Superintendencia de Sociedades

Plan de Seguridad y Privacidad de la Información 2026

Contenido

1. Introducción

En un entorno caracterizado por la acelerada transformación digital y el uso intensivo de las tecnologías de la información y las comunicaciones, la información se consolida como uno de los activos estratégicos más relevantes para las organizaciones públicas. Este contexto incrementa de manera significativa la exposición a riesgos y amenazas de seguridad digital, tales como accesos no autorizados, fugas de información, indisponibilidad de servicios y vulneraciones a la privacidad de los datos, lo cual exige la adopción de enfoques sistemáticos, integrales y actualizados para su gestión.

En respuesta a este escenario, el **Modelo de Seguridad y Privacidad de la Información (MSPI)**, definido por el Ministerio de Tecnologías de la Información y las Comunicaciones, constituye el marco de referencia para que las entidades del Estado implementen y fortalezcan un Sistema de Gestión de Seguridad y Privacidad de la Información, articulado con la Política de Gobierno Digital y basado en buenas prácticas internacionales. El MSPI orienta la identificación, análisis, tratamiento y seguimiento de los riesgos que afectan los activos de información y la infraestructura crítica cibernética, promoviendo una gestión preventiva, reactiva y proactiva de la seguridad digital.

El MSPI adopta un enfoque integral que combina controles tecnológicos, organizacionales, procedimentales y humanos, permitiendo a las entidades prevenir, detectar, responder y recuperarse frente a incidentes de seguridad de la información y seguridad digital. Asimismo, su estructura se fundamenta en el ciclo de mejora continua (Planear, Hacer, Verificar y Actuar – PHVA), lo que garantiza la revisión permanente de políticas, procesos y controles, de acuerdo con la evolución de los riesgos, los cambios tecnológicos y los requerimientos normativos aplicables.

Este conjunto de lineamientos, políticas, procedimientos y controles está orientado a salvaguardar los principios fundamentales de la seguridad de la información: **confidencialidad**, asegurando que la información sea accesible únicamente a personas autorizadas; **integridad**, garantizando su exactitud, completitud y protección frente a alteraciones no autorizadas; y **disponibilidad**, asegurando el acceso oportuno a la información y a los servicios que la soportan cuando sean requeridos. De igual forma, el

MSPI incorpora de manera transversal la protección de los datos personales, en cumplimiento de la normativa vigente en materia de habeas data y derecho de acceso a la información pública.

Adicionalmente, el MSPI se caracteriza por su flexibilidad y adaptabilidad, lo que permite a cada entidad ajustar su implementación de acuerdo con su contexto institucional, tamaño, nivel de madurez digital, sector y naturaleza de sus procesos misionales, estratégicos y de apoyo. Esta característica resulta esencial para fortalecer la resiliencia organizacional frente a un entorno de amenazas cada vez más dinámico y a un marco regulatorio en constante actualización, como el establecido mediante la Resolución 2277 de 2025, que actualiza los lineamientos del habilitador de Seguridad y Privacidad de la Información de la Política de Gobierno Digital.

En este sentido, el MSPI se consolida como una herramienta estratégica para apoyar a las entidades públicas en la gestión responsable, segura y transparente de la información, contribuyendo no solo a la protección de los activos institucionales y al cumplimiento normativo, sino también al fortalecimiento de la confianza de la ciudadanía, los grupos de interés y los entes de control, garantizando la continuidad de los servicios, la generación de valor público y el cumplimiento de la misión institucional.

2. Objetivo General

Gestionar de manera integral y sistemática los riesgos asociados a la seguridad y privacidad de la información, mediante la implementación, operación y mejora continua del Sistema de Gestión de Seguridad de la Información (SGSI), con el fin de preservar la confidencialidad, integridad y disponibilidad de los activos de información en cumplimiento del marco normativo y las buenas prácticas aplicables.

3. Objetivos Específicos

1. Identificar, analizar y tratar de manera sistemática los riesgos de seguridad y privacidad de la información, considerando los activos de información, los procesos institucionales, la infraestructura tecnológica y el contexto interno y externo de la entidad.
2. Implementar y mantener controles de seguridad de la información y seguridad digital, de tipo organizacional, técnico y procedimental, que permitan proteger la confidencialidad, integridad y disponibilidad de la información frente a amenazas y vulnerabilidades.
3. Fortalecer la gestión de incidentes de seguridad de la información y la continuidad del negocio, asegurando la capacidad institucional de prevenir, responder y recuperarse oportunamente ante eventos que afecten la operación y los servicios críticos.
4. Garantizar el cumplimiento del marco normativo y regulatorio aplicable, en materia de seguridad de la información, protección de datos personales, transparencia y gobierno digital, incorporando dichos requisitos en las políticas, procedimientos y controles institucionales.
5. Promover la mejora continua y la cultura organizacional de seguridad y privacidad de la información, mediante el seguimiento a indicadores, la realización de auditorías, la sensibilización del talento humano y la adopción de acciones correctivas y preventivas.

4. Alcance

Un Sistema de Gestión de Seguridad de la Información (SGSI) tiene como propósito establecer un marco integral para gestionar de manera efectiva la seguridad de la información dentro de cualquier organización. El SGSI tiene como objetivo principal proteger la confidencialidad, integridad y disponibilidad de la información, asegurando que los activos de información estén resguardados contra amenazas y vulnerabilidades.

Por lo anterior en la Superintendencia de Sociedades específicamente con el SGSI busca:

1. Evaluar y tratar los riesgos relacionados con la seguridad de la información mediante un proceso continuo de identificación, análisis y mitigación de amenazas potenciales.

2. Asegurar el cumplimiento de todas las leyes, regulaciones y normas aplicables en materia de seguridad de la información emitidas por el Ministerio de Tecnologías de la Información y Comunicaciones, Superintendencia de Industria y Comercio y demás entes reguladores, así como con los requisitos contractuales y reglamentarios pertinentes.

3.Implementar controles adecuados para salvaguardar la información contra accesos no autorizados, alteraciones, divulgaciones, destrucciones o pérdidas.

4. Desarrollar y mantener planes de continuidad del negocio y de recuperación ante desastres que permitan la resiliencia operativa y la rápida recuperación de servicios críticos.

5. Promover la concienciación y la formación continua en seguridad de la información entre todos los empleados y partes interesadas, fortaleciendo una cultura organizacional que valore y practique la seguridad en todas sus actividades.

6. Establecer un proceso de mejora continua del SGSI mediante la revisión regular de políticas, procedimientos y controles, adaptándolos a las nuevas amenazas y cambios en el entorno operativo y tecnológico.

7. Establecer roles y responsabilidades claras en la gestión de la seguridad de la información, garantizando la rendición de cuentas y la transparencia en todas las acciones y decisiones relacionadas con la seguridad.

5. Términos y Definiciones

- **Acceso a la Información Pública:** Derecho fundamental consistente en la facultad que tienen todas las personas de conocer sobre la existencia y acceso a la información pública en posesión o bajo control de sujetos obligados. (Ley 1712 de 2014, art 4)
- **Activo de información:** En relación con la seguridad de la información, se refiere a cualquier información o elemento relacionado con el tratamiento de ésta (sistemas, soportes, edificios, personas, etc.) que tenga valor para la organización. (ISO/IEC 27000).
- **Activos de Información y recursos:** se refiere a elementos de hardware y de software de procesamiento, almacenamiento y comunicaciones, bases de datos y procesos,

procedimientos y recursos humanos asociados con el manejo de los datos y la información misional, operativa y administrativa de cada entidad, órgano u organismo. (CONPES 3854 de 2016).

