PROCEDIMIENTO DE GESTIÓN DE INCIDENTES

Defensoría del Consumidor Financiero Laguado Giraldo

CONTENIDO

TABLA DE ILUSTRACIONES

ALCANCE

Para LA DEFENSORÍA DEL CONSUMIDOR FINANCIERO LAGUADO GIRALDO, la gestión de incidentes de Seguridad tiene un enfoque estructurado y planificado que facilite su correcto manejo, garantizando la confidencialidad, integridad y disponibilidad, de la información como parte del proceso de mejora continua de la Seguridad de la Información.

Para ello, se diseña el procedimiento de atención para la gestión de incidentes según la categorización y tipo de prioridad, lo que permite detectar, registrar y clasificar, asignar el personal encargado de la solución de éstos y dar rápida respuesta a aquellas partes interesadas.

OBJETIVO

Describir el proceso para la gestión de incidentes con el fin de proveer al personal implicado una guía de los pasos que se deberán seguir para su reporte, seguimiento, consulta, tiempos de respuesta, entre otros.

Para lograrlo, la Defensoría debe asegurar lo siguiente:

- Garantizar la operatividad de los sistemas.
- Mejorar la productividad de los usuarios.
- Cumplimiento de los niveles de servicio acordados con clientes y partes interesadas.
- Mayor control de los procesos y monitoreo del servicio.
- Optimización de los recursos disponibles.
- Una base de datos de conocimiento más precisa pues en ella se registran los incidentes.
- Mejorar la satisfacción general de clientes, partes interesadas y usuarios.

GLOSARIO

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.

CONFIDENCIALIDAD: Propiedad que determina que la información no esté disponible ni sea revelada a individuos, entidades o procesos no autorizados.

DISPONIBILIDAD: Propiedad que determina que la información sea accesible y utilizable a solicitud de una entidad autorizada.

EVENTO: Una alerta o notificación creada por algún componente de la plataforma tecnológica de la información o herramienta de monitoreo.

INCIDENTE DE SEGURIDAD DE LA INFORMACIÓN: Se define como un acceso, intento de acceso, uso, divulgación, modificación o destrucción no autorizada de información; un impedimento en la operación normal de las redes, sistemas o recursos informáticos; o una violación a la Política de Seguridad de la Información de LA DEFENSORÍA.

INTEGRIDAD: Propiedad de salvaguardar la exactitud y estado completo de los activos de información.

LOG: Es el registro de las acciones y de los acontecimientos que ocurren en un sistema computacional cuando un usuario o proceso está activo y sucede un evento que está configurado para reportar.

PROCEDIMIENTO: Los procedimientos, definen específicamente como las políticas, estándares, mejores prácticas y guías que serán implementadas en una situación dada. Los procedimientos son independientes de la tecnología o de los procesos y se refieren a las plataformas, aplicaciones o procesos específicos. Son utilizados para delinear los pasos que deben ser seguidos por una dependencia para implementar la seguridad relacionada con dicho proceso o sistema específico. Generalmente los procedimientos son desarrollados, implementados y supervisados por el dueño de un proceso o del sistema, los procedimientos seguirán las políticas de la organización, los estándares, y las mejores prácticas tan cerca cómo les sea posible, y a la vez se ajustarán a los requerimientos procedimentales o técnicos establecidos dentro de la dependencia donde ellos se aplican.

SEGURIDAD DE LA INFORMACIÓN: La Seguridad de la Información incluye tres dimensiones principales: Confidencialidad, Disponibilidad e Integridad. La Seguridad de la información involucra la aplicación y gestión de las medidas apropiadas de seguridad que tengan en cuenta un amplio rango de amenazas. La seguridad de la información es alcanzada por medio de la implementación de un conjunto aplicable de controles, seleccionados por medio de un proceso de gestión de riesgos y gestionados usando un Sistema de Gestión de Seguridad de la Información, incluyendo políticas, procesos, procedimientos, estructuras organizacionales, software o hardware para proteger los activos de información identificados.

