IGAC
INSTITUTO GEOGRÁFICO AGUSTÍN CODAZZI

Sistema de Gestión Integrado MIPG

SGC
Sistema de Gestión de Calidad

SGA
Sistema de Gestión Ambiental

SGSST
Sistema de Gestión de la Seguridad y Salud en el Trabajo

SGD
Sistema de Gestión Documental

SCI
Sistema de Control Interno

SLNS
Sistema Laboratorio Nacional de Suelos

SGSI
Sistema de Gestión de Seguridad de la Información

IGAC
INSTITUTO GEOGRÁFICO AGUSTÍN CODAZZI

Sistema de Gestión Integrado MIPG

Política

General de Seguridad de la Información del IGAC

Código: PL-GET-01 **Versión:** 1 **Vigente desde:** 24/07/2024

1. INTRODUCCIÓN

El Instituto Geográfico Agustín Codazzi (IGAC) es la autoridad en la regulación, producción y articulación de información geográfica, catastral y agrológica de alta calidad en el país. Esta información es crítica para la toma de decisiones en diversos ámbitos, y su pérdida, divulgación o manipulación indebida puede afectar la confiabilidad e integridad del trabajo realizado por la entidad. Por lo tanto, el IGAC se compromete a proteger la información que maneja, administra y recolecta, así como a minimizar los riesgos asociados con su uso y acceso indebidos. La seguridad de la información es fundamental para el éxito y la continuidad de las operaciones del IGAC y para la confianza que las partes interesadas depositan en la entidad.

La política de seguridad de la información tiene como objetivo establecer los principios generales y las directrices necesarias para garantizar la protección adecuada de la información del IGAC, tomando como marco de referencia la normativa legal vigente y las normas técnicas internacionales en materia de seguridad de la información. La política define los controles que la entidad debe seguir para proteger la información en sus tres pilares principales (confidencialidad, integridad, disponibilidad), y minimizar los riesgos asociados al manejo de esta.

Esta política es aplicable a todos los servidores públicos, contratistas y proveedores que tengan acceso a la información del IGAC, a todos los procesos y subprocesos definidos en la cadena de valor de IGAC, así como a todas las sedes del instituto (Sede Central, Direcciones Territoriales y Centro de Atención) y establece en sus roles y responsabilidades desde la línea estratégica al Comité Institucional de Gestión y Desempeño, en la línea de implementación a la Dirección de Tecnologías de la Información y las Comunicaciones, la Oficina Asesora Jurídica, la Subdirección de Talento Humano, la Secretaría General, la Oficina Asesora de Planeación, los Lideres de Proceso y Directores Territoriales, con respecto a la línea de seguimiento se encuentra la Oficina Asesora de Planeación y finalmente la línea de control y evaluación la Oficina de Control Interno. Además, se establecen medidas para la implementación y mantenimiento de los controles de seguridad de la información por medio del Manual de Seguridad de la Información el cual hace parte integral de este documento.

2. OBJETIVO

Establecer la estrategia de actuación institucional, directrices, criterios y establecimiento de controles para la adecuada gestión de la seguridad de la información en el Instituto Geográfico Agustín Codazzi-IGAC, de esta manera garantizar la confidencialidad, integridad y disponibilidad de la información, a su vez establecer criterios de administración de los riesgos y la revisión continua con el fin de validar la efectividad de las medidas implementadas para la protección de la información.

Los objetivos específicos de seguridad de la información del IGAC son los siguientes:

1. Establecer mecanismos, controles físicos y lógicos y lineamientos para el manejo adecuado de la información.
2. Identificar y gestionar los riesgos de seguridad de la información del IGAC, con el fin de reducir la probabilidad de ocurrencia de cualquier incidente de seguridad de la información en la entidad y/o minimizar el impacto en caso de que se presenten.
3. Fomentar una cultura de seguridad de la información en el instituto, con el fin de promover la conciencia y la responsabilidad en los funcionarios, contratistas y colaboradores del IGAC en relación con la protección de la información.
4. Garantizar la continuidad de los procesos críticos identificados por el IGAC en caso de un evento disruptivo, a través de la implementación de medidas adecuadas para la gestión de incidentes y la continuidad del negocio.
5. Mantener la confidencialidad, integridad, y disponibilidad de la información del IGAC, asegurando que los datos sean precisos, completos y estén disponibles para quienes se encuentren autorizados y que los necesiten, en el momento en que los requieran.

