Superintendencia de Sociedades

PLAN DE TRATAMIENTO DE RIESGOS 2026

TABLA DE CONTENIDO

1. Introducción (Opcional)

El panorama global actual, caracterizado por una acelerada transformación digital, la adopción generalizada de servicios en la nube, la automatización de procesos y el uso intensivo de inteligencia artificial (IA), ha consolidado la seguridad y privacidad de la información como riesgos estratégicos para las organizaciones públicas y privadas. Informes recientes de organismos multilaterales y firmas especializadas evidencian un incremento sostenido en la frecuencia, sofisticación y el impacto de los incidentes cibernéticos, posicionando los riesgos digitales entre las principales amenazas globales para la estabilidad institucional, económica y social.

Para el año 2026, este contexto se ha intensificado por la expansión de tecnologías emergentes como la inteligencia artificial generativa, el Internet de las Cosas (IoT), los entornos híbridos y multinube, la automatización robótica de procesos (RPA) y los avances en computación cuántica. Estas tecnologías, aunque habilitan mejoras en eficiencia y prestación de servicios digitales, amplían la superficie de ataque y potencian las capacidades de actores maliciosos mediante automatización de ataques, ingeniería social avanzada, uso de deepfakes y evasión de controles de seguridad.

En América Latina y el Caribe, los incidentes y los intentos de intrusión continúan en crecimiento, con incrementos anuales superiores al 50 %, afectando principalmente a entidades gubernamentales, financieras y de infraestructura crítica. En Colombia, el sector público ha sido identificado como un objetivo prioritario, evidenciando la necesidad de fortalecer las capacidades institucionales en gestión de riesgos digitales, ciberresiliencia y continuidad del negocio, en concordancia con la Política de Gobierno Digital, el Modelo Integrado de Planeación y Gestión (MIPG) y el Modelo de Seguridad y Privacidad de la Información (MSPI).

El contexto nacional evidencia una diversificación de vectores de ataque, incluyendo campañas avanzadas de phishing y spear phishing, suplantación de identidad digital, ataques de ransomware, denegación distribuida de servicios (DDoS), explotación de vulnerabilidades en infraestructuras críticas, compromisos de cuentas privilegiadas y ataques a la cadena de suministro tecnológica. Asimismo, se observa un incremento en ataques dirigidos a plataformas en la nube, proveedores externos y servicios compartidos, lo que incrementa los riesgos sistémicos y transversales para las entidades públicas.

La Superintendencia de Sociedades, en su calidad de entidad de inspección, vigilancia y control, administra información estratégica y sensible para el Estado, las

empresas y los ciudadanos. La materialización de riesgos de seguridad y privacidad de la información puede afectar la continuidad de las operaciones misionales, el cumplimiento normativo, la integridad de los procesos institucionales y la confianza pública. En este sentido, es fundamental fortalecer de manera continua el Sistema de Gestión de Seguridad de la Información (SGSI), alineado con los requisitos de la norma ISO/IEC 27001:2022, el MSPI del MinTIC, el MIPG, la Política de Gobierno Digital y los lineamientos de la Estrategia Nacional de Ciberseguridad.

La adopción y mantenimiento del estándar ISO/IEC 27001:2022, junto con la aplicación de controles definidos en ISO/IEC 27002:2022, permite a la entidad gestionar de manera sistemática los riesgos de seguridad de la información, estableciendo controles organizacionales, de personas, físicos y tecnológicos, bajo un enfoque basado en riesgo, mejora continua y gobernanza institucional. De manera complementaria, la articulación con marcos de referencia como NIST Cybersecurity Framework (CSF 2.0) e ISO/IEC 22301 fortalece las capacidades de continuidad del negocio y gestión de incidentes.

En este contexto, el Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información constituye una herramienta estratégica para la identificación, análisis, evaluación y tratamiento de los riesgos asociados a los activos de información, incorporando controles preventivos, detectivos y correctivos orientados a garantizar la confidencialidad, integridad y disponibilidad de la información institucional. Su actualización para el año 2026 integra los riesgos emergentes derivados de la transformación digital, la inteligencia artificial, la gestión de datos, la tercerización tecnológica y la interconexión con ecosistemas digitales públicos y privados.

