MPA
MINISTERIO
PÚBLICO DE LA
>ACUSACIÓN

RESOLUCIÓN N° 92

Santa Fe, 18 ABR 2024

VISTO:

El Expediente N° FG-000123/2024 del Registro de Información de Expedientes del Ministerio Público de la Acusación en el cual se gestiona la Aprobación del Protocolo de Procesos de Trabajo de los Laboratorios Informático Forenses del Organismo de Investigaciones; y,

CONSIDERANDO:

Que, el Ministerio Público de la Acusación es ejercido por la Fiscal General y los demás órganos contemplados en la ley 13.013, siendo ésta la responsable de la organización y el funcionamiento del mismo, velando por el cumplimiento de las misiones y funciones institucionales.

Que, el artículo 13 de la misma ley prevé al Organismo de Investigaciones como uno de los órganos de apoyo a la gestión que integran la estructura orgánica del Ministerio Público de la Acusación.

Que, la Ley 13.459 del Organismo de Investigaciones en su artículo 2 dispone que *"El Organismo de Investigaciones integra el Ministerio Público de la Acusación como órgano técnico de apoyo a la gestión, dependiente orgánica, financiera y funcionalmente del Fiscal General".*

Que, en dicha línea el artículo 6 dispone que *"El organismo actuará bajo las condiciones que reglamente el Fiscal General del Ministerio Público de la Acusación teniendo en cuenta la especificidad de su objeto y su capacidad operativa".*

Que, con fecha 5 de septiembre de 2023 se dictó la Resolución FG N.° 301, asignándose provisoriamente, por 90 días corridos, en la función de Directora

Provincial del Organismo de Investigaciones a la Dra. Carla Cerliani.

Que, en fecha 23.11.2023 la Dra. Cerliani presentó en esta Fiscalía General un "Proyecto de Protocolización de los Procesos de Trabajo de los Laboratorios Informático Forenses dependientes del Organismo de Investigaciones".

Que sin perjuicio que mediante Resolución FG N° 87/2019 -parcialmente modificada a través de la Resolución FG N°112/2019- se aprobaron las "Bases del funcionamiento operacional del Organismo de Investigaciones del Ministerio Público de la Acusación de la provincia de Santa Fe", dichas disposiciones no habían tenido operatividad en relación al LIF.

Que, es necesario que el Organismo de Investigaciones cuente con estrictos protocolos y específicos circuitos de trabajo para el funcionamiento de todas las áreas a los fines de optimizar su funcionamiento.

POR ELLO:

LA FISCAL GENERAL

RESUELVE:

ARTÍCULO 1: Aprobar el "Manual de Procedimientos del Laboratorio Informático Forense (LIF) del Organismo de Investigaciones" que como anexo forma parte integrante de la presente.

ARTÍCULO 2: Regístrese, comuníquese, publíquese en la página web del MPA y archívese.

MARIA CECILIA VRANICICH
FISCAL GENERAL
MINISTERIO PÚBLICO DE LA ACUSACIÓN
PROVINCIA DE SANTA FE

Manual de Procedimientos del Laboratorio Informático Forense (LIF) del Organismo de Investigaciones

MPA
MINISTERIO
PÚBLICO DE LA
>ACUSACIÓN

Índice

1. Procesos de trabajo..... .5

1.1. Introducción..... .5

1.2. Fundamentación técnica y jurídica..... .5

1.3. Proceso..... .8

1.3.1. Recepción (Punto de control - Mesa de Entradas y Salidas)..... .8

1.3.2. Extracción (Laboratorio)..... .9

1.3.3. Resguardo del dispositivo (Punto de control - Mesa de Entradas y Salidas)..... .10

2. Solicitud de extracción informática forense..... .11

3. Guía de procedimientos para la identificación, adquisición, recolección y preservación de evidencia digital..... .13

3.1. Glosario..... .13

3.2. Introducción..... .19

3.3. Objetivo..... .19

3.4. Alcance..... .19

3.5. Principios generales de intervención..... .20

3.6. Identificación, recolección, adquisición y preservación de Evidencia Digital ..... .20

3.6.1. Intervención inicial..... .20

3.6.2. Recolección y adquisición de PEPs..... .22

3.6.2.1. Recolección..... .22

3.6.2.2. Adquisición..... .22

3.6.2.2.1. Consideraciones generales..... .22

3.6.2.2.2. Escenarios Posibles al momento de realizar una adquisición de datos:..... .23

3.6.3. Preservación de la PEPs: embalaje, cadena de custodia y traslado.....24

3.6.3.1. Embalaje o envoltorio..... .24

3.6.3.2. Cadena de Custodia..... .25

3.6.4. Traslado..... .25

3.7. Procedimientos específicos de recolección por tipos de dispositivos electrónicos..... .25

3.7.1. Dispositivos móviles..... .25

3.7.2. Computadora portátil o equipo informático de escritorio.....26

3.7.3. Equipos servidores..... .27
3.7.4. Equipos de imagen y video..... .28
3.7.5. Redes informáticas..... .28
3.7.6. Criptoactivos..... .29
3.7.7. Rig de minería..... .29
3.7.8. Tarjetas SIM/USIM..... .29
3.7.9. Medios de almacenamiento digital..... .29
3.8. Anexo..... .30
3.8.1. Lista de verificación - Recolección de dispositivos móviles..... .30
3.8.2. Lista de verificación - Computadora portátil o equipo informático de escritorio..... .33
3.8.3. Lista de verificación - Equipos servidores..... .35
3.8.4. Lista de verificación - Equipos de imagen y video..... .37
3.8.5. Lista de verificación -Tarjetas SIM/USIM..... .39
3.8.6. Lista de verificación -Medios de almacenamiento digital..... .40
4. Depósito laboratorio informático forense (LIF)..... .41
4.1. Protocolo de resguardo de evidencias..... .41
4.1.1. Pautas de Trabajo para el personal del Depósito del LIF:..... .41

1. Procesos de trabajo

1.1. Introducción

El Laboratorio Informático Forense (LIF) del Organismo de Investigaciones del Ministerio Público de la Acusación (MPA) realiza extracción de datos almacenados en dispositivos electrónicos a través de la utilización de herramientas forenses con estándares de seguridad a nivel internacional[1].

El presente documento describe los procesos de trabajo utilizados por el laboratorio informático para garantizar su transparencia y trazabilidad con especial énfasis en la recepción y tratamiento de los elementos de evidencia recibidos en el marco de una investigación penal. Se hace énfasis en preservar la integridad de la cadena de custodia, la individualización, seguridad y preservación de la evidencia recolectada para su potencial uso como elemento de prueba durante el juicio. Este proceso está respaldado por fundamentos tanto técnicos como jurídicos.

1.2. Fundamentación técnica y jurídica

El procedimiento es realizado por personal idóneo del LIF a través de herramientas forenses, su utilización hacen que resulte imposible modificar los datos[2] al momento de su obtención, el personal no tiene acceso al contenido de la extracción sino hasta después de procesados los datos. Luego de obtenidos son decodificados[3] por un software forense, que trabaja mancomunadamente con la herramienta de extracción, generando recién en este punto el reporte con el contenido del dispositivo aportado que va a ser presentado al MPA.

De este modo se garantiza la trazabilidad e inalterabilidad de la evidencia obtenida por este medio, además de que dicho proceso (extracción) puede realizarse cuantas veces sea necesario, obteniendo en cada oportunidad el mismo resultado, por lo que, si hubiese algún tipo de duda en relación a los datos obtenidos, puede repetirse el proceso de extracción en cualquier laboratorio forense que cuente con el equipamiento adecuado.

También resulta relevante aclarar que si en el tiempo que transcurre entre ambas extracciones la herramienta forense se actualiza, es posible que dicha actualización permita decodificar una mayor cantidad de datos que los extraídos en la primera oportunidad, no

1. Actualmente se cuenta con las herramientas *UFED, AXIOM y AUTOPSY*. Con el avance de las tecnologías se descubren nuevas herramientas forenses y nuevas funcionalidades de las ya existentes, desde el OI constantemente se evalúa la pertinencia y posibilidad de incorporación.
2. Los **datos** son símbolos que describen condiciones, hechos, situaciones o valores. Los datos se caracterizan por no contener ninguna información. Un dato puede significar un número, una letra, un signo ortográfico o cualquier símbolo que represente una cantidad, una medida, una palabra o una descripción. La importancia de los datos está en su capacidad de asociarse dentro de un contexto para convertirse en información.
3. En el contexto de la informática forense, la palabra "decodificar" se refiere al proceso de convertir datos en un formato legible o comprensible a partir de su forma original codificada o encriptada. Este proceso es fundamental para el análisis de datos en casos de investigación forense digital.

obstante, nunca obtendremos menos datos en una segunda extracción, por lo que el éxito de la segunda extracción está garantizado. Contando con el dispositivo móvil siempre es posible volver a controlar la data contenida en el mismo y, por ende, despejar dudas en torno a si fue de algún modo alterada y/o manipulada desde el levantamiento del dispositivo hasta la adquisición de datos, en tanto cualquier modificación queda indefectiblemente reflejada en el dispositivo y puede corroborarse a partir de otra extracción de información, ya que esta es reproducible las veces que sea necesario.

