Proyecto de Apoyo al Sector Justicia

ABA Rule of Law Initiative

MANUAL DE EVIDENCIA DIGITAL

NCPP
Nuevo Código Procesal Penal

PERÚ | Ministerio de Justicia y Derechos Humanos | Despacho Ministerial | Comisión Especial de Implementación del Código Procesal Penal

MANUAL DE EVIDENCIA DIGITAL

Proyecto de Apoyo al Sector Justicia
Av. Larco 101, Oficina 802,
Miraflores, Lima - Perú
T: +51 (01) 447-6867
F: +51 (01) 447-6802
E: correocentral@abaroliperu.com
W: abaroliperu.com

Autor: *Alan Martín Nessi*
Director País - ABA ROLI: *Raúl Callirgos Velarde*
Diseño, diagramación e impresión: *Publimagen ABC sac*
Calle Collasuyo Nº 125, Independencia.
Primera edición, julio 2017

Hecho el Depósito Legal en la Biblioteca Nacional del Perú Nº 2017 - 14373
Tiraje: 3000 ejemplares

Este documento surge como resultado del trabajo de los colaboradores y de la Iniciativa para el Estado de Derecho del *American Bar Association* (Colegio de Abogados de EE.UU.). Las declaraciones y los análisis que aquí se expresan son únicamente de los autores, y no han sido aprobados por la Cámara de Delegados ni por el Consejo de Gobernadores del *American Bar Association* y, por lo tanto, no representan la posición o la política de tales organismos. Asimismo, nada de lo incluido en este manual deberá interpretarse como una asesoría legal para casos específicos.

El proyecto recibió financiamiento para su desarrollo por parte del Departamento de Estado de EE.UU., a través de la Oficina de Asuntos Internacionales contra el Narcotráfico y Aplicación de la Ley (INL). Las opiniones expresadas aquí no reflejan necesariamente las del Departamento de Estado de EE.UU. o las del gobierno de EE.UU.

El "Proyecto de Apoyo al Sector Justicia" inició sus actividades en Agosto de 2016, teniendo como principal antecedente el "Programa de Apoyo a la Justicia Penal en el Perú" ejecutado entre Mayo del 2012 y Julio de 2016 y de la misma manera surge como iniciativa de la Comisión Especial de Implementación del Código Procesal Penal y con el auspicio del Gobierno de los Estados Unidos de América a través de la Oficina de Asuntos Internacionales contra el Narcotráfico y Aplicación de la Ley (INL) del Departamento de Estado. La ejecución del proyecto ha sido nuevamente encargada a la Iniciativa para el Estado de Derecho del Colegio de Abogados de los Estados Unidos (American Bar Association Rule of Law Initiative), ABA ROLI (por sus siglas en inglés) quienes a través de su oficina en Perú vienen desarrollando actividades orientadas a fortalecer la implementación progresiva del Código Procesal Penal, el tratamiento de los casos en flagrancia, la investigación y procesamiento de los Delitos Contra la Administración Pública – Corrupción de Funcionarios, el acceso a la justicia de personas en condición de vulnerabilidad y el tratamiento de casos de menores infractores de la Ley Penal.

MANUAL DE EVIDENCIA DIGITAL

ÍNDICE

RESUMEN

A través de este Manual, se busca reducir los errores frecuentemente cometidos al abordar una escena del crimen en el que se pueden encontrar medios de prueba altamente sofisticados y cuyo aseguramiento, protección y análisis exige conocimientos y técnicas avanzadas que impidan su alteración e, incluso, su destrucción. En este sentido, este es un Manual útil para policías y fiscales –en tanto se encuentran a cargo de la investigación y procesamiento de casos criminales– así como de jueces –quienes podrán advertir la complejidad que reviste el abordaje de un caso en el que las Nuevas Tecnologías se encuentran presentes-.

Aquí, el operador encontrará definiciones útiles, explicadas de manera sencilla, que le permitirán comprender los términos que se emplean en el tratamiento de la evidencia digital. Además, conocerá la importancia del abordaje adecuado de aquel tipo de medio de prueba, sus características y la información que se puede obtener. Finalmente, en la sección denominada Anexos encontrará recomendaciones útiles que le dan practicidad a los conceptos teóricos esbozados a lo largo del documento.

PRÓLOGO

La comunidad académica y científica, conjuntamente con los gobiernos deben comprometerse a realizar más investigaciones sobre el delito de la tecnología informática (…)

Asociación Mundial de Derecho Penal
XV Congreso Internacional de Derecho Penal, 1994.

Las Nuevas Tecnologías forman parte de nuestra vida: Tenemos una cuenta de e-mail, utilizamos dispositivos electrónicos en nuestros trabajos, celulares para realizar llamadas, agendas electrónicas, relojes "inteligentes" que permiten controlar nuestro quehacer diario o, simplemente, empleamos aplicaciones para interactuar con el resto de la comunidad. Sin embargo, la delincuencia también ha cambiado. Se ha modernizado. Así, se emplean herramientas tecnológicas sofisticadas para la comisión de delitos pues el perpetrador busca ocultar su identidad (anonimato) y maximizar sus ilícitas ganancias. Si bien nuestro país ha fortalecido la lucha contra los delitos informáticos a través de la Ley Nº 30096 del 22 de octubre del 2013, lo cierto es que las Nuevas Tecnologías no son de uso exclusivo de los ciberdelincuentes pues se emplean para facilitar la comisión de delitos tradicionales. Por ejemplo, en la investigación de un homicidio será importante conocer con quién o quiénes se comunicó el investigado antes y después del suceso. En una investigación de trata de personas, será útil conocer los perfiles que en las diversas redes sociales pueden administrar los imputados. En una investigación de lavado de activos, la información contable necesaria no se encontrará únicamente en libros o documentos físicos, el investigador debe saber que mucha información se encuentra en la nube y en dispositivos electrónicos.

Así, cuando la policía y la fiscalía, con autorización judicial, allanan un inmueble y encuentran dispositivos telefónicos o aparatos electrónicos, ¿cómo deben proceder?, ¿cómo deben procesar la escena?, ¿qué información pueden obtener de ella?, ¿qué límites deben respetar a fin de salvaguardar el derecho a la intimidad o al secreto de las comunicaciones que le asiste a los investigados? Los operadores jurídicos también tienen a su disposición herramientas modernas para la investigación del delito; sin embargo, si no las emplean adecuadamente podrían generar la exclusión de importantes medios de prueba o el cuestionamiento de su actuación.

El "Manual de Evidencia Digital", elaborado por Proyecto de Apoyo al Sector Justicia, con la autoría del Dr. Alan Martín Nessi es un instrumento que le permitirá al operador jurídico conocer la importancia de una adecuada investigación en la que las herramientas tecnológicas tienen un rol protagónico. Es importante señalar que nuestro país será uno de los primeros en la región latinoamericana con tener un soporte que servirá de guía para mejorar la operatividad de policías y fiscales, mejorando así la práctica forense nacional.

Ricardo N. Elías Puelles
Training Coordinator
American Bar Association – Rule of Law Initiative

INTRODUCCIÓN

Nos encontramos frente a una realidad en las investigaciones penales que nos enfrenta con la utilización de las nuevas tecnologías por parte de los delincuentes, circunstancia que requiere de un conocimiento profundizado de los investigadores y del personal policial actuante de estos mecanismos innovadores.

La obtención de información, como elementos de prueba para el éxito de una investigación criminal, exige de los investigadores encargados de la recolección, preservación, análisis y presentación de la evidencia digital, una labor impecable que garantice su autenticidad e integridad, a fin de ser presentada por el fiscal en el juicio oral.

Es fundamental afianzar la relación entre policías y fiscales a fin de elaborar y coordinar, con dirección del fiscal, una estrategia de investigación en la que se discutan y optimicen los mecanismos de recolección de evidencia digital, las herramientas a utilizarse, con el objetivo que el pormenorizado trabajo realizado por los investigadores adquiera una legitimidad absoluta que, a la luz del procedimiento penal, pueda ser presentada ante el juez, en el juicio oral, con la solidez que ello requiere.

1. Objetivo del manual

El objetivo del presente Manual es conformar una guía de actuación para miembros de la policía, técnicos y fiscales, cuando en una escena del delito[1] se encuentran dispositivos de almacenamiento informático, dispositivos de telefonía, y dispositivos periféricos asociados a aquellos, que están relacionados con una investigación penal.

Ello dotará a investigadores judiciales y policiales de una herramienta práctica de trabajo, para darle conocimiento, legitimidad, practicidad y seguridad en su accionar, minimizando los márgenes de errores en los que puede incurrirse.

Fiscales e investigadores deben conocer el manual, pues es un instrumento concreto para planificar y controlar el proceso de una investigación y ello permite que la presentación de las evidencias digitales y dictámenes periciales durante el juicio sean eficientes, sólidos, facilitando que los jueces obtengan el conocimiento necesario a través de información de calidad suministrada por los testigos –investigadores y peritos técnicos e informáticos– durante el examen efectuado por el fiscal. Un buen trabajo, permitirá también, resistir con solidez, el contra examen que realizará la contraparte sobre el aseguramiento de la escena, el reconocimiento e identificación de la evidencia digital, su adquisición, preservación, análisis y posterior presentación, garantizando y transparentando una correcta cadena de custodia.

Desde el punto de vista de la defensa legal de los investigados e imputados, este instrumento y el cumplimiento de sus premisas, dotará de legalidad al accionar de los investigadores policiales y judiciales, garantizando el debido proceso penal.

[1] La escena es el lugar o espacio físico donde sucedieron los hechos investigados. Es el foco aparentemente protagónico en el cual el autor o partícipe consciente o inconscientemente deja elementos materiales o evidencias, huellas y rastros que puedan ser significativos para establecer el hecho punible y la identificación de los responsables. También se considerará como escena el entorno de interés criminalístico donde se realizaron los actos preparatorios, así como aquél donde se aprecien las consecuencias del mismo. La información suficiente, determinará la amplitud de la escena. (Artículo 9º Reglamento de la Cadena de Custodia de Elementos Materiales, Evidencias y Administración de Bienes Incautados. Aprobado por Resolución Nº 729-2006-MP-FN del 15.junio.2006)

La realización de actividades técnico-forenses deben estar alineadas a la posibilidad de ser utilizadas en el ámbito procesal penal; resultando fundamental adaptarlas a los aspectos jurídicos y estratégicos del director de la investigación.

Ahora bien, cabe efectuar una apreciación preliminar en cuanto a la visión integral del abordaje de la problemática que involucra este tipo de investigaciones. Un panorama completo contempla tres contextos posibles:

- La investigación previa de entornos digitales o informáticos
- El tratamiento de la escena del delito de estas características
- El análisis en laboratorio forense de las evidencias digitales incautadas y la presentación de los informes periciales ante el Tribunal

Estas tres etapas, configuran el universo integral en la investigación no sólo de los delitos propiamente informáticos, sino de todos los delitos cometidos mediante el uso o con ayuda de dispositivos tecnológicos, informáticos y de comunicaciones, ya que las mismas se encuentran íntimamente relacionadas y dependen una de la otra en el orden explicitado precedentemente.

En otras palabras, sin una adecuada investigación previa que nos conduzca a la existencia de una escena del delito de contexto digital o informático, resultará imposible arribar con éxito a un escenario de estas características, lo que impedirá obviamente un análisis forense de este tipo de dispositivos.

De allí la importancia de esta visión abarcativa, que si bien no será objeto de desarrollo exhaustivo en este manual, sí es necesario dejarla planteada, y esbozada (Ver Anexos Preliminares).

Sin perjuicio de ello, y tal como se explicaba al inicio de este acápite, el cometido de este manual es la generación de una guía de buenas prácticas para el adecuado tratamiento de la escena del delito en un entorno digital.

