Creando una Trayectoria Profesional en Seguridad Digital:
Gestión de Incidentes

Agosto, 2021

OEA Más derechos para más gente

Citi Foundation citi

Tabla de contenidos

Gestión de incidentes

Se presentará una introducción a metodologías establecidas como mejores prácticas de la industria para enfrentar, investigar y contener incidentes informáticos. **El módulo contiene una práctica y un examen en línea.**

Gestión de Incidentes (1/11)

En esta sesión se abordarán los siguientes temas:

- ¿Qué es un incidente informático?
- Conceptos básicos: evidencia digital y la cadena de custodia
- Fases de un incidente
- Infiltración y ex-filtración de información digital
- Identificación de incidentes: indicadores de compromiso
- Adquisición de información
- Orden de volatilidad

Gestión de Incidentes (2/11)

¿Qué es un incidente informático?

Es un conjunto de **eventos*** que afectan negativamente a la organización/compañía y/o generan una **violación de las políticas** de seguridad, o las políticas de uso aceptable, que además comprometen alguno de los objetivos de seguridad (integridad, disponibilidad y confidencialidad).

* *Ocurrencia de un suceso que puede ser observado, verificado y documentado.*

Gestión de Incidentes (3/11)

¿Qué es una cadena de custodia?

La cadena de custodia es un término legal que describe la **colección**, **transporte** y **almacenamiento de evidencia**; buscando prevenir su alteración, pérdida, daño físico o destrucción.

El objetivo de la cadena de custodia es **registrar de forma adecuada** *el manejo y almacenamiento que se da a una pieza de evidencia.*

En la siguiente lista se describe la información que provee la cadena de custodia:

- ¿Quién tuvo contacto con la evidencia?
- La fecha y hora en la que la evidencia fue manipulada
- Las circunstancias en que la evidencia fue manipulada

Gestión de Incidentes (4/11)

- ¿Qué cambios fueron hechos a la evidencia?
- En el caso de medios digitales, un *hash* de verificación de integridad de los archivos que corresponden al conjunto de evidencia

La cadena de custodia consiste en las siguientes cuatro etapas:

1. **Colección**: se identifica, etiqueta, registra y adquiere información relevante de diferentes orígenes
2. **Examinar**: se utiliza un proceso del tipo **forense** para recolectar los datos de manera manual o con herramientas automatizadas. En esta etapa el proceso de investigación es registrado y se completa el proceso de documentación
3. **Análisis**: es el resultado de la examinación. Se utilizan métodos y técnicas **justificables** para manejar la evidencia en cada caso particular

Gestión de Incidentes (5/11)

4. **Reporte**: se documenta la investigación y el análisis. Incluye una declaración que explica las herramientas, descripción del análisis, orígenes de los datos y recomendaciones

