# Metodología para el tratamiento de evidencias digitales acorde a la normativa salvadoreña de delitos informáticos

Manuel Molina, Pedro Trejo, Jonathan Mejía, Carlos Molina Medrano

**Revista Nuestro Tiempo. Universidad Luterana Salvadoreña**

Manuel Molina es estudiante de Licenciatura en Ciencias de la Computación en proceso de graduación en la Universidad Luterana Salvadoreña. Graduado de la especialización en Informática Forense y Delitos Informáticos. Correo: manuel.ntonio@gmail.com

Pedro Trejo es estudiante de Licenciatura en Ciencias de la Computación en proceso de graduación en la Universidad Luterana Salvadoreña. Graduado de la especialización en Informática Forense y Delitos Informáticos. peternoble82@gmail.com

Jonathan Mejía es estudiante de Licenciatura en Ciencias de la Computación en proceso de graduación en la Universidad Luterana Salvadoreña Graduado de la especialización en Informática Forense y Delitos Informáticos. Correo:jonathandanielm@gmail.com

Carlos Molina Medrano es Coordinador del Departamento de Ciencias de la Computación de la Universidad Luterana Salvadoreña. Docente Investigador , especialista en Educación Virtual y especialista en Informática Forense y Delitos Informáticos. Correo: kabimolina1932@gmail.com

## ABSTRACT

The Law on the Computer and Related Crimes approved in February 2016, brings with it challenges for the sector of justice in our country, as any implementation of a new law. One of the major challenges is to train the staff in the appropriate treatment of electronic devices that contain digital evidence, as well the appropriate analysis of them. This paper proposes a methodology based on ISO/IEC 27037:2012 and good practices compiled from other similar methodologies that adapts the reality of the Salvadoran legislation demands.

## RESUMEN

La Ley Especial de Delitos Informáticos y Conexos aprobada en febrero del año 2016, trae consigo retos para el sector justicia del país, como toda implementación de una nueva ley. Uno de los retos más grande es la de formar al personal en el adecuado tratamiento tanto de los aparatos electrónicos que contienen evidencias digitales, como el adecuado análisis de las mismas. En este trabajo se propone una metodología basada en la norma ISO/IEC 27037:2012 y buenas prácticas recopiladas de otras metodologías similares para adaptarla a la realidad que exige la legislación salvadoreña.

## PALABRAS CLAVES:

Informática Forense, Ley de Delitos Informáticos, Tratamiento de Evidencias Digitales.

## I. INTRODUCCIÓN

Los delitos informáticos han ido en crecimiento en El Salvador conforme avanza la penetración de las TIC y abarca a mayor población. La Policía Nacional Civil reporta haber investigado 131 delitos en el año 2016,

cuando en el año 2011 apenas investigó 47 (PNC, 2017).

De los datos anteriores se intuye que son apenas la punta del iceberg, ya que el acometimiento de ilícitos puede ser considerablemente mayor. En la mayoría de casos, la gente no suele denunciar este tipo de delitos por diversas causas entre ellas el desconocimiento de la misma ley.

El avance de este tipo de ilícitos supuso la creación de una Ley Especial, dicha ley fue aprobada en el mes de febrero del año 2016 en El Salvador y entró en vigencia el mes de marzo del mismo año.

Una de las grandes debilidades luego de su entrada en vigencia es la falta de formación del sector justicia, que para el caso de El Salvador está conformado por: el Órgano Judicial, el Ministerio de Justicia y Seguridad Pública, la Procuraduría General de la República y el Consejo Nacional de la Judicatura, otra debilidad marcada es la falta de unidades especializadas y laboratorios que trabajen bajo normativas internacionales en informática forense.

Como bien se sabe, en los procesos judiciales es de vital importancia la preservación de la evidencia para que pueda constituirse en prueba. Para considerarse como evidencia digital se debe garantizar su relevancia, confiabilidad, suficiencia e integridad. Solo una manipulación adecuada, empleando metodología, técnicas e instrumentos adecuados, asegurará que la evidencia digital extraída de los aparatos u objetos electrónicos, garantice los principios antes apuntados.

En este documento, se propone una metodología diseñada por etapas, que busca acercar criterios tendientes a emplear prácticas adecuadas en el manejo de los dispositivos electrónicos incautados y que al ser trasladados, almacenados y analizados para sustraer posibles las evidencias digitales, no puedan ser desvirtuadas en procesos judiciales.

