PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN 2024

Contenido

Control de cambios

Tabla 1. Cuadro de control			
Versión	Fecha	Instancia de Aprobación	Descripción
01	30- enero - 2024	Comité Institucional de Gestión y Desempeño	Formulación General del Plan de tratamiento de riesgos.

1. INTRODUCCIÓN

El Foro Económico Mundial ha publicado su Informe sobre Riesgos Globales 2024, en el que destaca la necesidad de diálogo ante las crecientes fracturas mundiales. Entre los principales riesgos se encuentran la ciberdelincuencia, los efectos adversos de la Inteligencia Artificial y los fenómenos meteorológicos extremos. Esto, debido a que los ciberdelincuentes también tienen acceso a la inteligencia artificial, lo que los hace mas peligrosos.

En Colombia, el número de ciberataques ha aumentado significativamente en los últimos años. Según un informe de **Fortinet**, América Latina y el Caribe sufrieron **137 mil millones** de intentos de ciberataques en la primera mitad de 2022, lo que representa un aumento del 50% en comparación con el mismo período del año anterior. En el caso de Colombia, hubo **6.300 millones** de intentos de intrusión, un aumento del 70% en comparación con el mismo período de 2021.
Desde el año 2022, Colombia se vio afectado por la materialización de ataques informáticos a entidades públicas y privadas. De acuerdo con el Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC), a través del Equipo de Respuesta a Emergencias Cibernéticas de Colombia -COLCERT, se recibieron 36 reportes de ataques entre los meses de noviembre y diciembre. De estos ataques 18 impactaron a entidades públicas de orden nacional, 5 a entidades públicas de orden territorial y los 18 restantes tuvieron como blanco a empresas y organizaciones del sector privado. Los tipos de ataques que se presentaron están catalogados como: la suplantación de sitios web, con 19 reportes y la suplantación de dominios de correo electrónico, con 8 reportes, como las prácticas más frecuentes. Los demás ataques (9) se dieron a través de acciones de compromiso de cuentas de usuarios, secuestro de información o ransomware, vulneraciones a aplicaciones web y denegación distribuida de servicios.
Como se puede deducir estos ataques representan la materialización de riesgos de seguridad y privacidad de la información, contra activos de información como pueden ser el sitio Web, el correo electrónico, la información y las aplicaciones entre otros.
La Superintendencia de Sociedades no es ajena a estos tipos de ataques y puede verse afectada en el cumplimiento de sus objetivos estratégicos si es impactada a futuro por estos u otros tipos de ataques informáticos y/o materialización de riesgos de seguridad y privacidad de la información.
Para mitigar estos riesgos es necesario establecer y ejecutar un plan de tratamiento de riesgos de seguridad y privacidad de la información, el cual debe estar adecuado al marco del Modelo Integrado de Planeación y Gestión MIPG, y sus políticas de Gobierno Digital y Seguridad Digital y demás regulaciones relacionadas como el CONPES 3854 de 2016, el Modelo de Seguridad y Privacidad de MINTIC y lo establecido en el decreto 1008 de 14 de junio 2018, en cuanto al fortalecimiento de la política de Gobierno Digital.
Asimismo, la Superintendencia de Sociedades ha adoptado buenas prácticas y lineamientos como los estándares ISO 27001:2013, ISO 31000:2018 y la guía para la administración del riesgo y el diseño de controles en entidades públicas - Versión 5 de diciembre de 2020, emitida por el Departamento Administrativo de la Función Pública DAFP, lo cual la ha llevado a certificarse en el Sistema de Gestión de Seguridad de la Información (ISO 27001:2013).
De acuerdo con lo anterior, Superintendencia de Sociedades define el Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información 2023, en el que se determinan las actividades, responsables y fechas orientadas para gestionar un adecuado proceso de administración de riesgos de seguridad y privacidad de la información y con el cual establece un proceso de mejora continua para cumplir con los principios de disponibilidad, integridad y confidencialidad de la información.

2. OBJETIVO

2.1 OBJETIVO GENERAL

Definir e implementar las actividades que permitan realizar la gestión de riesgos de Seguridad y Privacidad de la Información, establecidos en los procesos institucionales de la Superintendencia de Sociedades y sus intendencias, con el fin de prevenirlos, controlarlos y mitigarlos.

2.2 OBJETIVOS ESPECIFICOS

Para el cumplir del objetivo general del plan de tratamiento de riesgos se requiere el cumplimiento de los siguientes objetivos específicos:

- Establecer el plan de actividades para la gestión del riesgo de seguridad y privacidad de la información.
- Fortalecer la gestión de activos de información en los procesos e intendencias de la Superintendencia de Sociedades.
- Revisar y actualizar los activos de información establecidos en cada proceso institucional.
- Revisar y actualizar los riesgos de seguridad y privacidad de la información asociados a los activos de información.
- Fortalecer la cultura de gestión de riesgos de seguridad y privacidad de la información.
- Realizar seguimiento y monitoreo al cumplimiento de las medidas de seguridad y controles definidos para la mitigación de los riesgos determinados para los activos de información de la Superintendencia de Sociedades.
- Establecer parámetros para la mejora del sistema de riesgos y auditoria en lo referente al uso de nuevas tecnologías (inteligencia artificial, Big Data, etc).
- Fortalecer las capacidades institucionales en materia de riesgos de seguridad y privacidad de la información.

3. ALCANCE

Los lineamientos establecidos para la gestión de riesgos aplican a todos los procesos, proyectos y sedes de la Superintendencia de Sociedades y a todas las acciones ejecutadas por los servidores de la Entidad durante el ejercicio de sus funciones. Incluye los riesgos de seguridad de la información y de corrupción.
Para este Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información aplican a todos los procesos e intendencias de la Superintendencia de Sociedades, y contemplan las acciones orientadas a prevenir, controlar y mitigar la posible materialización de amenazas y ataques informáticos que afecten sus servicios, trámites y cumplimiento de los objetivos misionales establecidos.

