

**POLITICA DE GESTION DE INCIDENTES DE SEGURIDAD DE LA INFORMACION**

**Bogotá, D.C.,**

**FEBRERO DE 2021**

**Contenido**

[**1.** **INTRODUCCIÓN.** 3](#_Toc61361944)

[**2.** **OBJETIVOS.** 4](#_Toc61361945)

[**3.** **ALCANCE.** 5](#_Toc61361946)

[**4.** **DECLARACIÓN.** 6](#_Toc61361947)

[**5.** **REFERENCIA NORMATIVA.** 7](#_Toc61361948)

[**6.** **GLOSARIO.** 8](#_Toc61361949)

[**7.** **ROLES Y RESPONSABILIDADES.** 10](#_Toc61361950)

[**8.** **METODOLOGÍA.** 11](#_Toc61361951)

[**8.1.** **PREPARACIÓN.** 12](#_Toc61361952)

[**8.1.1.** **Recursos de Comunicación.** 12](#_Toc61361953)

[**8.1.2.** **Recursos para el Análisis de Incidentes.** 14](#_Toc61361954)

[**8.1.3.** **Recursos para la Mitigación de Incidentes.** 15](#_Toc61361955)

[**8.2.** **DETECCIÓN Y ANÁLISIS.** 15](#_Toc61361956)

[**8.2.1.** **Clasificación de Incidentes.** 15](#_Toc61361957)

[**8.2.2.** **Señales de un Incidente.** 17](#_Toc61361958)

[**8.2.3.** **Análisis de Incidentes.** 19](#_Toc61361959)

[**8.2.4.** **Documentación de Incidentes.** 21](#_Toc61361960)

[**8.2.5.** **Priorización de Incidentes.**  22](#_Toc61361961)

[**8.3.** **DETENCIÓN, ERRADICACIÓN Y RECUPERACIÓN DEL INCIDENTE.** 24](#_Toc61361962)

[**8.3.1.** **Recolección y Manejo de Evidencia.** 25](#_Toc61361963)

[**8.3.1.1.** **Aislamiento de la escena e identificación de la información.** 25](#_Toc61361964)

[**8.3.1.1.1.** **Cadena de Custodia.** 26](#_Toc61361965)

[**8.3.1.1.2.** **Fuentes de información:** 27](#_Toc61361966)

[**8.3.1.2.** **Conservación y Preservación.** 27](#_Toc61361967)

[**8.3.1.3.** **Análisis de la Información.** 28](#_Toc61361968)

[**8.3.1.4.** **Presentación de Evidencias.** 29](#_Toc61361969)

[**8.3.2.** **Erradicación y Recuperación.** 29](#_Toc61361970)

[**8.4.** **Actividad Post Incidente.** 30](#_Toc61361971)

## **INTRODUCCIÓN.**

La Unidad Administrativa Especial de Rehabilitación y Mantenimiento, a través de la presente política, establece los mecanismos necesarios que se deben tener en cuenta a la hora de enfrentar un incidente de seguridad de la información, permitiendo de esta manera reducir el impacto sustancial sobre los activos de información afectados.

El presente documento, establece los roles y responsabilidades, al interior de la entidad, permitiendo a los colaboradores de la Unidad Administrativa Especial de Rehabilitación y Mantenimiento Vial, conocer los medios de comunicación dispuestos, para que en caso de presentarse un evento y/o incidente de seguridad de la información puedan reportar de manera prioritaria las anomalías y de esta manera poder actuar de forma oportuna, mitigando las consecuencias que el evento y/o incidente de seguridad pudiese ocasionar.

Adicional, la presente política establece la metodología de gestión de incidentes de seguridad de la información, permitiendo manejar los incidentes presentados por medio de etapas, las cuales contribuyen a conocer el incidente junto con sus afectaciones y posteriormente lograr contenerlo y/o erradicarlo, recuperando la funcionalidad de los activos de información afectados.

Finalmente, establece las acciones que la Unidad Administrativa Especial de Rehabilitación y Mantenimiento Vial, debe seguir después de superar el incidente, con la finalidad de implementar las medidas correctivas correspondientes, evitando que se presente nuevamente el incidente de seguridad.

## **OBJETIVOS.**

* Asegurar que las causas, los tratamientos y la solución de los eventos de seguridad de la información, sirvan para la implementación de acciones correctivas y preventivas.
* Asegurar un enfoque coherente y eficaz para la gestión de incidentes de seguridad de la información de forma oportuna.
* Minimizar el impacto ocasionado por la materialización de los riesgos asociados con el uso de las tecnologías de la información y las telecomunicaciones.
* Fortalecer las capacidades tecnológicas al interior de la entidad, con el fin de proteger la infraestructura tecnológica y los activos de información.
* Establecer los roles y responsabilidades para el manejo de los eventos, debilidades y/o incidentes de seguridad de información de una manera efectiva

## **ALCANCE.**

Aplica para todos los colaboradores de la Unidad Administrativa Especial de Rehabilitación y Mantenimiento Vial, que tengan acceso a los recursos y activos de información, en todas sus formas (digital, impresa, escrita, y hablada) durante su ciclo de vida (creación, distribución, transmisión, almacenamiento, eliminación), y está orientada a preservar la confidencialidad, integridad y disponibilidad de la información de la entidad, los cuales están sujetos a los mismos requerimientos de seguridad, y tienen las mismas responsabilidades de salvaguardar la información; por lo tanto, están obligados a continuar protegiendo y cumpliendo las políticas de confidencialidad durante y una vez terminada su relación laboral y/o contractual con la entidad.

## **DECLARACIÓN.**

La presente política es de obligatorio y estricto cumplimiento para la Unidad Administrativa Especial de Rehabilitación y Mantenimiento Vial, para sus servidores públicos, contratistas, proveedores, terceros, visitantes y todas aquellas personas que guarden relación con la entidad, logrando salvaguardar los objetivos estratégicos y misionales y mejorando continuamente los procesos al interior de la entidad, salvaguardando los activos de información en lo relacionado con la confidencialidad, integridad y disponibilidad buscando prevenir, asegurar y/o recuperar el nivel habitual de funcionamiento de sus servicios en casos de materializarse incidentes de seguridad y minimizar el impacto negativo que estos puedan ocasionar.

## **REFERENCIA NORMATIVA.**

* **Ley Estatutaria 1581 de 2012:** *“Por la cual se dictan disposiciones generales para la protección de datos personales”.*
* **Ley Ordinaria 1273 de 2009:** *“por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado “de la protección de la información y de los datos”- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones”.*
* **Ley Ordinaria 527 de 1999:** “*por medio de la cual se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales, y se establecen las entidades de certificación y se dictan otras disposiciones”.*
* **Organización Internacional de Normalización ISO-27037:2012:** Tecnología de la información - Técnicas de seguridad - Directrices para la identificación, recopilación, adquisición y preservación de evidencia digital
* **Norma Técnica Colombiana NTC-ISO-IEC 27001:2013:**Norma técnica de sistemas de gestión de la seguridad de la información. Requisitos.
* **Organización Internacional de Normalización ISO-27035:2016:** tecnología de la información. técnicas de seguridad. gestión de incidentes de seguridad de la información.