La labor del Laboratorio Informático Forense se dirige a la obtención de datos contenida en los dispositivos electrónicos a solicitud de una autoridad fiscal o judicial en el marco de una investigación penal y no realiza análisis sobre dichos datos, por lo que se trata de un procedimiento técnico de auxilio y no una pericia, tal como lo ha reconocido la jurisprudencia local que ha entendido que

"*la actividad de los intervinientes al extraer mensajes, contactos, fotos y llamadas de teléfonos celulares secuestrados en la cárcel, tiene toda la apariencia de un asesoramiento al fiscal, más que una pericial normada o reglada, y ello es así porque los intervinientes no sacaron conclusiones sobre lo encontrado y en función de sus conocimientos sobre el tema; es como si se hubiera ordenado transcribir a un papel una escucha telefónica, ello nunca podrían considerarse una pericia judicial, sino más bien una actividad de auxilio a la justicia para un mejor entendimiento.* (...) *Pero lo más importante para avalar lo dicho es que la extracción no produjo un acto procesal irreproductible ya que luego de la extracción de datos, se podían hacer nuevamente (por ejemplo a pedido de la defensa) y conforme el método utilizado y el programa elegido, se garantizó la intangibilidad de los datos de los celulares*" (Acuerdo Nº. 581 Tº. LXVI, Fº. 291/415 emanado el 28 de noviembre de 2022 del Tribunal de Apelación Oral con sede en Rosario, con la integración para el caso de los Dres. José Luis Mascali, Gustavo Salvador y Daniel Curik, en el Legajo Judicial CUIJ Nº 21-06972393-1 en la causa "CÉSAR, Matías Nicolás; UBERTI, Lucía Estefanía; DELGADO, Daniel Alejandro; OLIVERA, Leandro Daniel; Fernández, Leonel Alejandro; Cantero, Ariel Máximo s/Apelación - Sentencia condena prisión efectiva").

Este criterio fue ratificado en el fallo emanado el 8 de julio de 2022 del Colegio de Jueces de Primera Instancia de Rosario, integrado por las Dras. María Isabel Mas Varela, Irma Patricia Bilotta y el Dr. Alejandro María Negroni en los siguientes términos: "(...) *corresponde determinar en primer lugar si nos hallamos frente a un acto definitivo e irreproductible, y en consecuencia le son aplicables las exigencias de los arts. 260, 282 y 283 (cc. 268 inc. 7) CPP. En este punto, este Tribunal disiente con la calificación atribuída por la Defensa, y entiende que el desbloqueo y la posterior extracción de la información contenida en el teléfono Iphone 8, perteneciente al imputado Esteban Alvarado no constituye un acto de tal naturaleza, toda vez que tal como explicaron John Chan, Franco Vallejos, Ordoqui y Adrián Vallejos, los procedimientos se limitan a una operación "mecánica" de extracción de la información a través de los dispositivos UFED, que como se vio, se llevó a cabo utilizando un software. Es decir, que se trató de una extracción forense y no de una pericia; la cual se equipara al acto de resguardo de evidencia, esto es, la*

obtención de una copia (o duplicación) de la información que obraba en los aparatos y su guarda en un soporte informático, que en el caso fue un disco rígido portable con teclado inserto y código de seguridad, previo generar su hash. A su vez, los expertos que realizaron esta actividad no desarrollaron una tarea de interpretación, valoración o dictamen en función de su especialidad científica o técnica" (N.º 560, F.º LXXVI y LXXVII, Fº. 1/683 CUI.J Nº 21-08012606-6 y acumuldos seguida a Esteban Lindar Alvarado y otros)

Este último fallo fue ratificado por el Colegio de Cámara de Apelación Penal de Rosario, integrada por la Dra. Carolina Hernández y los Dres. Alfredo Ivaldi Artacho y Guillermo Llaudet, asentando que "*la extracción forense de información digital de un teléfono celular secuestrado que contaba con autorización judicial para su apertura dicho sea de paso, de su tarjeta SIM, o la de memoria externa, a través de herramientas informáticas idóneas que no alteran el contenido almacenado, o el análisis pericial ulterior del material extraído, no conforman actos irreproducibles ni definitivos que, en los términos del art. 282 CPP, obliguen a la Fiscalía, para su validez* (...)" (Fallo Nº. 64, Tº. LXIX, Fº. 212/483, CUIJ Nº 21-08029147-4 y acumulados seguidos a Esteban Lindor ALVARADO y otros).

En este mismo sentido se ha pronunciado la Cámara Federal de Apelaciones de Mendoza al sostener que "*la falta de notificación de la fecha en que comenzó la extracción de los datos del celular secuestrado por parte de los peritos técnicos policiales no acarrea nulidad alguna ni puede llevar a excluir del expediente el informe respectivo.*" sosteniendo en este sentido que "*la pericia en cuestión se trata de un medio de prueba "reproducible" (conf. art. 261, 1°párrafo, del C.P.P.N.)*" (Sentencia emanada el 5 de noviembre de 2020 de la Sala B de la Cámara Federal de Mendoza en autos Nº FMZ 52277/2017/10/CA5 caratulados "LEGAJO DE APELACION EN AUTOS BARDINELLA DONOSO, WALTER EDUARDO p/ INFRACCION LEY 23.737").

La Cámara Nacional de Apelaciones en lo Criminal y Correccional - SALA 4 – en el caso "A., J. A. y otros s/ nulidad DET Asociación ilícita y otros" - JCC 53 CCC 81978/2018/11/CA9 de fecha 20 de septiembre de 2019 resolvió: *"Una vez reservado el elemento físico (el teléfono celular), la diligencia encargada para proceder a la copia de los datos acumulados en su interior no constituye una pericia en tanto operación que valore o dictamine en función de una especialidad científica o técnica (artículo 253, a contrario sensu, del CPPN), y por lo tanto la omisión puesta de resalto por los recurrentes no acarrea su invalidez, ya que resulta aplicable el artículo 233 del digesto ritual, que no contiene el requisito en cuestión, y que regula la facultad del juez de obtener copias o reproducciones de las cosas secuestradas".*

1.3. Proceso

1.3.1. Recepción (Punto de control - Mesa de Entradas y Salidas)

1. Los elementos se reciben en las dependencias de la Mesa de Entradas y Salidas del Organismo de Investigaciones ubicadas en las respectivas sedes del Laboratorio Informático Forense. Los elementos se reciben únicamente acompañados de la solicitud modelo[4] (Ver anexo 1) firmada por la autoridad fiscal. El personal del área corrobora que se encuentren correctamente empaquetados, identificados y con su correspondiente cadena de custodia, firmando su recepción.
2. Al momento de la recepción se deberá tener en cuenta:
    1.1. Si la evidencia se encuentra empaquetada de forma que no pueda verse el contenido, o el embalaje no estuviera debidamente cerrado, o hubiera más de un elemento en el embalaje, se procederá a la apertura y constatación de los elementos recibidos, proceso que será filmado y asentado en acta, quedando la filmación al resguardo del OI para que sea requerido por la autoridad fiscal. En este caso también se corrobora que los elementos se encuentren en las condiciones técnicas adecuadas considerando los recaudos y especificaciones detalladas en el Protocolo de identificación, recolección, adquisición y preservación de Evidencia Digital (Ver anexo 2), asegurando que no exista conexión a ninguna red y que se mantenga encendido en caso de que sea necesario.
    1.2. Si los elementos llegan sin cadena de custodia se confecciona una al momento de la recepción y se deja registro en un acta.
    1.3. Si los elementos recibidos no coinciden con lo descripto en la cadena de custodia se elabora un nuevo formulario que se anexa al original, remitiendo el acta correspondiente a la autoridad fiscal que ordenó la extracción, requiriéndole una nueva solicitud para continuar con el procedimiento sobre el elemento recibido.
    1.4. En caso que la evidencia se haya recibido con más de un elemento en un mismo envoltorio, se divide en tantos elementos se hayan recibido, copiando el acta de cadena de custodia para cada uno de ellos, continuando con sobres separados y dejando constancia de este paso y detalle del elemento individualizado en el acta de cadena de custodia que se elabore para cada uno de ellos.
    1.5. Si los elementos provienen de otra institución que no fuera el MPA, con la que no existan convenios de colaboración, se deberá dar ingreso por medio del sistema Panoptes (o el que en un futuro lo reemplace) y remitir a la Dirección Provincial del OI para su aprobación.
3. Se cargan los datos de la solicitud y de los elementos en el sistema de gestión vigente único a nivel provincial. Se toma vista fotográfica de cada uno de los elementos y se les asigna un número de Registro Único de Elementos de Prueba (RUEP) etiquetándolos con dicho número.

4. El modelo de solicitud realizado por el Organismo de Investigaciones forma parte del protocolo de trabajo del LIF y contempla los datos mínimos y necesarios para la extracción de información de los dispositivos móviles. El mismo debe ser utilizado por la totalidad de las autoridades fiscales que soliciten extracciones.

4. El/la responsable del depósito firma la recepción del elemento y lo guarda, con un protocolo de trabajo específico de resguardo de evidencias, hasta el momento de la extracción. (Ver anexo 3).
5. La/el responsable del depósito entrega el elemento al coordinador de personal idóneo, quien firmará su recepción y lo asignará al personal idóneo para la extracción de datos según el orden de ingreso y la disponibilidad de trabajo, salvo las prioridades que determinen los/las fiscales/as regionales en cada caso, quienes se lo comunicarán a la jefatura del LIF.

1.3.2. Extracción (Laboratorio)

1. ***Asignación de personal idóneo para realización de la extracción:*** El Coordinador de personal idóneo encarga la extracción de datos de un elemento a personal idóneo del laboratorio.