3. ALCANCE

La Política General de Seguridad de la Información es de estricta observancia y cumplimiento por los funcionarios, contratistas o proveedores que se encuentran vinculados o prestan servicios al IGAC, en Sede Central, Direcciones Territoriales y Centros de Atención, inclusive cuando las actividades de gestión o tratamiento de la información no sean parte de su función principal; se aplica a todas las fases de gestión y tratamiento de la información, incluyendo los canales de comunicación usados para su recolección, transporte, almacenamiento, custodia, preservación, conservación o intercambio, mediante los mecanismos, dispositivos, sistemas de información, servicios, comunicaciones e infraestructura tecnológica dispuesta por el instituto.

Adicionalmente, este documento proporciona los lineamientos requeridos para la implementación de un modelo de seguridad de la información confiable, estandarizado y define el marco básico que guiará la implementación de cualquier directriz, proceso, procedimiento y acción encaminada a la protección de la información física y digital que sea recibida, recolectada, producida, almacenada o transferida y que apoye el cumplimiento misional del Instituto.

4. POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

implementar el Modelo de Seguridad de la Información, para proteger, preservar y administrar la confidencialidad, integridad y disponibilidad de los activos de información en los procesos institucionales. Asimismo, se enfoca en la seguridad digital y la gestión de la continuidad operativa, orientados a la mejora continua y al alto desempeño, con el objetivo de contribuir a la producción, disponibilidad y calidad de la información geográfica, catastral y agrológica de alta calidad. Todo lo anterior se lleva a cabo mediante la administración de los riesgos de seguridad de la información, previniendo y mitigando el impacto de incidentes y cumpliendo con los requisitos legales y reglamentarios.

5. DESARROLLO

5.1 ROLES Y RESPONSABILIDADES

- **Comité de Gestión y Desempeño**
  - Respaldar y promover de la política general de seguridad de la información.
  - Revisar y aprobar periódicamente la política general de seguridad de la información.
- **Líderes de procesos en Sede Central y Directores Territoriales:**
  - Apoyar la implementación de la política general de seguridad de la información y su cumplimiento al interior de los procesos y/o direcciones territoriales a cargo.
- **Dirección de Tecnologías de la Información y las Comunicaciones-DTIC**
  - Liderar la formulación y aprobación de la política general de seguridad de la información.
  - Liderar la implementación y seguimiento a la política general de seguridad de la información.
- **Subdirección de Infraestructura Tecnológica**
  - Apoyar la definición e implementación de políticas específicas de seguridad de la información relacionadas con el proceso de gestión de servicios tecnológicos.
- **Secretaría General - Subdirección de Talento Humano:**
  - Apoyar en la definición de estrategias de uso y apropiación relacionados con el componente de seguridad de la información para los funcionarios del IGAC.
  - Apoyar la definición de políticas específicas de seguridad de la información en relación con uso y apropiación con el componente de seguridad de la información para los funcionarios del IGAC y teletrabajo.
- **Secretaría General -Subdirección Administrativa y Financiera** (Grupo Interno de Trabajo de Gestión Contractual):

- Apoyar en la definición de las estrategias de uso y apropiación relacionados con el componente de seguridad de la información para los contratistas del IGAC.
- Apoyar la definición de políticas específicas de seguridad de la información en relacionado con los proveedores.
- Apoyar en las acciones necesarias a realizar, en los casos que se presente un incumplimiento en lo establecido en la Política General de Seguridad de la Información por parte de algún contratista que represente un riesgo en la gestión de la Información del Instituto.

° **Secretaría General – Gestión Documental:**

- Liderar e implementar controles de seguridad para la información física que gestiona y mantiene el IGAC.
- Implementar estrategias de etiquetado de la información con el fin de realizar un proceso de clasificación más eficiente.
- Apoyar en los procesos de articulación entre las tablas de retención documental y la identificación, clasificación y aceptación de activos de información de cada uno de los procesos del Instituto.