4. MARCO NORMATIVO

JERARQUÍA	NUMERO / FECHA	TITULO
Ley	527 de 1999	Por medio de la cual se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales, y se establecen las entidades de certificación y se dictan otras disposiciones
Ley	1273 del 2009	Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado “de la protección de la información y de los datos”- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones
Ley	1581 de 2012	Por la cual se dictan disposiciones generales para la protección de datos personales.
Ley	2108 de 2021	Ley de internet como servicio público esencial y universal" o por medio de la cual se modifica la ley 1341 de 2009 y se dictan otras disposiciones
Ley	1712 de 2014	Por medio de la cual se crea la Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional y se dictan otras disposiciones.
Decreto	1377 de 2013	Por el cual se reglamenta parcialmente la Ley 1581 de 2012.
Decreto	886 de 2014	Por el cual se reglamenta el artículo 25 de la Ley 1581 de 2012, relativo al Registro Nacional de Bases de Datos.
Decreto	2573 de 2014	Por el cual se establecen los lineamientos generales de la Estrategia de Gobierno en línea, se reglamenta parcialmente la Ley 1341 de 2009 y se dictan otras disposiciones
Decreto	1083 de 2015	Artículo 74 de la Ley 1474 de 2011, deberán integrar los planes institucionales y estratégicos y publicarlos, en su respectiva página web, a más tardar el 31 de enero de cada año. (Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información y Plan de Seguridad y Privacidad de la Información, entre otros).
Decreto	1078 de 2015	Por medio del cual se expide el Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones
Decreto	728 de 2017	Se adiciona el capítulo 2 al título 9 de la parte 2 del libro 2 del decreto único reglamentario del sector TIC, 1078 de 2015, “Implementación de zonas de acceso público a internet inalambrico en entidades públicas del orden nacional para el fortalecimiento del modelo de gobierno digital.
Decreto	1499 de 2017	El Departamento Administrativo de la Función Pública, reglamentó el Sistema Integrado de Planeación y Gestión y actualizó el modelo para su implementación, denominado “Modelo Integrado de Planeación

		y Gestión – MIPG”
Decreto	1008 de 2018	Por medio del cual se establecen los lineamientos generales de la Política de Gobierno Digital y se subroga el capítulo 1 del título 9 de la parte 2 del libro 2 del Decreto 1078 de 2015, Decreto Único Reglamentario del sector de Tecnologías de la Información y las Comunicaciones.
Decreto	1389 de 2022	Por el cual se adiciona el Título 24 a la Parte 2 del Libro 2 del Decreto Único 1078 de 2015, Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones, con el fin de establecer los lineamientos generales para la gobernanza en la infraestructura de datos y se crea el Modelo de gobernanza de la infraestructura de datos
Resolución	511-004571 de Agosto de 2012	Por la cual se delegan funciones y asignan competencias
Resolución	511-004064 de Julio de 2012	La cual crea los grupos internos de trabajo que conforman la Superintedencia de Sociedades .
Resolución	165-2748 de 2005	Por la cual son asignadas funciones para el manejo y control del Sistema de Gestión de la Superintendencia de Sociedades
Resolución	3564 de 2015	Reglamentaciones asociadas a la ley de Transparencia y acceso a la información pública
Resolución	510-000356 de 2015	Por medio de la cual se implementa el Plan Piloto de Teletrabajo en la Superintendencia de Sociedades
Resolución	165-000368 de 2018	Por medio de la cual se adopta la política de Gestión Integral para la gestión socialmente responsable y designa el Representante de la Alta Dirección para el Sistema de Gestión Integrado.
Resolución	100-003113 del 05/03/2019	Por medio de la cual se asignan unas funciones y se definen los Grupos internos de trabajo en la Superintendencia de Sociedades.
Resolución	100-000040 de 2021	Por medio de la cual se asignan unas funciones y se definen los grupos internos de trabajo en la Superintendencia de Sociedades
Directiva Presidencial	02 de 2002	Derecho de autor y los derechos conexos, en lo referente a utilización de programas de ordenador (software)
Directiva Presidencial	03 de marzo de 2021	LINEAMIENTOS PARA EL USO DE SERVICIOS EN LA NUBE, INTELIGENCIA ARTIFICIAL, SEGURIDAD DIGITAL Y GESTiÓN DE DATOS.
Directiva Presidencial	24 de febrero de 2022	Reiteración de la política pública en materia de seguridad digital.

