PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

2026

DIRECCIÓN DE GESTIÓN DE INFORMACIÓN
GRUPO DE TRABAJO GESTIÓN PLATAFORMA DE TECNOLOGÍAS DE INFORMACIÓN
GESTIÓN DE TECNOLOGIAS DE INFORMACIÓN Y COMUNICACIONES

TABLA DE CONTENIDO

1. OBJETIVO

Fortalecer la protección de la integridad, confidencialidad y disponibilidad de los activos de información de la Entidad, mediante la reducción de los riesgos asociados a su gestión hasta niveles aceptables, a través de la implementación efectiva de las estrategias de seguridad digital definidas en el presente documento, orientadas a consolidar las capacidades institucionales durante el año en curso.

2. OBJETIVOS ESPECÍFICOS

- Definir y formalizar la estrategia de seguridad digital de la Entidad, asegurando su alineación con el marco normativo aplicable, las necesidades institucionales y las mejores prácticas internacionales en seguridad de la información.
- Identificar y establecer los requerimientos técnicos, organizacionales y de talento humano necesarios para la adecuada implementación y operación del Sistema de Gestión de Seguridad de la Información (SGSI).
- Priorizar, estructurar y planificar los proyectos estratégicos orientados a fortalecer la seguridad de la información, garantizando su alineación con los objetivos institucionales y la gestión eficaz de los riesgos identificados.
- Diseñar y ejecutar un plan de evaluación, seguimiento y verificación continua de los controles, lineamientos y políticas implementados en el marco del SGSI, con el fin de asegurar su eficacia y promover la mejora continua en la protección de los activos de información.

3. ALCANCE

El Plan Estratégico de Seguridad de la Información, orientado a la implementación del Sistema de Gestión de Seguridad de la Información (SGSI) y de la estrategia de seguridad digital de la Entidad, se encuentra alineado con el alcance definido en la Política General de Seguridad de la Información. En consecuencia, comprende la aplicación de los principios, lineamientos y controles de seguridad en todos los procesos institucionales, garantizando un enfoque integral para la protección de los activos de información y la mitigación de los riesgos asociados a su gestión.

4. DOCUMENTOS DE REFERENCIA

El Plan Estratégico de Seguridad de la Información (PESI) se fundamenta en los siguientes documentos, normas y lineamientos que orientan su estructura y funcionamiento:

Resolución 2277 de 2025 (MinTIC): Actualiza el Anexo 1 de la Resolución 500 de 2021 y fortalece/moderniza los lineamientos del MSPI, incluyendo su alineación con ISO/IEC 27001:2022.

ISO/IEC 27001:2022: Norma internacional que especifica los requisitos para establecer, implementar, mantener y mejorar un SGSI.

Resolución 500 de 2021 (MinTIC): Establece lineamientos y estándares para la estrategia de seguridad digital y adopta el MSPI como habilitador de la Política de Gobierno Digital (incluye Anexo 1).

Decreto 612 de 2018: Fija directrices para la integración de los planes institucionales y estratégicos al Plan de Acción; sirve de marco para exigir e integrar planes como el PESI dentro de la planeación institucional.

Ley 1581 de 2012: Establece disposiciones generales para la protección de datos personales, reforzando la protección de información personal y sensible dentro del PESI.

Decreto 1377 de 2013: Decreto reglamentario de la Ley 1581 de 2012 que complementa disposiciones para el tratamiento y protección de datos personales en el ámbito institucional.

Manual de Gobierno Digital – MinTIC: Instrumento técnico con lineamientos para transformación digital de entidades públicas, con seguridad de la información como eje transversal. (Si me compartes el enlace o versión exacta que están usando, lo dejo citado y con nombre formal tal cual.)

Modelo de Seguridad y Privacidad de la Información (MSPI) – MinTIC: Referente técnico para la gestión de seguridad y privacidad como habilitador de Gobierno Digital (documentación técnica asociada al Anexo 1).

Política General de Seguridad de la Información de la Entidad: Documento interno que define principios, objetivos y lineamientos aplicables a todos los procesos de la Entidad.