DIAGRAMA DE FLUJO DEL PROCESO

El siguiente diagrama de flujo, detalla las actividades descritas durante el procedimiento:

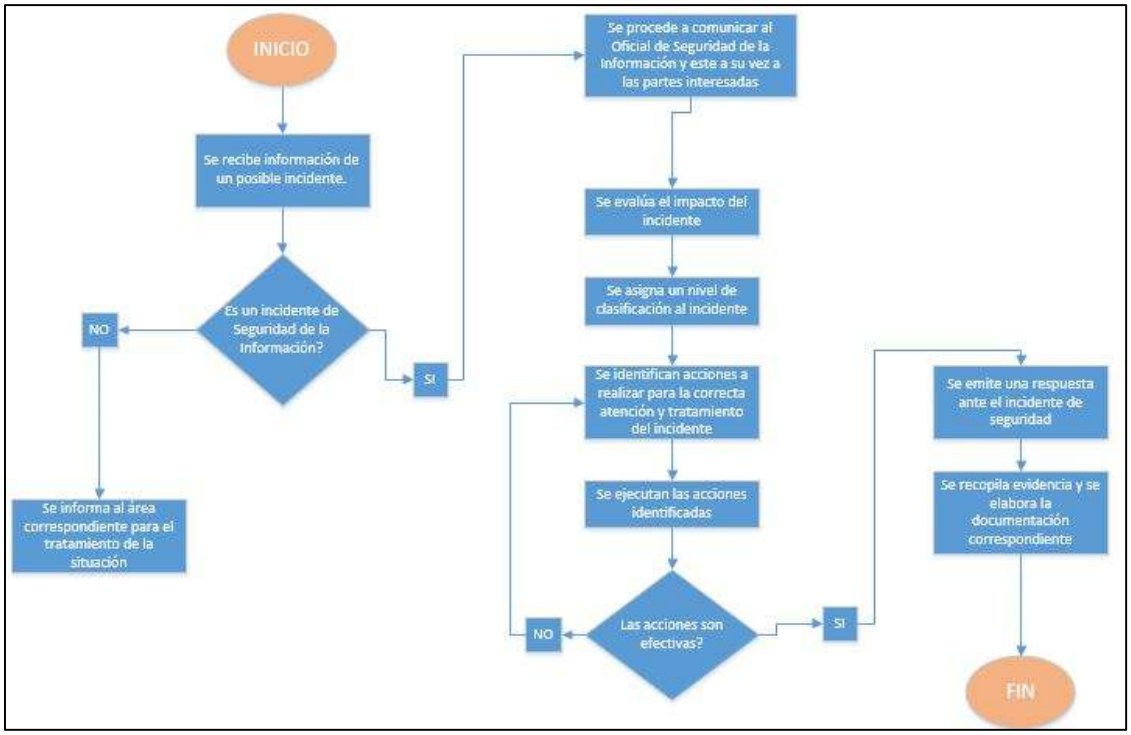

Figura 1 - Diagrama de flujo del Procedimiento de Gestión de Incidentes. Fuente PROPIA

PROCEDIMIENTO DE GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN:

Este procedimiento contiene indicaciones acerca de cómo deberá responder LA DEFENSORÍA en caso de presentarse algún incidente que afecte la Confidencialidad, Integridad o Disponibilidad, de su operación.

Deberán especificarse los roles, las responsabilidades y acciones requeridas para identificar, contener, documentar, recolectar evidencias y mejorar la respuesta ante un incidente de seguridad de la información, así mismo, deberá indicar en qué casos sería necesario pasar a la activación de los Planes de Continuidad (DRP) existentes, dependiendo de la criticidad asignada.

La notificación oportuna de los incidentes permitirá responder a los mismos eficientemente, reducir su probabilidad de ocurrencia, facilitar una recuperación

rápida y eficiente de las actividades, reducir la pérdida de información y la interrupción de los servicios.

PREPARACION

En esta etapa, LA DEFENSORÍA crea un modelo de respuesta ante incidentes, y también la forma en cómo éstos pueden ser detectados, evaluados y gestionar las vulnerabilidades para prevenirse, asegurando que los sistemas de información, redes, y aplicaciones son lo suficientemente seguros.