2. Marco legal y referencias bibliográficas

El Manual tiene como referencia básica el Código Procesal Penal del Perú, como así también los protocolos, lineamientos y guías que a continuación se detallan:

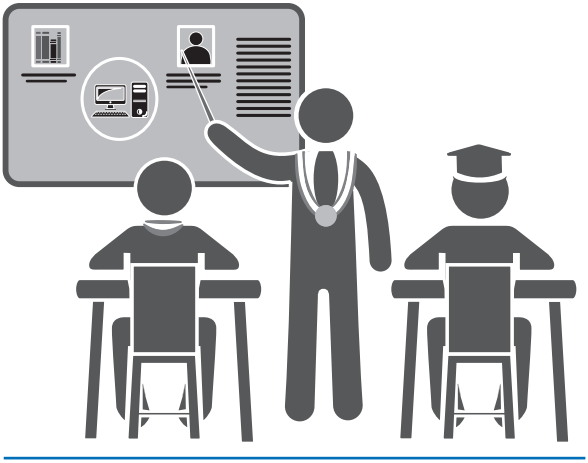
- Protocolo de la Agencia Europea de Seguridad de la Información (ENISA) "Identification and Handling of Electronic Evidence" - https://www.enisa.europa.eu
- Protocolo del Instituto Nacional de Justicia del Departamento de Justicia de los Estados Unidos "Forensic Examination of Digital Evidence: A Guide for Law Enforcement"
- Protocolo del grupo de trabajo científico en evidencia digital (SWGDE) "Best Practices for Computer Forensics" - https://www.swgde.org/
- Protocolo de las fuerzas policiales de Inglaterra, Gales y el Norte de Irlanda (ACPO) "Good Practice Guide for Digital Evidence"
- "Protocolo de Actuación para Pericias Informáticas" de la Provincia del Neuquén, República de Argentina.

- La "Guía Integral de Empleo de la informática Forense en el Proceso Penal" del Laboratorio de Investigación y Desarrollo de Tecnología en Informática Forense y la Universidad FASTA - Fraternidad de Agrupaciones Santo Tomás de Aquino- de Mar del Plata, Provincia de Buenos Aires, República de Argentina
- Manual de Manejo de Evidencias Digitales y Entornos Informáticos. Versión 2.0 Organización de los Estados Americanos.

- Norma ISO/IEC 27037:2012 “Guidelines for identification, colecction, adquisition and preservation of digital evidence” y la Norma ISO/ IEC 27042/2015 “Information Technology – Security Techniques – Guidelines for the analysis and interpretation of digital evidence”
- Guía del Federal Bureau of Investigation, Department of Justice “Digital Evidence Policy Guide”
- “Guía para recolectar y archivar evidencias – RFC 3227”, febrero 2002. Brezinski, Dominique. Killalea, Tom.
- Convención de Cibercriminalidad (Budapest, 2001)
- Reglamento de la Cadena de Custodia de Elementos Materiales, Evidencias y Administración de Bienes Incautados (Aprobado por Resolución Nº 729-2006-MP-FN del 15 de.junio de 2006)
- Acuerdos Plenarios Nº 5-2010/CJ-116 y Nº 6-2012/CJ-116, de la Corte Suprema de Justicia de la República. Perú

3. Principios básicos y generales

1. Es fundamental la capacitación y el entrenamiento de los investigadores, técnicos y fiscales para un correcto procedimiento, exento de falencias u objeciones procesales.
2. El personal policial no debe adoptar ninguna decisión en la escena del delito que pueda alterar o modificar los datos contenidos en los dispositivos de almacenamiento a utilizar sin previa consulta con el fiscal.
3. Del mismo modo, las herramientas y metodologías a utilizar en la escena del delito, deben ser previamente acordadas con el director de la investigación.



4. Principios del peritaje

1. **Objetividad:**

   Es un requisito que le compete tanto al fiscal que dirige la investigación y por ende elabora los puntos de pericia a realizarse, como al perito informático que analizará la información previamente identificada, asegurada, adquirida y preservada a los fines de su análisis.

2. **Legalidad:**

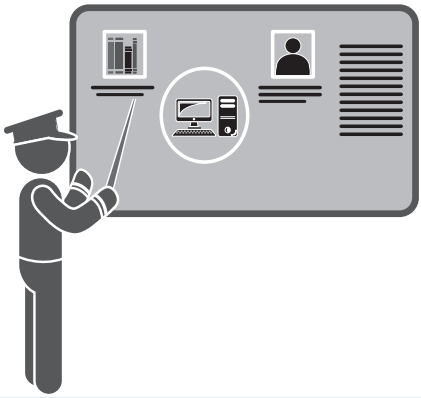
   El perito deberá ser preciso en sus conclusiones, en la metodología utilizada para arribar al resultado, y su actuación será acorde a la legislación de la actividad técnica-informática-pericial

3. **Idoneidad:**

   Las herramientas informáticas utilizadas deberán ser idóneas y validadas para otorgar apoyatura a las conclusiones arribadas

4. **Inalterabilidad:**

   Será fundamental el debido cumplimiento de la cadena de custodia que asegure que no ha existido alteración ni modificación en el peritaje.



5. Definición, importancia y tratamiento de la Evidencia Digital

La *evidencia digital* es todo registro informático almacenado en un dispositivo informático o que se transmite a través de una red informática y que pudiera tener valor probatorio para una investigación[2].

Se considera evidencia digital a cualquier información que, sujeta a una intervención humana, electrónica, y/o informática, ha sido extraída de cualquier clase de medio tecnológico informático –computadoras, etc. Técnicamente, es un tipo de evidencia física que está constituida por campos magnéticos y pulsos electrónicos que pueden ser recolectados y analizados con herramientas técnicas especiales[3].

La importancia de la evidencia digital reside en la necesidad de demostrarle al juez la prueba fehaciente que convierte en responsable al sospechoso. Por eso, es fundamental la correcta selección de la prueba relevante por parte del experto para no ser sobre abundante o superflua. El correcto tratamiento de la evidencia digital es fundamental para que sea admisible: haber sido obtenida respetando las garantías y procedimientos legales, basada en una previa autorización judicial o del director de investigación, justificando su tratamiento en los procedimientos de obtención, preservación, análisis y presentación ante el tribunal, respetando la cadena de custodia, cuyos pasos deberá desprenderse de un manual de buenas prácticas.

Asimismo, deben poder justificarse todos los métodos y acciones realizadas en el tratamiento de la evidencia digital, a través de la demostración de la validación de los métodos utilizados y de los procesos realizados.

También se deberá documentar las acciones realizadas y justificar todas las decisiones en las etapas del proceso, y se deben obtener los mismos resultados en caso de aplicar el mismo procedimiento, pero con herramientas diferentes, en cualquier momento.

[2] PRESMAN-SALLIS, *Procedimiento para el manejo, tratamiento y recolección de la evidencia digital.*

[3] Laboratorio de Investigación y Desarrollo de Tecnología en Informática Forense. Info-Lab. *Guia Integral de Empleo de la Informática Forense en el Procedimiento Penal.* Segunda Edición. Abril 2016.

6. Fuentes de la Evidencia Digital

La evidencia digital puede encontrarse almacenada en dispositivos informáticos (discos rígidos, por ejemplo); en la memoria RAM de procesamiento de un sistema informático; o bien, cuando se transmite a través de una red de dispositivos cuya recolección se realizará en tiempo real (tráfico de datos).

En este sentido, las fuentes de evidencia digital pueden ser clasificadas en los siguientes grupos:

a. Sistema de computación abiertos:

Son los que están compuestos de las computadoras personales y de sus periféricos; las computadoras portátiles, y los servidores.

b. Sistemas de comunicación:

Compuestos por las redes de telecomunicaciones, la comunicación inalámbrica e Internet.

c. Sistemas convergentes de computación:

Sólo los que están formados por los teléfonos celulares inteligentes (Smartphones), los asistentes personales digitales PDAs, las tarjetas inteligentes.

En este contexto, el hardware está conformado por todos los componentes físicos de un sistema informático, mientras que la información se refiere a los datos, programas almacenados y mensajes de datos transmitidos usando el sistema informático.

7. Características de la Evidencia Digital

1. **Volátil:**
   Si no es preservada adecuadamente puede cambiar o variar con facilidad de forma poco previsible.

2. **Duplicable:**
   Puede ser duplicada de manera exacta y copiada tal como si fuese el original.

3. **Alterable y modificable:**
   Con las herramientas adecuadas es relativamente fácil alterar destruir, alterar o modificar.

4. **Eliminable:**
   Con las herramientas adecuadas puede ser eliminada por completo.

8. Aseguramiento de la escena del delito

A partir de aquí, debemos tener en cuenta que quienes participen en los diferentes actos, ya sean estos, estrictamente de aseguramiento o análisis de la evidencia o de conducción de la investigación penal, lo harán bajo las prescripciones del Nuevo Código Procesal Penal –Decreto Legislativo n° 957.

En éste sentido, tal como surge del mencionado cuerpo normativo, en función de lo prescripto en su artículo 67, el aseguramiento de la escena del delito será llevado a cabo por funcionarios de la Policía Judicial que cuenten con un conocimiento técnico avanzado en cuanto al manejo de la evidencia digital, debiendo dar inmediata noticia de ello al Fiscal.

En cuanto a las atribuciones que le caben a funcionarios de la Policia Nacional, el artículo 68 establece, que bajo la conducción del Fiscal, podrán llevar a cabo numerosas tareas, siendo las más relevantes para este trabajo las que a continuación se detallan: a) Recoger y conservar los objetos e instrumentos relacionados con el delito, así como todo elemento material que pueda servir a la investigación; b) Levantar planos, tomar fotografías, realizar grabaciones en video y demás operaciones técnicas o científicas; c) Efectuar, bajo inventario, los secuestros e incautaciones necesarias en los casos de delitos flagrantes o de peligro inminente de su perpetración. El propio artículo 68 obliga a los funcionarios de la Policía Nacional que todo lo actuado quedará sentado en actas detalladas que se entregarán al Fiscal.

Luego de ello, la investigación quedará en cabeza del Ministerio Público, siendo el Fiscal quien puede realizar –si correspondiera las primeras diligencias preliminares o disponer que sean realizadas por la Policía Nacional (conforme Art. 65 del NCPP). Sobre este punto, ponemos de resalto que es de vital importancia que quienes intervengan en la escena del delito sean personas capacitadas sobre el manejo de la evidencia, ya que mediante un correcto desempeño de sus funciones se gaarantiza desde el inicio la integridad de los distintos dispositivos que puedan ser incautados.

En efecto si bien la norma, habilitaría al Fiscal a ejecutar el mismo las diligencias preliminares, para garantizar el éxito de esas medidas, sería atinado que las mismas sean cumplidas por personal técnico especializado, más aún, cuando la propia ley procesal, permite que ellas sean encomendadas a la Policía Nacional.

Asegurar la escena del delito consiste en proteger y delimitar la escena para evitar la modificación o destrucción de las evidencias digitales.

El personal que accede a la escena debe contar con experiencia previa o estar capacitado en el manejo de la evidencia digital para adoptar mejores decisiones. Toda actividad llevada a cabo fuera de los protocolos establecidos podría alterar la evidencia.