   Si al momento de la extracción pasaron más de dos meses desde su ingreso al Laboratorio debe consultar, a través de la Mesa de Entradas y Salidas, a la/el fiscal/a si la causa sigue abierta o es necesario realizar la extracción (parcial o total). En caso de que la causa se haya cerrado o la evidencia haya dejado de ser necesaria se remite el elemento a la Mesa de Entradas y Salidas para su devolución a la autoridad requirente con una nota, dejando constancia en el sistema.
2. **Extracción y Decodificación:** La persona designada procede a:
   2.1. Identificar modelo y detalles técnicos del dispositivo, tomar vistas fotográficas ampliatorias de ser necesario y cargar todos los datos faltantes en el sistema único de gestión.
   2.2. Preparar y configurar el elemento para conectarlo con las medidas de seguridad pertinentes a la herramienta forense según el tipo de dispositivo.
   2.3. Conectar a la herramienta forense y esperar hasta que esta finaliza el proceso de obtención de datos.
   2.4. Decodificar los datos obtenidos con el software forense acorde al dispositivo.
3. **Finalización de la extracción:** Una vez finalizada la extracción, la persona que la realizó debe:
   3.1. Confeccionar y firmar el informe técnico[5] con firma digital (Ver anexo 4).
   3.2. Almacenar en su computadora el trabajo realizado y entregárselo a quien sea responsable de control de calidad, que habiendo revisado el informe se lo hará llegar a la jefatura del Laboratorio, que firmará la remisión a la Unidad Fiscal o autoridad requirente.
   3.3. Remitir digitalmente la extracción realizada o, en caso de no ser posible, solicitar a través de la Mesa de Entradas y Salidas un dispositivo de almacenamiento externo que deberá enviar para tal fin la autoridad requirente, en la que grabará la información correspondiente y se le remite por Mesa de Entradas y Salidas.

5. El informe técnico es un documento de elaboración propia del LIF en el que consta el detalle de los elementos procesados, las herramientas forenses utilizadas para tal fin y los resultados técnicos obtenidos.

Los datos obtenidos se almacenarán digitalmente en el LIF por 90 (noventa) días, transcurrido ese lapso se borrarán.

3.4. Continuar con el registro de pases de la cadena de custodia del elemento con envoltorio propio del OI (dentro del cual debe incluir el anterior envoltorio) y remitir al depósito, cuyo responsable da aviso a la Mesa de Entradas y Salidas.

3.5. En caso que la evidencia se haya recibido con más de un elemento en un mismo envoltorio, se divide en tantos elementos se hayan recibido, copiando el acta de cadena de custodia para cada uno de ellos, continuando con sobres separados y dejando constancia de este paso y detalle del elemento individualizado en el acta de cadena de custodia que se elabore para cada uno de ellos.

1.3.3. Resguardo del dispositivo (Punto de control - Mesa de Entradas y Salidas)

1. La Mesa de entradas y salidas solicita instrucciones a la autoridad requirente sobre el destino del dispositivo. Hasta contar con una respuesta se guarda el mismo en el depósito propio (Ver anexo 3). Si la autoridad requirente considerase que no hay interés en el mantenimiento del dispositivo sólo podrá solicitar que le sea devuelto, en caso contrario debe mantenerse en los depósitos del LIF a fin de que sirva de respaldo de los datos obtenidos.
2. En caso de que el dispositivo haya sido requerido por la autoridad solicitante para su restitución o almacenamiento en otro recinto, a solicitud de la Mesa de Entradas y Salidas la/el responsable del depósito le remite el elemento con la cadena de custodia a dicha autoridad.
3. Al momento de la entrega de los elementos se deja constancia de quien recibe y la documentación respaldatoria se archiva. Este procedimiento se registra en el sistema único de gestión.

2. Solicitud de extracción informática forense

FECHA	
Nº CUIJ/FRO	
FISCAL	
UNIDAD FISCAL	
CARÁTULA	
CONTACTO EN FISCALÍA	

TIPO DE ELEMENTO	MARCA	MODELO	COLOR	ESTADO/ CONDICIÓN	OBSERVACIONES (Incorporar todos los detalles que se cuenten)	ORDEN DE PRIORIDAD (Enumerar)

(Agregar cantidad de filas que considere necesario)

ACLARACIONES:

DVR: indicar franja horaria y días para la extracción. Ej. 4/5/2022 10:00hs a 7/5/2022 20:00hs.

TELÉFONO CELULAR: indicar si posee chip, tarjeta de memoria.

PUNTOS DE INTERÉS - SOLICITUD	Marcar con una cruz
Contactos	
Llamadas telefónicas	
Mensajería: SMS, WhatsApp, Telegram. Signal, Napoleon, Surespot, entre otras	
Redes sociales	
Imágenes	
Videos	
Audios	
Documentos	
Notas	
Historial web	
Ubicaciones geográficas	
Contraseñas	
Elementos eliminados	
Cuentas de correo electrónico	
Aplicaciones/programas instalados	

Espacio para comentarios

Firma y Aclaración

Fiscal/a

3. Guía de procedimientos para la identificación, adquisición, recolección y preservación de evidencia digital

3.1. Glosario

Adquisición: proceso de creación de una copia de los datos contenidos en un dispositivo.

AFU: Por sus siglas en inglés "After First Unlock", se refiere al modo en el que se encuentra un dispositivo cuando un usuario ingresa el código de acceso correcto para el dispositivo después de un reinicio o un evento de encendido.

Autoridad fiscal: fiscal/a a cargo de una investigación penal, quien en el marco de su competencia ordena/requiere el secuestro o realización de una medida vinculada al potencial elemento de prueba.

BFU: Por sus siglas en inglés "Before First Unlock", antes del primer desbloqueo se refiere al modo en el que se encuentra un dispositivo inmediatamente después de reiniciarlo o encenderlo cuando aún no se ha desbloqueado.

Cadena de Custodia: conjunto de procedimientos que deben implementarse para el registro preciso y detallado del camino que siguen los elementos recolectados para ser eventualmente producidos como prueba en el proceso penal.

Caliente/frío: términos utilizados para describir el estado de la seguridad del dispositivo

Criptoactivos: Conjunto de activos digitales no tangibles, basados en la criptografía y la blockchain para su funcionamiento.

Datos no volátiles: todo dato guardado en un dispositivo de almacenamiento masivo que no se pierde o modifica con el correr del tiempo, no necesita alimentación eléctrica para mantenerse guardado.

Datos volátiles: todo dato almacenado en una memoria y que se pierde o borra si el dispositivo deja de tener alimentación eléctrica o si se reinicia.

Evidencia digital: cualquier información que, sujeta a una intervención humana, electrónica y/o informática, haya sido extraída de cualquier clase de medio tecnológico informático (computadoras, celulares, aparatos de video digital, medios ópticos, etc.)

Frases semillas: conjunto de 12 o 24 palabras aleatorias que se utiliza como respaldo de seguridad de las billeteras virtuales.

HASH: función matemática unidireccional e irreversible que convierte datos (archivo o conjunto de ellos, sean texto, ejecutables, de audio, imágenes, videos, etc.) en un identificador alfanumérico de longitud fija. El cálculo de dos tipos de Hash permite verificar la integridad de los datos preservados ante posibles maniobras posteriores de modificación y/o adulteración.

Personal especialista:persona idónea que reúne las condiciones necesarias y óptimas para la función o fin determinado en la materia de la presente guía.

Personal interviniente: personal capacitado y/o autorizado para actuar en el lugar del hecho al realizar el correcto secuestro de los PEPs.

Potencial elemento de prueba (PEP): aquellos dispositivos susceptibles de contener información (representación física), los cuales almacenan potencial evidencia digital (representación lógica).

RAM: por sus siglas en inglés "Random Access Memory", es la memoria a corto plazo de un dispositivo, allí se almacenan los datos que el procesador está utilizando en ese momento.

Recolección: proceso de recoger elementos físicos que contienen potencial evidencia digital.

Rig de minería: conjunto de elementos de hardware instalados y configurados para el minado de criptoactivos.

Secuestro: medida procesal por la cual se procede a la recolección de lo que se hallare en virtud de un allanamiento o de una requisa personal dejando constancia de ello en el acta respectiva y dando cuenta inmediata del procedimiento realizado al juez o fiscal intervinientes. Los elementos de prueba serán recolectados según las reglas aplicables al tipo de objeto, garantizando la cadena de custodia.

Tarjeta SIM: Por su siglas en inglés "Subscriber Identity Module", módulo de identidad del abonado

Triage: proceso de selección de dispositivos o filtrado de información, puede traer aparejada la alteración de datos informáticos. Este proceso debe ser ordenado por la autoridad fiscal y llevado a cabo por personal especializado.

Volcado de memoria RAM: imagen forense de la memoria RAM de un dispositivo encendido, siendo este el único momento en el que se puede ejecutar. A partir del volcado es posible obtener información importante tales como procesos activos, contraseñas, historial de navegación, etc.

Artículos de la Ley Nro. 12.734 Código Procesal Penal de Santa Fe mencionados:

Artículo 110: Validez. Para no ser invalidada la declaración del imputado deberá contar siempre con la presencia de su defensor y, antes de comenzar, se le hará saber que cuenta con el derecho de abstenerse de declarar sin que ello signifique ninguna presunción en su contra.

Artículo 131: Manifestaciones y su documentación. Las manifestaciones personales se recibirán en la forma y modalidad que asegure la cabal intelección de su contenido y la publicidad del juicio.

Artículo 169: Allanamiento. Cuando el registro deba efectuarse en un lugar habitado, casa de negocio o en sus dependencias y siempre que no se contara con la autorización libre y previamente expresada por quien tenga derecho a oponerse, el Tribunal, a solicitud fundada, autorizará el allanamiento.

