PERÚ | Ministerio del Interior

EL PERÚ PRIMERO

MANUAL PARA EL RECOJO DE LA EVIDENCIA DIGITAL

PERÚ | Ministerio del Interior

El Perú Primero

MANUAL
PARA EL RECOJO DE LA EVIDENCIA DIGITAL

PERÚ | Ministerio del Interior

MANUAL
PARA EL
RECOJO DE LA
EVIDENCIA DIGITAL

Ministerio del Interior
Plaza 30 de Agosto s/n Urb. Córpac. San Isidro, Lima.
Central Telefónica: 01 418-4030
www.mininter.gob.pe

Ministro del Interior
Jorge Eduardo Montoya Pérez

Viceministro de Orden Interno
Esteban Saavedra Mendoza

Director General Contra el Crimen Organizado
General PNP (r) Luis Ricardo Chávez Gil

Directora Contra Delitos de Crimen Organizado
Keila Miroslava Garrido Gonzales

Equipo Técnico:
Mayor PNP Juan Antonio Pozo Castillo

División de Investigación de Delitos de Alta Tecnología – PNP
Comandante PNP Oscar Lindolfo Liñan Gareca
Capitán SPNP Guido Jhonathan Ramos Hernández
ST1 PNP Wuilman Zabarburu Vargas

Dirección de Tecnología de Información y Comunicaciones de la PNP
Capitán PNP Wilber Medina Jimenez

Dirección de Criminalística de la PNP
Capitán SPNP Shirley Stana Poma Gonzales

Fotos:
Ministerio del Interior
Dirección de Comunicación e Imágen Institucional de la PNP
Fotos de Stock: Freepik

Resoluciones Supremas N° 066-2018-IN, N° 093-2018-IN y
su Fe de Erratas de fecha 14/11/2018
Decreto Supremo N° 023-2019-IN
RM N° 848-2019-IN

Julio 2020. Lima, Perú.
Primera Edición, MINISTERIO DEL INTERIOR 2020

Diseño e Impresión:
Tarea Asociación Gráfica Educativa
Pasaje María Auxiliadora 156-Breña
Julio 2020

MANUAL PARA EL RECOJO DE LA **EVIDENCIA DIGITAL**

Resolución Ministerial N° 848-2019-IN

VISTOS los informes N° 000024-2018/IN/DGCO/DCO y N° 000001-2019/IN/DGCO/DCO de la Dirección de Delitos de Crimen Organizado de la Dirección General Contra el Crimen Organizado; el Memorando N° 00265-2019/in/DGCO de la Dirección General Contra el Crimen Organizado, y el Informe N° 001229-2019/IN/OGAJ de la Oficina General de Asesoría Jurídica y

CONSIDERANDO:

Que, de acuerdo al artículo 4 del Decreto Legislativo N° 1266, Ley de Organización y Funciones del Ministerio del Interior, el Ministerio del Interior ejerce competencia exclusiva a nivel nacional en materia de orden interno y orden público; así como competencia compartida en materia de seguridad ciudadana, de acuerdo a Ley, es el ente rector del Sistema Nacional de Seguridad Ciudadana;

Que, conforme al artículo 4 del citado Decreto Legislativo N° 1266, el Ministerio del Interior tiene, entre otras funciones específicas: formular, dirigir, coordinar y evaluar las políticas de seguridad ciudadana en atención a la prevención del delito, seguridad privada, control y fiscalización; así como aprobar la normativa general y ejercer la potestad reglamentaria en las materias de su competencia;

Que, el Reglamento de Organización y Funciones (ROF) del Ministerio del Interior, aprobado por Decreto Supremo N° 004-2017-IN, establece la estructura orgánica, funciones generales y específicas de los órganos del Ministerio del Interior; asimismo, conforme a lo dispuesto en el artículo 78 del citado ROF, la Dirección General Contra el Crimen Organizado es el órgano encargado de proponer, promover, formular, conducir y supervisar, en el ámbito de su competencia, las políticas sectoriales en materia de lucha contra las drogas, erradicación de los cultivos ilegales y destrucción de drogas ilegales decomisadas, así como de promover y supervisar el cumplimiento de las estrategias para la lucha contra el crimen organizado y el terrorismo;

Que, de acuerdo a lo señalado por la Dirección Contra Delitos de Crimen Organizado de la Dirección General Contra el Crimen Organizado en los documentos del visto, el Manual de Recojo de la Evidencia Digital será una herramienta que servirá como guía de actuación de procedimientos para los miembros de la Policía Nacional del Perú, con la finalidad de recabar y preservar en forma técnica y profesional el recojo de dispositivos de almacenamiento de datos y/o registros en la escena del crimen que estén relacionados con la comisión de un hecho delictivo, evitando su contaminación, supresión y/o alteración, por lo cual es necesaria su aprobación;

Con la visación del Viceministerio de Orden Interno, de la Dirección General Contra el Crimen Organizado, de la Comandancia General de la Policía Nacional del Perú y de la Oficina General de Asesoría Jurídica;

De conformidad con el Decreto Legislativo N° 1266, Ley de Organización y Funciones del Ministerio del Interior y modificatorias; el Reglamento de Organización y Funciones del Ministerio del Interior, aprobado por Decreto Supremo N° 004-2017-IN.

SE RESUELVE:

Artículo 1.- Aprobar el Manual para el Recojo de la Evidencia Digital, que como Anexo forma parte integrante de la presente Resolución.

Artículo 2.- Disponer la publicación de la presente Resolución y su Anexo en el Portal Institucional y de Transparencia del Ministerio del Interior (www.gob.pe/mininter).

Regístrese y comuníquese.

Ministro del Interior

ÍNDICE

PRÓLOGO

El Ministerio del Interior tiene como función garantizar el orden interno, el orden público y la seguridad ciudadana, mediante la aplicación de políticas públicas orientadas a contener todas las manifestaciones del crimen, empleando herramientas legales, técnicas y tecnológicas, que contribuyan a fortalecer la labor de la Policía Nacional del Perú.

Así, el Manual para el Recojo de la Evidencia Digital es el primer documento institucional que regula los procedimientos en la compilación de evidencias digitales y la inviolabilidad de la cadena de custodia, para garantizar la preservación y validez de los dispositivos digitales como medios probatorios, hasta su traslado hacia la unidad especializada de la Policía Nacional para el análisis informático forense.

Esta herramienta permitirá que la Policía Nacional tenga un moderno procedimiento técnico científico para la obtención de prueba delictiva proveniente de las Tecnologías de la Información y el Conocimiento (TIC). Con ello combatiremos, también, el llamado cibercrimen, que viene aumentado en perjuicio nuestra sociedad.

Con su difusión en todas las unidades de la Policía Nacional, se afianzará el conocimiento que adquieran los efectivos policiales en las escuelas o como resultado de la experiencia que acumulen en el cumplimiento cotidiano de sus funciones. También será material pedagógico básico en actividades de capacitación y especialización policial, como un libro de consulta en la ejecución de pesquisas, en el contexto del Código Procesal Penal vigente.

De este modo, el Manual para el Recojo de la Evidencia Digital fortalece el conjunto de medidas que el sector Interior viene emitiendo a fin de reforzar la labor policial, unificando criterios y fortaleciendo su capacidad operativa para hacer frente a las organizaciones criminales y a la delincuencia común.

Expreso el reconocimiento del sector Interior al equipo técnico de la Dirección General contra el Crimen Organizado (DGCO) del Ministerio del Interior y al personal de la División de Investigación de Delitos de Alta Tecnología (Divindat) de la Dirección de Investigación Criminal (Dirincri) de la Policía Nacional, por su esfuerzo, dedicación y profesionalismo que hicieron posible la elaboración y entrada en vigencia de este aporte técnico científico a la investigación criminal en el Perú.

Ministro del Interior

INTRODUCCIÓN

Actualmente, con el desarrollo de las tecnologías informáticas y la globalización mundial, la sociedad viene siendo víctima de diferentes tipos de delitos en los cuales están involucrados dispositivos tecnológicos, generándose la necesidad que el personal de la Policía Nacional del Perú esté capacitado y especializado para prevenir, investigar y combatir la delincuencia común y el crimen organizado en sus diferentes modalidades, siendo necesaria la creación de una herramienta importante que coadyuve en la investigación, a través de un manual.