En términos generales, los investigadores que arriben a una escena del delito deberán cumplir los siguientes recaudos:

- **Establecer los parámetros de la escena del delito:** los primeros en llegar a la escena deberán observar las características físicas del área; la cual será extendida a los sistemas de información y de red que se encuentre dentro de la escena.
- **Observación, valoración y planificación:** la planificación de las actividades que se realicen durante la investigación previa que confluya en la escena del delito asegurarán su éxito. Mediante una observación detallada de la escena del hecho se establecerán escenarios principales y secundarios, se fijarán prioridades y se garantizará la seguridad de los especialistas. Deberá también relevarse la existencia en el lugar de sistemas integrados de videovigilancia, monitoreo de imágenes o CCTV, tanto en el interior de los locales o inmuebles a registrar como en las zonas adyacentes al ingreso a la propiedad en la vía pública. En caso de detectarse la existencia de estos dispositivos deberá procurarse la preservación de las imágenes que pudieren haber captado.
- **Delimitar la escena del delito:** demarcar específicamente el sitio donde tuvo lugar el hecho o donde se ubica la evidencia a recolectar, como así también, las vías de acceso y salida, zonas adyacentes, vehículos y/o medios de transporte asociados a las personas investigadas. Deberá perennizarse la escena, desde el ingreso mismo al local, vivienda, oficina o lugar cerrado que se trate, o si fuere en la vía pública o espacios abiertos, mediante el uso de fotografía, video, croquis y planos. Asimismo, deberán establecerse,

considerando previamente la existencia de riesgos para las personas o la vida, los perímetros de intervención primaria, secundaria y terciaria, delimitándose el ingreso a cada una de estas de los actores designados al efecto, conforme las reglas de la criminalística.

- **Asegurar la identificación de testigos, policías, médicos, bomberos, personal especializado.**
- **Establecer las medidas de seguridad:** ante todo la seguridad de los investigadores y de la escena. Se tomarán las medidas necesarias a fin de evitar todo tipo de riesgo (eléctrico, químicos o biológicos, o cualquier actividad criminal).
- **Facilitar los primeros auxilios:** se deberán arbitrar los medios para brindar el cuidado médico adecuado por parte del personal de emergencias en pos de cuidar la vida de las eventuales víctimas del delito, y para preservar las evidencias.
- **Asegurar físicamente la escena:** se deben retirar de la escena del delito a todas las personas extrañas a ella, con el fin de prevenir el acceso no autorizado para evitar la contaminación y/o alteración de las evidencias. En caso que hubiere duda acerca de la vinculación de las personas que se encontraren en el lugar con la evidencia digital a incautar, deberá asegurarse la identificación de estas personas, con el fin de establecer posibles conexiones con el hecho investigado y los dispositivos digitales a incautar (Artículo 209 del NCPP).
- **Asegurar físicamente las evidencias:** este paso es fundamental a fin de iniciar y preservar la cadena de custodia de las evidencias, debiendo identificarlas y etiquetarlas, de acuerdo a los principios y metodología correspondientes a la recolección de evidencias por parte de personal capacitado. Se deberá verificar que todas las evidencias se hayan recogido y almacenado correctamente, y que los sistemas y redes comprometidos pueda volver a su normal operación.
- **Documentar la escena:** los investigadores deberán documentar cada una de las etapas este proceso a fin de plasmar lo sucedido en la escena del delito, las evidencias encontradas y su posible relación con los sospechosos.

9. Reconocimiento e Identificación de la Evidencia Digital

Es la fase de la identificación de los equipos y dispositivos de almacenamiento informático cuya obtención y examen se considere pertinente y útil para la estrategia de investigación penal delineada por el Fiscal.

El objetivo de esta etapa, es preparar adecuadamente las fases de recolección y/o adquisición, para garantizar que la evidencia digital a obtener sea relevante, suficiente, confiable, y legalmente válida.

Es importante establecer los procesos de trabajos, efectuando un orden de prioridad y relevancia entre todas evidencias que se pretenden obtener (volcado de memoria, recolección, uso de la herramienta *triage*, etc.).

Cuando se planifica la recolección de la evidencia digital, y se releva para identificar los dispositivos de almacenamiento, se deberán priorizar las fuentes de evidencia más volátil.

Se deberá diferenciar los dispositivos que son transportables, los cuales serán objeto de recolección para su posterior análisis en laboratorio pericial, de los que, por su volumen, número, etc., no se podrán transportar y deberán ser procesados en el lugar (servidores).

Durante esta etapa intervendrán los especialistas en manejo de evidencia digital que integren las fuerzas de la Policía Nacional.

9.1 DÓNDE ENCONTRAR LA EVIDENCIA

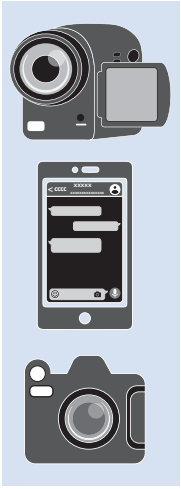
1. Dispositivos de almacenamiento informático

Pueden ser:

- **Unidades de disco rígido internas:** discos de aluminio o vidrio, recubiertos de material ferro magnético, cabeza de lectura/escritura.
- **Discos rígidos externos:** requieren fuente de alimentación y un USB, FireWire, Ethernet, conexión inalámbrica.

- **Medios extraíbles:** unidades de disco para almacenar, archivar y transportar datos.
- **Pendrive (USB):** Dispositivo de almacenamiento extraíble mediante conexión USB.
- **Tarjeta de memoria:** dispositivo de almacenamiento de datos de uso en cámaras digitales, teléfonos celulares, reproductores de música digital, notebook, consolas de videojuego, PDAs, Smart TV.

Posibles evidencias: mensajes de correo, historial de navegación de Internet, Chat de Internet, listas de registros, fotografías en distintos formatos de archivos (JPG, PNG, GIF, BMP, TIF), archivos de imágenes, documentos, archivos de texto, metadatos de archivos, claves en memoria, claves de encriptación,etc.

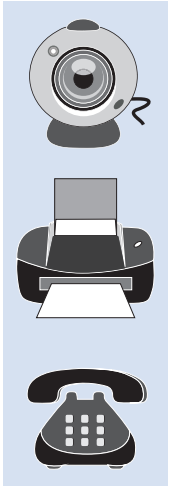


2. Dispositivos portátiles

- Teléfonos celulares
- Smartwatches
- PDAs
- Dispositivos digitales multimedia
- Cámaras digitales
- Sistemas de posicionamiento global (GPS)
- Reproductores
- Video filmadoras
- Localizador
- Sistemas en vehículos
- Cámaras de seguridad

Posibles evidencias: Listado de llamados, mensajes recibidos y enviados, páginas de Internet visitadas, datos de localización geográfica, aplicaciones de software, documentos, mensajes de correo, historial de navegación de Internet, chat de Internet, fotografías, archivos de imágenes, base de datos y registros, mensajes de voz, redes Wi-Fi detectadas.

3. Dispositivos periféricos



- Teclado
- Mouse
- Parlantes
- Cámaras
- Fax
- Teléfonos
- Router
- Módem
- Impresoras
- Escáners
- Fotocopiadoras
- Contestadores automáticos

Posibles evidencias: Entrada y salida de números de teléfonos y fax, llamados recientes, fax en la memoria, documentos impresos, impresiones dactilares, ADN, etc. Estos dispositivos pueden aportar evidencia física que permita vincular al usuario con el dispositivo digital incautado.

4. Redes de computadoras:

Consta de dos o más computadoras conectadas por cables de datos o conexiones inalámbricas que comparten recursos e incluso de impresoras, periféricos, y dispositivos de enrutamiento de datos (hubs, switches y routers).

Posibles evidencias: Pruebas de software, documentos, fotos, archivos de imágenes, mensaje de correo y archivos adjuntos, base de datos, historial de navegación de Internet, registros de eventos y chat, datos almacenados en dispositivos externos.

9.2 RECOMENDACIONES

- Separar las personas que se encuentren trabajando sobre los equipos informáticos. No permitirles volver a utilizarlos. Si es una empresa, institución o inmueble cuyos dispositivos informáticos estén vinculados

a un servidor, podrá procurarse identificar al administrador del sistema o gestor informático.

- Fotografiar la escena del hecho y los dispositivos digitales antes de moverlos o desconectarlos: toma completa del lugar donde se encuentren los equipos informáticos, y de las pantallas de las computadoras, si están encendidas.
- Verificar la existencia de consolas de videojuegos y Smart TVs, y otros con capacidad de almacenar información en formato digital, para proceder a su eventual incautación.
- Evitar tocar el material informático sin guantes descartables.
- Si los equipos están apagados, deben quedar así; al igual si están encendidos: comprobar ventiladores y LEDS; comprobar si el monitor está encendido; observar si hay acceso desde otros equipos o dispositivos remotos; buscar si hay comunicaciones en curso con otros usuarios o salas de chat, y cámara web activas.
- Si los equipos están apagados, desconectar de su respectiva toma eléctrica. Si son notebooks será necesario quitarle la batería. En caso de ser imposible, se deberá contar con un medio de resguardo o dispositivo adaptable que inhiba las vías de comunicación entrante y saliente del dispositivo en cuestión; ya sea un inhibidor de señales o un dispositivo de almacenamiento que bloquee las señales (bolsa de Faraday). Desconectar cables de red o apagar el router o Modem.
- Identificar si existen equipos que estén conectados a líneas telefónicas y, en su caso, el número telefónico para registrarlo en el acta de allanamiento e incautación.
- Impedir que se realicen búsquedas en los ordenadores, sobre directorios o ver la información almacenada ya que esto altera y destruye la evidencia. Lo expuesto incluye intentar hacer una copia sin tener el software forense específico y sin que quede documentado el procedimiento realizado. En caso de no contarse con el software forense específico para la extracción inalterable de datos o copias espejo de los dispositivos informáticos o de comunicaciones, o si se los tuviera, no se contara con la autorización judicial correspondiente para proceder de dicha forma en el lugar, deberá inmovilizarse y lacrarse el lugar y las posibles evidencias, proveyéndose la correspondiente custodia provisoria del mismo. (Artículo 68,1, b) del NCPP).
- Identificar correctamente todas las evidencias.

10. Adquisición y captura de la Evidencia Digital

Esta fase comprende la recolección de los objetos contenedores de evidencia digital.

Se seleccionarán los dispositivos que puedan contener evidencia digital y se preverá su correcto embalaje para ser transportados a un laboratorio especializado donde se efectúe la recolección y preservación correspondiente.

La recolección debe realizarse de un modo tal que asegure la utilidad procesal de los dispositivos de almacenamiento informático recogidos, garantizando la identidad e integridad de la evidencia.

El levantamiento debe ser realizado empleando las técnicas adecuadas, actuando dentro de los límites legales y procesales y sin exceder los alcances de la autorización judicial; debiendo consultar inmediatamente, en caso de duda, al director de investigación.

Se deberá registrar esta etapa con medios fotográficos, de video documentando lo actuado adecuadamente.

10.1 EVIDENCIA A RECOLECTAR

- Incautar preferentemente dispositivos informáticos que almacenen grandes volúmenes de información digital (computadoras, Notebooks, disco dirigidos externos). También se incautarán dispositivos de almacenamiento externos (DVD, CD, USB, etc.). Todo ello deberá estar específicamente detallado en la orden de allanamiento emanada por el juez a pedido del fiscal. Si los investigadores informáticos encuentran algún otro dispositivo que no se encuentre detallado expresamente en la orden judicial, deberán comunicarse telefónicamente desde lugar con el fiscal a fin de efectuar la correspondiente consulta a fin que analice y autorice la conveniencia de incautar dicho dispositivo informático.
- Cuando el material inspeccionado sea muy voluminoso, o se encuentran afectados derechos de terceros, o se requiera conocer de forma urgente el contenido de un dispositivo de almacenamiento, se

analizará la posibilidad de usar las herramientas de muestreo rápido *(triage). El triage* consiste en realizar una búsqueda rápida empleando criterios sencillos sobre la estructura del disco, evitando profundizar las búsquedas en áreas especiales del disco. Esta técnica, si bien ha demostrado ser de gran utilidad en allanamientos con gran cantidad de equipos, empleando criterios de búsquedas claros y acotados, existe un riesgo de dejar de lado evidencia potencial de utilidad para la investigación, privilegiando la velocidad o la urgencia del procedimiento.