## **GLOSARIO.**

* **Activos de Información:** Cualquier elemento de información o que interactúe con ella que sea necesario para desempeñar las actividades diarias y cuya no disponibilidad o deterioro supone un agravio o coste.
* **Amenaza:** Es un ente o escenario interno o externo que puede hacer uso de una vulnerabilidad para generar un perjuicio o impacto negativo en la organización.
* **Backup:** En tecnologías de la información e informática es una copia de los datos originales que se realiza con el fin de disponer de un medio de recuperación en caso de su pérdida.
* **Cadena De Custodia:** Su objetivo principal es demostrar 3 aspectos: El primero, que la información o evidencia está intacta al momento de presentarse, segundo, que la hora y fecha en la que se hace entrega al proveedor o las autoridades sea exacta y tercero, que no fue manipulada o alterada mientras se encontraba en custodia del proveedor.
* **Ciberseguridad:** la ciberseguridad se define como **una capa de protección para los archivos de información**, a partir de ella, se trabaja para evitar todo tipo de amenazas, las cuales ponen en riesgo la información que es procesada, transportada y almacenada en cualquier dispositivo.
* **Colaboradores:** Todos los servidores públicos, trabajadores oficiales, orden de prestación de servicios y todas las personas que se encuentren vinculadas a la Entidad y que deban generar algún trabajo para la misma.
* **Confidencialidad:** La confidencialidad se refiere a que la información no esté disponible ni sea revelada a individuos, entidades o procesos no autorizados.
* **CSIRT: (Computer Security Incident Response Team):** Equipo de Respuesta frente a Incidencias de Seguridad Informática.
* **Disponibilidad:** La disponibilidad es la propiedad de la información que se refiere a que ésta debe ser accesible y utilizable por solicitud de una persona entidad o proceso autorizada cuando así lo requiera esta, en el momento y en la forma que se requiere ahora y en el futuro, al igual que los recursos necesarios para su uso.
* **Evento de seguridad de la información:** Presencia identificada de una condición, alerta o notificación de un sistema, servicio o red, que indica una posible violación de la política de seguridad de la información o la falla de las salvaguardas o una situación desconocida previamente que puede ser pertinente para la seguridad.
* **Evidencia:** Todo aquel elemento que proporcione información que conduzca a alguna conclusión o hallazgo relacionado con el hecho que se investiga.
* **Evidencia Digital:** información o datos, almacenados o transmitidos en forma binaria los cuales pueden servir como prueba.
* **IDS:** Sistema de detección de Intrusos. (en inglés, Intrusión Detection System).
* **Incidente de seguridad de la información:** Un evento o serie de eventos de Seguridad de la Información no deseados o inesperados, que tienen una probabilidad significativa de comprometer las operaciones del negocio y amenazar la seguridad de la información.
* **IPS:** Sistema de Prevención de Intrusos. (en inglés, Intrusión Prevention System).
* **Seguridad de la Información:** Protección que se brinda a los activos de información mediante medidas preventivas con el fin de asegurar la continuidad del negocio y evitar la materialización de los riesgos.
* **Seguridad Informática:** Se encarga del aseguramiento de la infraestructura tecnológica mediante herramientas o elementos físicos, para evitar que se materialización las amenazas que se propagan por la red.
* **Riesgo**: Es la definición de un escenario bajo el cual una amenaza puede explotar una vulnerabilidad, generando un impacto negativo al negocio (por ejemplo, pérdida de la continuidad, incumplimiento, pérdida de ingresos, entre otros).
* **Vulnerabilidad**: Es una falencia o debilidad que puede estar presente en la tecnología, las personas o en las políticas y procedimientos de una organización.

## **ROLES Y RESPONSABILIDADES.**

La definición de los roles y responsabilidades permitirá gestionar los eventos y/o incidentes de seguridad de la información que se pudiesen presentar en la entidad, estableciendo las acciones correspondientes que se deben cumplir y/o ejecutar por cada uno de los actores involucrados, de esta manera se logrará disminuir el impacto que puede causar un incidente de seguridad de la información.

**Tabla No 1. Roles y Responsabilidades.**

|  |  |
| --- | --- |
| **ROL** | **RESPONSABILIDADES** |
| **PARTES INTERESADAS**  (Colaboradores de la Unidad Administrativa Especial de Rehabilitación y Mantenimiento Vial). | * Reportar cualquier evento y/o incidente de seguridad de la información que afecte la confidencialidad, integridad y disponibilidad de los activos de información. |
| **RESPONSABLES RIESGOS SEGURIDAD DE LA INFORMACIÓN**  (responsable y/o custodio de los activos de información). | * Reportar cualquier evento y/o incidente de seguridad de la información que afecten la confidencialidad, integridad y disponibilidad de los activos de información a su cargo. * Apoyar las gestiones correspondientes para la resolución de eventos y/o incidentes de seguridad de la información sobre los activos de información su cargo. * Colaborar en la clasificación y evaluación de los eventos y/o incidentes de seguridad de la información que se detecten en los activos de información a su cargo. |
| **ANALISTA PRIMER PUNTO DE CONTACTO** (Personal Mesa de Servicios). | * Registrar los eventos de seguridad de la información en la herramienta de gestión de tickets GLPI * Escalar e informar oportunamente al primer respondiente los eventos y/o incidentes reportados, según corresponda. |
| **PRIMER RESPONDIENTE GESTIÓN DE INCIDENTES SEGURIDAD DE LA INFORMACIÓN** (Líder de TI, Especialista Seguridad de la Información, Especialista Seguridad Informática, Grupo de Infraestructura, Grupo de Desarrollo). | * Revisar, analizar y proponer acciones para dar solución a los incidentes de seguridad de la información. * Dar gestión sobre el reporte de un evento o incidente de seguridad de la información desde cualquier ámbito, ejecutando acciones oportunas para contener, mitigar o erradicar las fuentes de ataque, amenazas o vulnerabilidades explotadas que permitan la afectación a las propiedades de seguridad de la información de los activos de la entidad. * Colaborar en el seguimiento o trazabilidad de la gestión del incidente de seguridad a cargo del responsable o custodio del activo implicado en el incidente de seguridad de la información. * Realizar y/o coordinar las acciones correspondientes para recuperar los activos de información o los servicios que hayan sido afectados por el incidente de seguridad de la información. * Documentar los eventos e incidentes de seguridad de la información. * Escalar incidentes de seguridad de la información al CSIRT Gobierno. |
| **\*CONTROL DISCIPLINARIO INTERNO - \*\*GESTIÓN CONTRACTUAL**  **\***(Cuando las fallas sean de personal de planta). **\*\***(Cuando las fallas sean de personal contratista). | * Tramitar las acciones disciplinarias correspondientes cuando los eventos y/o incidentes de seguridad de la información sean generados por los colaboradores de la entidad independientemente de su vínculo laboral o contractual. |

**Fuente: Desarrollo Propio.**

## **METODOLOGÍA.**

Para lograr los objetivos, la gestión de incidentes de seguridad de la información en la Unidad Administrativa Especial de Rehabilitación y Mantenimiento Vial tiene en cuenta los componentes definidos por el National Institute of Standard and Technology (NIST) alineados con los requerimientos de la ISO 27035 de 2016.