- **Archivo:** Conjunto de documentos, sea cual fuere su fecha, forma y soporte material, acumulados en un proceso natural por una persona o entidad pública o privada, en el transcurso de su gestión, conservados respetando aquel orden para servir como testimonio e información a la persona o institución que los produce y a los ciudadanos, o como fuentes de la historia. También se puede entender como la institución que está al servicio de la gestión administrativa, la información, la investigación y la cultura. (Ley 594 de 2000, art 3)
- **Amenazas:** Causa potencial de un incidente no deseado, que puede provocar daños a un sistema o a la organización. (ISO/IEC 27000).
- **Análisis de Riesgo:** Proceso para comprender la naturaleza del riesgo y determinar el nivel de dicho riesgo. (ISO/IEC 27000).
- **Auditoría:** Proceso sistemático, independiente y documentado para obtener evidencias de auditoría y obviamente para determinar el grado en el que se cumplen los criterios de auditoría. (ISO/IEC 27000).
- **Autorización:** Consentimiento previo, expreso e informado del Titular para llevar a cabo el Tratamiento de datos personales (Ley 1581 de 2012, art 3)
- Bases de Datos Personales: Conjunto organizado de datos personales que sea objeto de Tratamiento (Ley 1581 de 2012, art 3)
- **Ciberseguridad:** Protección de activos de información, mediante el tratamiento de las amenazas que ponen en riesgo la información que se procesa, almacena y transporta mediante los sistemas de información que se encuentran interconectados.
- **CERT:** (Computer Emergency Response Team) Equipo de Respuesta a Emergencias cibernéticas, por su sigla en inglés. Es el equipo que dispone de la capacidad centralizada para la coordinación de gestión de incidentes de seguridad digital.
- **Ciberespacio:** Red interdependiente de infraestructuras de tecnología de la información que incluye Internet, redes de telecomunicaciones, sistemas informáticos, procesadores y controladores integrados en industrias. (art. 2.2.21.1.1.3. del, Decreto 1078 de 2015).

- **Ciberdefensa:** Capacidad del Estado para prevenir y contrarrestar toda amenaza o incidente de naturaleza cibernética que afecte la sociedad, la soberanía nacional, la independencia, la integridad territorial, el orden constitucional y los intereses nacionales. Implica el empleo de las capacidades militares ante amenazas cibernéticas, ataques cibernéticos o ante actos hostiles de naturaleza cibernética.
- **CSIRT:** (Computer Security Incident & Response Team) Equipo de Respuesta a Incidentes de Seguridad Cibernética, por su sigla en inglés. Es el equipo que provee las capacidades de gestión de incidentes a una organización/sector en especial. Esta capacidad permitir minimizar y controlar el daño resultante de incidentes, proveyendo la respuesta, contención y recuperación efectiva, así como trabajar en pro de prevenir la ocurrencia de futuros incidentes.
- **CSIRT sectorial:** Son los equipos de respuesta a incidentes de cada uno de los sectores, para el adecuado desarrollo de sus actividades económicas y sociales, a partir del uso de las tecnologías de la información y las comunicaciones.
- **CSIRT sectorial crítico:** Son los equipos de respuesta a incidentes sectoriales de cada uno de los sectores identificados como críticos.
- **Control:** Las políticas, los procedimientos, las prácticas y las estructuras organizativas concebidas para mantener los riesgos de seguridad de la información por debajo del nivel de riesgo asumido. Control es también utilizado como sinónimo de salvaguarda o contramedida. En una definición más simple, es una medida que modifica el riesgo.
- **Datos Abiertos:** Son todos aquellos datos primarios o sin procesar, que se encuentran en formatos estándar e interoperables que facilitan su acceso y reutilización, los cuales están bajo la custodia de las entidades públicas o privadas que cumplen con funciones públicas y que son puestos a disposición de cualquier ciudadano, de forma libre y sin restricciones, con el fin de que terceros puedan reutilizarlos y crear servicios derivados de los mismos Ley 1712 de 2014.
- **Datos Personales:** Cualquier información vinculada o que pueda asociarse a una o varias personas naturales determinadas o determinables. (Ley 1581 de 2012, art 3)
- **Datos Personales Públicos:** Es el dato que no sea semiprivado, privado o sensible. Son considerados datos públicos, entre otros, los datos relativos al estado civil de las personas, a su profesión u oficio y a su calidad de comerciante o de servidor público.

Por su naturaleza, los datos públicos pueden estar contenidos, entre otros, en registros públicos, documentos públicos, gacetas y boletines oficiales y sentencias judiciales debidamente ejecutoriadas que no estén sometidas a reserva. (Decreto 1377 de 2013, art 3)

- **Datos Personales Privados:** Es el dato que por su naturaleza íntima o reservada sólo es relevante para el titular. (Ley 1581 de 2012, art 3 literal h)
- **Datos Personales Mixtos:** Para efectos de este documento es la información que contiene datos personales públicos junto con datos privados o sensibles.
- **Datos Personales Sensibles:** Se entiende por datos sensibles aquellos que afectan la intimidad del Titular o cuyo uso indebido puede generar su discriminación, tales como aquellos que revelen el origen racial o étnico, la orientación política, las convicciones religiosas o filosóficas, la pertenencia a sindicatos, organizaciones sociales, de derechos humanos o que promueva intereses de cualquier partido político o que garanticen los derechos y garantías de partidos políticos de oposición, así como los datos relativos a la salud, a la vida sexual, y los datos biométricos. (Decreto 1377 de 2013, art 3)
- **Derecho a la Intimidad:** Derecho fundamental cuyo núcleo esencial lo constituye la existencia y goce de una órbita reservada en cada persona, exenta de la intervención del poder del Estado o de las intromisiones arbitrarias de la sociedad, que le permite a dicho individuo el pleno desarrollo de su vida personal, espiritual y cultural (Jurisprudencia Corte Constitucional).
- **Encargado del Tratamiento de Datos:** Persona natural o jurídica, pública o privada, que por sí misma o en asocio con otros, realice el Tratamiento de datos personales por cuenta del responsable del Tratamiento. (Ley 1581 de 2012, art 3)
- **Evento:** Un evento es cualquier suceso observable en un sistema o red, como un usuario que se conecta a un recurso compartido de archivos, un usuario que envía un archivo electrónico o un firewall que bloquea un intento de conexión, entre otros. Igualmente, los eventos adversos, son aquellos que tienen consecuencias negativas, como fallos en un sistema, usos no autorizados de privilegios en un sistema, acceso no autorizados y ejecución de malware.

- **Defacement:** Ataque sobre un servidor web como consecuencia del cual se cambia su apariencia.
- **DoS / DDoS (Denial of Service / Distributed Denial of Service:** Se entiende como denegación de servicio, en términos de seguridad informática, a un conjunto de técnicas que tienen por objetivo dejar un servidor inoperativo. Mediante este tipo de ataques se busca sobrecargar un servidor y de esta forma no permitir que sus legítimos usuarios puedan utilizar los servicios por prestados por él. El ataque consiste en saturar con peticiones de servicio al servidor, hasta que éste no puede atenderlas, provocando su colapso.
- **Gestión de incidentes de seguridad de la información:** Procesos para detectar, reportar, evaluar, responder, tratar y aprender de los incidentes de seguridad de la información. (ISO/IEC 27000).
- **Gobernanza de la seguridad digital para Colombia:** Corresponde al conjunto de interacciones y enfoques entre las múltiples partes interesadas para identificar, enmarcar, proponer, y coordinar respuestas proactivas y reactivas a posibles amenazas a la confidencialidad, integridad o disponibilidad de los servicios tecnológicos, sistemas de información, infraestructura tecnológica, redes e información que en conjunto constituyen el entorno digital.
- **Incidente:** Un incidente es una violación o amenaza inminente a las políticas de seguridad digital, políticas de uso aceptable y o prácticas de seguridad básicas.
- **Información Pública Clasificada:** Es la que está en poder o custodia de un sujeto obligado pertenece al ámbito propio, particular y privado o semiprivado de una persona natural o jurídica, por lo que su acceso podrá negarse o exceptuarse si se trata de las circunstancias legítimas y necesarias y los derechos particulares o privados consagrados en el artículo 18 de la Ley 1712 de 2014. (Ley 1712 de 2014, art 6)
- **Información Pública Reservada:** Es aquella información que estando en poder o custodia de un sujeto obligado en su calidad de tal, es exceptuada de acceso a la ciudadanía por daño a intereses públicos y bajo cumplimiento de la totalidad de los requisitos consagrados en el artículo 19 de la Ley 1712 de 2014. (Ley 1712 de 2014, art 6).