La medida podrá ser cumplida personalmente por el Tribunal, o en su defecto éste expedirá autorización escrita en favor del Fiscal, o del funcionario judicial o policial a quien se delegue su cumplimiento, y comunicada por cualquier medio, incluso electrónico o informático. Si la diligencia fuera practicada por la Policía será aplicable en lo pertinente el artículo 268 inciso 6) y la diligencia deberá ser filmada desde el inicio del procedimiento. El Tribunal podrá, de manera fundada, eximir el cumplimiento del recaudo de la filmación.

La diligencia deberá autorizarse individualizando los objetos a secuestrar o las personas a detener. En cuanto a los objetos, podrá prescindirse de dicha individualización, dando suficientes razones de tal imposibilidad, brindando todos los detalles conducentes a la misma.

La diligencia sólo podrá comenzar entre las siete (7) y las veintiún (21) horas. Sin embargo, se podrá autorizar a proceder en cualquier hora cuando el interesado o su representante lo consientan, o en los casos graves y que no admitan demora por el riesgo de frustrarse la investigación, o cuando peligre el orden público.

La autorización de allanamiento será exhibida al que habita u ocupa el lugar donde deba efectuarse, o cuando estuviere ausente, a su encargado; a falta de éste, a cualquier persona mayor de edad que se hallare en el lugar, prefiriendo a los familiares del primero. A la persona se le invitará a presenciar el registro.

Cuando no se encontrare a nadie, ello se hará constar en el acta.

Si en el acto se hallaren objetos que presumiblemente estuvieran relacionados a otros hechos delictivos o armas de fuego cuya tenencia no estuviera legalmente justificada, deberán ser secuestrados informando al Tribunal.

Practicado el registro, se consignará en el acta su resultado, con expresión de todas las circunstancias útiles para la investigación.

El acta será firmada por los concurrentes. Si alguien no lo hiciere se expondrá la razón.

La autorización no será necesaria para el registro de los edificios públicos y oficinas administrativas, los establecimientos de reunión o de recreo, el local de las asociaciones, cualquier otro lugar cerrado que no esté destinado a habitación o residencia particular. En estos casos deberá darse aviso a las personas a cuyo cargo estuvieren los locales, salvo que ello fuere perjudicial a la investigación. Cuando para el cumplimiento de sus funciones o por razones de higiene, para prevenir daños ambientales o inundaciones, moralidad u orden público, alguna autoridad nacional, provincial, municipal o comunal competente necesite practicar registros domiciliarios, solicitará directamente al tribunal autorización de allanamiento, expresando los fundamentos del pedido. El tribunal resolverá la solicitud pudiendo requerir que se amplíe la información que se estime pertinente y ordenará los recaudos para su cumplimiento.

Artículo 177: Facultad de abstenerse. Podrán abstenerse de declarar y así serán previamente informados, quienes tengan con el imputado los siguientes vínculos:

cónyuge, ascendientes o descendientes, parientes consanguíneos o por adopción hasta el cuarto grado, y por afinidad hasta el segundo grado.

También podrán hacerlo los periodistas comprendidos en las leyes que reglamentan su actividad profesional sobre el secreto de las fuentes de información periodística, salvo que los interesados en su reserva expresamente los relevaren de guardar secreto.

Artículo 178: Testimonio inadmisible. No podrán ser admitidas como testigos las personas que, respecto del objeto de su declaración, tuvieran el deber de guardar un secreto particular u oficial. En caso de ser citadas, deberán comparecer, explicar el motivo del cual surge la obligación de guardar secreto y abstenerse de declarar.

Artículo 240: Secuestro. El Fiscal de Distrito podrá disponer en caso de urgencia, el secuestro de aquellas cosas relacionadas con el delito, las sujetas a decomiso o las que puedan servir como prueba.

Si mediare peligro en la demora, la medida podrá ser cumplida por la policía.

Se elaborará un acta de la diligencia, de acuerdo a las normas generales.

Las cosas recogidas serán identificadas y conservadas bajo sello, debiéndose adoptar, en todo momento, las medidas necesarias para evitar alteración.

Todo aquél que tenga en su poder objetos o documentos que puedan servir como medio de prueba, estará obligado a presentarlos y entregarlos cuando le sean requeridos, siendo de aplicación las medidas de coacción permitidas para el testigo que rehúsa declarar.

Si los objetos requeridos no son entregados, se dispondrá su secuestro.

Quedan exceptuadas de ésta disposición las personas que deba abstenerse de declarar como testigo.

Con autorización del Fiscal o en su caso, del Tribunal, las partes podrán tener acceso a las cosas secuestradas, a fin de reconocerlas o someterlas a pericia. Se llevará un registro en que conste la identificación de las personas autorizadas.

Serán de aplicación para el secuestro las normas previstas para la requisa y el registro.

Artículo 241: Objetos no sometidos a secuestro.- Sin perjuicio de lo establecido en el artículo 169, no podrán ser objeto de secuestro:

1) las comunicaciones entre el imputado y las personas que deban abstenerse de declarar como testigo;

2) las notas que hubieran tomado los nombrados anteriormente sobre comunicaciones confiadas por el imputado, o sobre cualquier circunstancia a la cual se extienda el derecho o el deber de abstenerse de declarar;

3) los resultados de exámenes o diagnósticos relativos a las ciencias médicas realizadas al imputado bajo secreto profesional.

Artículo 260: Formalidades para actos irreproducibles o definitivos.- Deberán constar en actas debidamente formalizadas, con expresa mención de la fecha, hora, intervinientes, firmas de los funcionarios actuantes y mención de cualquier otro dato útil a la eficiencia y acreditación de la autenticidad del documento, los operativos dirigidos a la búsqueda e incorporación de pruebas, inspecciones, constataciones, registros, requisas, secuestros, aprehensiones, detenciones, reconocimientos y toda otra diligencia que se considerara irreproducible o definitiva.

Las restantes diligencias de la investigación no guardarán otras formalidades que las exigidas por la reglamentación y por las instrucciones generales y especiales expedidas por el Ministerio Público Fiscal, salvo las que tuvieran una formalidad expresamente prevista en este Código.

Artículo 268: Deberes y atribuciones. La Policía investigará bajo dirección del Ministerio Público de la Acusación. Sin perjuicio de ello, deberá investigar todo delito de acción pública que llegue a su conocimiento en razón de su función, por orden fiscal o por denun-

cia, debiendo, en este último caso, comunicar dicho extremo en forma inmediata al Ministerio Público de la Acusación a los fines de recibir directivas.

La Policía tendrá los siguientes deberes y atribuciones:

1) recibir denuncias;

2) requerir la inmediata intervención del Organismo de Investigaciones o, en defecto, de la actuación operante del mismo, practicar sin demora las diligencias necesarias para hacer constar las huellas o rastros del delito, cuando hubiera peligro de que desaparezcan o se borren por retardo de estas diligencias;

3) impedir que los hechos cometidos sean llevados a consecuencias ulteriores e individualizar la evidencia que pueda dar sustento a la acusación;

4) realizar los actos que le encomendara el Fiscal;

5) aprehender, detener e incomunicar a las personas, en los casos que este Código autoriza, informándolo de inmediato al Fiscal. En todos los casos deberá poner a las mismas a disposición del Juez competente dentro de las veinticuatro (24) horas de efectuada la medida;

6) recoger las pruebas y demás antecedentes que pudiera adquirir en el lugar de la ejecución del hecho punible y practicar las diligencias urgentes que se consideraran necesarias para establecer su existencia y determinar los responsables, debiéndose recopilar por separado, en lo posible y de acuerdo a los distintos hechos que se investiguen, las respectivas actuaciones;

7) poner en conocimiento del Fiscal las informaciones y diligencias practicadas, requiriendo su autorización para realizar aquellas medidas probatorias que, por su naturaleza, sean definitivas e irreproducibles, y que deberán colectarse con control de la defensa, si el imputado estuviera individualizado. Si fuera imposible cumplir con estas exigencias ante el inminente peligro de frustración de la medida, la misma, excepcionalmente se realizará con intervención del Juez Comunitario de Pequeñas Causas o certificándose su fidelidad con dos (2) testigos mayores de dieciocho (18) años, hábiles y que no pertenezcan a la repartición, fotografías u otros elementos corroborantes. Si por las especiales circunstancias del caso no fuera posible la presencia de dos (2) testigos, la diligencia tendrá valor con la intervención de uno (1) solo y si ello fuera absolutamente imposible, de cuyas causales deberá dejarse constancia, con dos (2) funcionarios actuantes;

8) disponer que antes de practicarse las averiguaciones y exámenes a que debe procederse, no hubiera alteración alguna en todo lo relativo al hecho y estado del lugar en que fue cometido;

9) proceder a todos los exámenes, indagaciones y pesquisas que juzgara indispensables, recabando los informes y noticias que pudieran servir de utilidad al Fiscal o a la defensa, documentando las declaraciones sólo cuando se estime necesario;

10) secuestrar los instrumentos del delito o cualquier otro elemento que pudiera servir para el objeto de la investigación en caso de urgencia o peligro en la demora. Sin embargo, no podrá imponerse de la correspondencia, papeles privados, material informático y grabaciones que secuestrara, sino que los remitirá intactos al Fiscal competente para que éste requiera autorización al Tribunal;

11) impedir, si lo juzgara conveniente, que ninguna persona se aparte del lugar del hecho o sus adyacencias, antes de concluir las diligencias más urgentes de investigación, con comunicación a la Fiscalía;

12) identificar al imputado;

13) informar al imputado inmediatamente de que fuera citado, aprehendido o detenido, que cuenta con los siguientes derechos:

a. nombrar abogado para que lo asista y represente;

b. conferenciar en forma privada y libre con su defensor, antes de prestar declaración o realizar un acto que requiera su presencia;

c. abstenerse de declarar sin que ello signifique una presunción en su contra, o solicitar ser escuchado por el Fiscal;

d. solicitar del Fiscal la intimación de los hechos que se le atribuyen, la calificación jurídica penal que provisionalmente merezcan y la prueba que existe en su contra;

e. solicitar se practique la prueba que estimara de utilidad. La información precedente le será entregada al imputado por escrito, dejando constancia fehaciente de su entrega. Rige lo dispuesto por el artículo 110;

14) cumplimentar lo necesario para que el imputado sea revisado por el médico, bioquímico o psicólogo, en los casos en que así correspondiera;

15) cumplimentar con la información a enviar al Registro Único de Antecedentes Penales.

