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

Procedimiento

Gestión de Incidentes de Seguridad de la Información

Código: PC-GST-04 **Versión:** 1 **Vigente desde:** 03/07/2024

1. OBJETIVO

Establecer actividades que permitan identificar, gestionar, tramitar y documentar los incidentes de seguridad de la Información que se puedan presentar en el Instituto Geográfico Agustín Codazzi con el fin de preservar la confidencialidad, disponibilidad e integridad de la información institucional.

2. ALCANCE

Inicia con la detección y reporte a través de la herramienta de gestión de la Mesa de Servicio de TI de un incidente de seguridad de la información (física y/o digital) por parte de los funcionarios, contratistas, pasantes y proveedores del IGAC, continúa con el análisis, contención y erradicación para solucionar el mismo y finaliza con la documentación de la solución, lecciones aprendidas y cierre del incidente y/o evento de seguridad.

Aplica para todos los usuarios internos y externos del IGAC en todos los procesos y subprocesos del instituto, en Sede Central y Direcciones Territoriales, que requieran o tengan derechos de acceso a los sistemas de información, aplicaciones, recursos tecnológicos, información digital o física.

3. DEFINICIONES

- **Activo de Información:** Todo aquello que posea valor para el instituto y esté asociado con el manejo de los datos y la información misional, operativa y/o administrativa del instituto, es decir, la información que recibe transforma y produce el IGAC.
- **Amenaza**: Causa potencial de un incidente no deseado, que puede provocar daños a un sistema o a la organización.
- **ColCERT**: Por sus siglas en inglés Computer Emergency Response Team, es el Grupo de Respuesta a Emergencias Cibernéticas de Colombia, y tiene como responsabilidad central la coordinación de la Ciberseguridad y Ciberdefensa Nacional, la cual se encuentra enmarcada dentro del proceso misional de gestión de la seguridad y Defensa del Ministerio de Defensa Nacional.
- **CCOC**: Comando Conjunto Cibernético, es el equipo encargado de la Defensa de Colombia en el ciberespacio.
- **Confidencialidad:** Propiedad que determina que la información no esté disponible ni sea revelada a individuos, entidades o procesos no autorizados.
- **CSIRT**: Por sus siglas en inglés de Computer Security Incident Response Team, es el equipo de respuesta a incidentes de seguridad informática, creado para atender las necesidades de prevención, atención e investigación de los eventos e incidentes de seguridad informática de Colombia.
- **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.
- **DRP:** Por sus siglas en ingles Disaster Recovery Plan, es el Plan de Recuperación ante Desastres de tecnología que describe las acciones que deben realizarse antes, durante y después de un desastre y sus respectivas actividades para el restablecimiento de la disponibilidad de los servicios.
- **Evento de Seguridad:** Presencia identificada de una condición adversa de un sistema, servicio o red que indica una violación a 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.
- **Gestión de incidentes de Seguridad de la Información**: Procesos para detectar, reportar, evaluar, responder, tratar y aprender de los incidentes de seguridad de la información.
- **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.
- **Logs:** Es un registro secuencial y cronológico de las operaciones realizadas por un sistema informático.
- **NIST:** Instituto Nacional de Estándares y Tecnología de los Estados Unidos.
- **RNBD:** Registro Nacional de Base de Datos de Colombia.
- **SIC:** Superintendencia de Industria y Comercio de Colombia.
- **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.
- **Vulnerabilidad:** Ausencia de un control de seguridad. Las amenazas aprovechan las vulnerabilidades existentes para generar riesgos de seguridad de la información en el Instituto.

4. POLÍTICAS DE OPERACIÓN

4.1 LEGALES

- 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".

- Resoluciones.
  - Resolución 500 de 2021: MINTIC "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".