El presente documento constituye un Manual para el Recojo de la Evidencia Digital y se convierte en una herramienta importante que permite guiar al personal policial interviniente en una investigación donde se encuentren involucrados dispositivos tecnológicos, para que ejecuten el recojo de dicha evidencia respetando la parte técnica y enviarla a la unidad especializada de la Policía Nacional del Perú para su respectivo análisis informático forense, garantizando la integridad de la evidencia.

El Ministerio del Interior, con la finalidad de establecer y unificar criterios en los procedimientos de recojo y tratamiento de dispositivos tecnológicos, ha elaborado el presente Manual para el Recojo de la Evidencia Digital, que será de aplicación para todo el personal de la Policía Nacional del Perú, con la finalidad de salvaguardar la evidencia digital con valor probatorio desde la etapa de investigación preliminar hasta la etapa de juzgamiento.

MANUAL
PARA EL RECOJO DE LA EVIDENCIA DIGITAL

I. FINALIDAD

Establecer procedimientos para el adecuado recojo de medios de almacenamiento digital en la escena del crimen, garantizando su seguridad e integridad, con la finalidad de proteger la evidencia digital con valor probatorio para una investigación, en el marco de la normatividad vigente y el debido proceso.

II. CONTENIDO

El presente manual contiene temas relacionados para la recolección de evidencia digital, materiales de embalaje y lacrado, preservación de la cadena de custodia y requisitos del análisis informático forense.

III. ALCANCE

A todo el personal de la Policía Nacional del Perú en situación de actividad, especialmente aquellos que intervienen, a partir del conocimiento de la noticia criminal, en la protección y aislamiento de la escena del crimen, así como en la labor criminalística e investigación operativa criminal.

IV. MARCO LEGAL

A. Constitución Política del Perú.

B. Ley N° 29733, Ley de Protección de Datos Personales.

C. Ley N° 29867, Ley que incorpora diversos artículos al código penal relativos a la seguridad en los centros de detención o reclusión.

D. Ley N° 30077, Ley Contra el Crimen Organizado.

E. Ley N° 30096 Ley de Delitos Informáticos

F. Ley N° 30171 Ley que modifica la Ley N° 30096, Ley de Delitos Informáticos.

G. Decreto Legislativo N° 635, Código Penal.

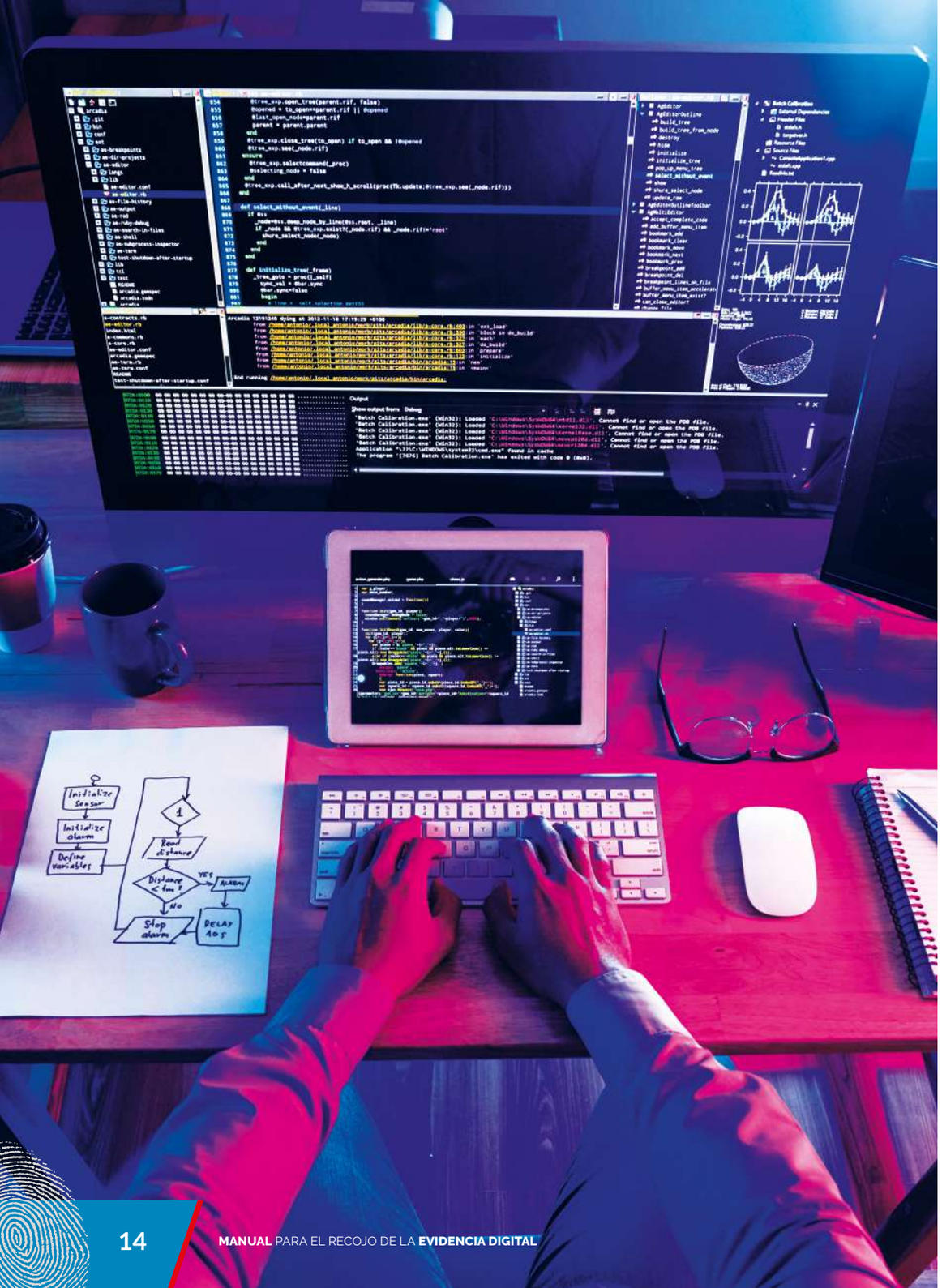
H. Decreto Legislativo N° 957, Código Procesal Penal.

I. Decreto Legislativo N° 1267, Ley de la Policía Nacional del Perú.

J. Decreto Supremo Nº 026-2017-IN, que aprueba el reglamento del Decreto Legislativo 1267 Ley de la Policía Nacional del Perú.

K. Resolución N° 729-2016-MP-FN, Reglamento de la cadena de custodia de elementos materiales, evidencias y administración de bienes incautados. y administración de bienes incautados.

L. Directiva Nº 03-19-2015-DIRGEN-PNP/EMG-DIRASOPE-B, Normas y procedimientos policiales para proteger la escena del delito y garantizar la cadena de custodia, aprobada mediante RD. N°751-2015-DIRGEN-EMG-PNP.



V. MATERIALES PARA EL RECOJO Y LACRADO DE LA EVIDENCIA DIGITAL

Se detalla los materiales y otros que se adecuen para el proceso de recojo y lacrado.

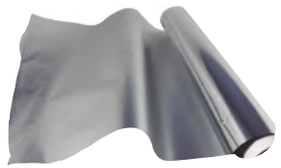
A. 

Guantes de látex.

B. 

Bolsa antiestática

(bolsa Faraday)

C. 

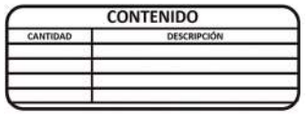
Papel de aluminio

D. 

Film alveolar (bolsa de burbuja)

E. 

Sobre de papel

F. 

Etiquetas para el rotulado

G. 

Marcadores permanentes para el rotulado

H. 

Cámara fotográfica y/o filmadora

I. 

Precintos de seguridad

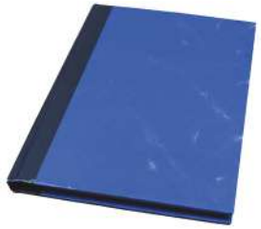
J. 

Cinta de seguridad (cascara de huevo)

K.

Cinta de embalaje

L.



Cuaderno para anotación y diseño de croquis

M.

Bolsa de polietileno o cajas de cartón

N.

Cintas adhesivas con diseño de fragilidad

O.

Instrumento óptico (lupa)

P.

Gorra quirúrgica

Q.

Kit de desarmadores

R.