Documento	CONPES 3650 de 2010	El presente documento somete a consideración del Consejo Nacional de Política Económica y Social – Conpes, la declaratoria del Programa Agenda de Conectividad - Estrategia de Gobierno en Línea que el Ministerio de Tecnologías de la Información y las Comunicaciones ha venido desarrollando a través del proyecto de inversión “Implementación y Desarrollo Agenda de Conectividad”, como de importancia estratégica para continuar con su implementación y promoción en el orden nacional y territorial.
Documento	CONPES 3701 de 2011	Lineamientos de Política para Ciberseguridad y Ciberdefensa
Documento	CONPES 3854 de 2016	Política Nacional de Seguridad Digital
Documento	NTC 5854 de 2012	Accesibilidad de páginas web
Circular	52 de 2007	Requerimientos mínimos de seguridad y calidad en el manejo de información a través de medios y canales de distribución de productos y servicios para clientes y usuarios.
Circular Interna	05 de 2000	Uso de software pirata
Circular Interna	25 de 2000	Agenda de conectividad del gobierno colombiano
Circular Interna	07 de 2001	Reglamento sobre el uso del correo electrónico y el servicio de Internet
Circular Interna	11 de 2001	Implantación del Sistema de Gestión
Circular Interna	03 de 2004	Implantación de los módulos de seguridad y notificaciones del Sistema de Gestión.
Norma técnica colombiana	NTC/ISO 27001:2013	Tecnología de la información. Técnicas de seguridad. Sistemas de Gestión de la Seguridad de la Información (SGSI). Requisitos.
Norma técnica colombiana	NTC/ISO 27001:2013	Gestión del Riesgo. Principios y directrices.
Documento Técnico Externo	2016	Modelo de Seguridad y Privacidad de la Información – MSPI Se encuentra alineado con el Marco de Referencia de Arquitectura TI y soporta transversalmente los otros componentes de la Política de Gobierno Digital, TIC para el Estado y TIC para la Sociedad. TIC, que son habilitados por tres elementos transversales: Seguridad de la Información, Arquitectura y Servicios Ciudadanos Digitales. Versión 3.0.2, julio de 2016
Documento Técnico Externo	2019	Manual para la Implementación de la Política de Gobierno Digital Implementación de la Política de Gobierno Digital (Decreto 1008 de 2018). Versión 7, abril de 2019.
Documento del Sistema de Gestión Integral	GC-I-001	Instructivo para la identificación, clasificación, valoración y etiquetado de activos de información.
Documento del Sistema de Gestión Integral	GC-I-002	Instructivo para la gestión de riesgos de seguridad de la información.

5. RESPONSABILIDADES

La identificación, clasificación, valoración y monitoreo de los riesgos está alineado a lo indicado en el documento GC-G-002 Guía Administración de Riesgos Institucionales, en el numeral 4.2.3 Responsabilidades y compromisos frente a la administración del riesgo, de la siguiente manera:

LINEA	ROL	FUNCIONES
Línea Estratégica	Alta Dirección	Define el marco general para la gestión del riesgo y el control y supervisa su cumplimiento.
Primera línea de defensa	Gerentes públicos y líderes de procesos, programas y proyectos	Desarrolla e implementa procesos de control y gestión de riesgos a través de su identificación, análisis, valoración, monitoreo y acciones de mejora.
Segunda línea de defensa	Oficina Asesora de Planeación, supervisores e interventores de contratos	Asegura que los controles y los procesos de gestión de riesgos implementados, estén diseñados apropiadamente y funcionen como se pretende.
Tercera línea de defensa	Oficina de Control Interno	Proporciona información sobre la efectividad del Sistema de Control Interno a través de un enfoque basado en riesgos. El alcance de este aseguramiento, a través de la auditoría interna cubre todos los componentes del Sistema de Control Interno.

Las auditorías externas de los sistemas de gestión también tienen una actividad de revisión de los riesgos de los procesos, al menos una vez al año.
Específicamente para los riesgos de seguridad de la información están definidas en el documento interno GC-I-002 (Instructivo para la gestión de riesgos de seguridad de la información), las actividades a desarrollar por parte de los funcionarios de los procesos y del Oficial de Seguridad de la Información.

6. DEFINICIONES

- **Aceptación del riesgo:** Es la decisión informada de aceptar las consecuencias y la probabilidad de un riesgo particular.
- **Activo de Información:** Es todo aquello que posee valor para una entidad, como: elementos de hardware, software de procesamiento, almacenamiento y comunicaciones, bases de datos, información física y digital, procedimientos y recursos humanos asociados con el manejo de los datos y la información misional, operativa, administrativa de la entidad, entre otros.
- **Análisis del riesgo:** Proceso sistemático para entender la naturaleza del riesgo y deducir su nivel.
- **Amenazas**: Situación potencial de un incidente no deseado, el cual puede ocasionar daño a un sistema o a la organización.
- **Causa**: Elemento específico que origina el evento.

- **Consecuencia:** El resultado de un evento expresado en forma cualitativa o cuantitativa, que genera pérdida, daño, desventaja o ganancia. Estos pueden ser un rango de posibles resultados asociados con el evento. En algunos escenarios también se conoce como Impacto.
- **Clasificación de la Información:** Ejercicio por medio del cual se determina que la información pertenece a uno de los niveles de clasificación estipulados en la entidad. Tiene como objetivo asegurar que la información recibe el nivel que le corresponda, con respecto a la confidencialidad, integridad y disponibilidad.
- **Contexto externo:** Ambiente externo en el cual la organización busca alcanzar sus objetivos (tecnológico, legal, regional, etc.).
- **Contexto interno:** Ambiente interno en el cual la organización busca alcanzar sus objetivos (gobierno, políticas, estructura organizacional, etc.).
- **Control del Riesgo:** Se refiere a la parte de la administración de riesgo, que involucra la implantación de políticas, estándares, procedimientos, dispositivos y cambios físicos para eliminar o minimizar los riesgos adversos.
- **Corrupción:** Uso del poder para desviar la gestión de lo público hacia el beneficio particular.
- **Criterios de riesgos:** Términos de referencia frente a los cuales se evaluará la importancia del riesgo.
- **Custodio del activo de información:** Es una parte designada de la entidad, un cargo, proceso, o grupo de trabajo encargado de administrar y hacer efectivos los controles de seguridad que el propietario de la información haya definido, tales como copias de seguridad, asignación privilegios de acceso, modificación y borrado. (tomado de la “Guía para la gestión y clasificación de activos de información”).
- **Confidencialidad:** Propiedad que determina que la información sólo esté disponible y sea revelada a individuos, entidades o procesos autorizados. (tomado de la “Guía para la gestión y clasificación de activos de información”).
- **Disponibilidad:** Propiedad de que la información sea accesible y utilizable por solicitud de una entidad autorizada, cuando ésta así lo requiera. (tomado de la “Guía para la gestión y clasificación de activos de información”).
- **Evaluación del Riesgo:** Comparar los resultados del análisis de riesgo frente a los controles implementados, con el fin de determinar el riesgo final.
- **Evento:** Posible ocurrencia de Incidente o amenaza de Seguridad de la Información.
- **Fuente:** Elemento que por sí solo o en combinación tiene el potencial intrínseco para dar lugar a riesgo; a fuente del riesgo puede ser tangible o intangible.
- **Gestión del riesgo:** Actividades coordinadas para dirigir y controlar una organización con respecto al riesgo.
- **Impacto:** Consecuencias que puede ocasionar a la organización la materialización del riesgo.
- **Identificación del riesgo:** Se determinan las causas, fuentes del riesgo y los eventos con base al contexto el proceso, que pueden afectar el logro de los objetivos de este.
- **Información:** Es un activo impreso, escrito, físico, digital, electrónico que se crea, procesa, envía y transfiere por los procesos.