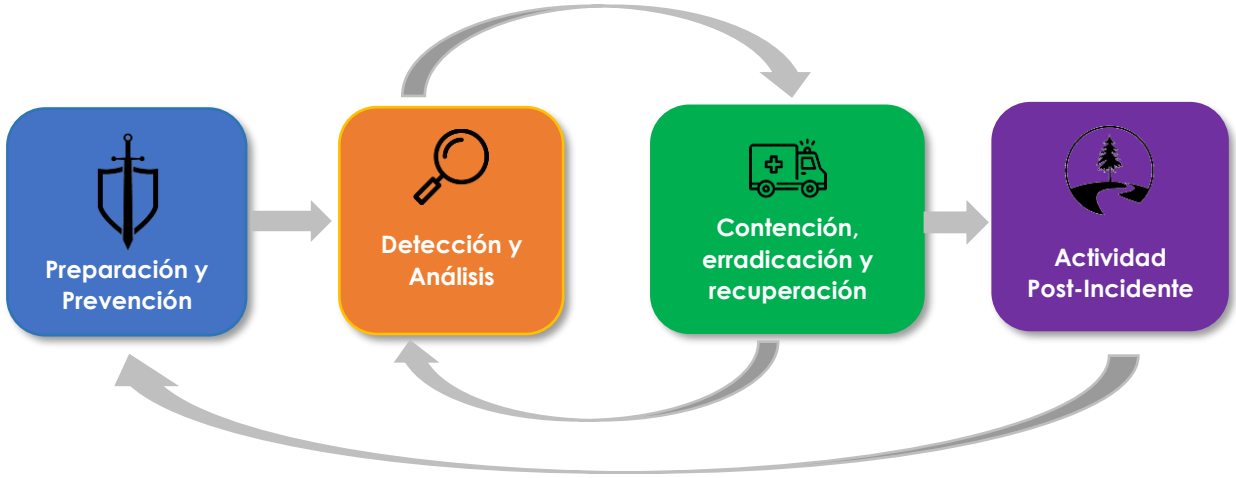
4.2 TÉCNICAS RELACIONADAS

- Normas Internacionales.
  - NTC-ISO-IEC 27001:2022 "Tecnología de la información. Técnicas de seguridad. Sistemas de gestión de la seguridad de la información (SGSI). Requisitos".
  - NTC-ISO-IEC 27002:2022 "Tecnología de la información. Técnicas de seguridad. Código de práctica para la gestión de la seguridad de la información ".
  - Políticas específicas de seguridad y privacidad de la información para la implementación de la norma ISO/IEC 27002:2022.
  - NTC-ISO-IEC 27035:2012 "Tecnología de la información. Técnicas de seguridad. Gestión de Incidentes de Seguridad".

- Otras.
  - Guía No. 21 Gestión de Incidentes, Ministerio de Tecnologías de la Información y las Comunicaciones MINTIC.
  - Manual de Seguridad de la Información

4.3 DEL PROCEDIMIENTO

- Un incidente de seguridad de la información se presenta cada vez que se vea afectada la integridad, disponibilidad o confidencialidad de la información sobre un activo de información del IGAC.
- De acuerdo con las buenas prácticas en la gestión de incidentes de seguridad de la información, el instituto adopta este procedimiento, con el fin de poder contar con la capacidad de responder de manera oportuna, evaluar, gestionar documentar los eventos e incidentes que se puedan presentar en materia de seguridad de la información.
- Este procedimiento y sus políticas de operación aplican para todos los usuarios de los activos de información del IGAC, 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.
- Los Incidentes de seguridad clasificados como Alto y Superior, deben reportarse para solicitar el apoyo y coordinación de la gestión de estos ante el CSIRT- Gobierno.
- Los incidentes de seguridad de la información clasificados como Medio, Bajo e Inferior deben reportarse a CSIRT- Gobierno una vez gestionados.
- La gestión de un incidente de seguridad de la información se desarrolla con base en las siguientes actividades:



Fuente: NIST SP 800 – 61r3 ipd

4.3.1 PREPARACIÓN Y PREVENCIÓN

En la fase de preparación y prevención se definen las capacidades de respuesta que debe tener el IGAC en caso de presentarse un evento o incidente de seguridad de la información. Dentro de esta etapa se deberán desarrollar las siguientes actividades:

- **Plan de uso y apropiación**: Definir actividades que permitan fortalecer la concientización en los funcionarios, contratistas, pasantes y proveedores del IGAC en materia de identificación de riesgos asociados a la confidencialidad, disponibilidad e integridad de la información. Todos los funcionarios, contratistas y personal de proveedores deben tener acceso y conocimiento del Manual de Seguridad de la Información y de los lineamientos de seguridad.
- **Directorio de escalamiento y comunicaciones**: Establecer y mantener actualizado un documento con la información necesaria que permita poder contactar de manera oportuna en caso de materialización de un incidente de seguridad de la información a las partes interesadas, autoridades competentes en materia de investigación de delitos cibernéticos, proveedores tecnológicos, entidades de emergencia entre otros.

- Para una efectiva comunicación de las actividades realizadas para la gestión del incidente de seguridad de la información se debe mantener actualizada la siguiente información de contacto:
  - Equipo de respuesta de incidentes o quienes realicen sus funciones.
  - Escalamiento de incidentes según la estructura del IGAC.
  - Administradores de las plataformas tecnológicas y Sistemas de Información (Servicios, Servidores, bases de datos, etc.)
  - Profesional de la Subdirección Administrativa y Financiera (Controles de seguridad físicos, Gestión Documental).
  - Proveedores de servicios
  - Autoridades de seguridad.

