




**POLÍTICA GENERAL DE SEGURIDAD DE LA INFORMACIÓN
DEL SERVICIO GEOLÓGICO COLOMBIANO**


COPIA NO CONTROLADA

Bogotá, diciembre 2022

	DOCUMENTO DE GESTIÓN	VERSIÓN: 2
		CÓDIGO: DG-GGC-012
	POLÍTICA GENERAL DE SEGURIDAD DE LA INFORMACIÓN DEL SERVICIO GEOLÓGICO COLOMBIANO	FECHA VIGENCIA: Diciembre 2022

Contenido

1. INTRODUCCIÓN	3
2. OBJETIVO	3
3. ALCANCE	3
4. BASE LEGAL	4
5. ELEMENTOS DE LA POLÍTICA	5
6.1. Metas de seguridad de la información	5
6.2. Declaración de la política	6
6.3. Principios	6
6.4. Consideraciones generales	7
6.4.1. Gestión documental	7
6.4.2. Líneas de acción para la seguridad de la información digital	8
6.5. Cumplimiento de la política	8
6.6. Incumplimiento de la política	10
6.7. Excepción	11
6. HISTORIAL DE VERSIONES	12

	DOCUMENTO DE GESTIÓN	VERSIÓN: 2
		CÓDIGO: DG-GGC-012
	POLÍTICA GENERAL DE SEGURIDAD DE LA INFORMACIÓN DEL SERVICIO GEOLÓGICO COLOMBIANO	FECHA VIGENCIA: Diciembre 2022

1. INTRODUCCIÓN

El Servicio Geológico Colombiano como Instituto de Ciencia y Tecnología, en cumplimiento de sus funciones y entendiendo la importancia de una gestión segura de la información, se ha comprometido con el establecimiento, implementación y mejora continua del Sistema de Gestión de Seguridad de la Información, como mecanismo para proteger los activos de información digital generados y administrados por el Servicio Geológico Colombiano. En consecuencia, la entidad deberá implementar estrategias y controles adecuados para los riesgos mapeados, tratando de establecer una gestión segura de los procesos y permitiendo brindar la mayor protección posible de los activos de información. Es por esto, que la seguridad de la información se considera pertinente y se estructura como un sistema de gestión que se integra con la protección de datos personales y la continuidad del negocio para cumplir con los marcos normativos establecidos en Colombia para las entidades públicas.

Para el Servicio Geológico Colombiano, el conocimiento geocientífico es la base 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 los productos misionales, se almacenan de forma integrada en los fondos documentales y repositorios institucionales, asegurando su confiabilidad para ser entregada a sus usuarios. El Sistema de Gestión de Seguridad de la Información, establece los mecanismos para proteger, recuperar y conservar la información digital en el tiempo, asegurando su integridad, confidencialidad y disponibilidad, consolidando la cultura de seguridad y privacidad de la información del Servicio Geológico Colombiano.


2. OBJETIVO

Establecer, implementar, mantener y mejorar continuamente el modelo general de los criterios, directivas, condiciones y pautas para proteger los activos de información digital del Servicio Geológico Colombiano, involucrando la información generada y administrada que por sus funciones debe operar, involucrando sus procesos, sistemas de información, entidades, personas interesadas en sus servicios y la transferencia de información.

3. ALCANCE

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

Esta Política cubre la totalidad de las dependencias de acuerdo con el organigrama Institucional y abarca la totalidad de sus procesos estratégicos, misionales y de apoyo del SGC.

	DOCUMENTO DE GESTIÓN	VERSIÓN: 2
	POLÍTICA GENERAL DE SEGURIDAD DE LA INFORMACIÓN DEL SERVICIO GEOLÓGICO COLOMBIANO	CÓDIGO: DG-GGC-012
		FECHA VIGENCIA: Diciembre 2022


Esta Política será difundida entre todos los funcionarios, contratistas, terceros y partes interesadas que posean cualquier vínculo contractual con el Servicio Geológico Colombiano.

De esta manera será de estricto cumplimiento por todos los funcionarios, contratistas, proveedores y la ciudadanía en general que generen, accedan o utilicen información de la Entidad, con el fin de garantizar su confidencialidad, integridad y disponibilidad.

