Evidencia Digital

SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

Guía No. 13

MINTIC vive digital Colombia TODOS POR UN NUEVO PAÍS PAZ EQUIDAD EDUCACIÓN

HISTORIA

VERSIÓN	FECHA	CAMBIOS INTRODUCIDOS
1.0	28/03/2016	Generación De Primera Versión De Documento

TABLA DE CONTENIDO

1. DERECHOS DE AUTOR

Todas las referencias a los documentos del Modelo de Seguridad y Privacidad de la Información, con derechos reservados por parte del Ministerio de Tecnologías de la Información y las Comunicaciones, a través de la estrategia de Gobierno en Línea.

Todas las referencias a las políticas, definiciones o contenido relacionado, publicadas en la norma técnica colombiana NTC ISO/IEC 27035 vigente, así como también se toma como referencia la publicación especial de NIST SP800-86 (National Institute of Standards and Technology – (*Guide to Integrating Forensic Techniques into Incident Response*).

2. AUDIENCIA

Entidades públicas de orden nacional y territorial, así como proveedores de servicios de Gobierno en Línea, y terceros que deseen adoptar el Modelo de Seguridad y Privacidad de la información en el marco de la Estrategia de Gobierno en Línea.

3. INTRODUCCIÓN

El presente documento da los lineamientos para realizar un proceso de informática forense adecuado, siendo a su vez un complemento al proceso de gestión de incidentes de seguridad de la información, ya que el enfoque de esta guía está relacionado con los eventos de seguridad de la información que pueden generar algún impacto a los activos de información.

Esta guía deberá ser de conocimiento para todos los involucrados en un incidente de seguridad de la información (desde el punto de contacto hasta el equipo de resolución del incidente ISIRT), teniendo en cuenta los roles en la *Guía de Gestión De Incidentes*.

Se recomienda que los lineamientos que se dan a continuación se empleen específicamente en la fase de *análisis, evaluación y decisión* de los incidentes, ya que en este punto aún no se realiza manipulación de la información ni se afecta la integridad de la misma, permitiendo obtener la evidencia necesaria adecuadamente.

En la fase de análisis, evaluación y decisión se debe considerar si el evento o incidente amerita realizar un procedimiento de informática forense para recolectar evidencia digital para emprender alguna acción de tipo legal, investigació disciplinaria interna o aprendizaje.

Es importante haber realizado la lectura y entendimiento de la G*uía # 25 "Gestión de incidentes de seguridad de la información"*, ya que la presente guía aplica, solo si un incidente de seguridad de la información se ha materializado en la entidad y se hace necesario la recopilación de evidencia digital, también es importante recalcar que las instituciones como COLCERT y CCP son el punto de apoyo para realizar investigaciones de este tipo.

4. OBJETIVO GENERAL

Indicar a las diferentes entidades del estado, como llevar a cabo una correcta identificación, recolección, análisis y manipulación de datos en caso de algún evento o incidente de seguridad que requiera de evidencias digitales para su investigación.

5. GLOSARIO

- **Informática Forense:** Aplicación de la ciencia para la identificación, recolección, examen y análisis de los datos, preservando correctamente su integridad, llevando a cabo a su vez una estricta cadena de custodia de la información.
- **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.
- **Información Volátil:** Datos de un determinado sistema que se pierden una vez dicho sistema es reiniciado o apagado.
- **Host Protected Area (HPA):** Conocido también como *hidden protected área*, se denomina de esta manera al espacio en un disco que no puede ser visibilizado por un sistema operativo.
- **Slack Space:** Es el espacio sobrante de un archivo que no alcanza a ocupar una unidad de almacenamiento asignada dentro de un sistema de archivos, es decir, que si un archivo pesa 20KB pero la unidad de almacenamiento es de 32KB, el espacio sobrante de 12KB se llamará slack space. Para los procedimientos de evidencia forense, estos espacios pueden guardar información de archivos borrados previamente entre otra información.