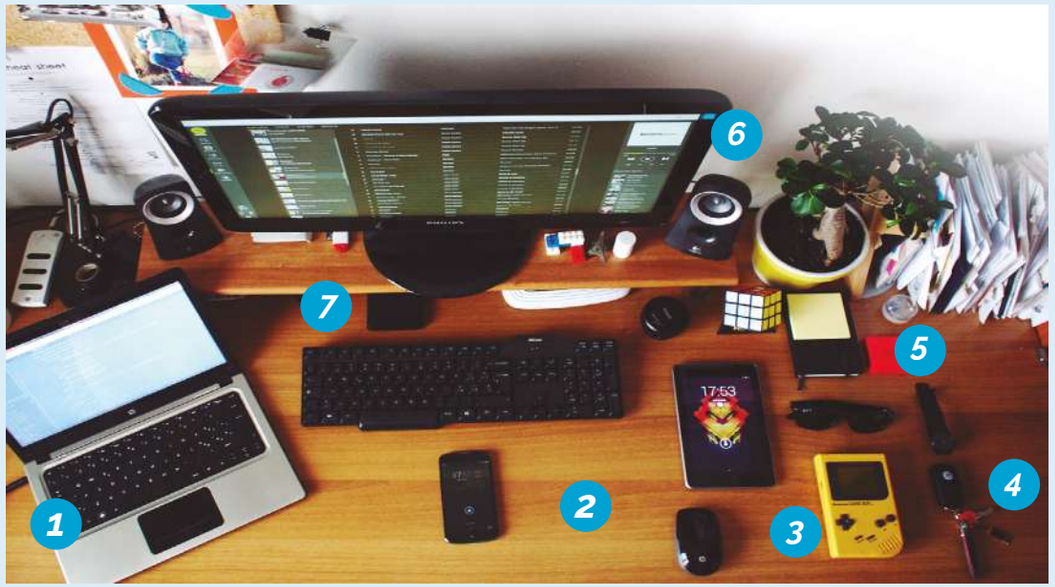
Y otros que se adecuen para el proceso de recojo y lacrado.

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.

ESCENA DEL CRIMEN



1. Dispositivos informáticos
2. Dispositivos móviles
3. Consola de videojuegos modificado
4. USB
5. Pendrive – Dispositivo lapicero con puerto USB
6. Computadora todo en uno
7. Disco duro externo

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 (PC).
   b. Computadora portátil (laptop, notebook).
   c. Servidor.
   d. Disco duro.
   e. Disco duro externo.
   f. Pen drive (USB).
   g. Memoria externa (SD, MicroSD).
   h. Lector de banda magnética (Skimmer).
   i. Tarjeta electrónica.

a.

Computador de escritorio

b.

Laptop

c.

Servidor

d.

Disco duro

e.

Disco externo

f.

Pen drive USB

g.

Memoria externa (SD, MicroSD).

h.

Lector de cinta magnética

j. Sistema de video vigilancia (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

i.

Tarjetas

j.

Cámaras de video vigilancia

k.

Router

l.

Impresora multifuncional

m.

Reproductor mp3

n.

Cámara espía.

o.

Caja de liberación y desbloqueo.

p.

Cámara fotográfica

q.

Cámara filmadora

2. Dispositivos móviles:

a. Equipo de terminal móvil (Teléfono celular)

b. Tarjeta SIM (Chip)

c. Modem 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

a.

Teléfono celular

b.

Tarjeta sim

c.

Internet móvil

d.

GPS

e.

Palm

f.

Tablet

g.

Drone

h.

Reloj inteligente (smartwatch)

i.

POS

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.

1. Dispositivos Informáticos

a. Computador personal: Encendido

(1) Verificar estado del monitor:

(a) Encendido con protector de pantalla, mover ligeramente el mouse sin presionar los botones.

(b) Apagado, encender monitor.

(c) De encontrarse protegido con contraseña, desconectar el cable de poder del computador.

(2) Desconectar el cable de poder del computador si se observa alteración o eliminación de archivos.

(3) Si se visualiza ventanas activas como sesiones de Redes sociales, correos electrónicos y otros, deberá consignarse en acta. Posteriormente; desconectar el cable de poder del computador.

(4) Verificar, desconectar los dispositivos conectados al computador (discos ópticos, memoria USB, cables, tarjetas de memoria), debiendo consignar en acta sus características (marca, modelo, serie, capacidad de almacenamiento, color y otros datos).

(5) Registrar marca, modelo, número de serie, color del computador personal (case) y otras características visuales.

(6) Proteger el (los) puertos USB, lectores de disco óptico, lectores de memoria, y otros puerto(s) de entrada y salida con cintas de seguridad.

(7) Embalar el case del computador personal y dispositivos desconectados en cajas de cartón, bolsas polietileno o papel resistente.

Para el computador personal tipo All in One (todo en uno) embalar en su totalidad.

(8) Rotular y lacrar el case del computador personal y los dispositivos embalados, de acuerdo con la normatividad vigente, consignando las firmas y post firmas de los participantes.

(9) Formular el acta de lacrado.

(10) Generar la respectiva cadena de custodia en el lugar de los hechos conforme a los formatos establecidos en la normatividad vigente.

(11) Enviar a la unidad especializada de la PNP para el análisis informático forense.

b. Computador personal: Apagado

(1) No encenderlo por ningún motivo.

(2) Verificar, desconectar los dispositivos conectados al computador (memoria USB, cables, tarjetas de memoria), debiendo consignar en acta sus características (marca, modelo, serie, capacidad de almacenamiento, color y otros datos).

Para las lectoras de CD, DVD o Blu-Ray, utilizar un clip u otro similar.

(3) Desconectar el cable de poder del computador.

(4) Registrar marca, modelo, número de serie, color del computador personal (case) y otras características visuales.

(5) Proteger el (los) puertos USB, lectores de disco óptico, lectores de memoria, y otros puertos de entrada y salida con cintas de seguridad.

(6) Embalar el case del computador personal y dispositivos desconectados en cajas de cartón, bolsas de polietileno o papel resistente. Para el tipo All in One, embalar en su totalidad.

(7) Rotular y lacrar el computador personal y dispositivos embalados, consignando las firmas y posfirmas de los participantes.

(8) Formular el acta de lacrado.

(9) Generar la respectiva cadena de custodia en el lugar de los hechos conforme a los formatos establecidos en la normatividad vigente.

(10) Enviar a la unidad especializada de la PNP para el análisis informático forense.

c. Computador portátil: Encendido

(1) Verificar estado de la pantalla:

(a) **Encendido con protector de pantalla**, mover el touch pad o mouse sin presionar los botones.

(b) **Pantalla apagada**, mover el touch pad o mouse sin presionar los botones o presionar ligeramente el botón de encendido.

(c) **De encontrarse protegido con contraseña**, apagar desconectando el cargador y/o presionando el botón de encendido por 10 segundos aproximadamente.

(2) Apagar el computador portátil si se observa alteración o eliminación de archivos.

(3) Si se visualiza ventanas activas como sesiones de redes sociales, correos electrónicos y otros, deberá consignarse en acta. Posteriormente, apaga tu computador portátil.

(4) Verificar, desconectar y perennizar con vistas fotográficas y/o video los dispositivos conectados al computador portátil (discos ópticos, memoria USB, cables, tarjetas de memoria), debiendo consignarse en acta sus características (marca, modelo,serie, capacidad de almacenamiento, color y otros datos).

(5) Registrar marca, modelo, número de serie, color del computador portátil y otras características visuales.

(6) Retirar la batería.

(7) Proteger el (los) puerto(s) USB, lectores de disco óptico, lectores de memoria, y otros puertos de entrada y salida con cintas de seguridad.

(8) Embalar el computador portátil en su totalidad, así como los dispositivos desconectados en cajas de cartón, bolsas de polietileno o papel resistente.

(9) Rotular y lacrar el computador portátil y dispositivos embalados, de acuerdo con la normatividad vigente, consignando las firmas y posfirmas de los participantes.

(10) Formular el acta de lacrado.

(11) Generar la respectiva cadena de custodia en el lugar de los hechos, conforme a los formatos establecidos en la normatividad vigente.

(12) Enviar a la unidad especializada de la PNP para el análisis informático forense.

d. Computador portátil: Apagado

(1) No encenderlo por ningún motivo.

(2) Verificar, desconectar los dispositivos conectados al computador (memoria USB, cables, tarjetas de memoria). Debiendo consignarse en acta sus características (marca, modelo, serie, capacidad de almacenamiento,color y otros datos). Para las lectoras de CD, DVD o Blu-Ray, utilizar un clip u otro similar.