  El Comité Institucional de Gestión y Desempeño o quien haga sus veces determinara que incidentes de seguridad de la información deben ser informados a los medios de comunicación y ciudadanía en general.
- **Plan de pruebas**: con el fin de evaluar el grado de madurez en la atención de incidentes de seguridad de la información se deberá establecer las pruebas necesarias basadas en simulaciones, ejercicios de simulación de un ataque, pruebas de ingeniería social entre otros, utilizando el formato vigente "Plan de pruebas Gestión Incidentes de Seguridad" establecido para tal fin.
- **Monitoreo:** Por medio de herramientas tecnológicas, procedimientos, manuales y automatización, se deben establecer actividades de monitoreo permanente que permitan generar alertas tempranas ante posibles eventos de seguridad de la información que se puedan presentar.
- **Gestión de vulnerabilidades:** Establecer estrategias que permitan identificar las actualizaciones necesarias a implementar en la plataforma tecnológica del IGAC, las cuales deben ser probadas en ambientes de pruebas antes de su implementación.
- **Aseguramiento de la plataforma tecnológica:** Se debe configurar la menor cantidad de permisos o accesos (principio de menor privilegio) con el fin de proveer únicamente aquellos privilegios necesarios tanto a usuarios como a otros equipos. Se deben revisar configuraciones de fábrica (usuarios, contraseñas y archivos compartidos). Los servidores deben tener habilitados sus sistemas de auditoría para permitir el registro de los eventos, se debe realizar configuraciones de seguridad de fábrica.
- **Prevención de código malicioso:** Todos los equipos de la infraestructura (servidores como equipos de usuario) deben tener activo una solución de prevención de malware, esta debe estar actualizada, monitoreada continuamente y debe estar configurada para impedir cambios en su parametrización o políticas por parte de usuarios.
- **Seguridad en redes:** Se debe realizar una gestión y monitoreo constante sobre los equipos tecnológicos de seguridad. Las reglas configuradas en equipos de seguridad deben ser revisadas continuamente. Las firmas y actualizaciones de todos los dispositivos deben encontrarse al día. Todos los elementos de seguridad y de red deben encontrarse sincronizados y sus logs deben ser enviados a un equipo centralizado de recolección de logs para su respectivo análisis, se debe revisar periódicamente el estado de cableado y puntos de red verificando que no existan interferencias o conexiones no autorizadas.
- **Seguridad física y del entorno:** Se debe realizar inspecciones periódicas de los accesos a áreas seguras, verificando el funcionamiento de los controles de acceso, que se encuentre actualizado el listado de personas autorizadas, así como que se lleven a cabo los registros de acceso y ejecución de actividades.
- **Gestión de riesgos:** Se debe identificar, valorar y gestionar los riesgos de seguridad de la información, así como evaluar los controles y si es necesario implementar planes de tratamiento de riesgos para mitigar la materialización de los incidentes de seguridad de la información.
- **Plan de Recuperación ante Desastres:** La Dirección de Tecnología establece un plan de Recuperación ante Desastres Tecnológicos que considerará la respuesta, recuperación, reanudación de la operación en contingencia y restauración ante la materialización de un incidente que afecte la infraestructura y los servicios tecnológicos.

- Los incidentes de seguridad de la información donde estén involucrados funcionarios públicos deben ser informados al proceso de Gestión Disciplinaria, con el fin de estimar si debe realizar alguna revisión adicional desde la perspectiva disciplinaria.
- Los incidentes de seguridad de la información que impacten los datos personales son informados por la DTIC a la Oficina Asesora Jurídica con el fin realizar revisión y evaluar si deben reportarlos a la SIC.
- El Oficial de Seguridad de la Información o profesional designado de la DTIC, es el único autorizado para reportar incidentes de seguridad ante las autoridades de seguridad; así mismo el Comité Institucional de Gestión y Desempeño o quien haga sus veces, son los que definen quien realizará pronunciamiento oficial ante Entidades externas.

4.3.3 DETECCIÓN

En esta fase se desarrollarán actividades encaminadas a la detección, identificación y clasificación de los diferentes eventos e incidentes de seguridad de la información.

La detección inicia con la identificación del incidente de seguridad de la información detectado por un funcionario, contratista, pasante, administrador de un recurso tecnológico o proveedor del IGAC.

El proceso de identificación, también se puede dar por medio de elementos que señalan la posible ocurrencia de un incidente de seguridad de la información, como son herramientas tecnológicas de monitoreo en la infraestructura tecnológica, alertas en las soluciones de seguridad informática, desviaciones a las políticas de seguridad de la información, fallos en los controles físicos y lógicos, monitoreo de cámaras de seguridad, eventos detectados por la Mesa de Servicio de TI, registros o hallazgos en auditorías internas o externas entre otros. Adicionalmente eventos de seguridad detectados por entes externos, como son: CSIRT Gobierno, COLCERT, Centro Cibernético de la Policía u otros organismos del Modelo Nacional de Gestión de Riesgos de Seguridad Digital.

4.3.4 REPORTE

Todo evento de seguridad debe ser comunicado inmediatamente sea detectado a través de la herramienta de gestión de la Mesa de Servicio de TI, esta realizará el análisis previo para determinar si se trata de un evento de seguridad de la información o de un requerimiento propio de la gestión de la DTIC, si es clasificado como un evento de seguridad de la información la Mesa de Servicio de TI debe notificar al Oficial de Seguridad de la información o profesional designado del IGAC quien será el punto de contacto interno para iniciar las actividades de gestión del evento de seguridad de la información.

Los eventos no asociados a la DTIC serán gestionados de acuerdo con la naturaleza de este.

El Oficial de Seguridad de la información o profesional designado por la DTIC y/o los integrantes del equipo de respuesta a incidentes deben evaluar y determinar si el evento reportado es un incidente de seguridad de la información posible o concluido, si es o no una falsa alarma.

Cuando se detecte un evento de seguridad se debe realizar el diligenciamiento del formato vigente de “Reporte Gestión Incidentes de Seguridad”, en su pestaña “Reporte”, se registran los siguientes datos:

- Datos del funcionario, contratista o tercero que reporta.
- Datos del primer respondiente.
- Descripción del incidente:
  - ¿Qué ocurrió?
  - ¿Cómo ocurrió?
  - Activos de información afectados
  - Procesos/áreas/servicios impactados

- Detalles del incidente:
  - Fecha y hora en que ocurrió
  - Fecha y hora en que se descubrió
  - Fecha y hora en que se reportó
- ¿El incidente ya finalizó?

4.3.5 ANÁLISIS

Con el fin de realizar un análisis adecuado, se debe validar y clasificar por parte del Oficial de Seguridad de la Información si el reporte realizado corresponde a un evento o incidente de seguridad de la información, por medio de la clasificación descrita en la herramienta de gestión de la Mesa de Servicio de TI.