6. CONSIDERACIONES INICIALES PARA LA CORRECTA EJECUCIÓN DE LA RECOLECCIÓN ANÁLISIS Y MANIPULACIÓN DE EVIDENCIA DIGITAL

Es importante tener presente las siguientes medidas iniciales al momento de realizar el procedimiento de Identificación, Recolección, Análisis y Manipulación de evidencia digital (**de ahora en adelante llamado *Procedimiento de Evidencia Digital***):

1. Verificar si en realidad ha ocurrido un incidente o no (*Tomado de la guía de gestión de incidentes*).
2. Verificar si existe la necesidad de realizar el procedimiento de evidencia digital al incidente reportado.
3. Minimizar la pérdida o alteración de datos.
4. Llevar bitácoras de todas las acciones, con fechas y ahora precisas.
5. Analice todos los datos recolectados.
6. Realice un reporte de los hallazgos.

Una vez definidas estas consideraciones generales, es importante conocer la estructura general del procedimiento de evidencia digital.

7. METODOLOGÍA GENERAL DEL PROCEDIMIENTO DE EVIDENCIA DIGITAL

La metodología general del procedimiento de evidencia digital, se centra en 4 pasos principales ilustrados a continuación:

***Figura 1*. Diagrama Del Proceso De Evidencia Digital**

8. VERIFICACIÓN Y CONFIRMACIÓN DEL INCIDENTE

Previo a la iniciación del procedimiento de evidencia digital, es necesario verificar que el evento que está siendo reportado, es realidad un incidente que atenta contra la confidencialidad, integridad o disponibilidad de la información. Esta labor es realizada en el proceso de evaluación y decisión de incidentes. Una vez se confirma la autenticidad, es necesario también determinar si dicho incidente requiere o no de un análisis forense (procedimiento de evidencia digital). Una vez se definen estas condiciones, se debe proceder con la primera fase.

9. FASE I. AISLAMIENTO DE LA ESCENA

Una vez el evento reportado se cataloga como un incidente de seguridad de la información, es necesario restringir el acceso a la zona donde se produjo el incidente para evitar cualquier tipo de alteración o contaminación a la evidencia que pueda recolectarse para la posterior investigación.

En el mejor de los casos, lo mejor sería que alguna autoridad competente (como el CCP o el COLCERT) realizara el aislamiento de la escena, pero dado que estos procedimientos deben ejecutarse a la mayor brevedad posible, debe proceder el personal de la institución (preferiblemente un ingeniero forense o de seguridad de la información) que esté en capacidad de describir detalladamente todos los procedimientos que realizó para aislar la escena y capturar evidencia en primera instancia (*ver en FASE II. Cadena de custodia*), se puede pedir acompañamiento del área de seguridad física de la institución para apoyar al aislamiento de ser necesario.

Dentro de los procedimientos más comunes para el aislamiento de la escena, se encuentran los siguientes:

- De ser preferible, tomar una fotografía del equipo o sitio del incidente antes de tocarlo.
- Establecer un perímetro de seguridad, para que nadie pueda acercarse.
- Si el equipo se encuentra encendido, no se debe apagar, deberá procederse a realizar los siguientes procedimientos:
  - Sellar los puertos USB, firewire, Unidades CD/DVDetc…para impedir alguna alteración posterior al registro de la escena.
  - Tomar fotografías de lo que se puede ver en la pantalla (software corriendo, documentos abiertos, ventanas de notificación, hora y fecha ilustrados)
  - Asegurar el equipo (Si es portátil, tratar de mantenerlo encendido con el cargador hasta hacer entrega o iniciar el análisis respectivo).
  - Si es posible capturar información volátil del equipo antes de que se apague, debe hacerse empleando las herramientas forenses necesarias.
- Si el equipo se encuentra apagado, no realizar el encendido, esto puede alterar la escena o borrar información que podría lograr obtenerse posteriormente.
- Llevar los elementos necesarios para la recolección de información como estaciones forenses, dispositivos de backups, medios formateados y/o estériles, cámaras digitales, cinta y bolsas para evidencia, papel de burbuja, bolsas antiestáticas, cajas de cartón, rótulos o etiquetas etc.…

- Almacenar la información original en un sitio con acceso restringido, para garantizar la cadena de custodia de la información.
- Obtener información de dispositivos que tuvieron contacto o interacción con el equipo en cuestión (switches, firewalls, Access points etc…).

9.1. CADENA DE CUSTODIA

La cadena de custodia es un procedimiento que debe tenerse en cuenta desde el mismo instante que se decida realizar el proceso de evidencia forense, ya que este procedimiento, basado en el principio de la “mismidad”, tiene como fin garantizar la autenticidad e integridad de las evidencias encontradas en alguna situación determinada, es decir, que lo mismo que se encontró en la escena, es lo mismo que se está presentando al tribunal penal o comité disciplinario según sea el caso.

