

1 OBJETIVO

Establecer los lineamientos para garantizar la atención de incidentes de seguridad y privacidad de la información, mediante la identificación, atención y respuesta que permitan mitigar acciones que pongan en riesgo la seguridad y privacidad de la información, los datos personales o los activos de información, así como el impacto asociado a la pérdida de confidencialidad, integridad y disponibilidad de la información de la Entidad.

2 ALCANCE

Desde la identificación de un evento o incidente que comprometa la confidencialidad, integridad, privacidad y disponibilidad de la información y/o datos personales que salvaguarda la Entidad, que obedezcan a la materialización de riesgos del proceso de Seguridad y Privacidad de la información, y/o de Seguridad Digital hasta el cierre de este, y aplica a todos los procesos de la Entidad.

3 NORMATIVIDAD

| Tipo | Número | Título | Fecha |
|---------------------|--------|--|------------|
| Ley | 1273 | 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. | 05/01/2009 |
| Ley | 1581 | Por la cual se dictan disposiciones generales para la protección de datos personales. | 17/10/2012 |
| Ley | 1712 | Por medio de la cual se crea la Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional y se dictan otras disposiciones. | 6/03/2014 |
| Decreto - Ley | 103 | Por el cual se reglamenta parcialmente la Ley 1712 de 2014 y se dictan otras disposiciones | 20/01/2015 |
| Decreto | 338 | Por el cual se adiciona el Título 21 a la Parte 2 del Libro 2 del Decreto Único 1078 de 2015, Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones, con el fin de establecer los lineamientos generales para fortalecer la gobernanza de la seguridad digital, se crea el Modelo y las instancias de Gobernanza de Seguridad Digital y se dictan otras disposiciones | 08/03/2022 |
| Resolución | 500 | 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 | 10/03/2021 |
| Resolución - COPNIA | 1197 | Por medio de la cual se adopta la Política de Protección de Datos Personales. | 31/08/2017 |

| Tipo | Número | Título | Fecha |
|----------------------------|-------------|---|------------|
| Ley | 1273 | 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. | 05/01/2009 |
| Resolución Nacional MINTIC | 1519 | Por la cual se definen los estándares y directrices para publicar la información señalada en la Ley 1712 del 2014 y se definen los requisitos materia de acceso a la información pública, accesibilidad web, seguridad digital, y datos abiertos. | 24/08/2020 |
| Resolución - COPNIA | R2024043248 | Por medio de la cual se actualiza el Modelo Integrado de Planeación y Gestión del COPNIA y se reglamentan sus respectivos comités. | 02/10/2024 |

4 DEFINICIONES

- **ACTIVO:** Cualquier cosa que tenga valor para una persona, una organización o un gobierno. [ISO 27032:2012]
- **ACTIVO DE INFORMACIÓN:** En relación con la privacidad de la información, se refiere al activo que contiene información pública que el sujeto obligado genere, obtenga, adquiera, transforme o controle en su calidad de tal.
- **CONFIDENCIALIDAD:** propiedad de la información que determina que esté disponible a personas autorizadas.
- **CONTROL:** Las políticas, los procedimientos, las prácticas y las estructuras organizativas concebidas para mantener los riesgos de seguridad de la información por debajo del nivel de riesgo asumido. Control es también utilizado como sinónimo de salvaguarda o contramedida. En una definición más simple, es una medida que modifica el riesgo.
- **DATO PERSONAL:** cualquier información vinculada o que pueda asociarse a una o varias personas naturales determinadas o determinables. Debe entonces entenderse el "dato personal" como una información relacionada con una persona natural (persona individualmente considerada). Ejemplo: Nombres, apellidos, fecha y lugar de nacimiento, número de identificación, teléfono, e información asociada a sus actividades, registro multimedia, preferencias ideológicas, políticas, creencias religiosas, entre otros.
- **DELITO INFORMÁTICO:** Son acciones ilegales que se cometen mediante el uso de herramientas informáticas y redes tecnológicas.
- **DERECHOS DE ACCESO PRIVILEGIADO:** se refieren a los privilegios y autorizaciones especiales otorgados a usuarios dentro de un sistema o red, concediéndoles niveles de acceso más elevados de lo habitual. Estos derechos permiten a los usuarios realizar acciones y operaciones que van más allá de las funciones estándar, como la capacidad de modificar configuraciones críticas, acceder a información sensible o realizar cambios en el entorno tecnológico. La gestión cuidadosa de los Derechos de Acceso Privilegiado es esencial para

garantizar la seguridad de la información, ya que un uso indebido o la explotación de estos privilegios pueden resultar en riesgos significativos de seguridad.

- **DISPONIBILIDAD:** Propiedad de la información de estar accesible y utilizable cuando lo requiera una entidad autorizada. [ISO/IEC 27000].
- **EVIDENCIA DIGITAL:** Es el registro de información electrónico o digital guardada o difundida a través de medios informáticos que permita probar un delito informático.
- **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. (ISO/IEC 27000).
- **INCIDENTE DE SEGURIDAD:** un acceso, intento de acceso, uso, divulgación, modificación o destrucción no autorizada de información; un impedimento en la operación normal de las redes, sistemas o recursos informáticos; o una violación a una Política de Seguridad de la Información de la entidad; que afecte a la confidencialidad, integridad o disponibilidad de los activos de información.
- **INFORMACIÓN:** se refiere a un conjunto organizado de datos contenido en cualquier documento que los responsables y/o encargados del tratamiento generen, obtengan, adquieran, transformen o controlen.
- **INTEGRIDAD:** característica de los activos de información que salvaguarda la exactitud y estado completo de la información o activos.
- **FIRMWARE:** programa integrado en dispositivos de hardware para ayudarlos a operar de manera efectiva.
- **PORTAL WHOIS:** es un protocolo y herramienta que se utiliza para consultar información sobre la titularidad y el registro de un dominio de Internet (como midominio.com), o una dirección IP.
- **PRIVACIDAD DE LA INFORMACIÓN/DATOS:** es el aspecto de las tecnologías de la información (TI) que trata sobre la capacidad que una organización o individuo tiene para determinar qué datos en un sistema informático se pueden compartir con terceros.
- **SEGURIDAD DE LA INFORMACIÓN:** Preservación de la confidencialidad, integridad y disponibilidad de la información, además, otras propiedades tales como autenticidad, responsabilidad, no repudio y confiabilidad pueden estar involucradas. [ISO/IEC 27000].

