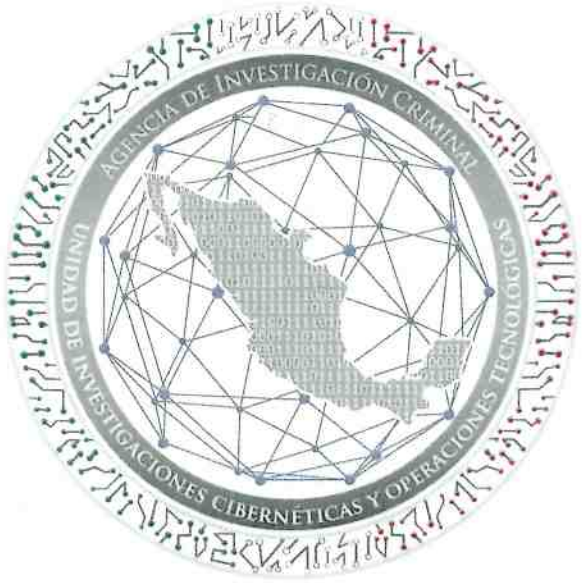


UNIDAD DE INVESTIGACIONES CIBERNÉTICAS
Y OPERACIONES TECNOLÓGICAS

AGENCIA DE INVESTIGACIÓN CRIMINAL

GUIA TÉCNICA DE CADENA DE CUSTODIA DE EVIDENCIA DIGITAL

JUNIO 2018

Relación Jurídica

La presente guía técnica utiliza como sustento los siguientes ordenamientos legales:

- Constitución Política de los Estados Unidos Mexicanos.
- Ley General del Sistema Nacional de Seguridad Pública.
- Código Nacional de Procedimientos Penales, y
- Código Penal Federal.

Instrumentos Internacionales

- Declaración Universal de los Derechos Humanos.
- Convención Americana sobre los Derechos Humanos.
- Convención de Palermo sobre Delincuencia Organizada Transnacional.
- Convención de las Naciones Unidas contra la Corrupción (ONU).
- Convención Internacional para la protección de todas las personas contra las desapariciones forzadas.
- Convención contra la Tortura y Otros Tratos o Penas Crueles, Inhumanos o Degradantes.
- Código de conducta para funcionarios encargados de hacer cumplir la ley.
- Manual de la escena del delito y las pruebas materiales. Sensibilización del personal no forense sobre su importancia.

Leyes Locales

- Constituciones Estatales.
- Leyes relacionadas con la Seguridad Pública e Instituciones Policiales de las Entidades Federativas.
- Leyes Orgánicas de las Procuradurías Generales o Fiscalías del Estado, y
- Códigos Penales de las Entidades Federativas.

Otros Instrumentos

- **Acuerdo A/009/15** de la Procuraduría General de la República, por el que se establecen las directrices que deberán observar los servidores públicos que intervengan en materia de Cadena de Custodia.
- **Protocolo Nacional de Actuación de Primer Respondiente.**
- **Guía Nacional de Cadena de Custodia.**

Objetivos

Generales

- Definir las acciones de todo servidor público, en los tres órdenes de gobierno, particularmente aquellos que den pronta respuesta a incidentes en los cuales existan indicios o elementos materiales probatorios relacionados con el entorno digital, para que sean capaces de reconocer, recopilar y salvaguardar los indicios o elementos materiales probatorios digitales y abordar situaciones donde han de ser localizados, descubiertos y/o aportados.

- Garantizar la mismidad y autenticidad de los indicios o elementos materiales probatorios digitales, para que reflejen la continuidad y trazabilidad dentro de la Cadena de Custodia y sean incorporados como pruebas en el proceso penal.

Específicos

- Homologar las actuaciones de los servidores públicos para el debido manejo de los indicios o elementos materiales probatorios digitales.
- Describir los lineamientos básicos para el uso e implementación de esta guía, mejorando el desempeño y eficiencia de los servidores públicos que tengan contacto con indicios o elementos materiales probatorios digitales.
- Estandarizar la ejecución del trabajo durante el manejo de los indicios o elementos materiales probatorios digitales, desde su localización, descubrimiento y/o aportación, hasta su disposición final.

Destinatarios de la guía

La guía está dirigida a los servidores públicos que tengan contacto con los indicios o elementos materiales probatorios digitales para su aseguramiento y conservación, así como hacer el registro de las modificaciones que sufran desde su recolección hasta su disposición final.

Actores

- Primer Respondiente.
- Policía.
- Policía de Investigación.
- Perito.
- Personal Facultado para el Traslado.
- Personal especializado.
- Encargado de bodegas de indicios y evidencias.
- Agente del Ministerio Público.

Roles.

- **Primer Respondiente:** Informa y entrega el lugar de intervención al Policía de Investigación; brinda apoyo en lo conducente.

- **Policía:** Realiza la preservación del lugar, traslado y entrega de los indicios o elementos materiales probatorios digitales, coordinándose con la Policía de Investigación y el Ministerio Público.

- **Policía de Investigación:** Dirigir los actos de investigación, coordinándose con los intervinientes durante el procesamiento y el traslado.

- **Perito:** Realizar las actividades del procesamiento de los indicios o elementos materiales probatorios digitales, dar recomendaciones para el traslado. Recibir y analizar los indicios o elementos materiales digitales en las instalaciones de servicios periciales y emitir el informe, requerimiento o dictamen correspondiente.

- **Personal Facultado para el Traslado:** Trasladar los indicios o elementos materiales probatorios, embalado, sellado, etiquetados, firmados con su respectiva Cadena de Custodia Digital.

- **Personal Especializado:** Realiza la recolección y traslado de los indicios o elementos materiales probatorios que requieren un manejo y control especial.

- **Encargado de bodegas de indicios y evidencias:** Recibir, registrar y custodiar los indicios o elementos materiales probatorios, anotar su participación en el respectivo registro de Cadena de Custodia Digital; documentar los ingresos y egresos de los indicios o elementos materiales probatorio digitales en la bodega de indicios y evidencias.

- **Ministerio Público:** Conducción y mando de la investigación de los delitos, ordenar y/o supervisar la aplicación de las medidas para impedir que se pierda, destruyan o alteren los indicios o elementos materiales probatorios digitales, además de verificar que se han seguido los protocolos correspondientes para su preservación y procesamiento.