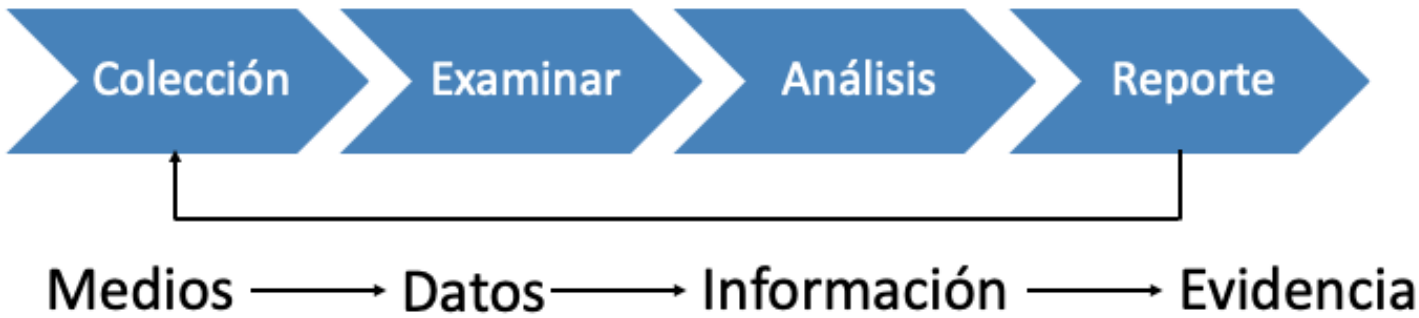
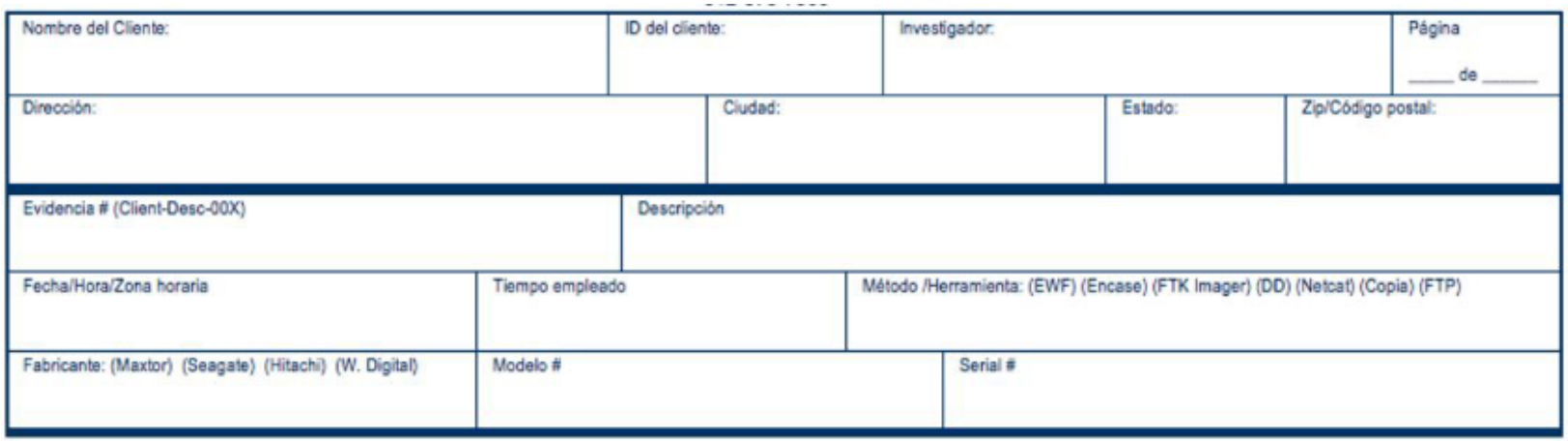


Figura 1: Etapas de la cadena de custodia.

Gestión de Incidentes (6/11)

Formato de cadena de custodia

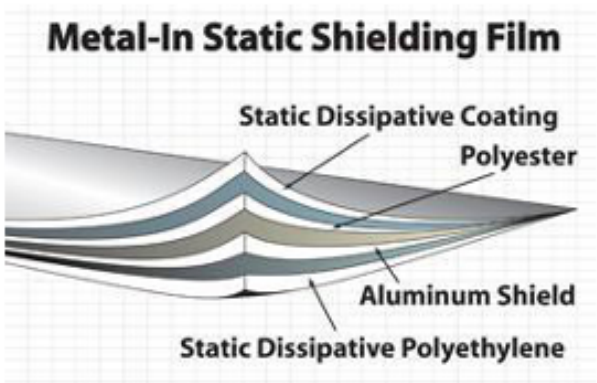
Es un formato permite **trazar el historial de actividades realizadas** con respecto a una evidencia; incluyendo la entrega de dicho ítem para ser analizada, duplicada, almacenada o destruida por una tercera persona.



Nombre del Cliente:	ID del cliente:	Investigador:	Página ____ de ____
Dirección:	Ciudad:	Estado:	Zip/Código postal:
Evidencia # (Client-Desc-00X)	Descripción		
Fecha/Hora/Zona horaria	Tiempo empleado	Método /Herramienta: (EWF) (Encase) (FTK Imager) (DD) (Netcat) (Copia) (FTP)	
Fabricante: (Maxtor) (Seagate) (Hitachi) (W. Digital)	Modelo #	Serial #	

Figura 2: Ejemplo de formato de cadena de custodia.

