# Manual de gestión de incidentes de seguridad de la información
# 2025

## Se adopta mediante resolución No. 33
## 28 de enero de 2025

"Los suscritos hemos revisado el documento y lo encontramos ajustado a las disposiciones técnicas o legales, en el marco de nuestras competencias, por tanto, bajo nuestra responsabilidad lo presentamos para firma"

| | |
|---|---|
| **Elaboró: Jefferson Silva Losada** | **Revisó: Rafael Augusto Sierra Rojas** |
| **Cargo:** Profesional de Sistemas | **Cargo:** Jefe Oficina Asesora de Planeación y Proyectos (E) |
| **Firma:** | **Firma:** |
| Aprobado mediante Resolución Administrativa N° 0003 de 2025 | |

## TABLA DE CONTENIDO



"Los suscritos hemos revisado el documento y lo encontramos ajustado a las disposiciones técnicas o legales, en el marco de nuestras competencias, por tanto, bajo nuestra responsabilidad lo presentamos para firma"

| Elaboró: Jefferson Silva Losada | Revisó: Rafael Augusto Sierra Rojas |
|---|---|
| Cargo: Profesional de Sistemas | Cargo: Jefe Oficina Asesora de Planeación y Proyectos (E) |
| Firma: | Firma: |

Aprobado mediante Resolución Administrativa N° 0003 de 2025

# 1. INTRODUCCION

La Empresa de Servicios Públicos Domiciliarios de Pitalito EMPITALITO ESP, con el ánimo de salvaguardar los activos de información, considerados como elementos fundamentales para el desarrollo de los procesos de la Entidad, ha implementado políticas de seguridad de la información que buscan minimizar el riesgo que se realicen actos que afecten negativamente el desempeño y la imagen de la Entidad, por lo cual, en concordancia desarrolla un modelo de gestión de incidentes de seguridad de la información.

Como referente para el desarrollo del presente manual de Gestión de incidentes, se tomó la Guía para la Gestión y Clasificación de Incidentes de Seguridad de la Información, que dispuso El Ministerio de las TIC, en el marco de la implementación del Modelo de Seguridad y Privacidad de la Información, la cual está basada en los lineamientos recomendados en Norma la ISO IEC 27001 – 2013 Numeral 16 de la misma, para la gestión de incidentes.

Implementar un plan de gestión de incidentes para Empresa de Servicios Públicos Domilciarios de Pitalito EMPITALITO ESP tendrá como beneficio optimizar los procesos que pueden incidir de manera significativa en la continuidad del negocio y por ende en la garantía del cumplimiento de la misión y los propósitos institucionales.

# 2. OBJETIVO

## 2.1. Objetivo General

Establecer acciones y lineamientos, que permita a la Empresa de Servicios Públicos Domiciliarios de Pitalito EMPITALITO EP, no solo estar en capacidad de responder en forma adecuada ante la ocurrencia incidentes de seguridad que afecten real o potencialmente sus servicios, sino también establecer la forma como pueden ser detectados y evaluados junto con la gestión de las vulnerabilidades, asegurando que los sistemas, redes, y aplicaciones sean lo suficientemente seguros.

Este manual involucra la forma de preparar, detectar, contener, erradicar, recuperar y hacer seguimiento de los incidentes de seguridad de la información que lleguen afectar a la Entidad, además de cumplir las especificaciones y prácticas de las Políticas de Seguridad de la Información.

### 2.2. Objetivos Específicos

- Definir roles y responsabilidades dentro de la Entidad como eje puntual para evaluar los riesgos y permita mantener la operación, la continuidad y la disponibilidad del servicio.
- Gestionar los eventos de seguridad de la información para detectar y tratar con eficiencia, en particular identificar si es necesario o no clasificarlos como incidentes de seguridad de la información.
- Permitir identificar los incidentes de seguridad de la información para ser evaluados y dar respuesta de la manera más eficiente y adecuada.
- Minimizar los impactos adversos de los incidentes en la organización y sus operaciones de negocios mediante las salvaguardas adecuadas como parte de la respuesta a tal incidente.
- Consolidar las lecciones aprendidas que dejan los incidentes de seguridad de la información y su gestión para aprender rápidamente. Esto tiene como objeto incrementar las oportunidades de prevenir la ocurrencia de futuros incidentes, mejorar la implementación y el uso de las salvaguardas y mejorar el esquema global de la gestión de incidentes de seguridad de la información.
- Definir los mecanismos que permitan cuantificar y monitorear los tipos, volúmenes y costos de los incidentes de seguridad de la información, a través de una base de conocimiento y registro de incidentes y a través de los indicadores del sistema de gestión de seguridad de la información.
- Definir los procedimientos formales de reporte y escalada de los incidentes de seguridad.
- Establecer variables de posible riesgo, en efecto, es la posible valoración de aspectos sensibles en los sistemas de información

## 3. ALCANCE

La atención y gestión de un incidente de seguridad de la información cubre todos los Activos de Información de la empresa de servicios públicos domiciliarios de Pitalito EMPITALITO ESP, bien sea que se encuentren

clasificados, o aquellos que no posean ningún tipo de clasificación, y a todos y cada uno de los colaboradores de planta que tienen algún acceso a los activos de la información, incluyendo a terceros, contratistas, o servicios en outsourcing, dentro de los cuales los activos de información de la entidad se encuentren involucrados.

El presente documento contiene los componentes generales de la gestión de incidentes, sus principales acciones las cuales son aplicables indistintamente de la plataforma operacional, o el tipo de información o activo de información sobre el cual se presente y/o exista un indicio de incidente de seguridad. Comienza con la preparación antes de la presencia de un incidente de seguridad de la información y finaliza con las lecciones aprendidas y seguimiento respectivo a los diferentes incidentes de seguridad de la información que se presentan en la organización.

## 4. DEFINICIONES

Dentro de la atención de incidentes de seguridad de la información es importante clarificar algunos conceptos con los cuales se define el procedimiento de gestión de incidentes. Entre ellos se encuentran:

- ✓ **Evento de Seguridad de la Información:**

Un evento de seguridad de la información es la ocurrencia identificada de un estado del sistema, servicio o red que indica una posible violación a la política de seguridad de la información, una falla de los controles, o una situación desconocida que puede ser relevante para la seguridad de la información. Se pueden presentar eventos de seguridad como intentos de acceso no autorizados, uso indebido de la información o de los recursos informáticos, impedimento normal de las redes, entre otros.

- ✓ **Incidente de Seguridad de la Información - ISI**

Se entiende por incidente de seguridad de la información, todo evento o grupo de eventos adversos o no esperados en materia de seguridad de la información que tiene una probabilidad importante de comprometer las operaciones del negocio y amenazar la seguridad de la información.

Para EMPITALITO ESP y dentro del espectro tan amplio que involucra la definición los incidentes se contemplan dentro de los siguientes tipos:

**Acceso No Autorizado:** El acceso no autorizado a la información o los recursos tecnológicos involucra todas aquellas actividades en las que sin autorización específica o que no se encuentre dentro de las funciones del usuario, se pueda utilizar la información o cualquier activo de información, bien sea de manera intencional o no, o en su defecto se explote una debilidad sobre la información y/o activo de información, con la cual se realicen operaciones no autorizadas, inesperadas o indebidas. Hacen parte de esta categoría:

- Accesos no autorizados exitosos, sin o con perjuicios visibles a los componentes tecnológicos.
- Robo de información.
- Borrado de información.
- Alteración de la información.
- Intentos recurrentes y no recurrentes de acceso no autorizado.
- Abuso y/o mal uso de los servicios informáticos internos o externos que requieren autenticación.