Procedimiento

La presente guía consta de cuatro etapas que son **procesamiento**, **traslado**, **análisis** y **almacenamiento**, las cuales se describen a continuación.

I. Procesamiento

Etapa inicial en la cual el Policía de Investigación, perito, servidor público y/o el personal especializado detecta, preserva y conserva los indicios o elementos materiales probatorios digitales dentro del lugar de intervención, concluyendo con el traslado para su análisis.

Preservación

Se deberá llevar a cabo la preservación del lugar de la intervención por el Primer Respondiente que arribe, quien deberá corroborar los hechos y los datos aportados previamente. A continuación, custodiará y dará vigilancia al lugar de intervención con el fin de evitar cualquier acceso indebido que pueda causar la pérdida, destrucción, alteración o contaminación de los indicios o elementos materiales probatorios digitales.

Identificación de posibles fuentes de información

Al momento de su intervención el personal especializado y/o perito realizará una observación del lugar de intervención para la detección de las fuentes de datos, siendo las más comunes computadoras de escritorio, los servidores, los dispositivos de almacenamiento en red y las computadoras portátiles. Estos sistemas suelen tener unidades que aceptan medios, como CD y DVD, al igual que tienen distintos tipos de puertos para el almacenamiento de datos externos como memorias USB, tarjetas de memoria flash, discos ópticos y magnéticos.

Los diversos sistemas informáticos pueden contener datos volátiles (que están disponibles temporalmente). Además, existe una gran variedad de dispositivos digitales portátiles (PDA, teléfonos celulares, cámaras digitales, grabadoras digitales, reproductores de audio, tabletas, relojes inteligentes y de manera general dispositivos con Internet de la Cosas (IoT, por sus siglas en inglés) los cuales se convierten en fuentes que pueden contener datos útiles. Los intervinientes serán capaces de examinar cualquier área física como una oficina y reconocer las posibles fuentes de datos, también catalogarán posibles fuentes de datos ubicadas en otros lugares dado que la información también puede ser grabada por otras entidades, como registros de actividad de red para un proveedor de servicios de Internet (ISP, CCT, etc).

Además, priorizar todas las conexiones de las cuales dependan los equipos informáticos, como: fuentes de alimentación eléctrica, conexiones físicas de red, conexiones inalámbricas a redes digitales, o cualquier otro tipo; con la finalidad de mantener el estado del equipo y se garantice el aislamiento total de personas, programas y/o procesos ajenos a la investigación de manera física o remota.

Extracción de Datos.

Después de identificar fuentes de datos potenciales, el servidor público necesitará obtener los datos de las fuentes. La adquisición de datos debe realizarse mediante un proceso de tres pasos que implica desarrollar un plan para adquirir los datos y verificar la integridad de los mismos.

1. **Plan para la extracción de datos.** En todos los casos, el personal especializado y/o perito deberán crear un plan que priorice las fuentes, estableciendo el orden en que se deben adquirir. Los factores para la priorización de datos e información son los que a continuación se señalan:

- **Valor probable.** Con base en la comprensión del personal especializado y/o perito de la situación, y la experiencia previa en situaciones similares, debe ser capaz de estimar el valor probable relativo de cada posible fuente de datos.
- **Volatilidad.** En muchos casos, la adquisición de datos volátiles debe tener prioridad sobre los datos no volátiles. Sin embargo, los datos no volátiles también pueden ser de naturaleza algo dinámica, como los archivos de registro que se sobrescriben a medida que ocurren nuevos eventos.
- **Cantidad de esfuerzo requerido.** El esfuerzo involucra no solo el tiempo dedicado por los servidores públicos, sino también el costo de los equipos y servicios.

En algunos casos, hay tantas fuentes de datos posibles que no es práctico adquirirlas todas por lo tanto es importante determinar qué fuentes se obtienen.

2. **Extracción de los datos**. El proceso general para extraer datos implica el uso de herramientas forenses especializadas para recopilar datos, duplicar fuentes de datos y asegurar el original. La extracción de datos se puede realizar de manera localmente o en una red. Por lo general, es recomendable extraer datos localmente debido a que hay un mayor control sobre el sistema y los datos. La recopilación local de datos no siempre es factible, por ejemplo, sistema en la habitación cerrada, sistema en otra ubicación. Al extraer datos a través de una red deben tomarse decisiones con respecto al tipo de datos que se recopilarán y la cantidad de esfuerzo que se utilizará; podría ser suficiente copiar un volumen lógico desde un solo sistema.

3. **Verifique la integridad de los datos**. Después de que los datos hayan sido extraídos, su integridad debe ser verificada. La verificación de la integridad de los datos usualmente consiste en utilizar herramientas específicas (*hardware* o *software*) para realizar una copia *bit* a *bit* del original, donde el uso de las herramientas es en sí una garantía de su integridad.

Se debe mantener un registro detallado de cada paso que se realizó para la recopilación de datos, incluida la información sobre cada herramienta utilizada en el proceso. La documentación en registro en la Cadena de Custodia Digital permite mantener la integridad del indicio o elemento material probatorio.

El servidor público debe dejar registro antes de interactuar con un sistema y/o dispositivo.

Recolección de indicios o elementos materiales digitales
El primer paso para la recolección consiste en ubicar las de posibles fuentes de información, así como dispositivos que se encuentren dentro del lugar de intervención.

La recolección deberá realizarse de forma manual, instrumental o digital de acuerdo a su tipo, con la finalidad de garantizar la integridad, autenticidad e identidad del indicio o elemento material probatorio, evitando su destrucción o alteración. Todo indicio o elemento material probatorio

digital, es frágil y alterable, lo cual debe de ser considerado para determinar embalaje y empaque adecuado.

Cada elemento debe de ser embalado de manera individual preferentemente, finalizando con el sellado, etiquetado y firma del responsable del procesamiento.

Documentación de los datos obtenidos

Previamente al llenado del registro de cadena de custodia digital, se deberá realizar un inventario completo de todos los indicios o elementos materiales probatorios digitales localizados en el lugar de la intervención, describiendo todas sus características, conexiones, estado en el que se encuentra y el lugar donde se ubica, sin olvidar registrar el estado de sus conexiones.