- **Información pública:** Toda información que un sujeto obligado genere, obtenga, adquiera, o controle en su calidad de tal. (tomado de la "Guía para la gestión y clasificación de activos de información").
- **Información pública clasificada:** Información disponible para todos los procesos de la entidad, y que en caso de ser conocida por terceros sin autorización, puede conllevar un impacto negativo para los procesos de la misma. Esta información es propia de la entidad o de terceros y puede ser utilizada por todos los funcionarios de la entidad para realizar labores propias de los procesos, pero no puede ser conocida por terceros sin autorización del propietario. (tomado de la "Guía para la gestión y clasificación de activos de información").
- **Información pública reservada:** Información disponible sólo para un proceso de la entidad y que en caso de ser conocida por terceros sin autorización puede conllevar un impacto negativo de índole legal, operativa, de pérdida de imagen o económica. (tomado de la "Guía para la gestión y clasificación de activos de información").
- **Integridad:** Propiedad de salvaguardar la exactitud y estado completo de los activos. (tomado de la "Guía para la gestión y clasificación de activos de información").
- **Inventario de activos de Información:** Identificación de todos aquellos recursos que posean valor para la entidad (físicos, de información, software, documentos, servicios, personas, intangibles, etc.) contemplados dentro del alcance del SGSI, los cuales requieran ser protegidos de potenciales riesgos.
- **Mapa de Riesgos:** Documento con la información resultante de la gestión del riesgo.
- **Oficial de Seguridad de la Información:** Profesional responsable de alinear las iniciativas de seguridad de la información con los objetivos misionales, garantizando que los bienes y las tecnologías de la información están adecuadamente protegidos.
- **Partes Involucradas (Stakeholders):** personas y organizaciones que pueden ser afectadas, son afectadas por, o perciben que ellos mismos pueden ser afectados por una decisión o actividad.
- **Pérdida:** Una consecuencia negativa, financiera o de cualquier otra índole.
- **Política de riesgos:** Orientación general en torno a la administración de riesgos emanada de la Ala Dirección. Política de riesgos: orientación general en torno a la administración de riesgos emanada de la Ala Dirección.
- **Probabilidad**: Posibilidad de ocurrencia del riesgo, ésta puede ser medida con criterios de frecuencia o factibilidad.
- **Propietario del activo de información:** Persona, grupo interno de trabajo o una dependencia al que se ha dado la responsabilidad formal por la seguridad de un activo o una categoría de activos de información. No significa que el activo pertenece al dueño en un sentido legal. Los propietarios de activos de información son responsables de manera formal por garantizar que los mismos, estén seguros mientras están siendo desarrollados, producidos, mantenidos, utilizados y almacenados (ciclo de vida del activo de información).
- **Proceso de Administración del Riesgo:** La aplicación sistemática de políticas gerenciales, procedimientos y prácticas, en las actividades para establecer el contexto, identificar, analizar, evaluar, tratar, monitorear y comunicar los riesgos
- **Riesgo:** Posibilidad de que algo suceda y genere un impacto sobre los objetivos. Está medido en términos de probabilidad de ocurrencia e impacto. *Nota: El riesgo con frecuencia se*

especifica en términos de un evento o circunstancia y las consecuencias que pueden derivarse de este. Es medido en términos de la combinación de la probabilidad de ocurrencia y las consecuencias del mismo.

- **Riesgo de Corrupción:** Posibilidad de que, por acción u omisión, se use el poder para desviar la gestión de lo público hacia un beneficio particular.
- **Riesgo de Seguridad de la Información:** Preservación de la confidencialidad, integridad y disponibilidad de la información (ISO/ IEC 27000).
- **Riesgo de Seguridad Digital:** Combinación de amenazas y vulnerabilidades en el entorno digital. Puede debilitar el logro de objetivos económicos y sociales, así como afectar la soberanía, la integridad, el orden y los intereses de la entidad. Incluye aspectos relacionados con ambiente físico, digital y personas.
- **Riesgo Inherente:** El máximo riesgo sin los efectos mitigantes de los controles (riesgo sin controles).
- **Riesgo residual:** Se refiere al margen o residuo de riesgo que puede darse a pesar de las medidas de tratamiento o mejoramiento tomadas para la administración del mismo.
- **Transferir el riesgo:** Transferir total o parcialmente la responsabilidad de la provisión para pérdidas a un tercero a través de la ley, contratos, seguros u otro medio. Transferir el riesgo puede también hacer referencia a mover físicamente el riesgo o parte del mismo a otro sitio.
- **Tratamiento al Riesgo:** Respuesta establecida por la primera línea de defensa para la mitigación de los diferentes riesgos, incluyendo los riesgos de corrupción.
- **Vulnerabilidad:** V**V** ulnerabilidad: Una debilidad de un sujeto o sistema expuesto a una amenaza, correspondiente a su predisposición intrínseca a ser afectado o ser susceptible de sufrir pérdida. En un sistema puede ser aprovechada para violar el comportamiento deseado del mismo relativo a la protección, seguridad, confiabilidad, confidencialidad, disponibilidad e integridad de la información.
- **Seguridad de la Información**: Conjunto de medidas preventivas y reactivas que permiten asegurar que los activos de información mantengan la confidencialidad, disponibilidad e integridad.
- **Usuario:** Persona que hace uso, o tiene acceso al activo de información, y tiene la responsabilidad de tomar conciencia y adoptar los requisitos de seguridad de la información, definidos y establecidos para los mismos.