**Código Malicioso:** Se entiende por código malicioso todos aquellos programas como virus, troyanos, gusanos, y algún otro tipo de programa o scripts que tiene como propósito afectar un sistema informático o en si misma a la información, de tal forma que pueda corromper, alterar, modificar y/o destruir la información. Hacen parte:

- Virus informáticos.
- Troyanos.
- Gusanos informáticos.
- Keyloggers, Screenloggers, Mouseloggers.
- Spyware, Rootkits.

**Denegación de Servicio:** Esta categoría incluye los eventos que ocasionan pérdida de un servicio, en nuestro caso, se considera esta clasificación cuando los usuarios autorizados a la información, o activos de información de la organización no pueden hacer uso de dichos recursos y la falla no es atribuible a problemas de operación normal. Dentro de este marco se contemplan las denegaciones de servicios a:

- Servicio de Correo electrónico.
- Interrupción de la red de transmisión de datos.
- Interrupción de Servicios WEB y/o Portales WEB.
- Interrupción de los Sistemas de Información.

**Mal Uso o abuso de los Recursos Tecnológicos:** Esta categoría agrupa los eventos que atentan contra los recursos tecnológicos por el mal uso. Comprende:

- Utilización del recurso correo electrónico para temas como: Spam, Phishing, Hoax, Cadenas de correo.
- Utilización del recurso como el correo electrónico, e Internet para temas como: Contenido pornográfico, divulgación de información reservada o propia de la empresa sin la debida autorización.
- Utilización de la red para temas como: Realización de pruebas de intrusión, Scan, o vulnerabilidades, sin autorización.
- Robo, fuga, espionaje o perdida de información para temas como: Medios externos de almacenamiento, transporte de material impreso.
- Violación de las políticas, normas y procedimientos de seguridad de la información.
- Uso inadecuado de las Redes Sociales.

**Análisis de Vulnerabilidades:** Esta categoría agrupa todas las posibles fallas de los sistemas que puedan afectar a los sistemas y dentro de las cuales las causas de dichas vulnerabilidades se deben a fallas de los productos, fallas de las configuraciones de los servicios, fallas de diseño de la infraestructura tecnológica, para ello la Oficina de Sistemas de la entidad realiza pruebas de vulnerabilidad periódicamente sobre la infraestructura tecnológica de la organización, identificando este tipo de vulnerabilidades.

✓ **Gestión de Incidentes de Seguridad de la Información (GISI)**

Para EMPITALITO ESP, la gestión de incidentes de seguridad de la información consiste en mantener un programa de atención oportuno, eficaz y eficiente de incidentes de seguridad sobre la información; de manera que se obtenga suficiente y objetiva evidencia del hecho, con el propósito de prevenir, detectar, y arreglar las fallas en la seguridad de la información.

La gestión de incidentes involucra el siguiente conjunto de actividades frente a un incidente:

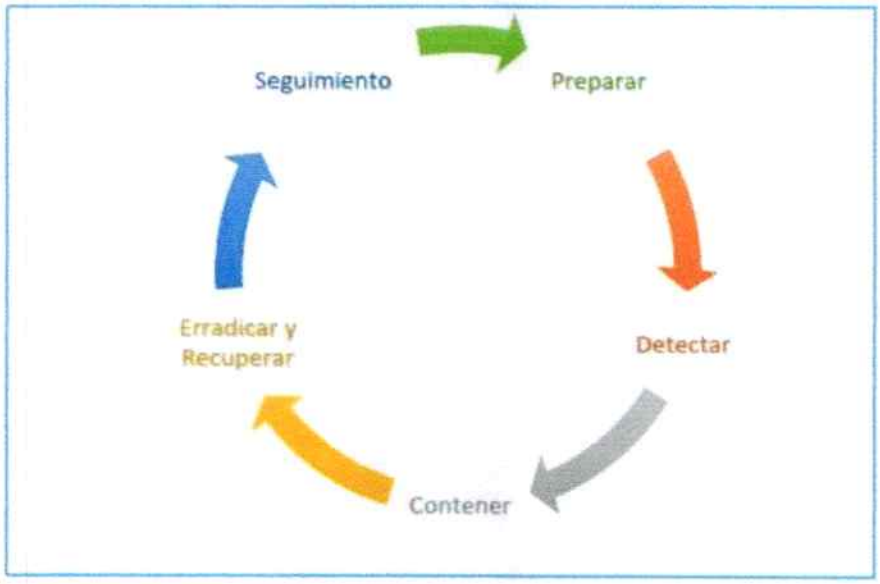


Figura 1. Proceso de Gestión de Incidentes de Seguridad de la Información.

Cabe aclarar que la gestión de incidentes de seguridad de la información no es una labor de ejecución unitaria de la Oficina de Tecnologías de la Información y Comunicaciones, sino un trabajo en donde debe involucrarse la Oficina de Control Interno y/o Niveles Gerenciales que correspondan y los dueños de la Información o activos de información, pues deben ser ellos quien en algún momento realicen las operaciones de configuraciones, cambios y suministro de información al momento de tratar un incidente de seguridad de la información.

## 5. ROLES Y RESPONSABILIDADES

Se crea el equipo de Respuesta a Incidencias de Seguridad Informática **CSIRT** (**Computer Security Incident Response Team**), enfocado principalmente en atender los incidentes de seguridad de la información que se presentan sobre los activos soportados por la plataforma tecnológica de la entidad, la plataforma para analizar nuevas vulnerabilidades y brechas de seguridad.

El equipo **CSIRT** de respuesta a incidentes no es normalmente responsable de la prevención de incidentes, es muy importante que se considere como un componente fundamental de los programas de respuesta. El equipo de respuesta a incidentes debe actuar como una herramienta de experiencia en el establecimiento de recomendaciones para el aseguramiento de los sistemas de información y la plataforma que los soporta.

- Definir los procedimientos para la atención de incidentes
- Definir la clasificación de incidentes
- Monitorear y verificar los elementos de control con el fin de detectar un posible incidente de seguridad de la información
- Detectar Incidentes de Seguridad: Monitorear y verificar los elementos de control con el fin de detectar un posible incidente de seguridad de la información.
- Atender Incidentes de Seguridad: Recibe y resuelve los incidentes de seguridad de acuerdo con los procedimientos establecidos.
- Recolectar y Analizar Evidencia Digital: Toma, preservación, documentación y análisis de evidencia cuando sea requerida.
- Realizar 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).
- Realizar Auditoria y trazabilidad de Seguridad Informática: El equipo debe realizar verificaciones periódicas del estado de la plataforma para analizar nuevas vulnerabilidades y brechas de seguridad.
- Certificar productos: El equipo verifica la implementación de las nuevas aplicaciones en producción para que se ajusten a los requerimientos de seguridad informática definidos por el equipo.
- Configurar y Administrar Dispositivos de Seguridad Informática: Se encargarán de la administración adecuada de los elementos de seguridad informática.
- Clasificar y priorizar servicios expuestos: Identificación de servicios sensibles y aplicaciones expuestas para la prevención o remediación de ataques.
- Investigar o Desarrollar nuevas herramientas: el equipo debe 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.

