SERVICIO GEOLÓGICO COLOMBIANO

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

**2020**

## 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 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.

Existen diferentes estándares que se desarrollaron para gestionar la seguridad de la información, algunos más generales, algunos centrados en la gestión de riesgos (serie ISO/IEC 27000). Este análisis permite realizar un diagnóstico para conocer las debilidades y fortalezas internas encaminadas en la generación de los controles adecuados y normalizados dentro de las políticas de seguridad informática que hacen parte de un Modelo de Seguridad y Privacidad de la Información (MSPI), además de facilitar su continuo monitoreo a través de procesos de auditorías y mejoras continuas

## 2. OBJETIVO DEL DOCUMENTO

Establecer los lineamientos para un proceso adecuado de gestión de riesgos de seguridad y 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.

Este es uno de los retos que debe asumir el SGC con el fin de estar acorde a los modelos y estándares actuales; para ello es necesario empezar con la ejecución del análisis de riesgos de la seguridad de la información que en un futuro será la base para implementar el Modelo de Seguridad y Privacidad de la Información (MSPI), que permitirá mantener un modelo de negocio estable logrando un valor agregado.

## 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 SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

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

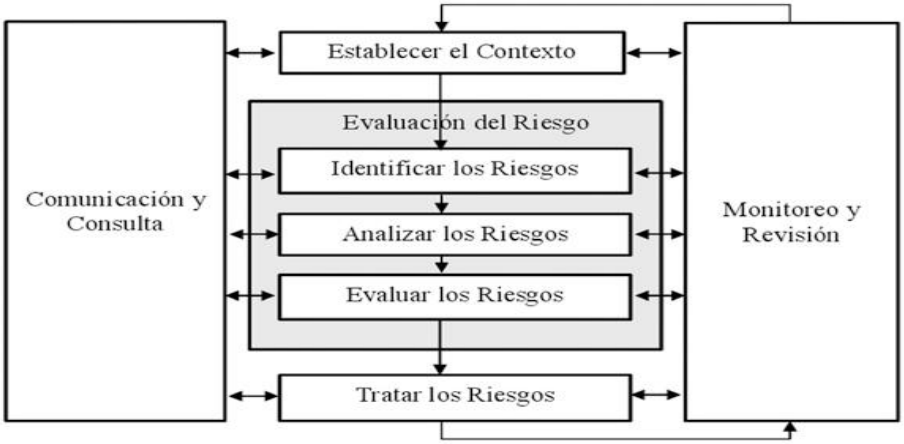
generar desventajas competitivas, pérdidas económicas, afecta la reputación y/o imagen y de la compañía" (Seguridad de la Información TGE, 2016).

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 en caso 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, 2011). 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 31000:2009:

*Ilustración 1. Proceso para la Gestión de Riesgos*



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 estable 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