5. ESTADO ACTUAL DE LA ENTIDAD RESPECTO AL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN

A continuación, se describe el estado actual del SGSI del Servicio Geológico Colombiano (SGC), organizado conforme a los cuatro grandes dominios de la ISO/IEC 27001:2022: Contexto de la organización, Liderazgo, Planificación y Soporte/Operación/Evaluación/Mejora.

5.1 Contexto de la organización (Cláusula 4)

El SGSI se enmarca en la protección integral de los activos de información del SGC; se evidencia la necesidad de consolidar y mantener actualizados los insumos base del sistema (inventario de activos, clasificación y criterios de criticidad), para asegurar que el alcance y las prioridades del SGSI respondan a los riesgos institucionales.
Se identifica oportunidad de fortalecer la gestión del cumplimiento y los requisitos aplicables (p. ej., actualización de instrumentos documentales como la TRD, y verificación periódica de obligaciones normativas asociadas a seguridad de la información y protección de datos).

5.2 Liderazgo (Cláusula 5)

El SGC cuenta con una Política de Seguridad de la Información actualizada; se recomienda establecer un mecanismo formal y periódico de revisión para asegurar su vigencia, trazabilidad y alineación con cambios institucionales.
Se requiere fortalecer la gobernanza del SGSI mediante la definición/ajuste de la estructura organizacional de seguridad, incluyendo la asignación formal de responsabilidades (p. ej., rol tipo OSI o equivalente) y la formalización de una matriz de roles y perfiles para asegurar rendición de cuentas y segregación de funciones.

5.3 Planificación (Cláusula 6)

Se evidencia la necesidad de mejorar la planeación basada en riesgos, incorporando de manera consistente análisis de riesgos en:
Control de acceso (eliminación de cuentas genéricas, ajuste de roles y privilegios).
Gestión criptográfica (criterios para gestión de llaves y selección de algoritmos, actualización de procedimientos).
Relación con proveedores (integración sistemática de evaluación/seguimiento de riesgos en servicios contratados).
Se identifican oportunidades para robustecer el tratamiento del riesgo en temas de continuidad (pruebas documentadas y fortalecimiento de capacidades de sitio alterno) y respuesta a incidentes (formalización del procedimiento y su ciclo de mejora).

5.4 Soporte, Operación, Evaluación del desempeño y Mejora (Cláusulas 7, 8, 9 y 10)

Soporte (Cláusula 7):
Recursos humanos: controles de selección, formación y disciplina se encuentran implementados; se recomienda actualización periódica para mantener alineación con normativa vigente y necesidades del SGSI.
Gestión documental y evidencia: se requiere reforzar la gestión documental de seguridad (p. ej., TRD, registros, trazabilidad de revisiones y auditorías).

Operación (Cláusula 8):
Gestión de activos: se avanza en inventario/gestión; se recomienda consolidar controles y revisiones periódicas.
Seguridad física: existen controles aplicados; se sugiere reforzar prácticas como escritorio limpio y mejorar almacenamiento/protección mediante verificaciones periódicas.
Seguridad de operaciones: se identifican oportunidades de mejora en separación de ambientes y en la sincronización NTP para fortalecer la seguridad operacional.
Seguridad de comunicaciones: se requiere fortalecer controles de segregación de redes y accesos a dispositivos críticos.

Adquisición, desarrollo y mantenimiento: se recomienda actualizar el manual/proceso de desarrollo para incorporar prácticas de desarrollo seguro y alinearlo con el estado tecnológico actual.
Gestión de incidentes: el procedimiento requiere formalización para asegurar respuesta consistente, roles claros, tiempos y escalamiento.
Continuidad: fortalecer mecanismos mediante pruebas documentadas, lecciones aprendidas y mejora del datacenter alterno.

