Control de Cambios		
Versión	**Fecha**	**Descripción de la Modificación**
1	14/11/2023	Versión inicial

Elaboró	Revisó	Aprobó
Francisco Daza Cardona Contratista Oficina Tecnologías de la Información y las Comunicaciones	Carmenza González Vargas Profesional Universitario Paola Cubides Suarez Contratista Oficina Asesora Planeación	Claudia Marcela Ladino Jefe Oficina Tecnologías de la Información y las Comunicaciones Nelson Jairo Rincón Martínez Jefe Oficina Asesora de Planeación

Tabla de contenido

1. Introducción

Como complemento y en atención a lo dispuesto en el artículo 3° **Política de Seguridad y Privacidad de la Información de la Resolución 419 de 2023**, a través de la cual la alta dirección adquiere el compromiso de implementar, mantener y mejorar el Sistema de Gestión Sistema de Gestión de Seguridad y Privacidad de la información – SGSI alineado a Modelo de Seguridad y Privacidad de la información – MSPI del MinTIC, en la presente Guía se definen los lineamientos y fases para la gestión de incidentes de seguridad de la información en El Instituto Distrital de gestión de Riesgos y Cambio climático – IDIGER, y está dirigida a los funcionarios, contratistas, proveedores de servicios y bienes de la entidad.

2. Objetivo

Establecer los lineamientos para gestionar la identificación, detección, análisis y tratamiento ante la ocurrencia de un incidente de seguridad de manera que se minimice al máximo los posibles impactos adversos que puedan afectar los activos de información de la entidad.

3. Alcance

Desde la etapa de planificación y preparación ante la ocurrencia de un incidente de seguridad de la información hasta la definición de los lineamentos para desarrollar las actividades Post-incidentes.

4. Roles y perfiles necesarios para la atención de incidentes

A continuación, se describen los Roles y perfiles que pueden intervenir ante la ocurrencia de un incidente de seguridad:

- **Usuario sensibilizado**: funcionarios, contratistas o terceros con acceso a la infraestructura de la entidad, con los que se pueden identificar eventos adversos sobre los activos de información, quienes es importante que se encuentre constantemente sensibilizados de la responsabilidad de reportar cualquier situación anormal que pueda llegar a materializarse en un incidente de seguridad de la información.

- **Administrador de sistema:** Profesionales encargados de la configuración, administración de la infraestructura tecnológica de la entidad, quienes deben estar sensibilizados en la identificación, clasificación y escalamiento de los incidentes de seguridad.

- **Administrador de sistema de seguridad:** Profesionales expertos encargados de la configuración, administración de la infraestructura de seguridad perimetral de la entidad, quienes deben estar sensibilizados y capacitados para identificar, analizar, contener y erradicar un incidente de seguridad.

- **Líder Grupo de atención de incidentes:** Profesional de Seguridad de la Información encargado de revisar y evaluar la gestión de incidentes que se presenten en la entidad en atención a la metodología definida.

5. Definiciones

- **Incidente de seguridad de la información**: Evento o serie de eventos de seguridad de la información no deseados o inesperados, que tienen la probabilidad significativa de comprometer las operaciones del negocio y amenazar la seguridad de la información. (GTC-ISO/IEC 27035:2015).

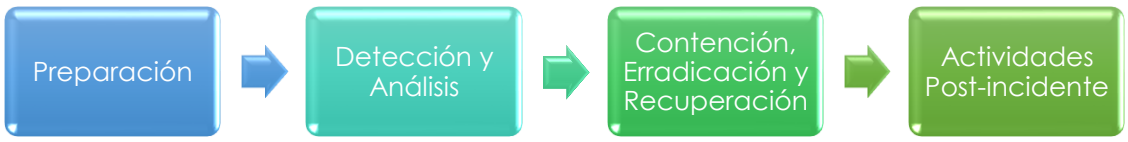
- **Equipo de respuesta a incidentes de seguridad:** Conformado por miembros confiables de la organización, que cuentan con las habilidades y competencias para tratar los incidentes de seguridad durante el ciclo de vida de éstos. (GTC-ISO/IEC 27035:2015).