**Ilustración No 1. Ciclo de Vida de la Gestión y Respuesta a un Incidente.**



**Fuente: Guía para la Clasificación de Incidentes de Seguridad de la Información.**

## **PREPARACIÓN.**

Esta fase consiste en la preparación que se debe tener al interior de la entidad, para responder ante posibles eventos y/o incidentes de seguridad de la información que se pudiesen presentar afectando los activos de información. Adicional, tiene como finalidad prevenir posibles incidentes de seguridad, por medio del aseguramiento apropiado de los sistemas de información e infraestructura tecnológica. De esta manera, la entidad puede realizar una gestión eficaz sobre los incidentes presentados, teniendo en cuenta tres pilares fundamentales, personas, procedimientos, tecnología.

La realización de las siguientes actividades permite mitigar el impacto sobre los activos de información:

* Identificar y aprovisionar los recursos necesarios en todas las fases de atención a incidentes.
* Identificar y definir los lineamientos para la prevención de incidentes, dentro de los cuales se destacan los siguientes:
  + Gestión de parches de seguridad.
  + Aseguramiento de plataforma.
  + Seguridad en redes: (Monitoreo de red, registros y eventos del sistema).
  + Prevención de código malicioso.
  + Sensibilización de usuarios.

Adicionalmente se debe preparar un kit de atención de incidentes que pueda ser transportado por los miembros del equipo de atención. El kit debe contener elementos como: Laptop con el software de atención de incidentes precargado (sniffer, software forense), medios de backup, medios para imagen forense, cables, medios de almacenamiento en blanco, copias de sistemas operacionales. El kit debe permanecer disponible, actualizado y completo para cuando sea requerido

## **Recursos de Comunicación.**

La entidad coloca a disposición los siguientes medios para reportar los eventos y/o incidentes de seguridad de la información en función de quien lo detecte:

**Tabla No 2. Medios para el Reporte de Incidentes de Seguridad.**

|  |  |  |
| --- | --- | --- |
| **ORIGEN DE REPORTE** | **MEDIO DE REPORTE** | **DETALLES DE REPORTE** |
| **PARTES INTERESADAS** | Herramienta de Servicios GLPI | <https://mesadeayuda.umv.gov.co> |
| Correo Electrónico Institucional | Para: [Mesadeayuda@umv.gov.co](mailto:Mesadeayuda@umv.gov.co)  CC: [Seguridaddigital@umv.gov.co](mailto:Seguridaddigital@umv.gov.co) |
| Teléfonos | Extensiones asignadas a la mesa de ayuda. |
| **PERSONAL EXTERNO A LA ENTIDAD** | Correo Electrónico Institucional | Para: [Mesadeayuda@umv.gov.co](mailto:Mesadeayuda@umv.gov.co)  CC: [Seguridaddigital@umv.gov.co](mailto:Seguridaddigital@umv.gov.co) |
| Teléfonos | Extensiones asignadas a la mesa de ayuda. |
| Colaboradores de la Entidad | Reportar el evento y/o incidente de seguridad a través de correo electrónico personal a algún colaborador de la entidad con el que tenga contacto, quien a su vez informará el reporte por medio de los mecanismos definidos anteriormente. |

**Fuente: Elaboración Propia.**

Para el caso de las partes interesadas, si sobre el evento y/o incidente de seguridad no es posible realizar su reporte por los medios establecidos, se deberá reportar el evento y/o incidente por medios alternos, como son:

* A través de un compañero
* De manera personal, entre otros,

en todo caso, es de carácter obligatorio realizar el respectivo reporte de los eventos y/o incidentes de seguridad de la información que se pudiesen presentar, por parte de los colaboradores de la entidad.

Si el evento y/o incidente de seguridad es detectado por personal externo a la Unidad Administrativa Especial de Rehabilitación y Mantenimiento Vial, el cual no tiene acceso a los medios de comunicación de la entidad, este puede reportar por cualquier medio la situación detectada al colaborador que autorizó su ingreso a la entidad, o con cualquier miembro del equipo de Gestión de Servicios e Infraestructura Tecnológica.

Durante todo el ciclo de vida del evento y/o incidente de seguridad, es de carácter obligatorio actualizar la información de la gestión realizada en el ticket registrado por la mesa de servicios GLPI, permitiendo informar sobre el avance y/o estado del evento y/o incidente de seguridad de la información.

En el momento de presentarse un incidente con un impacto alto, es importante comunicar a los procesos de los activos implicados, y en caso de ser necesario, a la Dirección y a la Secretaría General, con el fin de que éstas dependencias tomen las decisiones que puedan estar fuera del alcance del primer respondiente, con la siguiente finalidad:

* Informar a los colaboradores de la Unidad Administrativa Especial de Rehabilitación y Mantenimiento Vial, acerca de la afectación que está atravesando la entidad y las precauciones que se deben tener, para que estas sean adoptadas de manera transversal en cada una de las dependencias y/o áreas.
* Informar a la Superintendencia de Industria y Comercio – SIC, acerca de los incidentes que involucren datos personales, de acuerdo a la normatividad vigente.
* Informar a los colaboradores de la Unidad Administrativa Especial de Rehabilitación y Mantenimiento Vial, acerca de la pérdida de confidencialidad, integridad y disponibilidad de los activos de información, y el tiempo que tomará restaurarlo, recuperarlo y/o recrearlo según sea el caso.

## **Recursos para el Análisis de Incidentes.**

* **Listado de puertos:** Se debe tener una lista de todos los puertos conocidos y de los puertos utilizados por ataques.
* **Diagramas de red y listas de activos críticos:** Para una rápida ubicación de los recursos existentes y para el seguimiento de un ataque en curso.
* **Líneas Base:** Se debe levantar la información de los servidores (hoja de vida de los servidores), tales como nombre, dirección IP, parches, aplicaciones y usuarios configurados, con el fin de determinar el estado normal de los mismos y poder identificar de manera rápida un incidente de seguridad. Las líneas base deberán someterse a un sistema de administración de actualizaciones que permita identificar y documentar nuevos cambios a la plataforma con su debida justificación y responsable de la ejecución del cambio.
* **Comportamiento de la red:** Se debe realizar un análisis de las conexiones de red, para poder identificar un comportamiento normal. Este deberá incluir:
  + Puertos utilizados por los protocolos de red.
  + Horarios de utilización pico y valle.
  + Direcciones IP que generan más tráfico.
  + Direcciones IP que más reciben peticiones.