Se acude a la norma ISO/IEC 27037:2012 que es la Guía para la identificación, recolección, adquisición y preservación de evidencias digitales, además se acude a otras buenas prácticas en el tratamiento de las evidencias digitales para constituir esta propuesta que en general es adaptada a la legislación salvadoreña.

## II. ELEMENTOS DE TRABAJO Y METODOLOGÍA

En torno a la metodología empleada, se compararon y se extrajeron los elementos sustanciales de dos metodologías para tratar evidencias digitales, la primera que propone el Ministerio de Tecnologías de la Información y la Comunicación de Colombia (MINTIC) para las entidades gubernamentales de ese país, y la segunda es la que propone la Fiscalía General del Ecuador.

La guía de evidencias digitales del MINTIC de Colombia propone una metodología que toma de base la norma ISO/IEC 27037 y la norma NIST SP800-86. En el documento Manual de Manejo de Evidencias Digitales y Entornos Informáticos de la Fiscalía General del Estado del Ecuador, a pesar de ser un manual muy detallado ofrece una serie de buenas prácticas para el tratamiento de evidencias digitales, pero solo a nivel de buenas practicas porque no se hace referencia a la utilización de ninguna norma internacional.

Para elaborar la metodología se estudió la norma ISO/IEC 27037:2012 con el fin de incorporar sus principios fundamentales. Posteriormente, se hizo un análisis de los delitos informáticos tipificados en la Ley de Delitos Informáticos y Conexos de El

Salvador para identificar aquellos recursos u objetos electrónicos que pueden llegar a aportar evidencia digital en los procesos judiciales o civiles.

## III. RESULTADOS

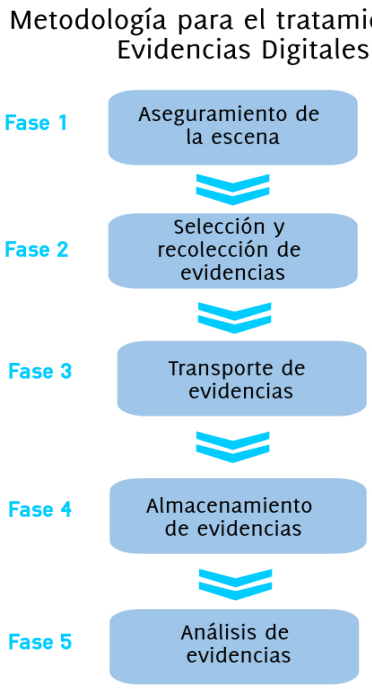
La norma ISO/IEC 27037:2012 define los siguientes procesos para el manejo de la evidencia digital: 1) Identificación: Es el reconocimiento de donde se halla la evidencia digital. 2) Recolección: Recolectar y almacenar para su adquisición. 3) Adquisición: Proceso para obtener copias binarias del contenido de los objetos involucrados. 4) Preservación: Se debe asegurar la integridad de la evidencia en todo el proceso.

La norma define de forma general el tratamiento de la evidencia, no obstante cada legislación en cada país cuenta con sus normativas procesales que van delineando las formas en las que se debe realizar el tratamiento de las evidencias. Para el caso de El Salvador, está definido en el código procesal penal. Es importante precisar que, en el Código Procesal Penal salvadoreño no se habla de la preservación y tratamiento de las evidencias de tipo digital. Solo se orienta en torno a las evidencias físicas, lo cual podría en su momento conllevar a vacíos en la aplicación de la ley.

La informática forense dista mucho de la medicina forense, lo cual conlleva a la necesidad de reformar dicho Código, para que sean incorporados por lo menos, elementos relativos al análisis y metodologías forenses, cadenas de custodias para el manejo de evidencias digitales, incautación y preservación de objetos y equipos electrónicos.

La informática forense delinea procedimientos específicos para el tratamiento científico de las evidencias digitales, que también es necesario considerar al momento de proponer una metodología para el tratamiento de las evidencias digitales.

Los principales resultados se sintetizan en la metodología que se propone, la cual se divide en cinco fases, que se toman de base de la norma ISO/IEC 2037:2012 define y a lo que la informática forense delinea para garantizar la confiabilidad de la misma.




La metodología propone aspectos relativos al tratamiento de equipos u objetos electrónicos contenedores de información, los cuales después de un análisis técnico se convierte en evidencia digital, y que en un juicio se puede constituir en material probatorio. Esta metodología no profundiza en la etapa de análisis, sugiriendo el uso de las buenas prácticas, desde la identificación hasta la adquisición y presentación de la evidencia.