**Conformación del equipo CSIRT:**

1. Gerente y/o representante legal de la entidad
2. Jefe oficina de planeación y proyectos
3. Profesional de Sistemas
4. Profesional de planeamiento y control

5. Profesional de calidad

Definiciones:

**Usuario Sensibilizado:** Servidores Públicos, proveedores, usuarios externos, contratistas o terceros con acceso a la infraestructura de la entidad, quien debe estar informado y concientizado sobre las políticas y procedimientos de seguridad de la información y en particular la guía de atención de incidentes, estos usuarios serán muchas veces quienes reporten los problemas y deberán tener en cuenta lo siguiente:

**Agente Primer Punto de Contacto:** Es el encargado de recibir las solicitudes por parte de los usuarios sobre posibles incidentes, también debe registrarlos en la base de conocimiento y debe ser el encargado de escalarlos a la persona encargada de la atención según sea el caso.

Este Agente debe contar adicionalmente con capacitación básica en Seguridad de la Información y debe conocer perfectamente la clasificación de Incidentes y los procesos de escalamiento de Incidentes.
Adicionalmente debe contar con una capacitación básica, específicamente en recolección y manejo de evidencia.

**Administrador del Sistema:** Es la persona encargada para configurar y mantener un activo informático. También debe ser notificado por el agente de primer punto de contacto sobre un incidente de seguridad con el fin de analizar, identificar, contener y erradicar un incidente de seguridad.

Debe documentar y notificar al agente de primer punto de contacto sobre la actuación o posible solución del mismo. Se recomienda que los administradores cuenten con capacitación en Seguridad de la Información y debe conocer perfectamente la clasificación de Incidentes y los procesos de escalamiento de Incidentes.

**Administrador de los sistemas de Seguridad:** Persona encargada de configurar y mantener un activo informático relacionado con la seguridad de la plataforma ej. Firewall, Sistemas de Prevención de Intrusos, Routers, Sistemas de Gestión y Monitoreo.

También debe ser notificado por el agente de primer contacto sobre un incidente de seguridad con el fin de analizar, identificar, contener y erradicar un incidente de seguridad. Este debe documentar y notificar al agente de primer contacto sobre la actuación frente al incidente y la solución del mismo. Se recomienda que

el administrador de esta tecnología tenga conocimientos en Seguridad de la Información (con un componente tecnológico fuerte en Redes y erradicación de vulnerabilidades, Ethical Hacking y técnicas forenses) y debe conocer perfectamente la clasificación de Incidentes de la entidad.

**Analista del Incidente:** debe estar disponible en caso de que un incidente de impacto bajo o medio, en caso de impacto alto que requiera una investigación completa (o uno que amerite acciones disciplinarias o legales o investigación profunda) debe trasladarlo a los Entes respectivos (Fiscalía, Contraloría).
Debe determinar:

- Qué sucedió.
- Dónde sucedió.
- Cuándo Sucedió.
- Quién fue el Responsable.
- Cómo sucedió.

Este actor debe ser un apoyo para los demás actores en caso de dudas sobre los procedimientos y debe ejercer un liderazgo técnico en el proceso de atención de Incidentes de seguridad de la información.

**Líder de Grupo de Atención de incidentes:** Responde a las consultas sobre los incidentes de seguridad que impacten de forma inmediata, y es el encargado de revisar y evaluar los indicadores de gestión correspondientes a la atención de incidentes de seguridad para poder ser presentados a los directivos.

El Líder Grupo de Atención de Incidentes estará en la capacidad de convocar la participación de otros funcionarios de la organización cuando el incidente lo amerita (Oficina de Comunicaciones, Talento Humano, Oficina Jurídica, Representante de las Directivas para el SGSI).

También debe estar al tanto del cumplimiento de los perfiles mencionados y de revisar el cumplimiento de los procedimientos y mejores prácticas, así como también de los indicadores de gestión, y en capacidad de disparar si lo amerita planes de contingencia y/o continuidad.
Finalmente, el Líder del Grupo de Atención de Incidentes será el responsable del modelo de Gestión de incidentes y debe estar en la capacidad de revisar todos los incidentes de seguridad y los aspectos contractuales que manejan herramientas de seguridad.

## 6. METODOLOGIA

La Empresa de Servicio Públicos Domiciliarios de Pitalito EMPITALITO ESP cuenta con un proceso de cinco fases para la Gestión de Incidentes de Seguridad de la Información, los cuales permiten gestionar un incidente desde el momento antes de la ocurrencia del incidente hasta la forma en cómo se debe aprender y obtener la experiencia y bases de conocimiento para eventos futuros:

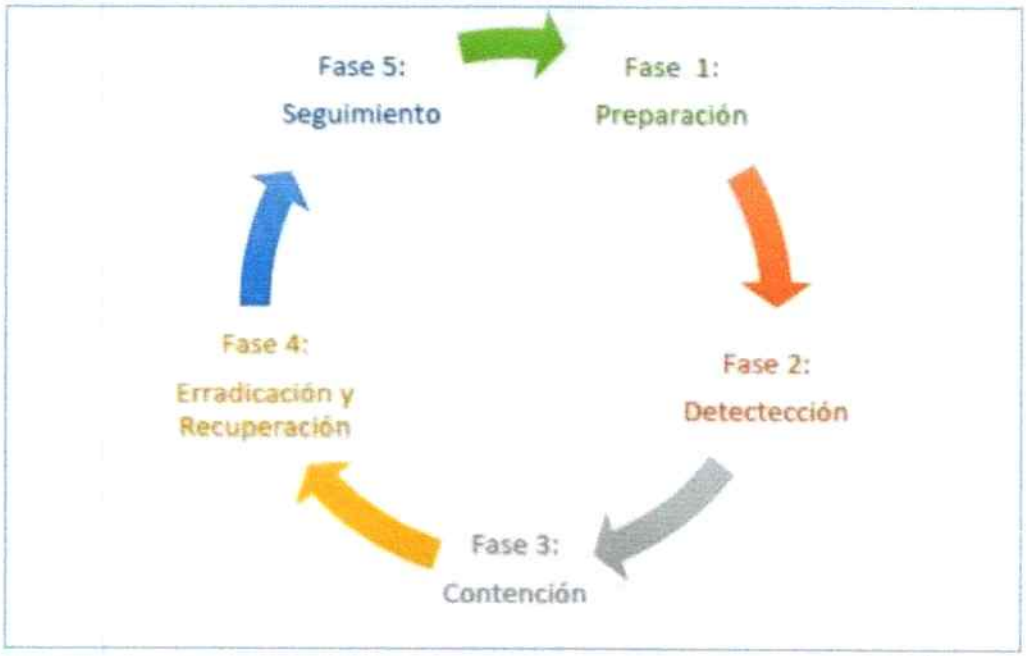


Figura 2. Fases Gestión de Incidentes de Seguridad de la Información

### 6.1. FASE 1: PREPARACIÓN

La fase de preparación, comprende las medidas que se encuentran implementadas y dispuestas para anticiparse a la ocurrencia de los incidentes de seguridad de la información, con las cuales se repelen los ataques que pueden llegar a presentarse, adicional a ello se han aplicado las mejores prácticas para el manejo de los recursos tecnológicos y de la información, y para ello se deben establecer los procedimientos necesarios para preparar la entidad en caso de presentarse algún evento o incidente de seguridad.