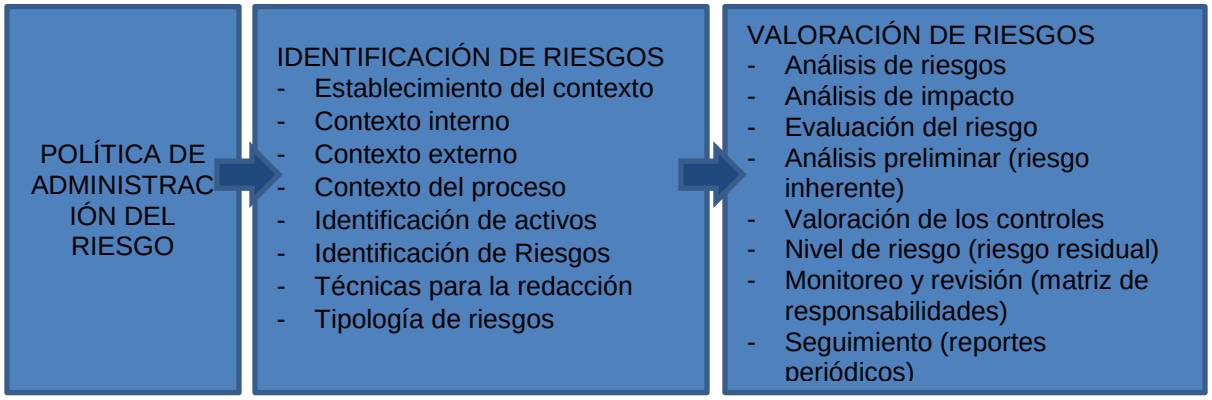
7. DESARROLLO DEL PLAN

La Gestión de riesgos en la superintendencia de Sociedades está enmarcada en el documento GC-G-002 Guía Administración de riesgos Institucionales, Esto, en virtud a la existencia de un Sistema Integrado de Gestión (NTC ISO 9001Gestión de Calidad, NTC ISO/IEC 27001 Sistema de Gestión de la Seguridad de la Información, NTC ISO 14001 sistema de Gestión Ambiental, El Sistema de Gestión de la Seguridad y Salud en el Trabajo (SG-SST), NTC 5906 (Centro de Conciliación y Arbitraje), el Modelo Estándar de Control Interno –MECI- y el Modelo Integrado de Planeación y Gestión definido en el Decreto 1499 de 2017.), que establece la aplicación de esta guía en todos los procesos que conforman el Sistema de Gestión Integrado y aquellos enfoques que involucren la identificación, medición, valoración, tratamiento y seguimiento de riesgos independientemente de si es para un proceso, proyecto, plan, o actividad. Es decir, el uso de un único sistema de gestión de riesgos basado en la norma ISO 31000:2019.

La Superintendencia de Sociedades basa su gestión de riesgos en los siguientes principios:

- La gestión del riesgo es inherente a todas las áreas, procesos y personas que prestan sus servicios a la Entidad.
- A partir de una adecuada gestión de riesgos la Entidad logra sus objetivos estratégicos, cuida la salud e integridad física de las personas, protege sus activos, imagen, información y mitiga su afectación al medio ambiente.
- La gestión de riesgos apoya la toma de decisiones, por ello se requiere que esta arroje información de excelente calidad.
- La Entidad actualiza y mejora constantemente el proceso para la gestión de riesgos utilizando sistemas de información eficientes.
- La Superintendencia de Sociedades reconoce, valora y respeta la diversidad y dignidad de las personas y por ello las involucra sin distingos en la gestión y mejoramiento continuo del proceso de administración de riesgos.

El proceso para la gestión de Riesgos en la Superintendencia de Sociedades, se encuentra alineada con la norma ISO 31000 y las guías emitidas por el Departamento Administrativo de la Función Pública. El proceso contempla las etapas de:

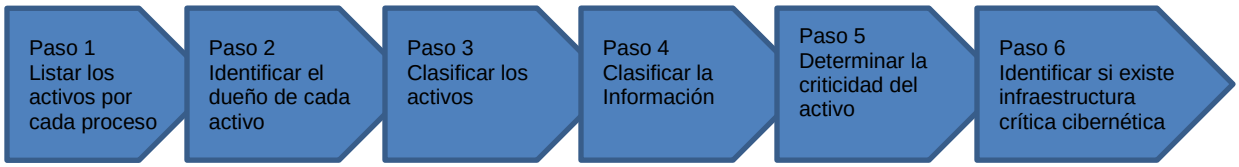


Para los riesgos de Seguridad de la Información, la guía GC-G-002 Guía Administración del Riesgo, determina las siguientes etapas:

Identificación de los activos de seguridad de la información:

Es responsabilidad de la primera línea de defensa identificar los activos de seguridad de la información en cada proceso. Dichos activos son los elementos que utiliza la Entidad para funcionar en el entorno digital tales como: aplicaciones, servicios web, redes, información física o digital, tecnologías de información (TI), tecnologías de operación (TO).

Para identificar los activos de seguridad de la información se requiere aplicar los siguientes pasos:



Identificación del riesgo de seguridad digital

En materia de seguridad digital se conocen tres tipos de riesgo: pérdida de confidencialidad, pérdida de la integridad y pérdida de la disponibilidad de los activos, que se aplican a cada activo.