El alcance de esta metodología está delineado por el preservamiento de la evidencia digital, para garantizar en todo momento su integridad hasta presentarse en forma de informe pericial a los tribunales. No ahonda

tampoco en el empleo de métodos y técnicas de análisis específicas, ni en los aspectos meramente administrativos y técnicos en lo judicial. En la imagen 1, se pueden ver las fases de las cuales se constituye.

*A. Fase 1. Aseguramiento de la escena*
En todo escenario de un hecho delictivo, de igual forma que se toman las debidas medidas y precauciones para no contaminar las escenas, de aquellos vestigios que sean susceptibles de ser enviados a los laboratorios para su examen (huellas digitales, ADN, elementos balísticos, así se deben tomar las debidas precauciones para no contaminar la escena, ya sea por medios físicos o electrónicos.

La contaminación física puede alterar una evidencia digital: una manipulación incorrecta puede conllevar a una modificación e incluso una pérdida total de la presunta evidencia. Sirva como ejemplo que la electricidad estática que se puede portar, al tocar un circuito, puede inutilizar éste completamente; un imán cerca de un dispositivo altera los datos almacenados en el mismo; los golpes no son favorables con las partes mecánicas de los disco duro rígidos.

La contaminación electrónica proviene de un mal aislamiento del dispositivo frente a su entorno, sobre todo en su embalaje. Dispositivos que acepten datos de forma inalámbrica (routers, teléfonos móviles, agendas electrónicas, tablets, entre otros) deben ser aislados adecuadamente para que la congelación de la escena sea efectiva, especialmente aquellos que no deben ser apagados.

También es importante asegurar cualquier equipo que remotamente pueda ser manipulado tales como: servidores, equipos de red, equipos de vigilancia, entre otros.

Principales actividades y recomendaciones a desarrollar en esta fase son:

*a) No tocar los equipos electrónicos contenidos en la escena*
Al ingresar a la escena se debe tener el debido cuidado de no contaminar los equipos electrónicos, ya que en la superficie de dichos objetos se podría recolectar algún tipo de material probatorio tal como huellas dactilares, entre otros. Dicho material debe también de ser levanto y enviado al laboratorio para su debido análisis.

*b) Fijar el lugar de la escena mediante el uso de fotografía y planimetría*
Se debe utilizar la técnica de la fijación de la escena tradicional, mediante el uso de fotografía y planimetría, debiendo de capturar imágenes de los aspectos generales del recinto e imágenes específicas tales como la parte trasera de la conexiones encontradas, estructura del cableado de red, de la red eléctrica, si existen cámaras de seguridad en el lugar se debe de fijar el ángulo de captación de estas, si el equipo se encuentra encendido tomar fotografías de la pantalla principal y elaborar un croquis planimétrico de la ubicación de los equipos con relación a puntos fijos del recinto.

*c) Búsqueda de evidencia y objetos no electrónicos que pueda contener material probatorio*
En la escena se debe de realizar una búsqueda de evidencia, no sólo de índole electrónico digital, sino también cualquier otro tipo de evidencia física que pueda tener indicios de constituirse como prueba, dicha búsqueda debe realizarse utilizando cualquier técnica de búsqueda de evidencia ya utilizada en los delitos comunes (búsqueda en espiral, lineal, de punto a punto), así como también se debe de garantizar la preservación de las mismas siguiendo los mecanismos ya establecidos para su recolección.

Algunas de las evidencias que se podrían

encontrar son:

a) Anotaciones en papeles de usuarios, claves de usuario, nickname, contraseñas, correos electrónicos.
b) Comprobantes de pago y/o facturas de servicios de internet, luz eléctrica, servicios telefónicos, así como también facturas o ticket de la compra de equipo electrónico.
c) Comprobantes de pago y/o facturas de tarjetas de crédito o estados de cuentas de tarjetas de débito.
d) Comprobantes emitidos por pagos electrónicos.
e) Tarjetas de crédito o débito, así como también cualquier otro tipo de tarjetas inteligentes y plástico con bandas magnéticas.
f) Otros objetos no electrónicos que puedan contener información sobre los hechores, transacciones o víctimas del ilícito investigado.

*B. Fase 2. Selección y recolección de evidencias*

Al tener la escena ya asegurada con toda clase de posibles evidencias que tenga relación con el ilícito investigado, viene la fase de selección de los equipos y componentes electrónicos que podrían contener información y que deben ser incautados para su respectivo análisis. Es importante evaluar tanto los aparatos electrónicos como otros artefactos que pueden aportar tanto evidencias físicas como evidencias digitales, para efectuar la incautación.