- **Evento de seguridad de la información:** Presencia identificada de una condición 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 a la seguridad. (GTC-ISO/IEC 27035:2015).

6. Metodología para la gestión de incidentes de seguridad

El modelo de operación de gestión de incidentes *"Guía para la Gestión y Clasificación de Incidentes de Seguridad de la Información"* del MinTIC[1], plantea una serie de etapas para dar cumplimiento con el ciclo de vida de la gestión y respuesta a un incidente de seguridad, así:

Gráfico No. 1 Ciclo de gestión de Incidentes



Fuente: Guía para la Gestión y Clasificación de Incidentes de Seguridad de la Información/MSPI/MinTIC

6.1 Preparación

Esta etapa consiste en crear un esquema a seguir que permita responder de forma adecuada ante una determinada situación, de manera que se pueda detectar y evaluar las posibles vulnerabilidades. En esta etapa es importante que el equipo de respuesta a incidentes identifique los recursos y herramientas disponibles para la

[1]https://gobiernodigital.mintic.gov.co/seguridadyprivacidad/704/articles-150509_G21_Gestion_Incidentes.pdf

atención de los incidentes de seguridad incluyendo las mejores prácticas conocidas para el aseguramiento de los sistemas de información e infraestructura que los soporta. Consiste en eliminar con anterioridad las posibles causas que pueden originar el incidente, en esta etapa se incluye tanto la prevención de los ataques como la preparación para responder a cada uno.

La preparación incluye la aplicación de parches de seguridad, configuración y aseguramiento de las plataformas con el principio de menores privilegio en los servicios prestados, mantener habilitados logs de auditoria en los servidores, entre otros.

Por otra parte, es preciso mantener una gestión constante en la infraestructura de redes y comunicaciones basados en configuración de reglas de seguridad en los equipos y sincronización de estos. La infraestructura debe contar con un antivirus activo y actualizado.

Todos los administradores de plataformas de seguridad e infraestructura deben estar sensibilizados y familiarizados con las políticas y procedimientos relacionados con el uso de redes, sistemas y aplicaciones incorporando estándares de seguridad, lo anterior, permite prevenir la ocurrencia de incidentes de seguridad de la información y la posible materialización de riesgos que afecten la infraestructura de la entidad, así como la integridad, disponibilidad y confidencialidad de la información.

Para minimizar la repercusión de los incidentes es conveniente:

- Establecer claramente y poner en práctica todas las directivas y procedimientos.
- Establecer programas de formación sobre la seguridad de la información, tanto para el personal de tecnología como para los usuarios finales.
- Monitoreo de red, registros y eventos del sistema.
- Gestión de parches de seguridad (Sistemas operativos, bases de datos, software).
- Aseguramiento de plataforma (configuraciones por defecto, hardening).
- Prevención de código malicioso.
- Sensibilización y entrenamiento de usuarios.

Es importante tener en cuenta lo descrito en el Plan de Seguridad y Privacidad de la Información, el Plan de Tratamiento de riesgos de Seguridad y Privacidad de la Información y el Manual de Políticas Complementarias de Seguridad de la Información con los que cuenta el Instituto Distrital de gestión de Riesgos y Cambio climático – IDIGER.

6.2 Comunicación

A continuación, se relacionan elementos importantes para la comunicación del equipo de atención de incidentes.

- **Información de Contacto:**
  Se pueden contactar a la(s) persona(s) de Seguridad de la Información a través del correo seguridaddigital@idiger.gov.co y al teléfono (601) 4292800 Oficina Tic.

- **Información de Escalamiento**: Para el escalamiento de incidentes se debe realizar a través de la persona encargada de seguridad de la información o de Infraestructura o de mesa de servicios de acuerdo con los procedimientos de Soporte Técnico y Gestión de Incidentes de Seguridad de la información con el fin de canalizar los incidentes de seguridad de la información a través de la Oficina TICS.

De requerirse acciones disciplinarias se escalará a través de Talento Humano y el Control Disciplinario Interno.

Política de Comunicación: La entidad a través de https://www.idiger.gov.co/plan-estrategico-de-comunicaciones y de los canales oficiales de comunicación informará de ser pertinente información relacionada con los incidentes que se puedan presentar en la entidad como medida de prevención.