- **Ingeniería social:** Son técnicas basadas en engaños que se emplean para dirigir la conducta de una persona u obtener información sensible. El afectado es inducido a actuar de determinada forma (pulsar en enlaces, introducir contraseñas, visitar páginas, etc.) convencido de que está haciendo lo correcto cuando realmente está siendo engañado por el ingeniero social.
- **Inyección de ficheros remota:** Estado de vulnerabilidad que se crea por métodos de codificación poco seguros, y que tiene como resultado una validación de entradas inapropiada, que permite a los atacantes transferir código malicioso al sistema subyacente a través de una aplicación web.
- **Inyección SQL:** Tipo de ataque a sitios web basados en bases de datos. Una persona malintencionada ejecuta comandos SQL no autorizados aprovechando códigos inseguros de un sistema conectado a Internet. Los ataques de inyección SQL se utilizan para robar información normalmente no disponible de una base de datos o para acceder a las computadoras host de una organización mediante la computadora que funciona como servidor de la base de datos.
- **Incidente de seguridad digital - Ciberincidente:** Ocurrencia de una situación que pone en peligro la confidencialidad, integridad o disponibilidad de un sistema de información o la información que el sistema procesa, almacena o transmite; o que constituye una violación a las políticas de seguridad, procedimientos de seguridad o políticas de uso aceptable.
- **Infraestructura crítica cibernética:** Sistemas y activos, físicos o virtuales, soportados por Tecnologías de la Información y las Comunicaciones, cuya afectación significativa tendría un impacto grave en el bienestar social o económico de los ciudadanos, o en el funcionamiento efectivo del gobierno o la economía.
- **Ley de Habeas Data:** Se refiere a la Ley Estatutaria 1266 de 2008.
- **Ley de Transparencia y Acceso a la Información Pública:** Se refiere a la Ley Estatutaria 1712 de 2014.
- **Mecanismos de protección de datos personales:** Lo constituyen las distintas alternativas con que cuentan las entidades destinatarias para ofrecer protección a los datos personales de los titulares tales como acceso controlado, anonimización o cifrado.

- **Modelo de Gobernanza de Seguridad digital:** Es el esquema de trabajo compuesto por un conjunto de políticas de operación, principios, normas, reglas, procedimientos de toma de decisiones y programas compartidos por las múltiples partes interesadas de la seguridad digital del país, con el fin de fortalecer las capacidades para la gestión de riesgos e incidentes de seguridad digital y para la respuesta proactiva y reactiva a posibles amenazas a la confidencialidad, integridad o disponibilidad de los servicios tecnológicos, sistemas de información, infraestructura tecnológica y las redes e información que, en conjunto, constituyen el entorno digital en el país.
- **Múltiples partes interesadas:** Corresponde al conjunto de actores que dependen del entorno digital para todas o algunas de sus actividades, económicas y sociales. Comprende a las autoridades, las organizaciones privadas, los operadores o propietarios de las infraestructuras críticas cibernéticas nacionales, los prestadores de servicios esenciales, la academia y la sociedad civil.
- **Partes interesadas (Stakeholder):** Persona u organización que puede afectar a, ser afectada por o percibirse a sí misma como afectada por una decisión o actividad.
- **Pharming:** Ataque informático que consiste en modificar o sustituir el archivo del servidor de nombres de dominio cambiando la dirección IP legítima de una entidad (comúnmente una entidad bancaria) de manera que en el momento en el que el usuario escribe el nombre de dominio de la entidad en la barra de direcciones, el navegador redirigirá automáticamente al usuario a otra dirección IP (Internet Protocol) donde se aloja una web(página) falsa que suplantará la identidad legítima de la entidad, obteniéndose de forma ilícita las claves de acceso de los clientes la entidad.
- **Plan de continuidad del negocio:** Plan orientado a permitir la continuación de las principales funciones misionales o del negocio en el caso de un evento imprevisto que las ponga en peligro. (ISO/IEC 27000).
- **Plan de tratamiento de riesgos:** Documento que define las acciones para gestionar los riesgos de seguridad de la información inaceptables e implantar los controles necesarios para proteger la misma. (ISO/IEC 27000).
- **Plan de Respuesta a Ciberincidentes:** Conjunto predeterminado y ordenado de instrucciones o procedimientos para detectar, analizar, contener, erradicar y recuperar para minimizar las consecuencias de un ciberincidente.

- **Ransomware:** Código malicioso para secuestrar datos, una forma de explotación en la cual la atacante cifra los datos de la víctima y exige un pago por la clave de descifrado, se propaga a través de archivos adjuntos de correo electrónico, programas infectados y sitios web comprometidos, secuestrando computadores y servidores (imposibilidad de usarlo) o cifrando los archivos, con la promesa de liberarlo tras el pago de una cantidad de dinero por el rescate.
- **RAT- Remote Acces Tool:** Pieza de software que permite a un "operador" controlar a distancia un sistema como si se tuviera acceso físico al mismo. Aunque tiene usos perfectamente legales, el software RAT se asocia habitualmente con ciberataques o actividades criminales o dañinas. En estos casos, el malware suele instalarse sin el conocimiento de la víctima, ocultando frecuentemente un troyano.
- **Registro Nacional de Bases de Datos:** Directorio público de las bases de datos sujetas a Tratamiento que operan en el país. (Ley 1581 de 2012, art 25)
- **Responsabilidad Demostrada:** Conducta desplegada por los responsables o Encargados del tratamiento de datos personales bajo la cual a petición de la Superintendencia de Industria y Comercio deben estar en capacidad de demostrarle a dicho organismo de control que han implementado medidas apropiadas y efectivas para cumplir lo establecido en la Ley 1581 de 2012 y sus normas reglamentarias.
- **Responsable del Tratamiento de Datos:** Persona natural o jurídica, pública o privada, que por sí misma o en asocio con otros, decida sobre la base de datos y/o el Tratamiento de los datos. (Ley 1581 de 2012, art. 3).
- **Riesgo:** Posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información. Suele considerarse como una combinación de la probabilidad de un evento y sus consecuencias. (ISO/IEC 27000).
- **Riesgo de seguridad digital:** Es la combinación de amenazas y/o vulnerabilidades que se pueden materializar en el curso de cualquier actividad en el entorno digital y que puede afectar el logro de los objetivos económicos o sociales al alterar la confidencialidad, integridad y disponibilidad.

- **Rootkit:** T Es una herramienta que sirve para ocultar actividades ilegítimas en un sistema. Una vez que ha sido instalado, permite al atacante actuar con el nivel de privilegios del administrador del equipo.
- **Scanner (Scanning) Escáner de vulnerabilidades:** Programa que analiza un sistema buscando vulnerabilidades. Utiliza una base de datos de defectos conocidos y determina si el sistema bajo examen es vulnerable o no.
- **Spam (correo basura):** Correo electrónico no deseado que se envía aleatoriamente en procesos por lotes. Es extremadamente eficiente y barata forma de comercializar cualquier producto. La mayoría de los usuarios que están expuestos a este correo basura que se confirma en encuestas que muestran que más del 50% de todos los e-mails son correos basura. No es una amenaza directa, pero la cantidad de e-mails generados y el tiempo que lleva a las empresas y particulares relacionarlo y eliminarlo, representa un elemento molesto para los usuarios de Internet.
- **Spear Phising:** Phishing dirigido de forma que se maximiza la probabilidad de que el sujeto objeto del ataque pique el anzuelo (suelen basarse en un trabajo previo de ingeniera social sobre la victima).
- **Spyware "spy software":** Tipo de software malicioso que al instalarse intercepta o toma control parcial de la computadora del usuario sin el consentimiento de este último.
- **Suplantación (Spoofing):** Técnica basada en la creación de tramas TCP/IP utilizando una dirección IP falseada; desde su equipo, un atacante simula la identidad de otra máquina de la red (que previamente ha obtenido por diversos métodos) para conseguir acceso a recursos de un tercer sistema que ha establecido algún tipo de confianza basada en el nombre o la dirección IP del anfitrión suplantado.
- **Seguridad de la información:** Preservación de la confidencialidad, integridad, y disponibilidad de la información en cualquier medio: impreso o digital. (ISO/IEC 27000).
- **Seguridad digital:** Preservación de la confidencialidad, integridad, y disponibilidad de la información que se encuentra en medios digitales.
- **Servicio esencial:** En el marco de la gestión de riesgos de la seguridad digital es aquel servicio necesario para el mantenimiento de las actividades sociales y económicas del país, que dependen del uso de tecnologías de la información y las comunicaciones, y

un incidente en su infraestructura o servicio podría generar un daño significativo que afecte la prestación de dicho servicio y la consecuente parálisis de las actividades.