3.2. Introducción

El presente documento tiene por objeto determinar pautas y procedimientos a los que deben adecuarse el personal interviniente y responsable en cada etapa de contacto con evidencia digital, manteniendo su integridad y autenticidad. Así como también el conjunto de pasos durante su levantamiento y secuestro (cadena de custodia).

Se entiende a la evidencia digital como cualquier información que, sujeta a una intervención humana, electrónica y/o informática, haya sido extraída de cualquier clase de medio tecnológico informático (computadoras, celulares, aparatos de video digital, medios ópticos, etc.). En términos técnicos es un tipo de evidencia física que está constituida por campos magnéticos y pulsos electrónicos que pueden ser recolectados y analizados con herramientas y técnicas especiales. En términos jurídicos puede cobrar valor probatorio en un proceso penal.

El sistema de Cadena de Custodia representa el conjunto de procedimientos que deben implementarse para el registro preciso y detallado del camino que siguen los elementos recolectados para ser eventualmente producidos como prueba en el proceso penal.

Cada uno de estos medios tecnológicos almacena los datos de distinta forma. Unificar pautas y criterios para su correcta identificación, tratamiento y preservación es fundamental para su aprovechabilidad en el marco de las investigaciones penales y es objeto de la presente guía.

Para su elaboración se toma como marco de referencia el Protocolo para la identificación, recolección, preservación, procesamiento y presentación de evidencia digital del Ministerio de Seguridad de la Nación (2023) y la Norma IRAM-ISO/IEC 27037 “Tecnología de la información. Técnicas de seguridad. Guías para la identificación, la recolección, la adquisición y la preservación de la evidencia digital”.

3.3. Objetivo

- Unificar y estandarizar pautas de actuación para la identificación, recolección, adquisición y preservación de evidencia digital.
- Garantizar la trazabilidad de la evidencia digital recabada en el marco de la investigación penal.
- Asegurar la legalidad y aprovechabilidad de la prueba que se produzca en juicio.

3.4. Alcance

La presente guía es aplicable para quienes intervienen en la investigación penal, identificando, recolectando y adquiriendo evidencia digital.

Los procedimientos descriptos deberán ser aplicados por la Policía de la Provincia de Santa Fe, personal del Organismo de Investigaciones, integrantes de las fuerzas de seguridad nacionales y quien participe colaborando en la investigación penal.

3.5. Principios generales de intervención

- Personal interviniente: Es el responsable de la exploración, localización, identificación y/o recolección de potenciales elementos de prueba (PEPs) que pudieran contener evidencia digital y se encuentren asociados al hecho investigado.
- Recolección, Adquisición, Aseguramiento y Transporte. Estos procesos priorizarán la no modificación de los PEP digitales.
- Documentación de las Actuaciones. Todo lo actuado durante la recolección, adquisición y transporte de los efectos que pudieran ser PEPs digitales debe estar completamente documentado y preservado.

3.6. Identificación, recolección, adquisición y preservación de Evidencia Digital

3.6.1. Intervención inicial

- La recolección y/o adquisición de evidencia digital podrá provenir de la escena del hecho, un procedimiento ordenado por una autoridad fiscal (allanamiento, registro, requisa, etc.); un procedimiento policial (inspección, requisa, aprehensión o detención, etc.); una entrega voluntaria efectuada en el marco de una investigación de un hecho delictivo.
- Resulta aconsejable que la intervención sea posterior a la exploración y levantamiento del PEP de interés papiloscópico y/o químico biológico que pudieran encontrarse sobre los medios tecnológicos informáticos. En tal caso, los especialistas en papiloscopía y en química biológica deberán consultar y acordar con el personal del LIF la aplicación de reactivos que resulten menos dañinos para el dispositivo explorado. Asimismo, en caso de que deban intervenir antes que los otros especialistas, corresponderá hacerlo con el empleo de guantes y la protección adecuada que impida o disminuya lo más posible la alteración o destrucción del PEP que pudieran encontrarse sobre los dispositivos.
- En caso de un procedimiento programado, previamente a su realización se recomienda coordinar con la autoridad fiscal las reglas de intervención en el caso de la existencia de efectos que pudieran contener PEP digitales. Dicha coordinación debería anticipar posibles formas de proceder ante las circunstancias presentadas, tales como posibles triage[6], inspección manual de dispositivos, volcados de memoria RAM, claves de accesos, acceso a datos de la nube, capacidades del personal interviniente, insumos, etc.

6. Proceso de selección de dispositivos o filtrado de información manual, ordenado por autoridad fiscal competente.

- En caso de que el personal interviniente verifique en el lugar del hecho la presencia de PEPs que pudiesen contener potencial evidencia digital, procurará en el acta labrada con las formalidades legales vigentes, con atención a lo estipulado en los artículos 169, 260 y 268, del Código Procesal Penal de Santa Fe (CPPSF), que conste una fijación narrativa, precisa y detallada que suministre una noción clara del lugar donde fueron hallados los medios tecnológicos informáticos, de toda la incidencia que hubiere acontecido durante el procedimiento, el estado en que éstos fueron hallados (encendido/apagado), incluyendo las características identificativas de cada dispositivo (según se detallará en el punto 6).
- Se deberá garantizar que las personas se alejen de los dispositivos y suministros de energía eléctrica. Si es una empresa, identificar al personal informático interno (administradores, programadores, etc.) o a los usuarios de aplicaciones específicas que deban someterse al procedimiento técnico. Dejar registrado el nombre del dueño o usuarios del equipamiento informático ya que luego pueden ser de utilidad para los procedimientos técnicos.
- En caso de considerarlo pertinente, el personal interviniente podrá realizar la consulta remota con el Laboratorio Informático Forense del Organismo de Investigaciones, a los efectos de preservar la información que los PEPs pudieran contener. No se debe interactuar innecesariamente ni buscar información en los mismos, excepto cuando se prevea adquirir datos volátiles o se efectúen operaciones urgentes de triage debiéndose en todos los casos documentar el proceso realizado.
- Cuando los PEP sean muy voluminosos (Ej. Centro de cómputos) o exista excesiva cantidad de ellos en el lugar del hecho y se tenga conocimiento preciso de los datos o clase de datos que se buscan, o se pudieren encontrar afectados derechos de terceros, se recomienda el uso de un triage para precisar el grado de relevancia de cada dispositivo electrónico, previa consulta y autorización con la autoridad fiscal interviniente dejando registro en el acta de procedimiento.
- Recolección de evidencia NO digital: Se deberá poner especial atención en determinar quién o quiénes son los usuarios de los dispositivos. De la misma manera, al momento del procedimiento, se deberá prestar atención a la presencia de anotaciones, papeles, credenciales de usuario, contraseñas, direcciones de criptoactivos, claves privadas, frases semilla y otros elementos de interés. Se recomienda buscar elementos, como notas adhesivas, papeles, computadoras, manuales de software y hardware, etc, detalles de relevancia sobre los dispositivos, como contraseñas o PIN.

  También se puede entrevistar a personas (administrador de sistemas, usuarios, dueños de dispositivos, etc.), que puedan tener información útil o pertinente sobre la potencial evidencia digital o los dispositivos digitales a recolectar, teniendo en cuenta las previsiones de los artículos 110, 131, 169, 177, 178, 240, 241 y 268 del CPPSF. Se puede pedir información tal como la configuración del sistema, contraseña de administrador, etc., haciendo saber sus derechos al entrevistado en. Esta información puede ser útil en la etapa de análisis de la potencial evidencia digital. Se recomienda documentar estas conversaciones para garantizar que los detalles son exactos y las declaraciones documentadas no se pueden modificar.

3.6.2. Recolección y adquisición de PEPs

La potencial evidencia digital puede ser adquirida o recolectada. Para decidir si llevar a cabo uno u otro procedimiento se debe tener en cuenta ciertos factores, entre los cuales podemos enumerar:

1. La volatilidad de la potencial evidencia digital.
2. Encontrar discos o particiones cifradas, cuando la clave del mismo puede encontrarse en la memoria RAM de dicho dispositivo.
3. La criticidad del sistema, cuando son indispensables para el correcto funcionamiento del lugar.
4. Recursos necesarios como la capacidad de almacenamiento requerido, el tiempo necesario para llevar a cabo cada proceso, personal disponible, etc.

Tanto la recolección como la adquisición, seguirá pasos distintos si el dispositivo se encuentra encendido o apagado (en el apartado de Procedimientos Específicos por tipo de dispositivo electrónico se explicará en detalle).

3.6.2.1. Recolección

Por recolección se entiende el proceso de recoger y secuestrar elementos físicos que contienen potencial evidencia digital. Se deben realizar procedimientos específicos por cada tipo de dispositivo, estos se describen en el punto 6.