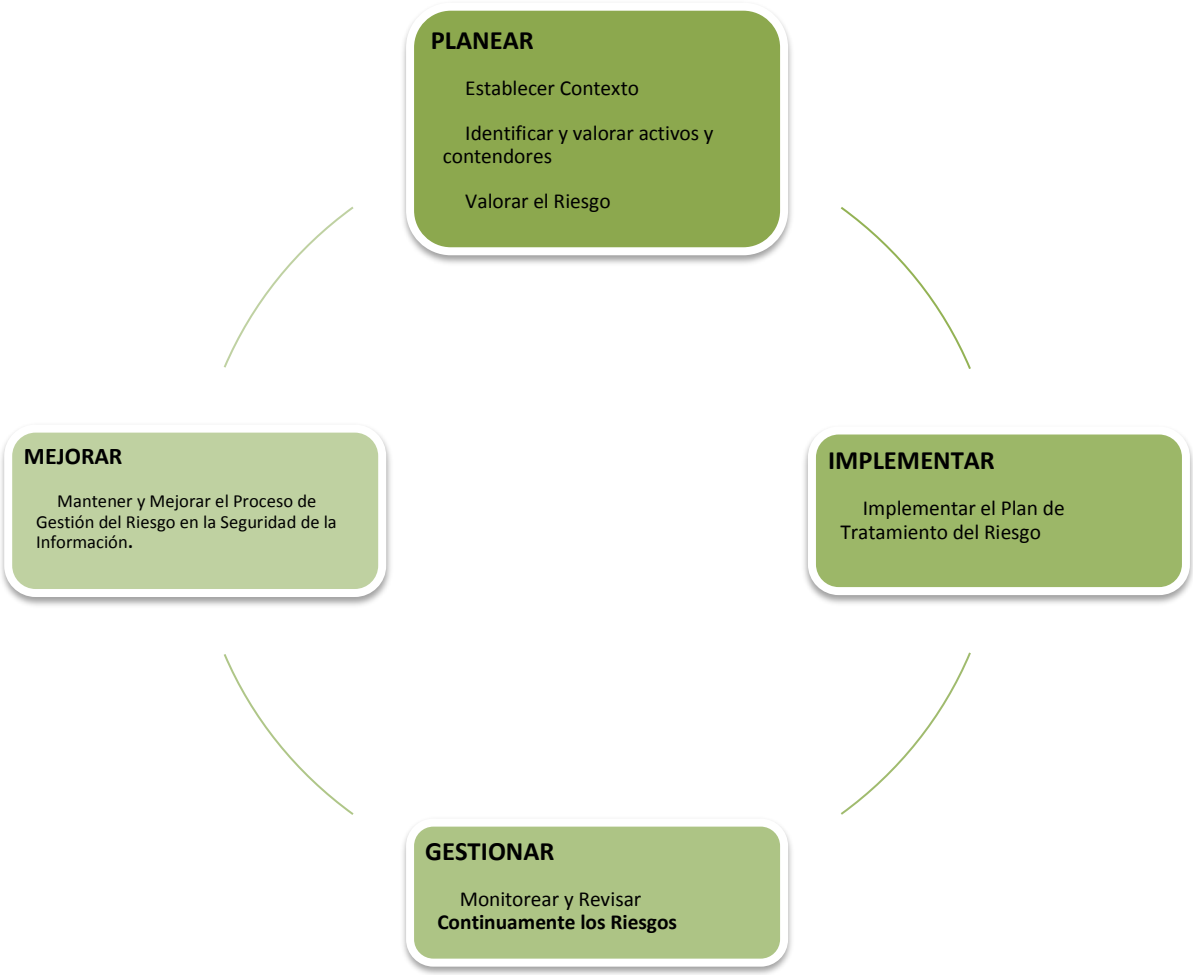
los mismos. La evaluación del riesgo es la comparación de los niveles de riesgo estimados con los criterios de evaluación y los criterios de aceptación del riesgo y los priorizados que se deben establecer cuando se consideró el contexto.

- **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

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*




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

*Ilustración 3. Pasó a paso para llevar a cabo el análisis de riesgos*


## 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*

| DESCRIPCIÓN DE FACTORES | |
| --- | --- |
| **CONTEXTO EXTERNO** | ● **Sector en el que opera:** Características, lineamientos y directrices del sector minas y energía.<br>● **Político:** Cambios de gobierno, legislación, políticas públicas, regulación.<br>● **Económico:** Patrimonio económico.<br>● **Social y cultural:** Responsabilidad social.<br>● **Tecnológico:** Avances en tecnología, acceso a sistemas de información externos, intercambio de información con otras entidades.<br>● **Ambiental:** Emisiones y residuos, catástrofes naturales, desarrollo sostenible.<br>● **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*

| DESCRIPCIÓN DE FACTORES | |
| --- | --- |
| **CONTEXTO INTERNO** | ● **Direccionamiento estratégico:** misión, visión, objetivos, funciones, organigrama.<br>● **Entes internos de control:** oficina de control interno, sistema de PQRD.<br>● **Financieros: I**nfraestructura.<br>● **Personas:** Competencia del personal, principales contactos.<br>● **Procesos:** Mapa de procesos, tipos de procesos.<br>● **Tecnología:** Conectividad general, gestión de la información geocientífica.<br>● **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*

| DESCRIPCIÓN DE FACTORES | |
| --- | --- |
| **CONTEXTO DEL PROCESO** | ● **Diseño del proceso:** Descripción de detallada de procesos.<br>● **Transversalidad:** Procesos que determinan lineamientos necesarios para el desarrollo de todos los procesos de la institución.<br>● **Procedimientos y formatos asociados:** Pertinencia de los procedimientos y formatos establecidos en los procesos y su ejecución en términos de tiempo y ubicación.<br>● **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.