La incautación es la toma legal de los bienes de personas que pueden estar involucradas en delitos. Es necesario reconocer aquellos equipos electrónicos en una escena que aporten elementos probatorios. Entre ellos, se pueden mencionar aquellas que procesan y tienen capacidad de entregar información de cualquier forma, las que guardan y registran información de forma volátil o permanente, así mismo, aquellas que tengan la función de comunicar datos e información y que puedan interferir en ese proceso.

También es necesario analizar si algunos equipos o partes de ellos pueden ser consideradas evidencias físicas, que no formarán parte del análisis para extraer evidencias digitales. En esos casos: mouse, monitor, teclados, cables, cases, ups, entre otros periféricos pueden ser considerados como este tipo de evidencia.

Lo que busca esta fase es asegurar que los objetos contenedores de información y los aparatos electrónicos a ser incautadas no sean dañados o alterados debido a una inadecuada manipulación. Es necesario recordar que de un adecuado manejo de los objetos electrónicos o evidencias electrónicas dependerá que puedan ser extraídas las evidencias digitales.

Recomendaciones a tomar en cuenta al momento de proceder a la recolección de recursos electrónicos:

- Utilizar pulseras anti estáticas.
- Utilizar guantes de látex.
- Tener extrema precaución de no halar, cortar, doblar o extraer de manera inadecuada cables de conexión o alimentación, de todos los periféricos de entrada y salida conectados a los ordenadores y demás equipo electrónico.
- Retirar teléfonos o asistentes electrónicos ajenos a la escena, ya que con dichos objetos se podría realizar alguna modificación a los equipos.
- Asegurar que todos los equipos que se encuentren encendidos y conectados a la energía eléctrica, sean inspeccionados, fotografiarlos, ya que si un ordenador o servidor es apagado de manera inadecuada podría perder parte de información, como por ejemplo de sesiones de inicio y

procesos ejecutados. En estos casos se recomienda utilizar algún software para poder copiar la información volátil contenida en los chips de memorias y caché del ordenador.

- Una vez garantizada la seguridad del área, y seleccionado los equipos a incautar, se deben tomar fotografías del estado y ubicación de cada equipo identificándose mediante un número, así como de sus puertos, de igual manera del estado en el que encuentre la pantalla, cables de alimentación eléctrica y todos lo demás periféricos de entrada y salida que se encuentren conectados.

Contextualizando en la legislación salvadoreña sobre delitos informáticos, se hace una referencia de los equipos electrónicos que se pueden seleccionar para su incalutación, ya que pueden ser portadores de evidencia digital, según cada capitulo de la Ley de Delitos Informáticos y Conexos de El Salvador, que se pueden ver en la tabla 1.

**Tabla 1. Delitos tipificados en la Ley de Delitos Informáticos y Conexos y los recursos electrónicos y ópticos de donde pueden extraerse evidencias digitales.**

| CAPÍTULO DE LA LEY | DELITOS INFORMÁTICOS | EVIDENCIAS DIGITALES | EQUIPOS ELECTRÓNICOS |
|---|---|---|---|
| **Delitos contra los Sistemas Tecnológicos de Información** | • Acceso Indebido a Sistemas Informáticos<br>• Acceso indebido a los programas o datos informáticos<br>• Interferencia del Sistema Informático<br>• Daños a Sistemas Informáticos<br>• Posesión de equipos o prestación de servicios para la vulneración de la Seguridad<br>• Violación de la seguridad del sistema | • Software o programas que vulneran seguridad de aplicaciones<br>• Logs de dispositivos de red<br>• Logs de base de datos<br>• Logs de servidores<br>• Bases de datos<br>• Cookies de navegadores<br>• Logs de proxys<br>• Correos electrónicos<br>• Archivos en cualquier formato | • CPU<br>• Dispositivos de almacenamiento<br>• Bluetooth<br>• Dispositivos de red<br>• Teléfonos Inteligentes<br>• Tabletas<br>• Laptops<br>• Bloqueadores de señal |
| **Delitos Informáticos** | • Estafa Informática<br>• Fraude Informático<br>• Espionaje Informático<br>• Hurto por medios | • Logs de dispositivos de red<br>• Logs de base de datos<br>• Logs de servidores | • Dispositivos de red<br>• Teléfonos inteligentes<br>• Dispositivos de |