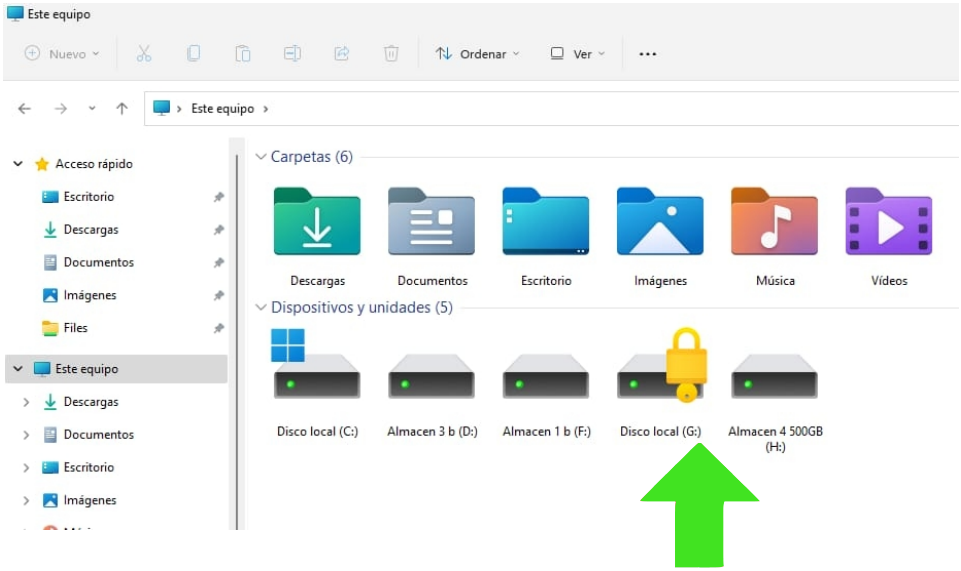
3.6.2.2. Adquisición

Por adquisición se concibe al proceso de creación de una copia de los datos dentro de un conjunto definido. Es posible realizar este procedimiento en computadoras portátiles, equipos informáticos de escritorio, equipos servidores y equipos de imagen y video.

3.6.2.2.1. Consideraciones generales

Este procedimiento debe ser realizado por personal con conocimiento en materia informática. Se aconseja garantizar la adquisición de los datos volátiles y en vivo antes de proceder a la recolección .

También se debe considerar la adquisición de datos volátiles en la RAM cuando se sospecha el uso de cifrado. En ese caso el cifrado de un dispositivo se puede detectar ingresando desde el menú del elemento a secuestrar, desde “este equipo” y observar si figura sobre algún disco un candado, como se muestra en el siguiente gráfico:



3.6.2.2.2. Escenarios Posibles al momento de realizar una adquisición de datos:

Se debe tener en cuenta para el caso de la adquisición tres escenarios diferentes:

A. Dispositivos digitales encendidos.

En este caso se recomienda, adquirir la potencial evidencia digital cuando se sospeche que se pueda perder información valiosa al apagar el dispositivo o cuando se sospecha el uso de cifrado de la información.

Cuando es necesario adquirir datos no volátiles del dispositivo que continúan en ejecución, se recomienda considerar la adquisición sobre un sistema encendido; en estos casos es necesario realizar una adquisición en vivo, la cuál se realizará siempre utilizando una herramienta para la obtención de la copia forense.

La adquisición en vivo de datos volátiles en RAM -como procesos en ejecución, conexiones de red, configuraciones de fecha/hora, estados de las aplicaciones y las contraseñas descifradas, etc- se deben guardar en un medio de almacenamiento digital que haya sido preparado previamente para tal fin, es decir formateado, al cual luego se le calculará el algoritmo HASH.

En caso de no estar formateado el dispositivo de almacenamiento digital, se procederá a la utilización de un contenedor como un archivo ZIP, al cual luego se le calculará el algoritmo HASH.

B. Dispositivos digitales apagados

La adquisición de datos en dispositivos apagados se lleva a cabo realizando una copia del disco de almacenamiento con una herramienta forense, que copia los datos y genera un HASH automáticamente.

C. Dispositivos encendidos que no pueden ser apagados

Cuando los dispositivos digitales no se pueden apagar debido a la naturaleza crítica de los sistemas, como servidores, sistemas médicos, sistemas de vigilancia, etc. recomendamos tener cuidados especiales y realizar adquisiciones parciales en estos casos. Existen ocasiones en la que es necesario la adquisición parcial de la información, las razones pueden ser las siguientes:

a) El sistema de almacenamiento es demasiado grande para adquirirlo (por ejemplo, servidor de base de datos);

b) El sistema es demasiado crítico para apagarlo;

c) El dispositivo para la adquisición contiene otros datos no pertinentes dentro del mismo sistema; o

d) Existe una restricción por parte de una autoridad legal tal como una orden de allanamiento que limite el alcance de la adquisición.

En todos los casos enumerados se deberá dejar registro documentado del procedimiento realizado y almacenar los datos obtenidos en los dispositivos de almacenamiento oportunamente suministrados por la autoridad fiscal interviniente con el HASH correspondiente.

3.6.3. Preservación de la PEPs: embalaje, cadena de custodia y traslado.

Los elementos recolectados y/o adquisiciones realizadas deben ser correctamente embalados, identificados con su correspondiente cadena de custodia para su posterior traslado.

3.6.3.1. Embalaje o envoltorio

Cada elemento que se haya recolectado debe preservarse en un embalaje o envoltorio individual preferentemente transparente, según la naturaleza y características del mismo.

Los PEPs deben quedar completamente cerrados, lacrados e identificados y firma de los actuantes sobre las cintas de embalaje (si el empaque lo permite), sin roturas o alteraciones, borraduras, tachaduras o cualquier situación que produzca ilegibilidad de las letras o el nombre.

Por cada uno de los embalajes y/o envoltorios se debe confeccionar un formulario de cadena de custodia tal como se detalla en el punto siguiente.

En relación a las computadoras portátiles o equipos informáticos de escritorio el embalaje se realizará fajando o clausurando todos los puertos por donde pueda ingresar o egresar información y/o energía, con cintas adhesivas, papel adhesivo, o elementos que el personal interviniente disponga, y que asegure tal medida. Se deberá prestar atención también a no dejar posibles accesos con tornillos.

3.6.3.2. Cadena de Custodia

Se debe utilizar el formulario de cadena de custodia previsto por las autoridades del Ministerio Público de la Acusación

Se recomienda que el registro de la cadena de custodia contenga, como mínimo, la información siguiente:

- un identificador único de evidencia;
- quién accedió a la evidencia, en qué momento y en qué lugar;
- nombre de el/la propietaria/o del PEP si se conoce;
- características físicas, técnicas según se detallan en el apartado 6.
- estado de conservación;
- si se incluyen las claves de acceso, las cuales no deben estar visiblemente expuestas;
- cualquier cambio inevitable en la potencial evidencia digital, así como el nombre de la persona responsable y la justificación para la introducción del cambio.

3.6.4. Traslado

Una vez terminado el proceso de recolección o adquisición y confeccionado el formulario de cadena de custodia, el PEP debe ser trasladado. Para ello, deberán tenerse en cuenta los recaudos de seguridad que permitan su adecuada protección. En caso de que por cuestiones accidentales o imprevistas, el PEP recolectado sufriera alguna alteración durante su traslado, el responsable deberá dejar constancia de tal evento y realizar un acta explicando lo sucedido, la que deberá adjuntarse al formulario de cadena de custodia.

3.7. Procedimientos específicos de recolección por tipos de dispositivos electrónicos

3.7.1. Dispositivos móviles

Pasos a seguir:

1. Si el dispositivo se encuentra apagado, dejarlo apagado, si se encuentra encendido, dejarlo encendido.
2. Se recomienda, una vez identificados los mismos, si se observa que el dispositivo se encuentra encendido (CALIENTE/AFU[7]), no apagarlo, procurando realizar los procedimientos detallados a continuación:
   2.1. Ponerlo en modo avión.
   2.2. En caso de no ser posible activar el modo avión, se debe sacar la tarjeta SIM, adjuntarla a la carcasa del equipo al cual pertenece con cinta transparente y hacerlo constar en cadena de custodia y acta de procedimiento, de esta forma se logra que el equipo no tenga comunicaciones entrantes y salientes.

7. After First Unlock: Se refiere al modo en el que se encuentra un dispositivo cuando un usuario ingresa el código de acceso correcto para el dispositivo después de un reinicio o un evento de encendido.

2.3. Cuando haya resultado imposible poner el dispositivo en modo avión o retirar la tarjeta SIM (ejemplo SIM Virtual), se procederá a envolver el dispositivo en papel aluminio, aconsejando dar mínimo cinco vueltas al elemento, para evitar todo tipo de señales.

2.4. Registrar la numeración y logo visibles en el exterior de la tarjeta SIM (ICCID[8]).

2.5. En caso de observarse más de un slot o ranura de SIM en el dispositivo, identificar y registrar el slot o ranura en el que se encontraban colocadas cada una de las tarjetas SIM.

2.6. Identificar el IMEI del dispositivo telefónico de ser posible, caso contrario, registrar "IMEI no visible / ilegible".

2.7. Identificar marca y modelo técnico del dispositivo de ser posible, caso contrario registrar "Marca/Modelo Técnico No visible".

2.8. Identificar Número de Serie si es visible.

2.9. De existir Tarjeta de Memoria consignar el tipo, capacidad e inscripción observada. En caso de no existir, registrar "No Posee Tarjeta de Memoria".

2.10. Registrar el estado de conservación del dispositivo, detallando cómo se encuentra el mismo, por ejemplo, pantalla dañada, sin batería, etc.