Es importante contar con la información actualizada de contacto de proveedores de servicios, soporte especializado, encargados de la infraestructura, administradores de redes y seguridad con el fin de garantizar el

contacto oportuno ante la generación de un evento de seguridad de la información. Ante una vulneración o compromiso de elementos de la infraestructura tecnológica, aplicaciones o sistemas de la entidad deberá reportarse el hecho a ColCERT- Grupo de Respuesta a Emergencias Cibernéticas de Colombia.

Contacto con áreas interesadas o grupos de interés como primer canal de atención:

- https://cc-csirt.policia.gov.co/
- http://www.colcert.gov.co/

6.3 Hardware y Software

De acuerdo con lo descrito en la *"Guía para la Gestión y Clasificación de Incidentes de Seguridad de la Información"* del MinTIC[2], para una adecuada gestión de los incidentes de seguridad es importante tener en cuenta elementos como analizadores de protocolos, software de recolección de evidencias, kit de respuesta a incidentes, medios de almacenamiento, entre otros. También se puede apoyar en los proveedores de productos de ciberseguridad para la entidad.

[2]https://gobiernodigital.mintic.gov.co/seguridadyprivacidad/704/articles-150509_G21_Gestion_Incidentes.pdf

6.4 Recursos para el análisis de incidentes

De igual forma para realizar un correcto análisis de los incidentes la "*Guía para la Gestión y Clasificación de Incidentes de Seguridad de la Información*" del MinTIC, recomienda contar con:

- Listado de los puertos conocidos y de los puertos utilizados para realizar un ataque. Ver listado de puertos conocidos[3].
- Diagrama de red para tener la ubicación rápida de los recursos existentes.
- Base de Información de: Servidores (Nombre, IP, Aplicaciones, Parches, Usuarios Configurados, responsable de cambios). Esta información siempre debe estar actualizada para poder conocer el funcionamiento normal del mismo y realizar una identificación más acertada de un incidente.
- Análisis del comportamiento de red estándar en este es recomendable incluir: puertos utilizados por los protocolos de red, horarios de utilización, direcciones IP con que generan un mayor tráfico, direcciones IP que reciben mayor número de peticiones.

Como la anterior información está catalogada como reservada en la entidad, se encontrará disponible a solicitud, por los equipos de trabajo y podrá ser consultada por el personal técnico autorizado de presentarse la necesidad de análisis de incidentes de seguridad.

Los miembros del equipo de respuesta a incidentes deben tener definidas claramente sus tareas para asegurar que no quede ningún área sin cubrir. Como se indicó en el apartado 6.1.1 Comunicación Información de contacto, es importante poder contactar al equipo de seguridad del IDIGER y de proveedores relacionados con el incidente.

Los actores que intervienen en la atención de un incidente de seguridad son:

- Equipo de Infraestructura y Redes.
- Equipo de Sistemas de Información y Bases de Datos.
- Responsable Seguridad de la Información.
- Jefe Oficina TIC
- Usuarios internos que se requieran (Contratistas, funcionarios y visitantes).

El equipo realizará las siguientes actividades:

- Supervisar los sistemas en busca de vulnerabilidades de seguridad.
- Servir como punto central de comunicación, tanto para recibir los informes de incidentes de seguridad como para difundir información esencial sobre los incidentes a las entidades correspondientes.
- Documentar y catalogar los incidentes de seguridad.
- Aumentar el nivel de conciencia y sensibilización con respecto a la seguridad dentro del Idiger.

[3] https://www.ionos.es/digitalguide/servidores/know-how/puertos-tcp-puertos-udp/

- Posibilitar la auditoria de sistemas y redes mediante procesos como la evaluación de vulnerabilidades y pruebas de penetración.
- Obtener más información sobre las nuevas vulnerabilidades y estrategias de ataque empleadas por los atacantes.
- Investigar acerca de nuevas revisiones de software.
- Analizar y desarrollar nuevas tecnologías para minimizar los riesgos y vulnerabilidades de seguridad.
- Perfeccionar y actualizar continuamente los sistemas y procedimientos actuales.