El registro de cadena de custodia digital, deberá contener la descripción de cada indicio o elemento material probatorio, y el tipo de documentación utilizada (fotográfica, videográfica y/o escrita). Se anexará el nombre, cargo, adscripción de los servidores públicos que participen en el procesamiento anexando copia de una identificación oficial.

En la cadena de custodia digital, se deberá hacer una descripción detallada del embalaje utilizado para cada uno de los indicios o elementos materiales probatorios digitales, al igual que las recomendaciones pertinentes para el traslado.

Todo indicio o elemento material probatorio digital deberá ser descrito a través de la percepción de los sentidos del interviniente, dando a notar las características específicas de cada uno, además de poder apoyarse de fichas técnicas, etiquetas, o textos.

II. Traslado

El servidor público que lleve a cabo el traslado tiene como encomienda, transportar los indicios o elementos materiales probatorios digitales, debidamente embalados, sellados, etiquetados, firmados y con el registro de Cadena de Custodia Digital, del lugar de intervención, hacia el lugar determinado por parte del Ministerio Público o el Órgano Jurisdiccional, dichos lugares pueden ser los servicios periciales, la bodega de indicios, las Instituciones que cuenten con áreas forenses, o a algún otro lugar con condiciones de preservación o conservación, en cumplimiento a las recomendaciones de los especialistas.

III. Análisis

Obtención de pruebas digitales

Dentro de una investigación donde se trabaja con indicios o elementos materiales probatorios digitales, se debe considerar que además de recabarlos, se tiene que sumar las marcas de tiempo relacionadas con cada uno de ellos, esto incluyendo el momento en el que se modificaron por última vez o se accedió a ellos.

El personal especializado y/o perito deberá de seleccionar los archivos, datos o elementos que serán útiles para su intervención y, a su vez, excluir aquellos que no sean relevantes. Una manera de

delimitar la información con la cual realizará su investigación será excluyendo todo dato que pone en riesgo la información sensible de personas, instituciones o empresas, entre otros mecanismos.

Durante la recopilación de datos, el personal especializado y/o perito deberá realizar copias múltiples de los archivos o sistemas de archivos considerados relevantes para la investigación, creando de esta manera una copia maestra y una copia de trabajo. Se usará siempre la copia de trabajo a manera de garantizar la integridad de los archivos originales y de la copia maestra.

Tipos de copiado

Existen dos tipos de copiado que se deben considerar en una investigación:

- **Logical Backup**: Aquella donde se realiza una copia de los directorios y archivos de un volumen lógico, ésta no captura otros datos que puedan estar presentes en los medios, como los archivos eliminados o los datos residuales almacenados en un espacio libre, este método NO debe de ser utilizado por el personal especializado y/o perito, dado que no garantiza de manera alguna la integridad de los datos involucrados.
- **Bit Stream Imaging (Imagen Forense):** Método que genera una copia *bit* a *bit* de los medios originales, por lo cual requieren más espacio de almacenamiento y tardan más en realizarse que una de tipo **Logical Backup**. Sin embargo, proporciona una garantía de la integridad de los datos, por lo cual debe de ser el único método implementado en una investigación.

Una vez obtenidas tanto la copia maestra y la copia de trabajo deberán ser documentadas en el registro de cadena de custodia digital, y al finalizar la intervención del personal especializado y/o perito deberán de ser tratadas como indicios o elementos materiales probatorios digitales; por ello, serán manejadas con la debida cautela, con la intención de garantizar su preservación y su mismidad, siendo empaquetadas, embaladas, selladas, etiquetadas y firmadas. Por último, el personal especializado y/o perito emitirá las recomendaciones de traslado y resguardo.

Integridad de los datos

Para garantizar el proceso de creación de la copia maestra como de trabajo, el personal especializado y/o perito usará un bloqueador de escritura para no alterar los datos en los medios originales.

Después de realizar una copia maestra y de trabajo, es importante verificar que los datos copiados sean un duplicado exacto de los datos originales, utilizando para ello la firma digital (*hash*) que identifica de manera única los datos y tiene la propiedad de que al cambiar un solo *bit* en los datos se generará una firma digital completamente diferente. Aun cuando existen muchos algoritmos para calcular la firma digital, deberá emplearse el SHA-256, SHA, o MD5 los cuales son estándares seguros, un ejemplo de esto sería:

SHA-256: 00C6EEB22B936CBD5696D12A2877C398A81D5DBBC7366FCE59DDE78730B4520D

La firma digital del medio original se debe calcular y registrar antes de realizar la imagen. Después de la creación, la firma digital de las copias maestra y de trabajo se debe calcular y comparar con la firma digital del original para verificar que se haya preservado la integridad de los datos. A su vez la firma digital de los medios originales se debe volver a calcular para verificar que el proceso de creación de imágenes no alteró al original, y todos los resultados deben registrarse.

Propiedades de un archivo

Es importante saber cuándo se creó, usó y manipuló un archivo, la mayoría de los sistemas operativos realizan un seguimiento de ciertas marcas de tiempo relacionadas con los archivos. Las marcas de tiempo más comúnmente utilizadas son los tiempos de creación, acceso y modificación, los cuales se describen a continuación:

- **Tiempo de creación.** Por lo general, esta es la hora y fecha en que se creó el archivo; sin embargo, cuando se copia un archivo a un sistema, el tiempo de creación se convertirá en la hora en que se copió el archivo en el nuevo sistema. El tiempo de modificación permanecerá intacto.
- **Tiempo de acceso.** Esta es la última vez que se realizó un acceso a un archivo (por ejemplo, visto, abierto, impreso).
- **Tiempo de modificación.** Esta es la última vez que se cambió un archivo de alguna manera, incluso cuando se escribe un archivo y otro programa lo cambia.

Los sistemas Windows conservan la última hora de modificación, la última hora de acceso y la hora de creación de los archivos. Los sistemas UNIX conservan la última modificación, el último cambio y los últimos tiempos de acceso; sin embargo, algunos sistemas UNIX (incluidas en las versiones de BSD y SunOS) no actualizan la última hora de acceso de los archivos ejecutables. Algunos sistemas UNIX registran el momento en que los metadatos de un archivo fueron modificados recientemente.