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.

Esta trazabilidad, brindará la confianza suficiente a quienes reciban las evidencias para certificar que toda la información ha conservado su integridad, que no ha sido alterada o modificada.

9.3. PROCEDIMIENTO OFICIAL DE LA FISCALIA PARA CADENA DE CUSTODIA

La fiscalía desarrolló el procedimiento llamado "***Manual Único 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:

http://www.fiscalia.gov.co/colombia/wp-content/uploads/2012/01/manualcadena2.pdf

10. FASE II. IDENTIFICACIÓN DE FUENTES DE INFORMACIÓN, PASOS INICIALES DE ADQUISICIÓN DE INFORMACIÓN

El primer paso a 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.

10.1. IDENTIFICACIÓN DE POSIBLES FUENTES DE DATOS:

Las fuentes más comunes para encontrar información son las siguientes:

- Computadoras de escritorio y portátiles
- Servidores (Web, DHCP, Email, Mensajería Instantánea, VoIP Servers, FTP o cualquier servicio de filesharing).
- Almacenamiento en red.
- Medios tanto internos como externos que contemplan: Dispositivos USB, Firewire, CD/DVD, PCMCIA, Discos Ópticos y Magnéticos, Discos Duros Extraíbles, Memorias SD y MicroSD etc…
- Dispositivos celulares, PDAs, Camaras Digitales, Gradaboras de video y audio.

A nivel de seguridad informática, pueden considerarse otras fuentes adicionales de información como por ejemplo:

- Logs de dispositivos de seguridad informática como IDS, Firewalls, Plataformas de Antispam, Proxy, bien sea ubicados dentro de los dispositivos o consolidados en algún sistema SIEM.
- Logs de dispositivos de red como switches o routers.
- Logs de proveedores de servicio (que pueden obtenerse bajo órdenes judiciales únicamente).

Siempre es importante tener presente cualquier sistema que pueda registrar información considerable, dado que pueden darse casos en que no sea posible obtener la fuente principal de información (computador privado de un tercero por ejemplo) para poder verificar y obtener información de primera mano.

10.2. ADQUISICIÓN DE DATOS:

La adquisición de los datos debe realizarse teniendo en cuenta 3 pasos principales:

- **Planificación de la adquisición de datos:** Se debe planificar bien a que fuentes de información se les extraerá la información y el orden en el que se debe hacer,

teniendo en cuenta aspectos como, volatilidad de la información, complejidad para obtener los datos o por experiencia propia del analista.

- **Adquisición de los datos (*FASE III de la Guía*):** El proceso general de recolección generalmente requiere del uso de herramientas forenses para copiar los datos volátiles y poderlos almacenar, así como también para adquirir la información de fuentes no volátiles. El proceso de recolección puede variar si es posible acceder localmente al sistema o si se puede hacer a través de la red.
- **Verificación de la integridad de los datos recolectados (*FASE III De la guía*):** Una vez se recolectan los datos, se debe asegurar que la información mantiene su integridad y no ha sido modifica. Esto se puede realizar empleando herramientas de cálculo de resumen de mensajes que generan un valor determinado. Dicho valor debe ser igual tanto en la fuente original como en la copia. Esta verificación de integridad se utiliza principalmente para efectos legales, para que la información se certifique como auténtica.

Es importante tener en cuenta que si la información va a utilizarse para fines legales, desde el inicio debe tenerse total cuidado con la manipulación, llevando a cabo la **cadena de custodia** adecuadamente, registrando cada acción, desde que se recolecta, se almacena, se guarda, quien lo hace y la hora exacta, que herramientas se han utilizado para la recolección etc.…

Es importante decidir hasta qué punto la organización se encontrará en capacidad de realizar la recolección y/o análisis de la evidencia que se presentará en las siguientes fases, es por ello que dependiendo el caso deberá contactarse al COLCERT o CCP para recibir instrucciones o colaboración en la realización de estos procedimientos.

11. FASE III. RECOLECCIÓN Y EXAMINACIÓN DE INFORMACIÓN

Una vez se han identificado las posibles fuentes de información, se debe proceder a realizar la recolección y examinación de los datos disponibles.

