solución que no permita él envió de información de tipo: clasificada o reservada, a menos que dicha información se encuentra cifrada.	Correctivo	100	Fuerte	Mediano plazo	No se ha implementado/adquirido solución DLP debido a la falta de presupuesto	Andrés Oliva	Dic- 2022
PT006	Definir 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	100	Fuerte	Corto plazo	Se está trabajando en el diseño del procedimiento y en la implementación del control NAC para acceso remoto (VPN)	Fabián Ceferino - Sofsecurity	Dic- 2022
PT007	Definir políticas de backups para sistemas de información y plataformas criticas del SGC, que incluyan backups completos e incrementales.	Correctivo	100	Fuerte	Corto plazo	Las políticas en Networker se trabajan con full e incremental	Heriberto Albutria - Diego Barragán	Dic- 2022
PT008	Desarrollar políticas de restauración periódica de backups aleatorios para garantizar que los backups se están haciendo correctamente.	Preventivo	100	Fuerte	Corto plazo	Se realizó eventualmente pruebas de restauración tanto de NAS como SAN Cada 4 meses en forma de laboratorio, en forma de requerimiento todos los meses se realiza	Heriberto Albutria - Diego Barragán	Dic- 2022
PT009	Contratar una auditoria externa para que verifique 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	100	Fuerte	Corto plazo	No se cuenta con presupuesto	Heriberto Albutria	Dic- 2022
PT010	Adquirir como servicio un centro alterno de operaciones	Correctivo	100	Fuerte	Mediano plazo	No se cuenta con presupuesto	Comité de Gestión y desempeño institucional	Dic- 2022
PT011	Adquisición de una solución tipo DLP para gestionar medios removibles de acuerdo al esquema de clasificación de la información.	Preventivo	100	Fuerte	Mediano plazo	No se cuenta con presupuesto	Andrés Oliva	Dic- 2022
PT012	Documentar procedimientos operativos para la administración adecuada de la red	Preventivo	100	Fuerte	Corto plazo	No se cuenta con presupuesto	Darío Agudelo	Dic- 2022
PT013	Revisar y aprobar el procedimiento de gestión de incidentes por parte de la DGI	Preventivo	100	Fuerte	Corto plazo	Está en proceso de oficialización	Andrés Oliva - Andrea Neira - William Condia	Dic- 2022

ID	Planes de tratamiento	Tipo de plan de acción	Peso de evaluación del plan de acción	Efectividad del plan de acción	Plazo	Cumplimiento	Responsable	Fecha en la que se ejecutó el plan
PT014	Desarrollar una política para el acceso de dispositivos móviles en redes externas (antivirus, sistema operativo y navegadores actualizados)	Preventivo	100	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)	Fabián Ceferino - Sofsecurity	Dic- 2022
PT015	Desarrollar e implementar una política de uso aceptable de activos de información.	Preventivo	100	Fuerte	Corto plazo	Está en proceso de oficialización	Andrés Oliva - Andrea Neira - William Condia	Dic- 2022
PT016	Cifrar bases de datos y carpetas compartidas a nivel institucional	Preventivo	100	Fuerte	Mediano plazo	No contamos con solución de cifrado de datos	Andrés Oliva	Dic- 2022
PT017	Definir un plan para implementar las políticas de escritorio limpio y pantalla limpia	Preventivo	100	Fuerte	Corto plazo	En desarrollo	Andrés Oliva	Dic- 2022
PT018	Sincronizar toda la plataforma tecnológica con el servidor NTP de la red sismológica, que es un servidor especializado de hora	Preventivo	100	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	Pablo Chamorro - Andrés Oliva	Continuo
PT019	Adquirir e implementar una solución que permita hacer el monitoreo de disponibilidad de los servicios internos	Preventivo / Detectivo / Correctivo	100	Fuerte	Largo plazo	No contamos con la solución	Andrés Oliva - Heriberto Albutria	Dic- 2022
PT020	Desarrollar e implementar políticas de seguridad de la información para la relación con proveedores o terceros	Preventivo	100	Fuerte	Corto plazo	Está en proceso de oficialización	Andrés Oliva - Andrea Neira - William Condia	Dic- 2022
PT021	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	100	Fuerte	Mediano plazo	Se desarrolló un plan de pruebas asociado a sistemas de apoyo críticos y al seiscom de RSNC	Heriberto Albutria - Andrea Neira - Equipo de plataforma de TI	Dic- 2022
PT022	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	100	Fuerte	Mediano plazo	Está en desarrollo del data center alterno en Pasto	Heriberto Albutria - Richard Mier - Equipo TI Pasto	Dic- 2022

ID	Planes de tratamiento	Tipo de plan de acción	Peso de evaluación del plan de acción	Efectividad del plan de acción	Plazo	Cumplimiento	Responsable	Fecha en la que se ejecutó el plan
PT023	Garantizar la revisión del SGSI por la dirección.	Preventivo	100	Fuerte	Corto plazo	Está en proceso de oficialización	Andrés Oliva - Andrea Neira - William Condia	Dic- 2022

5. MEDICIÓN

Se han ejecutado 32 de los 55 planes de tratamiento de riesgos desde el año 2020, 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.

6. 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 de Seguimiento a los Planes definidos en el Decreto 612 de 2018.