## **Recursos para la Mitigación de Incidentes.**

En este punto se consideran los elementos necesarios para la contención y mitigación de incidentes, como lo es la revisión de las estrategias de continuidad definidas.

## **DETECCIÓN Y ANÁLISIS[[1]](#footnote-1).**

Esta fase tiene la finalidad de identificar y/o detectar las características de cualquier ciberincidente, verificar lo que realmente ha sucedido y determinar su tipo y magnitud. Se debe tener en cuenta que no todos los eventos y/o alertas de ciberseguridad son ciberincidentes.

Por lo anterior, para realizar una correcta identificación y/o detención, la entidad se debe basar en las siguientes actividades:

* Registrar y monitorizar los eventos de las redes, sistemas y aplicaciones (alertas en la consola de administración del firewall, alertas en la consola de antivirus, alertas de equipos de seguridad perimetral, número elevado de conexiones en los servidores).
* Recolectar información situacional que permita detectar anomalías.
* Disponer de capacidades para descubrir ciberincidentes y comunicarlos a los contactos apropiados.
* Recopilar y almacenar de forma segura todas las evidencias.
* Compartir información con otros equipos internos y externos de forma bidireccional para mejorar las capacidades de detección.

## **Clasificación de Incidentes.**

La siguiente clasificación se emplea para normalizar las actividades de gestión de los incidentes y la generación de estadísticas.

**Tabla No 3. Clasificación de Incidentes.**

| **CLASIFICACIÓN DE INCIDENTES DE SEGURIDAD** | | |
| --- | --- | --- |
| **CLASE DE INCIDENTE** | **DESCRIPCIÓN** | **TIPO DE INCIDENTE** |
| **Código Malicioso** (Malware). | Los códigos maliciosos identifican un programa o parte de éste insertado en otro programa, con la intención de modificar su comportamiento original. | Virus, gusanos, troyanos, spyware, rootkit, Ransomware (secuestro informático), códigos móviles y combinaciones de estos |
| **Robo de Información.**  (Obtención de Información). | Ataques dirigidos a recabar información fundamental que permita avanzar en ataques más sofisticados, a través de ingeniería social o de identificación de vulnerabilidades. | * Robo de información digital (Carpetas, bases de datos). * Identificación de vulnerabilidades. * Sniffing. * Ingeniería social. * Phishing. |
| **Abuso/ uso inadecuado de los recursos informáticos.** | Este tipo de incidentes ocurre cuando un usuario viola las políticas de seguridad del sistema de información de la entidad. Ataques dirigidos a dañar la imagen de la entidad o a utilizar sus medios electrónicos para otros usos ilícitos. | * Descargar e instalar herramientas para piratería informática. * Usar el correo corporativo para correo basura o para la promoción de negocios personales. * Usar recursos corporativos para crear un sitio web no autorizado. * Usar actividades entre colegas para adquirir o distribuir archivos piratas (música, video, software). |
| **Borrado** (Compromiso de Información). | Incidentes relacionados con el acceso y fuga (Confidencialidad), modificación o borrado (Integridad) de información no pública. | * Acceso no autorizado a información. * Modificación y borrado no autorizada de información. * Publicación no autorizada de Información |
| **Acceso no Autorizado.** | Intentos reales no autorizados, para acceder o utilizar incorrectamente un sistema, servicio o red por parte de una persona, sistema o código malicioso. | * Intentos por recuperar archivos de contraseñas. * Ataques por desbordamiento de búfer para obtener acceso privilegiado a un objetivo. * Aprovechamiento de las vulnerabilidades del protocolo para secuestrar o dirigir equivocadamente las conexiones de red legítimas. * Intentos de elevar privilegios a recursos o información más allá de los que un usuario o administrador ya posee legítimamente. * Violaciones a las medidas de seguridad física. |
| **Denegación de Servicio (DoS) y Denegación de Servicio Distribuido (DDoS).**    (Disponibilidad) | Permiten que un sistema, servicio o red dejen de operar a su capacidad prevista consumiendo sus recursos (Memoria RAM CPU, Capacidad de almacenamiento y recursos de red). Estos tipos de ataques por lo general se realizan con frecuencia por medio de botnets, un grupo de robots de software (códigos maliciosos) que funcionan en forma autónoma y automática Los botnets pueden comunicarse con centenares o millones de computadores afectados. | * Robo, daño intencionado y destrucción de equipos. * Daño accidental al hardware por incendio o daño por agua/inundación. * Cambios en las condiciones ambientales por ejemplo las altas temperaturas. * Sobrecarga y mal funcionamiento de los sistemas de información, software y hardware |
| **Intrusiones.** | Ataques dirigidos a la explotación de vulnerabilidades de diseño, de operación o de configuración de diferentes tecnologías, al objeto de introducirse de forma fraudulenta en los sistemas de información y sitios web de la entidad. | * Compromiso de cuenta de usuario. * Defacement (desfiguración). * Cross-Site Scripting (XSS). * Cross-Site Request Forgery (CSRF). * Falsificación de petición entre sitios cruzados. * Inyección SQL. * Spear Phishing. * Pharming. * Ataque de fuerza bruta. * Inyección de Ficheros Remota. * Explotación de vulnerabilidad software. * Explotación de vulnerabilidad hardware. |

**Fuente: Elaboración Propia.**

## **Señales de un Incidente[[2]](#footnote-2).**

La parte más desafiante en el proceso de gestión de incidentes es detectar con precisión y evaluar posibles incidentes; determinar si ha ocurrido un incidente y, de ser así, el tipo, extensión y magnitud del problema. Lo anterior, se debe a los siguientes factores:

* Los incidentes pueden ser detectados por diferentes medios los cuales varían en el nivel de detalle y fidelidad. Las herramientas automáticas pueden incluir, sistemas de detección/prevención de intrusos, software de antivirus o analizadores de logs. Los incidentes también pueden ser detectados por medios manuales como reportes de problema de los usuarios. Aunque existen incidentes que pueden ser detectados fácilmente, existen otros que no se detectan hasta que sus efectos son notorios.
* El volumen de síntomas potenciales de un incidente por lo regular es alto, por ejemplo, un IDS puede generar miles de falsos positivos, por esa razón es necesario filtrar apropiadamente la información proveniente de herramientas automáticas.
* Se requiere conocimiento especializado y experiencia para realizar análisis detallados de la información recolectada durante la identificación de un incidente.

Las señales de los incidentes se pueden clasificar en dos categorías: Precursores e indicadores:

* **Precursor:** es una señal de que un incidente puede ocurrir en el futuro[[3]](#footnote-3).
* **Indicador:** es una señal de que un incidente puede haber ocurrido o puede estar ocurriendo[[4]](#footnote-4).