- En caso de considerarse pertinente, contar con la autorización judicial y el software necesario, podrá decidirse con el experto informático la realización de una copia o imagen forense, en la escena de delito. La recolección de evidencia digital mediante imágenes forenses requiere de la experticia y la disponibilidad de equipamientos e insumos para su realización. Una imagen forense es una copia bloque a bloque *–bit a bit-* del contenido digital almacenado, el que es autenticado mediante una función HASH[4] o digesto matemático (ANEXO I), a fin de asegurar la integridad de la evidencia colectada. Las imágenes forenses pueden realizarse mediante una computadora y un programa, o bien, utilizando un dispositivo autónomo denominado *duplicador forense* (ANEXO II).
- En el primer caso, y a fin de no contaminar la prueba, se deberá acceder al elemento de almacenamiento a través de un dispositivo que bloquee la escritura o empleando un sistema operativo que no escriba sobre el medio digital (ANEXO III).
- En cambio, la utilización de un duplicador forense lleva implícito el bloqueo de escritura y, al ser un dispositivo de hardware, el software se encuentra optimizado, mejorando drásticamente la velocidad del proceso, Incluso al producir múltiples copias.
- La excepción es *la investigación en vivo*. Excepción, pues se debe evitar acceder al contenido de los elementos electrónicos para evitar su contaminación. Sin embargo, en caso de urgencia o peligro de vida, el tiempo que insume la realización de copias forenses, puede

[4] El HASH se refiere a una función o método para generar claves que representen de manera casi unívoca a un documento, registro, archivo etc. Resumir o identificar un dato a través de la probabilidad, Utilizando una función hash o algoritmo hash. El hash permite darle mayor seguridad de que la evidencia digital obtenida no fue manipulada ni alterada, ya que el HASH generado es inviolable.

tener gran impacto en el desenlace de investigación, Por lo que, previa autorización del juez, se puede acceder en vivo al dispositivo, debiendo documentar detalladamente todo las acciones efectuadas, para comprender el impacto de las mismas en la interacción con el dispositivo[5].

- En el proceso de recolección de evidencia digital se debe tener en cuenta el orden de volatilidad, debiendo respetar el siguiente, ordenado de mayor a menor: a) contenido de registros, b) tablas de ruteo y memoria caché, c) procesos de ejecución, d) memoria RAM, e) dispositivos de almacenamiento masivo, f) contenedores de almacenamiento remoto, g) almacenamiento de resguardo y respaldo[6].
- Adquisición de datos volátiles: este proceso de trabajo consiste en la extracción de datos volátiles, que sólo se encuentran presentes en equipos encendidos y suelen ser eliminados con el apagado: registros contenidos de la caché, contenido de la memoria física, estado de las conexiones de red, tabla de rutas, procesos en ejecución, archivos temporales, información remota, etcétera.

10.2 DIFERENTES ESCENARIOS

Escenario I

- Monitor encendido mostrando aplicación, programa, imagen, mail: fotografiar pantalla y registrar información
- Monitor encendido mostrando protector de pantalla: mover el mouse (sin mover rueda ni cliquear). Fotografiar pantalla
- Monitor encendido mostrando pantalla en blanco: mover el mouse (sin mover rueda ni cliquear). Fotografiar pantalla
- Monitor apagado y ordenador encendido: encender el monitor y fotografiar la pantalla
- Monitor encendido y ordenador aparentemente apagado: mover mouse; si no cambia pantalla, verificar corriente, luces led del CPU para verificar encendido
- Verificar que el monitor no se trate de procesador del tipo All in One

[5] Presman,G., Sallis, E. Procedimiento para el manejo, tratamiento y recolección de la evidencia digital

[6] Lineamientos de la RFC 3227 Guidelines for Evidence Collection and Archiving publicada en Internet Society

(Todo en Uno). Si fuere de este tipo deberá procederse de acuerdo al escenario previsto para la incautación de un ordenador

Escenario II

- **Ordenador encendido:**

  Fotografiar pantalla. Registrar la hora del reloj del sistema. Evaluar con el Director de la investigación y con el perito informático, la captura de datos in situ o la incautación del equipo. Eliminar corriente de alimentación inmediata en caso de verificar actividad de eliminación o sobre escritura de datos No desconectar inmediatamente en caso de indicios activos de salas de chat, documentos de texto en ejecución, ventanas de mensajes instantáneos: fotografiar.

- **Ordenador apagado:**

  1. Documentar, etiquetar y fotografiar cables, dispositivos y puertos. Luego desconectarlos.
  2. Retirar cable de alimentación de parte posterior del CPU o batería. Encintar interruptor encendido.
  3. Verificar unidad CD o DVD, encintar ranura.
  4. Registrar marca, modelo, número de serie.
  5. Empaquetar y preservar cadena de custodia.

10.3 EMBALAJE Y ROTULADO (ANEXO IV)

- Este será primer paso del procedimiento de cadena de custodia[7]
- Rotular el hardware que se va a incautar con los siguientes datos:

[7] La cadena de custodia es el procedimiento destinado a garantizar la individualización, seguridad y preservación de los elementos materiales y evidencias, recolectados de acuerdo a su naturaleza o incorporados en toda investigación de un hecho punible, destinados a garantizar su autenticidad, para los efectos del proceso. Las actas, formularios y embalajes forman parte de la cadena de custodia. (Artículo 7º del Reglamento de la Cadena de Custodia de Elementos Materiales, Evidencias y Administración de Bienes Incautados. Aprobado por Resolución Nº 729-2006-MP-FN del 15.junio.2006). La cadena de custodia se inicia con el aseguramiento, inmovilización o recojo de los elementos materiales y evidencias en el lugar de los hechos, duranre las primeras diligencias o incorporados en el curso de la investigación preparatoria; y concluye con la disposición o resolución que establezca su destino final (Artículo 8º del Reglamento de la Cadena de Custodia de Elementos Materiales, Evidencias y Administración de Bienes Incautados, ya citado.)

a) **Para computadoras, notebooks, celulares, etc.:** número de expediente judicial, fecha y hora, número de serie, fabricante, modelo.

b) **Para DVDs, CDs, Pendrive (USB), etc.:** almacenarlos en conjunto, especie y cantidad. Verificar si en su etiqueta, los DVDs o CDs son del tipo regrabables, en cuyo caso se aconseja autenticación mediante generación de HASH.

- Periféricos específicos conectados hay equipos informáticos, incautar e identificar con etiquetas con números los cables para indicar donde se deben conectar
- Fotografiar los equipos con sus respectivos cables de conexión etiquetados
- Usar bolsas tipo polietileno o similar, resistentes para almacenar dispositivos de almacenamiento informáticos
- Se procurará no incluir en un mismo embalaje, evidencia que tenga diferentes destinos periciales
- Cada elemento deberá ser rotulado por separado
- El rótulo será pre impreso y de carácter inviolable
- El rótulo debe escribirse con tinta indeleble, grafías legibles y comprensibles, debiendo ser firmado por el especialista en recolección/adquisición, la autoridad a cargo del procedimiento, y de los testigos en caso de corresponder (Artículo 120, 4 del NCPP)
- Rotular en cada equipo informático todas sus entradas eléctricas, puertos periféricos y todas las partes que puedan ser abiertas o removidas
- Resguardado del material informático en un lugar limpio. No deberán exponerse los elementos incautados a altas temperaturas o campos electromagnéticos
- Mantener la cadena de custodia del material informático transportado
- Fotografiar la totalidad de los elementos incautados una vez embalados
- Recolectar cualquier elemento adicional que pueda ser de utilidad para el acceso al dispositivo (manuales técnicos, llaves electrónicas, fuente de alimentación, etcétera.)

10.4 ELEMENTOS Y MATERIALES PARA LA RECOLECCIÓN DE EVIDENCIA DIGITAL

- Cámara de fotos/Filmadora
- Cajas de cartón
- Cuadernos para anotaciones y croquis
- Guantes
- Bolsas para resguardo de dispositivos
- Etiquetas
- Bolsas antiestáticas (aislamiento Faraday o papel de aluminio)
- Marcadores permanentes
- Precintos
- Rótulos para precintado de puertos de entrada
- Herramientas desmagnetizadas
- Otros

10.5 DOCUMENTACIÓN Y REGISTRO DE LO ACTUADO

- Los requerimientos de allanamiento e incautación, conforme lo previsto por los Artículos 214 al 217 del NCPP solicitados por Fiscal al Juez competente, además de contemplar las prescripciones de forma pertinentes del Código Procesal Penal, podrán ampliarse a todas las dependencias o habitaciones que formaren parte del inmueble, local, vivienda o unidad funcional que se trate. También deberá procurarse abarcar el registro vehicular de los automotores que se encontraren en el lugar y que pudieren tener vinculación con los hechos o las personas involucradas, y la incautación de su interior de los elementos o efectos útiles para la investigación. Serán los funcionarios de la Policía Nacional los encargados de dar cumplimiento al allanamiento, el registro de personas y consecuentemente la incautación de bienes que puedan servir como prueba o ser objeto de decomiso.(Cfr. Artículos 67 y 68 del NCPP).
- Se deberán suscribir las actas pertinentes, que se elaborarán cumpliendo las formalidades previstas en el Código Procesal Penal, con las exigencias específicas relativas a la documentación de registros domiciliarios, revistas, incautación, inspección y

reconstrucción (Artículos 120, 155, 157, 158, 172/181, 177, 178, 202, 203, 208, 210, 214/217, 226, 227, 230 y 231 del Código Procesal Penal del Perú).

- El registro documental será de modo descriptivo mediante el relato preciso, detallado, e imparcial, suministrando una noción clara del lugar, de las evidencias incautadas y el estado que fueron halladas.[8]
- Las actas se complementarán con fotografía, filmaciones, planos del lugar y del sitio de ubicación de cada efecto.
- Cada evidencia recogida será identificada con un método uniforme de identificador único *(código de barras*, nomenclador alfanúmerico, por ejemplo) consignándose donde se levantó, en qué estado se encontraba, con cuáles equipos o sistemas estaba conectada, quien efectuó la recolección de la misma, actuando de ser el caso, en presencia de los testigos que hayan sido convocados al procedimiento.

[8] Los elementos materiales, evidencias y bienes incautados se registrarán en el formato de cadena de custodia mediante una descripción minuciosa y detallada de los caracteres, medidas, peso, tamaño, color, especie, estado, entre otros datos del medio en el que se hallaron los elementos materiales y evidencias, de las técnicas utilizadas en el recojo y pericias que se dispongan, en el cual no se admiten enmendaduras. En caso que amerite una corrección, ésta se efectuará entre paréntesis, explicando los motivos que la generaron. Los bienes materiales y las evidencias recolectadas o incorporadas, deberán ser debidamente rotuladas y etiquetadas para su correcta identificación y seguridad e inalterabilidad. (Artículo 11º del Reglamento de la Cadena de Custodia de Elementos Materiales, Evidencias y Administración de Bienes Incautados, ya citado.)

11. Dispositivos telefónicos

Ante el hallazgo de equipos móviles y/o cualquier otro dispositivo que utilice la red de comunicación se adoptara recaudos adicionales:

- No manipular el teléfono
- Dejar constancia en acta del lugar del hallazgo y usuario o poseedor del mismo
- Dejar constancia si estaba apagado o encendido: si está encendido, colocarlo en modo avión y quitar la batería, y si está apagado, también sacar la batería para consignar IMEI y CHIP, Memoria MicroSD. (ANEXO V)
- Para los dispositivos telefónicos que no tengan batería extraíble que pueda retirarse (IPhone), colocarlo en modo avión
- Si el aparato está apagado, déjelo apagado ya que al prenderlo puede alterar evidencia digital
- Detectar el número de IMEI del aparato y número de CHIP, asentarlo en el acta y fotografiar ambos
- Preservar cada celular y su batería en bolsa transparente precintada en forma separada y etiquetada

De los dispositivos telefónicos se obtiene evidencia digital, pues almacena información de contactos, envía y recibe correos y mensajes de texto, navegan por Internet, reproduce audio y video, servicio GPS, permite acceso a redes sociales, contraseña del correo de voz, número de acceso al correo de voz, números personales de identificación, información guardada en las tarjetas de expansión de memoria.