- **Titulares de la información:** Personas naturales cuyos datos personales sean objeto de Tratamiento. (Ley 1581 de 2012, art 3)
- **Tratamiento de Datos Personales:** Cualquier operación o conjunto de operaciones sobre datos personales, tales como la recolección, almacenamiento, uso, circulación o supresión. (Ley 1581 de 2012, art 3).
- **Trazabilidad:** Cualidad que permite que todas las acciones realizadas sobre la información o un sistema de tratamiento de la información sean asociadas de modo inequívoco a un individuo o entidad. (ISO/IEC 27000).
- **Vulnerabilidad:** Debilidad de un activo o control que puede ser explotada por una o más amenazas. (ISO/IEC 27000).
- **Troyano:** Programa que aparentemente, o realmente, ejecuta una función útil, pero oculta un subprograma dañino que abusa de los privilegios concedidos para la ejecución del citado programa.
- **Virus:** Programa que está diseñado para copiarse a sí mismo con la intención de infectar otros programas o ficheros.
- **Vulnerabilidad:** Debilidad de un activo o control que puede ser explotada por una o más amenazas. (ISO/IEC 27000).

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.

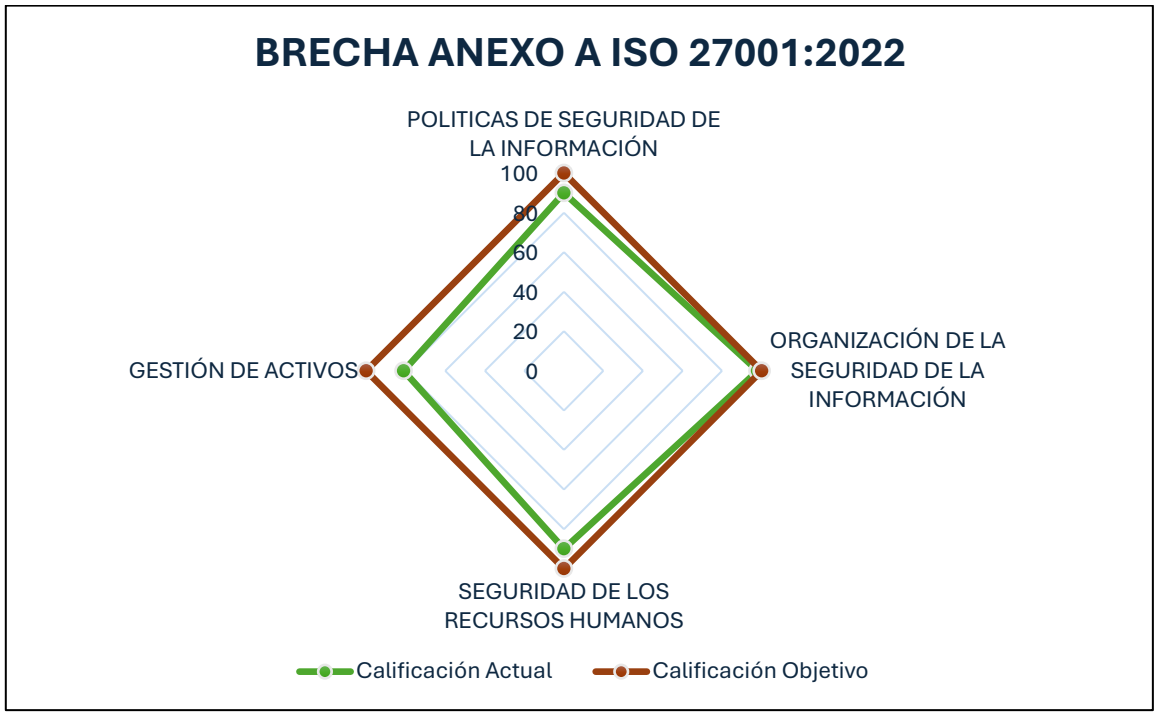
Este instrumento garantiza la coherencia normativa del Plan y su alineación con los procesos misionales, estratégicos y de apoyo de la entidad.

7. Principales Actividades

7.1 Diagnóstico

La evaluación de la efectividad de los controles de seguridad de la información en la Superintendencia de Sociedades, conforme al anexo A de la norma ISO 27001:2012, proporciona una visión detallada del estado actual de la seguridad de la información dentro de la entidad. Esta evaluación revela tanto fortalezas como áreas de mejora en la implementación de los controles de seguridad. A continuación, se presentan las conclusiones derivadas de este análisis y una serie de recomendaciones para optimizar aún más la seguridad de la información y cerrar las brechas identificadas.

Ilustración 1: Analsis de brecha ISO 27001:2022



Fuente: Elaboración realizada a partir de la aplicación de la herramienta de autodiagnostico.

Tabla 1: Resultado de análisis de controles ISO 27001:2022

No.	Evaluación de Efectividad de controles			
	DOMINIO	**Calificación Actual**	**Calificación Objetivo**	**EVALUACIÓN DE EFECTIVIDAD DE CONTROL**
A.5	CONTROLES ORGANIZACIONALES	90	100	**OPTIMIZADO**
A.6	CONTROLES DE PERSONAS	98	100	**OPTIMIZADO**
A.7	CONTROLES FISICOS	90	100	**OPTIMIZADO**
A.8	CONTROLES TECNOLÓGICOS	81	100	**OPTIMIZADO**
PROMEDIO EVALUACIÓN DE CONTROLES		**90**	**100**	

Fuente: Elaboración realizada a partir de la aplicación de la herramienta de autodiagnostico.

7.2 Análisis

Como se puede observar en la imagen anterior, se realizó una evaluación detallada de la efectividad de los controles de seguridad de la información, de acuerdo con el anexo A de la norma ISO 27001:2022. En general, la calificación promedio actual de los controles es de 80 sobre 100, lo que indica un nivel considerable de madurez y efectividad en la implementación de medidas de seguridad. Sin embargo, existen áreas clave donde la brecha entre la calificación actual y la calificación objetivo del 100 aún es notable.

Adicional de los hallazgos que presenta el análisis de brecha, es necesario enfocar esfuerzos para optimizar a la norma ISO 27001:2022 lo cual se presenta como una necesidad imperativa para la organización y asegurar la eficacia de su Sistema de Gestión de Seguridad de la Información (SGSI). La actualización de la norma refleja los cambios en

el panorama de riesgos y amenazas a la seguridad de la información, así como la evolución en las mejores prácticas internacionales.

La ISO 27001:2022 introduce modificaciones clave que permiten a las organizaciones abordar de manera más efectiva los desafíos actuales en ciberseguridad, tales como el incremento de ataques sofisticados, la expansión del trabajo remoto, y la creciente dependencia en la nube y en servicios de terceros. Estas adaptaciones no solo fortalecen la capacidad de las organizaciones para proteger sus activos de información, sino que también mejoran la resiliencia operativa y la capacidad de respuesta ante incidentes.

Además, la nueva versión de la norma ofrece una mayor flexibilidad en la implementación y gestión de los controles, alineándose mejor con las necesidades específicas de cada organización. También se enfatiza la importancia de una integración más estrecha entre el SGSI y otros sistemas de gestión, facilitando una visión más holística y coherente de la seguridad y del cumplimiento normativo.

7.3 Composición MSPI

El Modelo de Seguridad y Privacidad de la Información (MSPI) en la Superintendencia de Sociedades está compuesto por un conjunto integral de procesos estructurados que aseguran la protección de la información sensible y la continuidad operativa. Este modelo se basa en un ciclo continuo de mejora, que abarca desde el diagnóstico inicial hasta la implementación de controles y la evaluación constante de su eficacia.