Debido a que existen múltiples fuentes que pueden identificar un precursor o indicador, a continuación, se relacionan las señales más comunes que se deben supervisar al interior de infraestructura y sistemas de información:

**Tabla No 4. Fuentes Comunes Precursores e Indicadores.**

| **FUENTES** | **DESCRIPCIÓN** |
| --- | --- |
| **ALERTAS** | |
| Software de Antivirus | Cuando el software de antivirus o antispyware detecta código malicioso típicamente genera alertas. Si las firmas digitales de código malicioso del software de antivirus y antispyware están actualizadas, el mismo software puede aislar y erradicar el código malicioso. |
| Software de Verificación de Integridad. | El software de verificación de integridad de archivos puede detectar cambios realizados en archivos importantes durante incidentes. |
| Software de Monitoreo | El software de monitoreo de plataforma verifica a intervalos periódicos el funcionamiento de los servicios y la plataforma de tecnología, cuando el servicio o recurso no responde o presenta un comportamiento fuera de lo común se deben verificar las alertas para descartar ocurrencia de incidentes. |
| **REGISTROS** | |
| Registros del sistema operacional y las aplicaciones. | Los registros de los sistemas operativos y especialmente de los de auditoría son de gran valor para la identificación de incidentes, los registros no se deben deshabilitar, se debe preservar y el comportamiento rutinario de los servicios se debe establecer para detectar cambios que sean signos de la posible ocurrencia de incidentes de seguridad de la información. |
| Registros de los servicios de red | Por lo general los registros de firewall o routers no constituyen fuente primaria de precursores o indicadores debido a que por lo regular se configuran para grabar conexiones bloqueadas y proporcionan poca información sobre el comportamiento de un incidente, sin embargo, se debe verificar esto registros para identificar patrones de comportamiento en acceso a puertos de la red. |
| **INFORMACIÓN DISPONIBLE PUBLICAMENTE** | |
| Bases de datos de amenazas y vulnerabilidades | Los especialistas de servidores y seguridad informática deben verificar periódicamente las bases de datos de vulnerabilidades y amenazas para identificar indicadores de incidentes que puedan afectar a la entidad y prepararse para afrontar futuros ataques. Las bases de datos que se deben verificar con regularidad son US-CERT y CERT /CC.  Mantenerse al día con nuevas vulnerabilidades y exploits puede evitar que ocurran algunos incidentes y ayudar a detectar y analizar nuevos ataques. |
| **PERSONAL** | |
| Colaboradores. | Los usuarios, administradores de sistemas, administradores de red y en general todas las personas que hagan uso de servicios o recursos de la entidad, deben reportar posibles señales de incidentes de seguridad. |
| Informes de incidentes de otras entidades | El especialista de seguridad de la información de la entidad debe mantener contacto con los centros de respuesta a incidentes del gobierno colombiano y la Alta Consejería de la alcaldía de Bogotá. |

**Fuente: NIST 800 – 61 R2.**

## **Análisis de Incidentes.**[[5]](#footnote-5)

La detección y el análisis de incidentes serían fáciles si se garantizara que todos los precursores o indicadores preciso; sin embargo, no siempre se pueden identificar con precisión esos factores. Por lo anterior, es responsabilidad del primer respondiente la evaluación de la pertinencia de las señales detectadas y actuar de conformidad, en general los responsables de la gestión de incidentes deben asumir que el incidente está ocurriendo hasta que se confirme lo contrario. Los responsables de la gestión de incidentes deben analizar información ambigua, contradictoria o incompleta para determinar si está o no ocurriendo un incidente.

El grupo de gestión de incidentes debe trabajar con prontitud para analizar y validar cada incidente y documentar desde la fase de identificación del incidente cada paso que se realice para su tratamiento. Cuando el grupo de gestión de incidentes considere que está ocurriendo un incidente, se debe realizar un análisis rápido para determinar el alcance del incidente (redes, sistemas o aplicaciones afectadas), quién o cual es la fuente del incidente, cómo está ocurriendo el incidente (herramientas que se están usando para realizar el ataque, vulnerabilidades que están explotando). El análisis inicial del incidente debe contener información suficiente para priorizar las siguientes actividades de manejo del mismo.

Las siguientes recomendaciones se deben tener en cuenta al momento de realizar el análisis inicial del incidente[[6]](#footnote-6):

* **Perfiles de redes y sistemas:** Se deben mantener perfiles o registros actualizados del comportamiento de los diferentes dispositivos y sistemas, de esa forma se puede predecir el comportamiento de los mismos e identificar comportamientos no esperados o irregulares.
* **Comprender los comportamientos normales:** Se deben estudiar periódicamente las redes, sistemas y aplicaciones para obtener un conocimiento detallado de lo que se considera un comportamiento normal y así identificar comportamientos anormales y reconocer fácilmente la ocurrencia de incidentes.
* **Uso de log centralizado y política de retención de registros:** Los registros de los diferentes dispositivos de red, sistemas de información y servicios se deben consolidar en uno o puntos únicos de recolección centralizados y mantener copias de los mismos para facilitar el análisis de los incidentes.
* **Realizar correlación de eventos:** Debido a que los incidentes pueden implicar a varios recursos de información y tecnología, el equipo de atención a incidentes debe utilizar herramientas de software que les permitan realizar la correlación de los registros generados por cada uno de los dispositivos, sistemas y servicios implicados en el incidente.
* **Mantener los relojes de los sistemas sincronizados con una fuente única:** Para que el proceso de correlación de eventos sea efectivo es necesario mantener sincronizados los relojes de los diferentes dispositivos y sistemas.
* **Mantener y utilizar una base de conocimientos de información:** El equipo de respuesta a incidentes debe mantener registros de las lecciones aprendidas del manejo de incidentes, esta base de conocimiento se puede elaborar en hojas electrónicas o bases de datos que faciliten la recopilación de información como explicaciones y detalles de indicadores y/o precursores de incidentes de seguridad tales como alertas de detección de intrusos, registros de entrada a sistemas operativos y códigos de error de aplicaciones, lista de dominios reportados en listas negras por envío de spam.
* **Utilice motores de búsqueda de Internet para realizar investigaciones:** Los motores de búsqueda de Internet pueden ayudar a los analistas a encontrar información sobre actividad inusual.
* **Ejecutar sniffers para recolectar información adicional: Cuando** los indicadores del incidente no registran información suficiente en los dispositivos se debe utilizar software como sniffers para recopilar información en toda la red.
* **Filtrado de datos:** Debido a que durante un incidente se pueden generar un elevado volumen de datos que impiden su análisis total y detallado, el equipo de respuesta a incidentes debe filtrar la información recolectada para facilitar el análisis de los datos. Se debe identificar los mejores criterios de filtrado de datos de acuerdo con la naturaleza particular de cada incidente.
* **Búsqueda de asistencia externa:** Cuando el equipo de respuesta a incidentes requiera apoyo externo, debe realizar el escalamiento con los centros de respuesta a incidentes.

