1. OBJETIVO

Definir los pasos a seguir para realizar el reporte, gestión y cierre de los incidentes de Seguridad de la Información que se puedan presentar en el Instituto Geográfico Agustín Codazzi con el fin de velar por la protección de la información institucional y los datos personales, a través de la correcta gestión de estos.

2. ALCANCE

Inicia con la detección y reporte de un incidente de seguridad de la información (física y/o Digital) por parte de los usuarios (funcionarios y contratistas) del IGAC, a través de la plataforma tecnológica de la mesa de servicios de TI y finaliza con el cierre del incidente y/o evento.

3. DEFINICIONES

- **Confidencialidad:** Propiedad que determina que la información no esté disponible ni sea revelada a individuos, entidades o procesos no autorizados.
- **Denegación de servicio:** Ataque que inhabilita la disponibilidad y el uso de redes de comunicaciones, sistemas o aplicaciones mediante el consumo excesivo de los recursos de las mismas.
- **Disponibilidad:** Característica de la información y todos los activos asociados a ella, que deberán permanecer accesibles a los usuarios autorizados cuando ellos lo requieran para el desarrollo de sus funciones en el Instituto.
- **Evento de Seguridad:** Presencia identificada de una condición adversa de un sistema, servicio o red que indica una violación de la política de seguridad de la información o la manifestación de una vulnerabilidad o amenaza, falla de los controles, o materialización de una situación desconocida que afecta la seguridad de la información.
- **Hacking:** Acceso no autorizado a sistemas y redes, entre otros.
- **Impacto:** Consecuencias que genera un riesgo una vez se materialice.
- **Incidente de Seguridad de la Información:** Evento o serie de eventos de seguridad de la información no deseados o inesperados, que tienen una probabilidad significativa de comprometer la operación normal del negocio y amenazar la seguridad de la información comprometiendo la disponibilidad, integridad y confidencialidad de la misma. ISO/IEC 27035. Entre otros: Pérdida, daño, robo, alteración, indisponibilidad y divulgación no autorizada de información institucional.
- **Integridad:** Propiedad de salvaguardar la exactitud y estado completo de los activos.
- **Parche:** Componente de software realizado por los fabricantes de tecnología, el cual permite corregir una vulnerabilidad encontrada en un dispositivo
- **RNBD:** Registro Nacional de Base de Datos.
- **Equipo de cómputo:**
- **SIC:** Superintendencia de Industria y Comercia.
- **Vulnerabilidad:** Ausencia de un control de seguridad. Las amenazas aprovechan las vulnerabilidades existentes para generar riesgos de seguridad de la información en el Instituto.
- **Personal de soporte en sitio:** Técnicos y/o Ingenieros que realizan las actividades de soporte en sitio.**Seguridad de la Información:** Es el conjunto de medidas preventivas y reactivas del IGAC que permiten asegurar que los activos de información mantienen la confidencialidad, disponibilidad e integridad.**Usuario:** Persona que hace uso, o tiene acceso al activo de información, y tiene la responsabilidad de tomar conciencia y adoptar los requisitos de seguridad de la información, definidos y establecidos para los activos de información del IGAC.

4. NORMATIVIDAD

- Leyes
  - Ley 1273 de 2009. "Por medio de la cual se modifica el Código Penal, y se incluyen nuevos delitos penales relacionados con los delitos informáticos y se equipara en cuanto a la normatividad internacional sobre ciberdelitos
- Decretos

- Decreto 1008 de 2018 "Por el cual se establecen los lineamientos generales de la política de Gobierno Digital".