3. Si el personal especializado recomienda mantener el dispositivo encendido, con disponibilidad de los medios necesarios, se procurará conservar el dispositivo encendido manteniendo la carga del mismo con un powerbank (batería portátil), utilizando el método de aislamiento antes mencionado. En caso de no poseer este medio, se le dará prioridad para enviar al LIF, debiendo hacer saber de la necesidad de mantener el dispositivo con carga permanente dentro del laboratorio y mantener todas las medidas de seguridad pertinentes para evitar conexiones que afecten su integridad, hasta que se determine el procedimiento que se llevará a cabo con el dispositivo.

4. Si el dispositivo está apagado (FRIO-BFU[9]), se realizan los pasos detallados anteriormente el 2.2 y del 2.4 al 2.10 inclusive.

5. Si al momento del secuestro, algún usuario desea informar de forma voluntaria la/las clave/s del dispositivo, para ayudar en la etapa forense, la/las misma/s deben consignarse en el acta labrada oportunamente así como también al momento del empaquetado se deberá adjuntar un papel con la información suministrada de forma que el mismo no se encuentre visible. En la cadena de custodia se debe dejar constancia de que dentro del envoltorio se cuenta con la clave suministrada. El uso de las claves deberá ser acordado con la autoridad fiscal y debidamente registrado.

3.7.2. Computadora portátil o equipo informático de escritorio

Pasos a seguir:

1. Si el dispositivo está encendido se procederá a realizar los siguientes pasos:

8. El ICCID (Integrated Circuit Card ID) es una cadena de dígitos única que identifica una tarjeta SIM.
9. Before First Unlock: Antes del primer desbloqueo se refiere al modo en el que se encuentra un dispositivo inmediatamente después de reiniciarlo o encenderlo cuando aún no se ha desbloqueado.

1.1. De requerirse y de ser necesario, aislar el equipo de las redes y conexiones entrantes/salientes (Desconectar cable de red, desconectar wifi y bluetooth).

1.2. Si el monitor está encendido, registrar fotográficamente la pantalla y documentar la información que se observa, en especial documentar la fecha y hora del Sistema Operativo.

1.3. Si el monitor está encendido, pero visualiza el protector de pantalla, desplazar ligeramente el mouse (sin tocar ningún botón).

1.4. En caso de ser un equipo informático de escritorio encendido pero con el monitor apagado, se debe encender y registrar fotográficamente lo que se visualiza.

1.5. Si en algún caso el equipo estuviera encendido y bloqueado con contraseña, documentar también el usuario visible en la pantalla.

2. Los dispositivos deben apagarse a través de la interrupción del suministro energético. Si se trata de computadoras portátiles, se recomienda, primero quitar la batería y luego desconectar la fuente de energía. En dispositivos con batería integrada, se debe realizar un apagado forzoso, manteniendo presionado 10 (diez) segundos el botón de encendido. No se debe presionar una vez, esto se recomienda debido a que la acción de presionar el botón de encendido en un dispositivo digital puede ser configurada para iniciar una rutina que borre información del sistema antes de apagarse. Si el dispositivo está conectado a un Sistema de Alimentación Ininterrumpida, se debe desenchufar primero el suministro de energía eléctrica desde el dispositivo.

3. No se deben secuestrar monitores, teclados, mouses o cables. Solo se procederá al secuestro del cargador de las computadoras portátiles, que deberá ser embalado junto al dispositivo.

4. Antes del embalaje se debe:

4.1. Corroborar que las bandejas de las unidades de CD o DVD se encuentren retraídas correctamente: registrar si las bandejas de estas unidades se encuentran vacías, contienen discos o no; y encintar la ranura de la unidad cerrada para evitar que se abra.

4.2. Asegurar que no se encuentren conectados medios digitales, tales como pendrive, memorias, discos externos, etc. En ese caso proceder a recolectarlos de manera apropiada, tal como se indica en la presente guía.

3.7.3. Equipos servidores

Pasos a seguir:

1. En caso que el equipo se encuentre encendido, y se haya ordenado el secuestro, se procederá de igual forma que una computadora de escritorio. Es recomendable evaluar previamente si los servicios que corren en los servidores a secuestrar son críticos y qué posibles consecuencias puede generar su indisponibilidad, debiendo informar esto a la autoridad fiscal.

2. En caso que el equipo se encuentre apagado, y la orden sea el secuestro, se procederá al embalaje, rotulado y confección de cadena de custodia, de igual forma que un equipo informático de escritorio.
3. En caso que el equipo se encuentre encendido, y la orden judicial indique la copia de información específica se debe realizar siguiendo las indicaciones del punto 5.2.1.

3.7.4. Equipos de imagen y video

1. El personal interviniente deberá identificar el sistema de video, y determinar el lugar de almacenamiento, ya sea localmente (en un DVR, computadora, memoria extraíble, u otra unidad de almacenamiento), o de manera remota a través de internet (cámaras IP).
2. Identificar fecha y hora de la configuración de sistema de video.
3. En el caso que el dispositivo se encuentre encendido, proceder a desconectar el cable de alimentación de energía, y proceder a su secuestro.
4. En caso de ser un DVR, introducirlo en una caja, bolsa o sobre, fajada y firmada por el personal interviniente y los testigos.
5. En el caso de ser un equipo de computación, proceder a fajar o clausurar todos los puertos por donde pueda ingresar o egresar información, energía, y elementos que permitan su desarmado (tapas), con cintas adhesivas, papel adhesivo, o elementos que el personal interviniente disponga, a fin de asegurar la medida.
6. En caso de ser un disco rígido, colocarlo dentro de una caja u elemento, que asegure que éste no se dañe en su traslado. El elemento contenedor debe estar fajado y firmado por el personal interviniente y los testigos.
7. En casos que la autoridad fiscal lo ordene, el personal especialista procederá al volcado “en caliente” de los videos solicitados siguiendo los pasos de adquisición detallados en el punto 5.2.1.

3.7.5. Redes informáticas

Pasos a seguir:

1. A fin de minimizar posibles daños, tales como interrupciones en servicios críticos, se recomienda realizar un relevamiento de las conexiones críticas ligadas a la arquitectura de la red. Dicha labor debe ser realizada por personal especialista.
2. Si durante el procedimiento fuera de interés de la autoridad fiscal identificar datos relevantes de las redes informáticas (IP Privada, IP Pública, arquitectura de red, etc.), dicha labor debe ser realizada por personal especialista.
3. En el caso de no ser necesaria la actividad del punto anterior, se recomienda desconectar la alimentación de los routers y repetidores al inicio del procedimiento a fin de evitar accesos remotos indeseables. Dicha labor puede ser realizada por el personal interviniente.

3.7.6. Criptoactivos

Pasos a seguir:

1. Al momento del allanamiento se debe prestar atención a la presencia de billeteras frías (aspecto similar a un pendrive), como así a anotaciones con palabras claves, frases semillas, códigos QR, etc., que puedan estar asociadas a wallets/billeteras virtuales.
2. Ante la presencia de indicadores o identificadores propios de actividades ligadas a los criptoactivos se deberá realizar consulta con la autoridad fiscal, quién determinará el criterio a adoptar.

3.7.7. Rig de minería

Pasos a seguir:

1. Los rigs de minería pueden presentar distintos aspectos de acuerdo a su tecnología.
2. En la actualidad, lo más común es utilizar placas de video (GPU) o un hardware dedicado a un algoritmo en particular conocidos como ASIC. Debe considerarse que algunos rigs de minería representan un alto valor monetario, por lo cual su detección durante un procedimiento debe ser informada a la autoridad fiscal para la evaluación de su secuestro.
3. En caso de encontrarse en un allanamiento con equipos de minería (rig de minería), el personal interviniente coordinará con la autoridad fiscal y con el personal especialista y/o experimentado en criptoactivos del Organismo de Investigaciones cómo proceder.
4. En los casos en los que la autoridad fiscal ordene el secuestro, se procederá de igual forma que con un equipo informático encendido.

3.7.8. Tarjetas SIM/USIM

En caso de encontrar tarjetas SIM fuera de algún dispositivo electrónico, también pueden ser recolectadas, ya que son un dispositivo de almacenamiento y pueden contener mensajes de texto plano, llamadas y/o contactos.

Para su recolección se debe identificar y registrar la numeración (ICCID) y logo visibles en el exterior de la tarjeta tanto en el acta de procedimiento como en la cadena de custodia.

3.7.9. Medios de almacenamiento digital

Pendrive, Discos externos, SSD, Tarjetas de memoria SD, MP3, etc. Podemos encontrar distintos tipos de medios de almacenamiento digital en el lugar del incidente. Se debe comprobar y documentar la ubicación de cada medio de almacenamiento digital hallado. Por ejemplo, chequear bahías de discos, ranuras USB en computadoras, etc.

3.8. Anexo

3.8.1. Lista de verificación - Recolección de dispositivos móviles

Encendido		Apagado	

ENCENDIDO

1. Activar modo avión

1.1. Si		1.2. No	
En caso 1.1 pasar a punto 3.		En caso 1.2. continuar con punto 2.	

2. Extracción tarjeta SIM

2.1. Si		2.2. No	
	Registrar numeración y logo de la tarjeta.	En caso 2.2. envolver en papel aluminio, pero antes realizar puntos del 3 al 8.	
	Identificar y registrar el slot o ranura en el que se encontraban colocadas cada una de las tarjetas SIM.		
	Adherir la Tarjeta SIM al dispositivo con una cinta transparente.		