6.5 Recursos para la mitigación y remediación

Como elementos básicos para la contención de un incidente de seguridad es importante contar con copias y respaldo de la información, imagen de los servidores y cualquier otro elemento identificado como relevante que permita el restablecimiento de la operación y funcionamiento de un sistema o plataforma.

En el Instituto Distrital de Gestión de Riesgos y Cambio climático – IDIGER, los respaldos de información de los activos críticos se realizan y se almacenan en un lugar seguro, los cuales son consultados y utilizados por el personal técnico autorizado.

6.6 Detección y Análisis

En esta etapa es importante identificar las características de un ataque, verificar lo que realmente ha sucedido y en el caso afirmativo, determinar su tipo y magnitud. No es fácil en todos los casos determinar con precisión si se ha producido o no un incidente de seguridad de la información y si es así, identificar su tipo y evaluar su peligrosidad.

La correcta detección de un incidente de seguridad se realiza mediante diferentes fuentes: Antivirus, reportes de usuarios, monitoreo de la infraestructura tecnológica, logs y Alertas en los equipos de Seguridad Perimetral (Firewall) entre otros.

En el Instituto Distrital de Gestión de Riesgos y Cambio climático – IDIGER, la infraestructura se monitorea a diario por parte del equipo de Infraestructura el cual permite alertar ante la ocurrencia de incidentes o fallos en la plataforma tecnológica.

6.7 Identificación de la gravedad del incidente

Para poder recuperarse de forma eficaz de un ataque, se debe determinar la gravedad de la situación de peligro que han sufrido los sistemas.

Debemos determinar:

- La naturaleza del ataque.
- El punto de origen.
- La intención del ataque estaba dirigido específicamente a la entidad para conseguir información concreta o se trata de un ataque aleatorio.

- Accesos no autorizados
- Infraestructura afectada

6.8 Reporte de eventos e incidentes de seguridad de la información

La recepción de incidentes de seguridad a partir del personal de la entidad o de entes externos se realiza a través del correo seguridaddigital@idiger.gov.co Todo incidente se debe registrar y documentar su solución.

6.9 Análisis y evaluación del incidente

Para realizar el análisis de un incidente es importante tener conocimiento de las lecturas normales y comportamiento de la red, los sistemas y elementos de la infraestructura.

Es importante contar con logs de los sistemas de información, aplicaciones, servidores de manera que pueda llegar a realizarse una correlación de eventos para identificar posibles patrones o comportamientos anormales que permitan determinar la causa de un incidente.

Es preciso contar con una única fuente de tiempo, es decir que todos los equipos estén sincronizados con sus relojes para facilitar el análisis y correlación de eventos.

6.10 Clasificación de incidentes de seguridad

A continuación, se identifican algunos incidentes que pueden ocasionar situación de seguridad:

Tabla 1. Incidentes de Seguridad

CLASIFICACION DE INCIDENTES DE SEGURIDAD		
Clase de Incidente	**Descripción**	**Tipo de ataque**
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	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.
		(Scanning).
		Sniffing.
		Ingeniería social.
		Phishing.
Abuso/uso inadecuado de	Este tipo de incidentes ocurre cuando un usuario viola las políticas de seguridad del	Descargar e instalar herramientas para piratería informática.

CLASIFICACION DE INCIDENTES DE SEGURIDAD		
Clase de Incidente	**Descripción**	**Tipo de ataque**
sistemas de información	sistema de información de la organización. Ataques dirigidos a dañar la imagen de la organización o a utilizar sus medios electrónicos para otros usos ilícitos.	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 legitimas.
		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 la denegación del 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.	Defacement (desfiguración).
		Cross-Site Scripting (XSS).
		Cross-Site Request Forgery (CSRF).
		Falsificación de petición entre sitios cruzados.
		Inyección SQL.
		Spear Phishing.