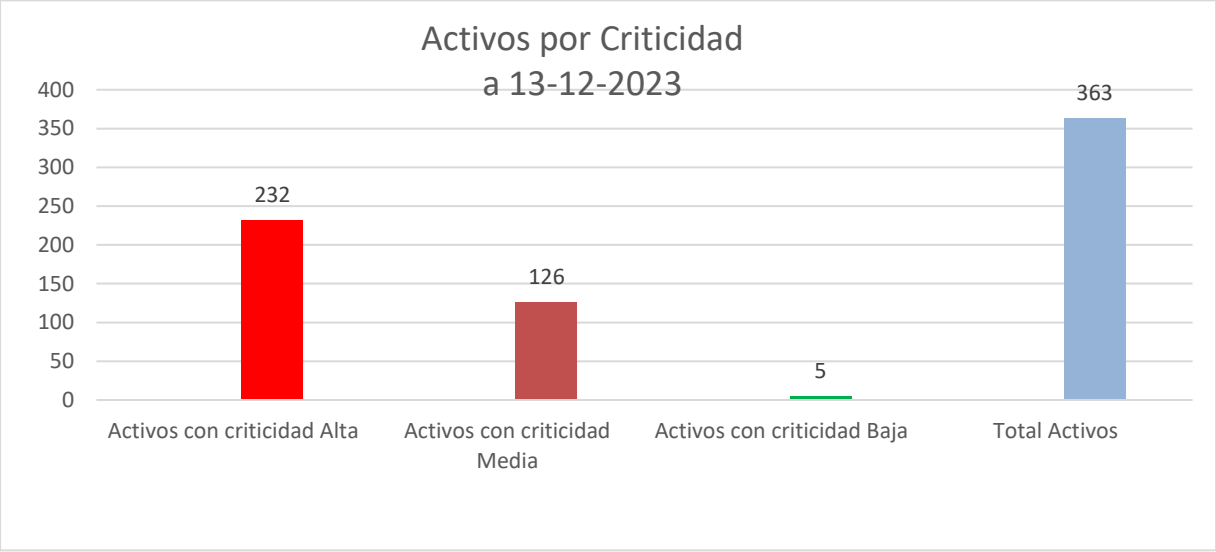
Activo	Riesgo	Descripción del riesgo	Amenaza	Tipo Riesgo	Causa/ Vulnerabilidad	Consecuencia

Estas variables, se tramitan acorde con las actividades a seguir para la identificación del riesgo existente en el documento GC-I-002 Instructivo para la gestión de riesgos de seguridad de la información, documento que enlaza los lineamientos de la guía GC-G-002 Guía Administración del Riesgo con el registro del riesgo en el sistema "Riesgos y Auditoria"

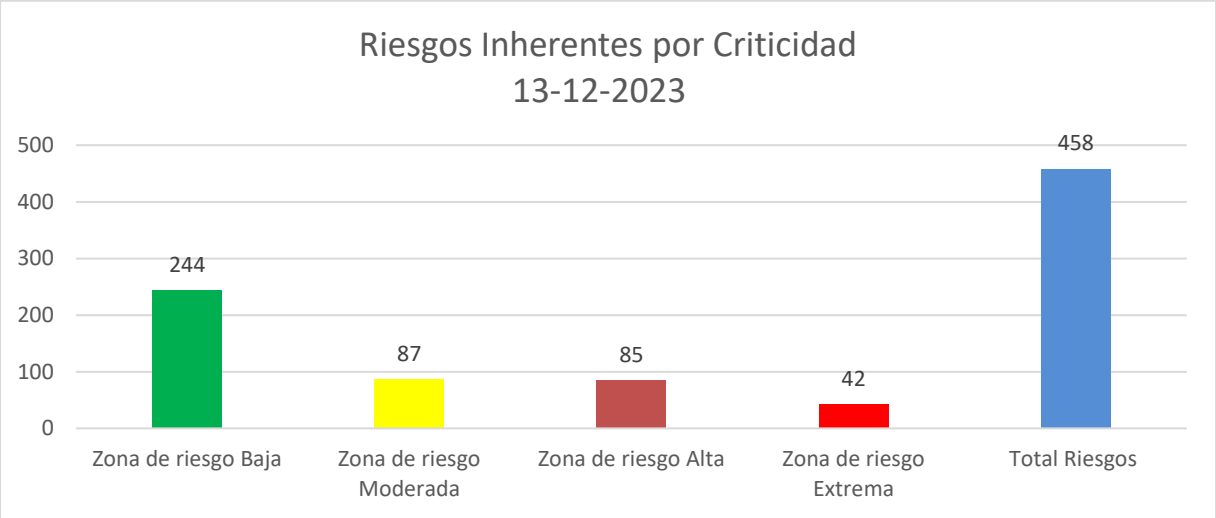
El proceso, se soporta en el aplicativo de gestión de riesgos denominado "Riesgos y Auditoria", el cual permite gestionar los riesgos de corrupción y de gestión para todos los procesos y sistemas de gestión. Los riesgos de Seguridad de la información se encuentran incluidos dentro del módulo de riesgos de gestión.

Durante el año 2023, se actualizaron y registraron en el aplicativo los activos de información, sus riesgos y los controles asociados que pueden mitigar su materialización. Como resultado de estas actividades de registro y valoración del riesgo de seguridad de la información, es necesario, indicar que dentro del proceso de gestión de riesgos que se ha venido implementando, a diciembre de 2023 se han **identificado y gestionado** para los 26 procesos y las 6 intendencias, los siguientes riesgos de seguridad de la información y/o seguridad digital, sobre los activos de información (Hardware, software, redes, datos, personal, instalaciones, servicios internos, proveedores, soportes de información, equipamiento auxiliar), riesgos que deben actualizarse.