° Normas técnicas aplicables
- NTC-ISO-IEC 27001. Tecnología de la información. Técnicas de seguridad. Sistemas de gestión de la seguridad de la información (SGSI). Requisitos.
- NTC-ISO-IEC 27002 - Tecnología de la información. Técnicas de seguridad. Código de práctica para la gestión de la seguridad de la información
- NTC-ISO-IEC 27035. Tecnología de la información. Técnicas de seguridad. Gestión de Incidentes de Seguridad.
- Políticas específicas de seguridad de la información para la implementación de controles de la norma ISO/IEC 27001:2013.[1]
- Guía No. 21 Gestión de Incidentes, Ministerio de Tecnologías de la Información y las Comunicaciones MINTIC

5. POLÍTICAS DE OPERACIÓN.

Estas políticas aplican a todos los usuarios de los activos de información del Instituto, sin importar su ubicación, incluyendo funcionarios públicos, personal pasante, contratistas y personal que labora en las instalaciones vinculado como proveedor de un servicio para el IGAC (personal contratado por una empresa o entidad externa) que requieran o tengan derechos de acceso a la información o a los recursos tecnológicos que la procesan.

° Cada vez que sea requerido y aprobado por la alta dirección, se debe solicitar el apoyo de las autoridades competentes (CSIRT-PONAL, CCOC: Comando Conjunto Cibernético, Grupo de respuesta a emergencias cibernéticas de Colombia – colCERT, Fiscalía General de la Nación, entre otros), para realizar la recolección de la evidencia.

° La gestión de un incidente de seguridad de la información se desarrolla con base en las siguientes actividades.

Fuente: GTC-ISO/ IEC 27035 – Guía Gestión de incidentes – MINTIC

5.1. PREPARACIÓN Y PREVENCIÓN

° La actividad de preparación y prevención involucra las acciones que deben desarrollarse en la gestión de la seguridad de la información para mitigar las causas que puedan originar un incidente de seguridad de la información tales como:

1) Identificación de riesgos de seguridad digital asociados a los activos de información.
2) Sensibilización y entrenamiento en seguridad de la información.
3) Implementación de herramientas de monitoreo de red, registros y eventos de los sistemas de información.
4) Gestión de parches.
5) Desarrollo de procedimientos seguros.

5.2. DETECCIÓN Y ANÁLISIS

° La detección y análisis inicia con la identificación del incidente de seguridad de la información por un usuario y/o administrador de un recurso tecnológico.

[1]http://igacnet2.igac.gov.co/intranet/UserFiles/File/P12000-Manual%20Sistema%20de%20Gestion%20Integrado.pdf#page=68

- Para realizar la evaluación de un incidente de seguridad de la información se debe tener en cuenta el tipo y nivel de impacto.

TABLA DE IMPACTO			
TIPO	**NIVEL**	**DESCRIPTOR**	**DESCRIPCIÓN** En caso de que el riesgo se materialice el impacto u afectación sería…
CONFIDENCIALIDAD EN LA INFORMACIÓN	1	INSIGNIFICANTE	Se afecta a una persona en particular.
	2	MENOR	Se afecta a un grupo de trabajo interno del proceso.
	3	MODERADO	Se afecta a todo el proceso.
	4	MAYOR	La afectación se da a nivel estratégico.
	5	CATASTRÓFICO	La afectación se da a nivel institucional.
CREDIBILIDAD O IMAGEN	1	INSIGNIFICANTE	Se afecta al grupo de funcionarios y contratistas del proceso.
	2	MENOR	Se afecta a todos los funcionarios y contratistas de la entidad.
	3	MODERADO	Se afecta a los usuarios de la Sede Central de la entidad.
	4	MAYOR	Se afecta a los usuarios de las Direcciones Territoriales.
	5	CATASTRÓFICO	Se afecta a los usuarios de la Sede Central y de las Direcciones Territoriales.
LEGAL	1	INSIGNIFICANTE	Se producen multas para la entidad.
	2	MENOR	Se producen demandas para la entidad.
	3	MODERADO	Se producen investigaciones disciplinarias.
	4	MAYOR	Se producen investigaciones fiscales.
	5	CATASTRÓFICO	Se producen intervenciones y o sanciones para la entidad por parte de un Ente de control u otro Ente regulador.
OPERATIVO	1	INSIGNIFICANTE	Se tendrían que realizar ajustes a una actividad concreta del proceso.
	2	MENOR	Se tendrían que realizar ajustes en los procedimientos del proceso.
	3	MODERADO	Se tendrían que realizar ajustes en la interacción de procesos.
	4	MAYOR	Se presentarían intermitencias o dificultades en la operación del proceso
	5	CATASTRÓFICO	Se presentaría paro o no operación del proceso.