CLASIFICACION DE INCIDENTES DE SEGURIDAD		
Clase de Incidente	**Descripción**	**Tipo de ataque**
		Pharming.
		Ataque de fuerza bruta
		Inyección de Archivos Remota
		Explotación de vulnerabilidad software
		Explotación de vulnerabilidad hardware

Fuente: Elaboración propia

6.11 Evaluación de los incidentes

Con el fin de realizar la evaluación de un incidente, es necesario identificar el nivel de criticidad e impacto de este, de acuerdo con el análisis realizado, el tipo de riesgo y la clasificación de los activos afectados, de acuerdo con lo descrito en la *Guía para la Gestión y Clasificación de Incidentes de Seguridad de la Información del MinTIC*[4] a continuación se presentan la Criticidad, Impacto y prioridad dadas para un incidente:

Nivel de Criticidad depende del valor o importancia dentro del IDIGER, del proceso que soporta y el o los sistemas afectados. Con el fin de permitir una atención adecuada a los incidentes (análisis, contención y erradicación).

Tabla 2. Niveles de Criticidad

Nivel Criticidad	Valor	Descripción
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 dependencias 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 (de acuerdo con el análisis de los activos de información de TI).

Fuente: Elaboración propia

El **nivel de impacto** de un incidente depende del valor o importancia dentro del IDIGER, del proceso que soporta y el o los sistemas afectados. Con el fin de permitir una atención adecuada a los incidentes (análisis, contención y erradicación).

[4]https://gobiernodigital.mintic.gov.co/seguridadyprivacidad/704/articles-150509_G21_Gestion_Incidentes.pdf

Tabla 3. Niveles de Impacto Actual y Futuro

Nivel Impacto	Valor	Definición
Inferior	0,10	Impactó leve: Si el hecho llegara a presentarse, tendría consecuencias o efectos mínimos sobre la entidad y no se vería afectado en su continuidad de cualquier sistema de información o estación de trabajo.
Bajo	0,25	Impacto Bajo: Si el hecho llegara a presentarse, tendría bajo impactó o efecto sobre la entidad y se vería afectado en su continuidad de manera mínima de cualquier sistema de información o estación de trabajo.
Medio	0,50	Impactó Medio: Si el hecho llegara a presentarse, tendría medianas consecuencias o efectos sobre la entidad y se vería afectado en su continuidad de manera moderada de cualquier sistema de información o estaciones de trabajo.
Alto	0,75	Impacto Alto: Si el hecho llegara a presentarse, tendría altas consecuencias o efectos sobre la entidad y se vería afectado en su continuidad de manera considerable interrumpiendo periódicamente los sistemas de información o estaciones de trabajo.
Superior	1,00	Impacto catastrófico: Si el hecho llegara a presentarse, tendría desastrosas consecuencias o efectos sobre la entidad y se vería afectado en su continuidad de manera total en los sistemas de información o estaciones de trabajo.

Fuente: Elaboración propia

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.

6.12 Priorización y Tiempos de respuesta

Luego de tener definidas las variables de criticidad e impacto se obtiene la prioridad mediante la siguiente formula:

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

De acuerdo con lo definido en la *Guía para la Gestión y Clasificación de Incidentes de Seguridad de la Información"* del MinTIC[5] para la atención de incidentes de seguridad es necesario contar con unos tiempos máximos de atención con el fin de atender adecuadamente los incidentes de acuerdo con su criticidad e impacto. A continuación, se presentan unos tiempos máximos en que el incidente debe ser atendido, y no al tiempo en el cual el incidente debe ser solucionado. Esto se debe a que la solución de los incidentes puede variar dependiendo del caso.

[5]https://gobiernodigital.mintic.gov.co/seguridadyprivacidad/704/articles-150509_G21_Gestion_Incidentes.pdf

Tabla 4. Tiempo Máximo de atención de incidentes

Nivel Prioridad	Valor	Tiempo de Respuesta
Inferior	00,00 - 02,49	64 horas
Bajo	02,50 - 03,74	32 horas
Medio	03,75 - 04,99	16 horas
Alto	05,00 - 07,49	8 horas
Superior	07,50 – 10,00	4 horas

Fuente: Elaboración propia

6.13 Declaración y notificación de incidentes

Teniendo en cuenta que un incidente de seguridad puede ser el acceso, manipulación, transformación, divulgación no autorizada de información o disposición de recursos tecnológicos que atentan contra la correcta operación de la entidad, es preciso poner en conocimiento o notificar un incidente permite responder a tiempo y minimizar su impacto, facilitando la recuperación rápida de una posible pérdida de información o servicios de TI.