Si el reporte es clasificado como evento de seguridad de la información se realiza solo el reporte en el formato vigente "Reporte Gestión Incidentes de Seguridad".

Dentro de las actividades de análisis se deberá tener en cuenta la naturaleza y el grado de criticidad que pueda tener en incidente a la información institucional, adicionalmente es importante tener en cuenta las siguientes recomendaciones:

- Recopilar la información necesaria que permita realizar un análisis detallado.
- Realizar procesos de triangulación de información y correlación de eventos, con el fin de identificar patrones de comportamiento anormales.
- Entrevistar a la persona que reportó el incidente, administradores de la infraestructura tecnológica, administradores o responsables de controles de seguridad donde informen si se ha presentado comportamientos anómalos y se verifique si se cuenta con evidencias del incidente.
- Realizar procesos de priorización de la gestión del incidente, basado en el impacto que éste represente hacia los activos de información.
- Se debe determinar el tipo de incidente y la categoría del mismo de acuerdo con los ítems establecidos en el formato vigente "Reporte Gestión Incidentes de Seguridad".
- El equipo de respuesta a inocentes debe registrar el análisis realizado del incidente, estableciendo los siguientes puntos:
  - Causas del incidente.
  - Relación y descripción de la evidencia recolectada.
  - Riesgos de seguridad de la información materializados por el incidente, si el riesgo no se había identificado en la matriz de riesgos de seguridad esta debe actualizarse.
  - Controles de seguridad de la información comprometidos.
  - El equipo de respuesta a incidentes puede complementar la información respecto al reporte realizado.
- Para realizar el análisis de las causas o causa raíz de un incidente de Hardware o Software se considera los siguientes aspectos:
  - Logs de auditoria.
  - Tráfico de red.
  - Copias de seguridad.
  - Información de registro o archivos de configuración.
  - Puertos de dispositivos en estado de escucha (Listening).
  - Procesos y servicios activos en el sistema.
  - Listas de acceso.
  - Políticas de Enrutamiento de red.
  - Uso de equipos de cómputo de funcionarios, contratistas o terceros.
  - Informes de Actualización de software / parches.
- Para realizar el análisis de las causas o causa raíz de un incidente asociado a Recursos Físicos se considera los siguientes aspectos:

- Reportes de la empresa de seguridad.
- Registros de cámaras de video.
- Registros de acceso físico.
- Fallas en los controles de acceso y monitoreo.

° Se debe considerar información que puedan entregar otros procesos, subprocesos o dependencias del instituto.

4.3.6 EVALUACIÓN

En esta etapa se realiza la evaluación del incidente de seguridad de la información por parte del Oficial de Seguridad de la Información para establecer la clasificación de la criticidad del incidente, el impacto actual y futuro, el nivel de prioridad y los tiempos de atención.

Los incidentes de seguridad de la información son valorados de acuerdo con la criticidad de los activos de información afectados el impacto actual y el impacto futuro con lo cual se determinará el nivel de prioridad y los tiempos de atención.

Niveles de criticidad: El nivel de criticidad se determina de acuerdo con la clasificación de los activos de información teniendo en cuenta si la afectación involucra a varios activos de información que tengan una valoración alta, este tomará el valor más alto y se tomará como referencia la siguiente tabla:

NIVEL	VALOR	DESCRIPCIÓN
Superior	1.00	Afectación de varios activos de información críticos de más de un proceso del IGAC.
Alto	0.75	Afectación de uno o varios activos de información críticos de un proceso del IGAC.
Medio	0.50	Afectación a uno o varios activos de información de más de un proceso del IGAC.
Bajo	0.25	Afectación a uno o varios activos de información de un proceso del IGAC.
Inferior	0.10	Afectación de un activo de información no crítico del IGAC.

Impacto: se debe valorar el impacto de acuerdo con la siguiente información:

° Impacto actual: depende de la cantidad de daño que ha provocado el incidente en el momento de ser detectado.

° Impacto futuro: depende de la cantidad de daño que pueda causar el incidente si no es contenido, ni erradicado.

Con el fin de realizar la valoración del impacto se define la siguiente tabla:

NIVEL	VALOR	DESCRIPCIÓN
Superior	1.00	El Incidente de seguridad impacta la prestación de los servicios de todo el IGAC, con afectación reputacional, legal y económica.
Alto	0.75	El incidente de seguridad impacta a uno o varios servicios de la Dirección de Tecnologías de la información y Comunicaciones o usuarios con roles críticos para el IGAC.
Medio	0.50	El incidente de seguridad de la información impacta a más de un proceso misional, estratégico o de apoyo.
Bajo	0.25	El incidente de información impacta a un proceso o a una dependencia específica.
Inferior	0.10	Afectación a un usuario especifico sin compromiso de información crítica.