(3) Registrar con vistas fotográficas y el acta correspondiente marca, modelo, número de serie, color del computador portátil y otras características visuales.

(4) Retirar la batería.

(5) Proteger el (los) puerto(s) USB, lectores de disco óptico, lectores de memoria, y otros puertos de entrada y salida con cintas de seguridad.

(6) Embalar el computador portátil en su totalidad, así como los dispositivos desconectados en cajas de cartón, bolsas de polietileno o papel resistente.

(7) Rotular y lacrar el computador portátil y dispositivos embalados, de acuerdo con la normatividad vigente, consignando las firmas y posfirmas de los participantes.

(8) Formular el acta de lacrado.

(9) Generar la respectiva cadena de custodia en el lugar de los hechos, conforme a los formatos establecidos en la normatividad vigente.

(10) Enviar a la unidad especializada de la PNP para el análisis informático forense.

e. Dispositivos de videovigilancia:

(1) Desconectar el cable de poder, en el estado en que se encuentre (encendido o apagado).

(2) Solicitar la contraseña de acceso si el dispositivo de videovigilancia cuenta con alguna medida de seguridad.

(3) Registrar marca, modelo, número de serie, color y otras características visuales.

(4) Proteger los puertos de entrada y salida visibles.

(5) Embalar el dispositivo de videovigilancia, incluyendo manuales, cable de poder y cable de datos, en bolsa film alveolar (bolsa de burbuja), bolsas de polietileno o papel resistente.

(6) Rotular y lacrar el dispositivo de videovigilancia embalada, de acuerdo con la normatividad vigente, consignando las firmas y posfirmas de los participantes.

(7) Formular el acta de lacrado.

(8) Generar la respectiva cadena de custodia en el lugar de los hechos conforme a los formatos establecidos en el Manual de Documentación Policial,

f. Otros dispositivos informáticos:

Pendrive (USB), disco duro, disco duro externo, tarjetas de memoria, discos ópticos, dispositivos multimedia y cámaras espía.

(1) Registrar marca, modelo, número de serie, color y otras características visuales.

(2) Proteger el (los) puerto(s) USB del dispositivo de almacenamiento con cintas de seguridad.

(3) Embalar el dispositivo de almacenamiento en su totalidad usando:

(a) Bolsas Faraday, que aíslan radiofrecuencia.

(b) Bolsa de burbuja para evitar golpes e impactos que dañen los dispositivos.

(c) De no contar con los materiales mencionados, utilizar otros similares.

(4) Rotular y lacrar los dispositivos de almacenamiento embalados, consignando las firmas y posfirmas de los participantes.

(5) Formular el acta de lacrado.

(6) Generar la respectiva cadena de custodia en el lugar de los hechos, conforme a los formatos establecidos en la normatividad vigente.

(7) Enviar a la unidad especializada de la PNP para el análisis informático forense.

2. Dispositivos móviles

a. Encendido:

(1) Mantener los dispositivos a la vista durante el desarrollo de las diligencias.

(2) De contar el dispositivo móvil con alguna medida de seguridad (patrón de bloqueo, PIN, reconocimiento facial o de iris, huella, entre otros), se solicitará al intervenido el desbloqueo del dispositivo y consignar en acta.

(3) Colocar en modo avión para el caso de celulares y tabletas, procediendo apagar el dispositivo móvil.

(4) Registrar las características físicas del:

(a) Dispositivo móvil: IMEI, marca, modelo, número de serie, color y otros datos.

(b) Tarjeta SIM (chip): Código identificador y logotipo del operador.

(c) Tarjeta de memoria externa: Marca, modelo, serie, capacidad de almacenamiento, color, entre otros datos.

(5) Antes del embalaje, cuando sea posible, separar la batería del dispositivo móvil.

(6) Embalar el dispositivo en:

(a) Bolsas Faraday, que aíslan radio frecuencia

(b) Bolsa de burbuja para evitar golpes e impactos que dañen los dispositivos.

(c) De no contar con los materiales mencionados, utilizar otros similares.

(7) Cubrir los puertos de entrada y salida del cdispositivo móvil con cintas de seguridad.

(8) De ser el caso, los dispositivos móviles deberán ser embalados con sus respectivos manuales, cables o cargador.

(9) Rotular y lacrar los dispositivos embalados, consignando las firmas y posfirmas de los participantes.

(10) Formular el acta de lacrado.

(11) Generar la respectiva cadena de custodia en el lugar de los hechos, conforme a los formatos establecidos en la normatividad vigente.

(12) Enviar a la unidad especializada de la PNP para el análisis informático forense.

b. Apagado:

(1) No encender el dispositivo móvil, puede alterar evidencia.

(2) Registrar las características físicas del:

(a) Dispositivo móvil: IMEI, marca, modelo, número de serie, color y otros datos.

(b) Tarjeta SIM (chip): Código identificador y logotipo del operador.

(c) Tarjeta de memoria externa: Marca, modelo, serie, capacidad de almacenamiento, color, entre otros datos.

(3) Antes del embalaje se debe separar la batería del dispositivo móvil, cuando ello sea posible.

(4) Embalar el dispositivo en:

(a) Bolsas Faraday, que aíslan radiofrecuencia.

(b) Bolsa de burbuja para evitar golpes e impactos que dañen los dispositivos.

(c) De no contar con los materiales mencionados, utilizar otros similares.

(5) Cubrir los puertos de entrada y salida del dispositivo móvil con cintas de seguridad.

(6) De ser el caso, los dispositivos móviles deberán ser embalados con sus respectivos manuales, cables o cargador.

(7) Rotular y lacrar los dispositivos móviles embalados, consignando las firmas y posfirmas de los participantes.

(8) Formular el acta de lacrado.

(9) Generar la respectiva cadena de custodia en el lugar de los hechos, conforme a los formatos establecidos en el Manual de Documentación Policial.

(10) Enviar a la unidad especializada de la PNP para el análisis informático forense.

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 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, inmovilización 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 permanecen intangibles, mientras hayan sido asegurados, fijados, recogidos y embalados técnicamente, y sometidos a la regla de cadena de custodia.

IX. LEGITIMIDAD Y LEGALIDAD EN LA ACTUACIÓN POLICIAL

A. La Policía Nacional del Perú tiene una función específica revestida dentro del marco Constitucional conforme a lo descrito en el artículo 166° de la Constitución Política del Perú, el mismo que señala lo siguiente: "...La Policía Nacional tiene por finalidad fundamental garantizar, mantener y restablecer el orden interno. Presta protección y ayuda a las personas y a la comunidad. Garantiza el cumplimiento de las leyes y la seguridad del patrimonio público y del privado. Previene, investiga y combate la delincuencia. Vigila y controla las fronteras...", dentro de este ámbito, la Policía Nacional del Perú desarrolla sus actividades en estricto respeto de los derechos humanos.

B. En el contexto de la investigación, la actividad estatal destinada al esclarecimiento de un hecho ilícito, mediante una investigación dentro del marco legal, se circunscribe en la Policía Nacional del Perú, quien, dentro de su competencia, asume la responsabilidad de preservar la escena del crimen, especialmente al momento del recojo de la evidencia. A la evidencia digital se le debe brindar un tratamiento especial por su peculiaridad, para que en el futuro su análisis pueda generar la emisión de un informe técnico pormenorizado que permita desarrollar la investigación y obtener la absolución y/o condena del imputado.

C. El Decreto Legislativo N° 1267, que aprueba la Ley de la Policía Nacional del Perú, determina en forma acertada en su artículo 2, numerales 8 y 9, las funciones de la Policía Nacional del Perú, relacionadas con el recojo y análisis de evidencia; "...8) Obtener, custodiar, asegurar, trasladar, y procesar indicios, evidencias y elementos probatorios, relacionados con la prevención e investigación del delito, poniéndolos oportunamente a disposición de la autoridad competente; 9) Practicar y emitir peritajes oficiales de criminalística para efecto de procesos

judiciales y otros derivados de la función policial…", dichas funciones, enmarcadas dentro del ámbito de investigación, legitima a la Policía Nacional del Perú y le permite desarrollar su actuación dentro del marco de la Ley.