La secuencia para llevar a cabo la recolección y examinación de medios/información es la siguiente:

11.1. CREACIÓN DEL ARCHIVO / BITÁCORA DE HALLAZGOS (CADENA DE CUSTODIA)

Consiste en la creación y aseguramiento de un documento, ya sea físico o electrónico, que permita llevar un historial de todas las actividades que se llevan a cabo durante el proceso, y de los hallazgos encontrados, de modo que se tenga un resumen que permita hacer la reconstrucción del caso tiempo después de que este haya sido analizado.

11.2. IMAGEN DE DATOS

Consiste en la generación de las imágenes de datos que conciernen al caso en investigación. Se recomienda utilizar herramientas de extracción de imágenes como *Linux dd* o *Encase Forensic Software*.

11.3. VERIFICACIÓN DE INTEGRIDAD DE LA IMAGEN

Para cada imagen suministrada se debe calcular su compendio criptográfico (SHA1/MD5), comparándolo luego con el de la fuente original. Si la comparación arroja un resultado negativo se debe rechazar la imagen proveída en el primer paso.

11.4. CREACIÓN DE UNA COPIA DE LA IMAGEN SUMINISTRADA

En un análisis de datos nunca se debe trabajar sobre la imagen original suministrada. Debe realizarse una copia master y a partir de esta, se reproducen las imágenes que se requieran.

11.5. ASEGURAMIENTO DE LA IMAGEN ORIGINAL SUMINISTRADA

Se debe garantizar que la imagen suministrada no sufra ningún tipo de alteración, con el fin de conservación de la cadena de custodia y del mantenimiento de la validez jurídica de la evidencia.

11.6. REVISIÓN ANTIVIRUS Y VERIFICACIÓN DE LA INTEGRIDAD DE LA COPIA DE LA IMAGEN

Una vez se ha obtenido la copia de la imagen, es necesario asegurar que no tenga ningún tipo de virus conocido.

Luego se debe verificar la integridad de la copia, de la misma forma como se hizo con la original (paso **9.3**). De hecho, esta actividad es de tipo transversal en la metodología, es decir, debe realizarse periódicamente durante el proceso de análisis de datos, de modo tal que se garantice la integridad de los datos desde el comienzo, hasta el fin de la investigación.

11.7. IDENTIFICACIÓN DE LAS PARTICIONES ACTUALES Y ANTERIORES

La identificación de las particiones en un dispositivo es de vital importancia, ya que reconocerlas implica la identificación de su sistema de archivos, mediante el cual se pueden reconocer características especiales de la organización de la información y se puede definir la estrategia de recuperación de archivos adecuada.

11.8. DETECCIÓN DE INFORMACIÓN EN LOS ESPACIOS ENTRE LAS PARTICIONES

Cuando se detectan datos en estas zonas de la imagen, se debe proceder a hacer un análisis para determinar si representan algún tipo de información relevante para la investigación. En caso de estar protegidos, estos archivos serán tenidos en cuenta en la fase de la identificación de archivos protegidos, de lo contrario, se incluirán en el conjunto de archivos potencialmente analizables.

11.9. DETECCIÓN DE UN HPA (*HOST PROTECTED AREA*)

Este paso debe realizarse solo si en los Meta-datos se indica la existencia del HPA ya que de otro modo es imposible de identificar. En el caso en que exista, se debe seguir el mismo procedimiento del paso anterior.

11.10. IDENTIFICACIÓN DEL SISTEMA DE ARCHIVOS

Para cada una de las particiones identificadas en el paso **9.7**, debe identificarse su sistema de archivos, con el fin de escoger la forma de realizar las actividades posteriores del análisis de datos.

11.11. RECUPERACIÓN DE LOS ARCHIVOS BORRADOS

Durante esta actividad se deben tratar de recuperar los archivos borrados del sistema de archivos, lo que es conveniente dado el frecuente borrado de archivos para destruir evidencia.

Dependiendo de las características técnicas y del estado del sistema de archivos puede no ser posible la recuperación de la totalidad de los archivos eliminados, por ejemplo si estos han sido sobre escritos, o si se han utilizado herramientas de borrado seguro para eliminarlos.

Los archivos recuperados exitosamente formarán parte de los archivos potencialmente analizables, exceptuando los archivos identificados como protegidos que serán tenidos en cuenta durante la fase de identificación de archivos protegidos.