4. BASE LEGAL

Conforme con lo establecido en la normatividad vigente el Servicio Geológico Colombiano - SGC, hace referencia a las siguientes normas, que se deben tener en cuenta para el desarrollo de la apropiación de la Política General del Sistema de Seguridad de la información en la Entidad:

- Constitución Política de Colombia. Artículos 15, 209 y 269.
- Ley 1581 de 2012. Por la cual se dictan disposiciones generales para la protección de datos personales.
- Ley 1712 de 2014. Por medio de la cual se crea la Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional.
- Ley 1915 de 2018. Por la cual se modifica la Ley 23 de 1982 y se establecen otras disposiciones en materia de derecho de autor y derechos conexos.
- Ley 1952 de 2019. Por medio de la cual se expide el código general disciplinario.
- Decreto 2609 de 2012. Por el cual se reglamenta el Título V de la Ley 594 de 2000, parcialmente los artículos 58 y 59 de la Ley 1437 de 2011 y se dictan otras disposiciones en materia de Gestión Documental para todas las Entidades del Estado.
- Decreto 1377 de 2013. Por el cual se reglamenta parcialmente la Ley 1581 de 2012.
- Decreto 886 de 2014. Por el cual se reglamenta el Registro Nacional de Bases de Datos.
- Decreto 103 de 2015. Por medio del cual se reglamenta parcialmente la Ley 1712 de 2014 y se dictan otras disposiciones.
- Decreto 1074 de 2015. Por medio del cual se expide el Decreto Único Reglamentario del Sector Comercio, Industria y Turismo. Reglamenta parcialmente la Ley 1581 de 2012 e imparte instrucciones sobre el Registro Nacional de Bases de Datos. Artículos 25 y 26.
- Decreto 1078 de 2015. Por medio del cual se expide el Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones.
- Decreto 1081 de 2015. Por medio del cual se expide el Decreto Reglamentario del Sector Presidencia.
- Decreto 1083 de 2015 “Por medio del cual se expide el Decreto Único Reglamentario del Sector de Función Pública”, el cual establece las políticas de Gestión y Desempeño Institucional, entre las que se encuentran las de “11. Gobierno Digital, antes Gobierno en Línea” y “12. Seguridad Digital”.
- 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.
- Decreto 2106 de 2019. Establece que las autoridades que realicen trámites, procesos y procedimientos por medios digitales, deberán disponer de una estrategia de seguridad

	DOCUMENTO DE GESTIÓN	VERSIÓN: 2
	POLÍTICA GENERAL DE SEGURIDAD DE LA INFORMACIÓN DEL SERVICIO GEOLÓGICO COLOMBIANO	CÓDIGO: DG-GGC-012
		FECHA VIGENCIA: Diciembre 2022


digital siguiendo los lineamientos que emita el Ministerio de Tecnologías de la Información y las Comunicaciones.

- Decreto 338 de 2022 - Lineamientos generales para fortalecer la gobernanza de seguridad digital, la identificación de infraestructuras cibernéticas críticas y servicios esenciales, la gestión de riesgos y la respuesta a incidentes de seguridad digital.
- Resolución 500 de 2021 - Lineamientos y estándares para la estrategia de seguridad digital y la adopción del Modelo de Seguridad y privacidad de la información.
- CONPES 3854 de 2016. Política Nacional de Seguridad Digital.
- MRAE - MinTIC 2021.
- Conpes 995 de 2020 - Política Nacional de confianza y seguridad digital
- Directiva presidencial 02 de 2022 - Reiteración de la política pública en materia de seguridad digital.