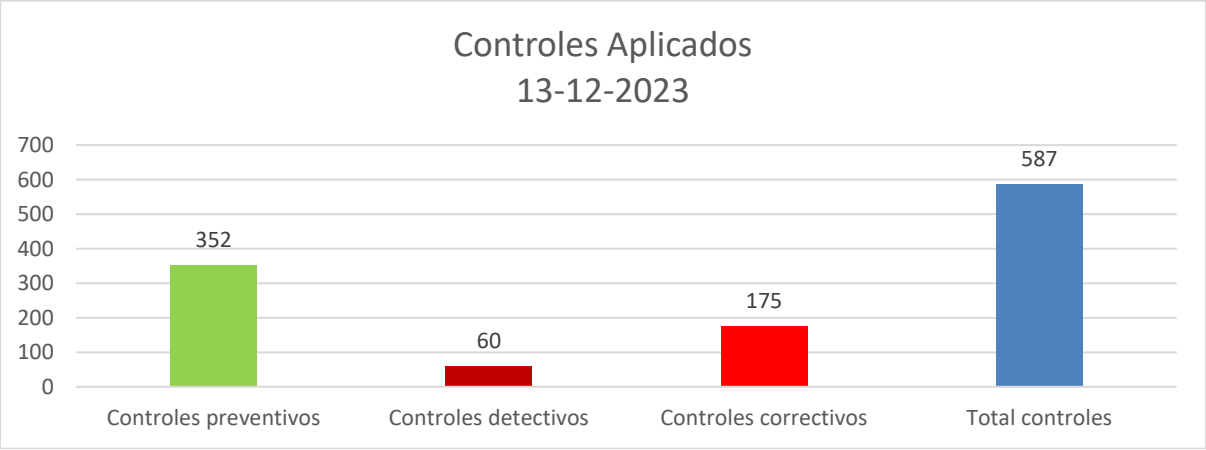
- Se han registrado 386 activos de información que acorde con su valoración (criticidad alta, criticidad media y criticidad baja), presentan la siguiente situación:



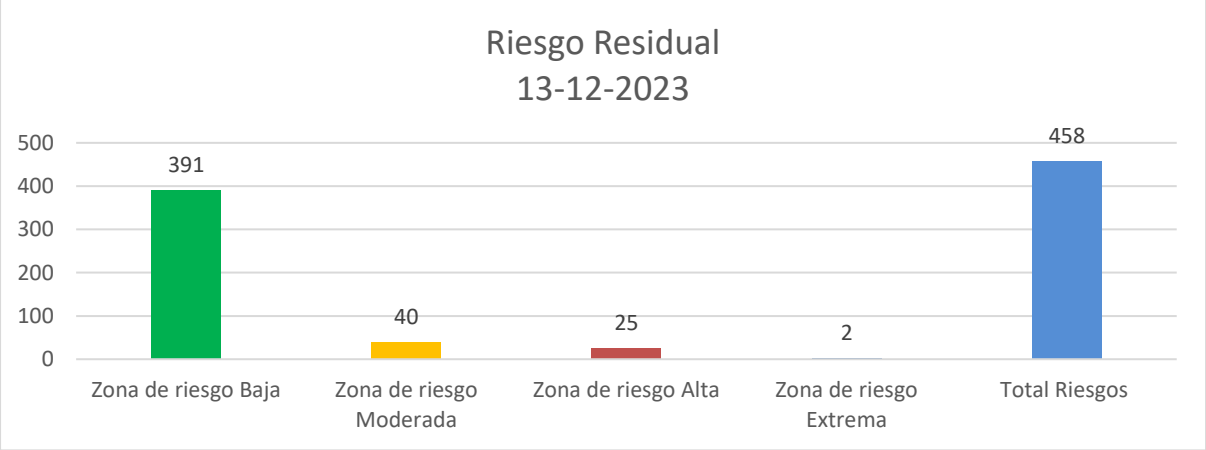
Sobre estos activos de información, los funcionarios encargados del riesgo en los procesos e intendencias han incluido en el sistema los riesgos de seguridad de la información (458), que han sido aprobados. La siguiente gráfica nos indica los riesgos por criticidad, acorde con la valoración definida por los procesos e intendencias:



Para mitigar estos riesgos, los funcionarios encargados del riesgo en los procesos e intendencias han incluido en el sistema los controles y medidas de seguridad, requeridos para disminuir estos riesgos, discriminados en controles preventivos, detectivos y correctivos.



Una vez aplicados estos controles, la situación encontrada de riesgo residual es la siguiente:



Como se refleja en las gráficas anteriores, los procesos e intendencias han realizado una buena gestión de riesgos, ya que, en zona de riesgo alta y extrema, tan solo han quedado 27 riesgos que corresponde a un 5.89%. sobre los cuales hay que continuar realizando gestión.
Para el año 2024, se debe iniciar con la transición de la norma ISO 27001:2013 a la versión de ISO27001:2022, en la cual se realizaron cambios en la identificación de los controles. Esto genera que el aplicativo sea modificado en lo referente a la selección de controles.

7.1 REVISIÓN Y ACTUALIZACIÓN DE ACTIVOS DE INFORMACIÓN

7.1.1 Determinación de gestores de Riesgos

En esta fase se buscará la actualización del grupo de trabajo para la gestión de riesgos, y se confirmará con los líderes de los procesos e intendencias incluidos en el alcance del SGSI de la Superintendencia de Sociedades, el funcionario designado como gestor de riesgos. que posiblemente haya cambiado por actualización de la estructura o de la planta de personal. Se enviarán las comunicaciones correspondientes para la definición de los gestores de riesgos para cada proceso e Intendencia.