- La clasificación de incidentes está sujeta a los riesgos y criticidad de los activos. Estos son algunos de los incidentes de seguridad que pueden presentarse en el Instituto:

Incidente	Descripción
Ejecución de Denegación de Servicio	Saturación del sistema de información. Excesiva actividad del sistema causante de la degradación o falla del rendimiento.
Hacking	Acceso no autorizado a sistemas y redes.
Modificación de información del sistema o red	Falsificación de dirección origen o destino del tráfico de red. Modificación de contenido del tráfico de red.
Espionaje	Interceptación no autorizada de la información.

Incidente	Descripción
Distribución de virus, troyanos o código malicioso	Distribución de virus informático, generalmente es ocasionada por el intercambio de información entre usuarios haciendo uso de medios magnéticos o a través de la red. También puede presentarse intencionalmente mediante archivos
Distribución de spam	Distribución excesiva de mensajes no solicitados (comerciales, correos electrónicos y telefónicos).
Acceso no autorizado	Tener acceso a información no autorizada
Cambio de privilegios sin autorización	Por ejemplo, hacer cambios no autorizados al software y a los datos
Instalación de software no autorizado	Instalación de software de una fuente no confiable
Robo de equipo de computo	Ocurre cuando componentes o software de la empresa son robados
Borrado o eliminación de información	Borrado o eliminación de información por error, de forma deliberada o malintencionada
Uso de software falso o copiado	Utilización de software pirata
Desastres naturales	Daños ocasionados por la naturaleza que son impredecibles. (Ej. Fenómenos climáticos, fenómenos sísmicos, fenómenos volcánicos, fenómenos meteorológicos, inundación)

5.3. CONTENER Y ERRADICAR

- La contención y erradicación involucra dispara las acciones necesarias para contener el incidente de seguridad con el fin de que no se propague y pueda generar más daños a la información o a la arquitectura de TI.
- Los recursos necesarios para gestionar los incidentes de seguridad son de tipo:
  1) **Humano:** Personal de planta y contratistas del IGAC, Administradores de plataforma, equipo de seguridad de la información, áreas interesadas (policía, fiscalía, entre otras).
  2) **Tecnológicos:** Firewall, Servidores, Consola antivirus, bases de datos, routers, switches, logs, copias de seguridad, entre otros.
- A continuación, se definen los tiempos en que se deben atender los incidentes de seguridad de la información, con el propósito de devolver los sistemas afectados por el incidente a su estado operativo.

Incidente	Tiempo de respuesta
Ejecución de Denegación de Servicio	6-10 Horas
Hacking	6-10 Horas
Modificación de información del sistema o red	6-10 Horas
Espionaje	6-10 Horas
Distribución de virus, troyanos o código malicioso	1-6 horas
Distribución de spam	6-10 Horas
Acceso no autorizado	6-10 Horas
Cambio de privilegios sin autorización	6-10 Horas
Instalación de software no autorizado	6-10 Horas

Incidente	Tiempo de respuesta
Robo de equipo de computo	6-10 Horas
Borrado o eliminación de información	6-10 Horas
Uso de software falso o copiado	6-10 Horas
Desastres naturales	12-24 Horas

- Después de tratado el incidente se debe recopilar y organizar las pruebas que soporten toda la gestión del incidente incluyendo una descripción de lo ocurrido, las acciones tomadas y la solución dada.