Los elementos técnicos que nos permite información investigativa son:

- ***SIM:*** Código de identificación del chip que contiene la línea telefónica. Se obtienen datos de llamadas entrantes y salientes con posicionamiento de antenas, datos comerciales de quien y donde la adquirió, donde se efectúan pagos y recargas, averiguación de IMEI

- ***IMEI:*** Es el código que identifica al aparato de telefonía. Se podrá averiguar acerca de las tarjetas SIM que impactaron en ese IMEI (información de todas las compañías telefónicas)
- ***Celda:*** Es el espacio de cobertura de telefonía celular, dividido en tres sectores. Se identifica posicionamientos de lugar en función de latitud y longitud

11.1 EXTRACCIÓN FORENSE DE CELULARES (ANEXO VI)

A través de la extracción forense de datos, pueden obtenerse la siguiente información, dependiendo del modelo y características tecnológicas del aparato.

- Permite recuperar y analizar evidencias de teléfonos móviles: Guardar, imprimir, exportar los datos extraídos
- Registros e historial de llamadas aún los borrados de la SIM
- Contactos
- Datos de teléfono (IMEI, número de teléfono)
- Mensajes de texto (SMS) aún los borrados de la SIM. Redes sociales (Facebook, WhatsApp, twitter, viber, etcetera)
- Fotografías
- Videos
- Archivos de sonido
- Información de localización de la SIM
- Clonación del ID de la SIM: permite extraer datos de SIM bloqueadas por PIN, de teléfonos sin tarjeta SIM y de teléfonos sin servicio de red. Permite acceder al teléfono sin conexión (mantiene el historial, sin nueva actividad)

12. Otros aparatos electrónicos

También podemos encontrar evidencia digital en otros aparatos electrónicos, como pueden ser, teléfonos inalámbricos, aparatos de mensajería instantánea, beepers y máquinas de Fax.

12.1 TELÉFONOS INALÁMBRICOS

En estos teléfonos se puede hallar potencial evidencia digital de interés para la investigación, entre las que se destacan:

- Llamadas realizadas
- Llamadas entrantes
- Números registrados en la memoria y el marcado rápido del dispositivo.
- Nombres y direcciones
- Correos de voz
- Dependiendo del dispositivo se podrá hallar también imágenes, grabaciones de voz, como así también, información resguardada en tarjetas de expansión de memoria

12.2 APARATOS DE MENSAJERÍA INSTANTÁNEA, BEEPERS

Existen varios tipos de equipos de mensajería instantánea:

- **Beepers Numéricos:** reciben y transmiten únicamente números y códigos
- **Beepers Alfanuméricos:** reciben números y letras y pueden cargar mensajes completos en texto
- **Beepers de Voz:** pueden transmitir mensajes de voz y también caracteres alfanuméricos
- **Beepers de dos vías:** envían mensajes de entrada y salida

A fin de adquirir y preservar la potencial evidencia en estos aparatos se deben adoptar las siguientes medidas:

Las buenas prácticas forenses recomiendan:

Una vez alejado el aparato del sospechoso, el mismo debe ser apagado. Si se lo mantuviera encendido, el dispositivo tiene capacidad de recibir mensajes y sin una orden judicial, ello puede ser considerado como una interceptación de correspondencia.

También se podrán efectuar búsquedas en la escena del hecho cuando:

El dispositivo contenga potencial evidencia que justifique una aprehensión.

Mediante la utilización del dispositivo se sospeche el cometimiento de un delito agrante.

12.3 MÁQUINAS DE FAX

En ellas se puede hallar:

- Listas de marcado rápido
- Fax guardados, ya sea enviados o recibidos
- Líneas de encabezados
- Fijación de la hora y fecha de la transmisión del Fax

Las buenas prácticas forenses recomiendan:

Si la máquina de fax es encontrada encendida, apagarla causaría la pérdida de memoria de los últimos números marcados, como así también de los facsímiles guardados. Por ello, mediante la debida documentación y registro de lo actuado se deberán adquirir esos datos de modo previo a su apagado e incautación.

12.4 IMPRESORAS

Las impresoras están diseñadas para imprimir, copiar y escanear documentos a una gran velocidad y esto es posible gracias los avances hechos en los últimos años -entre ellos, dotar a las impresoras de un

procesador central avanzado, memoria de almacenamiento y conexión a redes internas e Internet.

Son periféricos que escriben la información de salida sobre papel. Su comportamiento inicialmente era muy similar al de las máquinas de escribir, pero hoy día son mucho más sofisticadas, incluso algunas son fotocopiadoras o fax, conectadas con el ordenador. Todas estas características, son las que nos permitirán hallar en ellas evidencia que puede ser de interés en una investigación digital.

En ellas podemos hallar:

- Datos de la red a la que está conectada
- Su número de serie
- La versión del firmware que tiene instalada
- Documentos impresos recientemente almacenados en su memoria interna, en los que se podrá observar el contenido y los metadatos de la impresión –cantidad de hojas, copias, fecha y hora de la impresión, usuario que ordenó la impresión-
- También podrían contener pruebas biológicas (ADN, huellas digitales…), así como también documentos recientemente impresos

A fin de proceder al resguardo de la información que pueda contener el dispositivo el personal actuante deberá identificar el tipo de dispositivo frente al cual se encuentra y, allí establecer si el mismo, posee memoria interna que permita que luego de su apagado se pueda hallar evidencia en su interior sin ser alterada. Si ello no es posible, a fin de garantizar el éxito del hallazgo y la inalterabilidad de la posible evidencia mediante la debida documentación y registro de lo actuado se deberán adquirir esos datos previo a su apagado e incautación.

12.5 SMARTWATCHES

Un reloj inteligente (en inglés: smartwatch), es un reloj de pulsera dotado con funcionalidades que van más allá de las de uno convencional. Los primeros modelos desempeñaban funcionalidades muy básicas, pero los actuales ya son capaces de acceder a internet, realizar y recibir llamadas telefónicas, enviar y recibir emails y SMS, recibir notificaciones del smartphone e incluso consultar las redes sociales.

Estos dispositivos pueden incluir características como un acelerómetro, giroscopio, brújula, pulsómetro, barómetro, altímetro, geomagnetómetro, geolocalizador (GPS), altavoz, micrófono, etc. También cuentan con mecanismos de conectividad como el Bluetooth, NFC, WiFi, redes celulares o USB.

Cualquier dispositivo cuenta con un procesador, memoria, entrada y salida. Se puede recoger información de los sensores internos o externos. Se puede controlar, o recuperar datos de otros dispositivos.

Los Smartwatches tienen prácticamente las mismas funcionalidades que un Smartphone, razón por la cual, en ellos podemos hallar idéntica evidencia digital que un dispositivo telefónico.

Más allá de ello, se destaca que en virtud de la cercanía del Smartwatch con el usuario se pueden aprovechar datos específicos como: pulsaciones, geolocalización en un momento determinado, altura e inclusive establecer cual es el teléfono al que estaba vinculado si es que en el marco de la incautación no se había podido establecer a que persona pertenecía determinado Smartphone.

12.6 DISPOSITIVOS DE ALMACENAMIENTO

Los dispositivos de almacenamiento son utilizados para guardar mensajes de datos e información de los aparatos electrónicos. Hay tres clases de ellos: dispositivos magnéticos –discos duros o disquetes-; dispositivo de estado sólido –utilizados para para almacenar la información de forma constante como un disco rígido- o memorias sólidas –memorias flash y dispositivos USB- y; dispositivos ópticos –discos compactos y DVD´s-.

Las buenas prácticas forenses recomiendan:

- Obtener las instrucciones de uso, manuales y notas de cada dispositivo para una mejor interacción con el dispositivo
- Documentar todos los pasos al revisar y recolectar los dispositivos de almacenamiento, a fin de mantener la integridad probatoria del elemento incautado
- Alejar los dispositivos de almacenamiento de cualquier magneto, radio transmisores y otros dispositivos potencialmente dañinos

13. Correos electrónicos

El correo electrónico nos permite enviar y recibir cartas escritas ya sea desde la computadora, teléfono celular, Tablet y/o cualquier otro dispositivo con acceso a internet. El intercambio es casi instantáneo, a diferencia del correo normal. Se pueden enviar correos a cualquier persona sin importar el sitio físico donde se encuentra, requiriéndose únicamente que el emisor y el receptor cuenten con acceso a internet y dispongan de una cuenta de correo electrónico.

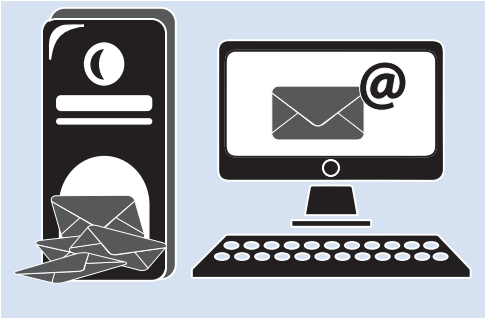
Al enviar un correo electrónico, el dispositivo emisor se identifica con una serie de números al sistema del *proveedor de servicios de Internet* (ISP –Internet Service Provider–). Inmediatamente, se le asigna una *dirección* IP y es dividido en pequeños paquetes de información a través del *protocolo TCP/IP (Protocolo de Control de Transferencia y Protocolo de Internet)*.

Esos paquetes pasan por una computadora que es llamada servidor que los fija con una identificación única –*message-ID*– y luego los sella con la fecha y hora de recepción.

Luego, al momento del envío se examina su dirección de correo para determinar si corresponde la dirección IP de alguna de las computadoras conectadas en una red local (dominio). Si no corresponde, envía los paquetes a otros servidores, hasta que encuentra al que reconoce la dirección como una computadora dentro de su dominio, y los dirigen a ella, es en este momento cuando los paquetes se unen otra vez en su forma original a través del protocolo TCP/IP, visualizándose en la interface gráfica del programa de correo electrónico utilizado en la máquina destinataria.

Los correos electrónicos permanecen alojados en un servidor de correo y no en la computadora del emisor o del destinatario, a no ser que el interesado los guarde allí. Entonces, al ser redactado un correo se transmite su contenido al servidor para ser enviado. Al recibirlo, la computadora hace una petición al Servidor del correo, para que los mensajes sean transmitidos luego a la computadora del destinatario, donde el operador la puede

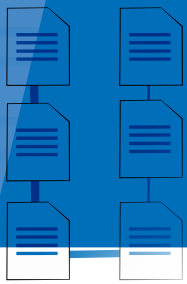
guardar o leer y cerrar. Así, al cerrar sin guardar, el correo desparece de la pantalla donde es visualizado, pero se mantiene en el servidor, hasta que el operador lo elimina.



Ahora bien, en ocasiones es necesario seguir el rastro de los Correos Electrónicos enviados por Internet. Los rastros se graban en el encabezamiento del mail recibido. Normalmente, el encabezamiento está sintetizado y su apariencia está determinada por la empresa proveedora del servicio de correo que recepciona el mensaje.

Sin perjuicio de ello, se podrá observar el encabezamiento completo o avanzado desde el panel de opciones de nuestro proveedor de correos. En él se podrá observar información sencilla y compleja para interpretar, como ser, los datos del *destinatario, emisor, una copia enviada y el título del mensaje*. Por otra parte, se verificarán datos como *direcciones IP:* 181.244.36.251; o *message ID:* qwXsfwWqNJ; los que necesariamente deberán ser interpretados por un especialista. (ANEXO VII).