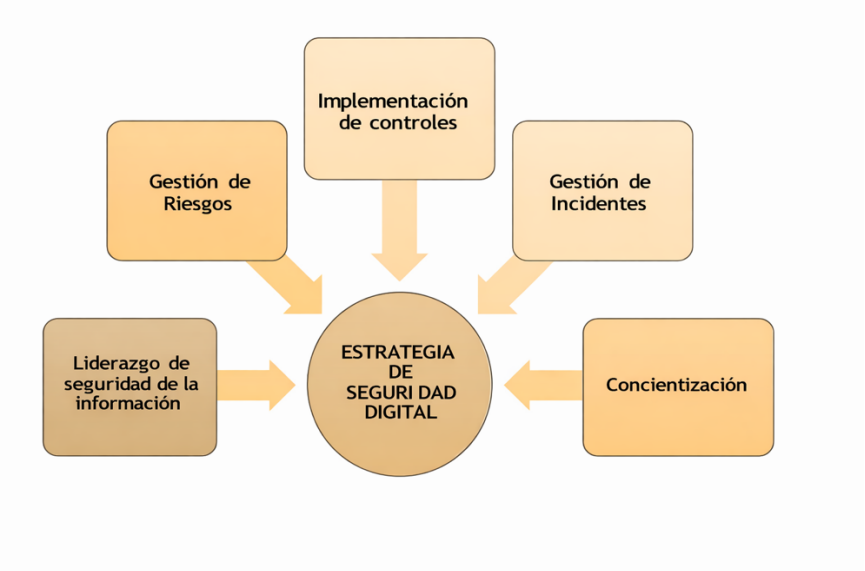
Evaluación del desempeño (Cláusula 9):
Se recomienda fortalecer la ejecución de auditorías internas e independientes de seguridad, así como el seguimiento sistemático a la eficacia de controles (indicadores, revisiones periódicas y planes de mejora).

Mejora (Cláusula 10):
Se requiere consolidar un ciclo de mejora continua (hallazgos → acciones correctivas → verificación de eficacia), priorizando brechas críticas en control de acceso, incidentes, continuidad, proveedores, criptografía y cumplimiento.

6. ESTRATEGIA DE SEGURIDAD DIGITAL

El SGC desarrollará una estrategia de seguridad digital que integre de manera armónica los principios, políticas, procedimientos, guías, manuales, formatos y lineamientos necesarios para la gestión efectiva de la seguridad de la información. Esta estrategia estará fundamentada en la implementación del Modelo de Seguridad y Privacidad de la Información (MSPI), la guía de gestión de riesgos de seguridad de la información y el procedimiento para la gestión de incidentes, el cual deberá ser establecido y formalizado.

En este contexto, el SGC define las siguientes cinco estrategias específicas, que en conjunto conformarán una estrategia general de seguridad digital integral:



Fuente: Elaboración Propia SGC

A continuación, se presentan los ejes estratégicos que estructuran la Estrategia de Seguridad Digital de la Entidad, en coherencia con el Modelo de Seguridad y Privacidad de la Información (MSPI). Estos ejes definen las líneas de acción prioritarias para orientar la gestión institucional de la seguridad de la información, integrando componentes de gobernanza y liderazgo, gestión del riesgo, cultura y apropiación, implementación de controles y gestión de incidentes, con el propósito de fortalecer la protección de la confidencialidad, integridad y disponibilidad de los activos de información.

ESTRATEGIA / EJE	DESCRIPCIÓN/OBJETIVO
Liderazgo de seguridad de la información	Asegurar que se establezca el Modelo de Seguridad y Privacidad de la Información (MSPI) a través de la aprobación de la política general y demás lineamientos que se definan buscando proteger la confidencialidad, integridad y disponibilidad de la información teniendo como pilar fundamental el compromiso de la alta dirección y de los líderes de las diferentes dependencias y/o procesos de la Entidad a través del establecimiento de los roles y responsabilidades en seguridad de la información.
Gestión de riesgos	Determinar los riesgos de seguridad de la información a través de la planificación y valoración que se defina buscando prevenir o reducir los efectos indeseados tendiendo como pilar fundamental la implementación de controles de seguridad para el tratamiento de los riesgos.
Concientización	Fortalecer la construcción de la cultura organizacional con base en la seguridad de la información para que convierta en un hábito, promoviendo las políticas, procedimientos, normas, buenas prácticas y demás lineamientos, la transferencia de conocimiento, la asignación y divulgación de responsabilidades de todo el personal de la entidad en seguridad y privacidad de la información.
Implementación de controles	Planificar e implementar las acciones necesarias para lograr los objetivos de seguridad y privacidad de la información y mantener la confianza en la ejecución de los procesos de la Entidad, se pueden subdividir en controles tecnológicos y/o administrativos.
Gestión de incidentes	Garantizar una administración de incidentes de seguridad de la información con base a un enfoque de integración, análisis, comunicación de los eventos e incidentes y las debilidades de seguridad en pro de conocerlos y resolverlos para minimizar el impacto negativo de estos en la Entidad.