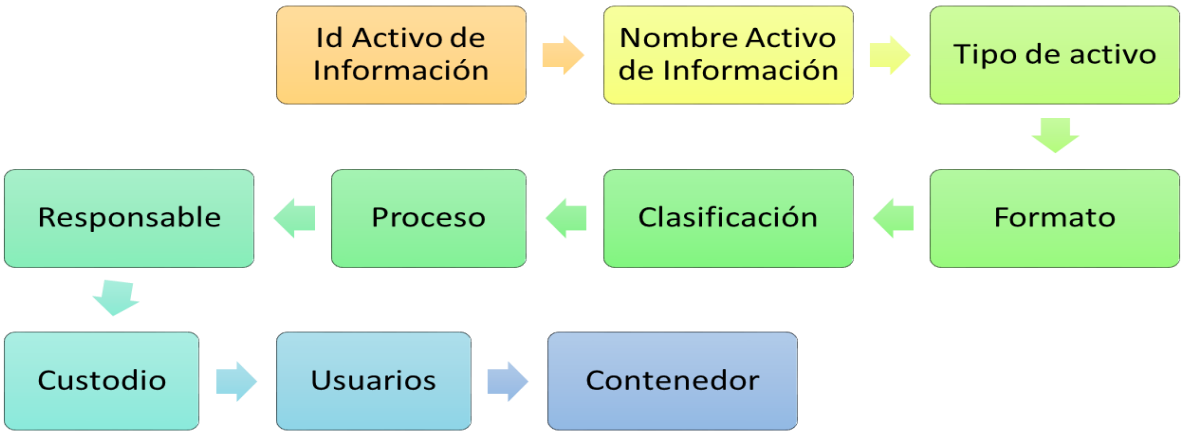
De aquí la importancia de la identificación y valoración de los activos de información, ya que el contenedor heredara la valoración de los impactos más altos de los activos que contiene, y los riesgos de seguridad de la información estarán asociados a dichos contenedores.

### 4.2.1. Identificación de activos de información y sus contenedores

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 y sus contenedores respectivos.

*Ilustración 4. Proceso de identificación de activos de información y contenedores*




**Notas:**

- Para la valoración de los activos de información se debe tener en cuenta los siguientes requisitos:
  a. Deben participar los dueños de los activos de información.
  b. Las escalas para valorar los impactos sobre cada principio se están definiendo en conjunto entre el Servicio Geológico Colombiano.
  c. 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 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.

- **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 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 este 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.

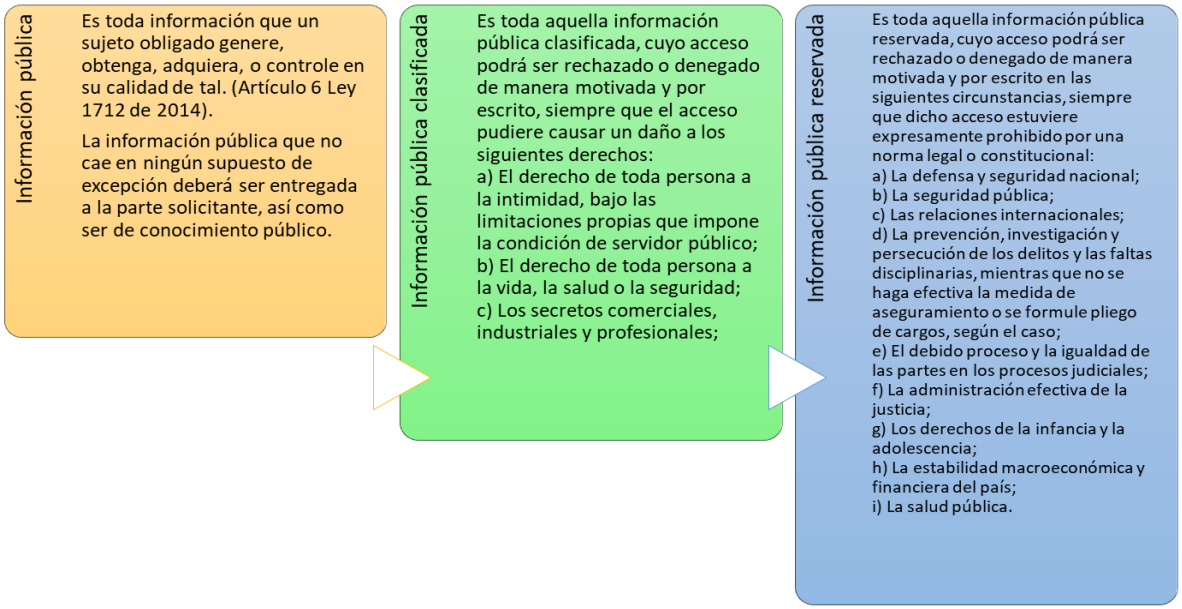
- **Usuario:** Cualquier persona, entidad, cargo, proceso, sistema automatizado o grupo de trabajo, que genere, obtenga, transforme, conserve o utilice información en