5.4. POST INCIDENTE (LECCIONES APRENDIDAS)

- Las lecciones aprendidas brindan los elementos necesarios para realizar la mejora continua al presente procedimiento, dado que se debe mantener la documentación y/o registros que permitan conocer lo que sucedió en un incidente de seguridad.

5.5. ROLES O GRUPOS OPERATIVOS PARA EL PRESENTE PROCEDIMIENTO

- **Custodio del activo de información:** Persona responsable de implementar las políticas, procedimientos, controles y protocolos que se establezcan por parte de la entidad y del propietario del activo de información.
- **Mesa de servicio OIT:** Punto único de contacto encargado de responder las solicitudes de los clientes, compuesto por un conjunto de recursos tecnológicos y humanos que se encuentra en la sede central y las direcciones territoriales.
- **Oficial de Seguridad de la Información:** Persona encargada de implementar los lineamientos de seguridad de la información aprobados por la alta dirección.
- **Propietario del activo de formación:** Es una persona, grupo interno de trabajo o una dependencia al que se ha dado la responsabilidad formal por la seguridad de un activo o una categoría de activos de información. No significa que el activo pertenece al dueño en un sentido legal. Los propietarios de activos de información son responsables de manera formal por garantizar que los mismos, estén seguros mientras están siendo desarrollados, producidos, mantenidos, utilizados y almacenados (ciclo de vida del activo de información).
- **Personal de soporte en sitio:** Técnicos y/o Ingenieros que realizan las actividades de soporte en sitio.
- **Seguridad de la Información:** Es el conjunto de medidas preventivas y reactivas del IGAC que permiten asegurar que los activos de información mantienen la confidencialidad, disponibilidad e integridad.
- **Usuario:** Persona que hace uso, o tiene acceso al activo de información, y tiene la responsabilidad de tomar conciencia y adoptar los requisitos de seguridad de la información, definidos y establecidos para los activos de información del IGAC.

6. DESARROLLO

N°	ACTIVIDAD	DESCRIPCIÓN DE LA ACTIVIDAD	RESPONSABLE (Dependencia)	DOCUMENTO O REGISTRO	PUNTOS DE CONTROL
1	Identificar el incidente de seguridad de la información	Identifica el incidente de seguridad de la información y lo reporta a través de la creación de un requerimiento en la plataforma de mesa de servicios de TI. El administrador de los recursos tecnológicos puede detectar a través de las alertas la no disponibilidad, integridad o confidencialidad de los recursos tecnológicos.	Usuario / Administrador de los recursos tecnológicos El Jefe de Oficina y/o director territorial y/o subdirector (Todas las dependencias de la Entidad)	Registro del requerimiento en la plataforma tecnológica de la mesa de servicios de TI	Si el incidente se relaciona con Bases de Datos de la RNBD, debe reportarlo en la plataforma de la SIC - Superintendencia de Industria y Comercio.
2	Recibir solicitud	Recibe la solicitud y analiza si la incidencia corresponde a un incidente de seguridad de la información para que esta se asignada al rol: oficial de seguridad de la información.	Administrador de la plataforma de la mesa de servicio (Oficina de Informática y Telecomunicaciones – OIT)	Seguimiento al requerimiento en la plataforma tecnológica de la mesa de servicio de TI.	¿Si es un incidente de seguridad de la información? **SI:** Continua en la actividad N° 3. **NO:** El estado del requerimiento registrado en la plataforma de la mesa de servicios TI cambia a cerrado. FIN DEL PROCEDIMIENTO
3	Validar el incidente de seguridad de la información	Contacta al solicitante del requerimiento y valida si el incidente de información es auténtico Se registra el seguimiento al requerimiento en la plataforma tecnológica de la mesa de servicio de TI, documentando la descripción y adjuntando las evidencias.	Oficial de Seguridad de la Información (Oficina de Informática y Telemunicaciones – OIT)	Seguimiento al requerimiento en la plataforma tecnológica de la mesa de servicio de TI.	. ¿Si es un incidente de seguridad de la información? **SI:** Continua con la actividad 4. **NO:** El estado del requerimiento registrado en la plataforma de la mesa de servicios TI cambia a cerrado. FIN DEL PROCEDIMIENTO
4	Analizar el incidente de seguridad de la información	Analiza el incidente de seguridad de la información e identifica: a) La causa raíz del incidente y los activos de información afectados por el mismo. b) Los mecanismos para detener o evitar la propagación del incidente, según su especialidad.	Oficial de Seguridad de la Información (Oficina de Informática y Telemunicaciones – OIT)	Seguimiento al requerimiento en la plataforma tecnológica de la mesa de servicio de TI.	
5	Gestionar actividades para contener y/o erradicar el incidente de	Gestiona las actividades necesarias para contener y/o erradicar el incidente de seguridad de la información y las documenta en la plataforma tecnológica de la mesa de servicio de TI.	Oficial de Seguridad de la Información (Oficina de Informática y	Seguimiento al requerimiento en la plataforma tecnológica de	Se debe verificar si el incidente de seguridad es solucionado