Valoración de la prioridad del incidente de seguridad de la información: Posterior a la definición de las variables de criticidad e impacto, se deberá valorar la prioridad con el fin de brindar una atención oportuna y adecuada al incidente la cual se obtiene a través de la siguiente formula:

Nivel Prioridad = (Impacto actual * 2,5) + (Impacto futuro * 2,5) + (Criticidad del Sistema * 5)

Y su resultado se deberá comparar con la siguiente tabla:

NIVEL	VALOR	DESCRIPCIÓN
Superior	07.50-10.00	Es un incidente que representa una amenaza critica para el IGAC, donde se ve afectado la totalidad de la información y pone en riesgo información reservada o clasificada, su imagen reputacional, económica y legal. Poniendo en riesgo la misionalidad del IGAC.
Alto	05.00-07.49	Es un incidente que afecta a varios procesos del IGAC ocasionando la interrupción total de los servicios prestados por el Instituto, generando incumplimientos legales, afectación reputacional y/o económica.
Medio	03.75-04.99	Es un incidente que afecta de manera parcial a uno o varios procesos del IGAC, causando reprocesos, incumplimientos legales y afectaciones económicas.
Bajo	02.50-03.74	Es un incidente que afecta a un proceso o dependencia de manera parcial, causando reprocesos.
Inferior	00.00-02.49	Es un incidente que afecta a un usuario en específico y no se ve afectación de información crítica para el IGAC.

Tiempos de atención de los incidentes de seguridad de la información: Se debe definir los tiempos de atención de un incidente de seguridad de la información, con el fin de atenderlos oportunamente de acuerdo con su criticidad e impacto. Para esto en la siguiente tabla se expresan los tiempos máximos para la atención, cabe aclarar que estos tiempos no son los tiempos de solución ya que esto depende de la afectación del incidente, la disponibilidad de recursos humanos y económicos, los planes de remediación entre otros.

NIVEL	DESCRIPCIÓN
Superior	El incidente de seguridad debe atenderse de forma inmediata (0-1) hora
Alto	El incidente de seguridad debe atenderse de forma prioritaria (1a 2) horas
Medio	El incidente de seguridad puede atenderse de (2 a 3) horas.
Bajo	El incidente de seguridad puede atenderse de (3 a 4) horas.
Inferior	El incidente de seguridad puede atenderse de (4 a 8) horas.

4.3.7 CONTENCIÓN, ERRADICACIÓN Y RECUPERACIÓN

Una vez analizado y priorizado el incidente de seguridad de la información se deberá implementar acciones para evitar su propagación y afectación a otros activos de información, así disminuir la perdida en la confidencialidad, integridad y disponibilidad de la información. Las posibles acciones de contención deben ser analizadas según el tipo de incidente y los criterios, adicionalmente deben estar bien documentados para facilitar la rápida y eficaz toma de decisiones.

Luego de ser identificados los elementos que hacen parte del incidente de forma inicial, así como posibles servicios afectados, para la contención y mitigación se deben seguir algunas de las siguientes opciones de contención:

- Apagar el activo de información afectado.
- Desconexión de redes eléctricas, alámbricas e inalámbricas.
- Deshabilitar funciones del sistema.
- Apagar servicios.
- Bloquear accesos físicos o lógicos

Posterior a la contención se procede a la erradicación de la causa del incidente de seguridad de la información y cualquier rastro dejado por este, durante esta actividad se deberá tener en cuenta las siguientes acciones:

- De acuerdo con el impacto y categorización del incidente o incidentes se determinará si es una situación de emergencia, lo que requeriría un manejo especial y prioritario.
- Determinar las causas del incidente, eliminándolas completamente.
- Mejorar los esquemas de protección actualmente implementados.
- Realizar pruebas de vulnerabilidad para revisar el estado posterior a la erradicación.
- Determinar y aplicar la restauración del sistema.
- Revalidar los lineamientos y políticas existentes, para identificar e implementar modificaciones.

Luego de la fase contención se debe continuar con el proceso de recuperación donde se realizan restauraciones a sistemas afectados, robustecimiento a controles vulnerados con el incidente con el fin de prevenir afectaciones similares en el futuro, para esto es importante tener en cuenta las siguientes consideraciones:

- Velar por la recuperación de los datos y configuraciones.
- Aplicar las actualizaciones necesarias.
- Robustecer las actividades de control.
- Garantizar el restablecimiento de los servicios e información afectados.
- La reactivación o recuperación de servicios se realiza de forma progresiva analizando el comportamiento de cada elemento inicializado detectando conductas irregulares o que representen algún peligro o reincidencia generando impacto negativo. Se mantiene monitoreo luego de la recuperación para detectar algún evento como los comentados anteriormente.

Las acciones de remediación al momento de su implementación o ejecución deben aportar a la restitución de los servicios, evitando generar traumatismos, obstaculización de procesos y por supuesto, evitar generar espacios o condiciones para que se generen nuevos incidentes. Es por lo anterior que las acciones de remediación deben ser planificadas y justificadas para su ejecución, siendo posible en cada caso, contar con el apoyo de fabricantes y agentes externos involucrados con tecnologías que hacen parte del incidente.

Desarrolladas las actividades de remediación que han logrado contener de forma permanente las causas generadoras del incidente y que impedirían que éstos se generen nuevamente con las mismas condiciones iniciales (vulnerabilidades, configuraciones débiles, protocolos de comunicación inseguros, etc.); se procede a restaurar servicios, aplicaciones y comunicaciones a su estado funcional previo al incidente

4.3.7 POST INCIDENTE (LECCIONES APRENDIDAS)

Las actividades post - incidentes abarcan la alimentación de bases de conocimiento con las acciones realizadas, cambios ejecutados y todo el análisis requerido para aplicar en caso de presentarse eventos o incidentes similares, de la misma manera se debe realizar la generación de reportes o informes con el fin de socializar a involucrados e interesados toda la información (no sensible) respecto al tratamiento realizado, investigación y lecciones aprendidas del incidente, buscando evitar que esto se presente nuevamente o que en caso de ocurrir se cuente con preparación para ello. Así mismo, se deben identificar los riesgos asociados a la gestión de incidentes de seguridad, y si se considera pertinente actualizar el mapa de riesgos de seguridad de la información. De ser necesario generar espacios para capacitar a los usuarios para enfrentar estas actividades y contar con preparación para futuros eventos.