A continuación, se relacionan los diferentes tipos de incidentes que se presentan en la plataforma tecnológica y las herramientas con las que cuenta la entidad para que estos puedan ser detectados:

| TIPOS DE INCIDENTES DE PLATAFORMA TECNOLÓGICA | HERRAMIENTAS | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| | FIREWALL PERIMETRAL | | | | PROXY | ANTIVIRUS / ANTIMALWARE | CONTROL DE ACCESO | NESSUS |
| | IDS/IPS | ANTIVIRUS | ANTIMALWARE | FIREWALL | | | | |
| Acceso No Autorizado | X | | | X | X | | | |
| Código Malicioso | | X | X | | X | X | | |
| Denegación de Servicios | X | | | X | | | | |
| Mal Uso o Abuso de los Recursos Tecnológicos | | | | | X | | X | |
| Análisis de Vulnerabilidades | | | | | | | | X |

Tabla 1. Incidentes de Seguridad de la Información Vs. Herramientas de Detección.

En esta fase se definen los lineamientos básicos con los cuales se afrontan los incidentes de seguridad de la información que se presentan dentro de la plataforma tecnológica de la entidad.

De la misma manera, se ha establecido como línea base de defensa la formulación de la atención de dichos incidentes a través de este manual el cual se concentra en las herramientas con las que se cuenta para identificar dichos incidentes de seguridad de la información.

### 6.1.1. Firewall Perimetral

La Entidad cuenta con un Firewall Perimetral que ofrece una combinación ideal de tecnologías de seguridad, implementación y administración de características. Este dispositivo ofrece un conjunto completo de características de seguridad perimetral incluyendo firewall, prevención de intrusiones, antivirus, Anti-Spam y filtrado Web, así como VPN's seguras de sitio a sitio y conectividad de acceso remoto.

### 6.1.2. Proxy

El proxy es un servidor que facilita el acceso a Internet desde la red interna de la entidad. El proxy integrado con el directorio activo permite autorizar usuarios para acceder a la web, al igual que permite el acceso de direcciones IP específicas. Los registros permiten generar reportes que permiten detectar el uso indebido de recursos.

### 6.1.3. Antivirus / Antimalware

El Antivirus/Anti-Malware gestiona los incidentes de seguridad basado en una infraestructura centralizada, la cual proporciona protección en estaciones de trabajo y los servidores. Esta infraestructura integra:

- Antivirus. Además de la detección basada en firmas, proporciona la detección heurística que emula una máquina virtual dentro del equipo, comprobando todos los archivos y códigos en busca de comportamiento malicioso. Esta técnica produce menos falsos positivos y tasas de detección significativamente más altas para amenazas desconocidas y de "día cero".

- Antispyware. La Herramienta detecta y previene el spyware y adware conocidos a través de diversos métodos de filtrado diferentes para prevenir las infecciones por spyware que puedan causar fuga de información.

- Troyanos y rootkits. Pueden ser detectados por el motor de análisis de la Herramienta de Antivirus/Anti-Malware

### 6.1.4. Control de Acceso

El control de acceso a la infraestructura tecnológica por parte de todos los colaboradores de planta y contratistas de la Secretaría es realizado por la Oficina de TIC de la entidad de acuerdo con las necesidades de los usuarios.

### 6.1.5. Herramienta de Identificación de Vulnerabilidades

Las herramientas utilizadas para el análisis de vulnerabilidades se ejecutan periódicamente y sus resultados se presentan en reunión de seguimiento de pares de seguridad informática con una periodicidad de cada seis meses. Esta actividad ayuda a la identificación de los componentes críticos, débiles o susceptibles a daños y/o interrupciones; así como a la generación de medidas de emergencia y/o mitigación para que éstas sean implementarse ante las amenazas previamente identificadas.

### 6.2. FASE 2: DETECCION

La notificación o reporte de los incidentes permite responder a los mismos en forma sistemática, minimizar su ocurrencia, facilitar una recuperación rápida y eficiente de las actividades minimizando la pérdida de información y la interrupción de los servicios, llevar a cabo un adecuado proceso de tratamiento de incidentes, y manejar correctamente los aspectos legales que pudieran surgir durante este proceso.

Las principales fuentes de detección de incidentes son:

- Los funcionarios de la Secretaría Jurídica Distrital.
- Monitoreo de la Infraestructura.
- Avisos de terceros.

Los usuarios que detecten los incidentes de seguridad deben abstenerse de ejecutar acciones propias y deben reportarla de inmediato.

**Reporte de usuarios:** Los usuarios de los diferentes servicios informáticos, sistemas de información y aplicaciones de la Entidad deben reportar de manera inmediata a la detección de incidentes, a la oficina TIC de la entidad o al profesional Universitario de Sistemas.

El reporte puede ser vía telefónica, correo electrónico o personal, en todo caso se debe recepcionar y diligenciar la información en la base de datos establecida. Se sugiere que en lo posible se presenten evidencias tales como pantallazos, e imágenes del incidente.

Los usuarios del sistema que detecten los incidentes de seguridad deben abstenerse de ejecutar acciones propias y deben reportarla de inmediato al contacto indicado.

**Monitoreo de infraestructura:** La oficina TIC debe realizar revisión continua del funcionamiento de los activos de información, para prevenir problemas, eventos no deseados e incidentes de seguridad de la información.

Es necesario contar con una serie de elementos indicadores que alerten que posiblemente ha ocurrido un incidente:

- Alertas en Sistemas de Seguridad
- Caídas de servidores

- Reportes de usuarios
- Informe Software antivirus
- Funcionamiento de los sistemas fuera de lo normal
- Tráfico de red excepcionalmente intenso
- Falta de espacio en el disco, o reducción considerable del espacio libre
- Utilización excepcionalmente alta de la CPU
- Creación de nuevas cuentas de usuario
- Uso o intento de uso de cuentas de administrador
- Cuentas bloqueadas
- Gran número de correos electrónicos rebotados con contenido sospechoso

Los siguientes elementos pueden alertar sobre la futura ocurrencia de un incidente, de tal forma que se preparen procedimientos para minimizar el impacto:

- Logs de servidores
- Logs de aplicaciones
- Logs de herramientas de seguridad
- Otras herramientas que permitan la identificación de un incidente de seguridad.

La fase de **detección** involucra la identificación del incidente de seguridad de la información y donde se lleva a cabo las actividades de:

- Validar si de acuerdo con los lineamientos definidos anteriormente el incidente se considera de seguridad de la información.
- Clasificar el incidente.
- Reportar el incidente ante las personas, áreas y/o autoridades que correspondan.

Esta fase involucra la atención del incidente, se encuentra definida en una escala de tiempo (Horas y días), encontrándose estrechamente relacionada de acuerdo con su clasificación, dicha escala se encuentra definida como el tiempo máximo que puede tardarse en atender o poner en marcha la gestión de atención de incidentes de seguridad de la información, pero no necesariamente en dar su respuesta.