Es así que ante la sospecha de un incidente de seguridad deberá notificarse al responsable de seguridad de la información a través del @idiger.gov.co, quien

se encargará de realizar el seguimiento correspondiente hasta su cierre definitivo.

7. Contención, Erradicación y Recuperación

La **contención** es una estrategia que permite proteger los activos de información, sistemas y redes limitando el daño, en esta fase se detecta el incidente con el fin de que no se propague y pueda generar más daños a la información o a la infraestructura tecnológica.

A través de la contención se 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 ha contenido el incidente es necesario realizar la eliminación y **erradicación** de los elementos que dieron origen al mismo, como por ejemplo un código malicioso, para posteriormente restablecer la funcionalidad y operación que se haya visto afectada.

Posteriormente se realizará la **recuperación**, es decir, devolver los sistemas afectados por el incidente a su estado operativo. También contempla la eliminación de los componentes que han provocado el incidente, igualmente es muy importante que en la entidad se implemente un PLAN DE CONTINUDIDAD DE NEGOCIO DE TI.

Tabla 5. Estrategia de contención, erradicación y recuperación

Incidente	Ejemplos de incidentes	Nivel Criticidad	Nivel Impacto	Estrategia de contención	Estrategia de erradicación y recuperación
Código malicioso (Malware)	virus, gusanos, troyanos, spyware, rootkit, ransomware (secuestro informático), códigos móviles y combinaciones de estos.	Alto	Superior	Desconexión de la red del equipo afectado.	Corrección de efectos producidos. Restauración de backup, reinstalación del equipo y recuperación de datos.
Robo de información	Robo de información digital (Carpetas, bases de datos).	Superior	Superior	Desconectar el recurso compartido.	Recuperación de datos a partir de copias de seguridad.
	Identificación de vulnerabilidades.				
	(Scanning).				
	Sniffing.				
	Ingeniería social.				
	Phishing.				
Abuso/uso inadecuado de sistemas de información	Descargar e instalar herramientas para piratería informática.	Alto	Alto	Uso de políticas de seguridad de información.	Aplicación de nuevas reglas en firewalls.
	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 compañeros para adquirir o distribuir archivos piratas (música, video, software).				
Borrado (compromiso) de información	Acceso no autorizado a información.	Superior	Alto	Desconectar el recurso compartido. Suspender o eliminar la publicación no autorizada.	Recuperación de datos.
	Modificación y borrado no autorizada de información.				
	Publicación no Autorizada de información.				
Acceso no autorizado	Intentos por recuperar archivos de contraseñas.	Alto	Alto	Apagado del sistema.	Cambios de contraseñas. Aplicación de nuevas reglas en firewalls.
	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 legitimas.				

Incidente	Ejemplos de incidentes	Nivel Criticidad	Nivel Impacto	Estrategia de contención	Estrategia de erradicación y recuperación
	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 la denegación del servicio distribuido (DDoS) (Disponibilidad)	Robo, daño intencionado y destrucción de equipos.	Superior	Superior	Desconexión de la red del equipo afectado.	Restitución del servicio caído.
	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	Compromiso cuenta de usuario.	Alto	Alto	Incorporación de reglas de filtrado en el firewall.	La reinstalación de parches o la aplicación de nuevas reglas en firewalls. Reparar el sitio web.
	Defacement (desfiguración).				
	Cross-Site Scnpting (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

8. Actividades Post- incidente

El equipo de respuesta de incidentes debe documentar, minuciosamente, todos los procesos al tratar con un incidente. Se debe incluir una descripción de la infracción y detalles de cada acción tomada (quién llevo a cabo la acción, cuando lo hizo y por qué motivos), para tal caso se debe tener el soporte digital.

Una de las partes más importantes de un plan de respuesta a incidentes de tecnología es aprender del incidente y procurar la mejora continua. 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 la documentación y recuperación, es preciso revisar el proceso minuciosamente para determinar qué pasos se siguieron correctamente y que 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.