PLAN ESTRATÉGICO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

SERVICIO GEOLÓGICO COLOMBIANO

PLAN ESTRATÉGICO DE SEGURIDAD DE LA INFORMACIÓN

Servicio Geológico Colombiano

SERVICIO GEOLÓGICO COLOMBIANO

2025

Control de Versiones

Versión	Fecha	Modificación
1.0		Versión para aprobación del comité de Gestión y Desempeño

Tabla de contenido

PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

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. Esto se logrará a través de la implementación efectiva de las estrategias de seguridad digital definidas en este documento, orientadas a fortalecer las capacidades institucionales durante el año 2025.

1.1OBJETIVOS ESPECÍFICOS

- Definir y formalizar la estrategia de seguridad digital de la Entidad, alineada con los marcos normativos, las necesidades institucionales y las mejores prácticas internacionales en seguridad de la información.
- Identificar y establecer los requerimientos técnicos, organizacionales y humanos necesarios para la adecuada implementación del Sistema de Gestión de Seguridad de la Información (SGSI) de la Entidad.
- Priorizar 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 y seguimiento continuo 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.

2.ALCANCE

El **Plan Estratégico de Seguridad de la Información**, orientado hacia la implementación del Sistema de Gestión de Seguridad de la Información (SGSI) y de la estrategia de seguridad digital de la Entidad, se alinea con el alcance establecido en la **Política General de Seguridad de la Información**. Dicho alcance contempla la aplicación de los principios y lineamientos de seguridad en todos los procesos de la Entidad, garantizando un enfoque integral en la protección de los activos de información y en la mitigación de riesgos asociados.

3. 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:

- **Decreto 612 de 2018**: "Por el cual se fijan directrices para la integración de los planes institucionales y estratégicos al Plan de Acción por parte de las entidades del Estado". Este decreto establece al PESI como un requisito fundamental para cumplir con las disposiciones normativas.
- **Resolución 500 de 2021**: "Por la cual se establecen los lineamientos y estándares para la estrategia de seguridad digital y se adopta el modelo de seguridad y privacidad como habilitador de la política de Gobierno Digital".
- **Ley 1581 de 2012**: "Por la cual se dictan disposiciones generales para la protección de datos personales". Esta ley refuerza el enfoque de protección de información sensible dentro del marco del PESI.
- **Decreto 1377 de 2013**: Reglamentario de la Ley 1581 de 2012, que complementa las disposiciones para la protección de datos personales en el ámbito institucional.
- **Manual de Gobierno Digital – MINTIC**: Instrumento técnico que define los lineamientos para la transformación digital de las entidades públicas, enmarcando la seguridad de la información como un eje transversal.
- **Modelo de Seguridad y Privacidad de la Información – MINTIC**: Referente técnico para la gestión de la seguridad y privacidad de la información en las entidades públicas, alineado con las mejores prácticas internacionales.
- **ISO/IEC 27001:2022**: Norma internacional que especifica los requisitos para establecer, implementar, mantener y mejorar un Sistema de Gestión de Seguridad de la Información (SGSI).
- **Política General de Seguridad de la Información de la Entidad**: Documento interno que define los principios, objetivos y lineamientos de seguridad aplicables a todos los procesos de la Entidad.

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

A continuación se describe el estado actual del sistema de gestión de seguridad de la información por cada uno de los dominios del MSPI del MinTIC.

5.Dominio 5 - Política de Seguridad de la Información

Se dispone de una política de seguridad actualizada, con la oportunidad de establecer un mecanismo periódico de revisión para garantizar su vigencia y adecuación.

6.Dominio 6 - Organización de la Seguridad de la Información

Es necesario fortalecer la estructura organizacional mediante la asignación de un Oficial de Seguridad de la Información (OSI) y el desarrollo de una matriz formal de roles y perfiles.