EMPITALITO ESP, debe aplicar las siguientes actividades a fin de garantizar la detección de incidentes de seguridad:

| No | DESCRIPCION ACTIVIDAD |
|---|---|
| 1 | Verificar la utilidad de Administración (Visor de Eventos) del sistema operativo de cada equipo Servidor que hacen parte del Datacenter. |
| 2 | Activar el módulo de auditoría del Gestor Base de Datos Oracle |
| 3 | Realizar acciones correctivas sobre los sucesos registrados |
| 4 | Verificar el registro de todas las acciones de autenticación con éxito y fallidos estén guardadas en archivo tipo log. |
| 5 | Verificar la transaccionalidad de datos de entrada exitosos y fallidos sean registradas en el log |
| 6 | Verificar la operatividad y funcionabilidad acciones plan de contingencia (Recreación copias de seguridad) |
| 7 | Verificar la operatividad Plan de Manejo de Riesgo |
| 8 | Verificar la eficacia de los planes de mejoramiento |

Una vez se detecta el incidente, ya sea por parte del usuario final o del administrador del sistema, se genera el reporte respectivo.

### 6.2.1. Análisis

Las actividades de análisis del incidente involucran otra serie de componentes, es recomendable tener en cuenta los siguientes:

- Tener conocimientos de las características normales a nivel de red y de los sistemas.
- Los administradores de TI deben tener conocimiento total sobre los comportamientos de la Infraestructura que están Administrando.
- Toda información que permita realizar análisis al incidente debe estar centralizada (Logs de servidores, redes, aplicaciones).
- Es importante efectuar correlación de eventos, ya que por medio de este proceso se pueden descubrir patrones de comportamiento anormal y poder identificar de manera más fácil la causa del incidente.
- Para un correcto análisis de un incidente debe existir una única fuente de tiempo (Sincronización de Relojes) ya que esto facilita la correlación de eventos y el análisis de información.
- Se debe mantener y usar una base de conocimiento con información relacionada sobre nuevas vulnerabilidades, información de los servicios habilitados, y experiencias con incidentes anteriores.
- Crear matrices de diagnóstico e información para los administradores menos experimentados.

- Determinar el alcance, las posibles consecuencias e impactos del incidente de seguridad en cuanto al desarrollo de los procesos, la confidencialidad, integridad y disponibilidad de la información, daños físicos a la infraestructura tecnológica y la percepción pública.
- Determinar la naturaleza del incidente en lo que respecta a la intención del atacante y a la amenaza existente.
- Determinar la causa raíz del incidente y establecer los controles y procedimientos para prevenir o mitigar su repetición en el futuro.
- Identificar la fuente del ataque y el atacante, y elaborar un perfil de este.

### 6.2.2. Evaluación

Para realizar la evaluación de un incidente de seguridad se debe tener en cuenta los niveles de impacto con base en los insumos entregados por el análisis de riesgos y la clasificación de activos de información de la entidad.

La severidad del incidente puede ser:

**Alto Impacto:** El incidente de seguridad afecta a activos de información considerados de impacto catastrófico y mayor que influyen directamente a los objetivos misionales de la Entidad. Se incluyen en esta categoría aquellos incidentes que afecten la reputación y el buen nombre o involucren aspectos legales. Estos incidentes deben tener respuesta inmediata.
**Medio Impacto:** El incidente de seguridad afecta a activos de información considerados de impacto moderado que influyen directamente a los objetivos de un proceso determinado.

**Bajo Impacto:** El incidente de seguridad afecta a activos de información considerados de impacto menor e insignificante, que no influyen en ningún objetivo. Estos incidentes deben ser monitoreados con el fin de evitar un cambio en el impacto.

#### 6.2.2.1. Priorización de los incidentes de seguridad y tiempos de respuesta.

Una vez se tiene conocimiento de la incidencia se procede a priorizarlas de acuerdo al impacto y posibles consecuencias que atenten contra la continuidad de los procesos y cumplimiento de los objetivos de la Entidad.

El equipo de Respuesta a Incidencias de Seguridad Informática, una vez tiene conocimiento del incidente, procede a realizar la verificación, análisis y evaluación de los mismos y establece niveles de prioridad de acuerdo al tipo de incidente y complejidad en las acciones de respuesta, Ver Plan de respuesta.

**Nivel de prioridad:** Depende del valor o importancia dentro de la empresa y del proceso que soporta el o los sistemas afectados.

| Nivel Criticidad | Valor | Definición |
|---|---|---|
| Inferior | 0,10 | Sistemas no críticos, como estaciones de trabajo de usuarios con funciones no críticas |
| Bajo | 0,25 | Sistemas que apoyan a una sola Dependencia o proceso de una Entidad |
| Medio | 0,50 | Sistemas que apoyan más de una dependencia o proceso de la Entidad |
| Alto | 0,75 | Sistemas pertenecientes al área de tecnología y estaciones de trabajo de usuarios con funciones críticas |
| Superior | 1,00 | Sistemas Críticos. La operación es crítica para la Entidad cuando al no contar con ésta, la función del proceso no puede realizarse |

Tabla Niveles de criticidad del impacto

**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.

| Nivel Impacto | Valor | Definición |
|---|---|---|
| Inferior | 0,10 | Impacto leve en uno de los componentes de cualquier sistema de información o estación de trabajo |
| Bajo | 0,25 | Impacto moderado en uno de los componentes de cualquier sistema de información o estación de trabajo |
| Medio | 0,50 | Impacto alto en uno de los componentes de cualquier sistema de información o estación de trabajo |

| | | |
|---|---|---|
| Alto | 0,75 | Impacto moderado en uno o más componentes de más de un sistema de información |
| Superior | 1,00 | Impacto alto en uno o más componentes de un sistemas de información |

Tabla Niveles de Impacto Actual y Futuro

**La prioridad se obtiene mediante la siguiente fórmula**
**Nivel de Prioridad= (Impacto actual*2,5) + (Impacto futuro *2,5) + (criticidad del sistema *5)**

Y el resultado se compara con la siguiente tabla para determinar el nivel de prioridad de atención:

| Nivel de Prioridad | Valor |
|---|---|
| Inferior | 00,00 - 02,49 |
| Bajo | 02,50 - 03,74 |
| Medio | 03,75 - 04,99 |
| Alto | 05,00 - 07, 49 |
| Superior | 07,50 - 10, 00 |

Tabla: Niveles de prioridad del incidente

**Tiempos de respuesta**

El tiempo de respuesta establecido en la siguiente tabla es aproximado al tiempo máximo para que el incidente sea atendido dependiendo del nivel de prioridad, y no corresponde al tiempo de solución del incidente, dado que la complejidad de la atención varía dependiendo del tipo de incidente y del activo de información impactado.