° **Secretaría General – Subdirección Administrativa y Financiera:**

- Apoyar en la definición de políticas específicas relacionadas con los controles físicos, para la protección de las Instalaciones del Instituto.

° **Oficina Asesora Jurídica:**

- Apoyar en los procesos de articulación entre el índice de información clasificada y reservada, identificación y clasificación de los datos personales y la identificación, clasificación y aceptación de activos de información de cada uno de los procesos del Instituto.
- Implementar estrategias para el fortalecimiento de la privacidad de la información del Instituto.

° **Oficina Control Interno Disciplinario:**

- Adelantar Acciones Disciplinarias a funcionarios en casos que se evidencie el incumplimiento a lo definido en la Política General de Seguridad de la Información y que esto ponga en riesgo la Información del IGAC.

5.2 SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN-SGSI

El Sistema de Gestión de seguridad de la Información-SGSI, hace parte del Sistema de Gestión Integrado-SGI del IGAC, como un componente estratégico, en el cual se establecen mecanismos necesarios para proteger la información institucional. El SGSI establece políticas, lineamientos, procedimientos, instructivos, guías y demás documentos que apoyen la implementación de controles lógicos y físicos, con el fin de mitigar riesgos asociados a la confidencialidad, integridad y disponibilidad, de la información. Por otra parte, el SGSI es adoptado por la alta Dirección del IGAC, con el fin de establecer el compromiso y asignar los recursos necesarios para la protección de la información.

5.3 PRINCIPIOS

La Política General de Seguridad de la Información está fundamentada en los siguientes principios:

a) La información es uno de los activos más importantes del IGAC y por lo tanto se espera que sea utilizada acorde con los requerimientos de sus funciones.
b) La Confidencialidad de la información del IGAC y de terceras partes debe ser mantenida, independientemente del medio o formato donde se encuentre y que sea accedida sólo por aquellos que tienen una necesidad legítima para la realización de sus funciones u obligaciones.
c) La Integridad de la información se debe preservar independientemente de su temporalidad, o la forma en que sea transmitida y que esté protegida contra modificaciones no planeadas, realizadas con o sin intención.
d) La Disponibilidad de la información de la Entidad debe garantizarse de forma permanente cuando sea requerida.

5.4 DECLARACIONES

La Dirección General por medio de la Dirección de Tecnologías de la Información y las Comunicaciones insta a que todos los funcionarios, contratistas y proveedores cumplan con los lineamientos en materia de seguridad de la información, con el fin de resguardar la información producida, recibida, recolectada, almacenada o transferida. Para ello se establecen las siguientes declaraciones de seguridad que soportan el SGSI:

1. Las responsabilidades frente a la seguridad de la información serán definidas, socializadas, publicadas por parte de la Dirección de Tecnologías de la Información y las Comunicaciones-DTIC y serán aceptadas por cada uno de los funcionarios, contratistas y proveedores que tengan acceso a la información institucional.
2. El IGAC es el responsable de los activos de información y los administradores de estos activos son los funcionarios, contratistas o demás colaboradores que estén autorizados y sean responsables por la información de los procesos a su cargo, de los sistemas de información o aplicaciones informáticas, hardware o infraestructura de Tecnología, y son los responsables de implementar los controles para su protección, de acuerdo con la clasificación de la información de su propiedad o en custodia.
3. Los funcionarios, contratistas o proveedores deben cumplir los lineamientos e instrucciones descritos en esta política y en los procedimientos, guías e instructivos definidos y los cuales se encuentran publicados dentro del listado maestro de documentos del Sistema Gestión Integrado, así como los conceptos y lineamientos en materia de seguridad de la Información generados a solicitud.
4. La información producida, recibida, recolectada, almacenada o transferida por el IGAC cuenta con la protección y seguridad mediante la definición, implementación, seguimiento y mejoramiento de herramientas, controles, procedimientos, etc., con el fin de evitar los riesgos asociados a su confidencialidad, integridad, y disponibilidad.
5. Los medios y equipos donde se almacena procesan o comunica la información, deben mantenerse con las medidas de protección físicas y lógicas, que permitan su monitoreo y correcto estado de funcionamiento.
6. Con el fin de mitigar las vulnerabilidades y amenazas relacionadas con el recurso humano, la alta dirección destinará los recursos suficientes para el desarrollo de programas de capacitación y sensibilización; es obligación de los funcionarios y contratistas asistir a estos eventos o cursos.
7. Los funcionarios y contratistas tienen la obligación y responsabilidad de la identificación y notificación de cualquier incidente o evento que pudiera comprometer la seguridad de sus activos de información. Asimismo, la Entidad deberá implementar procedimientos para la correcta gestión de los incidentes detectados.
8. El IGAC establece dentro del manual de seguridad de la información los roles y responsabilidades relacionados con el Sistema de Gestión de Seguridad de la Información en lo que tiene que ver con el gobierno, gestión, administración y operación en la seguridad de la información.
9. Es responsabilidad de los funcionarios y contratistas del Instituto realizar copia de seguridad de los archivos producidos, gestionados o administrados que se encuentren almacenados en los equipos de cómputo asignados; esta copia debe almacenarse en los medios designados por el IGAC tales como servidor de archivos, almacenamiento en la nube, entre otros. Una vez finalizada la vinculación con la Entidad se deberá entregar toda la información procesada dentro de los equipos a cargo al jefe inmediato o al supervisor de contrato.
10. Los equipos de cómputo de propiedad de los contratistas deberán cumplir con características mínimas antes de ser conectados en las redes de datos del IGAC, esto a nivel de seguridad (actualizaciones, antivirus, entre otros) y uso de software legal. En caso de presentarse algún incidente identificado con el equipo del contratista, la Entidad podrá iniciar las acciones legales y administrativas correspondientes.
11. Con el fin de desarrollar el marco de actuación adecuado para la protección de la información y dar a conocer los lineamientos específicos en materia de seguridad de la información, el IGAC establece esta política como el documento principal junto con el Manual del Sistema de Seguridad de la Información.

12. Los proyectos de tecnologías de la información relacionados con el desarrollo y/o adquisición de software o cualquier componente TIC deberá contar con el aval de la Dirección de Tecnologías de la Información y las Comunicaciones.

5.5 SEGUIMIENTO Y EVALUACIÓN

El seguimiento en el cumplimiento en la implementación y la mejora continua del SGSI, se realizará con la implementación de indicadores de gestión, recopilación y análisis de información, definición e implementación de acciones de mejora continua, evaluación de controles, monitoreo y control, medición y reportes de avance. Por otra parte, la Política General de Seguridad de la Información será revisada por la Dirección General, por medio del Comité Institucional de Gestión y Desempeño o el que este delegue al menos una vez al año o cuando ocurran cambios significativos, para asegurar su conveniencia, adecuación y eficacia continua.

5.6 PROCESO DISCIPLINARIO O SANCIONATORIO

El incumplimiento de la Política General de Seguridad de la Información y procedimientos derivados de está por parte de un servidor público o contratista será tratado como un incidente de seguridad de la información y este podrá dar lugar al inicio de procesos sancionatorios.

5.7 DEFINICIONES

- **Activo de información:** en relación con la seguridad de la información, se refiere a cualquier información o elemento relacionado con el tratamiento de esta (sistemas, soportes, edificios, personas, etc.) que tenga valor para la organización[1]
- **Confidencialidad:** Garantizar que la información es accesible sólo para aquellos autorizados a tener acceso.[2]
- **Control:** medida que modifica el riesgo. Sinónimo de salvaguarda.[3]
- **Disponibilidad:** Propiedad que tiene la información de ser accesible y utilizable cuando se requiera.[4]
- **Gestión de riesgos:** Actividades coordinadas para dirigir y controlar una organización con respecto al riesgo. Se compone de la evaluación y el tratamiento de riesgos.[5]
- **Información:** se refiere a un conjunto organizado de datos contenido en cualquier documento que los sujetos obligados generen, obtengan, adquieran, transformen o controlen.[6]
- **Integridad:** propiedad de salvaguardar la exactitud y estado completo de los activos.[7]
- **Observancia:** Cumplimiento exacto y puntual de lo que se manda ejecutar, como una ley, un estatuto o una regla.[8]
- **Protección de la información:** conjunto de medidas preventivas y reactivas que deben tomarse para mantener la confidencialidad, la integridad y disponibilidad de la información.[9]
- **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 consideraciones.[10]
- **Seguridad de la información:** es el conjunto de medidas preventivas y reactivas de las organizaciones y sistemas tecnológicos que permiten resguardar y proteger la información buscando mantener la confidencialidad, integridad y disponibilidad de la información.[11]