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.

- **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.

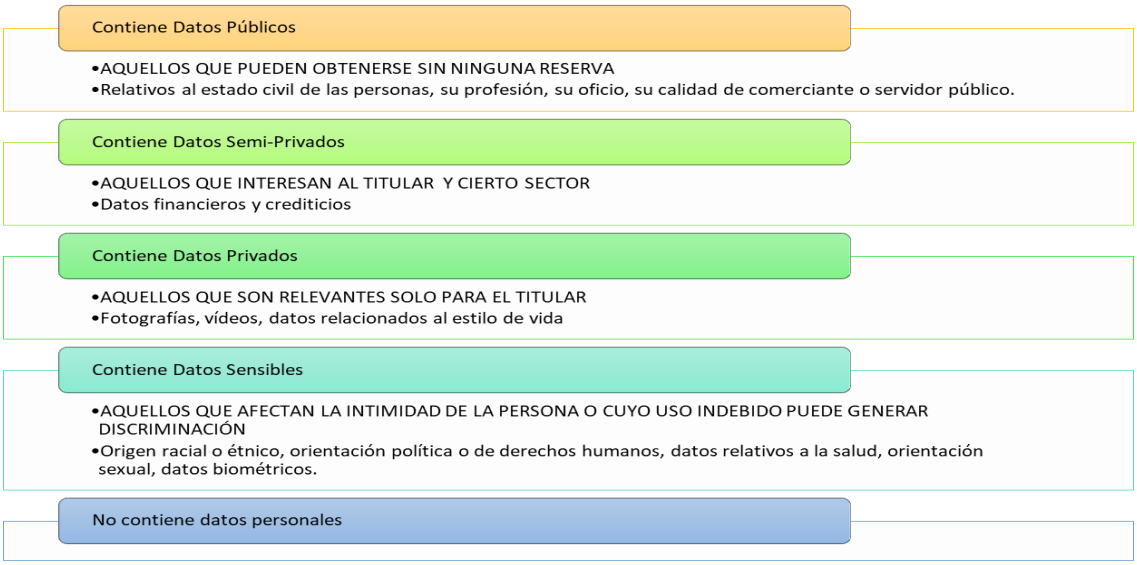
**Ley 1712 de 2014**

*Ilustración 5. Clasificación según Ley 1712*



**Ley 1581 de 2012**

*Ilustración 6. Clasificación según Ley 1581*




### 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*


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 principio en cada activo de información valorado, como se muestra a continuación:

*Ilustración 8. Evaluación de principios de seguridad de la información*

| **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*

| 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, pero no es fundamental en dicha actividad. | 2 |
| **Moderado** | La información hace parte de la toma de decisiones, pero se puede tomar 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*

| 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 se generan consecuencias para el SGC. | 2 |
| **Moderado** | Conduciría a una falta disciplinaria de tipo grave o gravísima sobre algún funcionario, pero no se generan consecuencias para el SGC. | 3 |

| | | |
|---|---|---|
| **Mayor** | Genera consecuencias de carácter penal sobre algún funcionario, pero no se 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*

| Impacto | Impacto Reputacional | Nivel |
|---|---|---|
| **Insignificante** | El incidente de seguridad no genera ninguna afectación a la reputación del SGC. | 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*