5. ELEMENTOS DE LA POLÍTICA

6.1. Metas de seguridad de la información

- Fortalecer la cultura de prevención de riesgos de seguridad de la información por medio de la sensibilización y el entrenamiento constante de funcionarios, contratistas, terceros y partes interesadas que hagan uso de los activos de información generados o administrados por el SGC.
- Gestionar oportunamente los riesgos de seguridad de la información a través del establecimiento e implementación de planes de tratamiento y el mejoramiento continuo de los controles de seguridad.
- Trabajar por la disponibilidad de la información para hacerla accesible y utilizable por una entidad autorizada, usando controles tales como copias de seguridad (backups), enlaces de red redundantes, protección perimetral, protección anti DDoS, entre otros.
- Procurar por la integridad de la información haciéndola precisa y confiable.
- Velar por la confidencialidad de la información mediante la restricción del acceso de los sistemas de información vitales para el desarrollo de los procesos de la entidad.
- Gestionar diligentemente los eventos e incidentes de seguridad de la información digital robusteciendo la infraestructura del SGC para hacer frente a ataques y amenazas informáticas.
- Actuar en pro de la Continuidad de las operaciones a través del establecimiento de herramientas y estrategias para mantener la operación referida a los servicios de TI y la información digital.

	DOCUMENTO DE GESTIÓN	VERSIÓN: 2
	POLÍTICA GENERAL DE SEGURIDAD DE LA INFORMACIÓN DEL SERVICIO GEOLÓGICO COLOMBIANO	CÓDIGO: DG-GGC-012
		FECHA VIGENCIA: Diciembre 2022

6.2. Declaración de la política


El SGC como responsable de garantizar la custodia, integridad, conservación, preservación, disponibilidad, clasificación, reserva legal, confidencialidad, y tratamiento seguro de la información que produce y a la que tiene acceso en desarrollo de su misión, funciones y deberes, se compromete a establecer estrategias, lineamientos, protocolos, controles, proyectos, programas, planes y mecanismos de seguridad de la información, para el tratamiento seguro de la misma, por parte de sus colaboradores.

Lo anterior, considerando una gestión apropiada de los riesgos y el cumplimiento de los requisitos legales, las necesidades de la entidad y las partes interesadas sobre la seguridad de la información digital.

6.3. Principios

Teniendo en cuenta las condiciones normativas antes mencionadas, los lineamientos, controles, protocolos, procesos, procedimientos y mecanismos que se deriven de esta política, estarán orientados al cumplimiento de los siguientes principios en pro de la seguridad de la información digital:

- **Principio de Gestión de Riesgos del Sistema Integrado:** el Sistema Integrado de Gestión de del SGC debe garantizar que los riesgos de la seguridad de la información sean conocidos, asumidos, gestionados y mitigados por el SGC, de una forma documentada, sistemática, estructurada, eficiente y adaptada a los cambios que se produzcan en los riesgos, en el entorno y en las tecnologías.
- **Principio de Ética:** los colaboradores del SGC deben velar por la protección de la información que contribuya a la misionalidad de la entidad, con el fin de garantizar su preservación, prevenir fugas y usos indebidos o ilegítimos. La objetividad, imparcialidad y la resistencia a cualquier tipo de presión que pretenda manipular la documentación o distorsionar los hechos hacen parte de este principio.
- **Principio de Confidencialidad:** el SGC establece los mecanismos necesarios para contar con la confidencialidad de la información recibida o generada en cumplimiento de su mandato constitucional y legal.
- **Principio de Integridad:** el SGC establece los mecanismos necesarios para realizar acciones orientadas a mantener la exactitud, completitud e inalterabilidad de la información recibida o generada en cumplimiento de su mandato constitucional y legal.
- **Principio de Disponibilidad:** el SGC establece los requisitos y criterios necesarios para localizar, recuperar, presentar, interpretar y leer la información en el momento pertinente o requerido por las personas debidamente autorizadas para ello.

	DOCUMENTO DE GESTIÓN	VERSIÓN: 2
	POLÍTICA GENERAL DE SEGURIDAD DE LA INFORMACIÓN DEL SERVICIO GEOLÓGICO COLOMBIANO	CÓDIGO: DG-GGC-012
		FECHA VIGENCIA: Diciembre 2022


- **Principio de Integralidad:** la Política de General de Seguridad de la Información, Protección de Datos Personales y Continuidad del Negocio de los Servicios de TI será observada por todas las personas, ya sean funcionarios, contratistas o personal delegado del SGC, inclusive cuando la gestión o actividades de tratamiento de la información no sean parte de su función principal.
- **Principio de control de la información:** la información clasificada, es decir, aquella relacionada con datos personales a la que tenga acceso el SGC, pertenece al sujeto al que hace referencia la misma y, por tanto, éste siempre tendrá el control sobre ella. El control sobre la información implica que la persona deberá estar enterada del tratamiento que se dé a sus datos personales confidenciales y en cualquier momento podrá solicitar a el SGC el borrado de su información.
- **Principio de uso racional de la información:** el SGC y sus colaboradores, tendrán acceso únicamente a la información que requieran para el desarrollo de su mandato y/o funciones.

