SERVICIO GEOLÓGICO COLOMBIANO

Política General de Seguridad de la Información

1. Introducción

El Servicio Geológico Colombiano (SGC), como Instituto de Ciencia y Tecnología, está comprometido con el cumplimiento de sus funciones y reconoce la importancia de gestionar la información de manera segura. Con base en este compromiso, ha establecido, implementado y continuamente mejora su Sistema de Gestión de Seguridad de la Información (SGSI). Este sistema es esencial para proteger los activos de información digital que el SGC genera y administra, asegurando su integridad, confidencialidad y disponibilidad.

Conscientes de los riesgos identificados, la entidad implementa estrategias y controles adecuados para establecer una gestión segura de sus procesos, garantizando la máxima protección posible de los activos de información. La seguridad de la información es, por tanto, un componente vital del SGC, estructurado como un sistema de gestión que se integra con la protección de datos personales y la continuidad del negocio, en cumplimiento con los marcos normativos establecidos en Colombia para las entidades públicas.

El SGC considera que el conocimiento geocientífico es un pilar fundamental para el progreso social y económico del país. Por lo tanto, los datos y la información generada en las etapas de investigación y desarrollo de productos misionales se almacenan de manera integrada en fondos documentales y repositorios institucionales, asegurando su confiabilidad para su entrega a los usuarios. El SGSI establece los mecanismos necesarios para proteger, recuperar y conservar la información digital a lo largo del tiempo, garantizando su integridad, confidencialidad y disponibilidad, consolidando así una cultura de seguridad y privacidad de la información dentro de la entidad.

2. Marco legal

El SGC se acoge a las siguientes normas para el desarrollo y apropiación de su Política General de Seguridad de la Información:

- Constitución Política de Colombia, artículos 15, 209 y 269.
- Ley 1581 de 2012: Ley de Protección de Datos Personales.
- Ley 1712 de 2014: Ley de Transparencia y Acceso a la Información Pública Nacional.
- Ley 1915 de 2018: modificación de la Ley 23 de 1982 sobre derechos de autor y conexos.
- Ley 1952 de 2019: Código General Disciplinario.
- Decreto 2609 de 2012: Reglamento de Gestión Documental para las Entidades del Estado.
- Decreto 1377 de 2013: reglamento parcial de la Ley 1581 de 2012.
- Decreto 886 de 2014: Registro Nacional de Bases de Datos.
- Decreto 103 de 2015: reglamento parcial de la Ley 1712 de 2014.

• Decreto 1074 de 2015: Decreto Único Reglamentario del Sector Comercio, Industria y Turismo.
• Decreto 1078 de 2015: Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones.
• Decreto 1081 de 2015: Decreto Reglamentario del Sector Presidencial.
• Decreto 1083 de 2015: Decreto Único Reglamentario del Sector de Función Pública.
• Decreto 612 de 2018: integración de planes institucionales y estratégicos al Plan de Acción de las entidades del Estado.
• Decreto 1378 de 2019: establece normas para la gestión de riesgos de seguridad digital en el ámbito de las entidades del Estado, complementando las disposiciones sobre seguridad digital.
• Decreto 2106 de 2019: estrategia de seguridad digital para trámites y procedimientos digitales.
• Decreto 333 de 2021: en relación con la Ciberseguridad y Ciberdefensa en Colombia, enfocado en la protección de infraestructura crítica del Estado y servicios esenciales.
• Decreto 338 de 2022: lineamientos para la gobernanza de seguridad digital y respuesta a incidentes.
• Decreto 767 de 2022: este decreto establece disposiciones sobre la gestión de incidentes de ciberseguridad e infraestructura crítica y dicta las directrices relacionadas con la seguridad digital en el país.
• Resolución 2710 de 2017 - MinTIC: lineamientos para la implementación de la estrategia de seguridad digital en las entidades públicas.
• Resolución 500 de 2021: lineamientos para la adopción del Modelo de Seguridad y Privacidad de la Información.
• CONPES 3854 de 2016: Política Nacional de Seguridad Digital.
• CONPES 3995 de 2020: Política Nacional de Confianza y Seguridad Digital.
• Directiva Presidencial 02 de 2022: reiteración de la política pública en seguridad digital.
• Norma Técnica Colombiana NTC-ISO/IEC 27001: sobre sistemas de gestión de seguridad de la información, si se está utilizando un enfoque basado en estándares internacionales.