5 CONDICIONES GENERALES

5.1 GENERALIDADES

- El único medio de contacto autorizado para la atención de incidencias de seguridad y privacidad de la información será a través de la mesa de ayuda estipulada en el procedimiento para la atención de incidencias y requerimientos TIC-pr-01 categoría SEGURIDAD DE LA INFORMACIÓN y/o por correo electrónico seguridadinformación@copnia.gov.co. En caso de que el incidente sea reportado mediante correo electrónico, este será documentado en la plataforma de tickets adoptada por la Entidad para mantener el control de estos, así como el seguimiento a los tiempos de

respuesta, por parte del Profesional de Gestión de la Oficina de Seguridad y Privacidad de la Información.

- Los funcionarios y/o contratistas, a través del supervisor de contrato, que detecten un incidente de seguridad y privacidad de la información, deberán reportarlo de manera inmediata aportando la mayor cantidad de evidencias posibles del incidente, a través de los medios autorizados e indicados en el punto anterior
- Para el reporte de incidentes de seguridad y privacidad de la información, es necesario que se indique claramente:
 - o Fecha y hora en que ocurrió el incidente.
 - o Fecha y hora en la que se detectó el incidente.
 - o Clasificación del incidente. (ver tabla numeral 5.4.2.1 Clasificación de incidentes)
 - o Descripción detallada del incidente: ¿Qué? ¿Cómo? ¿Qué activos de información están comprometidos o afectados?
- La identificación de incidentes de seguridad y privacidad de la información puede darse, entre otros, a través de:
 - o Alertas en el sistema de monitorización de redes y sistemas de detección de intrusos.
 - o Escalamiento de eventos identificados por los administradores de servidores.
 - o Escalamiento de eventos identificados por los administradores de la infraestructura tecnológica de la Entidad.
 - o Situaciones irregulares identificadas por los usuarios responsables del manejo de activos de información.
 - o Escalamiento de eventos identificados por las ventanillas de radicación.
 - o Alertas de seguridad nacional.
 - o Escalamiento de eventos identificados por entes de control.
 - o Uso indebido de datos personales identificados por los titulares de la información.
 - o Identificación de incidentes por funcionarios y/o contratistas.
- Para la identificación de incidentes de seguridad y privacidad de la información se tomará como base el mapa de riesgos de seguridad digital y/o del proceso de seguridad y privacidad de la información. Si el incidente de seguridad reportado obedece a la materialización de un riesgo de dicho mapa, este se tratará de acuerdo con el procedimiento de administración del riesgo DE-pr-02 Anexo 7 Lineamientos para el manejo de riesgos materializados y a lo establecido en este documento para realizar el análisis, recolección de información, mejoras y lecciones aprendidas; en caso contrario se atenderá conforme al procedimiento de atención de incidencias y requerimientos (TIC-pr-01). Ejemplo: En el caso de que se presente un correo electrónico sospechoso o dudas respecto al mismo, este se atenderá a través del procedimiento de atención de incidencias y requerimientos (TIC-pr-01), para lo cual, el funcionario colocará el ticket respectivo y el mismo se atenderá conforme a los Acuerdos de Niveles de Servicio allí estipulados. Sin embargo, si el incidente se relacionara con la divulgación de información de datos personales este se tratará por el procedimiento acá descrito.
- Cualquier incidente de seguridad y privacidad de la información en el que estén involucrados funcionarios de la Entidad, deberá ser reportado por el Profesional de Gestión de la Oficina de Seguridad y Privacidad de la Información a la Oficina de Control Interno Disciplinario.

- Todos los incidentes de seguridad y privacidad de la información deberán ser reportados al Subcomité de seguridad de la información por parte del Profesional de Gestión de la Oficina de Seguridad y Privacidad de la información.
- El Profesional de Gestión de la Oficina de Seguridad y Privacidad de la Información es el único funcionario autorizado para reportar incidentes de seguridad y privacidad de la información ante las autoridades competentes, con el apoyo de las áreas que se consideren pertinentes. Así mismo, se realizarán los pronunciamientos oficiales ante los ciudadanos, que se consideren pertinentes, teniendo en cuenta el procedimiento interno de comunicaciones oficiales (GD-pr-01).
- Durante la gestión y atención del incidente de seguridad y privacidad de la información todos los involucrados en la gestión de las etapas para el manejo de incidentes de seguridad y privacidad de la información deberán garantizar la recolección, entrega y custodia de las evidencias del incidente de acuerdo con cada etapa. La custodia de las evidencias será responsabilidad del Profesional de Gestión de la Oficina de Seguridad y Privacidad de la información, quien deberá garantizar su preservación digital en los repositorios adoptados por la Entidad (OneDrive, Gestor Documental), por lo que los involucrados deberán entregar todas las evidencias recolectadas a este.
- La Oficina de Seguridad y Privacidad de la información se encargará de:
 - o Detección de Incidentes de Seguridad: Monitorear y verificar los elementos de control con el fin de detectar un posible incidente de seguridad de la información.
 - o Anuncios de Seguridad: Deben mantener informados a los funcionarios, contratistas o terceros sobre las nuevas vulnerabilidades, actualizaciones a las plataformas y recomendaciones de seguridad informática a través de algún medio de comunicación (Web, Intranet, Correo).
 - o Certificación de productos: verificar la implementación de las nuevas aplicaciones en producción para que se ajusten a los requerimientos de seguridad y privacidad de la información establecidos por la Entidad conforme con el Manual de Seguridad de la información SPI-m-01.
 - o Clasificación y priorización de servicios expuestos: Identificación de servicios sensibles y aplicaciones expuestas para la prevención o remediación de ataques.
 - o Investigación y Desarrollo: Realizar la búsqueda constante de nuevos productos en el mercado o desarrollo de nuevas herramientas de protección para combatir brechas de seguridad, y la proposición de nuevos proyectos de seguridad de la información.

5.2 ROLES PARA EL MANEJO DE INCIDENTES DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

En cumplimiento con la normatividad y basado en la guía de roles y responsabilidades de MinTic¹, la Entidad establece un modelo de responsabilidades claramente definido para asegurar que todos los incidentes de seguridad, incluyendo aquellos que puedan afectar datos personales o información sensible, sean gestionados de manera eficiente, estructurada y conforme a procedimientos documentados. Dado que una adecuada gestión de incidentes requiere de la participación coordinada de diversas áreas y niveles jerárquicos dentro de la Entidad, se tienen los siguientes roles:

- **SUBCOMITÉ DE SEGURIDAD DE LA INFORMACIÓN:** debe generar las recomendaciones para la implementación de políticas, planes, programas y proyectos en materia de seguridad

de la información y controles en la implementación de sistemas o servicios, entre otras conforme a lo establecido en la Resolución R2024043248.