Las actividades descritas a continuación buscan prevenir la ocurrencia de incidentes de seguridad de la información que esta soportada por TI:

- **Seguridad en redes**: Se realiza una gestión constante sobre los elementos de seguridad.
  - Las configuraciones en equipos de seguridad como firewalls, switches, routers o módems u otros equipos de telecomunicaciones deberán ser revisadas con regularidad.
- **Prevención de código malicioso**: Todos los equipos de la infraestructura (ya sean servidores y/o equipos de usuarios propios o de terceros) tienen activo su antivirus y antimalware con las firmas de actualización al día.
- **Sensibilización y concientización de usuarios**: Todos los empleados en LA DEFENSORÍA han sido sensibilizados de acuerdo con las políticas y procedimientos existentes relacionados con el uso apropiado de redes, sistemas y aplicaciones en concordancia con los estándares de seguridad de la compañía. El rol encargado de la Seguridad de la Información establecerá las necesidades de capacitación de las personas encargadas de la protección de los datos.
- **Aseguramiento de plataformas**: Las plataformas utilizadas en LA DEFENSORÍA deberán ser aseguradas correctamente en los siguientes aspectos.
  - Validar la configuración de la menor cantidad de servicios (principio de menor privilegio) con el fin de proveer únicamente aquellos servicios necesarios tanto a usuarios como a otros equipos.
  - Revisión de configuraciones por default (usuarios, contraseñas y archivos compartidos por la nube, si aplican). Cada recurso que pueda ser accedido por externos, de existir, e incluso por usuarios internos deberá desplegar alguna advertencia.
  - Los servidores o aplicaciones en la nube deberán tener habilitados sus sistemas de auditoría para permitir visualizaciones de logs de eventos.

GESTIÓN DE LOGS Y AUDITORÍA

Se refiere a que los sistemas de información y aplicaciones del negocio cuenten con registros de auditoría, lo que permitirá a LA DEFENSORÍA cumplir con regulaciones, realizar investigaciones puntuales y verificar la veracidad de incidentes de seguridad.

Para esto se deben definir actividades que permitan disponer de estos y su correspondiente almacenamiento.

- **Activación de logs de auditoría:** Garantizar que todos los sistemas de información local o en la nube, sistemas operacionales, bases de datos, dispositivos de seguridad y/o servidores, deben contar con los logs o rastros de auditoria que registren las actividades de los usuarios, las excepciones, las fallas y eventos de seguridad. Es decir, logs y permisos autorizados en los servicios en la nube como dispositivos autorizados en los servicios de almacenamiento.
  - Es responsabilidad de los propietarios estar pendientes de la activación de los logs de auditoria.
  - El líder funcional o administrador del sistema de información (local o en la nube) deberá mantener un inventario periódico de los registros de auditoria existentes por aplicación y su ubicación.
- **Planes de respaldo de la información:** Adicionar a las políticas de respaldo de los Sistemas de Información (local o en la nube), los logs de estos y de los dispositivos que componen la infraestructura.
  - Elaboración del plan de copia de respaldo (backup) y restauración.
  - Revisión periódica de los planes de backup y restauración.
- **Verificación de logs:** Elaborar, conservar y revisar periódicamente los registros acerca de las actividades de los usuarios, excepciones, fallas, y eventos de seguridad de la información.
  - Es responsabilidad de los propietarios de la información (local o en la nube), solicitar y conocer que eventos se han producido sobre los sistemas de tratamiento de su información.
  - Es responsabilidad de quien ejerza el rol de administrador de los sistemas de información (local o en la nube), proveer la información de eventos solicitada por los usuarios.
- **Respaldo y restauración de logs:** Es responsabilidad de quien ejerza el rol de administrador de los sistemas de información (local o en la nube), establecer un plan de respaldo de logs de auditoria por medio de la herramienta con que se cuente, teniendo en cuenta todos los componentes de la plataforma tecnológica de producción.
  - Se deben establecer directrices de retención, respaldo y recuperación de los logs y registros de auditorías de los componentes de la plataforma tecnológica cuando aplique, ya que estos se constituyen en evidencia para la identificación de un incidente de seguridad.

- Configurar la rotación de logs automáticamente en la herramienta con que se cuente ya que ella debe consolidar la información de los logs de equipos y/o dispositivos que tenga configurados, si es posible, de lo contrario garantizar que no se pierda, ni se sobrescriba los archivos de los logs.
- De acuerdo con las directrices de retención, respaldo y recuperación, aplicar el borrado de los registros de logs consolidados en la herramienta utilizada para el respaldo de logs de auditoria.

Se generarán mensualmente consolidados estadísticos de logs y registros de auditoría.