11.12. RECUPERACIÓN DE INFORMACIÓN ESCONDIDA

En esta etapa se debe examinar exhaustivamente el *slack space*, los campos reservados en el sistema de archivos y los espacios etiquetados como dañados por el sistema de archivos.

Al igual que en la fase 10, los archivos protegidos también se tendrán en cuenta durante la fase de análisis de éste tipo de archivos.

11.13. IDENTIFICACIÓN DE ARCHIVOS EXISTENTES

Seguidamente, se clasifican los archivos restantes entre protegidos y no protegidos, donde estos últimos harán parte de los archivos potencialmente analizables, mientras los primeros harán parte la fase de análisis de archivos protegidos.

11.14. IDENTIFICACIÓN DE ARCHIVOS PROTEGIDOS

Esta es la fase de consolidación de archivos protegidos identificados en las fases anteriores. Durante esta fase se pretende descifrar o romper tal protección en estos archivos, con el fin de adicionarlos al conjunto de archivos potencialmente analizables. Los archivos cuya protección no pudo ser vulnerada formarán parte del conjunto de archivos sospechosos.

11.15. CONSOLIDACIÓN DE ARCHIVOS POTENCIALMENTE ANALIZABLES

Durante esta fase se reúnen todos los archivos encontrados durante las fases de

recuperación de archivos borrados, recuperación de información escondida, identificación de archivos no borrados e identificación de archivos protegidos.

11.16. DETERMINACIÓN DEL SISTEMA OPERATIVO Y LAS APLICACIONES INSTALADAS

Al determinar el sistema operativo y las aplicaciones instaladas, se está en la capacidad de obtener la lista de compendios criptográficos de los archivos típicos del sistema operativo y de las aplicaciones, para verificar posteriormente la integridad de los estos archivos de encontrarse en la imagen sometida a análisis.

11.17. IDENTIFICACIÓN DE INFORMACIÓN DE TRÁFICO DE RED

A parte de los sistemas de información, es convencional realizar una verificación minuciosa de la información registrada por los dispositivos de red, ya que puede ayudar a reconstruir y analizar ataques basados en red o a rastrear algún tipo de acceso o movimientos específicos que puedan estar relacionados con el incidente reportado (Ataques DoS, DDoS, mal uso de los recursos de la organización, comportamientos anómalos).

La principal fuente de información a consultar (de estar disponible), es un sistema tipo SIEM, que tiene la capacidad de almacenar logs de distintos dispositivos de red y relacionarlos por el tiempo en que son generados. Esto permite ver la trazabilidad de un paquete desde que ingresa, hasta que abandona la red.

Cuando se identifica algún evento de interés (en una hora exacta), el análisis puede llegar a consistir en solo acceder a verificar logs en los tiempos aproximados o puede llegar a ser más profundo y verificar varias fuentes de información adicionales, llegando a incluir a los proveedores de servicio de internet. Estos análisis se pueden llevar a cabo empleando software tipo NFAT (*Network Forensic Analysis Tool*) que puede ayudar a correlacionar dirección IP, direcciones MAC y realizar sus búsquedas en las fuentes de información disponibles.

Otras fuentes de información relevantes son servidores DHCP, Aplicaciones Cliente Servidor (Por ejemplo Correo Electrónico), Logs Del Proveedor De Servicios, Plataformas De Acceso Remoto (VPN).

Es importante que todas estas plataformas tecnológicas se encuentren previamente sincronizadas a través de NTP.

11.18. DEPURACIÓN DE ARCHIVOS BUENOS CONOCIDOS

El objetivo de este paso es descartar información que no será relevante para analizar. Con la lista de compendios criptográficos obtenida en el paso **9.16**, se procede a verificar la integridad de los archivos en la imagen que aparecen en tal lista. Si dicha comprobación es exitosa, estos archivos se consideran “buenos” y por lo tanto son descartados del proceso de análisis en la fase posterior.

11.19. CONSOLIDACIÓN DE ARCHIVOS SOSPECHOSOS

Como resultado del filtrado de “buenos conocidos”, se obtiene un conjunto de archivos susceptibles a análisis, este conjunto se llamará archivos sospechosos.