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

### 4.2.3. Valoración de los contenedores de información

Los contenedores, son los repositorios donde se almacenan los activos de información, en dichos repositorios es donde suelen llevarse a cabo los ataques contra los datos o presentarse pérdidas o alteraciones, por ende, son los lugares donde se aplican los controles de seguridad.

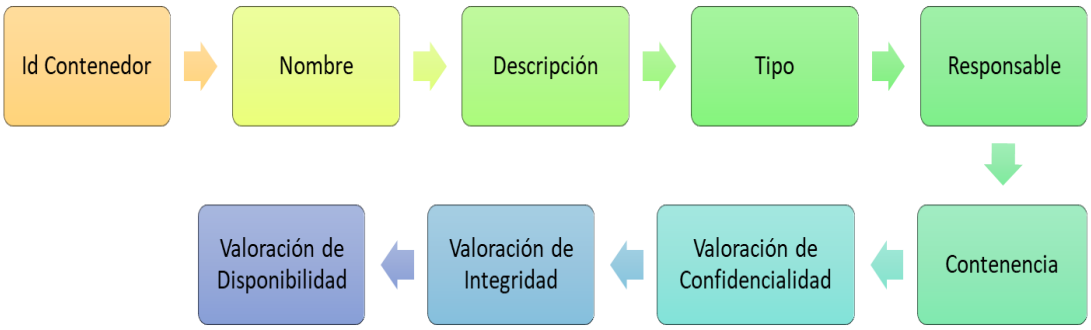
Pueden ser del tipo técnico, físico o humano, ya que la información puede encontrarse en formato digital (archivos en medios electrónicos u ópticos), en forma física (escrita o impresa en papel), así como información no representada, como las ideas o el conocimiento de los empleados.

Cuando se estén identificando los contenedores de información, se debe tener en cuenta lo siguiente: Un contenedor puede ser un elemento tecnológico (equipo de cómputo), un lugar físico (archivo físico de documentos) o un recurso humano en el que se encuentra el

activo de información analizado. Dicha información debe ser suministrada por el responsable, el custodio o los usuarios del activo de información, quienes saben en donde se encuentra almacenado, en donde es procesado o en donde es transmitido dicho activo de información.

A continuación, se presentan los pasos necesarios para valorar los contenedores de información:

*Tabla 8. Proceso de valoración de contenedores de información*




**Id del contenedor:** Es el identificador único de cada contenedor, ej: CONT001

**Nombre:** Nombre del contenedor de información.

**Descripción del contenedor:** Descripción detallada del contenedor con el fin de que sea clara la importancia de dicho contenedor para la institución.

**Tipo:** Elemento tecnológico, lugar físico o recurso humano.

**Responsable:** Líder de proceso o persona designada por el líder de proceso que tiene bajo su cargo:

- Verificar que se implementen los controles de acuerdo al nivel de clasificación de la información que contiene.
- Establecer los privilegios de acceso asociados con los activos de información que contiene.

**Contenencia:** La contenencia hace referencia a la relación de activos de información que se encuentran contenidos en dicho contenedor.

**Valoración:** Dependiendo del criterio analizado (Confidencialidad, integridad o disponibilidad) el contenedor heredara el impacto mayor de los activos que contiene en dicho criterio.