7. PORTAFOLIO DE PROYECTOS/ ACTIVIDADES

Para cada estrategia específica, el Servicio Geológico Colombiano (SGC) define los siguientes proyectos, actividades y productos esperados, orientados a asegurar la implementación, fortalecimiento y mejora continua del Sistema de Gestión de Seguridad de la Información (SGSI).

ESTRATEGIA / EJE	PROYECTO	PROYECTO (INDICADOR)	PRODUCTOS ESPERADOS
Implementación de controles	Adoptar formalmente el instrumento oficial vigente de autodiagnóstico del MSPI publicado por MinTIC, diligenciándolo íntegramente sin modificar su estructura, dominios ni campos, y documentando su aplicación como insumo oficial de la fase de diagnóstico del MSPI, garantizando su alineación normativa con el Documento Maestro MSPI 2025 y la ISO/IEC 27001:2022.	instrumento oficial vigente del MSPI	instrumento oficial vigente del MSPI
Implementación de controles	Completar y ajustar el diligenciamiento del instrumento oficial de autodiagnóstico MSPI asegurando que cada control cuente con una brecha claramente descrita, una acción de mejora específica, medible y verificable, y la evidencia correspondiente, fortaleciendo su uso como insumo válido para la fase de planificación del MSPI.	Avance del diligenciamiento= (Número de hojas del instrumento MSPI diligenciadas/ Número total de hojas del instrumento MSPI)×100	instrumento oficial vigente del MSPI diligenciado

ESTRATEGIA / EJE	PROYECTO	PROYECTO (INDICADOR)	PRODUCTOS ESPERADOS
Gestión de riesgos	Ampliar y actualizar el documento de contexto institucional del MSPI incorporando explícitamente los factores internos y externos definidos en el Documento Maestro MSPI 2025, vinculándolos con procesos, activos de información, servicios digitales y riesgos de seguridad de la información.	Documento con el contexto institucional del MSPI incorporando explícitamente los factores internos y externos definidos en el Documento Maestro MSPI 2025, vinculándolos con procesos, activos de información, servicios digitales y riesgos de seguridad de la información.	Documento con el contexto institucional del MSPI incorporando explícitamente los factores internos y externos definidos en el Documento Maestro MSPI 2025, vinculándolos con procesos, activos de información, servicios digitales y riesgos de seguridad de la información.
Liderazgo de seguridad de la información	Complementar el alcance actual del MSPI determinando claramente los límites, aplicabilidad, procesos, recursos, activos de información, sistemas y áreas seguras cubiertas por el modelo.	Documento complemento del alcance actual del MSPI determinando claramente los límites, aplicabilidad, procesos, recursos, activos de información, sistemas y áreas seguras cubiertas por el modelo.	Documento complemento del alcance actual del MSPI determinando claramente los límites, aplicabilidad, procesos, recursos, activos de información, sistemas y áreas seguras cubiertas por el modelo.
Implementación de controles	Actualizar la Declaración de Aplicabilidad conforme a ISO/IEC 27001:2022, incorporando el estado de implementación y la justificación de exclusiones, y gestionar su aprobación formal ante el Comité Institucional de Gestión y Desempeño.	Avance del SoA (%)=(Número de controles del SoA documentados /Número total de controles ISO/IEC 27001:2022) ×100	SoA diligenciado
Concientización	Gestionar, mediante correo electrónico, con el área de Talento Humano la inclusión	El área de Talento Humano hace la inclusión de temas de seguridad de la	Talento Humano incluyo temas de seguridad de la información en el