11.20. PRIMERA CLASIFICACIÓN DE ARCHIVOS

Divide los archivos sospechosos en:

- **Archivos “Buenos” Modificados:** Son identificados en la fase de filtrado como archivos buenos cuya versión original (descrita por la lista obtenida en el paso **10.15**) ha sido modificada.
- **Archivos “Malos”:** Se obtienen a partir de la comparación de los archivos sospechosos contra los compendios criptográficos de archivos “malos” relacionados con el sistema operativo particular. Estos archivos representan algún tipo de riesgo para el sistema en el que se encuentran o se ejecutan, por ejemplo: sniffers, troyanos, backdoors, virus, keyloggers entre otros.
- **Archivos Con Extensión Modificada**: Aquellos cuya extensión no es consistente con su contenido (para ello siempre es necesario verificar los encabezados de los archivos y no su extensión).

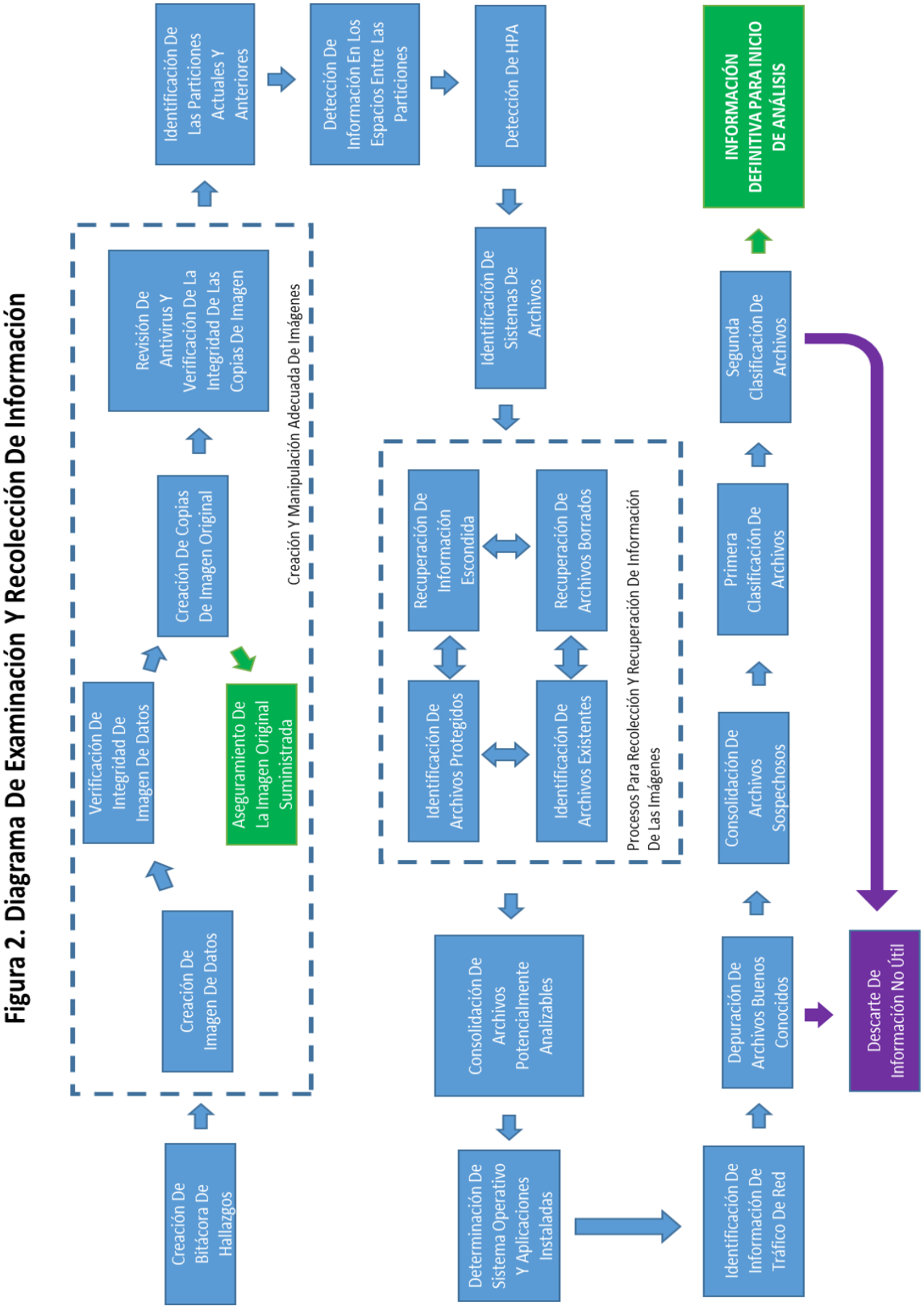
Los archivos que cumplen alguna de las anteriores características se convierten en archivos prioritarios para el análisis, ya que son sospechosos de haber sido alterados para no ser detectados. Los que no cumplen con alguna de estas 3 características se deben someter a la siguiente etapa de clasificación.