Si el personal especializado y/o perito necesitara establecer una línea de tiempo precisa de los eventos, entonces los tiempos de archivo deben conservarse. En consecuencia, el personal especializado y/o perito deberá ser consciente de que no todos los métodos para recopilar archivos de datos pueden conservar los tiempos de archivo.

Las *Bit Stream Imaging* (Imagen Forense) pueden conservar los tiempos de archivos porque se genera una copia de *bit* por *bit*. Realizar una copia de seguridad lógica con algunas herramientas pueden altear los tiempos de creación de archivos cuando se copia el archivo de datos; por este motivo, siempre que los tiempos de archivo sean esenciales, se deben usar imágenes de flujo de bits para recopilar datos. Los servidores públicos deben saber que los tiempos de archivo pueden no ser siempre precisos. Entre los motivos de tales imprecisiones se encuentran los siguientes:

- El reloj de la computadora no tiene la hora correcta.
- Es posible que el tiempo no se registre con el nivel de detalle esperado.
- Un atacante puede haber alterado los tiempos del archivo grabado.

Después de realizar una copia de seguridad lógica o una secuencia de *bits*, se debe acceder a los datos solo en forma de lectura para garantizar que los datos que se examinan no se modifiquen y que proporcionen resultados consistentes en las sucesivas ejecuciones.

Localización de Archivos

El primer paso en el examen es ubicar los archivos. Una imagen forense puede capturar muchos gigabytes de espacio libre, que podría contener una cantidad importante de archivos y fragmentos de archivos. La extracción manual de datos del espacio libre no utilizado puede ser un proceso lento, ya que requiere conocimiento del formato subyacente del sistema de archivos. Se puede automatizar el proceso de extracción de datos del espacio no utilizado y guardarlo en archivos de

datos, así como recuperar archivos y aquellos archivos eliminados dentro de una papelera de reciclaje.

Extracción de datos

El resto del proceso implica extraer datos de algunos o todos los archivos. Para dar sentido al contenido de un archivo, el personal especializado y/o perito necesita conocer qué tipo de datos contiene el archivo. El propósito de las extensiones de archivo es denotar la naturaleza del contenido de los archivos; por ejemplo, una extensión jpg indica un archivo gráfico, y una extensión mp3 indica un archivo de audio. Sin embargo, los usuarios pueden asignar cualquier extensión de archivo a cualquier tipo de archivo, como nombrar un archivo de texto mysong.mp3 u omitir una extensión de archivo. Además, algunas extensiones de archivos pueden estar ocultas o no ser compatibles en otros sistemas operativos. Por lo tanto, el personal especializado y/o perito no deberá suponer que las extensiones de archivos son precisas.

El personal especializado y/o perito puede identificar con mayor precisión el tipo de datos almacenados en muchos archivos mirando sus encabezados de archivo, los cuales podría ubicarse en un archivo separado de los datos de archivo reales. Otra técnica efectiva para identificar el tipo de datos en un archivo es un histograma simple que muestra la distribución de valores ASCII como un porcentaje del total de caracteres en un archivo. Otros patrones son indicativos de archivos encriptados o modificados mediante esteganografía.

Los usuarios pueden cifrar archivos, carpetas, volúmenes o particiones individuales para que otros no puedan acceder al contenido sin una clave de descifrado. El cifrado puede ser realizado por el sistema operativo o un programa de terceros. El personal especializado y/o perito podría identificar el método de encriptación examinando el encabezado del archivo, identificando los programas de cifrado instalados en el sistema o buscando claves de cifrado (que a menudo se almacenan en otros medios). Una vez que se conoce el método de encriptación, el personal especializado y/o perito puede determinar mejor la viabilidad de descifrar el archivo. En muchos casos, no es posible descifrar archivos porque el método de cifrado es sólido y la autenticación utilizada para realizar el descifrado no está disponible.
Algunas de las técnicas que el personal especializado y/o perito realiza incluye buscar metadatos y registros, usar histogramas y conjuntos de hash para buscar software de esteganografía conocido. Una vez que los datos estén disponibles, el personal especializado y/o perito podrá extraer los datos incrustados al determinar qué software creó los datos, o usar la fuerza bruta y los ataques criptográficos para determinar una contraseña.

El personal especializado y/o perito también puede necesitar acceder a archivos protegidos por contraseñas. Las contraseñas a menudo se almacenan en el mismo sistema que los archivos que protegen, pero en un formato codificado o encriptado. La mayoría de las utilidades forenses pueden intentar adivinar contraseñas, así como realizar intentos de fuerza bruta que prueban todas las contraseñas posibles. El tiempo necesario para un ataque de fuerza bruta contra una contraseña codificada o encriptada puede variar mucho, dependiendo del tipo de cifrado utilizado y la sofisticación de la contraseña en sí. Otro enfoque es eludir una contraseña.

Descompresión, descifrado y reproducción de archivos

El personal especializado y/o debe tener acceso a varias herramientas que les permitan realizar exámenes y análisis de datos, así como algunas actividades de recopilación. El kit de herramientas forenses debe contener aplicaciones que puedan realizar análisis de datos de muchas maneras y que se puedan ejecutar de manera rápida y eficiente desde disquetes, CD o una estación de trabajo forense. Los siguientes procesos se encuentran entre los que un analista debería poder realizar con una variedad de herramientas:

- **Visores de archivos**. Usar visores en lugar de las aplicaciones originales para mostrar los contenidos de ciertos tipos de archivos es una técnica importante para escanear o previsualizar datos, y es más eficiente porque el personal especializado y/o perito no necesita aplicaciones nativas para ver cada tipo de archivo. Varias herramientas están disponibles para ver tipos comunes de archivos, y también hay herramientas especializadas únicamente para ver gráficos.

- **Descomprimir archivos.** Los archivos comprimidos pueden contener datos con información útil, así como otros archivos comprimidos. Por lo tanto, es importante que el servidor público ubique y extraiga archivos comprimidos. La descompresión de los archivos se debe realizar al principio del proceso forense para garantizar que el contenido de los archivos comprimidos se incluya en las búsquedas y otras acciones.

