1. INTRODUCCIÓN

Un entorno digital se define como un ambiente, tanto físico como virtual sobre el cual se soporta la economía digital[1]. Los ciudadanos acceden a diferentes tramites y servicios que presta el Instituto Geográfico Agustín Codazzi - IGAC a través de estos entornos digitales, por lo cual surge la necesidad de identificar y gestionar los diferentes riesgos asociados a la seguridad digital.

En materia de Seguridad Digital, el Documento CONPES 3854 de 2016 incorpora la Política Nacional de Seguridad Digital coordinada por la Presidencia de la República, para orientar y dar los lineamientos respectivos a las entidades; por otro lado, Bajo el decreto 1008 de 2018 se establecen los lineamientos generales de la política de Gobierno Digital y se describen los principios que rigen la función y los procedimientos administrativos. Uno de estos principios es el de Seguridad de la Información, el cual soporta su implementación en el Modelo de Seguridad y Privacidad de la Información – MSPI definido por el Ministerio de Tecnologías de la Información y las Comunicaciones – MINTIC, dicho modelo contempla un ciclo de operación que consta de cinco (5) fases: Diagnóstico, Planificación, Implementación (Hacer), Evaluación de desempeño (verificar) y Mejora Continua (Actuar), un ciclo PHVA, lo cual lo enmarca dentro de un sistema de gestión en correlación con la norma ISO 27001.

De conformidad con lo dispuesto, es obligación del IGAC establecer, documentar e implementar un Sistema de Gestión, en el cual se incluye el Sistema de Gestión de Seguridad de la Información y se asigna al Director de la Dirección de Tecnologías de la Información y Comunicaciones como el responsable de liderar la implementación de este sistema de gestión y quien será el enlace sectorial de seguridad digital.

Para el presente documento cuando se enuncie la política de seguridad de la información, se entenderá que es la política de seguridad digital.

Así mismo, la Política de tratamiento de datos Personales del IGAC, donde se dan los lineamientos a seguir para la creación, tratamiento y cierre de las bases de datos que posean datos personales.

Esta Política contiene los lineamientos establecidos por la Alta Dirección y fue aprobada por el Comité Institucional de Gestión y Desempeño en la sesión del día 16 de junio del 2022.

2. OBJETIVO

Fortalecer los lineamientos para el cumplimiento de los objetivos de seguridad de la información en entornos digitales, a través de la identificación, valoración, tratamiento y mitigación de los riesgos de seguridad digital del IGAC en un marco de cooperación, colaboración y asistencia.

3. ALCANCE

Esta Política aplica a todos los procesos y subprocesos establecidos en la entidad en el marco del Modelo Integrado de Planeación y Gestión – MIPG.

4. ROLES Y RESPONSABILIDADES

La Política de Seguridad Digital del IGAC define los roles y responsables así:

- **Línea estratégica:**
  - Comité Institucional de Gestión y Desempeño

- **Línea de implementación:**
  - Dirección de Tecnologías de la Información y Comunicaciones

[1] Conpes 3854 - POLÍTICA NACIONAL DE SEGURIDAD DIGITAL. Ver https://colaboracion.dnp.gov.co/CDT/Conpes/Econ%C3%B3micos/3854.pdf al 2020-07-31.

- Oficina Asesora Jurídica.
- Subdirección de Talento Humano.
- Secretaria General.
- Oficina Asesora de Planeación.
- Líderes de Procesos y Directores Territoriales.
- Propietarios de Activos de Información.
- Custodios de la información.
-

° **Línea de seguimiento:**
- Oficina Asesora de Planeación.

° **Línea de control y evaluación**
- Oficina de Control Interno.

5. DESARROLLO

La política de seguridad de la información se soporta en la definición de políticas específicas de seguridad de la información que se describen a continuación:

5.1 POLÍTICA DISPOSITIVOS MÓVILES

Las medidas de seguridad de soporte, para gestionar los riesgos introducidos por el uso de dispositivos móviles serán orientadas con el objeto de mitigar los riesgos asociados al acceso, pérdida y divulgación no autorizados de la información del IGAC, a través de la asignación de controles asociados con la asignación de privilegios de acceso, borrado seguro de la información y aplicación de técnicas de cifrado.

5.2 POLÍTICA TELETRABAJO

El IGAC debe implementar medidas para proteger la información a la que se tiene acceso, que es procesada o almacenada en los lugares en los que se realiza teletrabajo (todas las formas de trabajo por fuera de la oficina, incluidos los entornos de trabajo no tradicionales, a los que se denomina "trabajo a distancia", "lugar de trabajo flexible", "trabajo remoto" y ambientes de "trabajo virtual").

