MINISTERIO DE AMBIENTE Y DESARROLLO SOSTENIBLE

Guía para la recolección de evidencia digital

PROCESO

Gestión de Servicios de Información y Soporte Tecnológico

Versión 1

22/12/2022

MADSIG
Sistema Integrado de Gestión

TABLA DE CONTENIDO

1. OBJETIVO

Orientar a los responsables de investigar, valorar, contener y reportar los incidentes de seguridad de la información en las acciones a seguir para la recolección de la evidencia digital.

2. ALCANCE

Inicia con el aislamiento de la escena, continua con la identificación, examinación y recolección de información desde diferentes fuentes, para luego realizar el análisis de datos y finaliza con la generación de informe o reporte final.

3. ÁMBITO DE APLICACIÓN

Aplica para todo incidente de seguridad de la información en el evento que se requiera la recolección de evidencia digital.

4. DOCUMENTOS ASOCIADOS A LA GUÍA

- Procedimiento de gestión de incidentes de seguridad
- Políticas específicas de seguridad y privacidad de la información

5. NORMATIVA Y OTROS DOCUMENTOS EXTERNOS

- Norma ISO 27001:2013, A.16.1.1,2,5,7
- Norma ISO 27002:2015, A.16
- NIST SP800-86 (Guide to Integrating Forensic Techniques into Incident Response).
- Ministerio de las tecnologías de la información y las comunicaciones MinTIC - Guía No. 13 – Evidencia Digital
- Fiscalía General de la Nación - **Manual del Sistema de Cadena de Custodia**

6. DEFINICIONES

- **COLCERT:** Grupo de Respuesta de Emergencias Cibernéticas de Colombia. Grupo liderado por el Viceministerio de Transformación Digital, mediante Resolución Número 473 de 17 de febrero del 2022, que adicionó al artículo 1. de la Resolución 002108 del 2020, el Grupo Interno de Trabajo de Respuesta a Emergencias Cibernéticas de Colombia – ColCERT, para continuar articulando y coordinando a nivel nacional los aspectos de ciberseguridad a todos los sectores públicos y privados del país.

- **CSIRT Gobierno** (Computer Emergency Response Team", que en español significa "Equipo de Respuesta para Emergencias Informáticas"). Brinda acompañamiento y apoyo a las entidades del estado, a través de su portafolio de servicios, con el fin de mejorar los procesos de seguridad de la infraestructura tecnológica, la gestión de los incidentes cibernéticos y generación de conciencia en seguridad digital.

7. MEDIDAS INICIALES

Es importante tener presente las siguientes medidas iniciales al momento de realizar las acciones de identificación, recolección, análisis y manipulación de evidencia digital.

a. Verificar si en realidad ha ocurrido un incidente de acuerdo con la clasificación de incidentes del procedimiento de gestión de incidentes de seguridad.
b. Verificar si existe la necesidad de realizar el procedimiento de evidencia digital al incidente reportado.
c. Minimizar la pérdida o alteración de datos.
d. Llevar bitácoras de todas las acciones, con fechas y hora precisas.
e. Analizar todos los datos recolectados.
f. Realizar un reporte de los hallazgos.

8. METODOLOGÍA DE RECOLECCIÓN DE EVIDENCIA DIGITAL

Se adopta la metodología general para la recolección de evidencia digital consignada en la Guía No. 13 – Evidencia Digital publicada por el Ministerio de las Tecnologías de la Información y las Comunicaciones MINTIC, la cual consta de cinco (5) pasos ilustrados a continuación:

Figura 1. Pasos para la recolección de evidencia Digital

Fuente: MINTIC, Guía No. 13 – Evidencia Digital

8.1. Aislamiento de la escena

Una vez verificado que el incidente ocurrido está dentro de la clasificación estipulada en el procedimiento de gestión de incidentes de seguridad, se procede a aislar la escena para evitar cualquier tipo de alteración que pueda contaminar la evidencia para un proceso de investigación.

Para realizar el aislamiento de la escena del líder de seguridad de la información contará con el apoyo del equipo de seguridad informática y/o de alguna autoridad competente (en caso de requerirlo)

- En el Ministerio, la gestión de incidentes debe tener en cuenta las siguientes consideraciones para la recolección de evidencia en el momento en que se detecta un evento o Incidente de Seguridad o Privacidad:

  i. En el momento de hacer la recolección de la evidencia se debe tener en cuenta que existen dos tipos: (i) Identificable a simple vista. *Ej. Captura de imágenes, logs de acceso de consulta abierta*. (ii) Oculta a simple vista *Ej. Log de acceso sobre las bases de datos con acceso restringido*.
  ii. Encontrar la evidencia digital que relacione directa o indirectamente tanto un recurso tecnológico (Hardware, Software) como un usuario con el evento o incidente.

iii. Reconstruir la sucesión de los acontecimientos a partir de los hechos sobre los cuales se encuentre evidencia obtenida de mecanismos de auditoría propios de los recursos tecnológicos involucrados.
iv. Los hallazgos deben ser documentados mediante la utilización de imágenes y la copia de archivos que sirvan como evidencia.
v. Los registros de auditoría (logs) de los sistemas de información, sistemas operativos, hardware, entre otros deben ser utilizados como insumo para detectar y obtener evidencia de los eventos e incidentes de seguridad, para lo cual es indispensable que se cuente con la fecha y hora de la creación y modificación (si la hay) de los registros.
vi. El registro fotográfico y de vídeo puede llegar a ser útil para obtener evidencia frente a los eventos e incidentes de seguridad relacionados con acceso físico (autorizado y no autorizado) a las instalaciones.
vii. Se deben evitar los siguientes errores, que son muy comunes dentro de la recolección de la evidencia a nivel de estaciones de trabajo:
    a. Añadir datos al sistema.
    b. "Terminar" procesos del sistema.
    c. Detener servicios del sistema.
    d. Usar herramientas o comandos no confiables.
    e. Actualizar el sistema operativo antes de recolectar la evidencia.
    f. Continuar trabajando con el equipo luego de presentarse el incidente.
    g. Apagar el equipo cuando se observa actividad sospechosa, porque esto elimina cualquier rastro del incidente y proporciona pérdida de evidencia digital que puede ser muy relevante y que está almacenada en medios volátiles como la Memoria RAM del componente.
    Si es estrictamente necesario apagar la estación de trabajo, esto se debe hacer desconectando la fuente eléctrica (el cable de poder) desde la toma ubicada en la canaleta de cableado estructurado. De esta forma, es posible dejar el sistema exactamente como estaba en el último instante, evitando que él mismo realice la limpieza de datos que se hace comúnmente con el apagado normal.

8.1.2 Cadena de Custodia

La cadena de custodia se activa desde el momento de la recolecta de información y se decida activar la ruta de denuncia por parte del comité respectivo; así mismo, se debe realizar el reporte ante el CSIRT. Una vez se instaure una demanda por parte del representante legal del Ministerio, se informa a la fiscalía general de la Nación, el cual llevará su procedimiento respectivo de cadena de custodia.

La información mínima que se maneja en una cadena de custodia, para cualquier caso, es la siguiente:

- ✓ 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;
- ✓ Recibos personales que guarda cada custodio y donde están datos similares a los de la hoja de ruta.
- ✓ Rótulos o etiquetas que van pegados a los empaques de las evidencias, por ejemplo, a las bolsas plásticas, sobres de papel, sobres de manila, frascos, cajas de cartón, etc.
- ✓ Libros de registro de entradas y salidas, o cualquier otro sistema informático que se deben llevar en los laboratorios de análisis y en los despachos de los fiscales e investigadores

Nota: La Fiscalía General de la Nación desarrolló el documento denominado **"Manual del Sistema de Cadena de Custodia",** que contiene los pasos completos para asegurar las características originales de los elementos (evidencia) desde su recolección hasta su disposición final el cual el Ministerio adoptará para su gestión.

8.2. Identificar fuentes de información

El primer paso por realizar para ejecutar la recolección de datos es identificar fuentes potenciales de información de donde se puedan extraer datos para soportar el proceso de evidencia digital.

Las fuentes más comunes para encontrar información son las siguientes:

- ✓ Computadoras de escritorio y portátiles
- ✓ Servidores (Web, DHCP, Email, Mensajería Instantánea, VoIP Servers, FTP).
- ✓ Almacenamiento en red.
- ✓ Medios de almacenamiento de información.
- ✓ Dispositivos móviles
- ✓ Cámaras de vigilancia

Otras fuentes adicionales de información se relacionan a continuación a manera de ejemplos:

- ✓ Registros de auditoría de dispositivos de seguridad informática como IDS, Firewalls, Plataformas de Antispam, Proxy, bien sea ubicados dentro de los dispositivos o consolidados en algún sistema de correlación de eventos.
- ✓ Registros de auditoría de dispositivos de red como switches o routers.
- ✓ Registros de auditoría de proveedores de servicio que pueden obtenerse bajo órdenes judiciales únicamente

Con base en el análisis y complejidad del incidente se requerirá apoyo especializado a las autoridades competentes para identificar las fuentes de información.

8.3. Examinación, recolección de la información.

Para realizar la recolección y análisis de la información se deberán tener en cuenta las siguientes consideraciones:

- ✓ Aislar el entorno para disminuir el impacto del incidente y evaluar sus consecuencias.
- ✓ Generar las imágenes y/o copias de disco para la investigación, evitar la mayor pérdida posible de información y afectación del servicio.

- ✓ El Ministerio validará el apoyarse con un tercero para un peritaje informático y/o investigación forense.
- ✓ Siempre se deberán realizar los análisis en copias de la información, nunca deberá hacerse en la información original, la cuál debe ser almacenada de manera segura para evitar que sea alterada.
- ✓ Es importante para los analistas de la información poder recibir u obtener toda la información recolectada con las estampas de tiempo precisas, es decir, que todas las plataformas de información se encuentren sincronizadas con un mismo reloj o servicio NTP. Esto garantizará mayor precisión en los estudios posteriores.
- ✓ La Entidad deberá definir un lugar o espacio fisco seguro para el almacenamiento del material probatorio recolectado, como también deberá disponer de un repositorio digital seguro para conservar la evidencia hasta que se la requiera transportar siguiendo las exigencias de seguridad a un laboratorio especializado en análisis forense.

8.4. Análisis de la información

En esta fase se realizará un análisis de la información por parte del equipo de seguridad de la información y el equipo, o si se requiere del apoyo de un laboratorio externo que la entidad haya definido, para hacer dicho análisis de los datos que se lograron extraer de las diferentes fuentes y que se considera relevante o prioritaria para ser estudiada. Se valora la afectación del activo respecto a su confidencialidad, integridad y disponibilidad, y se evaluará el impacto del daño causado por el incidente, al igual que el equipo deberá definir estrategias de mitigación respectiva.

8.5. Generación del Informe Final

Se elabora el informe de hallazgos, que contiene una descripción detallada de los hallazgos relevantes al caso y la forma como fueron encontrados. Este informe reposará en la herramienta de gestión de seguridad de la información definida por la entidad.