- **EQUIPO DIRECTIVO:** asegura que la gestión de incidentes de seguridad y privacidad de la información se lleve a cabo de forma eficaz, alineada con los principios de legalidad, transparencia, responsabilidad institucional y protección de la información pública y personal que custodia la entidad. De igual forma, proporciona los recursos necesarios para prevenir, detectar, responder y recuperarse de los incidentes de seguridad y privacidad de la información
- **PROFESIONAL DE GESTIÓN DE LA OFICINA DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN:** debe mantener actualizado el procedimiento de gestión de incidentes de seguridad y privacidad de la información, hacer el registro y realizar los reportes a las autoridades competentes en caso de ser necesario, lidera el equipo de respuesta de incidentes de seguridad y privacidad de la información, y debe recolectar las evidencias aportadas y custodiar las mismas.
- **PROFESIONAL DE GESTIÓN DEL ÁREA DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES:** en conjunto con el profesional de gestión de la Oficina de Seguridad y Privacidad de la Información, coordinar las labores de identificación, contención, erradicación, solución y documentación de los incidentes de seguridad, así como de buscar las mejoras para evitar incidentes a futuro.
- **ÁREA DE TECNOLOGÍAS DE LA INFORMACION Y LAS COMUNICACIONES:** garantiza la implementación de los lineamientos de seguridad y privacidad de la información a nivel de los sistemas de información, redes y software, así mismo debe mantener actualizados los sistemas de información. De igual forma, a través de los supervisores de contrato de la infraestructura tecnológica y software contratado debe garantizar la actualización, implementación y seguimiento de las medidas de seguridad establecidas, así como el cumplimiento de las políticas, lineamientos y procedimientos establecidos en materia de seguridad y privacidad de la información
- **PROFESIONAL DE GESTIÓN DEL ÁREA DE GESTIÓN HUMANA:** coordina la inclusión del tema de gestión de incidentes en el Plan Institucional de Capacitaciones y garantiza que todos los funcionarios reciban la capacitación correspondiente, conforme a lo solicitado por el Profesional de Gestión de la Oficina de Seguridad y Privacidad de la Información, y a lo aprobado en dicho plan.
- **PROFESIONAL DE GESTIÓN DEL ÁREA ADMINISTRATIVA:** garantiza la implementación de los lineamientos de seguridad y privacidad de la información a nivel de la gestión documental de la Entidad y la administración de activos físicos.
- **ÁREA DE RELACIONAMIENTO INTERINSTITUCIONAL Y COMUNICACIONES:** apoya, en articulación con el Equipo Directivo, la Subdirección Jurídica y el Subcomité de Seguridad de la Información, la generación de mensajes institucionales dirigidos a públicos internos, externos, incluyendo otras entidades del Estado, organismos de control y ciudadanía, cuando el incidente así lo amerite, generados por la Oficina de Seguridad y Privacidad de la Información.
- **SUBDIRECCIÓN DE PLANEACIÓN, CONTROL Y SEGUIMIENTO:** asegura que el procedimiento de gestión de incidentes de seguridad y privacidad de la información se encuentre, documentado y alineado con los sistemas de gestión institucionales.

- **SUBDIRECCION JURÍDICA:** mitiga riesgos legales y debe proteger los intereses jurídicos de la Entidad.
- **PROFESIONAL DE GESTIÓN DEL ÁREA DE CONTRATACIÓN:** debe garantizar la inclusión de cláusulas requeridas para el cumplimiento y aseguramiento de la seguridad y privacidad de la información dentro de cada uno de los contratos que así lo amerite.
- **OFICINA DE CONTROL INTERNO:** evalúa la eficacia de los controles de seguridad y la gestión de incidentes con el fin de fortalecer el Sistema de Control Interno Institucional y garantizar una gestión eficiente, transparente y orientada a la mejora continua.
- **OFICINA DE CONTROL INTERNO DISCIPLINARIO:** determina la existencia de faltas disciplinarias y adelanta las investigaciones administrativas correspondientes cuando el incidente esté relacionado con posibles conductas irregulares por parte de los funcionarios.
- **SUPERVISORES DE CONTRATO:** deben garantizar el cumplimiento, por parte de los contratistas, de las políticas, lineamientos y procedimientos establecidos en materia de seguridad y privacidad de la información.
- **FUNCIONARIOS Y/O CONTRATISTAS:** Todos los funcionarios de la Entidad y contratistas que manejen activos de información de la Entidad tienen la responsabilidad de reportar de manera oportuna cualquier incidente o evento que pueda derivar en un incidente de seguridad y privacidad de la información.

5.3 EQUIPO DE RESPUESTA A INCIDENTES DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN:

El equipo de respuesta a incidentes de seguridad y privacidad de la información estará liderado por el Profesional de Gestión de la Oficina de Seguridad y Privacidad de la información, quien, dependiendo del incidente y criticidad de este, podrá solicitar el apoyo, entre otros a:

- Profesional de Gestión del Área de Tecnologías de la Información y las Comunicaciones.
- Profesional de Gestión del Área Administrativa (En caso de que vulnere activos de información documental físicos o digitales).
- Profesional de Gestión de Atención al ciudadano (en caso de vulneración de datos personales).
- Líderes de procesos que se requieran.
- Demas funcionarios que se consideren necesarios para contener y atender el incidente de seguridad y privacidad de la información.

Dicho equipo deberá aunar esfuerzos de manera inmediata y brindar el apoyo correspondiente para abordar las etapas de contención, erradicación y recuperación, así como post – incidente, descritas en los numerales 5.4.3 y 5.4.4 del presente documento.

Este equipo que se conforme estará enfocado principalmente en atender incidentes de seguridad y privacidad de la información que se presentan sobre activos de información de la Entidad, sin embargo, dependiendo de la criticidad del incidente, este equipo podrá incluir a líderes de los procesos que se vean afectados, la alta dirección y la Oficina de Control Interno.

Dependiendo de la clasificación del incidente de seguridad y privacidad de la información, el equipo de respuesta a incidentes de seguridad de la información será el encargado de apoyar la definición de las acciones para la atención del incidente de seguridad y privacidad de la información, restablecer (en caso de ser necesario) los sistemas de información y brindar solución al incidente.