ESTRATEGIA / EJE	PROYECTO	PROYECTO (INDICADOR)	PRODUCTOS ESPERADOS
	de temas de seguridad de la información en el Plan Institucional de Capacitación (PIC).	información en el Plan Institucional de Capacitación (PIC).	Plan Institucional de Capacitación (PIC).
Gestión de riesgos	Gestionar, en articulación con el Grupo de Planeación Institucional y los líderes de proceso, la formalización del Plan de Implementación de Controles del MSPI, asegurando su validación y aprobación por los responsables de los procesos, la estructuración documental del plan y su elevación al Comité Institucional de Gestión y Desempeño (CIGD) cuando se requiera toma de decisiones o asignación de recursos, garantizando la trazabilidad entre los controles planificados y las decisiones de tratamiento del riesgo previamente definidas en el marco del MSPI, así como la identificación y documentación de los controles cuya implementación requiera priorización institucional.	Avance del Plan de Implementación de Controles (%)=Número de hitos completados /4×100	Plan de Implementación de Controles
Implementación de controles	Gestionar la formalización del seguimiento e indicadores de seguridad de la información mediante la incorporación de las hojas de vida de los indicadores del MSPI en el tablero de	Avances indicadores	Indicadores MSPI

ESTRATEGIA / EJE	PROYECTO	PROYECTO (INDICADOR)	PRODUCTOS ESPERADOS
	control del Plan de Acción institucional		
Gestión de Incidentes	Concientizar a usuarios finales para la prevención y reporte de incidentes de seguridad de la información	(Número de acciones de concientización ejecutadas/Número de acciones de concientización planeadas)x100	Piezas de sensibilización relizadas

8. CRONOGRAMA DE ACTIVIDADES/ PROYECTOS

El responsable de seguridad de la información, con base a los proyectos definidos en la sección anterior, deberá establecer un cronograma de actividades donde se evidencie como se llevarán a cabo cada uno de los proyectos previstos. Las actividades podrán desarrollarse de forma secuencial o paralela según se considere.

ESTRATEGIA / EJE	PROYECTO	T1	T2	T3	T4
Implementación de controles	Adoptar formalmente el instrumento oficial vigente de autodiagnóstico del MSPI (MinTIC).	■	■		
Implementación de controles	Completar y ajustar el diligenciamiento del autodiagnóstico MSPI (brechas, acciones y evidencias).	■	■	■	
Gestión de riesgos	Ampliar y actualizar el documento de contexto institucional del MSPI (factores internos/externos, procesos, activos, servicios y riesgos).		■	■	
Liderazgo de seguridad de la información	Complementar el alcance del MSPI (límites, aplicabilidad, procesos, activos, sistemas y áreas).		■	■	
Implementación de controles	Actualizar SoA ISO/IEC 27001:2022 y gestionar aprobación en CIGD.		■		
Concientización	Gestionar con Talento Humano inclusión de temas de seguridad de la información en el PIC.	■	■	■	■
Gestión de riesgos	Formalizar Plan de Implementación de Controles del MSPI (validación, aprobación y trazabilidad con tratamiento del riesgo).	■	■	■	
Implementación de controles	Formalizar seguimiento e indicadores: incorporar hojas de vida de indicadores		■	■	■

	MSPI al tablero del Plan de Acción.				
Gestión de Incidentes	Concientizar a usuarios finales para la prevención y reporte de incidentes de seguridad de la información			[redacted]	[redacted]

Nota: Al finalizar cada vigencia el SGC, realizará una actualización del cronograma, incorporando el estado del avance de los proyectos formulados y si en efecto se cumplieron o se plantean aplazamientos para las vigencias posteriores. Así mismo, el cronograma podrá ser modificado o ajustado de acuerdo con las necesidades o situaciones que surjan en la entidad.

9. REPONSABLES

Director(a)/Representante Legal de la Entidad

Garantizar la implementación del MSPI, asegurando la disponibilidad de los recursos necesarios para su ejecución y supervisando su cumplimiento.

Secretario(a) General

Respaldar la implementación del MSPI, velando por la adecuada asignación de recursos y promoviendo el cumplimiento de los lineamientos establecidos.