| Nivel de Prioridad | Tiempo de Respuesta |
|---|---|
| Inferior | 3 horas |
| Bajo | 1 hora |
| Medio | 30 minutos |

| | |
|---|---|
| Alto | 15 minutos |
| Superior | 10 minutos |

Tabla: tiempos máximos de respuesta

| Qué hacer | Cómo hacerlo | Quien lo hace | Cuando lo hace |
|---|---|---|---|
| Notificación o reporte del incidente | vía telefónica o personal.<br>Correo electrónico: tic@empitalito.gov.co / sistemasempitalito@gmail.com<br>Teléfono: 3118790495 | Funcionario, tercero o contratista, o Administrador de TI | Inmediatamente tiene conocimiento del incidente |
| Registro del incidente o evento | Toma los datos necesarios y realiza el registro en el formato correspondiente si se puede solucionar de inmediato, se documenta la solución aplicada entre otros. | Primer punto de contacto (Profesional de sistemas) | En el momento del reporte del incidente o evento |
| Identificar el tipo de incidente | Identificar el tipo de incidente, de acuerdo a la tabla de clasificación de incidentes, Verificar las evidencias, realizar pruebas para determinar la veracidad de la incidencia, las causas y el impacto | Primer punto de contacto (Profesional de sistemas) | Inmediatamente al reporte del incidente y según la tabla de tiempos de respuesta |
| Escalar el incidente | Informar a la persona encargada de atender el incidente para que tome las decisiones correspondientes. | Segundo punto de contacto (jefe oficina de planeación y proyectos) | Inmediatamente al reporte del incidente según la tabla de tiempos de respuesta |
| Aplicar la estrategia de Contención | Proceder a realizar las acciones contención tabla de clasificación y estrategias de respuesta | Profesionales y técnicos del Grupo de Infraestructura Tecnológica, Administrador de SI | Inmediato al reporte del incidente |

| | | | |
|---|---|---|---|
| Recolectar la evidencia | Para recolectar la evidencia tener en cuenta lo siguientes criterios<br>- Información basada en la red: Log's de IDSs, logs de monitoreo, información recolectada mediante Sniffers, logs de routers, logs de firewalls, información de servidores de autenticación.<br><br>- Información Basada en el Equipo: Live data collection: Fecha y hora del sistema, aplicaciones corriendo en el sistema, conexiones de red establecidas, puertos abiertos, aplicaciones escuchando en dichos puertos, estado de la tarjeta de red.<br><br>Otra información: Testimonio de funcionario o contratista que reporta el evento o incidente | Profesionales y técnicos del del Grupo de Infraestructura Tecnológica, Administrador de SI, responsable de la Seguridad | Desde el conocimiento del incidente |
| Manejo de la Evidencia | La información debe ser almacenada y custodiada, debe cumplir con un control de seguridad que garantice la confidencialidad, integridad y disponibilidad de las evidencias retenidas. Esta información incluye:<br><br>-Cantidad de incidentes presentados y tratados.<br>- Tiempo asignado a los incidentes.<br>- Daños ocasionados.<br>- Vulnerabilidades explotadas.<br>- Cantidad de activos de información involucrados.<br>- Frecuencias de ataques. | Responsable de seguridad | Al cierre del proceso |

| | | | |
|---|---|---|---|
| Identificar las fuentes de ataque | Se debe tener identificadas las posibles fuentes de ataque:<br>- Empleados Descontentos.<br>- Baja Concientización.<br>- Crecimiento de Redes.<br>- Falta de Previsión de Contingencias.<br>- Desastres Naturales.<br>- Inadecuada protección de la Infraestructura.<br>- Confianza creciente en los sistemas<br>- Virus.<br>- Vulnerabilidades de la seguridad perimetral.<br>- Robo de Información confidencial.<br>- Violación a la privacidad.<br>- Ingeniería social.<br>- Denegación de Servicios.<br>- Hacking | Analista de Incidente | Desde el conocimiento del incidente |
| Evaluar el impacto | Evaluar el impacto del incidente en la infraestructura tecnológica y en el desarrollo de los procesos de la Entidad.<br>Cuando el impacto sea alto o superior que ponga en riesgo la estabilidad, seguridad y resiliencia del sistema, se informa al Cai Virtual de la Policía Nacional www.ccp.gov.co, Centro Cibernético Policial de la Policía Nacional. | CSIRT | Según la tabla de tiempos de respuesta |
| Delegar responsabilidades | Asignar las acciones de erradicación de la incidencia al personal del Grupo de Infraestructura Tecnológica dependiendo de la competencia | Profesional de Sistemas | Durante las doce horas siguientes al reporte de la evaluación del impacto |

"Los suscritos hemos revisado el documento y lo encontramos ajustado a las disposiciones técnicas o legales, en el marco de nuestras competencias, por tanto, bajo nuestra responsabilidad lo presentamos para firma"

| Elaboró: Jefferson Silva Losada | Revisó: Rafael Augusto Sierra Rojas |
|---|---|
| Cargo: Profesional de Sistemas | Cargo: Jefe Oficina Asesora de Planeación y Proyectos (E) |
| Firma: | Firma: |
| Aprobado mediante Resolución Administrativa N° 0003 de 2025 | |

| | | | |
|---|---|---|---|
| Verificar existencia de recursos | Verificar la disponibilidad de recursos necesarios para la recuperación tales como manuales, backups de sistemas operativos, aplicativos, bases de datos, antivirus, equipos, sistemas eléctricos, servicios de internet, de correo | Profesionales y técnicos del Grupo de Infraestructura Tecnológica, Administrador de SI | Inmediatamente después de la delegación |
| Disponer de la logística | Asignar los recursos físicos, tecnológicos, comunicaciones, transporte y demás necesarios para la ejecución del plan de recuperación | Profesional de Sistemas | Durante las doce horas siguientes al reporte de la evaluación del impacto |
| Aplicar la estrategia de erradicación | Realizar las acciones de la estrategia de erradicación (tabla de clasificación y estrategias de respuesta | Profesionales y técnicos del Grupo de Infraestructura Tecnológica, Administrador SI | Según la tabla de tiempos de respuesta |
| Comunicar a los usuarios | Informar a los usuarios del proceso a intervenir, indicando el tiempo probable de suspensión del sistema, el cual dependen del nivel de complejidad del incidente, previamente establecido en el procedimiento. | Profesional de seguridad | Una vez se conozca la disponibilidad de recursos. |
| Aplicar la estrategia de recuperación | Realizar las acciones de la estrategia de recuperación (tabla de clasificación y estrategias de respuesta | Profesionales y técnicos del Grupo de Infraestructura Tecnológica, Administrador de SI | Según la tabla de tiempos de respuesta |
| Comunicar el restablecimiento del servicio | Informar a los usuarios la puesta en marcha del sistema | Profesional en seguridad | Inmediatamente a la terminación de las acciones de restauración |
| Pruebas | Monitorear el comportamiento del sistema durante tres horas y se deja registrado en bitácora | Responsable de seguridad | Inmediatamente a la terminación de las acciones de recuperación |

"Los suscritos hemos revisado el documento y lo encontramos ajustado a las disposiciones técnicas o legales, en el marco de nuestras competencias, por tanto, bajo nuestra responsabilidad lo presentamos para firma"

| Elaboró: Jefferson Silva Losada | Revisó: Rafael Augusto Sierra Rojas |
|---|---|
| Cargo: Profesional de Sistemas | Cargo: Jefe Oficina Asesora de Planeación y Proyectos (E) |
| Firma: | Firma: |
| Aprobado mediante Resolución Administrativa N° 0003 de 2025 | |

| | | | |
|---|---|---|---|
| Retroalimentación | Se aplica una encuesta sobre el funcionamiento del sistema o del Hardware | Profesional en seguridad | Inmediatamente a la terminación de las pruebas |
| Cerrar el proceso | Presentar un informe del incidente, de las acciones de respuesta aplicadas o acciones correctivas, proponer las acciones preventivas y de mejorar para evitar reincidencias | Profesional en seguridad. Primer punto de contacto | Posterior a las pruebas a satisfacción |

### 6.3. FASE 3: CONTENCIÓN

Para evitar la propagación del incidente, disminuir el impacto sobre los activos de información, y garantizar la confidencialidad, integridad y disponibilidad de la información, en la empresa de servicios públicos domiciliarios de Pitalito – EMPITALITO ESP, se establecen las siguientes actividades:

**Contención:** busca la detección del incidente con el fin de que no se propague y pueda generar más daños a la información o a la arquitectura de TI.