Gestión de Incidentes (7/11)



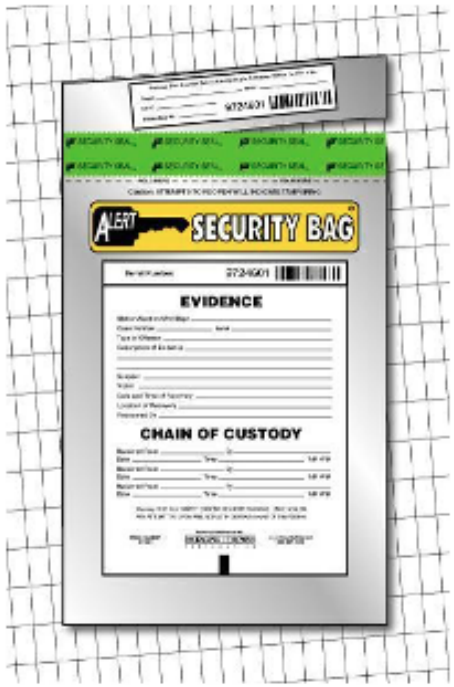


Figura 3: Es ideal contar con *evidence bags* para almacenar y transportar la evidencia digital.

Gestión de Incidentes (8/11)

A continuación de listan los elementos la anatomía de un incidente:

- **Infiltración**: acceso no autorizado, e.j. *SQLi, RAT, etc.*
- **Propagación**: movimiento lateral† en la red e.j. *relaciones de confianza, red no segmentada, etc.*
- **Agregación**: búsqueda y recopilación de información sensible, e.j. *tarjetas de crédito*
- **Ex-filtración**: transporte de la información hacia la infraestructura del atacante, e.j. *RAT, canal encubierto*, etc.*

† *Movimiento lateral es una técnica que utilizan actores maliciosos, después de ganar acceso inicial a un sistema comprometido, con el fin de moverse de manera más profunda mediante la red que lo soporta*

* *Un canal encubierto es un tipo de ataque que crea las capacidades necesarias para transferir objetos de información entre procesos que no están permitidos por una política de seguridad débil.*

Gestión de Incidentes (9/11)

Figura 4: Elementos la anatomía de un incidente.

Gestión de Incidentes (10/11)

Ejemplo de incidente en E-commerce

1. **Infiltración**: inyección de consultas SQL en una aplicación de reportes
2. **Propagación**: *movimiento lateral* usando el servidor de *backend* compartido MSSQL
3. **Agregación**: Acceso a tarjetas de crédito en la base de datos y en bitácoras (*logs* y modificación del código fuente de la página web
4. **Exfiltración**: Inyección de SQL y RCE (*Remote Code Execution*), para el envío de tarjetas mediante módulos asíncronos Javascript (AJAX).

Gestión de Incidentes (11/11)