Comité de Gestión y Desempeño

Aprobar los documentos estratégicos y de alto nivel relacionados con el MSPI, garantizando su alineación con los objetivos institucionales.

Responsable de Seguridad Digital / CIO

Coordinar y liderar las actividades relacionadas con la implementación del MSPI, supervisando la ejecución de las estrategias definidas y asegurando la articulación entre las diferentes áreas.

Grupo de Trabajo de Gestión de Plataforma de Tecnologías de Información

Brindar apoyo al responsable de Seguridad Digital / CIO en la implementación del Sistema de Gestión de Seguridad de la Información (SGSI), ejecutando tareas técnicas y operativas necesarias para alcanzar los objetivos del MSPI.

Grupo de Trabajo de Planeación

Brindar apoyo en las actividades relacionadas con la identificación, levantamiento y documentación de activos de información y riesgos asociados, coordinando con las diferentes áreas de la Entidad para garantizar un enfoque integral y alineado con los objetivos del MSPI y de la política de gestión de riesgos de la entidad.

Áreas de la Entidad

Participar activamente en la implementación del MSPI, cumpliendo con los roles y responsabilidades asignados, y asegurando la integración de las estrategias de seguridad digital en los procesos institucionales.

10. PRESUPUESTO Y RECURSOS

10.1 Recursos técnicos

El SGC dispone de recursos técnicos y de gestión que soportan la administración del plan estratégico de seguridad de la información:

- Repositorios y documentación de soporte (políticas, procedimientos, inventarios de activos, registros de incidentes, evidencias de control, reportes de seguimiento, etc.).

Articulación con el PETI (recursos habilitantes TIC):

En el marco del Plan Estratégico de Tecnologías de la Información (PETI), el SGC cuenta con el proyecto PR_A_03 – Gestión de tecnologías de información y comunicaciones, orientado a apoyar los procesos institucionales mediante la adopción y adaptación de normas, estándares y especificaciones para asegurar el acceso, almacenamiento, uso, intercambio y seguridad informática de la información, soportado en tecnologías de información y comunicaciones.

Este proyecto habilito, entre otros, los siguientes componentes:

- Plataforma tecnológica
- Enlace y comunicaciones
- Implementación de sistemas de información
- Servicio de atención al usuario y centro de soporte IT
- Estos componentes constituyen recursos técnicos fundamentales para la ejecución de controles de seguridad, la disponibilidad de servicios tecnológicos y la continuidad de la operación.

10.2 Recursos logísticos

El SGC dispone de recursos logísticos para realizar actividades de gestión del riesgo, incluyendo:

- Espacios, medios y herramientas para socializaciones, transferencia de conocimiento y sesiones de trabajo relacionadas con la seguridad de la información.
- Soportes para el seguimiento periódico a la ejecución de controles y planes de acción (reuniones, comités, actas, reportes y tableros de control institucionales).

10.3 Recursos financieros

El SGC cuenta con recursos financieros destinados a fortalecer capacidades institucionales relacionadas con la seguridad de la información y la continuidad de la operación, incluyendo adquisición de bienes/servicios, fortalecimiento de controles, apoyo técnico y ejecución de actividades asociadas a planes de trabajo y seguimiento.

Proyecto: proyecto PR_A_03 – Gestión de tecnologías de información y comunicaciones, orientado a apoyar los procesos institucionales mediante la adopción y adaptación de normas, estándares y especificaciones para asegurar el acceso, almacenamiento, uso, intercambio y seguridad informática de la información, soportado en tecnologías de información y comunicaciones.

Presupuesto asignado: $242.000.000

APROBACIÓN

El presente plan ha sido sometido a consideración y conocimiento de la alta dirección, el comité de gestión y desempeño institucional del SGC con el objetivo de ser aprobado y aplicado conforme a lo que aquí se define.

ELABORÓ	REVISÓ	APROBÓ
Andrea Neira Cargo: Contratista	Gloria Torres Cargo: Coordinadora Grupo de Trabajo de Gestión de Plataforma de Tecnologías de Información	Comité de Gestión y Desempeño Fecha:30/01/2026

Control de Versiones

Versión	Fecha	Modificación
1.0	30/01/2026	Versión para aprobación de CGD