- **Muestra gráfica de directorios.** Esta práctica facilita y agiliza que los servidores públicos recopilen información general sobre los contenidos de los medios, como el tipo de software instalado y la aptitud técnica probable de los usuarios que crearon los datos. La mayoría de los productos pueden mostrar estructuras de directorios de Windows, Linux y UNIX, mientras que otros productos son específicos de las estructuras de directorios de Macintosh.

- **Identificación de archivos conocidos**. Es beneficioso eliminar archivos sin importancia, como el sistema operativo y los archivos de la aplicación. El personal especializado y/o perito debe usar conjuntos de hash validados, como base para identificar archivos conocidos benignos y maliciosos.

- **Búsquedas de cadenas y coincidencias de patrones.** Las búsquedas de cadenas ayudan a leer grandes cantidades de datos para encontrar palabras clave o cadenas. Varias herramientas de búsqueda están disponibles que pueden usar lógica booleana, lógica difusa, sinónimos y conceptos, derivación y otros métodos de búsqueda. Las búsquedas comunes incluyen encontrar varias palabras en un solo archivo y localizar versiones mal escritas de ciertas palabras. Desarrollar conjuntos concisos de términos de búsqueda para situaciones comunes puede ayudar al personal especializado y/o perito a reducir el volumen de información para revisar.

- **Análisis de los datos extraídos.**
  El personal especializado y/o perito debe conocer el valor de utilizar los tiempos del sistema y los tiempos de archivo. Saber cuándo ocurrió un incidente, crear o modificar un archivo o enviar un correo electrónico puede ser crítico para el análisis forense, dicha información se puede usar para reconstruir una línea de tiempo de actividades. Aunque esto puede parecer una tarea simple, a menudo se complica por discrepancias intencionales o no intencionadas

en la configuración de tiempo entre los sistemas. Conocer las configuraciones de hora, fecha y zona horaria de una computadora cuyos datos se analizarán puede ser de gran ayuda para el desarrollo de una intervención del personal especializado y/o perito.

Informes y/o dictamen

Es el proceso de preparación y presentación de la información resultante de la fase de análisis. El personal especializado y/o perito deberá considerar la emisión de dos tipos de informes:

- **Informe Técnico.** El cual deberá expresar las técnicas, secuencias de obtención de datos, *software*, *hardware* y la manera en la que fueron manipulados para la obtención de los resultados. Los especialistas en la rama podrán requerir informes muy detallados de toda la información recopilada, y también puede requerir copias de todos los datos probatorios obtenidos.

- **Informe Ejecutivo.** Este explicará los resultados obtenidos con un lenguaje claro y entendible para cualquier persona ajena al lenguaje especializado. La alta dirección podría simplemente querer una visión general de alto nivel de lo que sucedió, como una representación visual simplificada de cómo ocurrió el ataque y qué se debe hacer para evitar incidentes similares.

- **Dictamen.** En este se plasman el resultado del análisis realizado por los peritos, que muestra la secuencia del estudio efectuado, los métodos y medios empleados. Todo dictamen deberá contener lo descrito a continuación.
  - Descripción de los elementos estudiados
  - Relación detallada de todos los análisis.
  - Los medios científicos o técnicos empleados y su verificación de que han sido validos para emitir un dictamen.
  - Las conclusiones a las que ha llegado a partir de lo anterior.

Cuando la información sobre un evento es incompleta, puede no ser posible llegar a una explicación definitiva de lo sucedido. Cuando un evento tiene dos o más explicaciones, deben ser consideras en el proceso de informe. El personal especializado y/o perito deberá usar un enfoque metódico para intentar probar o refutar cada posible explicación que se propone.

IV. Almacenamiento

Durante esta etapa se almacenan los indicios o elementos materiales probatorios digitales en alguna de las bodegas destinadas para dicho fin, previa autorización por parte del Ministerio Publico, el cual designará al servidor público que será encargado de realizar el traslado del indicio o elemento material probatorio digital, desde el lugar de intervención hasta su almacenamiento en la bodega de indicios.

Una vez que el servidor público arribe a la Bodega de indicios, el responsable de la misma recibirá los indicios o elementos materiales probatorios digitales, previa revisión de los mismos verificando

que la información contenida en la Cadena de Custodia Digital coincida con el indicio o elemento material probatorio digital presentado.

En caso de que sea necesario la salida de un indicio o elemento materia probatorio, solo será por dos razones:

1. **Salida temporal.** Tendrá que ser solicitada ante el Ministerio Público conteniendo el motivo de la salida y el servidor público que será designada para su traslado. Toda esta actividad se registrará en el sistema de la bodega de indicios.

2. **Salida definitiva.** La solicitud será emitida por parte de la autoridad competente, la cual se pronuncia acerca del destino final del indicio o elemento material probatorio. Toda esta actividad se registrará en el sistema de la bodega de indicios.

Glosario de definiciones

Archivo: Equivalente digital a archivos escritos u expedientes compuesto por un conjunto de bits que se almacena de forma ordenada dentro de un dispositivo digital.

Bit: Es la unidad mínima de información dentro de la informática, la cual puede obtener tan solo dos valores.

Bloqueador: Herramienta basada en hardware o software que impide que una computadora escriba en un medio de almacenamiento informático conectado a ella.

Bodega de indicios: Lugar con características específicas que tiene como finalidad el resguardo de indicios o elementos materiales probatorios para garantizar su integridad.

Byte: Conjunto de 8 bits el cual es el mínimo elemento de almacenamiento en una computadora.

Cadena de custodia: Sistema de control y registro que se aplica al indicio o elemento material probatorio, desde su localización, descubrimiento o aportación, en el lugar de intervención, hasta que la autoridad competente ordene su conclusión.

Cámara digital: Cámara fotográfica que, en vez de captar y almacenar fotografías en película química, recurre a un sensor electrónico que almacena las imágenes en una memoria.

CD (Compact Disc, por sus siglas en inglés): Es un disco óptico utilizado para almacenar datos, en formato digital.

Cifrado: En un procedimiento que utiliza un algoritmo con cierta clave para transformar un mensaje, sin modificar su estructura.