D. El Decreto Legislativo 957, Código Procesal Penal, en su artículo 67, establece expresamente que la Policía Nacional del Perú tiene como función "…reunir y asegurar los elementos de prueba que puedan servir para la aplicación de la Ley Penal…", así mismo, en el artículo 68° establece sus atribuciones "…d)Recoger y conservar los objetos e instrumentos relacionados con el delito, así como todo elemento material que pueda servir en la investigación…", por lo tanto, a nivel procesal, la actuación de la Policía Nacional del Perú se encuentra enmarcada dentro de los parámetros legales.

E. La Ley N° 30096 y su modificatoria Ley N° 30171 se implementan dentro del ámbito jurídico del Perú, con la finalidad de adecuar nuestra legislación al derecho comparado, enmarcar lo delitos informativos mediante leyes especiales, lo cual cumple una función importante, puesto que el dinamismo cibernético genera la necesidad de la Policía Nacional del Perú de desarrollar nuevos actos de investigación, siendo la recopilación y preservación de la evidencia digital de vital importancia. Por ello, la normativa permite la coordinación interinstitucional y la cooperación operativa, para enfrentarnos a todo tipo de criminalidad.

X. REFERENCIAS BIBLIOGRÁFICAS

A. Convenio sobre la Ciberdelincuencia, del 2001 (Budapest).

B. NORMA TÉCNICA PERUANA NTP-ISO/IEC 17799 2007, EDI. Tecnología de la información. Código de buenas prácticas para la gestión de la seguridad de la información. 13.2.3 Recolección de evidencia. Tecnología de la información, técnicas de seguridad y sistemas de gestión de la información, aprobada por Resolución 129-2014/CNB-INDECOPI.

C. La Norma ISO/IEC 27037:2012 "Information technology — Security techniques — Guidelines for identification, collection, acquisition and preservation of digital evidence"

D. RFC 3227 El "RFC 3227: Guía Para Recolectar y Archivar Evidencia" (Guidelines for Evidence Collection and Archiving) [GuEvCo02], escrito en febrero de 2002.

E. Manual de Documental Policial, aprobado mediante RD.N° 776-2016-DIRGEN/EMG-PNP.

F. https://www.definicionabc.com/

G. https://www.aboutespanol.com/

H. http://www.wordreference.com/

I. https://es.wikipedia.org/

J. https://isacriminalistica.weebly.com/

K. https://tecnologia-facil.com/

L. https://www.holographic-sas.com/

M. https://definicion.mx/

N. https://www.significados.com/

XI. ANEXOS

A. DEFINICIÓN DE TÉRMINOS

1. **All in One (todo en uno):** Computadora personal integrada, vale decir que en el monitor se encuentra incorporado el procesador, el disco duro, y toda la placa base, por lo tanto, solo tenemos un elemento.
2. **Análisis informático forense:** Conjunto de técnicas científicas y analíticas especializadas en infraestructuras tecnológicas que permiten identificar, preservar, analizar y presentar datos que sean válidos en un proceso legal.
3. **Blu-Ray:** Formato de disco óptico de nueva generación, desarrollado por la Blu-ray Disc Association (BDA), empleado para vídeo de alta definición (HD), 3D y UltraHD.
4. **Bolsa antiestática:** Bolsa diseñada para prevenir electricidad estática en componentes electrónicos cuando se empaquetan, se transporten o se almacenan.
5. **Bolsa Faraday:** Bolsa diseñada para proteger de los campos eléctricos estáticos.
6. **Cámara espía:** Cámara de fotos o vídeos usada para filmar de manera "oculta". Tienen diferentes presentaciones, tales como minicámaras espías, relojes espías, llaveros espías, lapiceros espías, encendedores espías y hasta ropa espías.
7. **Case:** Llamado también gabinete, carcasa, chasís o caja, es una estructura de metal y plástico, donde se aloja toda la arquitectura de la computadora personal (mainboard, tarjetas, disco duro, lectora, entre otros.)
8. **CD (Compact Disc):** Disco óptico utilizado para almacenar datos en formato digital, consistentes en cualquier tipo de información (audio, imágenes, vídeo, documentos y otros datos).
9. **Computadora personal (PC):** Dispositivo informático capaz de recibir, almacenar y procesar información. Está programada para realizar operaciones lógicas o aritméticas de forma automática. Generalmente como computadoras de escritorio.
10. **Computadora portátil (laptop, notebook):** Computadora personal que puede ser transportado fácilmente. Tienen la capacidad de operar por un período determinado sin estar conectadas a una red eléctrica. Por medio de baterías es.
11. **Debido proceso:** Principio jurídico procesal; según el cual toda persona tiene derecho a ciertas garantías mínimas, tendientes a asegurar un resultado justo y equitativo dentro de un proceso.
12. **Disco duro externo:** Disco duro acoplado a una carcasa con una interfaz que permite conectar a una computadora, laptop, servidor, entre otros, mediante un puerto USB, en oposición a los discos rígidos internos que se encuentran conectados directamente a la placa madre.
13. **Disco Duro:** Componente utilizado para almacenar datos de manera permanente, se le denomina dispositivo de almacenamiento masivo.
14. **Dispositivos multimedia:** Elementos electrónicos que permiten la captura o emisión de información de video, audio, imagen y texto.
15. **DVD (Disco Digital Versátil):** Disco digital del mismo tamaño que un CD, pero con una capacidad de almacenamiento de datos, imagen o sonido quince veces mayor.
16. **Embalaje:** Es el aseguramiento, inmovilización y protección de los indicios y evidencias o elementos materiales en un contenedor o recipiente idóneo y sellado, a fin de evitar su contaminación, alteración o destrucción durante su transporte, hasta el lugar en donde se estudiará y analizará.

17. **Equipo de comunicación (router y switch):** Equipamiento electrónico que permite recibir y transmitir señales digitales. En el caso de un router, permite interconectar una red local con otras redes, basada en una tabla de rutas. El switch sirve para establecer interconexiones en redes locales y ofrece conexión a los equipos que conforman una subred LAN.
18. **Escena del crimen:** Es el lugar o espacio físico donde sucedieron los hechos investigados. Es el foco protagónico en el cual el autor o participe; 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.
19. **Extracción de información:** Consiste en extraer información de dispositivos de almacenamiento masivo, manual o automáticamente, mediante herramientas forenses.
20. **Film alveolar (bolsa de burbuja):** Material de plástico flexible y transparente usado para embalar artículos frágiles y delicados.
21. **IMEI (identidad internacional de equipo móvil):** Es un identificador único que tiene cada móvil (celulares y tabletas), formado por 15 dígitos.
22. **Impresora multifuncional:** Dispositivo que posee funciones de impresora, escáner y fotocopiadora dentro de un mismo y único bloque físico.
23. **Intangible:** Que no puede ser tocado o no debe ser alterado o dañado.
24. **iPad:** Dispositivo electrónico, tipo tableta que asume la modalidad de computadora portátil desarrollado por la empresa Apple Inc.
25. **Lector de banda magnética (Skimmer):** Dispositivo electrónico que permite leer datos de una tarjeta, almacenados en la banda magnética.
26. **Modem USB:** Dispositivo USB portátil, que funciona como un módem y se conecta a una computadora portátil o de escritorio.
27. **Noticia criminal:** Es el conocimiento o información sobre la comisión de una conducta punible que llega a conocimiento de la Policía o Ministerio Público.
28. **Palm:** Llamado también PDA (Asistente Digital Personal). Computadora de mano diseñada como agenda personal electrónica.
29. **Patrón de bloqueo:** Medida de seguridad para teléfonos celulares, tabletas u otros dispositivos móviles, que consiste en unir puntos en direcciones predeterminadas para tener acceso al equipo.
30. **Pen drive (USB):** Dispositivo para el almacenamiento de información digital que utiliza memoria flash y una interfaz USB.
31. **PIN (Número de identificación personal):** Tipo de contraseña utilizado en ciertos sistemas, como teléfonos móviles o cajeros automáticos.
32. **Puertos USB (Universal Serial Bus):** Interfaz que permite la conexión de periféricos a diversos dispositivos.
33. **Recojo:** Acción de recoger o recopilar objetos, huellas, indicios y elementos que constituirán evidencia para resolver los casos.
34. **Reconocimiento facial:** Aplicación que identifica automáticamente a una persona mediante características faciales del sujeto extraídas de la imagen o de un fotograma.
35. **Reloj inteligente (smartwatch):** Reloj de pulsera capaz de acceder a internet, realizar y recibir llamadas telefónicas, enviar y recibir mensajes de texto y correo electrónico, así como realizar consultas en redes sociales.