## 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

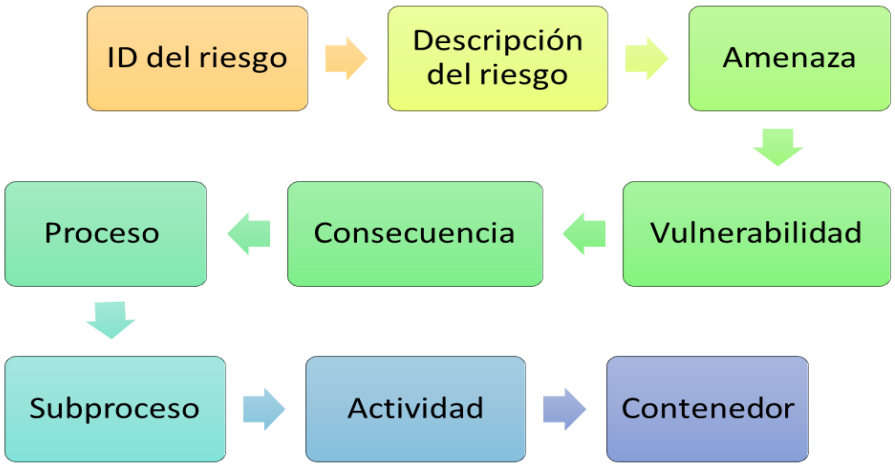
La identificación del riesgo consiste en establecer las fuentes de riesgo, los eventos, sus causas y sus consecuencias. Para el análisis se pueden involucrar datos históricos, análisis teóricos, opiniones informadas y expertas y las necesidades de las partes involucradas. (NTC ISO31000, Numeral 2.15).

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 disposiciones a las que está obligada y comprometida a cumplir.

A continuación, se presenta el proceso a seguir:

*Ilustración 9. Proceso de identificación del riesgo*




### 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*

| TABLA DE PROBABILIDAD | | | |
|---|---|---|---|
| **NIVEL** | **DESCRIPTOR** | **DESCRIPCIÓN** | **FRECUENCIA** |
| 1 | Raro | El evento puede ocurrir sólo en circunstancias excepcionales | No se ha presentado en los últimos 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 algún momento | Al menos una vez en el último año |
| 4 | Probable | El evento probablemente ocurrirá en la mayoría de las circunstancias | Al menos una vez en el último semestre |
| 5 | Casi seguro | Se espera que el evento ocurra en la mayoría de las circunstancias | El evento se presentó en el último 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.

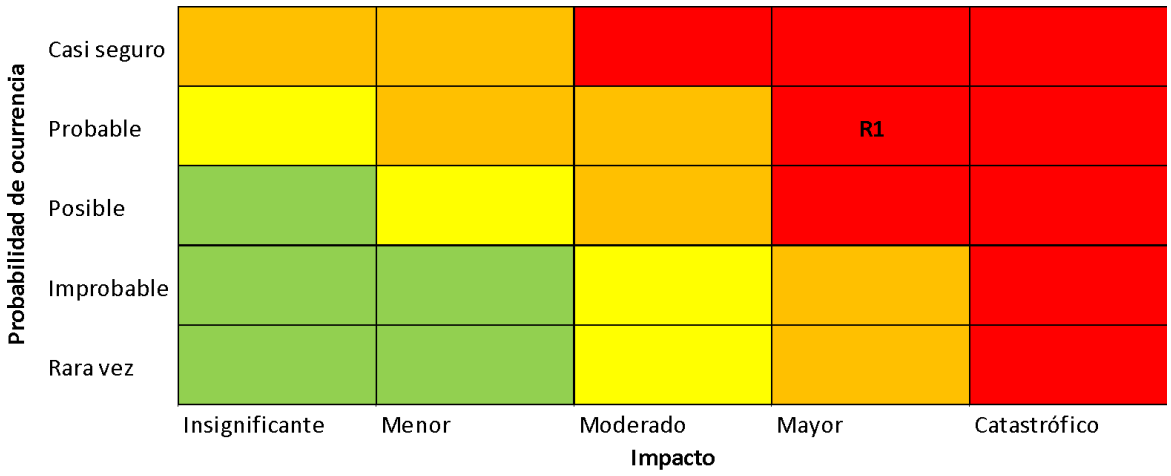
*Ilustración 10. Proceso de valoración del riesgo inherente*


**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*



### 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 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).

## 5. CONTROL DE VERSIÓN

| Versión | Fecha de aprobación | Descripción | Responsable |
| --- | --- | --- | --- |
| 1 | 27/01/2020 | Aprobación de Tratamiento de Riesgos de Seguridad y Privacidad de la Información | DT Gestión de Información |