Una vez se apliquen las estrategias de contención, se procede a la recolección de la evidencia, para lo cual se debe tener en cuenta:

- **Autenticidad:** Quien haya recolectado la evidencia debe poder probar que es auténtica.
- **Cadena de Custodia:** Registro detallado del tratamiento de la evidencia, incluyendo quienes, como y cuando la transportaron, almacenaron y analizaron, con tal fin de evitar alteraciones o modificaciones que comprometan la misma.
- **Validación:** Garantizar que la evidencia recolectada es la misma que la presentada ante las autoridades.

Durante el proceso de recolección de evidencias es necesario realizar las siguientes acciones:

- Registrar información que rodea a la evidencia.
- Tomar fotografías del entorno de la evidencia.
- Tomar la evidencia.

- Registrar la evidencia.
- Rotular todos los medios que serán tomados como evidencia.
- Almacenar toda la evidencia de forma segura.
- Generar copias de seguridad de la evidencia original.
- Realizar revisiones periódicas para garantizar que la evidencia se encuentra correctamente conservada

### 6.4. FASE 4: ERRADICACIÓN Y RECUPERACIÓN

Después de que el incidente ha sido contenido se debe realizar una erradicación y eliminación de cualquier rastro dejado por el incidente como código malicioso y posteriormente se procede a la recuperación a través de la restauración de los sistemas y/o servicios afectados para lo cual el administrador de TI o quien haga sus veces deben restablecer la funcionalidad de los sistemas afectados, y realizar un endurecimiento del sistema que permita prevenir incidentes similares en el futuro.

## CLASIFICACION Y TRATAMIENTO DE INCIDENTES

| CLASE DE INCIDENTE | CONCEPTO | TIPO DE INCIDENTE | TRATAMIENTO |
|---|---|---|---|
| Denegación del Servicio | Estos incidentes hacen que un sistema, servicio o red dejen de operar a su capacidad prevista y con mucha frecuencia deja sin acceso a usuarios legítimos del sistema o servicio tecnológico afectado. Existen dos tipos de incidentes DoS/DDoS causados por medios técnicos: eliminación y agotamiento de recursos.<br><br>**DoS:** son aquellos causados porque el número de peticiones lanzado desde un equipo cliente a un servidor excede el límite permitido y ello causa que el servidor afectado deje de estar disponible. | * Tiempo de respuesta fuera del normal.<br>* Interrupción de servicios tecnológicos<br>* Envío masivo de miles mensajes de correo electrónico ("mail bombing"), provocando la sobrecarga del servidor de correo y/o de las redes afectadas.<br>* Syb Flood<br>* Ataque a través de equipo Zombis<br>*Ataque contra algunos sistemas de Windows para disminuir su rendimiento<br>*Activación programas | CONTENCION<br><br>* Bloquear o redirigir los paquetes del ataque<br>* Buscar nuevos canales de comunicación entre el servicio y sus usuarios.<br>* Cambiar la URL de la página<br>* Detener las IPS Invalidas<br>* Terminar conexiones o procesos no deseados en servidores<br>y enrutadores y sintonizar sus configuraciones TCP / IP.<br>* Testing de servidor<br>ERRADICACION |

| | | | |
|---|---|---|---|
| | **DDoS:** varios equipos haciendo peticiones a un mismo servidor. El ciberataque busca desconectar el sitio web o al menos hacerlo tan lento que los visitantes dejen de intentar usarlo. Esto se logra saturando el sitio web con tráfico malicioso, ya sea dirigido a la red o al servidor. (Inundación UDP, DNS, HTTP, SYN flood) | bacterias para consumir la memoria y la capacidad del procesador<br>* Error Humano | * Involucrar el proveedor de ISP, - Filtrado.<br>* Restitución del servicio caído<br>RECUPERACION<br>*volver el servicio al estado original. |
| Acceso no Autorizado | Consiste en intentos reales no autorizados, para acceder o utilizar incorrectamente un sistema, servicio o red.<br><br>Es un incidente que involucra a una persona, sistema o código malicioso que obtiene acceso lógico o físico sin autorización adecuada del dueño a un sistema, aplicación, información o un activo de información | * Intentos reiterativos de acceso a recursos.<br>*Ataque de fuerza Bruta<br>*Captura de cuentas de usuario y contraseña mediante herramientas como el keyloggers<br>* Divulgación no autorizada de información personal.<br>* Intrusión física a las instalaciones<br>* Consultas no autorizadas<br>* Intento de acceso no autorizado a base de datos<br>* Acceso no autorizado a carpetas privadas<br>* Creación de usuarios sin autorización | CONTENCION<br>* Apagado del Sistema<br>* Bloqueo de la cuenta<br>ERRADICACION<br>*Implementar bloqueos automáticos por exceso de intentos.<br>* Cambio de contraseñas<br>*Uso de contraseñas seguras<br>* Determinar los puntos de acceso usados por el atacante e implementar las medidas adecuadas para evitar futuros accesos.<br>* Las medidas pueden incluir la deshabilitación de un módem.<br>* control de acceso en el firewall<br>* aumento de las medidas de seguridad físicas.<br>RECUPERACION<br>* Activar las cuentas de usuario<br>*Habilitar el sistema |
| Modificación de Recurso no Autorizado | Un incidente que involucra a una persona, sistema o código malicioso que | *Borrado de Información<br>*Modificación de información<br>* Modificación, instalación o | CONTENCION<br>* Bloqueo de la cuenta<br>ERRADICACION |

| | | | |
|---|---|---|---|
| | afecta la integridad de la información o de un sistema de procesamiento. | eliminación no autorizada de software | * Corrección de efectos producidos<br>* Sustitución de los archivos comprometidos con versiones limpias<br>RECUPERACION<br>* Restauración de copias de seguridad<br>* Instalar versiones actualizadas de software |
| Uso inapropiado de recursos | Un incidente que involucra a una persona que viola alguna política de uso de recursos: | * Abuso de privilegios o de políticas de seguridad* Fuga de Información* Mal uso y abuso de los servicios tecnológicos (correo, internet, intranet)* Captura de información confidencial* Infracciones de derecho de autor y piratería* Destrucción o alteración física de los componentes de red* Destrucción o alteración de la información de configuración* Uso prohibido del recurso de red* uso indebido de información crítica* Robo o pérdida de información* Robo o pérdida de equipos | CONTENCION<br>* Identificación del atacante<br>* Bloquear el usuario<br>*Aislarlo del recurso tecnológico<br>ERRADICACION<br>*Restauración de copias de seguridad<br>* Reconfigurar la seguridad de la base de datos<br>* Informar a Control Disciplinario<br>* Fortalecer y divulgar las políticas de seguridad<br>RECUPERACION<br>* Restaurar los servicios o los componentes de red |
| Código Malicioso | Programa o parte de éste insertado en otro con la intención de modificar su comportamiento original, usualmente | * Virus Informático<br>* Ransonware<br>* Malware | CONTENCION<br>* Aislar equipo de la red<br>ERRADICACION |