36. **Rótulo:** Del latín "rotulus", inscripción que se sitúa sobre algo para indicar qué es, hacia dónde se envía, para qué sirve, entre otros.

37. **Servidor:** Dispositivo informático que forma parte de una red y provee servicios a dispositivos clientes.

38. **Sistema de posicionamiento global (GPS):** Dispositivo que sirve para la localización de personas, vehículos, objetos, entre otros.

39. **Sistema de videovigilancia:** Componentes de cámaras, monitores, grabadores instalados, que permiten registrar en video acontecimientos de un lugar, conocidos como circuito cerrado de televisión. Los términos DVR, NVR y NDVR están referidos a los tipos de dispositivos de grabación y se diferencian en el tipo de cámaras que se conectan a ellas. DVR para cámaras analógicas, NVR para cámaras IP y NDVR combina ambas tecnologías, tanto analógicas y tecnología IP.

40. **Cinta de seguridad (cáscara de huevo):** Etiqueta de seguridad que no puede ser desprendida totalmente, sino en fracciones.

41. **Tableta (tablets):** Dispositivo electrónico que tiene un tamaño intermedio entre el ordenador y el móvil.

42. **Tarjeta de memoria externa:** Formato de tarjeta de memoria flash, que permite guardar y borrar información, utilizada en dispositivos portátiles.

43. **Tarjeta electrónica:** Tarjeta plástica que cuenta con un chip electrónico y/o con una banda magnética en el reverso y guarda información del suscriptor, utilizada para operaciones bancarias, comerciales, administrativas, entre otras.

44. **Tarjeta SIM (módulo de identificación de suscripción):** Tarjeta inteligente desmontable usada en teléfonos móviles y tabletas, que se conectan al dispositivo por medio de una ranura lectora o lector SIM. Conocida como CHIP.

45. **Equipo terminal móvil (teléfono celular):** Dispositivo inalámbrico electrónico que permite tener acceso a la red de telefonía celular o móvil.

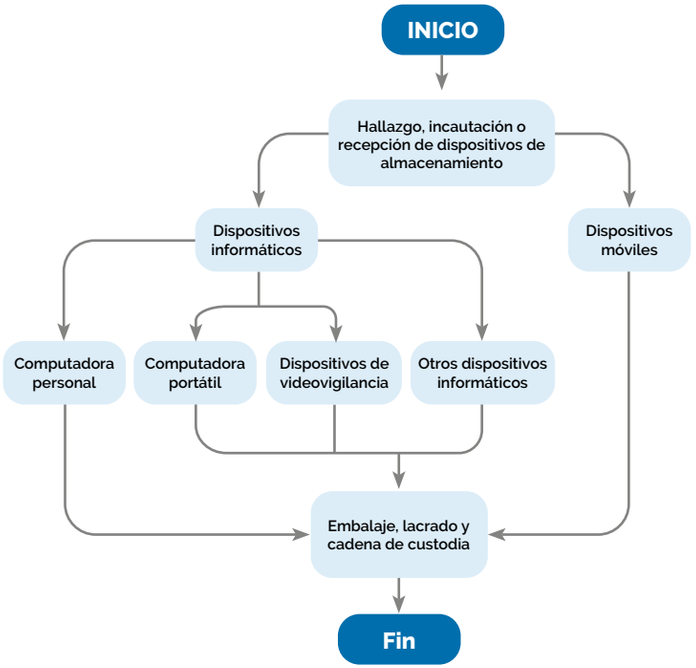
46. **Terminal de punto de venta (POS):** Dispositivo de tipo electrónico con una pantalla y un teclado, utilizada para transacciones de venta, depósito, pago, entre otras.

47. **Touch pad:** Panel táctil que permite controlar un cursor o facilitar la navegación a través de un menú o de cualquier interfaz gráfica.

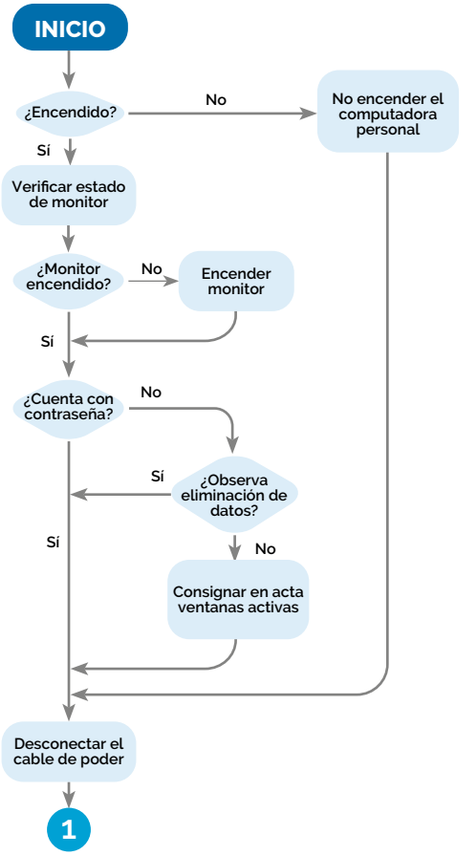
48. **Vehículo aéreo no tripulado (Dron):** Aeronave que vuela sin tripulación, reutilizable, capaz de mantener de manera autónoma un nivel de vuelo controlado y sostenido.

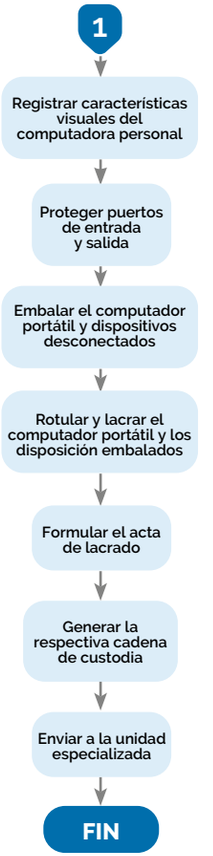
B. DIAGRAMAS DE FLUJO PARA EL HALLAZGO, INCAUTACIÓN O RECEPCIÓN DE DISPOSITIVOS DE ALMACENAMIENTO.