| | | | |
|---|---|---|---|
| | informáticos<br>• Técnicas de Denegación de Servicio | • Bases de datos<br>• Bitácoras de acceso<br>• Cookies de navegadores<br>• Logs de proxys.<br>• Archivos en cualquier formato.<br>• Documentos digitales.<br>• Cookies de navegadores<br>• Correos electrónicos. | almacenamiento<br>• Discos extraíbles<br>• Tabletas<br>• Laptos<br>• CPU<br>• Bloqueadores de señal<br>• Todo dispositivo que se conecte a Internet. |
| **Delitos Informáticos relacionados al Contenido de los Datos** | • Manipulación de Registros<br>• Manipulación fraudulenta de tarjetas inteligentes o instrumentos similares<br>• Obtención indebida de bienes o servicios por medio de Tarjetas Inteligentes o medios similares<br>• Provisión indebida de Bienes o Servicios<br>• Alteración, daño a la integridad y disponibilidad de los datos<br>• Interferencia de Datos<br>• Interceptación de transmisiones entre Sistemas de las Tecnologías de la | • Logs de servidores<br>• Logs de base de datos<br>• Logs de proxys<br>• Bases de datos<br>• Software o programas que vulneran seguridad de aplicaciones<br>• Correo electrónicos<br>• Logs de bases de datos<br>• Tarjetas inteligentes<br>• Perfiles de redes sociales | • Máquina impresora de Tarjetas Inteligentes<br>• Dispositivos de red<br>• Teléfonos inteligentes<br>• Dispositivos de almacenamiento<br>• Discos extraíbles<br>• Tabletas<br>• Laptops<br>• CPU<br>• Clonadores de tarjetas inteligentes<br>• Chips<br>• Reseteadores de chip<br>• Bluetooth |

| | | | |
|---|---|---|---|
| | Información y la Comunicación<br>• Hurto de identidad<br>• Divulgación no autorizada<br>• Utilización de datos personales<br>• Obtención y transferencia de información de carácter confidencial<br>• Revelación indebida de datos o información de carácter personal<br>• Acoso a través de Tecnologías de la Información y la Comunicación | | |
| **Delitos Informáticos contra niños y niñas o Personas con Discapacidad** | • Pornografía a través del uso de Tecnologías de Información y la Comunicación<br>• Utilización de Niñas, Niños, Adolescentes o personas con discapacidad en pornografía a través del uso de las Tecnologías de la Información y la Comunicación<br>• Adquisición o Posesión de Material Pornográfico de Niñas, Niños, Adolescentes o Personas con | • Logs de servidores<br>• Cookies de navegadores<br>• Logs de dispositivos de red<br>• Correos electrónicos<br>• Ficheros de texto, vídeo, imágenes, audio.<br>• Logs de base de datos<br>• Logs de proxys<br>• Cuentas de redes sociales | • Teléfonos inteligentes<br>• Dispositivos de almacenamiento<br>• Discos extraíbles<br>• Tabletas<br>• Laptops<br>• CPU<br>• Cintas magnéticas con almacenamiento de datos<br>• Bluetooth<br>• Cámaras de video y fotográficas |

| | | | |
|---|---|---|---|
| | Discapacidad a través del Uso de las Tecnologías de la Información y la Comunicación<br>• Corrupción de Niñas, Niños, Adolescentes o Personas con Discapacidad a través del Uso de las Tecnologías de la Información y la Comunicación<br>• Acoso a Niñas, Niños y Adolescentes o Personas con Discapacidad a través del Uso de las Tecnologías de la Información y la Comunicación | | |
| **Delitos contra el Orden Económico** | • Suplantación en Actos de Comercialización | • Documentos digitales<br>• Ficheros de texto, imágenes, audio, video<br>• Logs de servidores<br>• Bases de Datos<br>• Logs de Base de Datos | • Discos extraíbles.<br>• Tabletas<br>• Laptops<br>• CPU<br>• Dispositivos de red<br>• Impresores |

*Embalaje de los objetos a incautar*

Se trata de no alterar ni perder nada de los equipos electrónicos para garantizar la veracidad de la evidencia digital contenida en ellos, así como, también, de las evidencias físicas encontradas.