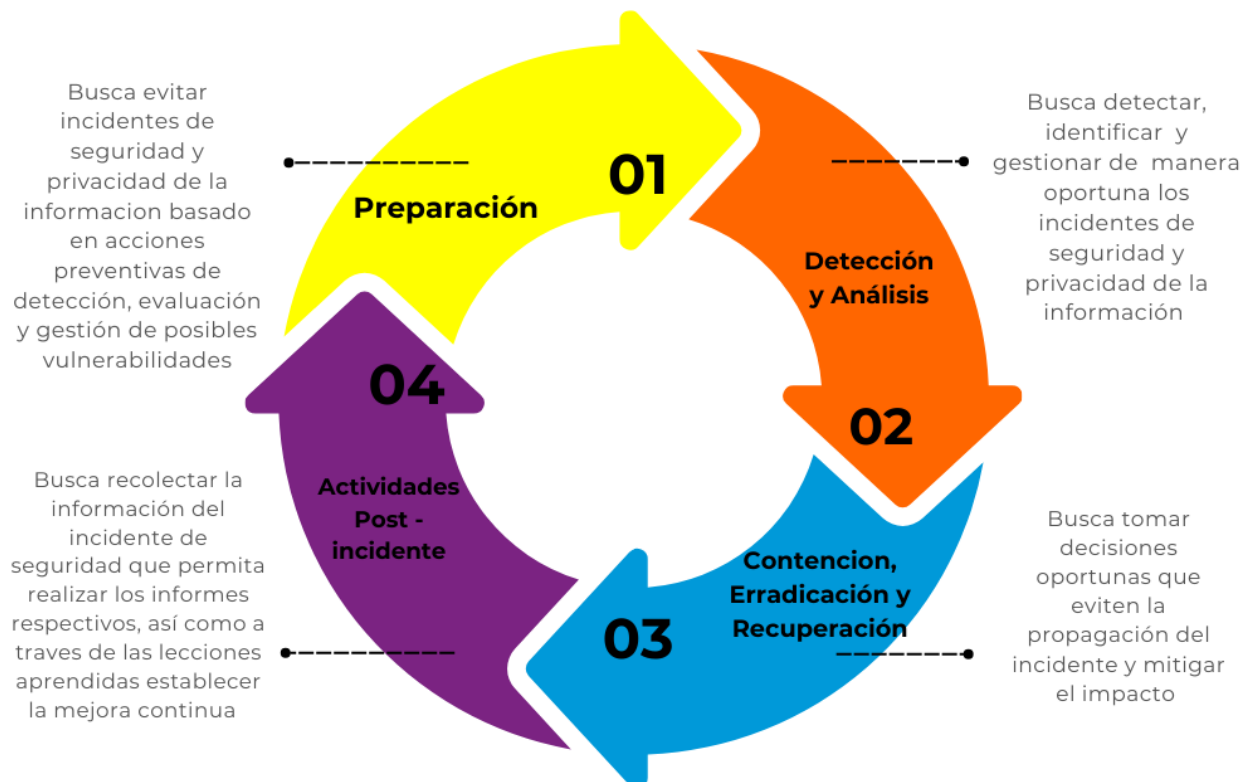
Una vez solucionado el incidente, el Profesional de Gestión de la Oficina de Seguridad y Privacidad de la Información, presentará un informe de la atención del incidente al Subcomité de seguridad de la información, quien tiene como funciones:

- Revisar y analizar los diagnósticos y consolidados de incidentes de seguridad y vulnerabilidades detectadas en la entidad y presentar recomendaciones con fundamento a las mejores prácticas.
- Participar en la formulación y evaluación de planes de acción para mitigar y/o eliminar riesgos.

5.4 ETAPAS PARA EL MANEJO DE INCIDENTES DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

Conforme con la guía para la gestión y clasificación de incidentes de seguridad de la información de MINTIC¹, la gestión de incidentes de seguridad y privacidad de la información debe estar enmarcada en 4 componentes para dar cumplimiento al ciclo de vida de la gestión y respuesta de los incidentes de seguridad y privacidad de la información:

Etapas para la gestión de incidentes



Fuente: Adaptado de la Guía para la gestión y clasificación de incidentes de seguridad la información – MinTic¹

5.4.1 ETAPA DE PREPARACIÓN

Esta etapa será liderada por el Profesional de Gestión de la Oficina de Seguridad y Privacidad de la información, quien recomendará políticas, procedimientos, estrategias y controles que permitan prevenir los incidentes de seguridad y privacidad de la información, a través de las siguientes actividades:

- Realizar contactos con grupos de interés especial que, a través de boletines, brinden conocimiento respecto a posibles amenazas, vulnerabilidades o riesgos a mitigar, así como nuevas tecnologías para la mitigación de estas. Algunas de las entidades que se toman como referencia para que a través de la suscripción (si aplica) a boletines, comunicados, alertas o reuniones que se organicen se pueda mantener el contacto activo, son:
 - CSIRT: <https://cc-csirt.policia.gov.co/>
 - COLCERT: <https://www.colcert.gov.co/>
 - Comando Conjunto Cibernético: <https://www.cgfm.mil.co/es/comando-conjunto-cibernetico>
 - Centro Cibernético policial: <https://caivirtual.policia.gov.co/observatorio/boletines>
 - Ministerio de Tecnología de la Información y las Comunicaciones.
 - Boletín CIP – CSIRT UNAD: <https://selloeditorial.unad.edu.co/produccion/boletines/boletines-cip-csirt>
- Analizar los boletines de conocimiento emitidos por los grupos de interés especial para determinar qué acciones se pueden implementar en la Entidad.
- Recomendar las mejores prácticas para el aseguramiento de redes, sistemas y aplicaciones, entre las cuales pueden estar:
 - Gestión de Parches de Seguridad: implementar programas de gestión de vulnerabilidades (Sistemas Operativos, Bases de Datos, Aplicaciones, Otro Software Instalado), este programa ayudará a los administradores en la identificación, adquisición, prueba e instalación de los parches.
 - Aseguramiento de plataformas tecnológicas: Se debe garantizar el aseguramiento de los sistemas de información y entorno tecnológico mediante el cumplimiento e implementación de la Política de Asignación y Uso de Derechos de Acceso Privilegiado y Política de Revisión y Mantenimiento de Matriz de Roles y Perfiles conforme a lo establecido en el Manual de Seguridad de la Información SPI-m-01.
 - Seguridad en redes: Debe realizarse una gestión constante y oportuna sobre los elementos de seguridad. Las reglas configuradas en equipos de seguridad como firewalls deben ser revisadas continuamente por el área de Tecnologías de la Información y las Comunicaciones con apoyo de los contratistas.
 - Controles de acceso: se deben garantizar los lineamientos de controles de acceso conforme a lo establecido en el Manual de Seguridad de la Información SPI-m-01.