1. ESQUEMA GENERAL

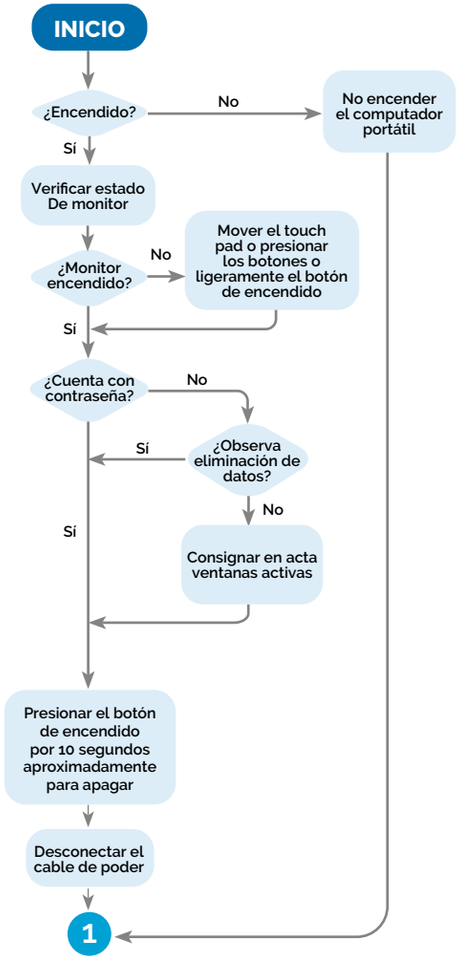


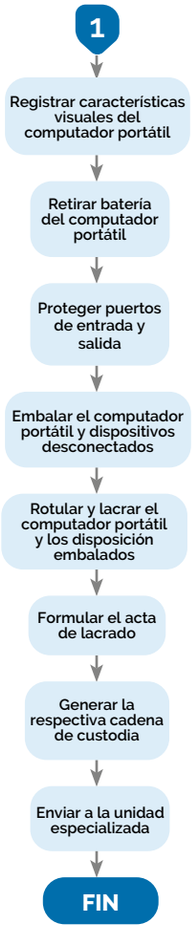
2. COMPUTADORA PERSONAL



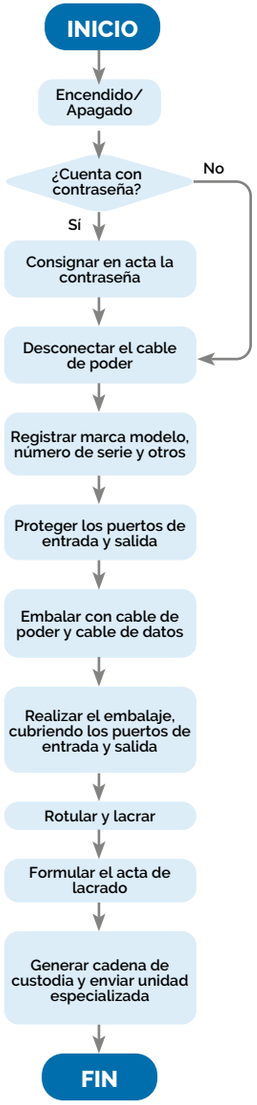


3. COMPUTADORA PORTÁTIL

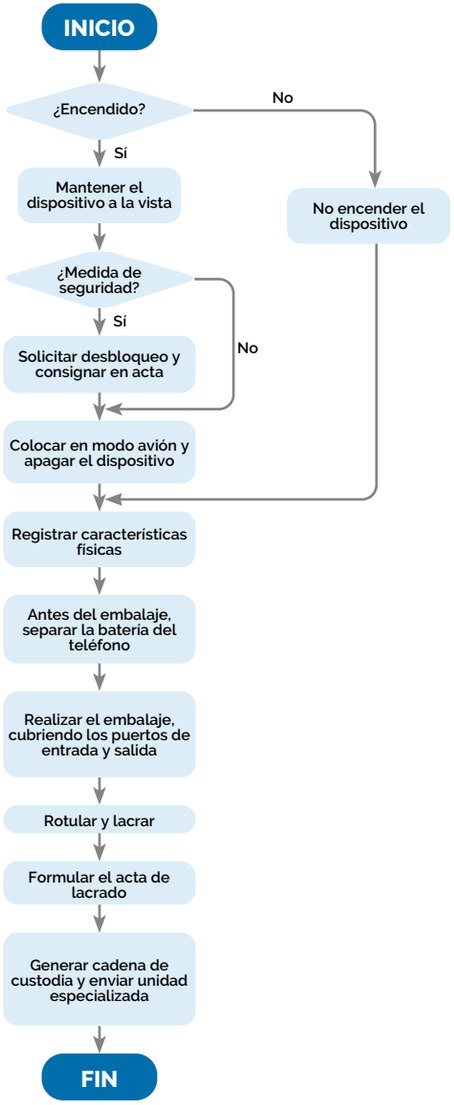




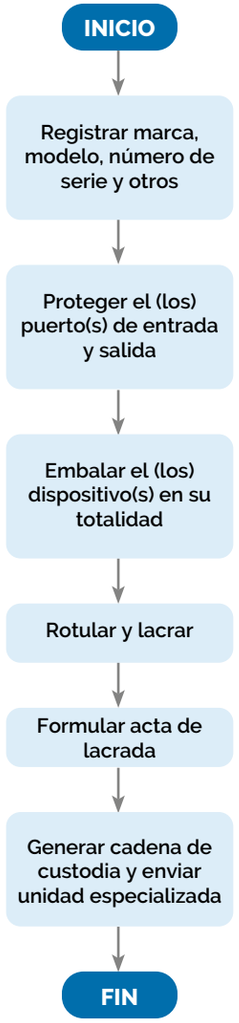
4. DISPOSITIVOS DE VIDEO VIGILANCIA



5. DISPOSITIVO MÓVIL



6. OTROS DISPOSITIVOS INFORMÁTICOS



C. FORMATOS

1. Acta de cadena de custodia.

FORMATO 04

ACTA DE CADENA DE CUSTODIA

EVIDENCIA LEVANTADA: ______________________
ESPECIE CONSISTENTE:
____
____
____
____
FECHA DE
LEVANTAMIENTO______________ HORA:______________
OCURRENCIA POLICIAL : Nº ______________________
TIPO DE DELITO : ______________________
EFECTIVO POLICIAL QUE REALIZA LEVANTAMIENTO: ______________
____
UNIDAD POLICIAL : ______________________
LUGAR : ______________________
OBSERVACIONES : ______________________
____
PERSONAL PNP A CARGO: ______________________
____
ENTREGADO POR : ______________________
CIP Y CARGO : ______________________
RECIBIDO POR : ______________________
FECHA Y HORA : ______________________
LUGAR : ______________________
MOTIVO DEL TRASLADO : ______________________
ENTREGADO POR : ______________________
CIP Y CARGO : ______________________
RECIBIDO POR : ______________________
FECHA Y HORA : ______________________
LUGAR : ______________________
MOTIVO DEL TRASLADO : ______________________
ENTREGADO POR : ______________________
CIP Y CARGO : ______________________
RECIBIDO POR : ______________________
FECHA Y HORA : ______________________
LUGAR : ______________________
MOTIVO DEL TRASLADO : ______________________

EL INSTRUCTOR   EL RECONOCEDOR

______________   ______________

2. Continuidad de cadena de custodia.

CONTINUIDAD DE CADENA DE CUSTODIA

DESCRIPCIÓN DEL ELEMENTO EN CUSTODIA (INDICIO O EVIDENCIA)

FECHA D /M /A	HORA	NOMBRE COMPLETO DE QUIEN EMBALA BIENES INCAUTADOS	NOMBRE COMPLETO DEL 1R0 QUE TRANSPORTA BIENES INCAUTADOS	DNI \ CPI	CARGO / INSTITUCIÓN	FIRMA

REGISTRO DE CONTINUIDAD DE CUSTODIA DE INDICIOS O EVIDENCIAS

FECH A D/M / A	HORA	GRADO, NOMBRES COMPLETO DE QUIEN RECIBE BIENES	DNI \ CPI	CARGO / INSTITUCIÓN	CODIGO DE RECEPCIÓN	PROPOSITO DEL TRASLADO	AUTORIDAD QUE AUTORIZA TRASLADO O DESTINO FINAL	FIRMA	OBSERVACIONES

3. Acta de lacrado.

ACTA DE LACRADO ...

En la ciudad _____el distrito de _____, siendo las _____ horas del _____, en el lugar ubicado en_____, el Instructor Policial que suscribe con el imputado o testigo (en caso de hallazgo) _____, de _____ años de edad, natural de _____, estado civil _____, ocupación _____, nacido el _____ hijo de don _____ y doña _____ Identificado con _____ y con domicilio en _____; se procede a levantar la presente **ACTA DE LACRADO**, con el siguiente detalle:

1. Describir la especie, evidencia, etc.
2. Detallar el embalaje.
3. Detallar el tipo de lacrado.
4. Sellar y firmar los cierres del lacrado.

_____

_____

_____

_____

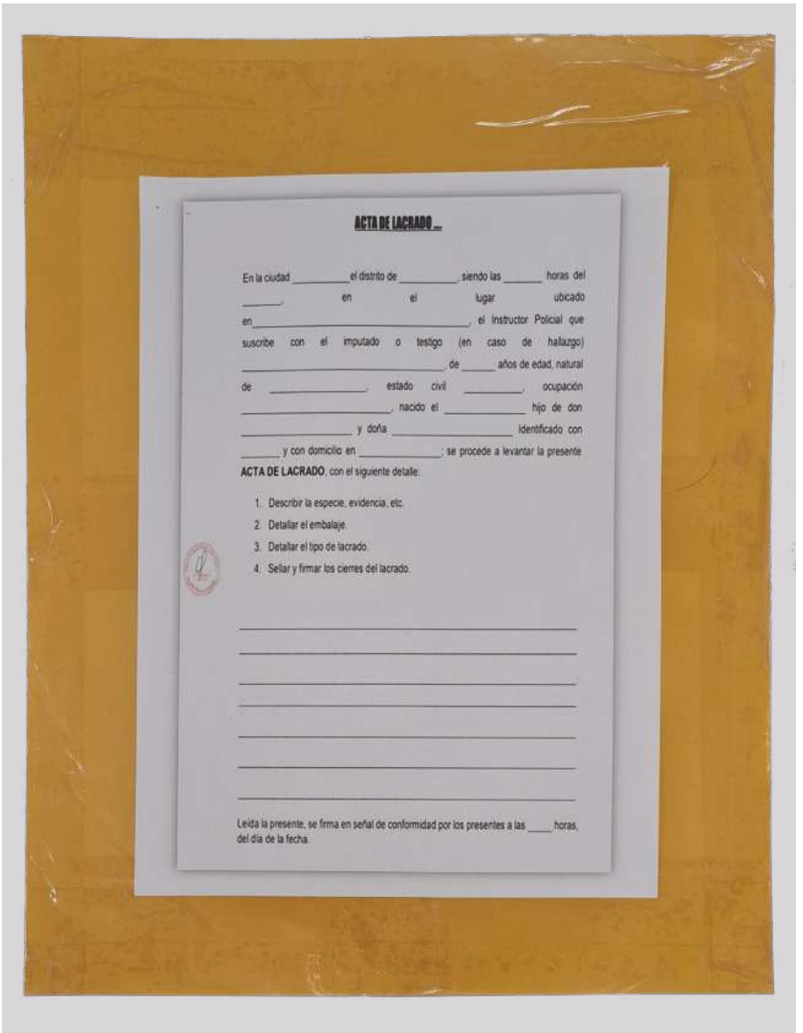
_____

_____

_____

Leída la presente, se firma en señal de conformidad por los presentes a las ____ horas, del día de la fecha.