6.4. Consideraciones generales

A continuación, se describen los elementos de política para la construcción de estrategias, lineamientos, protocolos, controles, proyectos, programas, planes y mecanismos de seguridad, protección y confidencialidad de la información digital que deben ser detallados dentro del Sistema Integrado de Gestión de la entidad.

6.4.1. Gestión documental

El modelo de gestión de información en el SGC se enmarca en una sola gestión documental que, en concordancia con el principio de confidencialidad, tiene en cuenta dos instancias. La primera instancia abarca, por una parte, la información misional que contribuye al desarrollo económico y social del país, a través de la investigación en geociencias básicas y aplicadas del subsuelo, el potencial de sus recursos, la evaluación y monitoreo de amenazas de origen geológico, la gestión integral del conocimiento geocientífico, la investigación y el control nuclear y radiactivo, atendiendo las prioridades de las políticas del Gobierno Nacional, por tanto, las actividades relacionadas con la creación, recepción, mantenimiento, uso, disposición y preservación de los documentos electrónicos a través de su ciclo vital, deben hacerse considerando las particularidades que exige la salvaguarda de la confidencialidad o reserva legal de la información, con el fin de garantizar la integridad, autenticidad, fiabilidad y accesibilidad únicamente por el personal autorizado, a lo largo del tiempo.

	DOCUMENTO DE GESTIÓN	VERSIÓN: 2
	POLÍTICA GENERAL DE SEGURIDAD DE LA INFORMACIÓN DEL SERVICIO GEOLÓGICO COLOMBIANO	CÓDIGO: DG-GGC-012
		FECHA VIGENCIA: Diciembre 2022


6.4.2. Líneas de acción para la seguridad de la información digital

Las líneas de acción hacen referencia a las Políticas que se describen en el Manual de Políticas Específicas del Sistema Integrado de Gestión de Seguridad de la Información, Protección de Datos Personales y Continuidad del Negocio del Servicio Geológico Colombiano.

6.5. Cumplimiento de la política

Todas las personas cubiertas por el alcance y aplicabilidad deberán dar cumplimiento al 100% de la política. De igual manera el Servicio Geológico Colombiano se compromete con lo siguiente:

- El SGC a través del equipo delegado para la gestión de Seguridad de la información de la DGI, deberá asegurar que las políticas y los objetivos del Sistema de Gestión de Seguridad de la Información, sean herramientas adecuadas para proteger los activos de información digital adecuados al propósito de la entidad.
- El SGC a través de su Consejo Directivo, dispondrá de los recursos administrativos y financieros necesarios para alcanzar y mantener los objetivos del Sistema de Gestión de Seguridad de la Información.
- El SGC a través del equipo delegado para la gestión de Seguridad de la información de la DGI, definirá las políticas para que las áreas y procesos del SGC logren proteger la información creada, procesada, transmitida y resguardada durante sus actividades del día a día, con el fin de minimizar impactos de los riesgos de seguridad de la información.
- El SGC a través del equipo delegado para la gestión de Seguridad de la información de la DGI, realizará un monitoreo preventivo, detectivo y correctivo sobre el adecuado funcionamiento de los controles en las áreas para proteger la información de acuerdo con su clasificación de los activos de información.
- El SGC a través del equipo delegado para la gestión de Seguridad de la información de la DGI, supervisará los perfiles de riesgos Seguridad de la Información, e informará de forma preventiva y proactiva a los interesados posibles desviaciones para tomar las decisiones necesarias.
- El SGC a través del equipo delegado para la gestión de Seguridad de la información de la DGI, implementará políticas específicas para salvaguardar los equipos y la infraestructura tecnológica que soporta sus procesos críticos.
- El SGC a través del equipo delegado para la gestión de plataformas tecnológicas de la DGI, proveerá los permisos y privilegios necesarios para la implementación de controles para realizar seguimiento a la operación de sus procesos de negocio, garantizando los