Código ASCII (American Standrad Code for Information Exchange, por sus siglas en inglés): Código basado integralmente en el alfabeto latino, que tiene distintos usos.

Computadora: Dispositivo electrónico, utilizado para el procesamiento de datos, el cual a su vez cuenta con dispositivos de entrada y salida los cuales le permiten a un usuario la interacción.

Conexiones: Es el enlace que se establece entre el emisor y el receptor a través del que se envía el mensaje.

Datos Volátiles: Se refiere a datos sensibles, es decir, que fácilmente pueden perderse o modificarse, perdiendo el valor de la información.

Dirección IP: Número único e irrepetible con el cual se identifica un dispositivo informático que se encuentre conectado a internet.

Directorio: Estructura que organiza los archivos que se utilizan.

Dispositivo Informático: Todo aquel dispositivo que cuenta con un sistema operativo, integrado por diferentes programas con uno o más propósitos, el cual puede ser o no manipulado por un usuario para su funcionamiento, el cual cuenta con diversas conexiones tanto materiales tangibles como lógicas.

DVD (Digital Versátil Disc, por sus siglas en inglés): Es el dispositivo que hace referencia a la multitud de maneras en las que se almacenan los datos.

Embalaje: Conjunto de materiales que envuelven, soportan, contienen y protegen al indicio o elemento material probatorio, con la finalidad de identificarlos, garantizar su mismidad y reconocer el acceso no autorizado durante su traslado y almacenamiento. El embalaje constituye un refuerzo del empaque y, en algunos casos, podrá fungir como empaque del indicio o elemento material probatorio.

Empaque: Todo aquel material que se utiliza para contener, proteger y/o preservar indicios o elementos materiales probatorios, relacionados con el hecho delictivo, que comprende las etapas de recolección, embalaje y etiquetado.

Encriptación: Es una manera de codificar la información para protegerla frente a terceros.

Equipamiento: Materiales para el procesamiento de indicios o elementos materiales probatorios y equipo de protección personal.

Equipo de protección personal: Cualquier equipo, objeto o instrumento que emplea el interviniente, para crear una barrera física entre él, el sitio de intervención, los indicios y las personas involucradas en un hecho, con la finalidad de evitar riesgos a la salud y la perdida, alteración, destrucción o contaminación de los indicios o elementos materiales probatorios.

Equipo informático: Sistema que permite almacenar y procesar información; es el conjunto de partes interrelacionadas: hardware y software.

Esteganografía: Es la disciplina que estudia el conjunto de técnicas cuyo fin es la ocultación de la información sensible, mensajes u objetos, dentro de otros contenedores, normalmente multimedia (imágenes digitales, videos o archivos de audio, etc.)

Etiqueta: Letrero escrito o impreso, que se añade al embalaje para identificarlo.

Etiquetado: Acción de adherir al embalaje la etiqueta tomando en consideración los siguientes.

Datos: Número de folio o equivalente, identificación del indicio, fecha y hora de recolección y tipo de indicio o elemento material probatorio.

Firma digital (HASH): Es un algoritmo matemático que transforma cualquier bloque arbitrario de datos en una nueva serie de caracteres con una longitud fija.

Grabadora digital: Es también conocidas como grabadora digital de voz, una grabadora digital no emplea cintas sino guarda los archivos en formato digital.

Hardware: Conjunto de elementos físicos que constituyen una computadora o sistema informático.

Histograma: Es una representación gráfica de una variable en forma de barras, donde la superficie de cada barra es proporcional a la frecuencia de los valores representados.

Identificación: Término utilizado para asignar un número, letra o una combinación de ambos, a los indicios o elementos materiales probatorios, en el momento de su localización, descubrimiento o aportación, hasta que la autoridad competente ordene la conclusión de la Cadena de Custodia.

Indicio: Término genérico empleado para referirse a huellas, vestigios, señales, localizados, descubiertos o aportados, que pudieran o no estar relacionados con un hecho que la ley señala como delito y, en su caso, constituirse en un elemento material probatorio.

Indicio digital: Es todo aquel conjunto de datos, archivos o registros, enviados, guardados, procesados en un dispositivo informático.

IoT (Internet of Things): Hace referencia a la interconexión digital de objetos cotidianos con internet.

Internet: Conjunto de redes lógicas que se interconectan a través de protocolos para poder comunicarse entre sí.

ISP (Proveedor de Servicios de Internet): es una organización que ofrece a sus usuarios acceso a Internet.

Lugar de intervención: Sitio en el que se ha cometido un hecho presuntamente delictivo, o en el que se localizan o aportan indicios relacionados con el mismo.

Marca de Tiempo: es una secuencia de caracteres que denotan la hora y fecha en las que ocurrió determinado evento.

Metadatos: Los metadatos son datos de datos; para los sistemas de archivos, los metadatos son datos que proporcionan información sobre el contenido de los archivos.

Observación: Detectar o reconocer los indicios o elementos materiales probatorios, mediante la aplicación de las técnicas de búsqueda seleccionadas (líneas, franjas, criba, espiral, entre otros).

Orientación: Se da referencia del lugar y la dirección de los indicios, con base a la ubicación del punto cardinal norte.

PDA (Personal Digital Assistant): Ayudante Personal Digital, es un dispositivo de pequeño tamaño que combina un ordenador, teléfono/fax, Internet y conexiones de red.

Preservación del indicio: Acciones para asegurar, resguardar, proteger y mantener el indicio o elementos materiales probatorios, con el objeto de mantener las condiciones originales de recolección, evitando la pérdida, alteración, destrucción o contaminación de los indicios o elementos materiales probatorios.

Preservación del Lugar: Acciones para custodiar y vigilar el lugar de los hechos o del hallazgo, con el fin de evitar cualquier acceso indebido, que pueda causar la pérdida, destrucción, alteración o contaminación de los indicios o elementos materiales probatorios.

Primer Respondiente: Es la primera autoridad con funciones de seguridad pública en el lugar de la intervención.

Priorización de indicios: Recolectar indicios o elementos materiales probatorios de forma inmediata, con el fin de prever riesgos asociados a la pérdida, alteración, contaminación y destrucción.