3. Objetivo general

El objetivo del SGSI es establecer, implementar, mantener y mejorar continuamente un modelo general de criterios, directrices, condiciones y pautas para proteger los activos de información digital del SGC. Este modelo incluye la información generada y administrada por el SGC en cumplimiento de sus funciones, así como sus procesos, sistemas de información, entidades interesadas y la transferencia de información.

3.1 Objetivos específicos

- Fortalecer la cultura de prevención de riesgos: a través de la sensibilización y el entrenamiento continuo de funcionarios, contratistas, terceros y partes interesadas que usen los activos de información del SGC.

- Gestionar oportunamente los riesgos: estableciendo e implementando planes de tratamiento y mejorando continuamente los controles de seguridad.

- Garantizar la disponibilidad de la información: haciéndola accesible y utilizable por entidades autorizadas mediante controles como copias de seguridad, enlaces de red redundantes, protección perimetral y defensa contra diferentes tipos de ataques.

- Asegurar la integridad de la información: manteniendo la precisión y confiabilidad de los datos.

- Preservar la confidencialidad: restringiendo el acceso a los sistemas de información críticos para el desarrollo de los procesos de la entidad.

- Gestionar incidentes de seguridad: robusteciendo la infraestructura del SGC para enfrentar ataques y amenazas informáticas.

- Promover la continuidad de las operaciones: mediante la implementación de herramientas y estrategias que aseguren la operación continua de los servicios de Tecnologías de la Información y la información digital.

4. Alcance

La Política General de Seguridad de la Información aplica a todos los activos de información digital del SGC, cubriendo todas las fases de gestión y tratamiento de la información, incluyendo los canales de comunicación utilizados para su recolección, transporte, almacenamiento, custodia, preservación, conservación o intercambio.

Esta política abarca todas las dependencias del SGC, de acuerdo con su organigrama institucional, y aplica a todos los procesos de la entidad.

La política será difundida entre todos los funcionarios, contratistas, terceros y partes interesadas con vínculos contractuales con el SGC. Su cumplimiento es obligatorio para todas las personas que generen, accedan o utilicen información de la entidad, a fin de garantizar su confidencialidad, integridad y disponibilidad.

5. Compromisos del SGC

El SGC, como responsable de la custodia, integridad, conservación, disponibilidad, clasificación, confidencialidad y tratamiento seguro de la información que produce y gestiona, se compromete a

establecer estrategias, lineamientos, protocolos, controles, proyectos, programas, planes y mecanismos que garanticen el tratamiento seguro de la información por parte de sus colaboradores.

Este compromiso incluye una gestión adecuada de los riesgos, el cumplimiento de los requisitos legales y la satisfacción de las necesidades de la entidad y las partes interesadas en materia de seguridad de la información digital.

6. Roles y responsabilidades

La adecuada gestión de la seguridad de la información dentro del SGC requiere la participación de múltiples actores, cada uno con responsabilidades específicas. A continuación, se detallan los roles y responsabilidades clave para garantizar la correcta implementación y mantenimiento del SGSI:

6.1 Alta dirección

La alta dirección del SGC tiene la máxima responsabilidad del SGSI y debe garantizar su implementación, mantenimiento y mejora continua. Sus responsabilidades incluyen:

Responsabilidad directa: la alta dirección es responsable de cualquier incidente de seguridad significativo que afecte los activos de información del SGC. En caso de un incidente, asumirá las consecuencias administrativas y legales derivadas de dicho suceso.