¹ ¹ Guía para la Gestión y Clasificación de Incidentes de Seguridad de la Información: https://gobiernodigital.mintic.gov.co/692/articles-5482_G21_Gestion_Incidentes.pdf

- Prevención de código malicioso: Todos los equipos de la infraestructura (servidores como equipos de usuario) deben tener activo su antivirus, antimalware con las firmas de actualización al día.
- Monitoreo a sitios web: De manera preventiva la Oficina de Seguridad de la Información deberá realizar monitoreos a sitios web con el fin de prevenir intentos de suplantación de dominio.
- Capacitación y sensibilización: Todos los funcionarios de la Entidad deben ser sensibilizados de acuerdo con el Plan Institucional de Capacitación, o a través de campañas de sensibilización sobre el uso apropiado de redes, sistemas de información, equipos de cómputo y en general sobre cualquier elemento que pueda afectar la seguridad y privacidad de la información. Dicha capacitación y/o sensibilización será liderada por el Profesional de Gestión de la Oficina de Seguridad y Privacidad de la información en coordinación con el Área de Gestión Humana.

La etapa de preparación debe ser apoyada por el Profesional de Gestión del Área de Tecnologías de la información y las comunicaciones incluyendo las mejores prácticas.

5.4.2 ETAPA DE DETECCIÓN Y ANÁLISIS

El objetivo de esta etapa es informar e identificar de manera oportuna cualquier irregularidad que pueda afectar la seguridad y privacidad de la información, impactando de forma negativa la confidencialidad, integridad y disponibilidad de los activos de información de la Entidad.

5.4.2.1 Clasificación de incidentes

La clasificación del incidente se realiza dependiendo de la infraestructura, riesgo y criticidad de los activos afectados, entre los siguientes tipos:

| Tipo de incidente | Descripción |
|--------------------------|---|
| Ciberataque externo | Incluye acciones como: <ul style="list-style-type: none"> - Ataques de denegación de servicio (DDoS). - Infiltración por parte de actores estatales extranjeros (APT – Amenazas Persistentes Avanzadas). - Vulnerabilidades en infraestructuras críticas. - Uso de software malicioso. - Suplantación de sitio web. |
| Acceso no autorizado | <ul style="list-style-type: none"> - Acceso lógico no autorizado respecto al correo electrónico, internet, servidores u otros servicios tecnológicos. - Acceso físico no autorizado a los recursos y/o instalaciones de la entidad. - Uso indebido de la información contenida en los recursos tecnológicos de la entidad o en medios físicos. - Divulgación no autorizada de información física. |

| Tipo de incidente | Descripción |
|--|--|
| | <ul style="list-style-type: none"> - Divulgación no autorizada de información digital. |
| Filtración o Exposición de Información | <ul style="list-style-type: none"> - Robo de datos ciudadanos o de funcionarios. - Publicación no autorizada de documentos clasificados. - Acceso indebido a bases de datos. |
| Incidentes internos | <ul style="list-style-type: none"> - Uso indebido de credenciales por parte de funcionarios. - Errores de configuración que exponen información. - Pérdida de dispositivos con información confidencial. - Cambios o modificaciones en registros de bases de datos sin previa autorización. - Realización de copias no autorizadas de software. - Instalación de Software no autorizado por el área TIC. |
| Infraestructura Crítica Comprometida | <ul style="list-style-type: none"> - Ataques a redes de comunicaciones. - Sabotaje o manipulación de sistemas eléctricos. - Eventos causados por fenómenos naturales. |
| Uso Inapropiado | <ul style="list-style-type: none"> - Violación de alguna de las políticas de seguridad de la información definidas por la entidad. - Uso indebido de la imagen institucional. |
| Violación de datos personales | <ul style="list-style-type: none"> - Pérdida de información (física o digital) en equipos o instalaciones físicas. - Robo de información digital. - Robo de información física. - Modificación o destrucción no autorizada de información. - Uso no autorizado de la información en formato físico o digital. |
| Multicomponente | Involucra más de un tipo de incidente categorizado anteriormente. |

5.4.2.2 Priorización de incidentes

Para priorizar los incidentes reportados se tendrá en cuenta el impacto del incidente, la criticidad del impacto y los sistemas afectados así:

| VALORACIÓN DE PROCESOS AFECTADOS | | |
|--|--------------|----------------|
| PROCESOS AFECTADO | VALOR | IMPACTO |
| Afecta varios procesos misionales o áreas de la Entidad con sus sistemas de información/ Afecta sistemas tecnológicos transversales que | 1.0 | Crítico |

| VALORACIÓN DE PROCESOS AFECTADOS | | |
|---|--------------|----------------|
| PROCESOS AFECTADO | VALOR | IMPACTO |
| afectan el cumplimiento de la misionalidad de la Entidad. | | |
| Afecta procesos no misionales o áreas no misionales. | 0.75 | Alto |
| Afecta un área de la Entidad o en varias áreas, pero no es de manera constante. | 0.50 | Medio |
| Afecta solo un área de la Entidad, pero el trabajo puede continuar. | 0.25 | Bajo |
| Aunque haya algún proceso afectado los efectos no se notan en ninguna área de la Entidad. | 0.00 | Ninguno |

Nota: La valoración de procesos afectados debe realizarse teniendo en cuenta tanto el impacto actual (en el momento del incidente) y/o a futuro dependiendo de la cantidad del daño que pueda causar el incidente si este no es contenido, ni erradicado.

| CRITICIDAD DEL SISTEMA | | |
|---|--------------|----------------|
| SISTEMA AFECTADO | VALOR | IMPACTO |
| Afecta los sistemas de información misionales, infraestructura tecnológica transversal a todos los sistemas de información y/o la mayoría de las estaciones de trabajo de los funcionarios de la Entidad. | 1.0 | Crítico |
| Afecta sistemas tecnológicos y estaciones de trabajo de usuarios con funciones críticas en la Entidad. | 0.75 | Alto |
| Afecta sistemas de información o herramientas tecnológicas que apoyan una sola área o dependencia de la Entidad. | 0.50 | Medio |
| Afecta solo alguna estación de trabajo, pero el trabajo puede continuar | 0.25 | Bajo |

Una vez se tengan definidas las variables, la prioridad se dará por la siguiente formula:

$$\text{Nivel Prioridad} = (\text{Impacto actual} * 2,5) + (\text{Impacto futuro} * 2,5) + (\text{Criticidad del Sistema} * 5)$$