Programa: Secuencia de instrucciones con el propósito de realizar una tarea específica en un dispositivo informático.

Recolección: Acción de levantar los indicios o elementos materiales probatorios, mediante métodos y técnicas que garanticen su integridad.

Registro de Cadena de Custodia Digital: Documento en el que se registran los indicios digitales o elementos materiales probatorios y las personas que intervienen, desde su localización, descubrimiento o aportación en el lugar de intervención, hasta que la autoridad ordene su conclusión.

Reproductor de audio: Es un tipo de reproductor para la reproducir de audio digital.

Sellado: Consiste en cerrar el embalaje, empleando medios adhesivos o térmicos, que dejen rastros visibles cuando sea abierto indebidamente o sin autorización.

Servidor: Es una aplicación en ejecución (software) capaz de atender las peticiones del cliente y devolverle una respuesta en concordancia.

SHA (Secure Hash Algorithm, por sus siglas en inglés): Es una función hash criptográfica que toma una entrada y produce un valor de salida, conocido como resumen del mensaje, normalmente presenta un numero hexadecimal de 40 dígitos.

Sistema informático: Conjunto de partes compuestas por hardware, software y sujetos que interactúan con él, los cuales se interrelacionan entre sí con algún propósito relacionado con la computación.

Sistema operativo: Conjunto de programas que gestiona los recursos tanto tangibles como intangibles de una computadora o dispositivo informático.

Software: Conjunto de elementos no tangibles, conocidos como procesos o programas que un sistema informático o computadora usa para realizar determinadas tareas.

Tablet: Dispositivo electrónico que tiene un tamaño intermedio entre la computadora y el smartphone, cuenta con una pantalla táctil con que se interactúa principalmente, sin la necesidad de un teclado físico o ratón.

Tarjeta De Memoria Flash: Memoria que permite la lectura y escritura de múltiples posiciones de memoria en la misma operación.

Teléfono Celular: Teléfono celular con pantalla táctil, que permite al usuario conectarse a internet, gestionar cuentas de correo electrónico e instalar aplicaciones y recursos a modo de pequeño computador.

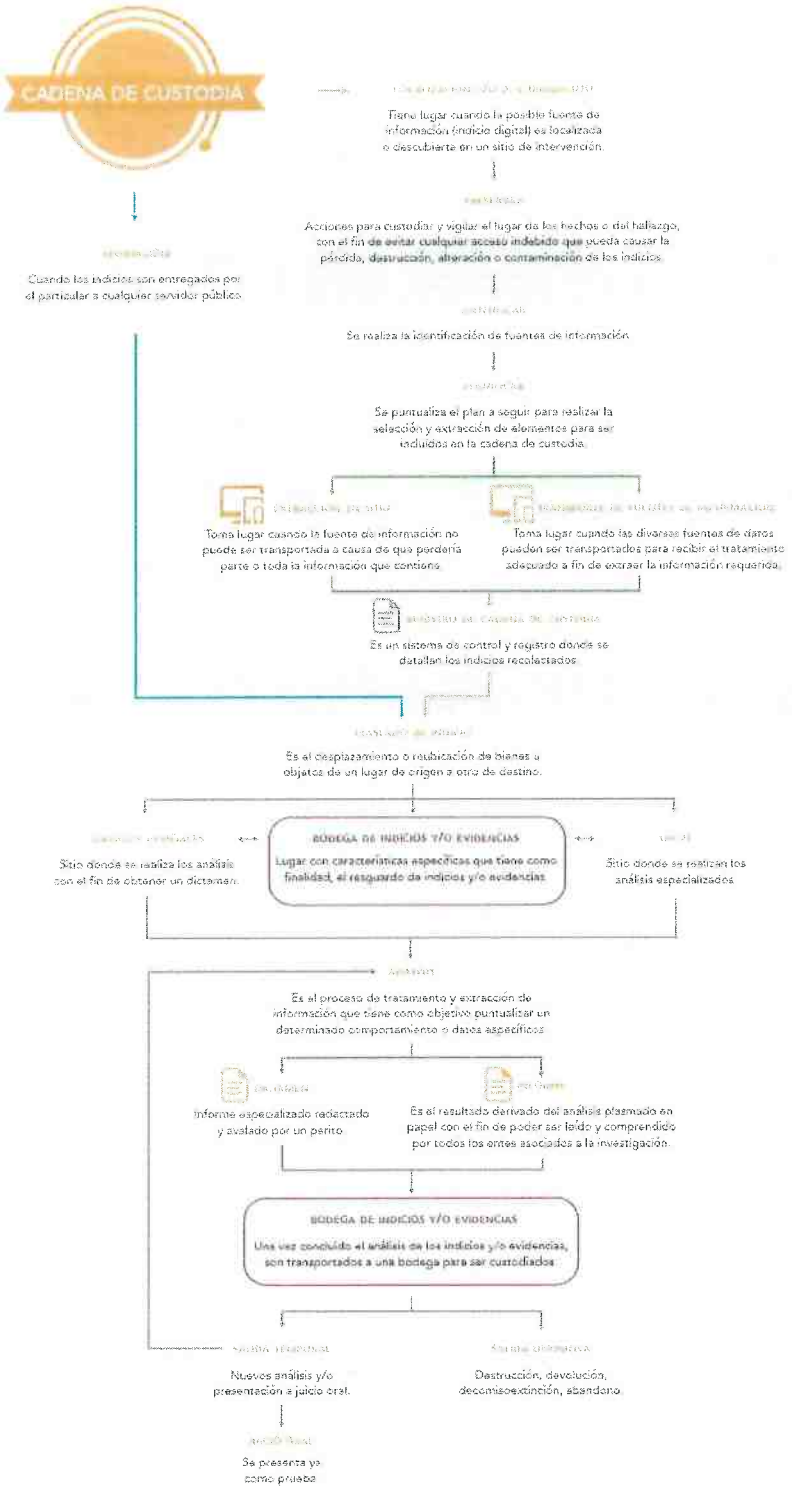
Traslado: Es el desplazamiento o reubicación de bienes u objetos de un lugar de origen a otro de destino.

USB (Universal Serial Bus, por sus siglas ingles): Dispositivo de almacenamientos de datos, que utiliza memoria flash para guardar datos e información.