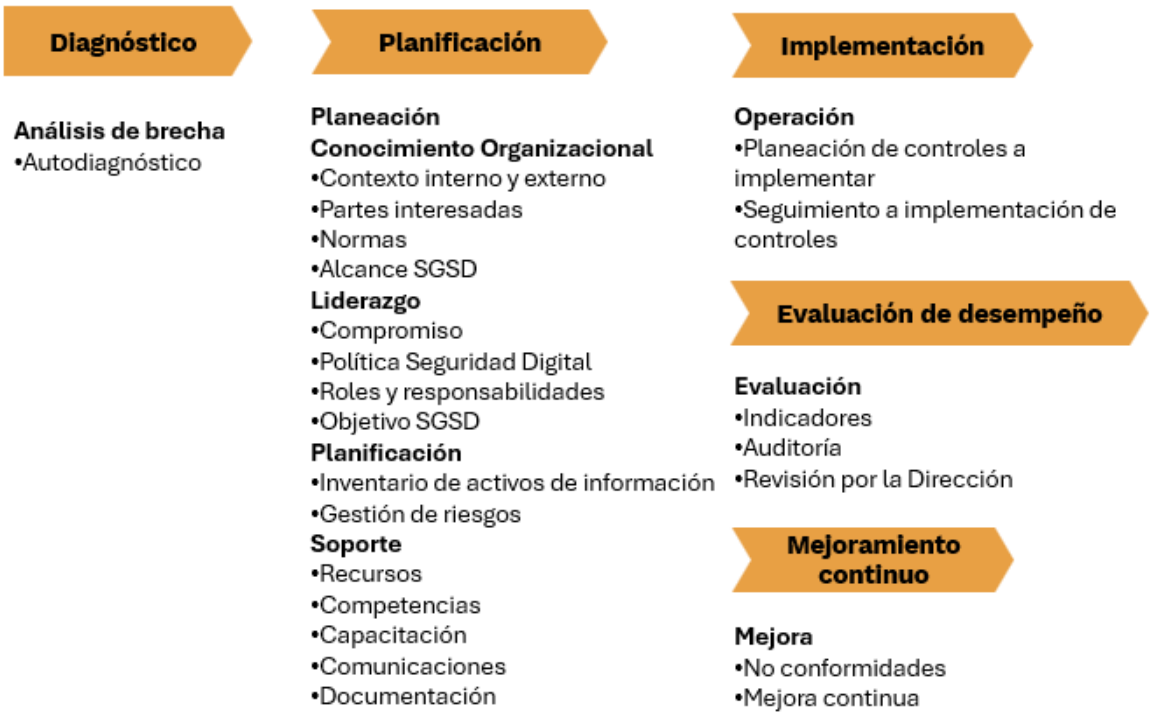
En la fase de Diagnóstico, se realiza un análisis de brechas y un autodiagnóstico para identificar las áreas críticas que requieren atención. Posteriormente, la Planificación se enfoca en el conocimiento organizacional, liderazgo, planificación detallada, y soporte, asegurando que todos los aspectos desde los recursos hasta las políticas de seguridad digital estén alineados con los objetivos del Sistema de Gestión de Seguridad Digital (SGSD).

La Implementación de este modelo se concentra en la operación efectiva de los controles planificados, garantizando un seguimiento riguroso de su ejecución. Este proceso es complementado por la Evaluación de Desempeño, donde se revisan indicadores clave,

auditorías y la revisión por parte de la dirección, asegurando que el sistema cumpla con las expectativas y se mantenga alineado con los objetivos estratégicos de la organización.

Finalmente, el ciclo se completa con el Mejoramiento Continuo, donde se abordan las no conformidades y se promueve la mejora continua para adaptarse a las nuevas amenazas y cambios en el entorno organizacional. Este enfoque holístico permite a la Superintendencia de Sociedades mantener un alto nivel de seguridad y resiliencia frente a las crecientes amenazas en el ámbito digital.

Ilustración 2: Fases y Composición MSPI



Fuente: Elaboración propia a partir de las fase establecidas en el MSPI.

7.4 Fase 1: Planificación

Contexto

En el contexto organizacional, la Superintendencia de Sociedades ha establecido un análisis de contexto detallado en su Manual Operativo para los sistemas integrados de gestión. Este análisis abarca tanto el contexto interno como el externo desde una

perspectiva estratégica, proporcionando una comprensión integral de los factores que influyen en su funcionamiento y operatividad.

Enlace: Contexto estratégico SuperSociedades

No obstante, en el ámbito específico de la Seguridad de la Información, es crucial desarrollar un análisis más profundo y detallado que permita identificar y gestionar adecuadamente las fortalezas, oportunidades, debilidades y amenazas relacionadas con este aspecto crítico.

Para lograr esto, se realiza un análisis utilizando la metodología DOFA (también conocida como FODA), específico para la Seguridad de la Información, en línea con el enfoque estratégico del Manual Operativo de la Superintendencia de Sociedades, proporcionará una visión integral y detallada que permitirá fortalecer la ciberseguridad y proteger de manera efectiva la información crítica de la entidad.

Tabla 2: Debilidades y Oportunidades en seguridad de la información

Debilidades	Oportunidades
1. Gestión de incidentes de seguridad de la información	1. Optimizar la respuesta y gestión de incidentes de seguridad.
2. Disminución posibles brechas de seguridad.	2. Implementar un sistema avanzado de gestión de incidentes.
3. Gestión de la continuidad del negocio	3. Fortalecer la continuidad del negocio.
4. Compromiso para mantener operaciones durante eventos disruptivos.	4. Mejorar la supervisión y control de proveedores.
5. Gestión de riesgos en la relación con los proveedores.	5. Capacitar continuamente al personal en ciberseguridad

Fuente: Elaboración realizada a partir del la aplicación de la matriz DOFA.

Tabla 3: Fortalezas y Amenazas en seguridad de la información

Fortalezas	Amenazas
1. Políticas de Seguridad y Privacidad de la Información formalizadas y robustas.	1. Debilidades en la gestión de incidentes de seguridad de la información y seguridad digital.
2. Alto nivel de cumplimiento del marco normativo y regulatorio aplicable.	2. Limitaciones en la articulación y coordinación de los equipos responsables de la continuidad del negocio.
3. Gestión del talento humano efectiva en materia de seguridad de la información.	3. Vulnerabilidades en la gestión de proveedores y terceros.
4. Gestión de activos de información estructurada, eficiente y controlada.	4. Brechas en la seguridad de las comunicaciones y el intercambio de información.
5. Implementación de controles relacionados a la protección de la información, adecuados y efectivos.	5. Riesgo de accesos no autorizados a los activos de información.

Fuente: Elaboración realizada a partir del la aplicación de la matriz DOFA.

Necesidades y expectativas de los interesados

La seguridad de la información es un pilar fundamental en la gestión organizacional, e cada rol dentro de la entidad tiene necesidades específicas que deben ser atendidas para garantizar la robustez del Sistema de Gestión de Seguridad de la Información (SGSI). Estas necesidades abarcan desde la alineación estratégica y la implementación de controles efectivos, hasta la supervisión continua y la gestión de riesgos. Asimismo, las expectativas se centran en lograr un sistema resiliente y adaptable, que cumpla con las normativas y proteja los activos críticos de la organización. El cumplimiento de estas necesidades y expectativas es crucial para asegurar que la seguridad de la información se mantenga como un componente dinámico y proactivo dentro de la estrategia institucional, alineándose con los objetivos organizacionales y respondiendo a las exigencias del entorno regulatorio y tecnológico.

Para la identificación de estas expectativas se ejecutaron las actividades de creación de la correspondiente matriz de expectativas y necesidades y adicional se gesto la matriz RACI, la cual asigna roles y responsabilidades claras para garantizar que todas las partes interesadas sean adecuadamente atendidas.