Figura 2 - Gestión de logs

DETECCION DE INCIDENTES DE SEGURIDAD

Los indicadores son los eventos que nos señalan que posiblemente un incidente ha ocurrido generalmente algunos de estos elementos son:

- Alertas de seguridad
- Reportes de empleados:
  - Los empleados de LA DEFENSORÍA pueden realizar reportes de incidentes de seguridad directamente al correo designado por la Gerencia General o del Oficial de Seguridad de la Información, adjuntando la información solicitada en el formulario destinado para ese fin.
- Informes de Software antivirus o de plataformas de monitoreo constante.
- Otros funcionamientos fuera de lo normal de los sistemas de información (local o en la nube).

Entre los elementos que permitirán dar alerta sobre la futura ocurrencia del mismo y preparar procedimientos para minimizar su impacto se encuentran:

- Logs de aplicaciones
- Logs de herramientas de seguridad de los sistemas de información (local o en la nube)
- Cualquier otra herramienta que permita la identificación de un incidente de seguridad

ANALISIS DE INCIDENTES DE SEGURIDAD

Las actividades de análisis de un incidente reportado mediante el formulario establecido para ello, involucran otra serie de componentes. LA DEFENSORÍA tendrá en cuenta los siguientes:

- Tener conocimientos de las características normales a nivel de red y de los sistemas.
- Quien ejerza el rol de administrador de los sistemas de información (local o en la nube) debe tener conocimiento total sobre los comportamientos de la Infraestructura.
- Toda información que permita realizar análisis al incidente debe estar centralizada (Logs de servidores, redes, sistemas de información (local o en la nube)).
- 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 de un 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.

EVALUACION Y CLASIFICACIÓN DE INCIDENTES

Para realizar la evaluación de un incidente de seguridad LA DEFENSORÍA tendrá 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.

CLASIFICACIÓN

La severidad del incidente de acuerdo a su impacto correspondiente puede ser:

Alto	El incidente de seguridad afecta a activos de información considerados de impacto catastrófico y mayor que influyen directamente a los objetivos misionales de la LA DEFENSORÍA. 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 y dependiendo del caso, los descargos correspondientes ameritarán o no un proceso disciplinario.
Medio	El incidente de seguridad afecta a activos de información considerados de impacto moderado que influyen directamente a los objetivos de un proceso determinado
Bajo	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

TIPOS DE INCIDENTES

De acuerdo a su infraestructura, sus riesgos y criticidad de los activos, LA DEFENSORÍA basará la clasificación de incidentes en los siguientes aspectos:

TIPO	OBSERVACION	TIEMPO DE RESPUESTA
Acceso no autorizado	Es un incidente que involucra a una persona, sistema de información (local o en la nube) o código malicioso que obtiene acceso lógico o físico sin autorización adecuada del dueño del proceso a un sistema de información (local o en la nube) o un activo de información	INMEDIATO
Uso inapropiado de recursos	Un incidente que involucra a una persona que viola alguna política de uso de recursos	1 HORA
Multicomponente	Un incidente que involucra más de una categoría anteriormente mencionada	INMEDIATO
Modificación de recursos no autorizado	Un incidente que involucra a una persona, sistema de información (local o en la nube) o código malicioso que	INMEDIATO

	afecta la integridad de la información	
No disponibilidad de los recursos	Un incidente que involucra a una persona, sistema de información (local o en la nube) o código malicioso que impide el uso autorizado de un activo de información	INMEDIATO
Otros	Un incidente que no puede clasificarse en alguna de las categorías anteriores. Este tipo de incidentes debe monitorearse con el fin de identificar la necesidad de crear nuevas categorías	DE ACUERDO A VALORACION DE IMPACTO

Existen muchas formas más de clasificar los incidentes, y para establecer la clasificación es necesario considerar dos parámetros:

- **Impacto**: es el daño que se causa en la LA DEFENSORÍA.
- **Urgencia**: velocidad con la que la LA DEFENSORÍA necesita corregir el incidente.

La intersección de los parámetros permite establecer la prioridad de cada incidente, por lo que de esta forma se procede a generar la siguiente tabla de valores:

		IMPACTO		
		Alta	Media	Baja
URGENCIA	Alta	1	2	3
	Media	2	3	4
	Baja	3	4	5

Figura 3 - Clasificación de incidentes. Fuente LA DEFENSORÍA

La figura indica que aquellos incidentes de valor 1 son críticos ya que la relación entre la urgencia y el impacto son elevados, por lo que se establece que lo mejor es obtener valores 2, 3, 4 o 5.