Aspectos a considerar al momento de embalar el equipo a incautar.

a) Utilizar material adecuado según el objeto a resguardar: plástico de burbujas de aire, plástico aislante a radiaciones, cajas de cartón resistente.

b) Emplear pulseras antiestáticas en todo el proceso de manipulación de cualquier equipo electrónico.
c) Emplear bolsas anti radiaciones.
d) Luego de realizar el embalaje de las evidencias adecuadamente, se debe de etiquetar los paquetes según el objeto que contenga, en dicha etiqueta se deben de plasmar características identificativas del objeto electrónico, por ejemplo: números de serie, marca, modelo, color, tamaño, y cualquier otra información referentes a su identificación.

*Elaboración de cadena de custodia*
La cadena de custodia, es el documento mediante el cual se garantiza autenticidad del objeto electrónico incautado en la escena, es decir, mediante el uso de dicho documento el cual puede ser elaborado mediante una acta notarial o policial, o simplemente un formato contenedor de los campos necesarios para rellenarlos con la información identificativa del objeto.

La mencionada cadena debe contener los responsables de la incautación y la información de las personas que tienen contacto con dicho objeto, hasta la entrega en el almacén u oficina receptora de evidencias. Garantizando que este objeto es el mismo y no ha sido reemplazado por otro de similares características, evitando así un fraude procesal o una duda razonable al momento de ser presentado en los tribunales.

*C. Fase 3. Transporte de evidencias*
Debe asegurarse que el transporte de las evidencias se haga adecuadamente, siempre con el objeto de preservar su integridad.

Se incluye como fase de esta metodología, el transporte de evidencias debido a que una de los recurrentes problemas de daño de recursos electrónicos se da precisamente en el traslado de los mismos.

Las recomendaciones generales en esta fase son:

- Asegurar que los equipos electrónicos en general no deben someterse a temperaturas superiores a los 50°C.
- Evitar que los equipos electrónicos puedan ser afectados por la contaminación por polvo u otro tipo de partículas.
- Asegurar que el humo también pueda afectar el funcionamientos de equipos y componentes electrónicos.
- Asegurar que a la hora de transportar recursos electrónicos no se haga en compañía de agua o de otro tipo de material que genere humedad.
- Aislar lo suficiente para evitar la corrosión, ya que ésta se puede dar en corto tiempo en algunos equipos electrónicos.
- Limitar considerablemente las vibraciones y golpes de los equipos o componentes electrónicos en los traslados, ya que también puede dañar memorias USB, discos duros o rígidos, memorias RAM, entre otros.
- Evitar al máximo el electromagnetismo y la radiofrecuencia, que también afecta a algunos recursos electrónicos.

Tomando esos elementos como base se debe asegurar que:

- El vehículo cuente con un espacio físico adecuado para evitar poner equipos a estriba.
- Deben emplearse cajas que aíslen la radiofrecuencias y energía estática, en su defecto procurar que no se expongan los recursos electrónicos a ese tipo de energías.
- Contar con compartimentos pequeños para los objetos electrónicos de menor tamaño.
- La textura del interior del almacén temporal para el transporte debe de estar

libre de impurezas, seco, y la textura del piso y paredes de los compartimientos debe de ser suave.

- Las cajas donde descansarán los equipos o componentes electrónicos incautados deben contener materiales que eviten las vibraciones.
- No conducir por mucho tiempo las evidencias en las cercanías del mar.
- Hay que cerciorarse que los equipos y componentes no se golpeen entre sí en los traslados.

*D. Fase 4. Almacenaje de la evidencia*

El objetivo principal del almacenamiento y custodia de evidencias y elementos de prueba es garantizar la autenticidad y mantener la inalterabilidad de los mismos.

La organización de un sistema de almacenamiento y custodia de evidencias, debe considerar varios aspectos, los más importantes son:

a) Personal encargado del manejo y control de evidencias, debidamente capacitado en la atención, identificación, clasificación, embalaje y control de ingreso y salida de evidencia.
b) Métodos manuales y automatizados de registro y control para el manejo de las evidencias.
c) La entrega del objeto electrónico incautado, se debe de hacer mediante el uso de la cadena de custodia, a la persona responsable de realizar su análisis o en todo caso al encargado de recibir las evidencias en el almacén.
d) Las condiciones de dicho almacén deben de garantizar el completo resguardo de los objetos, ya que si por condiciones de infraestructura del almacén o del laboratorio, el objeto a someter a análisis es alterado, deteriorado, o arruinado, será responsabilidad de las personas encargadas de sus custodia. De esta forma se pueden deducir responsabilidades según la cronología de la cadena de custodia. Por lo que es de suma importancia contar con infraestructuras adecuadas, y con el material y equipo necesario para su manipulación.
e) El almacén debe de mantenerse a temperatura ambiente normal, para evitar que los objetos embalados en materiales plásticos suden debido a las altas temperaturas, o que generen humedad debido a las bajas temperaturas. Debe de estar aislado de toda radiación electromagnética y energías estáticas (Jaula Faraday).
f) Contar con sistemas de detección y combates contra incendio.
g) Condiciones necesarias de asepsia.
h) Mecanismos adecuados de seguridad externa e interna en los almacenes.
i) Al momento de manipularse por parte de los analistas de evidencias, se deben asegurar todas las medidas ya expuestas.