De acuerdo con el resultado la prioridad se establecerá así:

| Nivel de Prioridad | Valor |
|---------------------------|--------------|
| Crítico | 7.50 - 10.00 |
| Alto | 5.00 - 7.49 |
| Medio | 3.75 - 4.99 |
| Bajo | 2.50 - 3.74 |
| Mínimo | 0.00 - 2.49 |

Para realizar la clasificación y priorización de los incidentes deberá utilizarse el formato SPI-fr-09. Este formato deberá ser diligenciado únicamente en los casos en que el incidente obedezca a la

materialización de un riesgo de la Matriz de Riesgos de Seguridad digital o la matriz de riesgos del proceso de seguridad y privacidad de la información

5.4.2.3 Tiempos de respuesta de los incidentes

Una vez clasificado y priorizado el incidente de seguridad, se realizará la atención y respuesta al mismo de acuerdo con la siguiente tabla

| Nivel de Prioridad | Responsable de atención | Tiempo de atención | Tiempo de respuesta |
|--------------------|--|--------------------|---------------------|
| Crítico | Equipo de respuesta a incidentes de seguridad de la información. | 0 - 45 minutos | 0 - 4 horas |
| Alto | Equipo de respuesta a incidentes de seguridad de la información. | 1 - 2 horas | 5 - 12 horas |
| Medio | Profesional de gestión Oficina de Seguridad y privacidad de la Información - Área TIC. | 3 - 4 horas | 12 - 18 horas |
| Bajo | Profesional de gestión Oficina de Seguridad y privacidad de la Información - Área TIC. | 4 - 12 horas | 18 - 24 horas |
| Mínimo | Profesional de gestión Oficina de Seguridad y privacidad de la Información. | 12 - 24 horas | 24 - 48 horas |

5.4.2.4 Directorio de contactos

En caso de presentarse un incidente de seguridad con nivel de prioridad crítico o alto, este debe ser reportado a los entes de control o autoridades competentes, por el Profesional de Gestión de la Oficina de Seguridad y Privacidad de la Información en coordinación con el Equipo Directivo, así:

| Descripción | Entidad | Contacto |
|--|--|---|
| Incidentes relacionados Violación de datos personales | Superintendencia de Industria y Comercio | https://sedeelectronica.sic.gov.co/ |
| Incidentes de seguridad que requieran asesoría para posterior judicialización: <ul style="list-style-type: none"> - Robo de información digital. - Robo de información física. - Ataques de denegación de servicio (DDoS). - Infiltración por parte de actores estatales extranjeros (APT - Amenazas Persistentes Avanzadas). - Vulnerabilidades en infraestructuras críticas. - Uso de software malicioso. - Suplantación de sitio web. | Centro Cibernético Policial https://caivirtual.policia.gov.co/ Denuncia presencial en estación de policía, SIJIN o URI DE Fiscalía, Líneas telefónicas (Líneas de atención nacional) 0180000919748 - Celular 122 Línea local para Bogotá y Cundinamarca 5702000 , opción 7 | |

| Descripción | Entidad | Contacto |
|---|--|--|
| | | para realizar su solicitud.) o mediante correo electrónico ges.documentalpgrs@fiscalia.gov.co |
| Incidentes de seguridad que afectan componentes de la infraestructura tecnológica. | Grupo de Respuesta a Emergencias Cibernéticas de Colombia – colCERT Equipo de Respuesta a Incidentes de Seguridad Digital | https://www.colcert.gov.co/contacto@colcert.gov.co Teléfono: 601 344 34 60. Csirtgob@mintic.gov.co Teléfono: 01 8000 910742 Opción 3. |
| Incidentes relacionados con los siguientes temas: - Robo - Acceso no autorizado - Emergencias por catástrofes naturales - Emergencias por incendio, uso de sustancias peligrosas. | Línea de Emergencia única | Teléfono: 123 |

5.4.3 ETAPA DE CONTENCIÓN, ERRADICACIÓN Y RECUPERACIÓN

Una vez analizado, clasificado y priorizado el incidente de seguridad se debe contener de manera inmediata, para evitar su propagación y que esto impida su erradicación.

Dependiendo de cada incidente el equipo de respuesta a incidentes, debe determinar el método de contención más eficaz, entre los cuales puede estar:

- Apagar el sistema o estación de trabajo afectado.
- Desconectar el sistema o estación de trabajo de la red de la Entidad.
- Deshabilitar funciones, cuentas comprometidas o con actividad inusual.
- Bloqueo de cuentas, direcciones IP maliciosas.
- Aplicar bloqueos de Firewall y listas negras
- Cerrar sesiones sospechosas.
- Generar avisos en página web y redes sociales que pongan en conocimiento a la ciudadanía de la situación (en caso de suplantación en página web o redes sociales).

Posterior a la contención del incidente, la Oficina de Seguridad y Privacidad de la información en conjunto con los líderes de los procesos afectados determinarán la estrategia de erradicación y recuperación dependiendo de cada caso, a través de la restauración de los sistemas y/o servicios afectados de manera controlada. Una vez contenido el incidente estas se informarán al equipo de respuesta a incidentes para que se planee la estrategia a seguir. En caso de tratarse de incidentes

de seguridad relacionados con el ecosistema tecnológico de la Entidad, esta etapa será llevada a cabo por el Área de Tecnologías de la Información y las Comunicaciones.

Dentro de las estrategias de erradicación pueden contemplarse, entre otras, las siguientes actividades:

- Desinfección de malware a través de uso de antivirus o escaneos de seguridad.
- Eliminación de archivos maliciosos.
- Eliminación de accesos no autorizados.
- Revocar credenciales comprometidas y restablecer contraseñas afectadas.
- Instalar actualizaciones de software y parches de seguridad para corregir brechas explotadas.
- Actualizar firmware y configuraciones de seguridad en dispositivos afectados.
- Revisar y reforzar configuraciones de seguridad en sistemas operativos, aplicaciones y redes.
- Aislamiento o restricción inmediata del área comprometida.
- Retiro o Aseguramiento de Dispositivos Físicos Afectados.
- Cambio o reforzamiento de Cerraduras, Códigos y Accesos Físicos.
- Reubicación Temporal de Funcionarios o Servicios Críticos.
- Coordinación con Brigadas de Emergencia o Gestión del Riesgo.

La restauración es una actividad fundamental para recuperar la operación, minimizar los efectos causados y fortalecer la seguridad de los activos de información. Para ello se sugiere usar, entre otras, las siguientes actividades:

- Restitución del servicio caído.
- Restauración de archivos desde Backup seguro.
- Reparación del sitio.
- Reinstalación del equipo o sistema y recuperación de datos.
- Verificar la integridad del sistema o los datos tras la recuperación.
- Restablecimiento del acceso físico controlado.
- Reorganización del entorno físico afectado.
- Revisión y actualización del inventario físico de activos.
- Reincorporación del personal a los espacios físicos.
- Validación de controles físicos reforzados.