14. Preservación de evidencia digital cadena de custodia



1. La cadena de custodia es una serie de recaudos destinados a asegurar el origen, la identidad o e integridad de la evidencia, evitando que se pierda, destruya o altere.
2. Se aplica a todo acto de aseguramiento, identificación, obtención, traslado, almacenamiento, entrega, recepción, exhibición y análisis de la evidencia, preservando su fuerza probatoria, permitiendo transparentar todo cambio o alteración de la evidencia.
3. Posibilita controlar la evidencia que contenga datos personales o sensibles, o correspondencia electrónica.
4. La cadena de custodia comienza desde el momento del hallazgo o recepción de la evidencia, y finaliza cuando la autoridad judicial competente decida sobre su destino.
5. La preservación es el resguardo seguro de la evidencia, durante los lapsos de tiempo en que esta no es transportada ni utilizada.
6. El depósito y preservación de la evidencia digital, y de sus contenedores, requiere contar con entornos adecuados en cuanto a la seguridad y reserva de los datos, suficiente capacidad de almacenamiento físico y virtual.
7. En la cadena de custodia participan todos los funcionarios y o empleados que intervengan durante las etapas del proceso sobre las evidencias.
8. El personal técnico deberá constatar el estado en que se encuentra el material recibido, el embalaje, los rótulos de seguridad, e identificación; cotejando la correspondencia entre los elementos recibidos y la documentación adjunta.

GLOSARIO

El presente glosario surge como necesidad de establecer un diccionario forense, de uso común para los destinatarios de este Manual. Las definiciones que a continuación se detallan se corresponde a terminología utilizada en este guía, como así también, se definen otros términos propios de la informática forense.

CONCEPTOS BÁSICOS:

- **Evidencia digital:** Información o datos, almacenado o transmitido en un medio informático, que puede ser utilizado como evidencia.
- **Copia de la evidencia digital:** Copia de una evidencia digital que se realiza para mantener la confiabilidad de la evidencia. Incluye tanto la evidencia digital como los medios de verificación. El método de verificación puede estar incluido en las herramientas utilizadas para la creación de la copia o ser independiente.
- **Adquisición:** Es el proceso de generar una copia de datos de un conjunto definido.
- **Identificación:** es el proceso de buscar, reconocer y documentar potencial evidencia digital.
- **Preservación:** es el proceso de mantener y resguardar la integridad y/o condición original de la potencial evidencia digital.
- **Recolección:** es el proceso de reunir/juntar objetos físicos pasibles de contener evidencia digital.

CONCEPTOS TÉCNICOS:

Los conceptos presentados en esta sección se basan en el Glosario de términos recolectado en la Guía Integral de Empleo de la Informática Forense en el Proceso Penal de la Universidad FASTA, de la Municipalidad de General Pueyrredón, Mar del Plata, Argentina:

ALMACENAMIENTO:

- **HPA - Host Protected Area:** es una zona de un dispositivo de almacenamiento donde puede almacenarse información, pero que en condiciones normales no se expone ni siquiera al sistema operativo. Su utilización permite ocultar información a los usuarios, usualmente para almacenar un programa de restauración del equipo.
- **RAID:** del inglés, Redundant Array of Independent Disks, es un conjunto de técnicas que permiten utilizar varios dispositivos de almacenamiento – usualmente discos de igual tamaño y rendimiento - como si fueran un sólo dispositivo. Esto permite mejoras en la integridad de los datos y velocidad de acceso.
- **Montar:** es el proceso de asociar un dispositivo con un directorio o unidad del sistema informático. Éste proceso es el que permite el acceso a los datos en un dispositivo, tanto para lectura como para escritura.
- **Partición:** es una porción lógica de un dispositivo de almacenamiento que tiene asociado un sistema de archivos.
- **Tabla de Particiones:** es una estructura que describe las particiones de un disco, su tamaño y su sistema de archivos asociado.
- **MBR:** es un formato de tabla de particiones que se utilizaba anteriormente. Hasta la década del 2010 aproximadamente.
- **GPT:** es un nuevo formato de tabla de particiones que tiene ventajas técnicas con respecto a MBR. Hasta que se adopte masivamente, ambos formatos conviven.

GENERAL:

- **Estructura de datos:** las estructuras de datos son formas de representar información en la memoria de una computadora. Diferentes estructuras de datos facilitan el trabajo con distintos tipos de información. Algunas estructuras características de determinados sistemas operativos o programas resultan útiles para el análisis forense.
- **Log:** un archivo que guarda un registro de información, acceso, funcionamiento y errores de un sistema.
- **Máquina Virtual:** es una emulación de otro equipo que se ejecuta sobre una computadora.
- **Hipervisor:** es un programa que administra los recursos de un equipo real para poder ejectuar una (o más) máquinas virtuales.

- **Almacenamiento distribuido:** un sistema de almacenamiento de información compuesto por varios equipos físicos (discos o servidores) que podrían encontrarse en distintos lugares físicos, incluso en ciudades, regiones o países diferentes.
- **Imagen:** una imagen es una copia exacta de un dispositivo de almacenamiento.
- **Volcado de memoria / imagen de memoria:** es una copia de los contenidos de la memoria volátil (usualmente llamada RAM) de un sistema informático.
- **ZIP:** Algoritmo de compresión de datos de uso extendido.
- **RAR:** Algoritmo de compresión de datos de amplio uso, competidor de ZIP.
- **GZip:** Algoritmo de compresión de datos, similar a ZIP, muy utilizado en ambientes UNIX.
- **Bzip2 / bz2:** Algoritmo de compresión de datos utilizado en ambientes UNIX. Tiene mejor rendimiento que GZip, aunque no está tan extendido.
- **Almacenamiento volátil:** es la región de almacenamiento de una computadora que tiene comunicación directa con el procesador. Usualmente se llama "memoria RAM", aunque en algunos sistemas de computación el término "almacenamiento volátil" es más abarcador y comprende otras partes adicionales de la computadora.
- **Hash:** es una función matemática que permite representar datos de longitud variable como un dato de longitud fija y donde pequeñas diferencias en los datos de entrada generan una gran diferencia en los datos de salida. Los valores resultados también se denominan hash (singular) o hashes y permiten identificar con gran nivel de precisión los datos originales, sin revelar el contenido real de los mismos.
- **MD5:** es un tipo particular de hash que genera claves de 16 bytes de longitud (128 bits). Por la facilidad para calcularla y sus características matemáticas, se utiliza ampliamente para verificar la integridad de archivos.
- **SHA-1:** es un tipo particular de hash que genera claves de 20 bytes de longitud (160 bits). Computacionalmente lleva más tiempo calcular que MD5, pero posee propiedades matemáticas que la hacen una mejor alternativa para usos criptográficos. En el ámbito forense suele usarse en conjunto con MD5 para complementar la validación que provee el otro algoritmo.
- **Tablas Rainbow:** son tablas de fragmentos de hashes pre calculadas que permiten acelerar el cálculo de hashes. Usualmente se utilizan para realizar ataques informáticos y adivinar contraseñas.

- **Filtros bloom:** es otro tipo de estructura de datos que permite calcular hashes en forma acelerada. Un filtro bloom además tiene asociado un componente probabilístico. Su uso es similar al de una Tabla Rainbow.
- **Encriptación:** técnica que permite convertir texto o datos en una representación ininteligible mediante el uso de un código de forma que, posteriormente, se pueda hacer la reconversión a la forma original.
- **TrueCrypt:** software que implementa algoritmos de encriptación, para archivos y dispositivos de almacenamiento, de forma transparente para el usuario.
- **BitLocker:** software incorporado con Windows (a partir de Windows Vista) para realizar la encriptación de dispositivos de almacenamiento.
- **TPM (BitLocker)**: es un criptoprocesador (un procesador especializado para almacenar claves criptográficas) específico para guardar claves de BitLocker.
- **FVEK (BitLocker):** es la clave que permite desencriptar información encriptada con BitLocker.
- **Bootkit:** es un programa que altera el proceso de inicio de una computadora.
- **Metadatos:** son "datos sobre los datos", información asociada a un archivo, que permite interpretar y organizar mejor los datos en una computadora (ej.: establecer fechas de acceso, creación, modificación, etc.).
- **EXIF:** es un protocolo que permite incorporar información de metadatos a distintos formatos de archivo. Es muy utilizado en archivos JPG.
- **ID3:** es un protocolo que permite incorporar información de metadatos a formatos de archivo. Se utiliza ampliamente en archivos de música, por ejemplo MP3.
- **XMP:** es un protocolo que permite incorporar información de metadatos a formatos de archivo. Se utiliza para algunos formatos de archivos de documentos, por ejemplo PDF.
- **Cadenas (de texto):** es una representación de textos en la memoria de la computadora. Una cadena de texto es una secuencia de números que representa texto. Los números hacen referencia a caracteres (letras) en una tabla de caracteres, y distintas tablas ayudan en la representación visual de la información contenida por la cadena. Por lo general, en los países con alfabetos Latinos se utiliza ASCII, y desde hace algunos años se utiliza Unicode, que tiene mejor soporte para alfabetos complejos.

- **ASCII:** un formato de codificación de textos, ampliamente utilizado en países angloparlantes y países con alfabetos latinos.
- **Unicode:** un formato de codificación de textos que permite representar caracteres de cualquier idioma. Tiene distintas implementaciones, las más comunes son UTF- 8 y UTF-16.
- **Expresiones regulares:** una expresión regular es un texto que describe la forma de un texto.
- **Carving / file carving:** se llama con este nombre a una familia de técnicas de recuperación de archivos e información que se basan en la estructura de los datos que interesa recuperar.
- **File signature / firma de archivo:** es una secuencia de caracteres característicos de un archivo o formato de archivo.
- **Header / Footer:** firmas de archivo usualmente asociadas con el encabezado y final de archivo típicos de un formato de archivo.
- **Malware:** software cuyo propósito es perjudicar a un usuario o sistema, en forma directa o indirecta.
- **Virus:** un tipo particular de malware, usualmente los virus están asociados con comportamiento dañino hacia la computadora en la que se ejecutan.
- **Botnet:** un conjunto de computadoras manejadas, directa o indirectamente, por un servidor de comandos. Las botnets usualmente se utilizan para realizar ataques de denegación de servicio masivos.
- **Librería:** es una especie de programa que se carga en la memoria principal de la computadora para proveer funcionalidad común a otros programas.
- **DLL:** del inglés, Dynamic Link Library, es un formato especial de librería utilizado en sistemas operativos Windows.

MÓVILES:

- **Tarjeta SIM:** es una tarjeta que contiene un chip de datos que almacena información relacionada con números de identificación, números de registro, claves, etc. para acceder a un sistema de telefonía celular.
- **JTAG:** es una arquitectura que define una interfaz y protocolo para analizar y verificar el estado interno de chips electrónicos. En la informática forense, provee un medio para acceder a la información de un chip independientemente del resto del sistema informático.

- **Almacenamiento en móviles:** los requerimientos particulares de los dispositivos móviles ocasionan que utilicen hardware muy especializado. En particular, el almacenamiento de información en dispositivos móviles usualmente se realiza con chips de memoria Flash. Además, también es común que un dispositivo móvil tenga 2 o más medios de almacenamiento.
- **Memoria interna (de dispositivo móvil):** es un medio de almacenamiento interno al dispositivo móvil, no removible. Usualmente la memoria interna almacena las aplicaciones y datos de usuario, aunque en dispositivos que no cuentan con memoria externa también almacena los archivos del usuario.
- **Memoria externa (de dispositivo móvil):** es un medio de almacenamiento removible, usualmente una tarjeta micro SD. En la memoria externa suelen encontrarse los archivos del usuario, y algunas ocasiones también datos de aplicación. En teoría es posible, aunque con muy baja probabilidad, encontrar también una partición swap.
- **Memoria Flash:** es una tecnología de almacenamiento que, por sus características, fomenta la fragmentación de los datos, a un nivel inferior que el sistema de archivos.