El Código Procesal Penal de El Salvador en su artículo 285, mandata a la Fiscalía General de la República a contar con un deposito de evidencias. Las evidencias digitales no deben estar junto con las evidencias físicas, en ningún momento.

El artículo 503 del mismo Código Procesal Penal, obliga a que si la Fiscalía no cuenta con un lugar adecuado, se puedan depositar en la Corte Suprema de Justicia, que está obligado a garantizar el almacenaje adecuado de las mismas.

*E. Fase 5. Análisis de la evidencia*

La etapa de análisis de los objetos electrónicos que contienen evidencia digital, es un proceso técnico que requiere de métodos y técnicas específicas, además de

software dedicado para los fines solicitados, por lo que en este apartado no se profundiza con respecto a las herramientas técnicas o herramientas de software a utilizar, ya que esto dependerá del tipo de laboratorio, criterios del perito y naturaleza de la información analizada. Lo importante de enfatizar es que se deben emplear herramientas que no alteren las evidencias, que no sean invasivas y que tengan certificaciones para su uso.

La metodología de análisis empleada debe respetar en todos los criterios siguientes:

- Obtener acceso a la evidencia. Si, por ejemplo, se trata de un disco duro debe extraerse y aislarse del sistema donde esté albergado. Si no es posible la extracción, se debe trabajar sobre el disco evitando, en la medida de lo posible, que el sistema donde esté alojado pueda alterar el contenido del mismo.
- Conectar la evidencia a un dispositivo de lectura bloqueando la posibilidad de escritura sobre la evidencia. Lo ideal es utilizar dispositivos físicos que eviten la escritura sobre la evidencia. En el caso de utilizar sistemas basados en software, se evitará la modificación de la evidencia mediante la configuración adecuada.
- Hacer una imagen (o varias) de la evidencia a analizar para no trabajar sobre el dispositivo original y preservar éste de modificaciones accidentales.
- Analizar la evidencia a partir de la imagen obtenida anteriormente.
- Documentar todo el proceso.
- Mantener en todo momento control absoluto sobre la ubicación y operaciones realizadas, sobre la evidencia mediante una aplicación estricta de la cadena de custodia.
- Generar respaldos de las evidencias encontradas, en medios de almacenamiento ópticos y resguardarlos en un almacén.

*Principios básicos operativos en el manejo de evidencias digitales*

Las evidencias a analizar contienen pruebas que serán utilizadas, en la mayoría de los casos durante un procedimiento judicial. Su manejo por parte del perito debe ser cuidadoso y escrupuloso. A continuación se enumeran unos principios básicos para el manejo de estas evidencias.

1) Documentar todas las acciones realizadas.
2) Mantener la cadena de custodia de la evidencia.
3) Garantizar la integridad de la evidencia:

i) Montar todos los volúmenes a analizar cómo solo lectura.
ii) Obtener, registrar y verificar la firma digital (HASH) de todas las evidencias digitales con las que se trabaje.
iii) Evitar daños sobre la evidencia (caídas, calor extremo, campos magnéticos, humedad).
iv) Trabajar durante la fase de análisis sobre una imagen de la evidencia de forma exclusiva.

*El informe ejecutivo*

La forma de presentar el análisis de una evidencia es a través de un informe del perito encomendado para tal labor. Todo el proceso que supone garantizar que la evidencia sea resguardada preservando su integridad, concluye cuando se presenta el informe pericial.