5.3 POLÍTICA DE USO ACEPTABLE

Los servidores Públicos, contratistas y terceros que laboran en las instalaciones del IGAC (vinculados con un proveedor (empresa o entidad externo)), deben conocer y aplicar las reglas para el uso aceptable de los activos de información, incluyendo los recursos tecnológicos, donde se realiza el procesamiento de la información.

5.4 POLÍTICA DE CONTROL DE ACCESO

El acceso de los servidores Públicos, contratistas y terceros que laboran en las instalaciones del IGAC (vinculados con un proveedor (empresa o entidad externo)) a la información y a los recursos tecnológicos del IGAC, debe ser debidamente solicitado y autorizado por el responsable de dicho recurso, basado en la premisa "Todo está restringido, a menos que esté expresamente permitido" a través de la creación de una solicitud en la mesa de servicios de TI.

5.5 POLÍTICA SOBRE EL USO DE CONTROLES CRIPTOGRÁFICOS

El intercambio de los datos clasificados como información pública reservada debe usar técnicas de cifrado de información para garantizar la protección y privacidad en el intercambio de la información; de igual manera se debe proteger y definir un tiempo de vida de las llaves criptográficas durante todo su ciclo de vida.

La adopción de controles de cifrado y firma digital de datos serán un mecanismo que minimice la materialización de riesgos de seguridad de la información.

5.6 POLÍTICA DE ESCRITORIO Y PANTALLA LIMPIOS

Los papeles, medios de almacenamiento removibles y archivos que se encuentran desplegados en las pantallas de las terminales/equipos de cómputo, deben mantenerse de forma protegidos.

5.7 POLÍTICAS DE TRANSFERENCIA DE INFORMACIÓN

La información que es transferida internamente o hacia terceros, debe ser protegida contra interceptación, copiado, modificación, enrutado y destrucción, de acuerdo con su clasificación de información.

5.8 POLÍTICA DE DESARROLLO SEGURO

Los desarrollos de software deben ser efectuados con base en la aplicación de reglas y técnicas de programación seguras, que refuercen la seguridad del nuevo sistema o la mejora de los ya existentes.

5.9 POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN PARA LAS RELACIONES CON PROVEEDORES

Los requisitos de seguridad de la información para mitigar los riesgos asociados con el acceso de proveedores en la etapa precontractual y contratistas a los activos de información del IGAC, se deben acordar durante las etapas de planeación (que inicia con la identificación de la necesidad y finaliza con la elaboración de los estudios previos) y precontractual del proceso de contratación que recae en el establecimiento de la relación contractual con un proveedor a través de la inclusión de cláusulas en los estudios previos y técnicos que den cumplimiento a los requisitos de seguridad de la información conforme a la norma ISO27001:2013.

6. IMPLEMENTACIÓN

A continuación, se describe la estrategia de planificación y control operacional necesaria para implementar el SGSI, la cual estará soportada por el desarrollo de planes que garanticen la gestión de riesgos de seguridad digital de forma efectiva, y el cumplimiento de los objetivos de seguridad de la información.

6.1 OBJETIVOS DE SEGURIDAD DE LA INFORMACIÓN

Para dar cumplimiento a los objetivos de seguridad de la información del IGAC que se encuentran relacionados en el Manual del sistema de gestión integrado - SGI, a continuación, se presentan los mecanismos que evidencian su establecimiento:

Para el objetivo de seguridad de la información 1: *Definir lineamientos, políticas y procedimientos de seguridad de la información*, se deben documentar y socializar a los usuarios internos y externos del IGAC donde dichos documentos estén protegidos, controlados y disponibles para su uso, dónde y cuándo se necesite.

Para esto, el IGAC establece bajo la política del Sistema de Gestión Integrado del IGAC, donde incorpora los requisitos de cada uno de los sistemas de gestión y control que lo conforman y en el cual se incluye la del SGSI, resaltando la importancia de orientar este sistema "hacia la protección de la privacidad, confidencialidad, integridad y disponibilidad de la información y activos, de los clientes y los grupos de interés, para habilitar el desarrollo de la misión institucional, en un ambiente controlado de riesgos de la información. La información es un activo primordial en la prestación de los servicios a la ciudadanía y la toma eficiente de decisiones, razón por la cual existe un compromiso expreso hacia la protección de las propiedades más significativas como parte de la estrategia orientada a la continuidad del negocio, la administración de riesgos asociados a la seguridad y privacidad de la información y la consolidación de una cultura de seguridad de la información".

Así mismo, el IGAC a través del procedimiento Control de la Información Documentada Establecida en el Sistema de Gestión Integrado – SGI, estableció las actividades para identificar, elaborar, actualizar, derogar, revisar, aprobar, oficializar, divulgar y controlar los documentos correspondientes a los

procesos establecidos en el Sistema de Gestión Integrado – SGI.

