

IGAC
INSTITUTO GEOGRÁFICO
AGUSTÍN CODAZZI



Sistema de Gestión
Integrado
MIPG



IGAC
INSTITUTO GEOGRÁFICO
AGUSTÍN CODAZZI



Sistema de Gestión
Integrado
MIPG



Plan de
Tratamiento de Riesgos de Seguridad y Privacidad de la Información
Código: PN-GET-02 **Versión:** 1 **Vigente desde:** 31/01/2025

Contenido

1.	INTRODUCCIÓN	4
2.	OBJETIVO	4
3.	ALCANCE	4
4.	MARCO LEGAL	4
5.	DESARROLLO	5
5.1	CONTEXTO Y JUSTIFICACIÓN	5
5.2	ESTRATEGIAS Y ACCIONES	6
5.3	RECURSOS	6
5.4	ANEXOS	6
6.	CONTROL DE CAMBIOS	6

1. INTRODUCCIÓN

El Instituto Geográfico Agustín Codazzi – IGAC como responsable de la gestión de riesgos de seguridad de la información que recibe, produce y transfiere establece la hoja de ruta para la identificación, análisis y evaluación de los riesgos de seguridad que puedan impactar al IGAC a través del desarrollo de actividades que permitan realizar una adecuada gestión del riesgo.

Para esto la Dirección de Tecnologías de la Información y Comunicaciones del IGAC mediante la política PL-PRC-01 Administración del Riesgo y el procedimiento PC-PRC-03 Administración del Riesgo realiza la gestión de los riesgos de seguridad de la información del IGAC. Adicionalmente, Este documento se encuentra articulado con el Plan de Estratégico de Seguridad de la Información

2. OBJETIVO

Establecer las actividades a ejecutar en la vigencia 2025 contempladas en el Sistema de Gestión de Seguridad de la Información, alineadas con la, la PL-GET-01 Política de Seguridad de la Información, el manual MN-GET-02 Seguridad de la Información, la norma NTC/IEC ISO 27001:2022 y los Modelo de Seguridad y Privacidad de la información de MINTIC para la gestión de riesgos de Seguridad de la Información.

3. ALCANCE

El Plan Estratégico de Tratamiento de Riesgos Seguridad de la Información busca realizar la identificación de riesgos de seguridad de la información asociados a la posible pérdida de confidencialidad, integridad o disponibilidad de la información recibida, producida y transferida por el IGAC, este plan aplica a todos los procesos y subprocesos definidos en la cadena de valor de IGAC, niveles funcionales, organizacionales, a todos sus funcionarios, contratistas y proveedores, así como a todas las sedes del instituto (Sede Central, Direcciones Territoriales y Centro de Atención).

4. MARCO LEGAL

Relacionar los aspectos de orden legal que tienen que ver directamente con el plan; se deben relacionar en orden jerárquico y cronológico de la más reciente a la última, el número de la norma, artículo (si aplica) y “considerando”.

° Leyes.

- Ley 23 de 1982: “Sobre derechos de autor”.
- Ley 527 de 1999: “Por medio de la cual se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales, y se establecen las entidades de certificación y se dictan otras disposiciones”.
- Ley 1273 de 2009: “Por medio de la cual se modifica el código penal, se crea un nuevo bien jurídico tutelado -denominado “De la protección de la información y de los datos”- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones”.
- Ley 1221 de 2018: “Por la cual se establecen normas para promover y regular el Teletrabajo y se dictan otras disposiciones.”

- Decretos.
 - Decreto 235 de 2010: "Por el cual se regula el intercambio de información entre entidades para el cumplimiento de funciones públicas".
 - Decreto 2573 de 2015: "Por el cual se establecen los lineamientos generales de la Estrategia de Gobierno en línea, se reglamenta parcialmente la Ley 1341 de 2009 y se dictan otras disposiciones".
 - Decreto 728:2017: " Por el cual se adiciona el capítulo 2 al título 9 de la parte 2 del libro 2 del Decreto Único Reglamentario del sector TIC, Decreto 1078 de 2015, para fortalecer el modelo de Gobierno Digital en las entidades del orden nacional del Estado colombiano, a través de la implementación de zonas de acceso público a Internet inalámbrico".
 - 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."
- Resoluciones.
 - Resolución externa 2160 MINTIC de 2020: "Por la cual se expide la Guía de lineamientos de los servicios ciudadanos digitales y la Guía para vinculación y uso de estos"
 - 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"
 - Resolución externa 746 MINTIC de 2022: "Por la cual se establecen los lineamientos de transformación digital para las estrategias de ciudades y territorios inteligentes de las entidades territoriales, en el marco de la Política de Gobierno Digital"
- Conpes.
 - CONPES 3701 de 2011: Lineamientos de la política para la ciberseguridad y ciberdefensa
 - CONPES 3854 de 2016: Política nacional de Seguridad Digital
 - CONPES 3975 de 2019: Política Nacional para la Transformación Digital e Inteligencia Artificial
 - CONPES 3995 de 2020: Política Nacional de Confianza y Seguridad Digital