	DOCUMENTO DE GESTIÓN	VERSIÓN: 2
	POLÍTICA GENERAL DE SEGURIDAD DE LA INFORMACIÓN DEL SERVICIO GEOLÓGICO COLOMBIANO	CÓDIGO: DG-GGC-012
		FECHA VIGENCIA: Diciembre 2022

procedimientos de seguridad de la información afines a los recursos tecnológicos y las redes de datos.

- El SGC a través del equipo delegado para la gestión de Seguridad de la información de la DGI, trabajará para que la seguridad sea parte integral del ciclo de vida de los sistemas de información.
- El SGC a través del equipo delegado para la gestión de Seguridad de la información de la DGI, procurará por una adecuada gestión de los eventos de seguridad y las vulnerabilidades asociadas a los sistemas de información, a través de una mejora continua y efectiva de su modelo de seguridad.
- El SGC a través del equipo delegado para la gestión de Seguridad de la información de la DGI, procurará mantener la disponibilidad de sus procesos de negocio y la continuidad de su operación basada en el análisis de los eventos.
- El SGC a través del equipo delegado para la gestión de Seguridad de la información de la DGI, deberá velar por el cumplimiento de los requisitos legales o reglamentarios y las obligaciones contractuales en materia de Seguridad de la Información.
- La Política de Seguridad de la Información debe ser revisada, por los Comités establecidos en el sistema de gestión al menos una vez al año, y/o cuando ocurran cambios significativos en la entidad, garantizando su evolución y cumplimiento, con el fin de lograr la mejora continua del Sistema de Gestión de Seguridad de la Información
- La Alta Dirección garantizará que el personal del SGC relacionado directamente con el establecimiento, implementación y mejora continua del Sistema Integrado de Gestión de Seguridad de la Información, cuente con las competencias, formación y capacitación necesarias para ejercer las funciones y responsabilidades establecidas en dicho sistema, con el fin de asegurar el cumplimiento de sus objetivos.

Por otra parte, los usuarios de información del SGC se comprometen a:

- Toda persona que tenga acceso a información Institucional del SGC, debe mantenerla en estricta confidencialidad y no deberá compartirla ni modificarla sin la debida autorización.
- Los funcionarios, contratistas y terceros deben acceder exclusivamente a la información a la que tienen permisos y que es necesaria para cumplir sus funciones.
- Los usuarios tienen la obligación de reportar los incidentes que afecten la Seguridad de la Información de acuerdo a los procedimientos y los canales establecidos en el Sistema

	DOCUMENTO DE GESTIÓN	VERSIÓN: 2
	POLÍTICA GENERAL DE SEGURIDAD DE LA INFORMACIÓN DEL SERVICIO GEOLÓGICO COLOMBIANO	CÓDIGO: DG-GGC-012
		FECHA VIGENCIA: Diciembre 2022


Integrado de Gestión de Seguridad de la Información, Protección de Datos Personales y Continuidad de Negocio de los Servicios de TI.

- Los funcionarios, contratistas, proveedores y público en general del SGC deben conocer, cumplir y divulgar, ésta y todas las políticas y buenas prácticas de Seguridad de la Información del SGC.
- Las Políticas de Seguridad de la Información son de aplicación obligatoria para todos los funcionarios, contratistas y proveedores del SGC, así como a cualquier persona que tenga acceso a la información de carácter institucional independientemente del área en la que se encuentren y sin importar las características de las tareas que desempeñen.
- Es de carácter obligatorio la implementación de las Políticas de Seguridad de la Información, en cada una de las direcciones, así como el cumplimiento de dichas políticas por funcionarios, contratistas, terceros y partes interesadas.

