# RECOJO Y ANÁLISIS DE EVIDENCIA DIGITAL

## CARTILLA TEMÁTICA 393

### RECOLECCIÓN

En el contexto de la investigación, la PNP asume la responsabilidad de preservar la escena del crimen, especialmente al momento del recojo de la evidencia.

| | |
|---|---|
| ASEGURAMIENTO DE LA ESCENA DEL CRIMEN | Evaluar los riesgos y adoptar las medidas de seguridad; aislar y proteger la escena del crimen; y, conservar en forma original el espacio físico, evitando cualquier alteración, manipulación, contaminación, destrucción, pérdida o sustracción de dispositivos de almacenamiento digital. |
| IDENTIFICACIÓN DE DISPOSITIVOS DE ALMACENAMIENTO | En la escena del crimen, se puede encontrar evidencias digitales contenidos en dispositivos informáticos (computadora, disco duro, USB, entre otros) y dispositivos móviles (teléfono celular, tarjeta SIM, GPS, DRON, Smartwatch, entre otros). |
| HALLAZGO, INCAUTACIÓN O RECEPCIÓN DE DISPOSITIVOS DE ALMACENAMIENTO | Una vez asegurada la escena y haber hallado, incautado y recibido los dispositivos de almacenamiento, se formulan las actas. Si son transportables serán objeto de recojo y, de no serlo, se comunicará al personal policial especializado para su adquisición. Se perenniza la escena del crimen y se embalan y lacran los dispositivos individualmente. |

### ANÁLISIS FORENSE

Permite obtener elementos de convicción relevantes para la investigación; los cuales son descritos y detallados en el informe pericial.

| | |
|---|---|
| IDENTIFICACIÓN FÍSICA E IDENTIFICACIÓN LÓGICA | En la identificación física, se individualiza los dispositivos relacionados al hecho investigado; en la lógica, se realiza la búsqueda y reconocimiento de evidencia en los dispositivos encendidos relacionados al hecho investigado, dando prioridad a la recopilación de evidencias volátiles. |
| ADQUISICIÓN Y PRESERVACIÓN | Se requiere el uso de herramientas forenses que permitan la recolección de datos volátiles y no volátiles, a través del volcado de memoria y de la creación de una imagen forense (copia bit a bit), debiendo generarse los códigos hash respectivos para garantizar su integridad. |
| ANÁLISIS | Se realiza el análisis sobre la imagen forense de los dispositivos y el volcado de la memoria. Se inicia con la búsqueda, recuperación y/o recopilación de los archivos digitales generados, almacenados y transmitidos, relacionados a los hechos materia de investigación. |
| DOCUMENTACIÓN | Redacción del informe pericial que debe contener toda la información y la evidencia obtenida en la fase de análisis forense, la conclusión debe ser redactada de forma clara, concisa y utilizando un lenguaje comprensible para el solicitante (operadores de justicia). |

**Los lineamientos para desarrollarse en el presente manual no descartan el uso de procedimientos alternativos de acuerdo con el avance tecnológico y/o buenas prácticas internacionales de la comunidad científica forense.**

**BASE LEGAL:** R.M. N° 848-2019-IN, MANUAL DE RECOJO DE EVIDENCIA DIGITAL.
R.C.G. N° 79-2024-CG PNP/EMG, MANUAL DE ANÁLISIS FORENSE DE EVIDENCIA DIGITAL.

# RECOJO Y ANÁLISIS DE EVIDENCIA DIGITAL


## RECOJO Y ANÁLISIS DE EVIDENCIA DIGITAL

1. **DECRETO SUPREMO N° 026-2017-IN, REGLAMENTO DEL DECRETO LEGISLATIVO N° 1267, LEY DE LA POLICÍA NACIONAL DEL PERÚ**

**Artículo 29.- División de Laboratorio Criminalístico**

La División de Laboratorio Criminalístico es la unidad orgánica de carácter técnico y especializado; responsable de analizar los indicios y evidencias hallados en la escena del crimen o los producidos por la comisión de un hecho criminal, mediante procedimientos técnicos científicos de sus distintos campos funcionales forenses; en apoyo técnico científico a los órganos y unidades orgánicas de la Institución Policial, Ministerio Publico, Poder Judicial y autoridades competentes en la investigación de hechos penales.

(…)

La División de Laboratorio Criminalístico de la Policía Nacional del Perú tiene las funciones siguientes:

(…)

10) Realizar exámenes periciales en audio y video forense, informática forense, telefonía forense y sobre cualquier otro medio, soporte analógico o digital; velando por la integridad de la evidencia digital;

(…)

2. **RM Nº 848-2019-IN, MANUAL DE RECOJO DE EVIDENCIA DIGITAL**

**VI. RECOLECCIóN DE LA EVIDENCIA DIGITAL**

**A. ASEGURAMIENTO FÍSICO DE LA ESCENA DEL CRIMEN**

1. Evaluar los riesgos y adoptar las medidas de seguridad.
2. Aislar y proteger la escena del crimen.
3. Conservar en forma original el espacio físico en el que aconteció el hecho criminal, con la finalidad de evitar cualquier alteración, manipulación, contaminación, destrucción, pérdida o sustracción de dispositivos de almacenamiento digital.