REDES:

- **Red local:** red de comunicación que proporciona interconexión entre varios dispositivos de comunicación en un área pequeña.
- **Cloud computing:** conocido también como servicios en la nube, informática en la nube, nube de cómputo o nube de conceptos, (del inglés cloud computing), es un paradigma que permite ofrecer servicios de computación a través de Internet. En este tipo de computación todo lo que puede ofrecer un sistema informático se ofrece como servicio de modo que los usuarios puedan acceder a los servicios disponibles “en la nube de Internet, siendo un paradigma en el que la información se almacena de manera permanente en servidores de Internet.
- **Dirección de red:** un número que identifica unívocamente a un dispositivo en una red. Las direcciones de red no pueden repetirse en una red bien configurada. Si dos equipos comparten la misma dirección de red, uno de ellos no podrá comunicarse y estará efectivamente desconectado de la red.
- **Dirección IP:** dirección de 4 bytes (32 bits) que representa a un equipo en una red IP (Internet Protocol). Las direcciones IP no representan unívocamente equipos porque hay mecanismos que permiten conectar

múltiples equipos con una misma dirección IP, sin afectar la conectividad de los mismos.

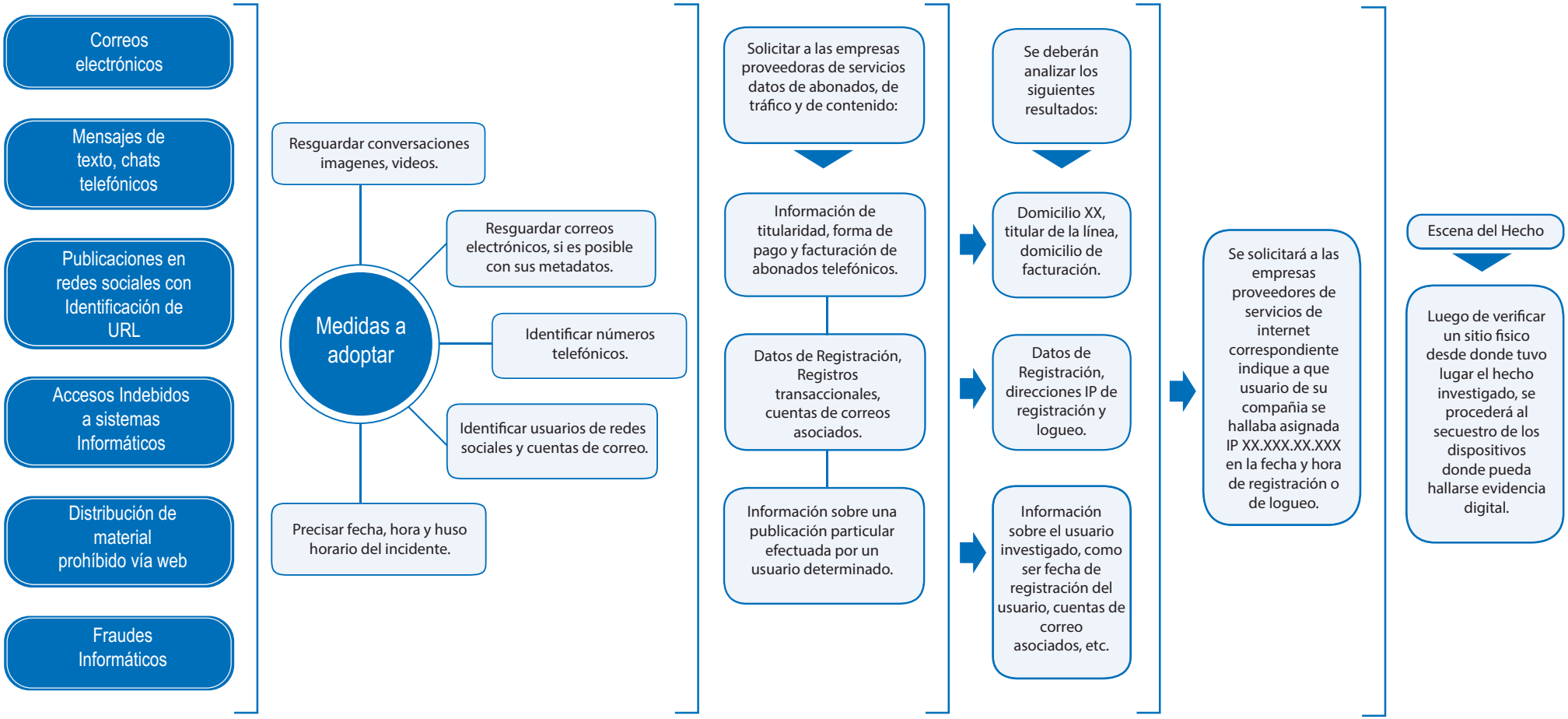
- **Dirección MAC:** dirección de 6 bytes (48 bits) que identifica a un equipo en el medio físico de una red local tipo IEEE 802. Las direcciones MAC son unívocas y, en teoría, no se repiten en todo el mundo, aunque hay métodos para cambiarlas y generar direcciones MAC repetidas.
- **Dump de red / volcado de red:** es una copia del tráfico de una red en un segmento de tiempo, que permite analizar a posteriori las comunicaciones de uno o varios dispositivos.

SISTEMAS OPERATIVOS:

- **Sistema Operativo:** software que controla la ejecución de programas y ofrece servicios tales como la asignación de recursos, la planificación, el control de entrada/salida y la gestión de los datos.
- **Filesystem / Sistema de archivos:** es un conjunto de reglas, estructuras y protocolos que definen cómo se almacena, organiza y distribuye la información en una partición. Además los sistemas de archivos definen metadatos que permiten conocer fechas de acceso, modificación, permisos de usuario y otra información relevante a los archivos que se guardan.
- **FAT (filesystem):** un sistema de archivos simple creado por Microsoft para el sistema operativo DOS, luego extendido y adaptado a entornos más modernos. En la actualidad algunos pen drives vienen formateados con una variante moderna, llamada exFAT.
- **File Allocation Table (tabla de archivos):** es una tabla de asignación de espacio de la partición a los archivos. Indica que un determinado sector de la partición (denominado “cluster”) pertenece a un archivo. También establece la secuencia ordenada de clusters que permite recuperar los datos de un archivo.
- **NTFS:** es un sistema de archivos creado por Microsoft para los sistemas operativos Windows basados en Windows NT. Presenta una serie de ventajas y mejoras con respecto a FAT, y actualmente tiene un uso extendido.
- **MFT:** es la tabla de archivos de NTFS, pero sustancialmente distinta a la File Allocation Table de FAT. Debido a los cambios y mejoras introducidos, la MFT es una tabla mucho más importante y una mayor fuente de información que la FAT.

- **Ext:** es una familia de sistemas de archivos asociados con el sistema operativo GNU/Linux. Las versiones más comunes son ext2, ex3 y ext4. Operativamente trabajan con el concepto informático de i-nodos, lo que ocasiona que tengan, en promedio, mayor fragmentación de los archivos que NTFS o FAT (pero sin la consecuencia negativa al rendimiento).
- **Fragmentación:** es una consecuencia de algunos sistemas de archivos en la cual un archivo, en lugar de almacenarse en sectores contiguos de la partición, se almacena separado en bloques. En las cuestiones de informática forense, la fragmentación es importante porque dificulta la recuperación física de archivos por medio de técnicas como el file carving.
- **Driver:** es un programa que se ocupa de comunicar comandos específicos a una parte del hardware de la computadora (por ejemplo la impresora) para que realice acciones específicas.
- **Proceso:** programa en ejecución, controlado y planificado por el Sistema Operativo.
- **Memoria virtual:** es un espacio de almacenamiento que el sistema operativo considera como memoria principal, que se encuentra limitado por la capacidad de almacenamiento de la memoria secundaria (usualmente el disco) del equipo.
- **Área de paginado:** es la parte de la memoria secundaria que se destina a funcionar como memoria virtual en los esquemas de paginación. Es importante desde el punto de vista forense porque ofrece una parte de la memoria principal para ser analizada como parte de la memoria secundaria.
- **Pagefile / archivo de página:** es un archivo que contiene el área de paginado de los sistemas operativos Windows.
- **Partición swap:** es una partición que se utiliza como área de paginado. Los sistemas operativos UNIX, GNU/Linux y otros derivados de UNIX utilizan una partición swap en lugar de un archivo de página.
- **Registro de Windows:** es un conjunto de archivos que concentran configuraciones de bajo nivel de un sistema operativo Windows. Desde el punto de vista de la informática forense, es importante porque se almacena mucha información relacionada con el uso del sistema y los usuarios.
- **Archivos de Configuración Linux:** en los sistemas operativos UNIX y GNU/Linux, la configuración usualmente se almacena en archivos. Hay distintos sistemas de organización que dependen de la distribución y versión del sistema operativo.

INVESTIGACIONES EN ENTORNOS DIGITALES



PLAN DE TRABAJO PREVIO: Metodología de trabajo del personal y de la relación de éste con la evidencia digital. Preparación de las herramientas necesarias para proceder al tratamiento y secuestro de la evidencia de interés. Contar con protocolos de acuerdo al tipo de ilícito que enfrentamos: fraude, pornografía infantil, extorsión, etc.

ESCENA DEL HECHO

ASEGURAMIENTO DE LA ESCENA

Consiste en proteger y delimitar la escena para evitar la modificación o destrucción de las evidencias digitales

El personal que accede a la escena debe contar con experiencia previa o estar capacitado en el manejo de evidencia digital. Cualquier actividad llevada a cabo fuera de los protocolos establecidos podría alterar la evidencia. Eso, permitirá que adopten mejores decisiones.

RECONOCIMIENTO E IDENTIFICACIÓN DE EVIDENCIA DIGITAL

¿Dónde? Discos Rígidos en computadoras, palms/PDA, teléfonos celulares, cámaras digitales, faxes, electrodomésticos con acceso a internet. También contamos con medios de almacenamiento propiamente dichos: diskettes, disco rígido externo, Cd/Dvd, Pen Drive, Memory Stick, Cintas magnéticas, etc.

Una vez individualizada la evidencia:

I. No se la deberá manipular.
II. Se deberá dejar constancia del lugar del hallazgo y de ser posible a quien pertenece.
III. Se deberá verificar por procedimientos adecuados si esta encendido o apagado el dispositivo.
IV. Si esta encendido deberá ser apagado por métodos seguros.
V. Se deberá individualizar el dispositivo con mayor precisión posible.
VI. Se procederá a su resguardo.

¿Qué tipo de evidencia digital podemos encontrar?

I. Memoria de Almacenamiento
II. Memoria RAM
III. Tráfico de Red

ADQUISICIÓN Y CAPTURA DE LA EVIDENCIA DIGITAL

De datos volátiles: Se trata de aquellos existentes en dispositivos encendidos que podrían perderse con su apagado.

De medios de almacenamiento persistentes.

También se pueden utilizar otras técnicas como el Triage: permite la búsqueda y adquisición de evidencia digital, empleando criterios superficiales.
Una vez individualizado el material de interés se podrá hacer una copia forense.

Para minimizar la interacción con el dispositivo a recolectar se recomienda –siempre que el tiempo y recursos lo permitan- efectuar una copia o imagen forense ya sea en la escena del hecho o en el laboratorio.

Imagen o copia forense: es una copia bit a bit del contenido digital almacenado en el dispositivo, que es autenticada con un código HASH, que asegura la integridad de la evidencia recolectada.

Se realiza mediante un dispositivo autónomo denominado duplicador forense.

De ser posible se deberá registrar esta etapa con medios fotográficos, de video y escrito, para comprender cual era la ubicación física de cada evidencia recolectada

PRESERVACIÓN DE LA EVIDENCIA DIGITAL

Debe ser tenida en cuenta desde el inicio y consiste en una secuencia de recaudos que evitarán que la evidencia: Se pierda, destruya o altere.

Comienza desde el hallazgo y se aplica a la identificación, obtención, traslado, almacenamiento, entrega, recepción, exhibición y análisis, preservándose así su valor probatorio.

Participan de ella todos los funcionarios y/o empleados policiales y judiciales que intervengan en las diferentes etapas.