Para el objetivo de seguridad de la información 2: *Establecer la gestión de riesgos de seguridad asociados a la información de la Entidad*, se debe establecer lineamientos con base en lo establecido en el Modelo Integrado de Planeación y Gestión – MIPG, de forma integrada, donde la identificación de los riesgos de seguridad digital sean compatibles con la libertad de expresión, el libre, flujo de la información, la confidencialidad de la información, la protección de la privacidad y los datos personales, en concordancia con lo establecido en el CONPES 3854 Política Nacional de Seguridad Digital.

Para esto, el IGAC ha establecido una Política de Administración del Riesgo la cual tiene como objetivo fomentar la cultura de la prevención del riesgo en todos los niveles de la Institución, gestionar de forma anticipada las vulnerabilidades o eventos que puedan afectar el logro de los objetivos institucionales. Dicha política integra los lineamientos para identificar, tratar y manejar los riesgos de seguridad digital, de corrupción y de gestión.

Para el objetivo de seguridad de la información 3: *Implementar controles de seguridad con el objetivo de optimizar la gestión de la seguridad de la información en la Entidad, teniendo en cuenta los recursos disponibles*, se debe determinar los límites y la aplicabilidad del SGSI considerando la autoevaluación de la implementación del SGSI definiendo las prioridades frente a su implementación.

Para esto, el IGAC ha decidido implementar controles de seguridad de la información, de acuerdo con las necesidades y expectativas evidenciadas en el documento denominado *Declaración de aplicabilidad*.

Así mismo aplica de forma continua el instrumento de autoevaluación (herramienta de diagnóstico) que hace parte del Modelo de Seguridad y Privacidad de la Información – MPSI y el cual arroja como resultado el estado actual de la entidad con respecto a la implementación de los objetivos de control de seguridad de la información y el nivel de madurez de dichos controles.

En relación con la implementación de los controles planeados para la presente vigencia, el IGAC se ha apoyado en recurso humano adicional a través de la contratación de servicios profesionales.

Para el objetivo de seguridad de la información 4: *Realizar la identificación y clasificación de los activos de información de la Entidad teniendo en cuenta los principios de confidencialidad, integridad y disponibilidad*, se deben identificar los activos asociados con la información y las instalaciones de procesamiento de información, y se debe elaborar y mantener un inventario de estos activos.

Para esto, el IGAC ha establecido el procedimiento de Gestión de Activos el cual tiene por objeto gestionar la identificación y/o revisión, clasificación, publicación y etiquetado de los activos de información teniendo en cuenta los respectivos niveles de confidencialidad, integridad y disponibilidad, los propietarios, custodios y usuarios.

Para el objetivo de seguridad de la información 5: *Promover la cultura de seguridad de la información en la Entidad*, se deben establecer actividades de sensibilización, capacitación y educación en seguridad de la información de acuerdo con la caracterización de usuarios y la tipificación de estos con base en el acceso a la información del IGAC que cada uno tiene.

Para esto, el IGAC anualmente establece un plan de comunicación, sensibilización y capacitación en seguridad de la información el cual se mide a través de indicadores establecidos en el Plan de Acción anual de la Dirección de Tecnologías de la Información y Comunicaciones.

Para el objetivo de seguridad de la información 6: *Mantener el SGSI actualizado, vigente, auditado y velar por la mejora continua de la seguridad de la información de la Entidad*, se debe definir una estructura organizacional con funciones y responsabilidades que permita asegurar la dirección y apoyo gerencial, para soportar la administración y desarrollo de estrategias sobre seguridad de la información.

Para esto, el IGAC define un *Manual Sistema De Gestión Integrado – SGI* en el cual se describe el Sistema de Gestión Integrado (SGI) implementado en el IGAC y los sistemas que lo conforman; el SGSI hace parte de éste.

Estratégicamente el IGAC ha conformado un Comité Institucional de Gestión y desempeño, a través de la resolución N° 320 de 2018 "Por la cual se crea y conforma el Comité Institucional de Gestión y Desempeño del IGAC" en la cual se definen funciones específicas relacionadas con la Gestión de la Seguridad de la Información – "Artículo 4. Funciones del Comité Institucional de Gestión y Desempeño, numeral 6".

Así mismo, se puede identificar como en el manual de funciones del IGAC se establecen responsabilidades frente a la ejecución de funciones específicas con relación a la seguridad de la información: "Dar cumplimiento al componente de Seguridad y Privacidad de la Información de la Estrategia de Gobierno en Línea y a los estándares internacionales aplicables."