11.21. SEGUNDA CLASIFICACIÓN DE ARCHIVOS

Esta clasificación toma archivos que no han sido considerados de máxima prioridad, los examina y los evalúa respecto a dos criterios: relación de los archivos con los usuarios involucrados en la investigación y contenido relevante para el caso, derivado del marco circunstancial. De esta manera, se busca obtener información complementaria útil para la fase de análisis.

A continuación se muestra un diagrama que ilustra un posible orden lógico para la ejecución del procedimiento de examinación y recolección de información:

Figura 2. Diagrama De Examinación Y Recolección De Información



11.22. RECOMENDACIONES PARA EXAMINACIÓN Y RECOLECCIÓN DE INFORMACIÓN

- El analista forense deberá trabajar junto con el equipo de incidentes, para decidir la manera adecuada de contener el incidente permitiendo a su vez recolectar la mayor cantidad de información posible (siempre y cuando sea posible).
- En ocasiones el sistema afectado debe aislarse del entorno para disminuir el impacto del incidente o para preservar la evidencia (de hecho es el método más común).
- Debe evaluarse el impacto o la consecuencia de sacar un sistema de línea por mucho tiempo para poder generar las imágenes y/o copias de disco para la investigación, se debe evitar la mayor pérdida posible.
- Para realizar las manipulaciones de los sistemas, es pertinente que se tengan a la mano herramientas de tipo forense (software y hardware como una estación forense), que asegurará la integridad de la información a la hora de ser recolectada y verificada por primera vez.
- 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 forenses 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.
- **Es importante decidir hasta qué punto la organización se encontrará en capacidad de realizar la recolección y/o análisis de la evidencia que se presentará en las siguientes fases, es por ello que dependiendo el caso deberá contactarse al COLCERT o CCP para recibir instrucciones o colaboración en la realización de estos procedimientos.**

12. FASE IV. ANÁLISIS DE LA INFORMACIÓN

En esta fase se realizará un análisis de la información que logró extraerse de las diferentes fuentes y que se considera relevante o prioritaria para ser estudiada (después de realizar la depuración en las fases anteriores).

Dicho análisis puede involucrar y relacionar los eventos, archivos, logs, testimonios, fotografías, videos de vigilancia etc… para así llegar a alguna conclusión determinada.

Dentro del análisis de la información se involucran las siguientes etapas:

12.1. ANÁLISIS DE LA INFORMACIÓN PRIORITARIA.

Este proceso se basa en la discriminación de los archivos prioritarios con respecto a su relevancia con el caso y el criterio del investigador.

Es importante resaltar que los procesos de la segunda clasificación y análisis (Pasos **9.20** y **9.21**), pueden ser iterativos con el fin de obtener más cantidad de evidencia pertinente.

En cada iteración cada archivo de alta prioridad puede ser descartado o catalogado como archivo comprometido en el caso, y los archivos con poca prioridad son sometidos a una nueva iteración.

Este proceso cesa cuando el investigador, a partir de su criterio y experiencia, considera suficiente la evidencia recolectada para resolver el caso, o porque se agotan los datos por analizar.

12.2. GENERACIÓN DE LISTADO DE ARCHIVOS COMPROMETIDOS CON EL CASO.

Es el conjunto de archivos que forman parte de la evidencia del caso, este criterio es definido por el investigador, quien indicará lo que finalmente se empleará como evidencia a presentar en el informe final o en el proceso judicial según sea requerido.

12.3. OBTENCIÓN DE LA LÍNEA DE TIEMPO DE LA EVIDENCIA.

Se procede a realizar la reconstrucción de los hechos a partir de los atributos de tiempo de los archivos, lo que permite correlacionarlos enriqueciendo la evidencia.