Volatilidad. Se refieren a los datos de un sistema en vivo que se pierde después de que una computadora se apaga o debido al paso del tiempo.

ANEXOS

Diagrama de flujo de la Guía de cadena de custodia.



Formato de Registro de Cadena de Custodia Digital.

No. de referencia

Registro de Cadena de Custodia Digital

Institución o Unidad administrativa	Folio o llamado	Lugar de intervención	Fecha y hora de intervención

Inicio de la cadena de custodia. (Marque con "X" el motivo por el cual comienza el registro).

Localización		Descubrimiento		Aportación	

1. **Identidad.** (Número, letra o combinación alfanumérica asignada al indicio digital y seleccione una de las opciones preexistentes, descripción general, incluyendo en su caso el estado o condición original en el momento de su recolección, ubicación en el lugar de intervención y hora de recolección. Relacione la identificación por secuencias cuando se trate de indicios digitales del mismo tipo o clase; en caso contrario, registre individualmente. Cancele los espacios sobrantes).

Identificación	Tipo		Descripción	Ubicación en el lugar	Hora de recolección
	Celular	USB			
	Computadora	Disco Duro			
	Laptop	CD / DVD	Firma digital:		
	Tableta	Otro			
	Celular	USB			
	Computadora	Disco Duro			
	Laptop	CD / DVD	Firma digital:		
	Tableta	Otro			
	Celular	USB			
	Computadora	Disco Duro			
	Laptop	CD / DVD	Firma digital:		
	Tableta	Otro			
	Celular	USB			
	Computadora	Disco Duro			
	Laptop	CD / DVD	Firma digital:		
	Tableta	Otro			

No. de referencia

2. **Documentación.** (Marque con 'X' los métodos empleados o especifique cualquier otro en caso necesario).

Escrito: Sí ☐ No ☐ Fotográfico: Sí ☐ No ☐ Croquis: Sí ☐ No ☐

Otro: Sí ☐ No ☐

Especifique:_____

3. **Recolección.** (Coloque el número, letra o combinación alfanumérica de los indicios digitales de acuerdo a las condiciones de cómo fueron levantados según corresponda. Puede emplear intervalos).

Manual	Instrumental	Digital

4. **Empaque/embalaje.** (Coloque el número, letra o combinación alfanuméricas de los indicios digitales de acuerdo al tipo de embalaje que se empleó para su preservación o conservación, según corresponda. Puede emplear intervalos).

Bolsa	Caja	Recipientes

5. **Servidores públicos.** (Todo servidor público que haya participado en el procesamiento de los indicios digitales deberá escribir su nombre completo, la Institución a la que pertenece, su cargo, la etapa del procesamiento en la que intervino y su firma autógrafa. Se deberán cancelar los espacios sobrantes).

Nombre completo	Institución y cargo	Etapa	Firma

No. de referencia

6. **Traslado.** (Marque con "X" la vía empleada. En caso de ser necesaria alguna condición especial para la conservación o preservación de un indicio digital en particular, el personal pericial o policial con capacidades para el proceser, según sea el caso, deberá recomendarla).

a) Vía:		Terrestre		Aérea	Marítima
b) Se requieren condiciones especiales para su traslado:		No		Sí	
Recomendaciones:					

7. **Continuidad y trazabilidad.** (Fecha y hora de la entrega-recepción, nombre completo de quien entrega y de quien recibe los indicios digitales en los cambios de custodia que realicen, institución a la que pertenecen, cargo o identificación dentro de la misma, propósito de la transferencia, firmas autógrafas y lugar de permanencia en la actividad respectiva. Anota las observaciones relacionadas con el embalaje, el indicio digital o cualquier otra que considere necesario realizar. Agregue cuantas hojas sean necesarias. Cancele los espacios sobrantes después de que se haya cumplido con el destino final del indicio digital).

Fecha y hora de entrega recepción	Nombre, institución y cargo o identificación de quien entrega	Actividad/propósito	Firma
Lugar de permanencia	**Nombre, institución y cargo o identificación de quien recibe**	**Actividad/propósito**	**Firma**
Observaciones			
Fecha y hora de entrega recepción	**Nombre, institución y cargo o identificación de quien entrega**	**Actividad/propósito**	**Firma**
Lugar de permanencia	**Nombre, institución y cargo o identificación de quien recibe**	**Actividad/propósito**	**Firma**
Observaciones			
Fecha y hora de entrega recepción	**Nombre, institución y cargo o identificación de quien entrega**	**Actividad/propósito**	**Firma**
Lugar de permanencia	**Nombre, institución y cargo o identificación de quien recibe**	**Actividad/propósito**	**Firma**
Observaciones			

Formato de Entrega-Recepción de Indicios Digitales.

PGR
PROCURADURÍA GENERAL DE LA REPÚBLICA

Entrega-recepción de indicios digitales

No. de referencia

Folio o llamado	Lugar de la entrega-recepción	Fecha y hora entrega/recepción

1. **Inventario.** (escriba el número, letra o combinación alfanumérica con la que se identifica a cada indicio digital que se entrega, así como su tipo o clase. Cancele los espacios sobrantes)

Identificación	Tipo		Descripción	Ubicación en el lugar	Hora de recolección
	Celular	USB			
	Computadora	Disco Duro			
	Laptop	CD / DVD	Firma digital:		
	Tableta	Otro			
	Celular	USB			
	Computadora	Disco Duro			
	Laptop	CD / DVD	Firma digital:		
	Tableta	Otro			
	Celular	USB			
	Computadora	Disco Duro			
	Laptop	CD / DVD	Firma digital:		
	Tableta	Otro			
	Celular	USB			
	Computadora	Disco Duro			
	Laptop	CD / DVD	Firma digital:		
	Tableta	Otro			

2. **Embalaje.** (Señale las condiciones en las que se encuentran los embalajes. Cuando alguno de ellos presente alteración, deterioro o cualquier otra anomalía, especifique dicha condición).

Persona que entrega	Persona que recibe
Nombre completo, institución, cargo y firma	Nombre completo, institución, cargo y firma

Página No. ___ de ___

Se anexa continuación de entrega-recepción: SI [ ] NO [ ]