ANÁLISIS EN EL LABORATORIO FORENSE

Especialistas en evidencia digital examinarán la evidencia y elaborarán un informe. Acreditarán su experiencia con título habilitante y las certificaciones correspodientes relativas a las herramientas forenses utilizadas.

Estructurarán el trabajo en etapas:

I. Actos iniciales y formalidades
II. Preparación del análisis
III. Análisis
IV. Interpretación
V. Elaboración del informe

Trabajarán sobre lo requerido por el encargado de la investigación, siguiendo una metodología forense y empleando herramientas adecuadas certificadas para cada caso.

Los resultados obtenidos se expondrán en un lenguaje claro y en un formato adecuado conforme los requerimientos del investigador.

PRESENTACIÓN DE PRUEBAS ANTE EL TRIBUNAL

El especialistas encargado de presentar el dictamen ante el tribunal deberá estar en condiciones de acreditar su capacitación y experiencia en el área, la objetividad de su actuación y el cumplimiento de las exigencias legales durante su desempeño.

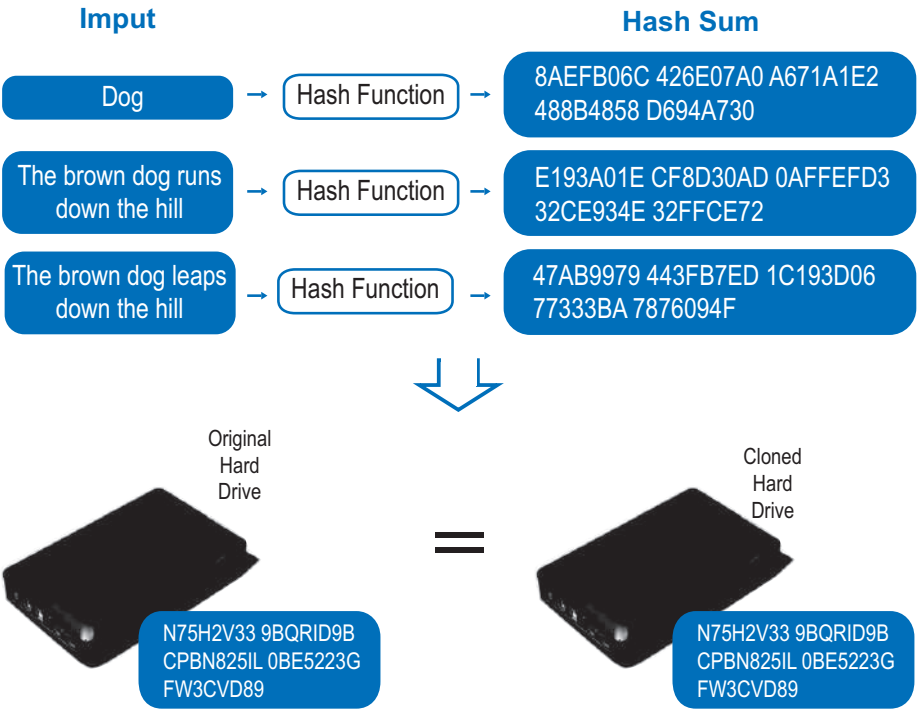
Deberá precurar que la explicación de las conclusiones y los métodos elegidos para exponerla lo sean en un idioma claro, que pueda ser interpretado por los mienbros del tribinal.

Anexos I: Función Hash

Para asegurar la integridad de la copia forence, se la autentica mediante un función HASH o digesto matemático (ANEXO III). Las imágenes forenses pueden realizarse mediante una computadora, un programa específico y un bloqueador de escritura, o bien, utilizando un dispositivo autónomo denominado duplicador forence.

EL HASH se refiere a una función o método para generar claves que representen de manera casi unívoca a un documento, registro, archivo etc. Resumir un dato a travéz de la probabilidad, Utilizando una función hash o algoritmo hash. El HASH permite darle mayor seguridad de que la evidencia digital obtenida no fue manipulada ni alterada, ya que el HASH generado es inviolable.

= 79054025 255fb1a2 6e4bc422 aef54eb4



Es un dispositivo autónomo que lleva implícito el bloqueo de escritura y, al ser un dispositivo de hardware, el software se encuentra optimizado, mejorando drásticamente la velocidad del proceso, Incluso al producir múltiples copias.

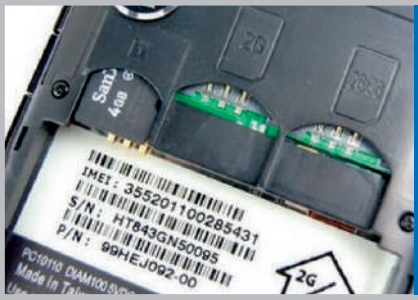
Cuando no se encuentra con un duplicador forense, para evitar la contaminación del disco duro, normalmente se utilizan bloqueadores de escritura de hardware, los cuales evitan el contacto de lectura con el disco, lo que provocaría una alteración no deseada en los medios.

Al momento de secuestrar evidencia digital, será necesario mantener la cadena de custodia del material secuestrado. No se podrá asegurar la integridad de la evidencia digital si el material informático tiene roto los precintos, fajas o embalajes colocados al momento de ser entregado.

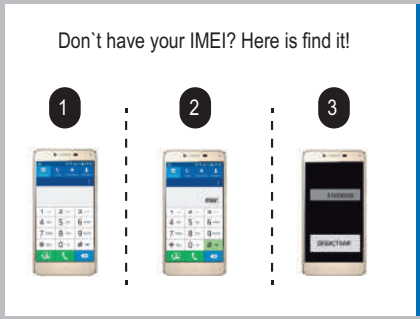
Se deberá fotografiar la totalidad de los elementos secuestrados una vez embalados en sus respectivas bolsas cerradas con los precintos, fajas o embalajes de seguridad, en forma individual y panorámica de la totalidad.

Anexos V: Identificación de IMEI

El IMEI (del inglés Internacional Mobile Station Equipment Identity, identidad de equipo móvil) es un código USSD pregrabado en los teléfonos móviles GSM. En este código identifica al aparato de forma exclusiva a nivel mundial, y es transmitido por el aparato a la red al conectarse a esta. En base a las características propias del IMEI, habitualmente para identificar al dispositivo móvil secuestrado.



Habitualmente el número de IMEI de un dispositivo móvil es verificado al observar en las etiquetas de fábrica del dispositivo que se pueden hallar al quitar la tapa de la batería del aparato. Este método de verificación no altera el modo alguno de la evidencia digital que podría encontrarse en el dispositivo.



También se puede verificar EL IMEI de un equipo accidentado al teclado Touch o analógico donde se deberían introducir las teclas #06# y a continuación el teléfono indica que IMEI tiene asignado. Este método requiere del acceso al teléfono y eventualmente puede modificar o alterar la evidencia digital del dispositivo.

Español	Inglés	Contenido
De:	FROM:	Abelardo Lópe <abelardolopez98@prodigy.net.mx>
ENVIADO:	SENT:	Miercoles, 11 de febrero, 2004 7:16 pm
PARA:	TO:	<kylegrimes@msn.com>
COPIA:	CC:	Gabriel Grimes <grimesgk@hotmail.com>
TITULO:	SUBJECT:	Hace mucho tiempo

→ Encabezado simple

MIME-Versión: 1.0
Received: from {216.136.226.197} by hotmail.com (3.2) with ESMTP id MHotMailBD737B61008E2C506160; Thu, 20Sep 2001 11:07:30-0700
Received: from {12.26.159.122} by web20808.mail.yahoo.com via HTTP; Thu, 20Sep 2001 11:07:29PDT
From: Polaris9999200@yahoo.com Thu,20 Sep 2001 11:07:58-0700
Message-id:<20010920180729.36281.gmail@web200808.mail.yahoo.com>

→ Encabezado completo o avanzado

POLICIA NACIONAL DEL PERÚ

XI - DIRTEPOL AREQUIPA

FORMATO A - 7
CADENA DE CUSTODIA

Código Único de carpeta Fiscal	
Distrito Judicial	
Prioridad	

FECHA D/M/A	HORA	NOMBRE COMPLETO DEL 1RO QUE EMBALA Y TRANSPORTA ELEMENTOS MATERIALES, EVIDENCIAS Y BIENES INCAUTADOS	HORA	CARGO/INSTITUCIONAL	FIRMA	OBSERVACIONES

REGISTRO DE CONTINUIDAD DE CUSTODAIA DE ELEMENTOS MATERIALES, EVIDENCIAS Y BIENES INCAUTADOS

FECHA D/M/A	HORA	NOMBRE COMPLETO DE QUIEN RECIBE BIENES INCAUTADOS	DNI / CIP	CARGO O INSTITUCIÓN	REGISTRO O CÓDIGO DE RECEPCIÓN	PROPÓSITO DEL TRASLADO	AUTORIDAD QUE AUTORIZA EL TRASLADO O DESTINO FINAL	FIRMA	OBSERVACIONES

IMPORTANTE ESTE FORMATO DE CADENA DE CUSTODIA DEBE PERMANECER CON LOS ELEMENTOS MATERIALELS. EVIDENCIAS Y BIENES INCAUTADOS

RECONOCIMIENTO Y AGRADECIMIENTO

El presente manual fue elaborado con la participación de miembros del Ministerio Público y la Policía Nacional del Perú. Ello en la necesidad de contar con un instrumento que respondiera eficientemente a las expectativas de fiscales y policías peruanos para el tratamiento de la Evidencia Digital en nuestro país, considerando las condiciones y realidades de nuestro medio.

Por tal razón mediante:

- Resolución de la Fiscalía de la Nación Nº 2500 – 2017 – MP – FN se designó a los señores **IVAN VLADIMIR MELGAR CACERES**, Fiscal Adjunto Superior de la Primera Fiscalía Superior Nacional Especializada en Delitos de Corrupción de Funcionarios, **SONIA HILDA ZEVALLOS MATEO**, Fiscal Adjunto Provincial de la Primera Fiscalía Supraprovincial Corporativa Especializada en Delitos de Lavado de Activos y Pérdida de Dominio, como representantes del Ministerio Público, para que colaboren con ABA ROLI en la elaboración del Manual de Evidencia Digital; y
- Oficio Nº 3357-20º17-DIRINCRI PNP/DIVINDAT/Sec. se designó al Capitán PNP **WILBER MEDINA JIMENEZ** y al Suboficial Técnico de Primera **WUILMAN ZABARBURU VARGAS** para realizar las coordinaciones necesarias con ABA ROLI en la elaboración del Manual de Evidencia Digital.

En tal sentido queremos expresar nuestro más profundo agradecimiento y reconocimiento a los funcionarios designados por su interés, entusiasmo, dedicación y compromiso en el desarrollo del presente Manual.

Ellos trabajaron en coordinación directa con el consultor Alan Martín Nessi, autor del presente material.

Proyecto de Apoyo al Sector Justicia
American Bar Association Rule of Law Initiative
ABA ROLI - Perú

Alan Martín Nessi

Abogado por la Universidad de Buenos Aires. Con estudios de posgrado en Derecho Penal por la Universidad de Palermo (Argentina). Ha sido Director del Cuerpo de Investigaciones Judiciales – Policiales Judiciales del Ministerio Público Fiscal de la Ciudad Autónoma de Buenos Aires. Consultor del Programa de Reforma Modelo para las Administraciones de Justicia Provinciales, contratado por el Banco Interamericano de Desarrollo. Coautor del Plan Nacional de Reforma Judicial y Coordinador del Observatorio Metropolitano de Seguridad Pública. Asesor Técnico Jurídico del Ministro de Seguridad y Justicia del Gobierno de la Ciudad Autónoma de Buenos Aires.

Av. Larco 101, Oficina 802,
Miraflores, Lima - Perú
T: +51 (01) 447-6867
F: +51 (01) 447-6802
E: correocentral@abaroliperu.com
W: abaroliperu.com