---

[1] Lista de términos relacionados con la serie ISO 27000 y la seguridad de la información (s.f.). Tomado de https://www.iso27000.es/glosario.html
[2] NTC ISO/IEC 27002:2013
[3] Lista de términos relacionados con la serie ISO 27000 y la seguridad de la información. (s.f.). Tomado de https://www.iso27000.es/glosario.html
[4] Definición propia
[5] Lista de Glosarios de términos especializados (2017.febrero 17). Recuperado de https://glosarios.servidor-alicante.com/
[6] 1712 del 6 de marzo de 2014, Artículo 6
[7] NTC ISO/IEC 27000:2013
[8] Martínez Ferreras, D. (s. f.). Los Tesauros. Universidad Oberta de Cataluña, (PID_00143963), p. 7.
[9] Definición propia
[10] ISO/IEC 27000, (ISO Guía 73:2002)
[11] Seguridad de la Información [En Wikipedia]. Recuperado (2022, mayo 23) de https://es.wikipedia.org/wiki/Seguridad_de_la_informaci%C3%B3n

6. CONTROL DE CAMBIOS

FECHA	CAMBIO	VERSIÓN
24/07/2024	◦ Se adopta como versión 1 debido a la actualización de la Cadena de Valor en Comité Institucional de Gestión y Desempeño del 3 de marzo del 2023, nuevos lineamientos frente a la generación, actualización y derogación de documentos del SGI. ◦ Cambia de proceso de Gestión de Servicios Tecnológicos a Gestión Estratégica de Tecnología. ◦ Hace parte del proceso de **Gestión Estratégica de Tecnología.** ◦ Se actualiza la política de "Seguridad Digital", código **PL-GIN-01**, versión 1, a política "General de Seguridad de la Información del IGAC", código **PL-GET-01**, versión 1.	**1**
16/06/2022	◦ Se adopta como versión 1 debido a la actualización del Mapa de Procesos en Comité Directivo del 29 de junio del 2021, nuevos lineamientos frente a la generación, actualización y derogación de documentos del SGI. ◦ Se ajusta el documento según la nueva Estructura Orgánica aprobada por Decreto 846 del 29 de Julio del 2021. ◦ Hace Parte del proceso **Gestión de Sistemas de Información e Infraestructura**, subproceso de **Gestión de Infraestructura de Información**. ◦ Se actualiza la política "Seguridad Digital", código **PL-GTI-02,** versión 1, a política del mismo nombre, código **PL-GIN-01**, versión 1. ◦ Se revisa y se actualiza el contenido técnico de la política siguiendo los lineamientos establecidos en la Dimensión de Gestión con valores para resultados del MIPG. Esta política es aprobada por el Comité Institucional de Gestión y Desempeño en la sesión del día 16 de junio del 2022.	**1**

ELABORÓ Y/O ACTUALIZÓ	REVISÓ TÉCNICAMENTE	REVISÓ METODOLÓGICAMENTE	APROBÓ
Nombre: Diego Ramírez Pulido. **Cargo:** Contratista. Dirección de Tecnologías de la Información y Comunicaciones.	**Nombre:** Cristian José Petro Petro. **Cargo:** Subdirector. Subdirección de Infraestructura Tecnológica. **Nombre:** Alexandra Ruiz Bedoya. **Cargo:** Subdirectora. Subdirección de Información. **Nombre:** Fernando Pérez Moreno. **Cargo:** Subdirector (E) Subdirección de Sistemas de Información.	**Nombre:** Lida Carolina Zuleta Alemán **Cargo:** Profesional especializado. Oficina Asesora de Planeación.	**Nombre:** Perla Yadira Rojas Martínez. **Cargo:** Directora. Dirección de Tecnologías de la Información y Comunicaciones.