4.3.8 REGISTRO LECCIONES APRENDIDAS

Las lecciones aprendidas brindan los elementos necesarios para realizar la mejora continua al presente procedimiento, dado que se debe mantener la documentación, plan de mejoramiento y/o registros que permitan conocer lo que sucedió en un incidente de seguridad. Adicionalmente, este tipo de soluciones se deben registrar en una base de conocimiento de la herramienta de gestión de la Mesa de Servicio de TI para lo cual se deberán tener en cuenta las siguientes consideraciones:

- Mantener la documentación de los eventos e incidentes de seguridad de la información, donde evidencie toda la gestión realizada en la atención y recuperación.
- Mantener actualizada las bases de datos de conocimiento.
- Integrar los eventos e incidentes a la Matriz de Riesgos de los Activos de información.
- Realizar capacitaciones a los funcionarios, contratistas, pasantes y proveedores del IGAC en lo relacionado a eventos e incidentes de seguridad de la información.

- A partir del resultado del tratamiento de los incidentes, se debe hacer seguimiento a los planes de acción y mejora, a la implementación de controles y medidas correctivas, al fortalecimiento de seguridad física y lógica de los procesos, a las campañas de sensibilización en seguridad de la información

4.3.9 ROLES O GRUPOS OPERATIVOS PARA EL PRESENTE PROCEDIMIENTO

- **Autoridades de Seguridad:** autoridades competentes de Colombia (CSIRT-PONAL, CCOC (Comando Conjunto Cibernético), colCERT (Grupo de respuestas a emergencias cibernéticas de Colombia), Fiscalía General de la Nación, entre otros.
- **Comité Institucional de Gestión y Desempeño o quien haga sus veces**: Grupo de personas o delegados responsables de supervisar y evaluar el Sistema de Gestión de Seguridad de la Información - SGSI del IGAC.
- Este comité o sus delegados será convocado por el Oficial de Seguridad cuando se presente un incidente de seguridad de la información y podrán ser invitados al mismo funcionario, contratistas, proveedores, entre otros necesarios para realizar la gestión de incidentes de seguridad de la información según aplique.
- **Custodio del activo de información:** Persona responsable de implementar las políticas, procedimientos, controles y protocolos que se establezcan por parte del instituto y del propietario del activo de información.
- **Equipo de respuesta a incidentes:** Equipo conformado por miembros confiables del IGAC, que cuentan con las habilidades y competencias para tratar los incidentes de seguridad de la información, durante el ciclo de vida de éstos:
  - Propietario y custodio del activo de información.
  - Oficial de seguridad de la información o profesional designado de la DTIC.
  - Director DTIC
  - Subdirector de Infraestructura Tecnológica
  - Subdirector de Sistemas de Información
  - Subdirector de Información
  - Nivel 2 o 3 de la DTIC.
  - Profesional de la Subdirección Administrativa y Financiera
- Este equipo de respuesta será organizado y convocado por el Oficial de Seguridad de la información o profesional designado por la DTIC de acuerdo con las necesidades de gestión del incidente, de igual manera serán convocados funcionarios, contratistas o proveedores que se requieran para la gestión del incidente diferentes a los relacionados.
- **Usuario solicitante:** corresponde al funcionario, pasante, contratista, proveedor o colaborador del IGAC que detecta un posible evento o incidente de seguridad y lo registra a través de la herramienta de gestión de la Mesa de Servicio de TI.
- **Nivel 1:** Este rol representa al técnico, tecnólogo o ingeniero que ejecuta las actividades de atención de primer nivel, correspondiente a la Mesa de Servicio de TI, SNC y profesionales de las Direcciones Territoriales. Es quien mantiene comunicación directa con el usuario.
- **Nivel 2 o 3**: profesional, especialista o proveedor de la DTIC encargado de la administración de la infraestructura, sistemas, plataformas o activos.
- **Oficial de Seguridad de la Información o profesional designado:** Persona encargada de implementar los lineamientos de seguridad de la información aprobados por la alta dirección. Actúa como coordinador o punto focal de información relacionada con las actividades de gestión de incidentes, para la información entregada a terceros o al público en general el Comité Institucional de Gestión y Desempeño o quien haga sus veces decidirá quien ejerce este rol
- **Propietario del activo de información:** 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).

- **Profesional de la Subdirección Administrativa y Financiera:** persona responsable de los controles de seguridad físicos.