Provisión de recursos: garantizará la asignación de recursos humanos, técnicos y financieros necesarios para la implementación efectiva del SGSI.

Monitoreo y auditoría: asegurar que se realicen auditorías periódicas para verificar la efectividad del sistema de seguridad de la información y aplicar medidas correctivas si es necesario.

Cumplimiento normativo: garantizar que la entidad cumpla con las normativas legales vigentes en materia de seguridad de la información.

6.2 Oficial de Seguridad de la Información (OSI)

El Oficial de Seguridad de la Información (OSI) es el responsable de la supervisión operativa del SGSI. Sus principales responsabilidades son:

Supervisión y control: supervisar la implementación de las políticas de seguridad de la información y garantizar que se cumplan los controles establecidos.

Gestión de incidentes: coordinar la gestión de incidentes de seguridad, desde su detección hasta la resolución.

Sensibilización: desarrollar programas de sensibilización y concientización en seguridad de la información para todo el personal.

Auditorías y revisiones: participar en la planificación y ejecución de auditorías internas y revisiones periódicas del SGSI.

6.3 Responsables de áreas funcionales

Los responsables de áreas funcionales tienen la tarea de asegurar que las políticas de seguridad de la información se implementen adecuadamente dentro de sus respectivas áreas. Entre sus responsabilidades están:

Cumplimiento local: asegurar que los procesos bajo su supervisión cumplan con las políticas y procedimientos de seguridad de la información.

Reportes de vulnerabilidades: informar al OSI sobre cualquier vulnerabilidad o incidente de seguridad que afecte los activos de información de su área.

Protección de activos: garantizar que los activos de información bajo su control estén protegidos de acuerdo con las políticas de la entidad.

6.4 Usuarios finales

Todos los usuarios finales del SGC, incluidos funcionarios, contratistas y terceros, son responsables de:

Cumplir con las políticas de seguridad: adherirse estrictamente a las políticas y procedimientos establecidos para la seguridad de la información.

Confidencialidad: mantener la confidencialidad de la información a la que tienen acceso y no compartirla sin la debida autorización.

Reportar incidentes: notificar al Responsable de Seguridad de la Información de inmediato sobre cualquier incidente de seguridad o actividad sospechosa que pudiera comprometer la seguridad de la información.

6.5 Administradores de servicios de TI y administradores de sistemas

Los administradores de servicios de TI y los administradores de sistemas comparten la responsabilidad de implementar y mantener los controles técnicos que aseguren la protección de los sistemas de información del SGC. Entre sus responsabilidades están:

Gestión de accesos: asegurar que solo el personal autorizado tenga acceso a los sistemas de información.

Actualizaciones y mantenimiento: mantener los sistemas actualizados y aplicar parches de seguridad según sea necesario para garantizar que los servicios de TI estén protegidos contra vulnerabilidades.

Monitoreo continuo: realizar un monitoreo constante de los sistemas y servicios de TI para detectar y prevenir posibles amenazas y asegurar la continuidad del servicio.

7. Control de versiones

Versión	Fecha	Descripción
1	Diciembre de 2022	Creación de la política de gestión de seguridad de la información.
2	Enero de 2025	Aprobación de la política por el Comité de Gestión y Desempeño.

Esta política será publicada y difundida a todos los funcionarios, colaboradores y terceros.

HÉCTOR JULIO FIERRO MORALES
Director General
Servicio Geológico Colombiano

Elaboró: Andrea Catherine Neira Bustamante - Contratista DGI
Revisó: Alberto García Bolívar – Director de Gestión de Información
Gloria Stella Torres – Coordinadora GT Gestión de Plataforma de Tecnologías de Información
Óscar Omar Gómez Calderón – Jefe de la Oficina Asesora Jurídica
Aprobó: Comité Institucional de Gestión y Desempeño