## 6. PLANES DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

| N° | ACTIVIDADES | N° | TAREAS | PRODUCTO | RESPONSABLE | PROGRAMACIÓN DE TAREAS | |
|---|---|---|---|---|---|---|---|
| | | | | | | FECHA INICIO | FECHA FIN |
| 1 | Sensibilización | 1 | Socialización Gestión de Riesgos de Seguridad y privacidad de la Información y Seguridad digital | Actas de reunión, listados de asistencia | DGI | Enero 2020 | Diciembre 2020 |
| 2 | Identificación de Riesgos de Seguridad y Privacidad de la Información, Seguridad Digital y continuidad de la Operación | 1 | Identificación, Análisis y Evaluación de Riesgos - Seguridad y Privacidad de la Información, Seguridad Digital y Continuidad de la Operación y regionales del SGC | Matriz de riesgos, actas de reunión, correos electrónicos | DGI | Enero 2020 | Diciembre 2020 |
| | | 2 | Realimentación, revisión y verificación de los riesgos identificados (Ajustes) | Actas de reunión - Correos Electrónicos - Registro Bitácora Soporte a Regionales y Procesos, Video Conferencias | DGI – Soporte Técnico Regional | Enero 2020 | Diciembre 2020 |

| N° | ACTIVIDADES | N° | TAREAS | PRODUCTO | RESPONSABLE | PROGRAMACIÓN DE TAREAS | |
|---|---|---|---|---|---|---|---|
| | | | | | | FECHA INICIO | FECHA FIN |
| 3 | Aceptación de Riesgos Identificados | 1 | Aceptación, aprobación Riesgos identificados y planes de tratamiento | Memorando Aceptación de riesgos Identificados - Matriz de riesgos, Plan de tratamiento | Líderes de Proceso / Director Regional | Enero 2020 | Diciembre 2020 |
| 4 | Publicación | 1 | Publicación Matriz de riesgos - Intranet | Matriz de riesgos publicada en la intranet de la entidad | Comunicaciones | Enero 2020 | Diciembre 2020 |
| 5 | Seguimiento Fase de Tratamiento | 1 | Seguimiento Estado planes de tratamiento de riesgos identificados y verificación de evidencias | Actas de reunión, Memorandos, Correos electrónicos - evidencias del estado de tratamiento - Matriz de riesgos | DGI – responsables de los riesgos residuales | Enero 2020 | Diciembre 2020 |
| 6 | Evaluación de riesgos residuales | 1 | Evaluación de riesgos residuales | Actas de reunión, Correos electrónicos - Matriz de | DGI – responsables de los riesgos residuales | Enero 2020 | Diciembre 2020 |

| N° | ACTIVIDADES | N° | TAREAS | PRODUCTO | RESPONSABLE | PROGRAMACIÓN DE TAREAS | |
|---|---|---|---|---|---|---|---|
| | | | | | | FECHA INICIO | FECHA FIN |
| | | | | riesgos | | | |
| 7 | Mejoramiento | 1 | Identificación de oportunidades de mejora acorde a los resultados obtenidos durante la evaluación de riesgos residuales | Actas de reunión, Correos electrónicos - Matriz de riesgos | DGI – responsables de los riesgos residuales | Enero 2020 | Diciembre 2020 |
| | | 2 | Actualización Guía Gestión de Riesgos Seguridad de la información, de acuerdo con los cambios solicitados. | Guía y Herramienta de Gestión de Riesgos | DGI | Enero 2020 | Diciembre 2020 |

## 7. MEDICIÓN

La medición se realiza con un indicador de gestión que está orientada principalmente determinar el porcentaje de ejecución de actividades definidas en el tratamiento de riesgos de seguridad y privacidad de la información, ubicados en zonas extremas, altas y moderadas.

## 8. SEGUIMIENTO Y CONTROL

El seguimiento y monitoreo a la ejecución de las actividades establecidas para el 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.

| Versión | Fecha de aprobación | Descripción | Responsable |
|---|---|---|---|
| 1 | 27/01/2020 | Aprobación del Plan Tratamiento de riesgos de Seguridad y Privacidad de la Información | DT Gestión de Información |