5. DESARROLLO

N°	ACTIVIDAD	DESCRIPCIÓN DE LA ACTIVIDAD	RESPONSABLE (Dependencia)	DOCUMENTO O REGISTRO	PUNTOS DE CONTROL
1.	Identificar y reportar el posible evento de seguridad de la información.	Identifica el evento de seguridad de la información y lo reporta a través de la creación de un caso en la herramienta de gestión de Mesa de Servicio de TI. El administrador de los recursos tecnológicos puede detectar un posible evento a través de las alertas relacionadas con la afectación de la disponibilidad, integridad o confidencialidad de los recursos tecnológicos.	Usuario solicitante. (Todos los procesos)	Caso registrado en la herramienta de gestión de la Mesa de Servicio de TI.	El usuario que identifique el posible evento de seguridad debe anexar en el caso generado toda la información para la atención respectiva (Ejm: correo electrónico con el detalle del mensaje, alerta, pantallazos, videos, fotos, etc.)
2.	Recibir y validar el caso.	Recibe la solicitud y valida si el caso efectivamente corresponde a un evento de seguridad de la información. Realiza la correcta tipificación y selecciona la categoría según corresponda. Realiza escalamiento del caso al oficial de Seguridad de la Información o profesional designado.	Nivel 1 (Dirección de Tecnologías de la Información y Comunicaciones) Nivel 1 (Direcciones Territoriales)	Caso reportado en la herramienta de gestión de la Mesa de Servicio de TI.	¿Es un evento de seguridad de la información? **SI:** Continúa actividad N° 3. **NO:** Sigue Procedimiento de Gestión de Incidentes de TI código PC-GST-02 (Fin del procedimiento).
3.	Gestionar el evento de seguridad de la información.	Realiza la validación del evento y gestiona con los niveles de atención, custodio o propietario del activo para su análisis y gestión según aplique. Revisa que las evidencias correspondan y gestiona las que se requieran. Si el caso no es un evento de seguridad devuelve al nivel 1. Si el caso es un evento de seguridad se realiza la gestión respectiva.	Oficial de Seguridad de la Información o profesional designado (Dirección de Tecnologías de la Información y Comunicaciones)	Incidente en la herramienta de gestión de la Mesa de Servicio de TI.	¿Es un incidente de seguridad de la información? **SI:** Continúa actividad N° 4. **NO:** Continúa actividad N° 7.
4.	Analizar y gestionar el incidente de seguridad de la información.	El oficial de seguridad lidera y convoca a reunión al Equipo de respuesta a incidentes según aplique.	Equipo de respuesta a incidentes (Todos los procesos)	Seguimiento al incidente en la herramienta de gestión de la Mesa de Servicio de TI. Formato	Continúa actividad N° 5.

N°	ACTIVIDAD	DESCRIPCIÓN DE LA ACTIVIDAD	RESPONSABLE (Dependencia)	DOCUMENTO O REGISTRO	PUNTOS DE CONTROL
		En la reunión analizan el incidente de seguridad de la información e identifican: ° Realizar el registro en formato establecido. ° La causa raíz del incidente, riesgo y los activos de información afectados por el mismo. ° Valorar el incidente de seguridad de acuerdo con las políticas de operación de este procedimiento. ° Notifica por medio de correo electrónico cualquier novedad. Si el incidente es clasificado como superior o alto, el oficial de seguridad reportará y coordinará con el ColCERT Gobierno mediante los canales de contacto. Para todos los casos se debe realizar la recolección de la evidencia.		Reporte Gestión de Incidentes de Seguridad	
5.	Detener/Contener el incidente de seguridad de la información.	El Equipo de respuesta a incidentes realizará las actividades o tareas necesarias para detener o evitar la propagación del incidente de seguridad. El Oficial de Seguridad de la Información realizará el seguimiento pertinente. Los incidentes que no estén en el alcance de la DTIC y que no puedan ser contenidos serán escalados al Comité Institucional de Gestión y Desempeño o quien haga sus veces.	Equipo de respuesta a incidentes (Todos los procesos)	Seguimiento al incidente en la herramienta de gestión de la Mesa de Servicio de TI. Formato Reporte Gestión de Incidentes de Seguridad	¿Se logró contener el incidente? **SI:** Continúa actividad N° 6. **NO:** Continúa actividad N° 8.
6.	Gestionar actividades para erradicar y solucionar el incidente de seguridad de la información.	Se gestionarán las actividades necesarias para erradicar el incidente de seguridad de la información bajo la coordinación del Oficial de Seguridad de la Información o profesional designado de la DTIC y las documenta en el Formato Reporte Gestión Incidentes de Seguridad. El Oficial de Seguridad de la Información o profesional designado de la DTIC deberá validar con los diferentes	Equipo de respuesta a incidentes (Todos los procesos)	Seguimiento al incidente en la herramienta de gestión de la Mesa de Servicio de TI. Formato Reporte Gestión de Incidentes de Seguridad	¿Se requiere Gestión de Cambios de TI? **SI:** Continuar con el procedimiento de Gestión de Cambios de TI-Código PC-GST-01, continúa actividad N° 7. **NO:** ¿El incidente de seguridad se logró erradicar? **SI:** continúa actividad N° 7.