Tabla 4: Matriz RACI

Criterios del ajuste

- **R (Responsible):** Ejecuta la actividad.
- **A (Accountable):** Tiene la responsabilidad final y toma decisiones.
- **C (Consulted):** Aporta insumos técnicos o estratégicos.
- **I (Informed):** Es informado del avance o resultados.

Actividad / Rol clave	Jefe Oficina Asesora de Planeación	Director/a TIC	Oficial de Seguridad de la Información	Control Interno	Grupo Seguridad Informática y Forense	Dueños de Procesos
Definición y alineación estratégica del SGSI/MSPI	A	C	R	I	I	C
Formulación y actualización de políticas de seguridad	C	C	R	I	I	C
Aprobación institucional de políticas y lineamientos	A	C	R	I	I	I
Gestión y valoración de riesgos de seguridad de la información	C	C	R	I	C	R

Actividad / Rol clave	Jefe Oficina Asesora de Planeación	Director/a TIC	Oficial de Seguridad de la Información	Control Interno	Grupo Seguridad Informática y Forense	Dueños de Procesos
Implementación de controles de seguridad (organizativos y técnicos)	I	A	C	I	R	R
Gestión de incidentes de seguridad de la información	I	A	C	I	R	C
Gestión de continuidad del negocio (BCP/DRP – componente TI)	C	A	C	I	R	R
Gestión de activos de información (inventario y clasificación)	I	C	C	I	I	R
Gestión de accesos y privilegios	I	A	C	I	R	R
Gestión de proveedores y terceros con acceso a información	I	A	C	I	C	R
Seguimiento de indicadores del SGSI	I	C	R	I	R	C
Auditorías internas al SGSI	R	I	I	I	I	I

Actividad / Rol clave	Jefe Oficina Asesora de Planeación	Director/a TIC	Oficial de Seguridad de la Información	Control Interno	Grupo Seguridad Informática y Forense	Dueños de Procesos
Atención a auditorías externas y entes de control	R	C	A	I	I	I
Mejora continua del SGSI (acciones correctivas y preventivas)	C	C	R	C	R	R
Sensibilización y cultura de seguridad de la información	C	R	R	I	C	R

Fuente: Elaboración realizada a partir del la aplicación de la matriz RACI.

Definición del alcance del MSPI

Aplica a todos los procesos definidos en el Sistema de Gestión Integral y a todas las sedes de trabajo de la Superintendencia de Sociedades.

El Sistema de Gestión Integrado de la Superintendencia de Sociedades se ha desarrollado e implementado de acuerdo con los requisitos de las normas NTC ISO 9001, NTC ISO/IEC 27001, NTC ISO 14001, NTC ISO 45001, NTC 5906 (Centro de Conciliación y Arbitraje) y el Programa Integral de Gestión de Datos Personales el cual se establece para dar cumplimiento a la Ley 1581 de 2012 reglamentado mediante el decreto 1377 de 2013 y el cual fue compilado en el decreto 1074 de 2015 Por medio del cual se expide el Decreto Único Reglamentario del Sector Comercio, Industria y Turismo.

Identifica la Política de Gestión Integral, los Objetivos del Sistema de Gestión Integrado, los Procesos y la Estructura del Sistema de Gestión Integrado. Este manual aplica a todos los procesos y servicios a través de los cuales la Entidad busca la satisfacción de los requisitos de las partes interesadas.

Liderazgo

La alta dirección de la Superintendencia de Sociedades demuestra un firme liderazgo y un profundo compromiso con el desarrollo y la implementación del Sistema de Gestión Integrado (SGI), así como con la mejora continua de su eficacia, eficiencia y efectividad. Este compromiso se manifiesta a través de la asunción de la responsabilidad y la rendición de cuentas en relación con la eficacia del sistema, garantizando que la política integral y los objetivos estratégicos estén alineados con el contexto y la dirección estratégica de la organización. Además, la alta dirección asegura la integración de los requisitos del SGI en todos los procesos de negocio, disponiendo de los recursos necesarios para su correcta implementación.

Asimismo, comunica de manera efectiva la importancia de una gestión integral que cumpla con los requisitos establecidos, y se compromete a dirigir y apoyar a todo el personal para contribuir a la eficacia del sistema. Finalmente, la alta dirección promueve activamente la mejora continua, asegurando que el SGI alcance los resultados previstos y se mantenga como un pilar fundamental en el cumplimiento de los objetivos organizacionales.

Adicional, se cuenta con el manual de operaciones y del SGI y la matriz de responsabilidades, autoridad, rendición de cuentas y competencias, documentos que dan las directrices para cada una de las partes interesadas a nivel organizacional en el componente del SGI

Ver: Manual de Operaciones y del SGI, matriz de responsabilidades, autoridad, rendición de cuentas y competencias.

Planificación

En alineación con el objetivo estratégico de la Superintendencia de Sociedades, y en aras de fortalecer la entidad por medio de la optimización de los procesos clave y el fortalecimiento de la administración de riesgos, se ha adoptado el Sistema de Gestión de Seguridad de la Información (SGSI) el cual tiene como propósito implementar, operar y mantener controles efectivos que permitan gestionar los riesgos de seguridad digital, garantizando la protección de los activos de información de las partes interesadas de la entidad.

Adicional la administración de la seguridad de la información define los roles y responsabilidades dentro de la organización, con el objetivo de implementar, mantener y mejorar continuamente el Sistema de Gestión de Seguridad de la Información, todo esto por medio del Documento de Políticas de Seguridad y Privacidad de la Información (GIN-PO-003) el cual da lineamientos necesarios para alcanzar los objetivos establecidos en el SGSI.

Ver: Documento de Políticas de Seguridad y Privacidad de la Información.

Identificación de activos de información e infraestructura critica

La correcta gestión de los activos de información es fundamental para garantizar la seguridad y continuidad operativa de la Superintendencia de Sociedades. Este capítulo establece los lineamientos para la identificación, clasificación, valoración y etiquetado de dichos activos, siguiendo las directrices establecidas por las normativas estatales y las políticas de gobierno en materia de seguridad digital. En cumplimiento con las disposiciones del Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC) y dentro del marco del Modelo Integrado de Planeación y Gestión (MIPG), se busca asegurar que todos los activos de información críticos sean gestionados de manera eficiente, alineando las prácticas de la entidad con los estándares de seguridad nacional.

Para dar cumplimiento a lo anterior la SuperSociedades cuenta con el Instructivo para a Identificación, Clasificación/Valoración y Etiquetado de Activos de Información el cual entrega los pasos requeridos para tal fin.

Ver: GIN-IN-001 Instructivo para la identificación, clasificación/valoración y etiquetado de activos de información.

Valoración de los riesgos de seguridad de la información

La valoración de los riesgos de seguridad de la información es un componente esencial en el marco del Sistema de Gestión de Riesgos de la Superintendencia de Sociedades. Este capítulo tiene como propósito definir una metodología de trabajo clara y efectiva para la identificación, medición, valoración, tratamiento y seguimiento de los riesgos relacionados con la seguridad de la información.

Dirigido a todos los funcionarios y líderes de procesos de la entidad, este enfoque busca garantizar que los riesgos sean gestionados adecuadamente en todos los procesos, proyectos y actividades que conforman el Sistema de Gestión Integrado.

El documento se alinea con la Guía para la administración del riesgo y el diseño de controles en entidades públicas del Departamento Administrativo de la Función Pública, así como con estándares internacionales como ISO 31000 e ISO 27005

Ver: Guía de Administración de Riesgos Institucionales

Plan de tratamiento de los riesgos de seguridad de la información

El Plan de Tratamiento de los Riesgos de Seguridad y Privacidad de la Información tiene como propósito establecer los lineamientos, criterios y acciones para la gestión integral y sistemática de los riesgos que puedan afectar la confidencialidad, integridad y disponibilidad de la información en la Superintendencia de Sociedades. Este plan contempla el análisis, identificación, valoración y priorización de los riesgos, así como la definición e implementación de controles orientados a su tratamiento, mitigación o aceptación, de acuerdo con el nivel de riesgo establecido por la entidad.