7.1.2 Programación y Agendamiento de Entrevistas con gestores de Riesgos

Una vez conocidos los gestores de riesgos de los procesos e intendencias, se programa la agenda de entrevistas para la revisión de los activos de información y actualización en el sistema de Riesgos y Auditoria.

7.2 REVISIÓN Y ACTUALIZACIÓN DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN.

7.2.1 Desarrollar y ejecutar plan de reuniones con gestores de riesgos.

Conocidos los activos de información, se desarrolla un plan de trabajo para realizar la actualización en el sistema de Riesgos y Auditoria, mediante el análisis de riesgos, su valoración, su tratamiento y registro en el sistema.

7.2.2 Aprobación de los riesgos definidos sobre los activos de Información.

Ingresados los riesgos, su valoración y tratamiento en el sistema de riesgo y auditoria, se tramita por medio de este sistema la revisión por parte del asesor asignado por la Oficina Asesora de Planeación y el envío a aprobación por parte del líder del proceso.

7.2.3 Emisión de mapas de riesgos de seguridad de la Información.

Con la aprobación de los riesgos ya se pueden emitir los informes de riesgos que se requieran y los mapas de riesgo por cada proceso. Con esta información se puede consolidar los riesgos de Seguridad de la Información para la Superintendencia de sociedades.

7.3 MONITOREO DE LOS RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA

INFORMACIÓN.

7.3.1 Desarrollar y ejecutar plan de reuniones con gestores de riesgos para monitoreo de cumplimiento de los controles asignados que mitigan los riesgos.

Una vez gestionados los riesgos en el sistema de Riesgos y Auditoria, es necesario y mandatorio, realizar una revisión de los controles asignados a cada riesgo para verificar su eficacia y/o encontrar desviaciones de los mismos, con el fin de mejorarlos.

7.3.2 Determinar evidencias de cumplimiento de los controles.

Para cada control una vez determinadas las evidencias de cumplimiento, deben registrarse en el sistema de Riesgos y Auditoria, como confirmación de la revisión y monitoreo de los riesgos de seguridad de la información. Monitoreo que es revisado por el asesor de riesgos de la Oficina Asesora de Planeación y por la Oficina de Control Interno.

8. CRONOGRAMA

ACTIVIDAD	RESPONSABLE(S)	FECHA DE INICIO	FECHA FIN
Determinación de gestores de riesgos en los procesos y en las intendencias	Oficina Asesora de Planeación. Coordinación de seguridad e Informática Forense	01/02/2024	15/02/2024
Desarrollar plan de reuniones con gestores de riesgos de procesos e intendencias para revisión de los activos de información, riesgos asociados y controles, en sistema de Riesgos y Auditoria	Coordinación de seguridad e Informática Forense Gestores de riesgos de procesos	19-02-2024	29-02-2024
Desarrollar y ejecutar plan de reuniones con gestores de riesgos de procesos e intendencias para actualización de activos de información, riesgos y controles en sistema de Riesgos y Auditoria	Coordinación de seguridad e Informática Forense Gestores de riesgos de procesos	01-03-2024	31-08-2024
Desarrollar y ejecutar plan de reuniones con gestores de riesgos de procesos e intendencias para determinar evidencias que comprueben la eficacia de la aplicación de los controles definidos para la mitigación de los riesgos e ingresarlas al sistema de Riesgos y Auditoria.	Coordinación de seguridad e Informática Forense Gestores de riesgos de procesos	01/5/2024	10/12/2024
Apoyar el ingreso de las evidencias en el sistema de Riesgos y Auditoria.	Coordinación de seguridad e Informática	01/08/2024	10/12/2024

	Forense Gestores de riesgos de procesos		

9. RECURSOS

El desarrollo de las actividades estará sujeto a la disponibilidad de recursos (humanos y , tecnológicos) que faciliten el cumplimiento de las actividades.

RECURSO	DESCRIPCIÓN
Humano	Profesionales de la Oficina Asesora de Planeación Profesionales de la Coordinación de Seguridad e informática Forense Gestores de Riesgo de los procesos Líderes de Proceso e Intendentes Contratista
Tecnológicos	Aplicativos, sistemas y aplicaciones para la gestión de los riesgos de seguridad y privacidad de la información (entre ellos el Aplicativo Riesgos y Auditoría, correo electrónico, TEAMS, sharepoint, entre otros).
Normativos y reglamentarios	Guías, Modelos, Políticas, Sistemas de Gestión, etc, que orientan la gestión e implementación de los riesgos de seguridad y privacidad de la información.

10. SEGUIMIENTO Y MEDICIÓN

La oficina asesora de Planeación realiza control a la gestión de riesgos de seguridad de la información y emite concepto de cumplimiento de las tareas definidas para el cumplimiento del presente plan.
La oficina de Control interno realiza revisión del cumplimiento del monitoreo de los riesgos y controles y conceptúa acerca de las evidencias registradas en el sistema de Riesgos y Auditoria, así como de las fechas de cumplimiento de monitoreo de los controles.
Con la información registrada en el sistema de Riesgos y Auditoria pueden emitirse indicadores por proceso, por riesgos de seguridad de la información o consolidados a nivel entidad.
La eficacia de la Gestión de riesgos puede medirse con un indicador “Riesgos de Seguridad digital y seguridad de la información mitigados” que está orientado principalmente a disminuir el número de riesgos identificados con nivel alto y extremo, a través de la implementación de controles asociados al cumplimiento de la Norma ISO 27001:2013.

$$\frac{\text{Número de Riesgos Residuales con nivel no aceptable}}{\text{Total de riesgos de Seguridad de la Información}}$$

Este indicador puede establecerse a cualquier nivel institucional que se requiera, con información del sistema de Riesgos y Auditoria.