Para garantizar la restauración de los sistemas o activos de información afectados es primordial que el área de Tecnologías de la Información y las Comunicaciones, dé estricto cumplimiento a las políticas de objetivos de punto de recuperación (RPO) y objetivos de tiempos de recuperación (RTO) de 24 horas para los sistemas de información, establecida en el Manual de seguridad de la información (SPI-m-01).

- Suplantación de sitios web

En caso de detectarse la suplantación de sitios web, se deberá informar de manera inmediata a la Oficina de Seguridad y Privacidad de la información y proceder con la recolección de evidencias, incluyendo la verificación del proveedor del dominio a través del portal *Whois*. Es indispensable capturar imágenes y videos que respalden la existencia del sitio fraudulento. Durante esta fase, se debe verificar si existen redireccionamientos sospechosos y asegurarse de que el sitio web oficial de la Entidad no se encuentre comprometido ni redirigiendo hacia el sitio falso. Así mismo, con el apoyo del Área de Relacionamento Institucional y Comunicaciones se deben generar avisos en página web y redes sociales que alerten a la ciudadanía para evitar posibles fraudes.

Una vez obtenidas todas las evidencias, se debe informar la situación mediante correo electrónico al proveedor del dominio identificado y a COLCERT (contacto@colcert.gov.co), solicitando la deshabilitación del dominio fraudulento. Posteriormente, se deberán interponer las denuncias correspondientes ante las autoridades competentes, remitiendo toda la evidencia recolectada a través del portal oficial de la Policía Nacional: <https://caivirtual.policia.gov.co/>.

- Suplantación o uso indebido de imágenes institucionales en Redes Sociales (Facebook, Instagram, WhatsApp)

En caso de identificarse la suplantación o el uso no autorizado de imágenes institucionales en redes sociales (incluyendo logotipos, nombres, fotografías oficiales, contenido gráfico o audiovisual), se debe informar de manera inmediata a la Oficina de Seguridad y Privacidad de la Información e iniciar de inmediato el proceso de recolección de evidencias, esto incluye capturas de pantalla, grabaciones en video y enlaces directos a las publicaciones, perfiles o cuentas involucradas. Así mismo, con el apoyo del Área de Relacionamento Institucional y Comunicaciones se deben generar avisos en página web y redes sociales que alerten a la ciudadanía para evitar posibles fraudes.

Es fundamental verificar si el contenido está siendo utilizado para suplantar a la Entidad, generar desinformación o afectar su reputación institucional.

- Una vez reunidas las evidencias, se procederá a reportar la situación directamente a la plataforma o red social donde se detectó el incidente, utilizando los mecanismos oficiales de denuncia por suplantación de identidad, uso indebido de marca o contenido engañoso. Paralelamente, se deberá interponer las denuncias ante las autoridades competentes adjuntando el material probatorio correspondiente través del portal de la Policía Nacional: <https://caivirtual.policia.gov.co/>, denuncia presencial en estación de policía, SIJIN o URI DE Fiscalía, líneas telefónicas (Líneas de atención nacional **0180000919748** – Celular **122** Línea local para Bogotá y Cundinamarca **5702000**, opción 7 para realizar su solicitud.) o mediante correo electrónico ges.documentalpqr@fiscalia.gov.co

5.4.4 ETAPA POST – INCIDENTE

Una vez que la amenaza ha sido eliminada y los sistemas restaurados, es fundamental analizar el incidente para extraer lecciones aprendidas. Este proceso ayuda a mejorar la postura de seguridad, fortalecer las defensas y prevenir futuros ataques similares.

Para esta etapa es muy importante contar con el reporte completo del incidente de donde se podrán extraer a futuro lecciones aprendidas. Para la descripción de lecciones aprendidas se debe tener en cuenta:

- Medidas o acciones que se podrían haber implementado para impedir el incidente.
- Medidas o acciones que podrían haber impedido la recuperación.
- Cambios o ajustes a implementar para futuros incidentes.
- Herramientas o recursos adicionales que se requieran a futuro para detectar, analizar y mitigar incidentes en el futuro.

Las lecciones aprendidas deben traducirse en un proceso de mejora, para lo cual es necesario que cada vez que se presente un incidente de seguridad y privacidad de la información se diligencie el formato de evaluación, análisis y diagnóstico de incidentes de seguridad y privacidad de la información (SPI-fr-09).

6 DESCRIPCIÓN DE LA ACTIVIDAD

| Nº | Nombre de la actividad | Descripción | Responsable | Registros |
|----|---|---|--|--|
| 1 | Informar el incidente de seguridad y privacidad de la información | Informar de manera inmediata la ocurrencia de un incidente de seguridad y privacidad de la información a través de los canales establecidos. | Funcionario o supervisor de contrato que identifica el incidente de seguridad de la información. | Correo electrónico de informe de incidente de seguridad y privacidad de la información. |
| 2 | Registrar el incidente de seguridad y privacidad de la información | Realizar el registro detallado del incidente reportado en el formato de evaluación, análisis y diagnóstico de incidentes de seguridad y privacidad de la información (SPI-fr-09). | Profesional de Gestión de la Oficina de Seguridad y Privacidad de la Información | Formato de evaluación, análisis y diagnóstico de incidentes de seguridad y privacidad de la información (SPI-fr-09). |
| 3 | Clasificar, valorar y definir la prioridad del incidente de seguridad de la información | Clasificar, valorar y determinar la prioridad del incidente y las medidas que se requieran para su contención, con base en el numeral 5.4.2 ETAPA DE DETECCIÓN Y ANÁLISIS y el numeral 5.4.3 ETAPA DE CONTENCIÓN, ERRADICACIÓN Y RECUPERACIÓN | Profesional de Gestión de la Oficina de Seguridad y Privacidad de la Información / Equipo de respuesta a incidentes de seguridad de la información | Formato de evaluación, análisis y diagnóstico de incidentes de seguridad y privacidad de la información (SPI-fr-09) |
| 4 | Ejecutar las actividades de contención. | Realizar las actividades de contención que se hayan definido en la etapa anterior conforme a lo establecido en el numeral 5.4.3 Etapa de Contención, erradicación y recuperación. NOTA: se debe recopilar y organizar las evidencias producto del análisis y la investigación del incidente de seguridad y privacidad de la información que servirán como | Profesional de gestión de la Oficina de Seguridad y Privacidad de la Información / Equipo de respuesta a incidentes de seguridad de la información | Formato de evaluación, análisis y diagnóstico de incidentes de seguridad y privacidad de la información (SPI-fr-09) Evidencias del incidente de |