El Plan es aplicable a todos los procesos, dependencias e intendencias de la Superintendencia y se desarrolla a partir del análisis del contexto organizacional y del inventario y clasificación de los activos de información. Con base en la valoración de la probabilidad y el impacto de los riesgos identificados, se establecen controles técnicos, organizacionales y procedimentales, los cuales son objeto de monitoreo y seguimiento permanente para evaluar su efectividad. La implementación y seguimiento del Plan se realiza bajo la coordinación del Oficial de Seguridad de la Información, en articulación con los dueños de proceso y las áreas responsables, con el fin de asegurar una gestión efectiva de los riesgos y la protección de los activos de información críticos de la entidad.

Soporte

La Fase de Soporte en el marco de la implementación del Modelo de Seguridad y Privacidad de la información es fundamental para garantizar el éxito continuo y sostenible del sistema. En esta fase, se establecen los recursos necesarios, las competencias, la toma de

conciencia y la documentación requerida para respaldar la implementación, operación y mejora del modelo.

Recursos

Para dar soporte al Modelo de Seguridad y privacidad de la Información (MSPI), es necesario contar con una serie de recursos que permitan implementar, operar y mejorar continuamente el sistema. Estos recursos abarcan áreas como personal, tecnología, infraestructura y herramientas específicas. A continuación, se describen los principales recursos requeridos:

Recursos Humanos

Personal con formación y experiencia en ciberseguridad, gestión de riesgos, auditoría de seguridad y cumplimiento normativo, incluido un Oficial de Seguridad de la Información (CISO).

En algunos casos, se puede requerir la contratación de consultores especializados para realizar auditorías, evaluaciones de riesgos o implementaciones puntuales en áreas de mayor complejidad.

Tecnología y Herramientas

El soporte al sistema de gestión de seguridad de la información incluye diversas herramientas críticas para monitorear, detectar y gestionar incidentes de seguridad conforme a la arquitectura de seguridad definida. También se implementan tecnologías para identificar y mitigar vulnerabilidades en los sistemas, junto con herramientas de autenticación y autorización, además se debe tener en cuenta que el objetivo es preservar la confidencialidad, integridad y disponibilidad por lo que acorde a las necesidades y a la arquitectura definida se deberán implementar y desplegar nuevas soluciones.

Infraestructura Tecnológica

La provisión de fondos para la adquisición de tecnologías y sistemas necesarios para la protección de la información y el monitoreo continuo de riesgos esto redunda en una infraestructura de red protegida y segmentada para reducir la exposición a riesgos, asegurando que los centros de datos y servidores donde se almacena la información estén físicamente protegidos y equipados con controles de acceso y medidas de seguridad física.

Recursos Financieros

Se necesita asignar un presupuesto adecuado para la implementación, mantenimiento y mejora continua, lo cual incluye la adquisición de herramientas de seguridad, contratación de personal especializado y auditorías periódicas.

Competencia, toma de conciencia y comunicación

Para dar cumplimiento a los requisitos de Competencia, Toma de Conciencia y Comunicación en un Sistema de Gestión de Seguridad de la Información (SGSI), es necesario implementar una serie de acciones clave que aseguren que el personal de la organización esté adecuadamente preparado y alineado con los objetivos de seguridad. A continuación, se detallan los elementos necesarios para cumplir con estos requerimientos:

- Desarrollar y ejecutar programas de formación específicos en materia de seguridad de la información. Estos programas deben cubrir las normativas, controles de seguridad, políticas internas y mejores prácticas.
- Desarrollar campañas periódicas de concienciación que resalten la importancia de la seguridad de la información y el rol de cada empleado en la protección de los datos de la organización.
- Organizar sesiones de concienciación a todos los niveles de la organización, donde se expliquen los riesgos asociados a la seguridad de la información y las medidas que los empleados deben adoptar para mitigarlos.
- Realizar simulaciones de incidentes de seguridad (como ataques de phishing o brechas de datos) para fortalecer la conciencia del personal sobre cómo actuar en caso de un incidente real.

7.5 Fase 2: Operación

La entidad debe llevar a cabo la planificación e implementación de las acciones establecidas en el plan de tratamiento de riesgos, y esta información debe documentarse por cada proceso de acuerdo con lo planificado. Los planes de tratamiento deben ser definidos y aprobados por los líderes de cada proceso. Los proyectos o controles de seguridad que no puedan implementarse a corto o mediano plazo, generalmente debido a limitaciones presupuestales, deberán ser escalados al comité institucional de gestión y

desempeño para que tome decisiones y asigne los recursos necesarios. Estos documentos deben recibir la aprobación del comité institucional de gestión y desempeño.

Planificación e implementación

La planificación e implementación requiere una comprensión clara del contexto organizacional, una evaluación exhaustiva de los riesgos de seguridad y la implementación de controles que mitiguen esos riesgos. La capacitación del personal, el monitoreo continuo, las auditorías internas y la mejora continua son esenciales para mantener la efectividad del sistema.

- Plan de implementación de controles de seguridad y privacidad de la información que contenga como mínimo: controles, actividades, fechas, responsable de implementación y presupuesto.
- Evidencia de la implementación de los controles de seguridad y privacidad de la información.

7.6 Fase 3: Evaluación de desempeño

La evaluación del es un proceso clave para garantizar su efectividad y alineación con los objetivos de la organización. Este capítulo describe los mecanismos y herramientas utilizados para medir el rendimiento del MSPI, incluyendo auditorías internas, monitoreo de controles, análisis de incidentes de seguridad, y revisiones por la alta dirección. El objetivo de esta evaluación es asegurar que los controles implementados cumplan con los requisitos de la norma ISO 27001, así como con las políticas internas de seguridad de la organización, permitiendo identificar áreas de mejora y garantizar la protección continua de los activos de información. Una evaluación efectiva del desempeño del MSPI es fundamental para la mejora continua, permitiendo a la organización adaptarse a nuevas amenazas y cumplir con sus compromisos de seguridad de manera eficiente.

Seguimiento, medición, análisis y evaluación

Es fundamental que las organizaciones evalúen de manera regular y rigurosa la efectividad de su MSPI. Esto implica establecer mecanismos de seguimiento, definir indicadores clave de desempeño y realizar auditorías periódicas que abarquen aspectos como la seguridad

digital. Los resultados de estas evaluaciones deben ser compartidos con el Comité Institucional para tomar decisiones informadas.

Para garantizar el cumplimiento de la Política de Gobierno Digital, las entidades deben implementar un sistema de gestión del desempeño que permita medir y analizar la eficacia del MSPI. Este sistema debe incluir indicadores cuantitativos y cualitativos, así como auditorías regulares para verificar la conformidad con los estándares de seguridad, adicional se busca:

Evidencia del cumplimiento

- **Conformidad con los controles:** Se demuestra que los controles de seguridad establecidos en el MSPI se están implementando y siguiendo de manera consistente.
- **Cumplimiento normativo:** Se verifica que el MSPI cumple con los requisitos de la norma ISO 27001 y otras regulaciones aplicables.

Identificación de desviaciones

- **Detección de brechas:** Se identifican las áreas donde el sistema no cumple con los requisitos o donde existen vulnerabilidades.
- **Evaluación de riesgos:** Se evalúa si los riesgos identificados están siendo gestionados de manera adecuada.

Mejora continua

- **Información para la toma de decisiones:** Se proporciona información relevante para tomar decisiones sobre mejoras en el MSPI.
- **Identificación de oportunidades de mejora:** Se identifican áreas donde se pueden optimizar los procesos y controles.
- **Implementación de acciones correctivas:** Se establecen y ejecutan acciones para corregir las desviaciones y mejorar el desempeño del MSPI.

Auditoría Interna

El compromiso con la seguridad de la información se evidencia en la implementación de un riguroso programa de auditorías internas anuales, basadas en riesgos, que abarca todos los procesos y sistemas críticos. Estas auditorías permiten evaluar de manera exhaustiva

la conformidad con los requisitos del SGSI, identificar y mitigar vulnerabilidades, y garantizar la protección continua de los activos de información.

Revisión por la dirección

La aprobación de temas como seguridad de la información, privacidad de datos y políticas de seguridad debe ser un asunto prioritario para el comité institucional. Este comité, o el designado por la máxima autoridad, será el encargado de validar cualquier cambio o actualización en estos aspectos, considerando siempre las necesidades de todos los involucrados.