Se debe tener en cuenta que muchos los sistemas pueden manejan varias estampas de tiempo para sus archivos. Las estampas de tiempo más comunes son:

- **Fecha De Modificación:** Indica la última vez que el archive fue modificado de cualquier manera, así sea a través de otro programa.
- **Fecha De Acceso:** Es la última vez que el archivo fue accedido (abierto, impreso o visto).
- **Fecha De Creación:** Es la fecha en la que el archivo fue creado por primera vez en un sistema, sin embargo, cuando un archivo es copiado hacia otro sistema, la fecha de creación se renovará para dicho sistema, sin embargo la fecha de modificación si permanecerá intacta.

Estas estampas de tiempo pueden llegar a ser fundamentales para el proceso de análisis del incidente de seguridad de la información que se encuentra activo o recientemente contenido, por ello, se recalca de la importancia de la sincronización de todos los sistemas de información (incluyendo PC, Laptops) a través de NTP.

En algunas ocasiones, y dependiendo del sistema de archivos del volumen analizado, puede ser imposible realizar un análisis temporal, situación que como todos los hallazgos, debe ser consignada en el informe final.

12.4. GENERACIÓN DE 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, apoyándose en la documentación continua de la aplicación metodológica.

13. FASE V. REPORTE

La fase final del procedimiento de evidencia digital es el reporte, el cuál presenta toda la información y la evidencia obtenida en la fase de análisis. Este reporte debería contemplar 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 la audiencia a la cual se presentará el informe, dado que si debe presentarse a nivel gerencial, el contenido técnico no debe tener la misma densidad que para un grupo de ingeniería, ya que en este punto es probable que se deba indicar exactamente ¿Qué ocurrió?, ¿En que 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 crimen), como por ejemplo mejorar 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.
- Recomendaciones relacionadas a mejoramiento en las políticas, procedimientos, herramientas de detección y otras observaciones para mejorar el proceso forense.

14. RECOMENDACIONES GENERALES

- La Cadena De Custodia, es esencial para el desarrollo de un buen procedimiento de evidencia digital, ya que brinda la confiabilidad de que la información ha sido manipulada apropiadamente asegurando su integridad.
- **Recurrir a las entidades públicas COLCERT y CCP para la gestión de incidentes de seguridad de la información, según el tipo de incidente que se presente (En la Guía # 25 "*Gestión De Incidentes De Seguridad De La Información*"), se dan indicaciones sobre este tema.**
  Las entidades deberán evaluar hasta que fase del procedimiento de evidencia digital pueden o desean llegar, pero siempre pueden recurrir a las instituciones mencionadas previamente.
- Los sistemas operativos pueden configurarse para auditar y almacenar ciertos tipos de eventos, como intentos de autenticación, cambios en las políticas de seguridad entre otra información útil.
- Los sistemas tipo SIEM con NTP configurado correctamente, son unas de las herramientas más poderosas de trazabilidad y de detección de incidentes o comportamiento anómalos. Es importante disponer de un sistema con estas características, de lo contrario, una gestión de logs de los dispositivos, puede ser de gran utilidad, debe invertirse en sistemas que permitan retener cantidades considerables de dichos logs.
- Siempre debe trabajarse con copias de la información original y a cada una de las copias deberá verificarse su integridad para certificar que sean copias válidas de la información base.
- Disponer de un kit forense (software, herramientas, estación forense) para realizar la obtención de la información necesaria en los sistemas, con el fin de asegurar la preservación de la integridad de la información a analizar y que pueda ser presentada como evidencia.
- Debe existir un grado de entrenamiento suficiente en las áreas de gestión de incidentes para poder realizar los procedimientos de evidencia forense, así como también deben poseer conocimientos sobre protocolos de red, aplicaciones, amenazas basadas en red y métodos de ataque.
- Siempre debe primar el restablecimiento del servicio y la contención del impacto del incidente que el encontrar el responsable de los mismos (es decir realizar la toma de evidencia forense).

15. BIBLIOGRAFÍA

- NIST 800-86 *Guide to Integrating Forensic Techniques into Incident Response*.
- ISO/IEC 27035, Information Technology. Security Techniques. Information Security incident management
- ISO/IEC 27000, Information Technology. Security Techniques. Information Security Management Systems. Overview and Vocabulary
- ISO/IEC 27001, Information Technology. Security Techniques. Information Security Management Systems. Requirements
- Manual de Manejo de Evidencias Digitales y Entornos Informáticos. Versión 2.0, ***Organización De Estados Americanos***