ANVERSO



REVERSO

4. Acta de hallazgo y recojo.

ACTA DE HALLAZGO Y RECOJO

En la ciudad de _____, Distrito _____, siendo las _____, del _____ 20__, sito en _____, **el instructor policial** que suscribe _____ PNP_____ identificado con CIP _____, perteneciente a la unidad _____,en presencia **del imputado y/o testigo** identificado con ____, edad ____, natural de _____, estado civil_____, ocupación_____, con instrucción _____identificado con: _____, domiciliado en _____ procede a realizar la presente diligencia, en las circunstancias siguientes:

_____
_____
_____
_____
_____
_____
_____

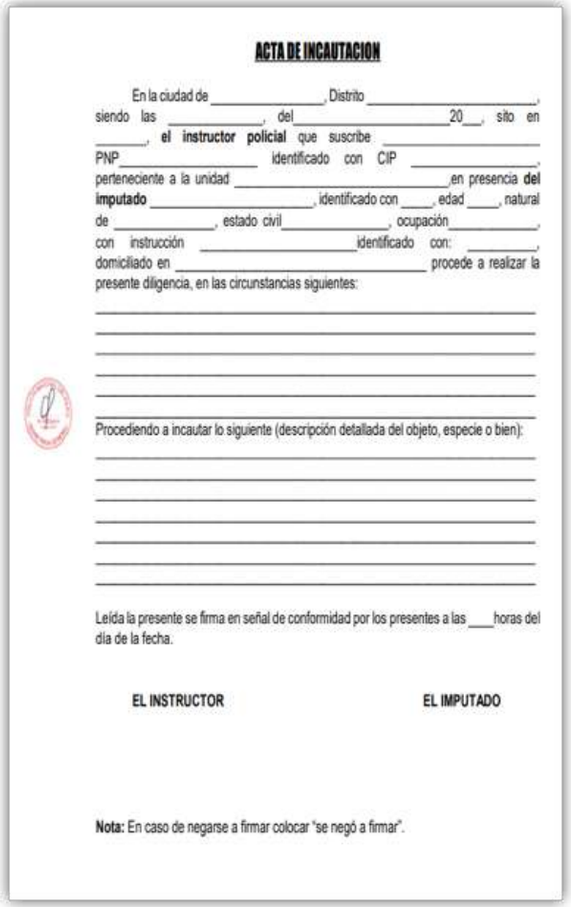
Procediendo a recoger lo siguiente (descripción detallada del objeto, especie o bien):

_____
_____
_____
_____
_____
_____
_____

Leída la presente se firma en señal de conformidad por los presentes a las_____ horas del día de la fecha.

EL INSTRUCTOR **EL IMPUTADO Y/O TESTIGO**

5. Acta de incautación.



ACTA DE INCAUTACION

En la ciudad de _____, Distrito _____, siendo las _____, del _____20__, sito en _____, **el instructor policial** que suscribe _____ PNP_____ identificado con CIP _____, perteneciente a la unidad _____,en presencia **del imputado** _____, identificado con ____, edad ____, natural de _____, estado civil_____, ocupación_____, con instrucción _____identificado con: _____, domiciliado en _____ procede a realizar la presente diligencia, en las circunstancias siguientes:

_____
_____
_____
_____
_____
_____

Procediendo a incautar lo siguiente (descripción detallada del objeto, especie o bien):

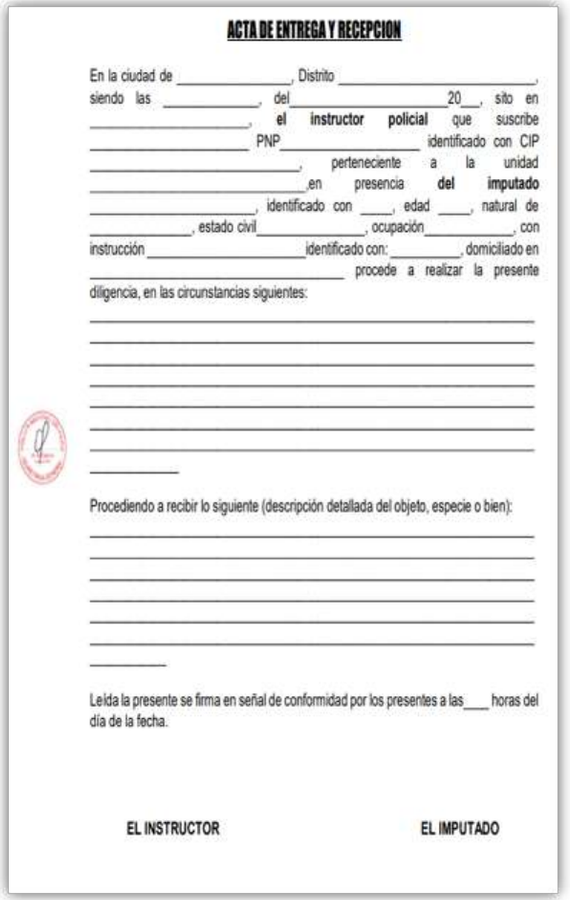
_____
_____
_____
_____
_____
_____
_____

Leída la presente se firma en señal de conformidad por los presentes a las ___ horas del día de la fecha.

EL INSTRUCTOR **EL IMPUTADO**

Nota: En caso de negarse a firmar colocar "se negó a firmar".

6. Acta de entrega y recepción.



ACTA DE ENTREGA Y RECEPCION

En la ciudad de _____, Distrito _____, siendo las _____, del_____20__, sito en _____, **el instructor policial** que suscribe _____ PNP_____ identificado con CIP _____, perteneciente a la unidad _____,en presencia **del imputado** _____, identificado con ____, edad ____, natural de _____, estado civil_____, ocupación_____, con instrucción _____identificado con: _____, domiciliado en _____ procede a realizar la presente diligencia, en las circunstancias siguientes:

_____
_____
_____
_____
_____
_____
_____
_____

Procediendo a recibir lo siguiente (descripción detallada del objeto, especie o bien):

_____
_____
_____
_____
_____
_____
_____

Leída la presente se firma en señal de conformidad por los presentes a las ___ horas del día de la fecha.

EL INSTRUCTOR **EL IMPUTADO**

7. Acta de Autorización del Usuario.

Acta de Autorización del Usuario.

Yo, _____, debidamente identificada con DNI N° _____, con estado civil _____, natural de_____, domiciliado en _____**OTORGO AUTORIZACIÓN** de manera voluntaria a que personal especializado de la PNP realice el análisis informático forense (extracción, visualización y otros) de la información contenida en mis dispositivos informáticos (teléfono celular, discos duro, computadora, laptop, entre otros).

Lima, ____de _____ del_____

INSTRUCTOR PNP **USUARIO**

MANUAL
PARA EL RECOJO DE LA
EVIDENCIA DIGITAL

DIRECCIÓN GENERAL CONTRA EL CRIMEN ORGANIZADO

PERÚ | Ministerio del Interior

Plaza 30 de agosto Nº 150 Urb. Córpac, San Isidro
Tlf.: (01) 418 4030, anexo 2302
www.mininter.gob.pe

EL PERÚ PRIMERO

Siguenos en:

@MininterPerú @MININTERPERU @mininterperú MininterPeru mininter