El panorama de la ciberseguridad para 2026 exige un enfoque adaptativo y proactivo, basado en la gestión del riesgo, la ciberresiliencia y la mejora continua. La Superintendencia de Sociedades deberá continuar fortaleciendo sus capacidades mediante la inversión en tecnologías de seguridad, la operación de capacidades de monitoreo y respuesta (SOC), la implementación de controles de prevención de fuga de información (DLP), la gestión de identidades y accesos, la protección de infraestructuras críticas, la capacitación del talento humano y la articulación con entidades del sector TIC y autoridades competentes. El éxito de la gestión de riesgos dependerá de la capacidad institucional para anticipar amenazas, evaluar impactos, implementar controles robustos y garantizar la resiliencia operativa y digital de la entidad.

2. Objetivo General

Fortalecer la gestión integral de los riesgos de Seguridad y Privacidad de la Información en la Superintendencia de Sociedades e Intendencias, mediante la definición, implementación y seguimiento de actividades de prevención, control y mitigación aplicables a los procesos institucionales, en concordancia con la norma ISO/IEC 27001:2022, el Modelo de Seguridad y Privacidad de la Información (MSPI) y la normativa vigente, con el propósito de proteger los activos de información y garantizar la continuidad de las operaciones misionales.

3. Objetivos específicos

- Identificar, analizar y evaluar los riesgos de Seguridad y Privacidad de la Información asociados a los activos, procesos y servicios institucionales, mediante la aplicación de metodologías alineadas con ISO/IEC 27005, MSPI y los lineamientos de gestión del riesgo del MIPG.
- Definir e implementar controles preventivos, detectivos y correctivos de carácter organizacional, técnico y legal, conforme a los controles establecidos en ISO/IEC 27001:2022 e ISO/IEC 27002:2022, para mitigar los riesgos identificados y reducir su impacto sobre la confidencialidad, integridad y disponibilidad de la información.
- Realizar el seguimiento, medición y mejora continua del tratamiento de riesgos, mediante indicadores, auditorías internas y revisiones periódicas del SGSI, con el fin de asegurar la eficacia de los controles implementados, el cumplimiento normativo y la continuidad de las operaciones misionales.
- Promover la sensibilización y capacitación del personal en prácticas y normativas relacionadas con la prevención, control y mitigación de riesgos de Seguridad y Privacidad de la Información.

4. Alcance

El presente Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información, así como los lineamientos para la gestión integral de riesgos, aplican a todos los procesos institucionales, proyectos, sistemas de información, infraestructura tecnológica y sedes de la Superintendencia de Sociedades, incluyendo todas sus Intendencias.

Este alcance involucra a todos los servidores de la Entidad, independientemente de su tipo de vinculación, durante el ejercicio de sus funciones y responsabilidades

relacionadas con el manejo de información y el uso de recursos tecnológicos de la Superintendencia.

El plan contempla acciones específicas orientadas a prevenir, controlar y mitigar la posible materialización de amenazas y ataques informáticos que puedan afectar la confidencialidad, integridad y disponibilidad de la información, así como la continuidad de los servicios, trámites y el cumplimiento de los objetivos misionales de la Superintendencia de Sociedades e Intendencias.

5. Términos y 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.
- 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.
- Vulnerabilidad: 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.

6. Marco normativo

El marco jurídico que sustenta el presente Plan de Seguridad y Privacidad de la Información se encuentra debidamente articulado con la caracterización del proceso de Gestión Integral, específicamente en el apartado de Normograma, el cual consolida y actualiza las disposiciones legales, reglamentarias y normativas aplicables a la entidad. Dicho normograma constituye el referente oficial para la identificación, seguimiento y cumplimiento de los requisitos jurídicos en materia de seguridad de la información, protección de datos personales, transparencia, gobierno digital y control interno, y se encuentra disponible para su consulta en el repositorio institucional, a través del siguiente enlace: https://www.supersociedades.gov.co/documents/107391/3473426/02_NormogramaIntegral.xlsx.