7.7 Fase 4: Mejoramiento continuo

La fase de mejora continua en un MSPI es un proceso dinámico y cíclico que busca la excelencia en la gestión de la seguridad de la información. Al implementar esta fase de manera efectiva, las organizaciones pueden garantizar la protección de sus activos más valiosos y obtener una ventaja competitiva.

Mejora

La fase de mejora continua en un Sistema de Gestión de Seguridad y Privacidad de la Información (SGSI) es un ciclo iterativo que busca perfeccionar constantemente el sistema. Su objetivo principal es garantizar que la organización mantenga un alto nivel de seguridad de la información, adaptándose a las nuevas amenazas y requisitos.

Los resultados esperados de esta fase son:

- **Mayor madurez del SGSI:** El sistema se vuelve más robusto, eficiente y adaptable a los cambios del entorno.
- **Aumento de la eficacia de los controles:** Los controles de seguridad se vuelven más efectivos en la protección de la información.
- **Reducción de riesgos:** Se minimiza el riesgo de incidentes de seguridad y sus consecuencias.
- **Cumplimiento normativo:** Se garantiza el cumplimiento continuo de los requisitos legales y regulatorios en materia de seguridad de la información.
- **Mayor confianza de los stakeholders:** Los clientes, socios y empleados confían más en la capacidad de la organización para proteger su información.

- **Optimización de recursos:** Se optimizan los recursos utilizados en la gestión de la seguridad de la información.
- **Cultura de seguridad:** Se fomenta una cultura de seguridad de la información en toda la organización.
- **Adaptación a los cambios:** El SGSI se adapta de manera proactiva a los cambios en el entorno de amenazas y en las necesidades del negocio.

Específicamente, esta fase debe permitir:

- **Identificar oportunidades de mejora:** A través de análisis de datos, auditorías, revisiones de gestión y retroalimentación de los empleados.
- **Implementar acciones correctivas:** Resolver las no conformidades y las causas raíz de los problemas.
- **Establecer acciones preventivas:** Anticipar y prevenir futuros problemas.
- **Actualizar la documentación:** Mantener la documentación del SGSI actualizada y alineada con los cambios realizados.
- **Medir la efectividad de las mejoras:** Evaluar el impacto de las acciones de mejora en el desempeño del SGSI.

8. Evaluación y seguimiento del Plan de Seguridad y Privacidad de la información.

Las actividades definidas para la vigencia 2026 corresponden a las acciones estratégicas y operativas orientadas al fortalecimiento del Sistema de Gestión de Seguridad y Privacidad de la Información (SGSI) de la entidad. Estas actividades fueron desarrolladas a partir del Plan Diamante Estrategia de Seguridad Digital desarrollado por la Dirección de Tecnología de la Información y las Comunicaciones, lo permiten consolidar la gestión de activos de información, riesgos, controles de seguridad, cultura organizacional y capacidades de detección y respuesta a incidentes, desde un enfoque de colaboración dando cumplimiento a lo requerido por la Resolución 500 de 2021 emitida por MINTIC, garantizando la protección de la información y el cumplimiento del marco normativo y las buenas prácticas aplicables.

Objetivo Estratégico	Actividad	Producto	Indicador	Meta	Responsable	Fecha Inicio	Fecha cierre
Gestión de Vulnerabilidades	Ejecutar pruebas de vulnerabilidades	Informes de pruebas	≥ 1 ciclo anual de pruebas	Realizar mínimo 1 ciclo completo de escaneo y análisis de vulnerabilidades en 2026	DTIC	1/07/2026	31/12/2026
Gestión de Vulnerabilidades	Seguimiento al plan de remediación 2025 acciones COLCERT y DNI	Informe de seguimiento	% vulnerabilidades detectadas mitigadas ≥ 95%	Alcanzar ≥95% de remediación de vulnerabilidades críticas y altas	DTIC	1/02/2026	30/06/2026
Consolidación SOC	Implementar y operar SOC	Dashboard SOC y/o reportes mensuales	Disponibilidad SOC ≥ 97%	SOC operativo con disponibilidad ≥ 97%	DTIC	1/02/2026	30/06/2026
Consolidación SOC	Informes SOC	Reportes mensuales	Reportes mensuales ≥4	Emitir mínimo 4 informes SOC en 2026	DTIC	1/07/2026	31/12/2026
Consolidación SOC	Implementar playbooks SOAR	Playbooks documentados	≥ 3 playbooks	Implementar al menos 3 playbooks automatizados	DTIC	1/07/2026	31/12/2026
Gestión de Amenazas	Ejecutar threat hunting	Informes threat hunting	≥ 2 ejercicios/año	Realizar mínimo 2 ejercicios de threat hunting en 2026	DTIC	1/07/2026	31/12/2026
Contingencia tecnológica	Realizar pruebas de contingencia	Informe pruebas realizadas a los sistemas incluidos	8 pruebas	Ejecutar mínimo 1 prueba anual a cada uno de los planes de contingencia (8) para en 2026	DTIC	1/05/2026	30/11/2026

Objetivo Estratégico	Actividad	Producto	Indicador	Meta	Responsable	Fecha Inicio	Fecha cierre
Protección de Información Sensible	Desplegar e implementar la solución institucional de Prevención de Pérdida de Datos (DLP) en correo, endpoints y nube.	Informe de despliegue	% cobertura DLP en endpoints/correo/nube ≥ 80%	Cobertura DLP ≥80% en endpoints, correo y nube	DTIC / Oficial de Seguridad	1/02/2026	30/08/2026
Gestión de Incidentes	Gestionar incidentes reportados	Registro incidentes	% incidentes cerrados ≥ 95%	Cerrar ≥95% de incidentes dentro del SLA definido	DTIC / Oficial de Seguridad	1/02/2026	31/12/2026
Gestión de Activos de Información	Actualizar inventario y clasificación de activos	Matriz de activos aprobada	% activos identificados ≥ 90%	Clasificar ≥90% de activos de información críticos	Oficial de Seguridad	1/02/2026	30/06/2026
Certificación ISO 27001	Recibir auditoria externa	Informe de Auditoria	≥ 1 auditoría Externa	Realizar mínimo 1 auditoría externa de certificación o seguimiento	Oficial de Seguridad	1/06/2026	30/07/2026
Gobierno del SGSI/MSPI	Actualizar análisis y tratamiento de riesgos	Matriz riesgos	% riesgos tratados ≥ 90%	Tratar ≥90% de riesgos identificados	Oficial de Seguridad	1/02/2026	30/05/2026
Gobierno del SGSI/MSPI	Actualizar Guía de Gestión de Riesgos	Guía publicada, acta comité	1 Guía actualizada y aprobada	Publicar y aprobar 1 versión	Oficial de Seguridad	1/02/2026	30/03/2026

Objetivo Estratégico	Actividad	Producto	Indicador	Meta	Responsable	Fecha Inicio	Fecha cierre
				actualizada de la guía			
Cultura de Seguridad	Ejecutar estrategia de cultura	Informes campañas	≥ 4 campañas	Realizar mínimo 4 campañas de cultura de seguridad	DTIC / Oficial de Seguridad	1/02/2026	30/11/2026
Cultura de Seguridad	Capacitación en seguridad de la información	Listados asistencia	≥ 85% funcionarios capacitados	Capacitar al menos 85% del personal	DTIC / Oficial de Seguridad	1/02/2026	30/11/2026
Analisis de vulnerabildiades CSIRT	Solicitar al CSIRT Gobierno realización de análisis de vulnerabilidades a los sitios de la SSOC	Reportes equipo COLCERT Plan de cierre de brechas identificadas	1 escaneo	Realizar mínimo 1 análisis CSIRT y plan de remediación	Oficial de Seguridad	1/02/2026	30/05/2026
Gobierno de Datos Personales	Realizar reporte RNBD	Certificado de cargue de datos	1 cargue de información realizado	Realizar 1 cargue de bases de datos al RNBD	Oficial de Protección de Datos	1/02/2026	30/04/2026