**B. IDENTIFICACIÓN DE DISPOSITIVOS DE ALMACENAMIENTO**

En la escena del crimen, se podrá encontrar evidencias digitales contenidos en dispositivos tecnológicos, tales como:

1. **Dispositivos informáticos**
   a. Computadora personal.
   b. Computadora portátil (laptop, notebook).
   c. Servidor.
   d. Disco duro.
   e. Disco duro externo.
   f. Pen drive (USB).
   g. Memoria externa (SD, Micro SD).
   h. Lector de banda magnética (Skimmer).
   i. Tarjeta electrónica
   j. Sistema de videovigilancia (DVR, NVR, NDVR).
   k. Equipo de comunicación (router, switch).
   l. Impresora multifuncional.
   m. Dispositivos multimedia.
   n. Cámara espía.
   o. Caja de liberación y desbloqueo.


p. Cámaras filmadoras y fotográficas.
q. Otros dispositivos informáticos.

2. **Dispositivos móviles**
   a. Equipo de terminal móvil (Teléfono celular).
   b. Tarjeta SIM (Chip).
   c. Módem USB (internet móvil).
   d. Sistema de posicionamiento global (GPS).
   e. Palm.
   f. Tableta (tablets).
   g. Vehículo aéreo no tripulado (DRON).
   h. Reloj inteligente (smartwatch).
   i. Terminal de punto de venta (POS).
   j. Otros dispositivos móviles.

**C. HALLAZGO, INCAUTACIÓN O RECEPCIÓN DE DISPOSITIVOS DE ALMACENAMIENTO DIGITAL**

Una vez asegurada la escena del crimen y después de haber hallado, incautado o recibido los dispositivos de almacenamiento, se formularán las actas correspondientes, teniendo en cuenta lo siguiente:

- Si los dispositivos son transportables o no (por su volumen, limitaciones legales, funcionales, entre otros).
- Los dispositivos transportables serán objeto de recojo.
- Para los dispositivos no transportables, se deberá comunicar al personal policial especializado para la adquisición de la evidencia digital.
- Perennizar la escena del crimen mediante la grabación de video y la toma de vistas fotográficas (panorámicas y de detalle) antes, durante y después de las actividades realizadas.
- Embalar y lacrar los dispositivos individualmente.

(…)

**VII. REQUISITOS PARA EL ANÁLISIS INFORMÁTICO FORENSE**

**A.** Oficio precisando el objetivo del análisis forense, de acuerdo al tipo y modalidad del hecho investigado.

**B.** Disposición Fiscal que autoriza la participación de las fiscalías competentes o adscritas a las unidades policiales.

**C.** Documentos según el caso:
1. Acta de hallazgo y recojo.
2. Acta de incautación.
3. Acta de entrega y recepción.

**D.** Acta de lacrado.

**E.** Acta de cadena de custodia y continuidad de cadena de custodia.

**F.** Autorización del usuario o resolución judicial (medida limitativa de derecho, levantamiento del secreto de las comunicaciones y/o documentos privados), que disponga el análisis informático de los dispositivos de almacenamiento digital.

**VIII. PRESERVACIóN DE LA CADENA DE CUSTODIA**

**A.** La cadena de custodia garantiza la autenticidad y la intangibilidad de los elementos materiales y evidencias físicas


recogidas en la escena del crimen.

**B.** Se inicia con el aseguramiento y/o recojo de los elementos materiales encontrados en la escena del crimen.

**C.** Se deberá adoptar las medidas de seguridad para mantener intangible e inalterable la cadena de custodia hasta su disposición o resolución final en el proceso de modificación.

**D.** Los elementos materiales probatorios y la evidencia física son auténticos y permanencen intangibles, mientras hayan sido asegurados, fijados, recogidos y embalados técnicamente, y sometidos a la regla de cadena de custodia

**3. <u>RCG Nº 79-2024-CG PNP/EMG, MANUAL DE ANÁLISIS DE EVIDENCIA DIGITAL</u>**

**II. CONTENIDO ESPECÍFICO**

**2.1. METODOLOGÍA DEL ANÁLISIS FORENSE DIGITAL**

**2.1.1. IDENTIFICACIóN**

En esta fase se realiza la identificación física y/o lógica de la evidencia, considerando que:

**2.1.1.1.** En la identificación física, se individualiza los dispositivos de almacenamiento digital relacionado al hecho investigado.

**2.1.1.2.** Para la identificación lógica, se debe realizar la búsqueda y reconocimiento de evidencia en los dispositivos encendidos relacionados al hecho investigado, dando prioridad a la recopilación de evidencias volátiles considerando el período de tiempo en que los datos son accesibles en el sistema.