N°	ACTIVIDAD	DESCRIPCIÓN DE LA ACTIVIDAD	RESPONSABLE (Dependencia)	DOCUMENTO O REGISTRO	PUNTOS DE CONTROL
		administradores para confirmar si la erradicación fue efectiva. Los incidentes que no estén en el alcance de la DTIC y que no puedan ser erradicados o solucionados serán escalados al Comité Institucional de Gestión y Desempeño o quien haga sus veces.			**NO:** Continua actividad N° 8.
7.	Validar la solución del evento o incidente de seguridad.	Revisar que las causas del incidente hayan sido erradicadas.	Oficial de Seguridad de la Información o profesional designado (Dirección de Tecnologías de la Información y Comunicaciones)	Seguimiento al incidente en la herramienta de gestión de la Mesa de Servicio de TI. Formato Reporte Gestión de Incidentes de Seguridad	Continúa con la actividad N° 9
8.	Activar plan de recuperación de desastres.	Evaluar estrategias para garantizar la continuidad de los servicios.	Nivel 2 o 3 Oficial de Seguridad de la Información o profesional designado (Dirección de Tecnologías de la Información y Comunicaciones)	Seguimiento y solución al incidente en la herramienta de gestión de la Mesa de Servicio de TI.	Continúa con la actividad N° 7.
9.	Reportar e informar el incidente de seguridad de la información al Comité Institucional de Gestión y Desempeño o quien haga sus veces.	El Oficial de Seguridad de la Información o profesional designado de la DTIC informará y gestionará con el comité todo lo referente (evidencias, riesgos, afectaciones, impacto, etc.)	Oficial de Seguridad de la Información o profesional designado (Dirección de Tecnologías de la Información y Comunicaciones)	Acta de reunión Comité Formato Reporte Gestión de Incidentes de Seguridad Correo electrónico citando al Comité Institucional de Gestión y Desempeño o quien haga sus veces.	
10.	Actualizar la matriz de riesgos de seguridad de la información.	En el caso que, dentro del análisis, contención y recuperación del incidente de seguridad de la información se haya identificado un riesgo que no se encuentra dentro del mapa de riesgos de seguridad de la información,	Oficial de Seguridad de la Información o profesional designado (Dirección de Tecnologías de la	Matriz de riesgos de seguridad de la información actualizada.	

N°	ACTIVIDAD	DESCRIPCIÓN DE LA ACTIVIDAD	RESPONSABLE (Dependencia)	DOCUMENTO O REGISTRO	PUNTOS DE CONTROL
		se debe documentar para su gestión incluyendo el plan de tratamiento del riesgo. Para esta actividad se requiere involucrar al Oficial de Seguridad de la Información o profesional designado de la DTIC y las áreas involucradas en el incidente de seguridad de la información.	Información y Comunicaciones)		
11.	Documentar y socializar las lecciones aprendidas y afinamiento.	Socializa mediante reunión a los interesados y documenta las lecciones aprendidas sobre la gestión realizada y valida la efectividad de los controles con el fin de fortalecer e interiorizar mediante diferentes estrategias y generar conciencia a los usuarios del IGAC. Se gestiona actualización de la base de conocimiento de la herramienta de gestión de la Mesa de Servicio de TI.	Oficial de Seguridad de la Información o profesional designado (Dirección de Tecnologías de la Información y Comunicaciones)	Acta de reunión Incidente solucionado en la herramienta de gestión de la Mesa de Servicio de TI. Formato Reporte Gestión de Incidentes de Seguridad	En caso de requerir ejecutar acciones posteriores al cierre del incidente, se puede generar un plan de mejoramiento.
FIN DEL PROCEDIMIENTO					

6. FORMATOS ASOCIADOS

- Plan de Pruebas de Gestión de Incidentes
- Registro Gestión Incidentes de Seguridad
-

7. CONTROL DE CAMBIOS

FECHA	CAMBIO	VERSIÓN
03/07/2024	° 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. ° Se ajusta el documento según la nueva Estructura Orgánica aprobada por Decreto 846 del 29 de Julio del 2021 ° Hace parte del proceso de **Gestión de Servicios Tecnológicos**. ° Se actualiza el procedimiento "Gestión de Incidentes de Seguridad de la Información", código **PC-GTI-02**, versión 1, a procedimiento del mismo nombre, código **PC-GST-04**, versión 1 ° Se crean los formatos: ▪ Plan de Pruebas de Gestión de Incidentes, código **FO-GST-PC04-01**, versión 1 ▪ Registro Gestión Incidentes de Seguridad, código **FO-GST-PC04-02**, versión 1 ° Se realizaron ajustes en las fases (preparación y prevención, detección, reporte, análisis, evaluación, contención, erradicación y recuperación, lecciones aprendidas de la gestión de incidentes de seguridad brindando detalle de las actividades, responsables y gestiones realizadas. ° Se incluyó la valoración de acuerdo con la criticidad de los activos de información afectados, el impacto actual y el impacto futuro con lo cual se determinará el nivel de prioridad y los tiempos de atención. ° Se incluyó roles o grupos operativos con su respectiva responsabilidad. ° Se ajustan las actividades en el flujo establecido del numeral 5, relacionando y cambiando los responsables bajo los roles o grupos representativos, se ajustan los pasos para el reporte de un posible evento de seguridad.	**1**

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. ◦ Se actualiza ambia de Manual de procedimiento" Gestión de incidentes de seguridad de la información", código **P15000-02/18.V1**, version 1, a Procedimiento del mismo nombre, código **PC-GTI-02**, versión 1. ◦ Se deroga totalmente la circular 231 del 31 de agosto de 2018.	**anterior**

ELABORÓ Y/O ACTUALIZÓ	REVISÓ TÉCNICAMENTE	REVISÓ METODOLÓGICAMENTE	APROBÓ
Nombre: Juan de Jesús Aponte Buitrago. **Cargo:** Contratista. Dirección de Tecnologías de la Información y Comunicaciones. **Nombre:** Diego Ramirez 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.