N°	ACTIVIDAD	DESCRIPCIÓN DE LA ACTIVIDAD	RESPONSABLE (Dependencia)	DOCUMENTO O REGISTRO	PUNTOS DE CONTROL
	seguridad de la información		Telemunicaciones – OIT)	la mesa de servicio de TI.	El incidente es solucionado: **SI:** Continua a la actividad 7. **NO:** Escala el incidente de seguridad a la alta dirección para establecer las acciones a seguir, continua en la actividad 6
6	Informar al Comité institucional de gestión y desempeño.	Informa al Comité institucional de gestión y desempeño para validar las acciones a seguir como notificar a las autoridades competentes y/o informar al respecto a la Oficina de Control Interno Disciplinario y si es el caso, remitir el acta del Comité a dicha Oficina para su gestión.	Oficial de Seguridad de la Información (Oficina de Informática y Telemunicaciones – OIT)	Acta de Comité	
7	Documentar las lecciones aprendidas	Documenta las lecciones aprendidas sobre la gestión realizada y cambia el estado del requerimiento a cerrado a solucionado.	Oficial de Seguridad de la Información (Oficina de Informática y Telemunicaciones – OIT)	requerimiento en la plataforma tecnológica de la mesa de servicio de TI pasa a cerrado. Plan de Mejoramiento	En caso de requerir ejecutar acciones posteriores al cierre del incidente, se puede genera un plan de mejoramiento.
FIN DEL PROCEDIMIENTO					

7. FORMATOS ASOCIADOS

No aplican a este procedimiento

8. CONTROL DE CAMBIOS

Registra las dos últimas versiones (para el caso de actualizaciones de documentos) así:

FECHA	CAMBIO	VERSIÓN
29/09/2020	° Se adopta como versión 1 debido a cambios en la Plataforma Estratégica (actualización del mapa de procesos), nuevos lineamientos frente a la generación, actualización y derogación de documentos del SGI tales como: cambios de tipos documentales y nueva codificación por procesos. Emisión Inicial Oficial. ° Cambia de Manual de procedimiento a Procedimiento, código **P15000-02/18.V1**, versión 1, al código **PC-GTI-02**, versión 1. ° Se deroga totalmente la circular 231 del 31 de agosto de 2018.	1
31/08/2018	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:** Profesional Especializado	**Nombre:** Isis Johanna Gómez Peralta **Cargo:** Profesional Especializado	**Nombre:** Lida Zuleta Alemán **Cargo:** Profesional Especializado Oficina Asesora de Planeación	**Nombre:** José Luis Ariza Vargas **Cargo:** J efe Oficina de Informática y Telecomunicaciones