LINEAMIENTOS PARA LA OBTENCIÓN Y TRATAMIENTO DE LOS RECURSOS INFORMÁTICOS Y/O EVIDENCIAS DIGITALES

Junio 2016

Contenido

LINEAMIENTOS PARA LA OBTENCIÓN Y TRATAMIENTO DE LOS RECURSOS INFORMÁTICOS Y/O EVIDENCIAS DIGITALES

Introducción

Los presentes lineamientos están destinados a ser puestos en operación por el personal autorizado de la Dirección General de Tecnologías de la Información, independientemente de su adscripción. Tienen como fin constituirse en recomendaciones para la obtención y tratamiento de recursos informáticos y/o evidencia digital, que en estricto apego al marco constitucional y normativo, auxilien en la integración de las investigaciones y procedimientos que realizan en su respectivo ámbito de competencia las Secretarías Ejecutivas de Vigilancia, Información y Evaluación, la de Disciplina, ambas del Consejo de la Judicatura Federal, así como la Visitaduría Judicial y la Contraloría del Poder Judicial de la Federación.

I. ACTUACIÓN EN SITIO

De manera inicial, se deben constituir en el o los lugares para la investigación al menos dos personas autorizadas por la Dirección General de Tecnologías de la Información. Se deben identificar los recursos informáticos y sus poseedores, indicando lugar, hora, fecha, nombre y órgano jurisdiccional o área administrativa, así como la interacción posterior y su resguardo en el lugar que al efecto se señale.

Se registrará la totalidad de los recursos informáticos involucrados, a saber: computadoras, tabletas, celulares, entre otros. Para ello, es necesario generar un inventario de hardware en la inspección, mismo que quedará consignado en el “Registro de Cadena de Custodia” y “Formato de la entrega-recepción de recursos informáticos y/o evidencia digital”.

Es necesario realizar una imagen forense para su análisis en el lugar de la investigación y posteriormente en el lugar designado por la Dirección General de Tecnologías de la Información, consecuentemente, el personal autorizado procederá a:

- Verificar las condiciones mínimas de seguridad.
- Para llevar a cabo las actividades, hacer uso del equipo necesario:
  - Guantes.
  - Pulseras antiestáticas.
  - Cámara fotográfica.
  - Bolsas antiestáticas.
  - Cables UTP.
  - Hule-espuma.
  - Dispositivo Duplicador Forense.
  - Laptop con software forense especializado.
  - Medios de almacenamiento debidamente formateados.
- Efectuar reporte fotográfico de todas las actividades previas y durante la recolección de evidencia digital.
- Generar una imagen forense de los recursos informáticos y/o evidencias digitales.
- Sellar cada entrada o puerto periférico con cintas.
- Identificar con etiquetas y registrar los recursos informáticos y/o evidencia digital.
- Embalar, haciendo uso de bolsas antiestáticas, discos duros y otros dispositivos de almacenamiento informáticos que sean electromagnéticos (si no se cuenta con ellas, se pueden utilizar bolsas de papel). Evitar el uso de bolsas plásticas, ya que pueden causar una descarga de electricidad estática que puede destruir los datos.
- Trasladar los recursos informáticos y/o evidencia digital al lugar de resguardo.

Resulta importante que la o las imágenes forenses de los discos, se realicen a través de un dispositivo duplicador especializado para la captura en su totalidad del disco duro origen (espacios libres, no asignados, así como los archivos de intercambio, eliminados y ocultos).

El dispositivo duplicador deberá cumplir con las siguientes características:

- Debe asegurar que no alterará el disco duro original.
- Podrá acceder tanto a discos SATA, ATA, SCSI e IDE.
- Deberá verificar la integridad de la imagen de disco generada.
- Debe bloquear la escritura, para asegurar la inalterabilidad del elemento de almacenamiento accedido.

II. OBTENCIÓN DE LA INFORMACIÓN DINÁMICA O EN PROCESAMIENTO

Previo a la generación de la o las imágenes forenses y estando en el lugar autorizado para la investigación, es necesario considerar la obtención de los datos en tiempo real así como de la información dinámica o en procesamiento, la cual es aquella que se pierde al interrumpirse la alimentación eléctrica, es decir al apagar el recurso informático. Por ello, se deben realizar los siguientes pasos:

a) Registrar la fecha, hora del sistema y zona horaria.
b) Determinar quién o quienes se encuentran con una sesión abierta, ya sean usuarios locales o remotos.
c) Obtener la configuración de red del equipo.
d) Verificar y registrar todas las conexiones activas.
e) Registrar los puertos TCP/UDP abiertos, así como aplicaciones asociadas a la escucha.
f) Consultar las tablas de ruteo y ARP.
g) Registrar todos los procesos activos.

h) Documentar todas las tareas y comandos efectuados durante la recolección.

i) Examinar y extraer los registros de eventos.

j) Obtener y examinar los archivos de configuración relevantes del sistema operativo.

k) Verificar los registros de eventos de seguridad, del sistema, aplicaciones y servicios activos.

l) Configuración de las políticas de auditoría del sistema operativo.

m) Documentar archivos temporales, de correo electrónico y de navegación en internet.

n) Documentar en el "Registro de Cadena de Custodia" y "Formato de la entrega-recepción de recursos informáticos y/o evidencia digital".

III. GENERACIÓN DE IMAGEN FORENSE

Una vez finalizado el proceso de revisión de la información dinámica o en procesamiento, el personal autorizado debe realizar la imagen forense del equipo, atendiendo los siguientes pasos:

a) Apagar el equipo de ser posible desde el sistema operativo.

b) Desconectar el cable de alimentación eléctrica.

c) Retirar unidades extraíbles.

d) Descargar la propia electricidad estática, mediante pulseras antiestáticas.

e) Desconectar el bus de datos del disco duro (SATA, ATA, SCSI e IDE).

f) Desconectar el cable de alimentación eléctrica del disco duro.

g) Desmontar el disco duro del chasis del recurso informático, para no dañar el circuito electrónico.

h) Montar el disco duro origen al dispositivo duplicador.

i) Montar el disco duro destino al dispositivo duplicador.

j) Efectuar una o dos copias de la evidencia. En caso de realizar dos copias, una se deja en el lugar del hecho, para permitir la continuidad de las actividades, otra

copia se utiliza para el análisis en el laboratorio del personal autorizado y el original se asegura para su posterior embalaje y traslado.

k) Generar una suma de comprobación de la integridad de cada copia mediante el empleo de funciones hash tales como MD5 o SHA1.

l) Guardar el resultado generado por las copias duplicadas.

m) Documentar en el "Registro de Cadena de Custodia" y "Formato de la entrega-recepción de los recursos informáticos y/o evidencias digitales".

IV. ANÁLISIS DE IMAGEN FORENSE

Una vez obtenida y trasladada la imagen forense, se debe realizar un análisis pormenorizado en el lugar designado por la Dirección General de Tecnologías de la Información y, por medio de un conjunto de herramientas informático forenses obtener la siguiente información para su documentación:

- Tipo de sistema operativo.
- Fecha, hora y zona horaria del sistema operativo.
- Versión del sistema operativo.
- Número de particiones.
- Tipo y esquema de particiones.
- Listado de todos los nombres de archivos, fecha y hora.
- Registro del espacio no asignado.
- Recuperación de archivos eliminados.
- Búsqueda de archivos ocultos con palabras claves.
- Listado de todas las aplicaciones existentes en el sistema.
- Búsqueda de programas ejecutables sospechosos.
- Identificación de extensiones de archivos sospechosos.
- Listado de todos los archivos protegidos con claves.

- Listado del contenido de los archivos de cada usuario en el directorio raíz y si existen, en los subdirectorios.
- Generar la certificación de los datos a través del algoritmo de hash al finalizar la detección, recolección y registro.
- Conservar las copias del software utilizado.

V. INFORMES

Posterior al análisis correspondiente realizado al recurso informático y/o evidencia digital, el personal autorizado por la Dirección General de Tecnologías de la información, deberá hacer entrega de dos reportes:

1) **Informe Ejecutivo:** Resumen del análisis efectuado empleando una explicación no técnica, con lenguaje común, en el que se expondrán los hechos más destacables de los recursos informáticos y/o evidencia digital analizados, así como de las conclusiones a que se arribaron. A modo de orientación, deberá contener al menos los siguientes puntos:

    - Motivos de la investigación.
    - Desarrollo de la obtención y tratamiento de los recursos informáticos y/o evidencias digitales.
    - Resultado del análisis.
    - Conclusión.

2) **Informe Técnico:** Exposición detallada del análisis efectuado a los recursos informáticos y/o evidencia digital que describe en profundidad la metodología, técnicas empleadas y los hallazgos que contengan la información empleada para sustentarlo. Se describen los procedimientos y elementos técnicos utilizados para llevar acabo el examen, en el que se precisan las razones o los elementos considerados para orientar las conclusiones de manera clara, firme y

congruente. A modo de orientación, deberá contener al menos los siguientes puntos:

- Descripción de la evidencia.
- Información relevante del sistema analizado.
- Análisis de la evidencia digital documentada.
- Metodología utilizada.
- Descripción de los hallazgos.
- Conclusiones claras, firmes y congruentes.
- En su caso, identificar al autor o autores de la evidencia digital.
- Identificar problemas que deban solucionarse.
- Nombre y firma de quien lo elaboró.

VI. PERFIL DEL PERSONAL AUTORIZADO

Debe ser un profesional con conocimientos, habilidades y experiencia suficiente, con la finalidad de contribuir en las diligencias de las áreas del Consejo de la Judicatura Federal que requieran extracción de evidencias digitales irrefutables, esenciales para la deliberación de las mismas.

El personal debe ser capaz de extraer y recuperar datos, evidencias electrónicas, análisis de información, manejo de herramientas y software forense, redacción de informes, estructuras y protocolos.

Formación académica

El informático forense debe contar con formación universitaria con perfil tecnológico o afín:

- Licenciado en Sistemas Computacionales.
- Licenciado en Administración de Tecnologías de Información.

- Licenciado en Informática Administrativa.
- Ingeniero en Electrónica y Comunicaciones.
- Ingeniero en Sistemas Computacionales.
- Ingeniero en Sistemas Electrónicos.
- Ingeniero en Tecnologías Computacionales.
- Ingeniero en Tecnologías Electrónicas.
- Ingeniero en Telecomunicaciones y Sistemas Electrónicos.

Conocimientos mínimos necesarios

- Sistemas Operativos: Windows, Linux, MacOS X.
- Redes.
- Firewall.
- Routers y Switches.
- Proxys.
- Manejo de protocolos TCP/IP.
- Tipos de datos.
- Sistemas de archivos.
- Adquisición de evidencias en dispositivos de cómputo, red y móviles.
- Software forense.
- Respuesta a incidentes.
- Prevención de perdida de información.

Conocimientos deseables

- Hackeo ético.
- Metodología de la investigación.
- Aplicaciones web.
- Bases de datos.
- Técnicas de intrusión.
- Manejo de filtrado de contenido.
- Herramientas de análisis de penetración.
- Filtrado de correo.
- Sniffer.
- IPS.
- IDS.
- Cifrado.

Cursos y/o certificaciones deseables

- **ISO** 27001 / 27018 / 20000 / 22301.
- **EnCase** Forensic/Enterprise IT Professional.
- **CEH:** Certified Ethical Hacking.
- **CGEIT:** Certified in the Governance of Enterprise IT.
- **CHFI:** Computer Hacking Forensic Investigator.
- **GCFA:** GIAC Certified Forensic Analyst.
- **GCFE:** GIAC Certified Forensic Examiner.
- **GCIH:** GIAC Certified Incident Handler.
- **GCIA:** GIAC Certified Intrusion Analyst.

- **NIST:** National Institute of Standards and Technology.
- **OWASP:** Open Web Application Security Project.
- **COBIT:** Control Objectives for Information and related Technology.
- **ITIL:** Information Technology Infrastructure Library.
- **CISA:** Certified Information Systems Auditor.
- **CISSP:** Certified Information Systems Security Professional.
- **CRISC:** Certified in Risk and Information Systems Control.