7.Dominio 7 - Seguridad de los Recursos Humanos

Los controles en selección, formación y disciplina están implementados, con posibilidades de ser actualizados regularmente para alinearse con normativas vigentes.

8.Dominio 8 - Gestión de Activos

Se avanza en la gestión de activos, con el potencial de consolidar controles más efectivos y realizar revisiones periódicas.

9.Dominio 9 - Control de Acceso

Se requiere optimizar el control de acceso mediante la eliminación de cuentas genéricas y la actualización de la matriz de roles.

10.Dominio 10 - Criptografía

La política de criptografía puede ser fortalecida mediante la actualización de procedimientos y la definición de criterios claros para la gestión de llaves y selección de algoritmos seguros.

11.Dominio 11 - Seguridad Física

Se aplican controles adecuados, con la oportunidad de reforzar la política de escritorio limpio y mejorar el almacenamiento de información a través de auditorías periódicas.

12.Dominio 12 - Seguridad de las Operaciones

La separación de ambientes y la sincronización del servidor NTP pueden ser optimizadas para mejorar la seguridad operacional.

13.Dominio 13 - Seguridad de las Comunicaciones

La segregación de redes y los controles de acceso a dispositivos críticos pueden ser fortalecidos para garantizar comunicaciones más seguras.

14.Dominio 14 - Adquisición, Desarrollo y Mantenimiento de Sistemas

El manual de desarrollo tiene la oportunidad de ser actualizado para incorporar prácticas de desarrollo seguro y reflejar avances tecnológicos recientes.

15.Dominio 15 - Relaciones con los Proveedores

Es necesario incorporar análisis de riesgos en la gestión con proveedores para fortalecer la relación y garantizar la seguridad en los servicios contratados.

16.Dominio 16 - Gestión de Incidentes de Seguridad

El procedimiento de gestión de incidentes puede ser formalizado para garantizar una respuesta organizada y eficiente ante cualquier eventualidad.

17.Dominio 17 - Continuidad

Se pueden fortalecer los mecanismos de continuidad mediante la documentación de pruebas y la mejora de la infraestructura del datacenter alterno.

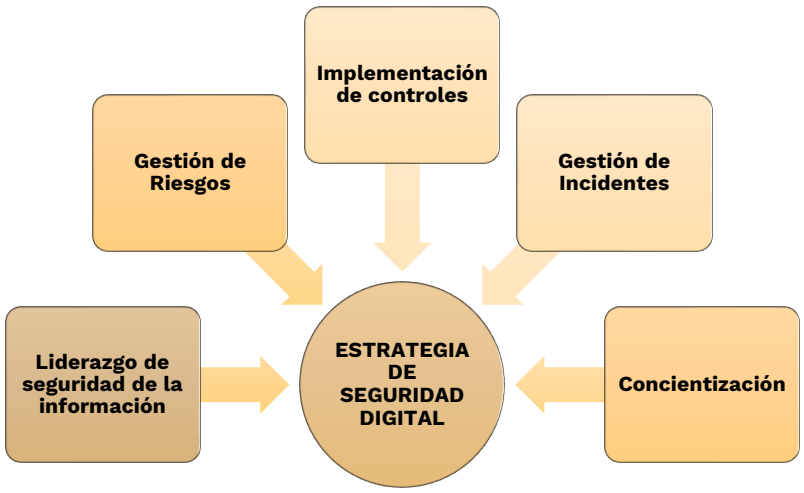
18.Dominio 18 - Cumplimiento

Se requiere fortalecer el cumplimiento normativo mediante la actualización de la tabla de retención documental, la designación de un Oficial de Protección de Datos Personales (OPDP) y la realización de auditorías de seguridad independientes.

19.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:



19.1 DESCRIPCIÓN DE LAS ESTRATEGIAS ESPECÍFICAS (EJES)

A continuación, se describe el objetivo de cada una de las estrategias específicas a implementar, alineando las actividades a lo descrito dentro del MPSI y la resolución 500 de 2021:

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.