## **Documentación de Incidentes.**

Una vez que el equipo de respuesta a incidentes sospeche que un incidente está ocurriendo u ocurrió, se debe iniciar la documentación del mismo. Es necesario documentar únicamente los hechos relacionados con el incidente, se debe evitar el registro de opiniones personales o subjetivas.

Los miembros del equipo de gestión de incidentes deben llevar registro de las acciones ejecutadas para la atención del incidente, el registro de debe llevar en una bitácora de seguimiento del incidente, el mecanismo más simple es el uso de una libreta de anotaciones, pero también se puede usar computador personal, Smartphone u otro tipo de tecnología que permita llegar registro de las actividades. Las notas de las acciones ejecutadas se deben transcribir en limpio. Las notas originales no deben ser destruidas, borradas o alteradas, no se deben retirar hojas de los cuadernos de notas o borrar las anotaciones realizadas en equipos electrónicos. Todas las notas deben quedar firmadas y fechadas por el autor. Todas las notas realizadas pueden constituir evidencias en procesos legales. Las diferentes actuaciones del equipo de respuesta a incidentes deben registrarse en la mesa de ayuda. Los datos que los miembros del equipo de respuesta a incidentes deben registrar incluyen:

* El estado actual del incidente (nuevo, en curso, remitido para investigación, resuelto, etc.)
* Un resumen del incidente
* Indicadores relacionados con el incidente
* Otros incidentes relacionados con este incidente
* Acciones tomadas por todos los manejadores de incidentes en este incidente
* Cadena de custodia, si corresponde
* Evaluaciones de impacto relacionadas con el incidente
* Información de contacto de otras partes involucradas (por ejemplo, propietarios del sistema, administradores del sistema)
* Una lista de las pruebas reunidas durante la investigación del incidente.
* Comentarios de los manejadores de incidentes
* Próximos pasos a seguir (por ejemplo, reconstruir el host, actualizar una aplicación).

El equipo de respuesta a incidentes debe preservar toda la información de las acciones y evidencias recolectadas durante el proceso de atención del incidente y restringir el acceso a ellos, debido a que muchas veces contiene información sensible como: vulnerabilidades no detectadas, acciones indebidas realizadas por usuarios o atacantes, brechas de seguridad en los sistemas o la plataforma tecnológica. Los correos, documentos, y reportes relacionados con el manejo del incidente deben ser cifrados para evitar acceso no autorizado a los mismos.

## **Priorización de Incidentes.[[7]](#footnote-7) [[8]](#footnote-8)**

Todos los incidentes deben ser priorizados para garantizar que son atendidos de acuerdo con su nivel de criticidad. Para todos los incidentes se debe evaluar los siguientes factores:

* Efectos técnicos reales y potenciales del incidente.
* Recursos críticos afectados por el incidente.

Los incidentes que impactan directamente la continuidad de las actividades misionales de la entidad requieren atención prioritaria. La primera labor para priorizar los incidentes es calificar el nivel de los efectos.

La siguiente tabla permite establecer el nivel de efectos del incidente:

**Tabla No 5. Nivel de Efectos del Incidente (Impacto Actual – Impacto Potencial).**

|  |  |  |
| --- | --- | --- |
| **Nivel criticidad** | **Valor** | **Definición** |
| **Ninguno** | 0.0 | No se afectan sistemas críticos, No se afectan múltiples áreas. |
| **Inferior** | 0.10 | Efectos imperceptibles (no los nota ningún área de la entidad). |
| **Bajo** | 0.25 | Efectos moderados (los nota el proceso, dependencia y/o área afectada, pero el trabajo puede continuar). |
| **Medio** | 0.50 | Efectos severos en un proceso, dependencia y/o área de la entidad o efectos imperceptibles en varias áreas o efectos imperceptibles en un recurso crítico |
| **Alto** | 0.75 | Efectos moderados en múltiples procesos, dependencias y/o áreas de la entidad, moderados en un recurso crítico (el recursos o servicio trabaja de manera degradada). |
| **Superior** | 1.00 | Efectos severos en varias áreas de la entidad (no se puede continuar laborando) o efectos severos en un recurso crítico (no puede prestar servicios). |

**Fuente: Desarrollo Propio.**

Una vez realizada la valoración de efectos del incidente, se debe asignar un nivel de criticidad a los sistemas afectados:

**Tabla No 6. Niveles de Criticidad.**

|  |  |  |
| --- | --- | --- |
| **Nivel criticidad** | **Valor** | **Definición** |
| **Inferior** | 0.10 | No es un sistema crítico o componente de infraestructura |
| **Bajo** | 0.25 | Sistema o componente que apoya la operación de un (1) proceso, dependencia y/o área de la entidad. |
| **Medio** | 0.50 | Sistema o componente que apoya la operación de más de un proceso, dependencia y/o área de la entidad. |
| **Alto** | 0.75 | Sistema o componente crítico que soporta la operación de un proceso, dependencia y/o área de la entidad. |
| **Superior** | 1.00 | Sistema o componente que soporta la operación misional de todos los procesos, dependencias y/o áreas de la entidad. |

**Fuente: Desarrollo Propio.**

Con el fin de permitir una atención adecuada a los incidentes (análisis, contención y erradicación), se debe determinar el nivel de prioridad de este, y de esta manera atenderlos adecuadamente según la necesidad.

* **Nivel de Prioridad:** Depende del valor o importancia dentro de la entidad y del proceso que soporta el o los sistemas afectados.
* **Impacto Actual:** Depende de la cantidad de daño que ha provocado el incidente en el momento de ser detectado.
* **Impacto Potencial:** Depende de la cantidad de daño que pueda causar el incidente si no es contenido, ni erradicado.

Luego de tener definidas las variables, se obtiene la prioridad mediante la siguiente fórmula:

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

Los resultados obtenidos se deben comparar con la siguiente tabla para determinar la prioridad de atención:

**Tabla No 7. Nivel de Prioridad del Incidente.**

|  |  |
| --- | --- |
| **Nivel Prioridad** | **Valor** |
| Inferior | 00 – 2.49 |
| Bajo | 2.50 – 3.74 |
| Medio | 3.75 – 4.99 |
| Alto | 5.00 – 7.49 |
| Superior | 7.50 – 10 |

**Fuente: Desarrollo Propio.**

## **DETENCIÓN, ERRADICACIÓN Y RECUPERACIÓN DEL INCIDENTE.**[[9]](#footnote-9)

Una vez analizado y priorizado el incidente se debe contener su acción para evitar que su propagación impida su erradicación y afecte a otros sistemas. Cada incidente tiene su forma particular de contención que debe ser estudiada, definida y adoptada por el equipo de respuesta a incidentes, algunas de las opciones de contención incluyen (apagar el sistema afectado, desconectar el sistema de redes alambradas o inalámbricas, deshabilitar funciones del sistema, apagar servicios).