**2.1.1.3.** De acuerdo a la naturaleza de los hechos materia de investigación, se considera la volatilidad de los datos en dispositivos encendidos, por lo que se deben adquirir en el orden de mayor a menor volatilidad.

Por lo tanto, se deben identificar evidencias digitales de acuerdo al orden de volatilidad. Según la Request For Comments - RFC 3227, “Guía para Recolectar y Archivar Evidencia” (Brezinski & Killalea, 2002).

**Orden de volatilidad - RFC 3227 (Brezinski & Killalea, 2002)**

Identificadas las evidencias de mayor y menor volatilidad que pueda contener el dispositivo de almacenamiento digital, que debe establecer cuáles son útiles y necesarias para la investigación, las mismas que deben ser recolectadas para su análisis.


**2.1.1.4.** El personal especializado puede realizar un análisis rápido (triage) sobre un dispositivo electrónico, y determina si contiene evidencia relacionada a los hechos materia de investigación.

**2.1.2. ADQUISICIÓN Y PRESERVACIÓN**

Esta fase requiere el uso de herramientas forenses que permitan la recolección de datos volátiles y no volátiles, a través del volcado de memoria y de la creación de una imagen forense (copia bit a bit), debiendo generarse los códigos hash respectivos para garantizar su integridad.

Es necesario que el dispositivo se encuentre operativo para realizar este procedimiento, de lo contrario se formulará la documentación respectiva.

**2.1.3. ANÁLISIS**

En esta fase, se realiza el análisis sobre la imagen forense de los dispositivos de almacenamiento digital y sobre el volcado de la memoria. Se inicia con la búsqueda, recuperación y/o recopilación de los archivos digitales generados, almacenados y transmitidos, como: logs, archivos de ofimática, fotogramas, videogramas, audios, entre otros; relacionados a los hechos materia de investigación.

Es importante señalar que no existe un procedimiento estandarizado de análisis para cada dispositivo de almacenamiento digital, por lo tanto, deben ser examinados teniendo en cuenta las diversas casuísticas y experiencias adquiridas.

En consecuencia, se pueden desarrollar sub-fases según cada caso:

**2.1.3.1.** Preparar un entorno de trabajo de acuerdo a las necesidades técnicas del requerimiento, considerándose si el análisis de la evidencia digital se debe realizar en caliente o en frio.

**2.1.3.2.** Realizar un listado de archivos comprometidos con el caso que deben ser empleados como evidencia para ser presentados en el informe respectivo.

**2.1.3.3.** Crear una línea tiempo que describa las fechas de creación, modificación y accesos de los archivos, así como aplicaciones instaladas o portables que permiten crear puntos claves en el tiempo.

**2.1.4. DOCUMENTACIÓN**

Es la fase final del análisis forense digital, consiste en la redacción del informe pericial


que debe contener toda la información y la evidencia obtenida en la fase de análisis forense, la conclusión debe ser redactada de forma clara, concisa y utilizando un lenguaje comprensible para el solicitante (operadores de justicia).

Teniendo en cuenta lo señalado en el párrafo anterior, la estructura del informe pericial debe tener como base la estructura del contenido del informe pericial oficial que se indica taxativamente en el Código Procesal Penal (Artículo 178°), conforme se describe a continuación:

**2.1.4.1.** Nombres y apellidos, domicilio, documento nacional de identidad del perito, así como el número de su registro profesional en caso de colegiación obligatoria.

**2.1.4.2.** La descripción de la situación o estado de hechos sea persona o cosa, sobre los que se hizo el peritaje.

**2.1.4.3.** La exposición detallada de lo que se ha comprobado en relación al encargo.

**2.1.4.4.** La motivación o fundamentación del examen técnico.

**2.1.4.5.** La indicación de los criterios científicos o técnicos, médicos y reglas de los que se sirvieron para hacer el examen.

**2.1.4.6.** Las conclusions.

**2.1.4.7.** La fecha, sello y firma.

**3.1. APLICACIÓN DE LA METODOLOGÍA**

Los lineamientos para desarrollarse en el presente manual no descartan el uso de procedimientos alternativos de acuerdo con el avance tecnológico y/o buenas prácticas internacionales de la comunidad científica forense, tales como el uso de softwares libres, análisis forense en la nube, la técnica Chip-off para recuperación de datos del chip de memoria de teléfonos celulares, entre otros.

Por lo tanto, al conocimiento del hecho criminal, el personal policial debe tomar las medidas necesarias para asegurar la escena del crimen, a fin de evitar alteración, manipulación, contaminación, destrucción, pérdida o sustracción de dispositivos de almacenamiento digital para su posterior análisis por la unidad especializada. En esta fase se debe tomar en consideración lo descrito en “El Manual para el Recojo de la Evidencia Digital".

La autoridad solicitante debe considerar que antes de remitir el requerimiento pericial, debe de evaluar si el examen puede ser atendido por el laboratorio forense digital.

(...)