6.2 DOCUMENTACIÓN DEL SGSI

En el marco de la implementación del SGSI, el IGAC debe mantener documentada la información que es necesaria para su eficacia, asegurando que:

En la creación y actualización de los documentos, éstos sean identificados y se defina el tipo de soporte (análogo, digital y electrónico).

El IGAC ha establecido el procedimiento *Manejo de Archivos de Gestión y Central*, el cual tiene como objetivo proporcionar a los funcionarios y contratistas una herramienta que los guie para el desarrollo de actividades de Gestión Documental relacionadas con la aplicación de las Tablas de Retención Documental (TRD), atendiendo las directrices del Archivo General de la Nación y el Programa de Gestión Documental del IGAC.

6.3 PLANIFICACIÓN Y CONTROL DE CAMBIOS DEL SGSI

En el marco de la implementación del SGSI, el IGAC debe controlar los cambios planificados y revisar las consecuencias de los cambios no previstos, tomando acciones para mitigar los efectos adversos cuando sea necesario.

Para esto, los cambios en los sistemas de procesamiento de información se realizan a través de la *Administración del Control de Cambios en Infraestructura Tecnológica,* donde se establece un procedimiento que permita administrar y controlar los cambios realizados en los sistemas de información, aplicativos, portales y plataforma tecnológica del IGAC, para atender las solicitudes que generan los usuarios, minimizar los errores que puedan presentarse en los sistemas de información, mejorar los servicios e implementar medidas de seguridad.

7. SEGUIMIENTO

El seguimiento de la política se enmarca en la dimensión de "Evaluación de resultados" del MIPG, incluye el Plan de Acción del IGAC y los indicadores vigentes al igual que el seguimiento al cumplimiento de la política de Administración de Riesgos establecida en el IGAC.

El seguimiento se implementa como una función continua de recolectar y analizar sistemáticamente información sobre indicadores que permiten a la entidad determinar el progreso y el cumplimiento de los logros y objetivos, así como el uso de los recursos asignados en cada proyecto y el plan a ejecutar. Este seguimiento constituye la base para la gestión de una iniciativa del conocimiento y la innovación, ya que provee información sobre el progreso en la ejecución de la política, al comparar los avances logrados frente a las metas propuestas, en términos de los compromisos y los resultados.

El proceso de Direccionamiento Estratégico y Planeación del IGAC desarrolla la tarea de verificar la eficacia de las acciones de esta política en cada uno de los procesos y subprocesos establecidos en la entidad.

Lo resultados del seguimiento se deben registrar en las herramientas de autoevaluación establecidas dentro del MIPG de acuerdo con las frecuencias establecidas en los planes de medición y seguimiento.

8. EVALUACIÓN

La evaluación está a cargo del proceso de Seguimiento y Evaluación, quienes en el IGAC se encargan de la tercera línea de defensa tal como lo establece el MIPG en la Dimensión 7 "Control Interno". El objetivo de esta evaluación es el de proporcionar información sobre la efectividad de los controles aplicados en su desarrollo por la primera y segunda línea con un enfoque basado en riesgos.

La evaluación a la presente política se realiza con el fin de verificar la conveniencia, adecuación, eficacia y alineación continua de los requisitos para la calidad y la mejora continua. Se hará anualmente y con los criterios establecidos en los diferentes mecanismos implementados dentro del Sistema de Gestión Integrado:

- Cumplimiento de la normatividad legal
- Cumplimiento de los requisitos establecidos por el IGAC
- Cumplimiento de los planes
- Seguimiento a Indicadores
- Seguimiento a Riesgos
- Acciones correctivas y de mejora.

9. CONTROL DE CAMBIOS

FECHA	CAMBIO	VERSIÓN
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**

FECHA	CAMBIO	VERSIÓN
13/08/2020	° Se adopta como versión 1 por corresponder a la creación del documento. Emisión Inicial Oficial.	**1**

Elaboró y/o Actualizó	Revisó Técnicamente	Revisó Metodológicamente	Aprobó
Nombre: Isis Johanna Gómez Peralta **Cargo:** Dirección de Tecnologías de la Información y Comunicaciones.	**Nombre:** Urías Romero Hernández **Cargo:** Director de Tecnologías de la Información y Comunicaciones. **Nombre:** Adriana Rocío Tovar Cortés **Cargo:** Jefe Oficina Asesora de Planeación	**Nombre:** Carlos Rafael González Contreras **Cargo:** Contratista Oficina Asesora de Planeación **Nombre:** Laura González Barbosa **Cargo:** Contratista Oficina Asesora de Planeación	**Nombre:** Comité de Institucional de Gestión y Desempeño del 16 de Junio de 2022.