Entrando más en detalle en este tipo de informes, cabe destacar que será un resumen de toda la tarea que se ha llevado a cabo con las evidencias digitales. Aunque será un documento de poca extensión, al menos comparado con el informe técnico, éste

deberá contener al menos los siguientes apartados:

- ¿Por qué se ha producido el incidente?
- ¿Qué finalidad tenía el atacante?
- Desarrollo de la intrusión.
- ¿Cómo lo ha logrado?
- ¿Qué ha realizado en los sistemas?
- Resultados del análisis.
- ¿Qué ha pasado?
- ¿Qué daños se han producido o se prevén que se producirán?
- ¿Es denunciable?
- ¿Quién es el autor o autores?
- Recomendaciones.
- ¿Qué pasos dar a continuación?
- ¿Cómo protegerse para no repetir los hechos?

*El informe técnico*

Se hace una exposición muy detallada de todo el análisis con profundidad en la tecnología usada y los hallazgos. En este caso se deberá redactar, al menos:

- Antecedentes del incidente.
- Puesta en situación de cómo se encontraba la situación anteriormente al incidente.

En la recolección de datos se debe considerar :

- ¿Cómo se ha llevado a cabo el proceso?
- ¿Qué se ha recolectado?
- Descripción de la evidencia.
- Detalles técnicos de las evidencias recolectadas, su estado, su contenido, etc.
- Entorno de trabajo del análisis.
- ¿Qué herramientas se han usado?
- ¿Cómo se han usado?
- Análisis de las evidencias.
- Se deberá informar del sistema analizado aportando datos como las características del sistema operativo, las aplicaciones instaladas en el equipo, los servicios en ejecución, las vulnerabilidades que se han detectado y la metodología usada.
- Descripción de los resultados.
- ¿Qué herramientas ha usado el atacante?
- ¿Qué alcance ha tenido el incidente?
- Determinar el origen del mismo y como se ha encontrado. Dar la línea temporal de los hechos ocurridos con todo detalle.
- Redactar unas conclusiones con las valoraciones que se crean oportunas a la vista de todo el análisis realizado.
- Dar unas recomendaciones sobre cómo proteger los equipos para no repetir el Incidente o sobre cómo actuar legalmente contra el autor.

## IV. CONCLUSIONES

1. La normativa existente en en El Salvador sobre Delitos Informáticos y otras leyes secundarias, no especifican mecanismos para el tratamiento de la evidencia digital, luego de la entrada en vigencia de la Ley Especial de Delitos Informáticos y Conexos, es requerido incorporar elementos que adviertan de su adecuado tratamiento. El código Procesal Penal ofrece directrices generales en el tratamiento de las evidencias, sin embargo, cuando se trata de la preservación de evidencias digitales no ofrece procedimientos y técnicas claras que se deben emplear para la identificación, recolección, adquisición y preservación, así como lo hace con otro tipo de evidencias.

2. La Ley Especial de Delitos Informáticos se vuelve un instrumento para perseguir los Delitos Informáticos. No obstante, el sector justicia del país no fue capacitado para su entrada en vigencia. Lo medular de un proceso jurídico es la adecuada obtención y

preservación de las evidencias digitales, para lo que se necesita de competencias específicas, entre los que se destacan: competencias sobre electrónica, informática, informática forense, derecho informático y las competencias jurídicas.

3. El empleo de metodologías, protocolos de acción y guías específicas para la manipulación y procesamiento de las evidencias digitales, se vuelven instrumentos vitales para que el personal encargado de manipularlas, lo haga de forma adecuada y no afecte los procesos judiciales.

## V. BIBLIOGRAFÍA


[1] «ISO/IEC 27037:2012 - Information technology -- Security techniques -- Guidelines for identification, collection, acquisition and preservation of digital evidence», ISO. [En línea]. Disponible en: http://www.iso.org/iso/catalogue_detail?Csnumber=44381.

[2] PNC, «Análisis de Ley de Delitos Informáticos y conexos de El Salvador».

[3] MINTIC, «Evidencia Digital. Seguridad y Privacidad de la Información.» MINTIC, 2016.

[4] Fiscalia General del Ecuador, «Manual de Manejo de Evidencias Digitales y Entornos Informáticos».

[5] «LEY ESPECIAL CONTRA LOS DELITOS INFORMÁTICOS Y CONEXOS. — Asamblea Legislativa». [En línea]. Disponible en: http://www.asamblea.gob.sv/eparlamento/indice-legislativo/buscador-de-documentos-legislativos/ley-especial-contra-los-delitos-informaticos-y-conexos.

[6] «CÓDIGO PROCESAL PENAL — Asamblea Legislativa». [En línea]. Disponible en: http://www.asamblea.gob.sv/eparlamento/indice-legislativo/buscador-de-documentos-legislativos/codigo-procesal-penal.