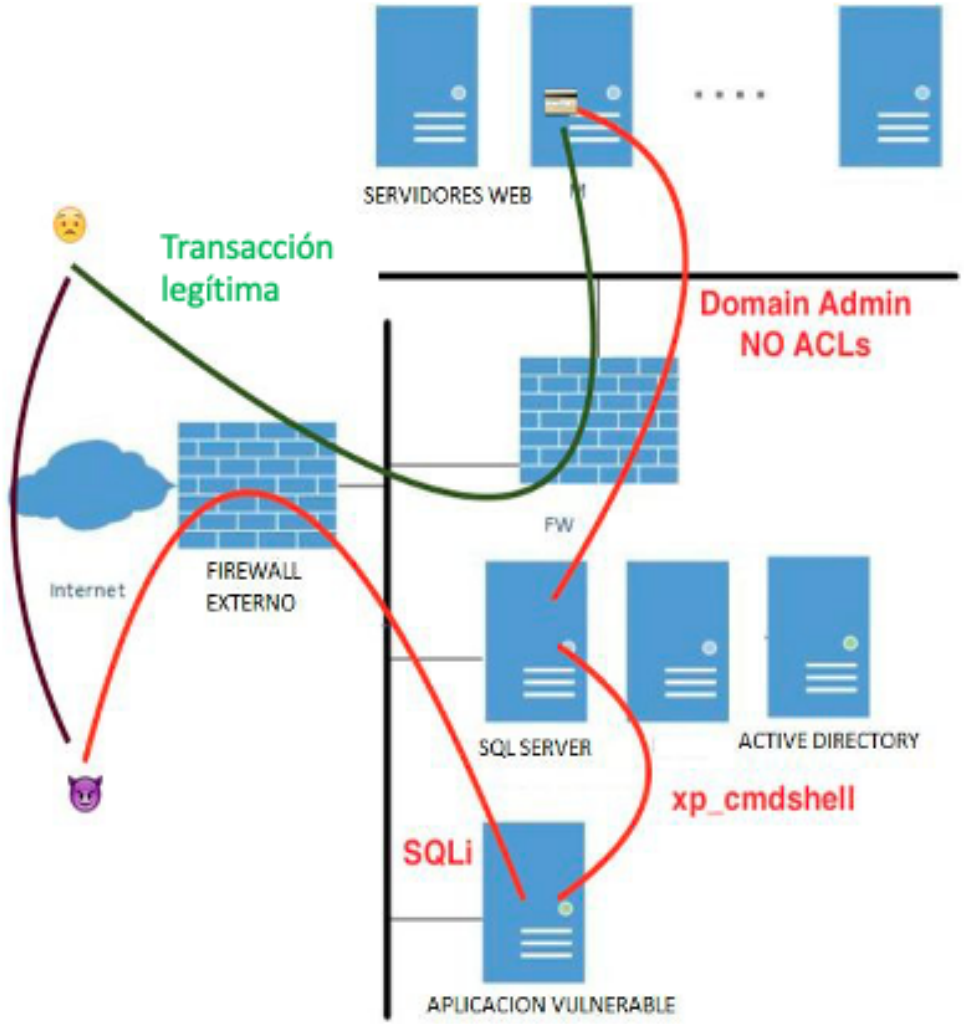


Figura 5: Diagrama del incidente.

Indicadores de compromiso

¿Qué es un indicador de compromiso?

Son **piezas forenses de evidencia**, que sirven para identificar intrusiones potenciales en un host o red.

Es importante identificar el comportamiento **normal** de los sistemas investigados (línea base):

- Identificar cuáles fuentes de información están disponibles e.j. *alarmas, bitácoras, SIEM (Security Information Event Management), IPS (Intrusion Prevention Systems), IDS (Intrusion Detection Systems), antivirus, información del firewall, entrevistas, etc.*
- ¿Existen patrones en la periodicidad de las actividades?
- ¿Existen patrones en los flujos de tráfico de red?
- ¿Existen patrones en el consumo de recursos de los sistemas?
  - Pérdida de datos, bitácoras, etc.
  - Cambios/accesos no autorizados

Ciclo de la gestión de incidentes (1/3)

¿Qué es el ciclo de la gestión de incidentes?

Es un ciclo compuesto por seis etapas, propuesto para manejar apropiadamente brechas en los datos.

En la siguientes Figuras se detallan los componentes de las seis fases del ciclo de la gestión de incidentes.

Ciclo de la gestión de incidentes (2/3)

Figura 6: Fases de la gestión de incidentes.

Ciclo de la gestión de incidentes (3/3)

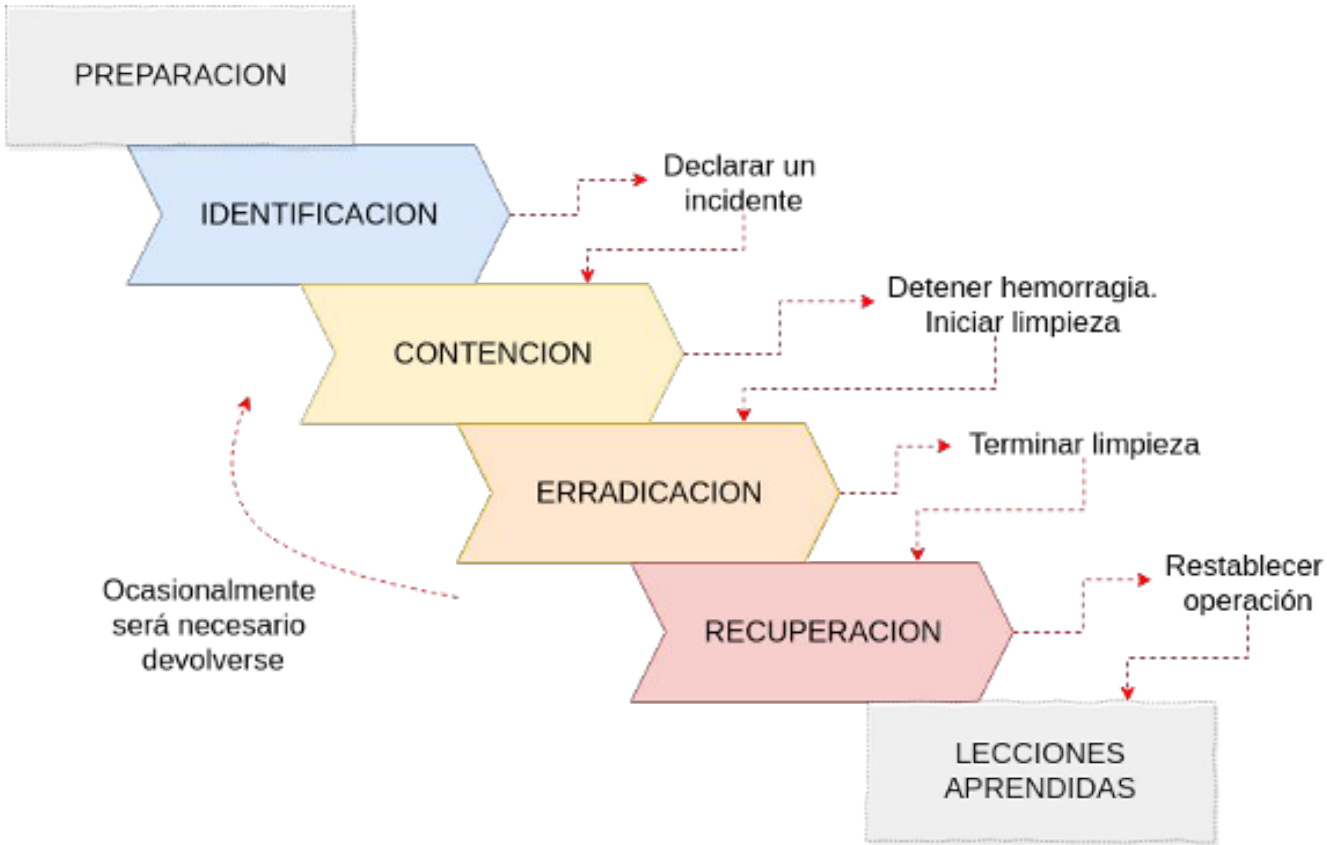


Figura 7: Ciclo de la gestión de incidentes.

Adquisición forense de información (1/5)

¿Qué es la adquisición forense de información?

Es un procedimiento que tiene como objetivo **crear una copia forense** de una fuente de medios, que sea pieza de evidencia en un caso.

- Existe gran diferencia entre la adquisición **live** (*con datos volátiles*) y **post-mortem** (*con el sistema apagado*)
- Adicional a la interacción con el sistema, existe una **gran cantidad** de información volátil que **puede perderse** cuando el sistema es **apagado** o **reiniciado**. Estos datos incluyen: *datos en la memoria del sistema, procesos activos, conexiones de red, contenido del porta-papeles, etc.*

Adquisición forense de información (2/5)

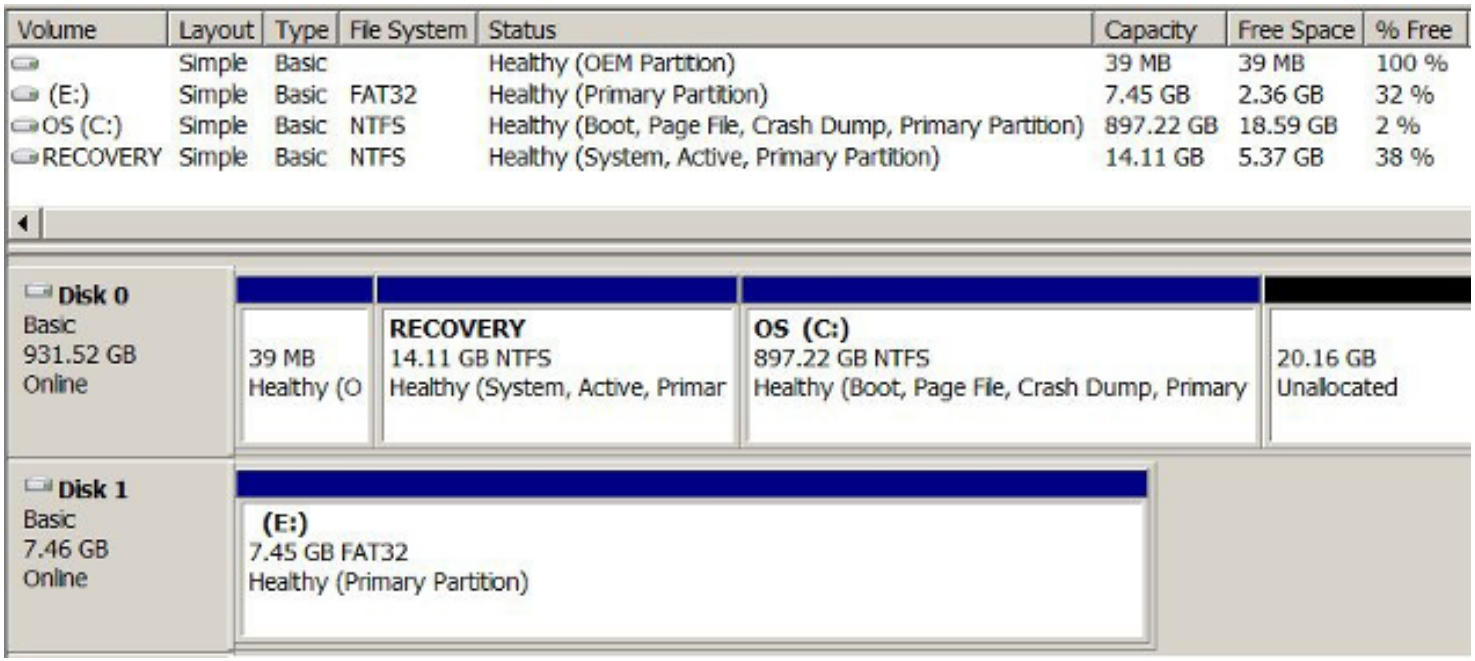


Figura 8: Copia del contenido de un disco en el S.O. Windows, que permite capturar **toda** la información almacenada en el disco (*archivos + espacio en blanco*). Se pueden crear imágenes lógicas o físicas.

Adquisición forense de información (3/5)

Las herramientas de adquisición permiten tomar la imagen de una partición, una unidad, un **arreglo RAID** o una unidad montada en un sistema operativo.

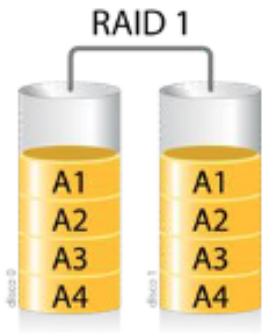


Figura 9: RAID: múltiples discos duros que funcionan de forma lógica como un solo disco; de forma que se incremente disponibilidad, resiliencia y se eliminen los puntos únicos de falla.

Adquisición forense de información (4/5)

Acerca de los **writeblockers o bloqueadores de escritura**

- Los bloqueadores de escritura son dispositivos que permiten la adquisición de información en una unidad **sin la posibilidad de dañar** accidentalmente el contenido de la misma
- Pueden ser dispositivos de *hardware* o *implementaciones de software*

Adquisición forense de información (5/5)

Figura 10: Ejemplo de un bloqueador de escritura, adquiriendo datos (*dumping*) de un disco duro.