En cuanto a la ***priorización*** y con el fin de permitir una atención adecuada a los incidentes (análisis, contención y erradicación) se debe determinar el nivel de prioridad del mismo, y de esta manera **atenderlos adecuadamente según la necesidad**. Ésta depende del valor o importancia dentro de la entidad y del proceso que soporta el o los sistemas afectados.

EQUIPO DE ATENCIÓN DE INCIDENTES

LA DEFENSORÍA conformará un equipo de atención de incidentes de seguridad **CSIRT** (Computer Security Incident Response Team, Equipo de Respuesta ante Incidentes de Seguridad, Comité de Crisis) o un grupo que haga sus veces, enfocado principalmente en **atender los incidentes de seguridad de la información,** que se presentan sobre los activos soportados por su plataforma tecnológica y reportados por los empleados mediante el establecido para tal fin, se encargaran de definir los procedimientos a la atención de incidentes, realizar la atención, manejar las relaciones con entes internos y externos, definir la clasificación de incidentes, y además de esto se encargaran de lo siguiente:

- **Detección de Incidentes de Seguridad**: Monitorear y verificar los elementos de control con el fin de detectar un posible incidente de seguridad de la información.
- **Atención de Incidentes de Seguridad**: Recibe y resuelve los incidentes de seguridad de acuerdo con los procedimientos establecidos.
- **Recolección y Análisis de Evidencia Digital**: Toma, preservación, documentación y análisis de evidencia cuando sea requerida.
- **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).
- **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.
- **Certificación de 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.
- **Clasificación y priorización de servicios expuestos**: Identificación de servicios sensibles y aplicaciones expuestas para la prevención o remediación de ataques.
- **Investigación y Desarrollo**: Deben 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.

RECURSOS PARA LA GESTIÓN DE INCIDENTES

COMUNICACIÓN

Los siguientes son los recursos que son necesarios para la comunicación del equipo de atención de incidentes en LA DEFENSORÍA:

- **Formulario de reporte**: Cada incidente debe ser registrado y/o reportado en el formato establecido para tal fin.
- **Información de Contacto**: Se debe tener una lista de información de contacto de cada una de las personas que conforman el grupo de gestión de incidentes o quienes realicen sus funciones.
- **Información de Escalamiento**: Se debe contar con información de contacto para el escalamiento de incidentes según la estructura de LA DEFENSORÍA.
    - Información de los administradores de la plataforma tecnológica o quien ejerza el rol de administrador de los sistemas de información (local o en la nube)
    - Contacto con el área de recursos humanos o quien realice sus funciones (por si se realizan acciones disciplinarias).
    - Contacto con áreas interesadas o grupos de interés.
- **Política de Comunicación**: LA DEFENSORÍA deberá contar con una política de comunicación de los incidentes de seguridad para definir qué incidente puede ser comunicado a los medios y cual no.
- **Respuesta a incidentes**: De acuerdo a la criticidad del incidente y su clasificación, éste tendrá los tiempos de respuesta como se indica al inicio de esta sección.

HARDWARE Y SOFTWARE

Para una correcta y eficiente gestión de incidentes de alto nivel, LA DEFENSORÍA debería tener en cuenta los siguientes elementos:

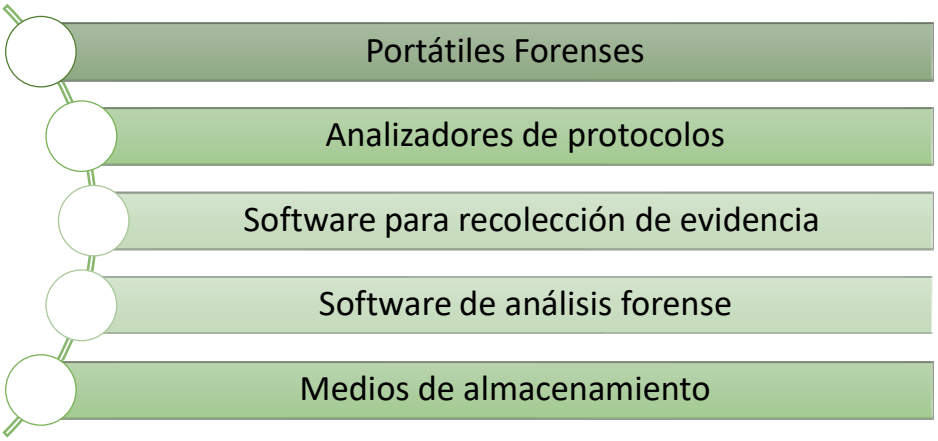

Figura 4 - Elementos de hardware y software

RECURSOS PARA EL ANÁLISIS DE INCIDENTES

- Tener un listado de los puertos conocidos y de los puertos utilizados para realizar un ataque.
- Tener la ubicación rápida de los recursos de red existentes.
- Una Línea – 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.
- Se debe tener un análisis del comportamiento de red estándar para el cual es se incluirá información como: 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.

RECURSOS PARA LA MITIGACIÓN Y REMEDIACIÓN

En este punto se consideran todos los elementos básicos para la contención de un posible incidente, Backup de Información, y cualquier información base que pueda recuperar el funcionamiento normal del sistema:

CONTENCIÓN ERRADICACIÓN Y RECUPERACIÓN

Es importante para LA DEFENSORÍA implementar una estrategia particular por cada proceso, que permita tomar decisiones oportunamente para evitar la propagación del incidente y así disminuir los daños a los recursos de TI y la pérdida de la confidencialidad, integridad y disponibilidad de la información.

Contención	Esta actividad buscará 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, se documentará la estrategia de contención previamente definida para poder tomar decisiones, por ejemplo: desconectar red, deshabilitar servicios.
Erradicación y Recuperación	Después de que el incidente ha sido contenido se deberá 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 el personal encargado deberá restablecer la funcionalidad de los sistemas afectados, y

	realizar un endurecimiento del sistema que permita prevenir incidentes similares en el futuro. Se dejará registro de la estrategia y resultados de la erradicación y recuperación en la carpeta designada para tal fin.

LECCIONES APRENDIDAS

LA DEFENSORÍA mantendrá un proceso de "lecciones aprendidas" después de un incidente grave, y periódicamente después de los incidentes menores. Dependiendo de la clasificación del incidente, se evaluarán las mejoras en las medidas de seguridad y el proceso de gestión de incidentes, para lo cual se detalla que el registro de lecciones aprendidas contendrá la siguiente información:

- Exactamente lo que sucedió, en qué momento y cómo el personal gestionó el incidente.
- Los procedimientos documentados.
- 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.

DOCUMENTACIÓN Y RESULTADOS

En esta etapa se realiza una descripción detallada de los hallazgos relevantes al caso y la forma como fueron encontrados, apoyándose en la documentación continua de la aplicación metodológica.

REPORTE
Se procede a presentar toda la información, reporte de incidente existente en el formato para tal fin y evidencias obtenidas de las etapas anteriores.

Para la elaboración de un reporte, se considerará tener en cuenta los siguientes aspectos:

- **Resultado** de los análisis.
- **Cómo y por qué** fueron utilizadas las diferentes herramientas y procedimientos para recolectar y analizar la información, eso sustentará el trabajo realizado.

- Se debe tener en cuenta el público objetivo al cual se presentará el informe, ya que en este punto es probable que se deba indicar exactamente **¿Qué ocurrió?, ¿En qué plataforma?, ¿Qué tipo de ataque fue realizado?,** sus consecuencias y las posibles contramedidas para evitar que ocurra nuevamente.
- **Acciones** a tomar (si es para remediar algún incidente o delito), como por ejemplo optimizar determinados controles de seguridad, reducir alguna vulnerabilidad encontrada, refuerzo en el entrenamiento del personal (sea usuario final o equipo de respuesta a incidentes), todo esto depende de contexto del incidente.
- Determinar si es necesario realizar más estudios para llegar a una **conclusión definitiva** o si únicamente es posible llegar a explicaciones alternativas o hipótesis, estas deben ir plasmadas en el documento con su justificación respectiva.
- **Lecciones de mejora y recomendaciones** de mejoramiento a las políticas, procedimientos, herramientas de detección y otras observaciones.

CONTROL DE VERSIONES Y CAMBIOS

Versión	Fecha aprobación	Nota de cambio	Elaboró	Firma	Aprobó	Firma