5. DESARROLLO

Plan Estratégico de Tratamiento de Riesgos Seguridad de la Información comprende las actividades establecidas para la vigencia 2025, teniendo en cuenta los resultados de la identificación y evaluación de riesgos adelantada en la vigencia anterior

5.1 CONTEXTO Y JUSTIFICACIÓN

El Plan Estratégico de Tratamiento de Riesgos Seguridad de la Información se desarrollará a nivel de Sede Central, Direcciones Territoriales y Centro de Atención, contemplando las actividades realizadas por los procesos y sub procesos, la clasificación y características de los activos de información, las amenazas, vulnerabilidades y controles implementados en el momento de realizar el análisis y evaluación de riesgos así como las brechas de seguridad identificadas en la infraestructura tecnológica, servicios, sistemas de información u otros activos de información de la entidad, así como los eventos y alertas que se presenten en estos.

El Plan Estratégico de Tratamiento de Riesgos Seguridad de la Información se establece con el fin de mitigar la materialización de riesgos de seguridad de la información a la que se le realiza tratamiento

en el IGAC; con la implementación de esta plan se busca mejorar el nivel de anticipación y gestión de los riesgos de seguridad.

5.2 ESTRATEGIAS Y ACCIONES

A continuación, se describen las acciones específicas a desarrollar durante la vigencia 2025, los responsables de su ejecución y los plazos establecidos:

Actividades	Fecha Inicio (DD/MM/AAAA)	Fecha Fin (DD/MM/AAAA)	Dependencia responsable
Actualización/alineación del documento de tratamiento de riesgos de seguridad de la información de acuerdo con los lineamientos del Modelo Nacional de Gestión de Riesgos de Seguridad Digital. -MNGRSD	15-feb-25	25-abr-25	Dirección de Tecnologías de la Información y Comunicaciones
Sensibilización instrumentos que soportan la gestión de riesgos de seguridad de la información y seguridad digital.	25-abr-25	23-may-25	Dirección de Tecnologías de la Información y Comunicaciones
Identificación, análisis y valoración de riesgos de seguridad de la información y seguridad digital.	23-abr-25	28-nov-25	Todos los procesos del IGAC
Socialización de los riesgos identificados.	28-nov-25	19-dic-25	Dirección de Tecnologías de la Información y Comunicaciones
Realizar seguimiento a los informes de vulnerabilidades y planes de remediación	03-feb-25	31-dic-25	Dirección de Tecnologías de la Información y Comunicaciones
Identificar, analizar, contener y documentar los incidentes de seguridad que se presenten	15-ene-25	31-dic-25	Dirección de Tecnologías de la Información y Comunicaciones

5.3 RECURSOS

Describir:

1. Recurso humano: Equipo de seguridad de la información de la DTIC, enlaces de los procesos y subprocesos, administradores de herramientas de seguridad e infraestructura tecnológica, líderes de los procesos.
2. Materiales: Equipos de cómputo.
3. Presupuesto: \$147.890.000.

5.4 ANEXOS

El anexo al plan es la matriz de seguimiento de las actividades propuestas (excel) que contiene entre otros:

1. Cronograma de actividades
2. Seguimiento.
3. Evaluación.

6. CONTROL DE CAMBIOS

FECHA	CAMBIO	VERSIÓN
31/01/2025	<ul style="list-style-type: none"> 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. Hace parte del proceso de Gestión Estratégica de Tecnología. Se crea el Plan de "Tratamiento de Riesgos de Seguridad y Privacidad de la Información" código PN-GET-02, versión 1. 	1

ELABORÓ Y/O ACTUALIZÓ	REVISÓ TÉCNICAMENTE	REVISÓ METODOLÓGICAMENTE	APROBÓ
<p>Nombre: Diego Ferney Ramírez Pulido</p> <p>Cargo: Contratista. Dirección de Tecnologías de la Información y Comunicaciones.</p>	<p>Nombre: Fernando Pérez Moreno.</p> <p>Cargo: Director. Dirección de Tecnologías de la Información y Comunicaciones.</p> <p>Nombre: Cristian José Petro Petro.</p> <p>Cargo: Subdirector. Subdirección de Infraestructura Tecnológica.</p> <p>Nombre: Alexandra Ruiz Bedoya.</p> <p>Cargo: Subdirectora. Subdirección de Información.</p> <p>Nombre: Diego Ramírez Pulido.</p> <p>Cargo: Contratista. Dirección de Tecnologías de la Información y Comunicaciones.</p>	<p>Nombre: Lida Carolina Zuleta Alemán</p> <p>Cargo: Profesional Especializado. Oficina Asesora de Planeación.</p> <p>Nombre: Carlos Rafael González Contreras</p> <p>Cargo: Contratista. Oficina Asesora de Planeación.</p> <p>Nombre: Laura Isabel Gonzalez Barbosa</p> <p>Cargo: Contratista. Oficina Asesora de Planeación.</p>	<p>Nombre: Comité Institucional de Gestión y Desempeño del IGAC.</p>