| | | | |
|---|---|---|---|
| | para realizar actividades maliciosas como robo de información y de identidad, alteración o destrucción de la información y los recursos. | | *Corrección de efectos producidos.<br>* Remover código malicioso<br>* Limpiar/Wiping/Zeroing<br>* Localizar la copia de seguridad limpia más reciente antes del incidente.<br>* Mejora de las defensas<br>* Análisis de Vulnerabilidad<br>* Instalación de parches.<br>RECUPERACION<br>* Restauración de backups |
| Reconocimiento | se emplea para designar la acción de analizar, por medio de un programa, el estado de los puertos de una máquina conectada a través de una red de comunicaciones. Detecta si un puerto está abierto, cerrado o protegido por un cortafuegos o firewall. Se utiliza para detectar qué servicios comunes está ofreciendo la máquina y posibles vulnerabilidades de seguridad según los puertos abiertos. También puede llegar a detectar el sistema operativo que está ejecutando la máquina según los puertos que tiene abiertos | * Escaneo de puertos<br>* Intento de conexiones arbitrarias a través de un puerto | CONTENCION<br>*Identificación y cierre de puertos<br>ERRADICACION<br>* Incorporación de reglas de filtrado en el firewall<br>RECUPERACION |
| Vandalismo | Deformación o cambio producido de manera intencionada a la página web. Ataque al sitio web que cambia la apariencia visual del sitio. Los defacement ingresan al servidor web y reemplazan el sitio web alojado por uno propio. | *Ataque por Injection de scripts maliciosos<br>* Modificación del sitio web | CONTENCION<br>* Suspensión del servicio web<br>ERRADICACION<br>* Aplicar parches de seguridad faltantes<br>* Reparar el sitio web<br>RECUPERACION<br>*Restaurar el servicio web |
| Daños Físicos | | | CONTENCION |

"Los suscritos hemos revisado el documento y lo encontramos ajustado a las disposiciones técnicas o legales, en el marco de nuestras competencias, por tanto, bajo nuestra responsabilidad lo presentamos para firma"

| | |
|---|---|
| **Elaboró: Jefferson Silva Losada** | **Revisó: Rafael Augusto Sierra Rojas** |
| **Cargo:** Profesional de Sistemas | **Cargo:** Jefe Oficina Asesora de Planeación y Proyectos (E) |
| **Firma:** | **Firma:** |
| Aprobado mediante Resolución Administrativa N° 0003 de 2025 | |

| | | | |
|---|---|---|---|
| | Son los sucesos del entorno y la naturaleza que causan daños a los activos de información, pueden ser causados por el hombre, la naturaleza o por averías del hardware y la infraestructura. | * Fuego<br>* Inundaciones<br>* Daños de hardware por fallos en el suministro de energía eléctrica<br>* Terremotos y eventos naturales | * Uso de extintores<br>* Llamada a los bomberos si es el caso<br>* Desconectar y retirar equipos<br>**ERRADICACION**<br>* Restaurar copias de seguridad* Mantenimiento técnico de equipos para su recuperación<br>* Datacenter alterno<br>*Activación del plan de continuidad del negocio<br>**RECUPERACION**<br>* Reinstalar equipos y dejar en funcionamiento. |

## 6.5. FASE 5: SEGUIMIENTO

Esta fase involucra comprobar que todo realmente vuelve a la normalidad, y además se mantenga de la misma manera o mejor hasta una nueva eventualidad.

El responsable de realizar el seguimiento de los Incidentes de Seguridad de la Información es la Oficina de sistemas quien realizará informes gerenciales y se medirá la gestión mediante los indicadores operacionales y tácticos definidos. La documentación de los incidentes se realizará mediante la mesa de ayuda de Tecnología, a excepción del análisis de vulnerabilidades que se realiza mediante informes presentados a la gerencia.

Las actividades Post-Incidente básicamente se componen del reporte apropiado del Incidente, de la generación de lecciones aprendidas, del establecimiento de medidas tecnológicas, disciplinarias y penales de ser necesarias, así como el registro en la base de conocimiento para alimentar los indicadores.

- Organizar reuniones.
- Mantener la documentación.

- Crear bases de conocimiento.
- Integrar la gestión de incidentes al análisis de riesgo.
- Implementar controles preventivos.
- Elaborar tableros de control.

**Lecciones Aprendidas**

Posterior a un incidente grave, y periódicamente después de los incidentes menores, es necesario la mejora de las medidas de seguridad y el proceso de gestión de incidentes, por lo tanto, es útil mantener un adecuado registro de lecciones aprendidas que permitan conocer:

- Exactamente lo que sucedió, en qué momento y cómo el personal gestionó el incidente.
- Los procedimientos documentados
- Evaluar si se tomaron las medidas o acciones que podrían haber impedido la recuperación.
- Cuál sería la gestión de personal y que debería hacerse la próxima vez que ocurra un incidente similar.
- Acciones correctivas pueden prevenir incidentes similares en el futuro.
- Cuales herramientas o recursos adicionales son necesarios para detectar, analizar y mitigar los incidentes en el futuro.

Este proceso de lecciones aprendidas puede evidenciar que hace falta un paso o que haya una inexactitud en los procedimientos, lo cual se convierte en una oportunidad de mejora.

## 7. CONTROL DE CAMBIOS

| VERSIÓN N°. | FECHA DE APROBACIÓN. | DESCRIPCIÓN DEL CAMBIO. |
|---|---|---|
| 1 | 17-09-2024 | Manual de Gestión de Incidentes de Seguridad de la Información |
| 2 | 28-01-2025 | Actualización del Manual de Gestión de Incidentes de Seguridad de la Información |

## 8. APROBACIÓN

"Los suscritos hemos revisado el documento y lo encontramos ajustado a las disposiciones técnicas o legales, en el marco de nuestras competencias, por tanto, bajo nuestra responsabilidad lo presentamos para firma"

| | |
|---|---|
| **Elaboró: Jefferson Silva Losada** | **Revisó: Rafael Augusto Sierra Rojas** |
| **Cargo:** Profesional de Sistemas | **Cargo:** Jefe Oficina Asesora de Planeación y Proyectos (E) |
| **Firma:** | **Firma:** |
| Aprobado mediante Resolución Administrativa N° 0003 de 2025 | |

| | Elaboró | Revisó | Aprobó |
|---|---|---|---|
| **Nombre** | Jefersson Silva Losada | Rafael Augusto Sierra Rojas | Carolina Calderón Valderrama |
| **Cargo** | Profesional de Sistemas | Jefe Oficina de Planeación y Proyectos (E) | Gerente |

**CAROLINA CALDERÓN VALDERRAMA**
GERENTE

"Los suscritos hemos revisado el documento y lo encontramos ajustado a las disposiciones técnicas o legales, en el marco de nuestras competencias, por tanto, bajo nuestra responsabilidad lo presentamos para firma"

| | |
|---|---|
| **Elaboró: Jefferson Silva Losada** | **Revisó: Rafael Augusto Sierra Rojas** |
| **Cargo:** Profesional de Sistemas | **Cargo:** Jefe Oficina Asesora de Planeación y Proyectos (E) |
| **Firma:** | **Firma:** |
| Aprobado mediante Resolución Administrativa N° 0003 de 2025 | |