Las estrategias de contención varían según el tipo de incidente, por lo anterior, se deben crear estrategias separadas para cada tipo de incidente, teniendo en cuenta los siguientes criterios:

* Daño potencial y pérdida de recursos.
* Necesidad de preservación de evidencias.
* Disponibilidad del servicio.
* Tiempo y recursos necesarios para implementar la estrategia de manejo del incidente.
* Efectividad de la estrategia seleccionada.
* Duración de la solución.

## **Recolección y Manejo de Evidencia.**[[10]](#footnote-10)

Aunque la razón principal para la recolección de evidencias es la gestión del incidente también es necesaria para eventuales procesos legales. Por lo anterior, se debe documentar, minuciosamente, todos los procesos al tratar con un incidente en el formato **EGTI-FM-011 Formato Reporte de Incidentes.**

## **Aislamiento de la escena e identificación de la información.**[[11]](#footnote-11) [[12]](#footnote-12) [[13]](#footnote-13)

Una vez el evento reportado se cataloga como un incidente de seguridad de la información, es necesario restringir el acceso a la zona donde se produjo el incidente para evitar cualquier tipo de alteración o contaminación a la evidencia.

Dependiendo la rigurosidad del incidente y teniendo en cuenta que los procedimientos se deben ejecutar en la brevedad posible debe proceder el personal de la entidad, que esté en capacidad de describir detalladamente todos los procedimientos que realizó para aislar la escena y capturar evidencia en primera instancia, para lo cual debe diligenciar el formato **EGTI-FM-012 Formato cadena de custodia aseguramiento digital.**

Procedimiento por realizar para aislar la escena:

* Tomar fotografías del equipo antes de entrar en contacto.
* Se debe prevenir el acceso no autorizado de personal a la escena, estableciendo un perímetro de seguridad, para que nadie pueda acercarse.
* Identificar todos aquellos posibles elementos que sea susceptibles de almacenar (dispositivos que pueden almacenar datos electrónicamente.
* Si el equipo se encuentra encendido y se verifica que se está destruyendo la evidencia apagar inmediatamente, desconectando o retirando batería.
* Si el equipo se encuentra encendido, no se debe apagar, se debe sellar puertos USB, unidades, tomar fotografías de la pantalla, mantener el equipo encendido y evitar que se bloquee.
* Capturar la información volátil (RAM) y verificar cifrado del disco duro (si está cifrado se debe sacar imagen encendido), debe hacerse empleando las herramientas forenses necesarias.
* Si el equipo se encuentra apagado, no realizar el encendido, esto puede alterar la escena o borrar información que podría lograr obtenerse posteriormente.

## **Cadena de Custodia.**

La cadena de custodia es un procedimiento que debe tenerse en cuenta desde el mismo instante que se decida realizar el proceso de evidencia forense, diligenciando **EGTI-FM-013 Formato Registro Cadena de Custodia** (en caso de que la hoja registro cadena de custodia no alcance para diligenciar todos los registros, se debe diligenciar **EGTI-FM-013 Formato Adicional Registro Cadena de Custodia** y **EGTI-FM-014 Formato rotulo elementos materiales probatorios y evidencia física**, adicional, se debe tener en cuenta:

* Hacer un inventario y descripción de los elementos.
* Embalar las evidencias inventariadas en el contenedor, cerrado y etiquetado.
* Etiquetar con: Fecha y hora del hallazgo, numero de evidencia, número de registro (folio), dirección exacta del lugar de los hechos y descripción del material, observaciones, nombre completo del agente policial, perito o auxiliar responsable de la recolección y el embalaje.
* Una hoja de ruta, en donde se anotan los datos principales sobre descripción de la evidencia, fechas, horas, custodios, identificaciones, cargos y firmas de quien recibe y quien entrega.
* Contar con los elementos necesarios para la recolección de información como estaciones forenses, dispositivos de backups, medios formateados y/o estériles, cámaras digitales, cinta y bolsas para evidencia, papel de burbuja, bolsas antiestáticas, cajas de cartón, rótulos o etiquetas.

## **Fuentes de información:**

* Entrevistas administradoras de los sistemas de información y red, revisión topología de red, entrevistas con el personal de la empresa que se hubiera tenido con el incidente, correos electrónicos, documentación referida del caso.
* Computadores de escritorio y portátiles.
* Servidores (Web, DHCP, Email, Mensajería Instantánea, VolP Servers, FTP o cualquier servicio de filesharing).
* Almacenamiento en red.
* Medios tanto internos como externos que contemplan: Dispositivos USB, Firewire, CD/DVD, PCMCIA, Discos Ópticos y Magnéticos, Discos Duros Extraíbles, Memorias SD y MicroSD.
* Dispositivos celulares, Tabletas, PDAs, Cámaras Digitales, Grabadoras de video y audio.

## **Conservación y Preservación.**

Una vez identificada la evidencia se debe garantizar su preservación frente a la utilidad, de tal forma que se respete su originalidad e integridad, garantizando a futuro que la evidencia sea admisible en un proceso judicial. De acuerdo con la Norma ISO 27037 la evidencia digital potencial debe ser tratada de acuerdo a los siguientes principios: Reducir al mínimo la manipulación, documentar los cambios y las acciones adelantadas, cumplir con las normas locales de evidencia, no tomar acciones más allá de su competencia.

El procedimiento para preservar las evidencias digitales se debe tener en cuenta los siguientes pasos:

* Para el almacenamiento de las imágenes forenses se debe contar con medios estériles con una capacidad igual o superior a los discos identificados.
* Usar bloqueadores de escritura.
* Generación de las imágenes forenses de tipo bit a bit mediante herramientas de extracción de imágenes como Linux dd o Encase Forensic Software, se sugiere sacar mínimo dos imágenes forenses.
* Verificar Integridad de la evidencia y cadena de custodia, para cada imagen suministrada se debe calcular su compendio criptográfico (SHA -256), comparándolo luego con el de la fuente original. Si la comparación arroja un resultado negativo se debe rechazar la imagen proveída en el primer paso.
* Evitar una alteración no deseada en los medios.
* No se trabaja sobre el bien informático (sobre escritura).
* En las zonas físicas se deben garantizar las medidas de seguridad necesarias para evitar alteración o intrusión a las evidencias halladas.

## **Análisis de la Información.**

Una vez se han definido los elementos materiales probatorios o evidencia, entramos a la fase de extraer, procesar e interpretar la información, en esta fase se determina toda una cadena de acontecimientos desde que se produjeron los hechos hasta su descubrimiento, dicho análisis puede involucrar y relacionar los eventos, archivos, logs, testimonios, fotografías, videos de vigilancia etc., para así llegar a alguna conclusión determinada.