7. Principales Actividades

La Gestión de riesgos en la superintendencia de Sociedades está enmarcada en el documento GIN-GU-002 Guía Administración de riesgos Institucionales, esto, en virtud a la existencia de un Sistema Integrado de Gestión, 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.

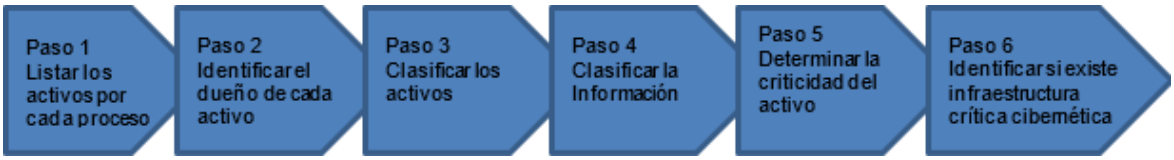
El proceso para la gestión de Riesgos en la Superintendencia de Sociedades se encuentra alineada con las guías emitidas por el Departamento Administrativo de la Función Pública y contempla las etapas de:

Para los riesgos de Seguridad de la Información, la guía GIN-GU-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.

Estas variables, se tramitan acorde con las actividades a seguir para la identificación del riesgo existente en el documento la guía GIN-GU-002 Guía Administración del Riesgo.

8. Evaluación y seguimiento del plan

Objetivo Estratégico	Actividad	Producto	Indicador	Meta	Responsable	Fecha inicio	Fecha fin
Fortalecer la gestión integral del riesgo	Actualizar la metodología de gestión de riesgos acorde a la guía de DAFP expedida en 2025	Guía de gestión de riesgos actualizada	Metodología aprobada	1 documento actualizado	Oficial de Seguridad	1/02/2026	1/04/2026
Fortalecer la gestión integral del riesgo	Actualizar el inventario de activos de información	Inventario actualizado	% activos identificados	≥95%	DTIC / Oficial Seguridad	1/02/2026	1/04/2026
Fortalecer la gestión integral del riesgo	Realizar análisis y valoración de riesgos institucionales	Matriz de riesgos actualizada	Riesgos evaluados	100% procesos	Oficial de Seguridad	1/06/2026	1/07/2026
Fortalecer la gestión integral del riesgo	Definir y aprobar el Plan de Tratamiento de Riesgos	PTR aprobado	Plan aprobado	1 plan aprobado y publicado	Oficial de Seguridad	20/01/2026	31/01/2026
Fortalecer la gestión integral del riesgo	Ejecutar el plan de seguridad y privacidad de la información	Controles implementados	% controles implementados plan de SPI ejecutado	≥80%	DTIC / Oficial Seguridad	1/03/2026	31/12/2026

Objetivo Estratégico	Actividad	Producto	Indicador	Meta	Responsable	Fecha inicio	Fecha fin
Fortalecer la gestión integral del riesgo	Implementar controles organizacionales (políticas, procedimientos, SoA)	Documentos aprobados	Documentos actualizados	≥5 documentos actualizados y/o creados que se relaciones a seguridad de la información	Oficial de Seguridad	1/03/2026	1/09/2026
Fortalecer la gestión integral del riesgo	Capacitar al personal en riesgos y seguridad de la información	Registros de capacitación	% funcionarios capacitados	≥80%	Oficial de Seguridad	1/05/2026	1/11/2026
Fortalecer la gestión integral del riesgo	Realizar pruebas de recuperación de desastres (DRP)	Informes de pruebas	Pruebas ejecutadas a los elementos indicados y planeados para 2026	≥1 prueba anual de los elementos contenidos en el DRP	DTIC	1/05/2026	1/11/2026
Fortalecer la gestión integral del riesgo	Auditoría interna del SGSI y riesgos	Informe auditoría	Auditoría realizada	1 auditoría	OAP	1/10/2026	1/11/2026
Fortalecer la gestión integral del riesgo	Revisión por la Dirección del SGSI	Acta revisión	Revisión realizada	1 sesión	Alta Dirección	1/04/2026	15/05/2026