6.6. Incumplimiento de la política

En caso del incumplimiento de la política, el SGC a través de la secretaria general, ha establecido un proceso disciplinario formal para los funcionarios y contratistas que hayan cometido alguna violación de la Política de Seguridad de la Información, es considerada dentro de otras:

- El incumplimiento a las políticas traerá consigo las consecuencias que apliquen según el procedimiento disciplinario del SGC y asumirá las responsabilidades de tipo disciplinario o legal incluyendo lo establecido en las normas que competen al Gobierno Nacional en cuanto a Seguridad de la Información se refiere y las disposiciones sobre contratación pública.
- La copia, sustracción, daño intencional o utilización para fines distintos a labores propias de la entidad serán consideradas como una violación a las Políticas de Seguridad de la Información de SGC.
- La descarga, instalación o uso de software ilegal o sin licenciar será considerada como una violación a las Políticas de Seguridad de la Información y datos personales del SGC.
- Los funcionarios, contratistas o terceros que de la investigación del incidente se encuentren responsables, deben asumir las consecuencias legales, administrativas, disciplinarias o de otra índole que apliquen a la normativa del SGC, incluyendo lo establecido en las normas que competen al Gobierno nacional en cuanto a Seguridad de la Información se refiere.

	DOCUMENTO DE GESTIÓN	VERSIÓN: 2
	POLÍTICA GENERAL DE SEGURIDAD DE LA INFORMACIÓN DEL SERVICIO GEOLÓGICO COLOMBIANO	CÓDIGO: DG-GGC-012
		FECHA VIGENCIA: Diciembre 2022


Tenga en cuenta: el incumplimiento a las políticas traerá consigo las consecuencias que apliquen según el procedimiento disciplinario del SGC y asumirá las responsabilidades de tipo disciplinario o legal incluyendo lo establecido en las normas que competen al Gobierno Nacional en cuanto a Seguridad de la Información se refiere y las disposiciones sobre contratación pública.

6.7. Excepción

El manejo de excepciones en la presente Política de Seguridad de la Información será validado por el Oficial de la Seguridad de la Información, siempre que sean evaluadas y autorizadas por la Dirección General. Si la EXCEPCIÓN se encuentra documentada, su aplicación dependerá de la acción establecida para llevarla a cabo

Ante la necesidad de una nueva excepción a la política de seguridad se deberá solicitar al Oficial de Seguridad de la Información mediante el registro de un incidente de seguridad (conforme al procedimiento de gestión de incidentes de seguridad), analizar el riesgo correspondiente y determinar las acciones de mitigación para llevar a cabo la excepción.

COPIA NO CONTROLADA

	DOCUMENTO DE GESTIÓN	VERSIÓN: 2
	POLÍTICA GENERAL DE SEGURIDAD DE LA INFORMACIÓN DEL SERVICIO GEOLÓGICO COLOMBIANO	CÓDIGO: DG-GGC-012
		FECHA VIGENCIA: Diciembre 2022

6. HISTORIAL DE VERSIONES

Versión	Fecha	Control de Cambios
1	15/jul./2019	Elaboración primera versión del documento
2	27/dic/2022	Se realizó el ajuste del formato del documento y del contenido en cuanto a su objetivo, alcance, roles y responsabilidades, principios y normatividad.

ELABORÓ		REVISÓ		APROBÓ	
Nombre:	Andrea Catherine Neira Bustamante	Nombre:	Jaime Andrés Oliva Ortega	Nombre:	Victoria Eugenia Díaz Acosta
Cargo:	CONTRATISTA	Cargo:	CONTRATISTA	Cargo:	DIRECTORA
Fecha:	Diciembre 2022	Fecha:	Diciembre 2022	Fecha:	Diciembre 2022
Nombre:	Manuel Antonio Calvache	Nombre:	Andrea Catherine Neira Bustamante	Cargo:	TÉCNICA GESTIÓN DE INFORMACIÓN GEOCIENTÍFICA
Cargo:	CONTRATISTA	Cargo:	CONTRATISTA	Fecha:	Diciembre 2022
Fecha:	Diciembre 2022	Fecha:	Diciembre 2022		
		Nombre:	Franks Oróstegui Forero		
		Cargo:	CONTRATISTA		
		Fecha:	Diciembre 2022		