Se debe tener en cuenta:

* Entorno de trabajo, a nivel físico un espacio que garantice la seguridad de los elementos probatorios recolectados.
* La evidencia se procesa para poder obtener información que entiendas los investigadores.
* Para interpretar se necesita conocimiento profundo como encajan las piezas.
* Obtención de la línea de tiempo de la evidencia.
* El análisis efectuado por el forense debe poder ser repetido.
* Aplicación de técnicas científicas a los medios duplicados, mediante las siguientes acciones:
  + Examinar los logs del sistema, fechas y horas del sistema, su respectiva zona horaria, los recursos y hardware instalado.
  + Usos de dispositivos USB.
  + Determinar sistema operativo y las aplicaciones instaladas.
  + Búsqueda de archivos específicos.
  + Recuperación archivos eliminados.
  + Identificación de información de tráfico de red.
  + Identificación de archivos existentes.
  + Identificación de archivos protegidos.
  + Clasificación de archivos (modificados, sospechoso, extensión modificada).
  + Identificación de correos electrónicos.
  + Acciones que el usuario realizo (historia, archivos abiertos).

## **Presentación de Evidencias.**

Se elabora el informe de hallazgos, que contiene una descripción detallada de los hallazgos relevantes al caso y la forma como fueron encontrados.

En el reporte se debe contemplar los siguientes aspectos:

* El destino del informe, donde se relacione el cliente, autoridad o entidad solicitante.
* Descripción de los Procedimientos Técnicos empleados, entre ellos, la documentación fotográfica o videográfica, el proceso de extracción de la imagen forense y las actividades adelantadas.
* Cómo y por qué fueron utilizadas las diferentes herramientas y procedimientos para recolectar y analizar la información.
* Se debe tener en cuenta a la entidad o autoridad a presentar el informe, para lo cual se sugiere realizar dos informes, un informe técnico orientado al equipo técnico y/o ingenieros donde se contemple los equipos y herramientas forenses empleados, las técnicas y/o procedimientos, resultados y descripción de hallazgos. Por último, un informe gerencial y/o ejecutivo presentado en un lenguaje coloquial (no técnico) y de menor densidad que el informe técnico.
* Acciones por tomar (si es para remediar algún incidente o crimen), como por ejemplo mejorar determinados controles de seguridad.
* Presentación de resultados y su interpretación, las cuales señalan la información o datos obtenidos frente a la solicitud.

## **Erradicación y Recuperación.**

Después contener el incidente, es necesario realizar actividades de erradicación para eliminar los componentes que fueron empleados para el desarrollo del mismo, las acciones pueden incluir eliminar el código malicioso y remover cuentas de usuario creadas por el atacante. En algunos ataques la erradicación no es necesaria o se realiza durante las actividades de recuperación.

En la fase de recuperación los administradores restauran los sistemas a su operación normal, lo cual puede implicar, restaurar sistemas a partir de copias de seguridad limpias, reconstruir sistemas desde cero, reemplazar archivos comprometidos con versiones limpias, instalación de parches, cambio de contraseñas y ajuste de red seguridad perimetral, si aplica, se realiza el endurecimiento (hardenning) de los equipos para prevenir acciones futuras.

## **Actividad Post Incidente.[[14]](#footnote-14)**

Una de las fases más importantes de la atención a incidentes, es aprender del incidente y mejorar continuamente. Por tal motivo se debe mantener documentación y/o registros que permita conocer exactamente lo que sucedió, en qué momento y cómo el personal gestionó el incidente. Una vez que se hayan finalizado las fases de documentación y recuperación, debemos revisar el proceso minuciosamente, determinar qué pasos se siguieron correctamente y qué errores se cometieron.

Las actividades en esta fase incluyen:

* Escribir el informe de incidente.
* Analizar los problemas encontrados durante la respuesta a incidentes.
* Verificar las herramientas o recursos adicionales son necesarios para detectar, analizar y mitigar los incidentes en el futuro.
* Proponer mejoras basadas en los problemas encontrados.
* Presentación del informe a las partes interesadas pertinentes.

**REVISIÓN Y APROBACIÓN:**

|  |  |  |
| --- | --- | --- |
| **Elaborado y/o Actualizado por:** | **Validado por**  **RESPONSABLE DIRECTIVO del Proceso:** | **Aprobado**  **Representante de la Alta Dirección:** |
| **LUIS ENRIQUE PARIS GARCIA /**  **GLORIA MÉNDEZ**  **Contratista / Proceso EGTI** | Firma: | Firma: |
| **Revisado por:** |
| **ALEXANDER PEREA MENA**  **Contratista/ Proceso DESI** |
| **MARTHA PATRICIA AGUILAR COPETE**  **Secretaría General** | **DIANA MARCELA DEL PILAR REYES TOLEDO**  **Representante de la Alta Dirección** |

**CONTROL DE CAMBIOS:**

|  |  |  |  |
| --- | --- | --- | --- |
| **VERSIÓN** | **DESCRIPCIÓN** | **FECHA** | **APROBADO**  **Representante de la Alta Dirección** |
| 1 | Se implementa la política Gestión de incidentes de seguridad para establecer el proceder para la atención de los incidentes y su utilización como lecciones aprendidas para evitar su ocurrencia. | OCTUBRE 2019 | Jefe Oficina Asesora de Planeación |
| 2 | Se complementan fases de clasificación de incidentes, se modifican roles y responsabilidades, se incorpora medios para el reporte de incidentes, se incorpora manejo de la evidencia digital, se incorpora normatividad, se modifica declaración institucional, establecida en el capítulo 4 del documento. | FEBRERO 2021 | Jefe Oficina Asesora de Planeación |

1. Nist-SP-800-61-R2 Computer Security Incident Handling Guide. [↑](#footnote-ref-1)
2. Nist-SP-800-61-R2 Computer Security Incident Handling Guide. P.26 [↑](#footnote-ref-2)
3. Nist-SP-800-61-R2 Computer Security Incident Handling Guide.P.26 [↑](#footnote-ref-3)
4. Ibidem [↑](#footnote-ref-4)
5. Nist-SP-800-61-R2 Computer Security Incident Handling Guide. P.28 [↑](#footnote-ref-5)
6. Nist-SP-800-61-R2 Computer Security Incident Handling Guide.P.29 [↑](#footnote-ref-6)
7. Nist-SP-800-61-R2 Computer Security Incident Handling Guide. P.32. [↑](#footnote-ref-7)
8. Guía para la Gestión y Clasificación de Incidentes de Seguridad de la Información. P.16. [↑](#footnote-ref-8)
9. Nist-SP-800-61-R2 Computer Security Incident Handling Guide. P.35. [↑](#footnote-ref-9)
10. Nist-SP-800-61-R2 Computer Security Incident Handling Guide. P.46 [↑](#footnote-ref-10)
11. ISO 27037:2012 Guidelines for identification, collection, acquisition, and preservation of digital evidence. [↑](#footnote-ref-11)
12. ISO 27035:2016 Information security incident management [↑](#footnote-ref-12)
13. Evidencia Digital MinTIC. [↑](#footnote-ref-13)
14. Nist-SP-800-61-R2 Computer Security Incident Handling Guide. P.38 [↑](#footnote-ref-14)