| Nº | Nombre de la actividad | Descripción | Responsable | Registros |
|----|---|--|---|---|
| | | soporte del formato de evaluación, análisis y diagnóstico de incidentes de seguridad y privacidad de la información. | | seguridad y privacidad de la información. |
| 5 | Realizar la restauración y recuperación de los activos de información afectados | De acuerdo con la evaluación, detección y análisis del incidente de seguridad y privacidad de la información reportado, se deberán poner en marcha las actividades planteadas para restaurar y recuperar de manera controlada los activos de información afectados. | Profesional de gestión de la Oficina de Seguridad y Privacidad de la Información / Equipo de respuesta a incidentes de seguridad de la información. | Formato de evaluación, análisis y diagnóstico de incidentes de seguridad y privacidad de la información (SPI-fr-09) |
| 6 | Documentar lecciones aprendidas | Se realiza la documentación de las lecciones aprendidas del incidente en el formato de evaluación, análisis y diagnóstico de incidentes de seguridad y privacidad de la información (SPI-fr-09). NOTA: Dependiendo de la criticidad y la valoración del incidente de seguridad y privacidad de la información, se debe informar a las autoridades competentes y entes de control conforme al numeral 5.4.2.4 Directorio de contactos. | Profesional de gestión de la Oficina de Seguridad y Privacidad de la Información / | Formato de evaluación, análisis y diagnóstico de incidentes de seguridad y privacidad de la información (SPI-fr-09) |
| 7 | Comunicar el incidente a titulares de la información | En caso de que el incidente de seguridad y privacidad de la información esté relacionado con violación de datos personales y que el incidente haya propiciado la fuga de datos personales de los cuales es responsable la Entidad, este deberá ser comunicado al titular de la información indicando los datos que pudieron ser filtrados, las acciones que se tomaron y las acciones sugeridas que deberá tomar el titular de la información. Para generar estas comunicaciones se deberá tener en cuenta el procedimiento de comunicaciones oficiales (GD-pr-01) en lo que | Profesional de Gestión Oficina de Seguridad y Privacidad de la Información | Comunicación a titulares de la información. |

| Nº | Nombre de la actividad | Descripción | Responsable | Registros |
|----|------------------------|--|-------------|-----------|
| | | respecta a comunicaciones oficiales de salida. Nota: en caso de requerirse apoyo en el envío de las comunicaciones, se informará a la dirección general para coordinar lo que se requiera. | | |

7 ANEXOS

7.1 Formato de evaluación, análisis y diagnóstico de incidentes de seguridad y privacidad de la información (SPI-fr-09)

8 CONTROL DE CAMBIOS

| No. | Fecha | Descripción del cambio o modificación |
|-----|------------|---|
| 1 | Julio/2025 | Primera emisión, Creación del documento y del formato SPI-fr-09 Formato de evaluación, análisis y diagnóstico de incidentes de seguridad y privacidad de la información, versión 1. |

| | | |
|--|--|--|
| JOHANNA TRINIDAD CAÑÓN LONDOÑO Firmado digitalmente por JOHANNA TRINIDAD CAÑÓN LONDOÑO Fecha: 2025.07.11 08:42:30 -05'00' JOHANNA CAÑÓN LONDOÑO | ANGELA PATRICIA ALVAREZ LEDESMA Firmado digitalmente por ANGELA PATRICIA ALVAREZ LEDESMA ÁNGELA PATRICIA ÁLVAREZ LEDESMA | Firmado digitalmente por RUBEN DARIO OCHOA ARBELAEZ RUBÉN DARIO ÓCHOA ARBELÁEZ |
| Profesional de Gestión Oficina de seguridad y privacidad de la Información | Subdirectora de Planeación, Control y Seguimiento | Director General |
| ELABORÓ | REVISÓ | APROBÓ |



EVALUACION, ANALISIS Y DIAGNOSTICO DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN

Código: SPI-fr-09
Versión: 1
Vigencia: Jul. 25

| | | | |
|-----------------------|--|-------------------------|--|
| Fecha reporte | | Nombre de quien reporta | |
| Entidad / Contratista | | Correo electrónico | |
| Dependencia / Área | | Teléfono | |

| | | | |
|-----------------------------------|--|----------------------------------|--|
| Fecha de ocurrencia del incidente | | Hora de ocurrencia del incidente | |
| Fecha de detección del incidente | | Hora de detección del incidente | |

| CLASIFICACIÓN DEL INCIDENTE | | |
|-----------------------------|---|-------------|
| Clasificación | Tipo de incidente | Descripción |
| Incidentes_internos | Cambios o modificaciones en registros de bases de datos sin previa autorización | |
| | | |
| | | |

| VALORACION DE PROCESOS AFECTADOS | | |
|---|---------|-------------|
| Impacto Actual | | |
| Valoración | Impacto | Descripción |
| Aunque haya algún proceso afectado los efectos no se notan en ninguna área de la Entidad. | Ninguno | |
| Impacto Futuro | | |
| Valoración | Impacto | Descripción |
| Afecta varios procesos misionales o áreas de la Entidad que afectan el cumplimiento de la misionalidad de la Entidad. | Crítico | |

| CRITICIDAD DE SISTEMAS AFECTADOS | | |
|--|---------|-------------|
| Criticidad | Impacto | Descripción |
| Afecta los sistemas de información misionales, infraestructura tecnológica transversal a todos los sistemas de información y/o la mayoría de las estaciones de trabajo de los funcionarios de la Entidad | Crítico | |

| PRIORIZACIÓN | | |
|--------------------|------------|--------------------|
| Nivel de prioridad | Valoración | Tiempo de repuesta |
| Crítico | 7,5 | |



**EVALUACION, ANALISIS Y DIAGNOSTICO DE
INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN**

Código: SPI-fr-09
Versión: 1
Vigencia: Jul. 25

DIAGNOSTICO Y ANÁLISIS DEL INCIDENTE REPORTADO

| |
|--|
| |
| |
| |
| |
| |
| |

ESTRATEGIA DE CONTENCIÓN, ERRADICACIÓN Y RECUPERACIÓN

| |
|--|
| |
| |
| |
| |
| |
| |

LECCIONES APRENDIDAS

| |
|--|
| |
| |
| |
| |
| |
| |