19.2 PORTAFOLIO DE PROYECTOS / ACTIVIDADES:

Para cada estrategia específica, el SGC define los siguientes proyectos y productos esperados, que tienen por objetivo lograr la implementación y mejoramiento continuo del Sistema de Gestión de Seguridad de la Información (SGSI):

ESTRATEGIA / EJE	PROYECTO	PRODUCTOS ESPERADOS

Liderazgo de seguridad de la información	PROYECTO 1: Desarrollar e implementar una política de seguridad PROYECTO 2: Definición de Roles y Responsabilidades de Seguridad de la Información.	Política de Seguridad Formalizada e Implementada. Definición de los Roles y Responsabilidades en Seguridad de la Información formalizados dentro de las políticas de seguridad.
Gestión de riesgos	PROYECTO 1: Identificar, valorar y clasificar los riesgos asociados a los activos de información PROYECTO 2: Definir planes de tratamiento de riesgos de seguridad	Matriz de riesgos de seguridad digital Definir planes de tratamiento de riesgos
Concientización	PROYECTO 1: Establecer desde el inicio de cada año la planeación de sensibilización para todo el año. PROYECTO 2: Realizar jornadas de sensibilización a todo el personal. PROYECTO 3: Medir el grado de sensibilización a toda la Entidad.	1. Plan de Sensibilización 2. Evidencias de las actividades desarrolladas 3. Resultado de las encuestas de medición
Implementación de controles	CONTROL 1 Política de teletrabajo CONTROL 2 Revisión del manual de políticas de seguridad. CONTROL 3 Procedimiento de Clasificación de la información. CONTROL 4 Política de Desarrollo Seguro	Política de respaldos de información. Procedimiento de Gestión de Cambios. Clasificación de la información. Políticas de Desarrollo Seguro WAF desplegado y funcional.

Gestión de incidentes	**PROYECTO 1:** Definir y formalizar un procedimiento de Gestión de Incidentes de seguridad de la información. **PROYECTO 2:** Sensibilizar al personal en la gestión de incidentes de seguridad de la información.	1. Procedimiento de gestión de incidentes de seguridad formalizado. 2. Piezas gráficas con la sensibilización acerca del procedimiento y del reporte de incidentes de seguridad de la información.

19.3 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.

<table>
<tr><th colspan="4">AÑO 2025</th></tr>
<tr><th>TRIMESTRE 1</th><th>TRIMESTRE 2</th><th>TRIMESTRE 3</th><th>TRIMESTRE 4</th></tr>
<tr><td colspan="2">Realizar diagnóstico seguridad y privacidad
Aprobar política de seguridad de la información por resolución
Asignar al Oficial de Seguridad de la Información por resolución</td><td>Definir y formalizar un procedimiento de Gestión de Incidentes de seguridad de la información.</td><td>Sensibilizar al personal en la gestión de incidentes de seguridad de la información.</td></tr>
<tr><td colspan="3">Identificación de activos procesos misionales</td><td>Gestión de Riesgos de Seguridad</td></tr>
<tr><td colspan="4">Implementación de controles de seguridad informática acordes al presupuesto</td></tr>
<tr><td>Desarrollo Plan de Sensibilización 2025</td><td colspan="2">Adquisición e implementación Sistema de Análisis de Vulnerabilidades</td><td>Desarrollo Sensibilización 2025</td></tr>
</table>

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.

20.RESPONSABLES

1. 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.

2. Secretario(a) General

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

3. Comité de Gestión y Desempeño

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

4. 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.

5. 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.

6. 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.

7. 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.

21.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
Nombre: Andrea Neira **Cargo: Contratista**	Nombre: Gloria Torres **Cargo: Coordinadora Grupo de Trabajo de Gestión de Plataforma de Tecnologías de Información**	Nombre: Comité de Gestión y Desempeño Fecha: