1. OBJETIVO

Definir las tareas de recolección y preservación de la evidencia digital, en el caso que un incidente de seguridad de la información requiera un proceso de judicialización o recolección y análisis de evidencia. Lo anterior se realiza en apoyo y complemento al procedimiento de Gestión de Incidentes de Seguridad de la Información establecido por la Contaduría General de la Nación (CGN).

2. ALCANCE

Comprende las actividades a realizar en caso de requerirse la recolección y análisis de evidencia digital.

3. DEFINICIONES

Antivirus: Software con la capacidad para prevenir y realizar la búsqueda de código malicioso y de toda aquella programación que pueda ser potencialmente peligrosa para el sistema.

Bloqueador: Dispositivo de hardware que protege un dispositivo de almacenamiento contra escritura para evitar modificaciones sobre el mismo.

Datos Volátiles: Es aquella información que se encuentra almacenada en la memoria RAM y en donde puede existir evidencia frente al evento o incidente de seguridad que se está administrando, la cual puede desaparecer una vez la maquina es apagada y jamás ser recuperada.

Elementos Materiales de Prueba: Son todos los materiales u objetos (sólidos, líquidos o gaseosos), que pueden servir para la determinación de la verdad durante la investigación, es un medio de prueba real y tangible (que se puede ver, tocar, oler, pesar o medir); para que tengan valor probatorio deben ser debidamente recolectados, protegidos, embalados, rotulados, transportados y entregados al Servidor competente, manejando la cadena de custodia.

Estampa Cronológica: El estampado cronológico es un servicio mediante el cual se puede garantizar la existencia de un documento (o mensaje de datos en general) en un determinado instante de tiempo. Mediante la emisión de una estampa de tiempo es posible garantizar el instante de creación, modificación,

recepción, etc., de un determinado mensaje de datos impidiendo su posterior alteración, haciendo uso de la hora legal colombiana.

Evidencia Digital: También conocida como evidencia computacional, única y conocida como: registros o archivos generados por computador u otro medio equivalente, registros o archivos no generados sino simplemente almacenados por o en computadores o medios equivalentes y registros o archivos híbridos que incluyen tanto registros generados por computador o medio equivalente como almacenados en los mismos.

Hardware: Se denomina hardware o soporte físico al conjunto de elementos materiales que componen un computador. En dicho conjunto se incluyen los dispositivos electrónicos y electromecánicos, circuitos, cables, tarjetas, armarios o cajas, periféricos de todo tipo y otros elementos físicos.

Hash o Huella Digital: Son funciones algorítmicas que tiene como entrada un conjunto de elementos, que usualmente son cadenas y las convierte en un rango de salida finito, normalmente cadenas de longitud fija; estas cadenas pueden ser de 32 o 40 bits y permite identificar de una manera única e inequívoca un archivo digital sin importar su extensión.

Investigación Forense de Seguridad de la Información: Aplicación de técnicas de investigación y análisis para recolectar, registrar y analizar información de incidentes de seguridad de la información.

MD5: (Abreviatura de Message Digest Algorithm 5, Algoritmo de Resumen del Mensaje 5) es un algoritmo de reducción criptográfico de 128 bits ampliamente usado. Su función es generar un código hash o huella digital.

Metadatos: Son datos que describen otros datos, es decir, las propiedades que posee cada uno de los archivos al momento de ser creados, y estos van cambiando en la medida que el usuario realiza ingresos y/o modificaciones sobre el mismo.

Pulsera o Manilla Antiestática: Es un elemento de protección, protege los componentes electrónicos de descargas de electricidad estática con la que se carga el cuerpo humano, y que les puede afectar y en algunos casos incluso destruir.

SHA1: (Abreviatura de Secure Hash Algorithm, Algoritmo de Hash Seguro) es un algoritmo de reducción criptográfico de 160 bits. Su función es generar un código hash o huella digital.

Software de Borrado Seguro: Software que permite esterilizar los medios de almacenamiento tecnológico, de tal manera que no queden residuos de información que puedan modificar o alterar el análisis de las imágenes forenses.

Software Forense: Herramienta avanzada para el Análisis Forense de Sistemas e Investigaciones Digitales.

4. CONTENIDO

4.1. IDENTIFICACIÓN DEL LUGAR A INTERVENIR

Se determina el (los) lugar(es) a intervenir, en donde se encuentran los medios de almacenamiento de tipo tecnológico que serán objeto de investigación forense, es decir, en donde se encuentra la evidencia digital que debe ser administrada por el equipo de respuesta a incidentes.

Es posible que las evidencias digitales puedan ser aportadas por entidades externas, por ende, las mismas serán analizadas directamente.

4.2. PREPARACIÓN DEL AMBIENTE DE TRABAJO

- Definir actividades a realizar: El Equipo de Respuesta a Incidentes de seguridad debe reunirse con la finalidad de planear, diseñar y ejecutar las actividades necesarias para intervenir el lugar de los hechos.

- Preparar los métodos y herramientas a utilizar: Así mismo, el equipo de respuesta a incidentes de seguridad debe preparar del kit de herramientas forenses para la recolección de la evidencia digital y la definición de roles de cada uno de los miembros del equipo que va a intervenir en la investigación forense.

4.3. INTERVENCIÓN DEL LUGAR DE LOS HECHOS

Una vez se interviene el lugar de los hechos por parte de los integrantes del equipo de respuesta a incidentes, éste deberá realizar la búsqueda minuciosa de evidencia digital presente en PCs, laptops, cámaras fotográficas, cámaras de video, DVRs, discos duros externos, memorias usb, medios ópticos, agendas digitales, tablets, celulares, smartphones, sim cards, micro SD, entre otros.

4.3.1. Medios de Fijación

Sin importar la evidencia digital que se recaude (medios de almacenamiento de tipo tecnológico, correos electrónicos, log de seguridad o contenido de páginas web), todo el procedimiento de intervención al lugar de los hechos debe quedar documentado, haciendo especial énfasis en la recolección de la evidencia y su descripción; para ello existen los siguientes medios de fijación:

4.3.1.1. Descriptivo

Es el diligenciamiento de la documentación con una descripción exacta de las actividades realizadas en el lugar de los hechos y una explicación detallada del procedimiento ejecutado frente al recaudo y administración de la evidencia digital.

4.3.1.2. Fotográfico

Es una representación gráfica de la intervención al lugar de los hechos, así como de la identificación de todas las evidencias recaudadas en el sitio, resaltando obviamente las digitales.

4.3.1.3. Video gráfico

Es el registro fílmico de todos los procedimientos realizados en la escena, así como una descripción visual del lugar de los hechos y una identificación detallada de los elementos materiales probatorios recaudados; este registro es uno de los mejores medios de fijación teniendo en cuenta su continuidad, lo que asegura una intervención detallada y sin omisión de las acciones realizadas en el lugar de los hechos.

4.3.1.4. Planimétrico

Es el levantamiento de un bosquejo en donde se describe el lugar de los hechos y la ubicación de cada una de las evidencias recaudadas, para ello se utilizan

medidas las cuales deben ser fijadas a elementos que permanezcan en el tiempo (columnas, puertas, ventanas, entre otros). Este medio de fijación sirve para realizar reconstrucciones de escenas, si así se hiciera necesario.

4.4. RECOLECCIÓN DE LA EVIDENCIA DIGITAL

Proceder según sea el caso, de acuerdo a la evidencia digital recaudada:

4.4.1. Medios de almacenamiento Tecnológico

Cuando se llegue al lugar de los hechos se deben buscar todos los medios de almacenamiento tecnológico, para que los mismos sean recolectados de una manera técnica, aplicando todos los principios de la informática forense y de la cadena de custodia. Si se encuentran computadores encendidos, de ser viable y si así lo amerita el incidente de seguridad de la información se deben recolectar los datos volátiles, los metadatos y las huellas digitales de cada uno de los archivos contenidos en este medio de almacenamiento que está siendo intervenido; es importante resaltar que esta información extraída (datos volátiles, metadatos y huella digital) debe ser exportada a un medio de almacenamiento externo (memoria USB, disco duro externo, entre otros), haciendo especial énfasis en que estos datos NO PUEDEN SER almacenados en el equipo intervenido. Todo este procedimiento debe ser documentado a través de actas y/o formatos y/o informes, para que hagan parte de la carpeta de la administración del incidente de seguridad de la información.

4.4.2. Correos electrónicos

El equipo de respuesta a incidentes deberá administrar la escena en donde se encuentren los correos electrónicos, que para este caso en particular se trata de una escena virtual (cuenta (s) de correo electrónico); para ello, ingresará al e-mail con la finalidad de extraer todos los mensajes relacionados con los hechos del evento o incidente de seguridad de la información, así mismo, se configuraran los mensajes de tal manera que se puedan extraer los encabezados de direccionamiento IP (configuración de la cuenta de correo electrónico dependiendo del proveedor). Este procedimiento será documentado mediante herramientas informáticas que permitan capturar la información contenida en la pantalla, y se deben grabar los mensajes en su formato original que permitan extraer el contenido del mensaje, así como su encabezado. Estos archivos generados serán copiados en un medio de almacenamiento tecnológico

(se recomienda un medio de almacenamiento óptico), a los cuales se les extraerá la imagen forense y/o la huella digital a través del hash, con el propósito de identificar cada uno de ellos de una manera única e inequívoca.

4.4.3. Log de eventos

Cuando se trate de hechos en donde se encuentren vinculadas plataformas tecnológicas y/o sistemas de información, y/o bases de datos, se deberán recaudar los logs de eventos (log de seguridad y/o auditoria y/o trazas) de éste(os) sistema(s), para lo cual se tendrán en cuenta las fechas de ocurrencia del incidente y/o evento de seguridad de la Información. Adicionalmente se deberá consignar en actas la explicación de los esquemas de seguridad que poseen estos sistemas informáticos y/o telemáticos para cumplir con los principios orientados hacia la información como lo son la integridad, disponibilidad, confidencialidad, seguridad y no repudio. A estos logs de seguridad se les extraerá la imagen forense y la huella digital a través del hash.

4.4.4. Contenido de páginas Web

Se trata de evidencia digital presente en sitios web cuyos contenidos deban ser intervenidos por tratarse de un incidente de seguridad de la información. Para ello, se documentará paso a paso la navegación que se haga por el sitio web, teniendo en cuenta todos los links y/o hipervínculos registrados en ésta. Es importante resaltar que esta actividad debe ser registrada mediante la utilización de herramientas informáticas (Capturadores de Pantalla, ejemplo: Print Screen), y de ser posible guardar esta página bajo el formato en que fue hecha (html, htm, xml, entre otras), almacenando estos hallazgos en un medio de almacenamiento tecnológico (se sugiere un medio óptico), para que este sea sometido a los protocolos de cadena de custodia como elemento material probatorio demostrando la existencia de este sitio web.

Por otra parte, se deberá determinar la dirección IP en donde se encuentra alojado dicho sitio web, para los cual podrá utilizar el intérprete de comandos (MS-DOS), utilizando la instrucción ping seguida de la dirección electrónica, ejemplo: ping www.mysite.com; posteriormente se determinara el ISP o Hosting en donde se encuentra alojada esta página web, para ello se podrán utilizar sitios web públicos que tengan relación con la organización IANA (Internet Assigned Numbers Authority), buscando a través de la palabra Who is. El resultado de esta intervención serán los archivos extraídos con ocasión de la captura de la página, así como la documentación de la dirección IP y Proveedor

o Hosting en donde se halla alojada, por ende y con el propósito de asegurar la evidencia es necesario extraer la imagen forense y/o la huella digital a través del hash.

4.5. EXTRACCIÓN DE IMÁGENES FORENSES

4.5.1. Imagen física forense

Cuando se haga necesario extraer una imagen física (Copia bit a bit de todo el medio de almacenamiento, es decir, del sector 0 hasta el último sector) del medio de almacenamiento tecnológico original, se utilizarán las herramientas (Clonadores de disco) forenses de hardware y/o software que tengan el aval por parte de la comunidad técnica - científica.

4.5.2. Imagen lógica

Cuando el Equipo de Respuesta a Incidentes determine que no es necesario extraer toda la información del equipo intervenido, sino solamente un fragmento (archivos, carpetas, volúmenes lógicos (VBR), log de seguridad, Bases de Datos), extraerá una imagen lógica. Cuando se trata de la intervención de servidores que tengan configurados arreglos de discos de hardware o software, se recomienda extraer una imagen lógica frente a los volúmenes lógicos (VBR) que éste posea; esta actividad se recomienda que en lo posible se haga cuando el equipo se halla encendido, con la finalidad de no afectar su sistema de archivos.

4.6. CADENA DE CUSTODIA

4.6.1. Embalaje

La evidencia digital es de origen electrónico, por ello, es necesario tener en cuenta las siguientes recomendaciones frente al contenedor en donde se vaya alojar este medio de almacenamiento de tipo tecnológico:

- El contenedor debe permitir aislar la energía estática producida por los seres humanos, lo anterior teniendo en cuenta el contacto permanente de esta evidencia con los funcionarios que la recaudan, transportan, custodian y analizan.

- El contenedor debe aislar la evidencia frente a campos magnéticos producidos por imanes, señales electromagnéticas de radios, celulares o cualquier otro medio de comunicación. Lo anterior se basa, en que la exposición permanente a estos campos puede alterar algunos de los bits de información contenidos en estos dispositivos, yendo en detrimento de las características de integridad y autenticidad de la evidencia.

La cadena de custodia es la documentación que permite hacer una descripción de la evidencia digital recaudada, el lugar en donde fue hallada, el tipo de embalaje utilizado y los funcionarios que han tenido algún tipo de intervención frente a este elemento. Es necesario tener en cuenta el diligenciamiento de dos (2) formatos, Extracción de Imágenes Forenses y Rótulo y Cadena de Custodia, una vez se haga el recaudo de la evidencia y ésta haya sido alojada en el contenedor respectivo que permita proteger la misma de acuerdo con las directrices anteriores. Se utilizará el formato de cadena de custodia proporcionado por La Fiscalía General de la Nación, que a la fecha esté disponible.

4.6.2. Transporte de la evidencia

Al momento de realizar el transporte de la evidencia digital es necesario tener los mínimos cuidados con la finalidad de que estos medios no vayan a sufrir deterioros, por ende, se recomienda lo siguiente:

- Cuando se traslade la evidencia hay que tener cuidado de no pasar este elemento por puertas o dispositivos que hacen barridos electromagnéticos (utilizados para verificar contenidos de paquetes, o elementos metálicos en la indumentaria o humanidad de una persona); se debe advertir con una etiqueta que se trata de elementos susceptibles a daños por campos electromagnéticos.

- Al transportarla en un vehículo se debe tener especial cuidado de donde se ubica la evidencia, se recomienda que la misma pueda ir en un lugar dentro de éste que no permita la generación de golpes, movimientos extremos o que algunos elementos pueda caer sobre esta, ya que podría generar daños físicos irreversibles, y con ello, la perdida de información total o parcial.

4.6.3. Almacenamiento

El bodegaje de la evidencia resulta ser muy importante, ya que, si la evidencia digital es alojada en un sitio que no posea las condiciones adecuadas, el contenedor (hardware) podría sufrir deterioros que redundaran en la perdida, daño, deterioro o modificación de la evidencia lógica. Por ello se recomienda tener en cuenta lo siguiente:

- Alojar la evidencia digital en un lugar seco, con condiciones climáticas adecuadas para el almacenamiento de ésta.
- Almacenar la evidencia lejos de dispositivos que generen campos magnéticos, señales electromagnéticas, o energía estática.
- Tener espacios adecuados para alojar los medios de almacenamiento tecnológico de manera individual, con su respectiva descripción para su posterior ubicación.

4.7. ANÁLISIS DE LAS IMÁGENES EXTRAÍDAS

Una vez recaudadas las imágenes forenses (físicas o lógicas), se determinará el tipo de análisis que se deberá realizar teniendo en cuenta la información del incidente de seguridad, así como la selección de las herramientas forenses adecuadas para este fin.

NOTA: Es importante hacer una copia de las imágenes forenses. El análisis se realizará sobre la copia y las imágenes forenses originales se almacenarán para ser presentadas como material probatorio.

4.8. HERRAMIENTAS DE ANÁLISIS FORENSE

4.8.1. Distribuciones para análisis forense

- SIFT (SANS Investigative Forensic Toolkit)

Una agrupación internacional de expertos forenses, desarrolló este entorno de trabajo con base a una distribución de código abierto (Ubuntu) para la respuesta a incidentes y el análisis forense digital. Tienen en cuenta operaciones como el montado de imágenes, creación de líneas de tiempo, recopilación de memoria volátil o efímera y el uso de herramientas como Sleuthkit o Autopsy.

- CAINE (Computer Aided Investigative Enviroment)

Esta distribución, creada por desarrolladores y especialistas italianos, se basa en Ubuntu con una arquitectura de 64bits. Una de sus excelentes funciones es que permite bloquear dispositivos como discos o unidades de almacenamiento y ponerse en modo de solo lectura con una simple herramienta que posee una interfaz gráfica.

- DEFT (Digital Evidence and Forensic Toolkit)

Distribución Linux basada en Xubuntu 9.10 con un kernel 2.6.31, escritorio LXDE además de una GUI con aplicaciones forenses pensada para policía, investigadores, administradores de sistemas o especialistas forenses.

4.8.2. Herramientas de clonado de disco o copiado de archivos

- Dd (Duplicate DisK)

Herramienta que se ejecuta mediante la terminal de comandos y se utiliza para clonar o copiar información bit a bit del disco duro, o también para copiar particiones o discos completos unos sobre otros. Esta herramienta, también tiene la capacidad de crear imágenes completas de disco, para que luego puedan ser analizadas como evidencia.

- Air (Imagen y Restauración Automática)

Air es una aplicación en modo gráfico para el uso del comando dd/dclfdd (Datataset Definition (dd)). Fue diseñado como una mejora en modo gráfico de todas las variantes de dd; su fácil uso permite crear imágenes forenses de discos y de particiones completas del mismo. Soporta hashes MD5/SHAx, cintas SCSI, proyección de imágenes sobre una red TCP/IP, imágenes partidas, y registro detallado de la sesión.

- FTK Imager

Herramienta que permite crear imágenes de discos duros, Zip, CD-ROMs, DVD-ROMs, carpetas o archivos individuales; hacer una vista previa de los archivos y carpetas en discos duros, discos Zip, CD-ROMs y DVD-ROMs; montar la imagen para visualizar el contenido de la misma exactamente como el usuario la conserva en la unidad original; exportar archivos y carpetas de imágenes de disco; ver y recuperar archivos que se han borrado desde la papelera de reciclaje, pero que aún no se han sobreescrito en la unidad; crear hashes de archivos mediante dos funciones: MD5 y SHA-1; generar informes de hashes por

archivo y por imagen de disco para comprobar la integridad de los contenidos.

- Helix

Herramienta destinada al análisis forense para entornos Microsoft Windows, GNU Linux y MacOS X, que permite realizar imágenes forenses de la memoria RAM y discos duros.

- Encase

Herramienta de pago para clonado de disco. Permite crear copias comprimidas de los discos origen usando un estándar sin pérdida (loss-less); buscar y analizar varias partes de la evidencia. Muchos investigadores utilizan varios discos duros, discos extraíbles, etc. Esta utilidad nos permite buscar todos los datos involucrados en un caso en un mismo paso; permite ordenar los archivos de acuerdo a diferentes campos incluyendo las tres estampillas de tiempo (cuando se creó, último acceso, última escritura), nombres de los archivos, firma de los archivos y extensiones; recuperar archivos internos y meta-datos con la opción de montar directorios como un sistema virtual para la visualización de la estructura de estos directorios y sus archivos; realizar búsquedas automáticas y análisis de archivos de tipo ZIP y adjuntos de correos electrónicos.

4.8.3. Bloqueadores de escritura

- FIREBrick
  Alternativa de código abierto (firmware) a los bloqueadores de escritura (write blockers) de hardware comercial y generador de imágenes de disco.

- Fastbloc
  Bloqueador de escritura de comercial de la empresa Guidance Software. Este bloqueador viene incorporado en Encase, pero también puede comprarse individualmente.

- Lockdown
  Bloqueador de escritura de comercial de la empresa Paraben.

4.8.4. Generadores de Hash

- WinMD5

Software libre para la generación de códigos hash MD5 en entornos Windows.

- HashMyFiles

Herramienta que permite calcular los hashes MD5 y SHA1 de uno o más archivos en un sistema en entornos Windows. Puede copiar fácilmente la lista de hashes MD5/SHA1 en el portapapeles o guardarlos en archivo de texto/html/xml.

- GTK Hash

4.8.5. Analizadores de Tráfico

- Wireshark

Analizador de protocolos compatible con entornos GNU/Linux y Windows.

- Xplico

Herramienta para interpretar capturas .pcap realizadas con Tshark, Wireshark, Windump, TCPDump, entre otros.

4.8.6. Comandos

Algunos comandos útiles se presentan a continuación:

- Enumerar las direcciones IP del sistema y mapear la asignación de direcciones físicas MAC con dichas IP (ipconfig, arp, netstat, net).
- Enumerar puertos TCP y UDP abiertos y sus procesos asociados (netstat)
- Analizar el tráfico de red (tcpdump, windump).
- Tablas de enrutamiento (route print).
- Leer, copiar y escribir a través de la red (netcat, crypcat).

Obtener fecha y hora del sistema (date, time).