3. Identificación IMEI

Si		No	

4. Identificación Marca/modelo técnico

Si		No	

5. Identificación número de serie

Si		No	

6. Tarjeta de memoria

Si		No	

7. Recomendación de mantener el dispositivo encendido

Si		No	

8. Se aporta clave

Si		No	

APAGADO

1. Extracción tarjeta SIM

2.1. Si		2.2. No	
	Registrar numeración y logo de la tarjeta.	En caso 2.2. envolver en papel aluminio, pero antes realizar puntos del 3 al 8.	
	Identificar y registrar el slot o ranura en el que se encontraban colocadas cada una de las tarjetas SIM.		
	Adherir la Tarjeta SIM al dispositivo con una cinta transparente.		

3. Identificación IMEI

Si		No	

4. Identificación Marca/modelo técnico

Si		No	

5. Identificación número de serie

Si		No	

6. Tarjeta de memoria

Si		No	

7. Se aporta clave

Si		No	

Preservación. Procedimiento para dispositivos ENCENDIDOS y APAGADOS.

- Embalaje en bolsa transparente individual.
- Confección de la cadena de custodia incluyendo los siguientes datos:
  - un identificador único de evidencia;
  - quién accedió a la evidencia, en qué momento y en qué lugar;
  - nombre de el/la propietaria/o del si se conoce;
  - tarjeta SIM
  - IMEI
  - marca/modelo técnico
  - número de serie
  - tarjeta de memoria

- estado de conservación
- si se incluyen las claves de acceso, las cuales no deben estar visiblemente expuestas.

3.8.2. Lista de verificación - Computadora portátil o equipo informático de escritorio

Adquisición		Recolección	
Proceso de creación de una copia de los datos dentro de un conjunto definido.		Proceso de recoger y secuestrar elementos físicos que contienen potencial evidencia digital.	

ADQUISICIÓN

1. Escenarios

1.1. Equipos encendidos	
1.2. Equipos apagados	
1.3. Equipos que no pueden ser apagados	

Pasos a seguir:

- Copia forense
- Hasheado
- Almacenamiento de la copia en un dispositivo de almacenamiento
- Confección de la cadena de custodia del disco incluyendo los siguientes datos:
  - un identificador único de evidencia;
  - quién accedió a la evidencia, en qué momento y en qué lugar;
  - nombre de el/la propietaria/o del sí se conoce;
  - marca visible, modelo, número de serie;
  - detalle del contenido del disco.

RECOLECCIÓN

Encendido		Apagado	

ENCENDIDO

- De requerirse aislar el equipo de las redes y conexiones entrantes/salientes (Desconectar cable de red, desconectar wifi y bluetooth).
- Registro fotográfico de la pantalla del monitor.
- Apagado:
  - Equipos de escritorio: interrupción del suministro energético.
  - Computadoras portátiles: primero quitar la batería y luego desconectar la fuente de energía.

    - Dispositivos con batería integrada: realizar un apagado forzoso manteniendo presionado 10 (diez) segundos el botón de encendido.
    - Dispositivo conectado a un Sistema de Alimentación Ininterrumpida: desenchufar primero el suministro de energía eléctrica desde el dispositivo.
- Corroborar que las bandejas de las unidades de CD o DVD se encuentren retraídas.
- Asegurar que no se encuentren conectados medios digitales, tales como pendrive, memorias, discos externos, etc.
- Embalar los dispositivos fajando o clausurando todos los puertos por donde pueda ingresar o egresar información y/o energía. Prestar atención también a no dejar posibles accesos con tornillos.
    - Equipos de escritorio: solo se secuestra y se embala el CPU
    - Computadoras portátiles: secuestrar y embalar junto al cargador.
- Confección de la cadena de custodia incluyendo los siguientes datos:
    - un identificador único de evidencia;
    - quién accedió a la evidencia, en qué momento y en qué lugar;
    - nombre de el/la propietaria/o del sí se conoce;
    - marca visible, modelo, número de serie;
    - estado de conservación;
    - si se incluyen las claves de acceso, las cuales no deben estar visiblemente expuestas.

APAGADO

- Desconectar los cables de alimentación y de red.
- Corroborar que las bandejas de las unidades de CD o DVD se encuentren retraídas.
- Asegurar que no se encuentren conectados medios digitales, tales como pendrive, memorias, discos externos, etc.
- Embalar los dispositivos fajando o clausurando todos los puertos por donde pueda ingresar o egresar información y/o energía. Prestar atención también a no dejar posibles accesos con tornillos.
- Confección de la cadena de custodia incluyendo los siguientes datos:
    - un identificador único de evidencia;
    - quién accedió a la evidencia, en qué momento y en qué lugar;
    - nombre de el/la propietaria/o del sí se conoce;
    - marca visible, modelo, número de serie;
    - estado de conservación;
    - si se incluyen las claves de acceso, las cuales no deben estar visiblemente expuestas.

3.8.3. Lista de verificación - Equipos servidores

Adquisición		Recolección	
Proceso de creación de una copia de los datos dentro de un conjunto definido.		Proceso de recoger y secuestrar elementos físicos que contienen potencial evidencia digital.	

ADQUISICIÓN

1. Escenarios

1.1. Equipos encendidos	
1.2. Equipos apagados	
1.3. Equipos que no pueden ser apagados	

Pasos a seguir:

- Copia forense
- Hasheado
- Almacenamiento de la copia en un dispositivo de almacenamiento
- Confección de la cadena de custodia del disco incluyendo los siguientes datos:
  - un identificador único de evidencia;
  - quién accedió a la evidencia, en qué momento y en qué lugar;
  - detalle del contenido;
  - marca visible, modelo, número de serie;
  - detalle del contenido del disco.

RECOLECCIÓN

Encendido		Apagado	

ENCENDIDO

- Apagado del dispositivo a partir de la interrupción del suministro energético.
- Embalar fajando o clausurando todos los puertos por donde pueda ingresar o egresar información y/o energía. Prestar atención también a no dejar posibles accesos con tornillos.
- Confección de la cadena de custodia incluyendo los siguientes datos:
  - un identificador único de evidencia;
  - quién accedió a la evidencia, en qué momento y en qué lugar;

- nombre de el/la propietaria/o del sí se conoce;
- marca visible, modelo, número de serie;
- estado de conservación;

APAGADO

- Desconectar los cables de alimentación y de red.
- Embalar fajando o clausurando todos los puertos por donde pueda ingresar o egresar información y/o energía. Prestar atención también a no dejar posibles accesos con tornillos.
- Confección de la cadena de custodia incluyendo los siguientes datos:
  - un identificador único de evidencia;
  - quién accedió a la evidencia, en qué momento y en qué lugar;
  - nombre de el/la propietaria/o del sí se conoce;
  - marca visible, modelo, número de serie;
  - estado de conservación;

3.8.4. Lista de verificación - Equipos de imagen y video

Adquisición		Recolección	
Proceso de creación de una copia de los datos dentro de un conjunto definido.		Proceso de recoger y secuestrar elementos físicos que contienen potencial evidencia digital.	

ADQUISICIÓN

1. Escenarios

1.1. Equipos encendidos	

Pasos a seguir:

- Copia forense
- Hasheado
- Almacenamiento de la copia en un dispositivo de almacenamiento
- Confección de la cadena de custodia del disco incluyendo los siguientes datos:
  - un identificador único de evidencia;
  - quién accedió a la evidencia, en qué momento y en qué lugar;
  - nombre de el/la propietaria/o del sí se conoce;
  - marca visible, modelo, número de serie;
  - detalle del contenido del disco.

RECOLECCIÓN

Encendido		Apagado	

ENCENDIDO

- Identificación de fecha y hora de la configuración de sistema de video.
- Apagado del dispositivo a partir de la interrupción del suministro energético.
- Embalar fajando o clausurando todos los puertos por donde pueda ingresar o egresar información y/o energía. Prestar atención también a no dejar posibles accesos con tornillos.
- Equipos de escritorio: solo se secuestra y se embala el CPU
- Computadoras portátiles: secuestrar y embalar junto al cargador.
- Confección de la cadena de custodia incluyendo los siguientes datos:
  - un identificador único de evidencia;
  - quién accedió a la evidencia, en qué momento y en qué lugar;

- nombre de el/la propietaria/o del sí se conoce;
- marca visible, modelo, número de serie;
- estado de conservación;

APAGADO

- Desconectar los cables de alimentación y de red.
- Embalar fajando o clausurando todos los puertos por donde pueda ingresar o egresar información y/o energía. Prestar atención también a no dejar posibles accesos con tornillos.
- Confección de la cadena de custodia incluyendo los siguientes datos:
  - un identificador único de evidencia;
  - quién accedió a la evidencia, en qué momento y en qué lugar;
  - nombre de el/la propietaria/o del sí se conoce;
  - marca visible, modelo, número de serie;
  - estado de conservación;

3.8.5. Lista de verificación -Tarjetas SIM/USIM

Preservación

- Embalaje en bolsa transparente individual.
- Confección de la cadena de custodia incluyendo los siguientes datos:
  - un identificador único de evidencia;
  - quién accedió a la evidencia, en qué momento y en qué lugar;
  - nombre de el/la propietaria/o del sí se conoce;
  - marca visible, modelo, número identificador
  - estado de conservación;

3.8.6. Lista de verificación -Medios de almacenamiento digital

Pendrive, Discos externos, SSD, Tarjetas de memoria SD, MP3.

Preservación

A) Embalaje en bolsa transparente individual.
B) Confección de la cadena de custodia incluyendo los siguientes datos:
    - un identificador único de evidencia;
    - quién accedió a la evidencia, en qué momento y en qué lugar;
    - nombre de el/la propietaria/o del sí se conoce;
    - marca visible, modelo, número de serie;
    - estado de conservación;

4. Depósito laboratorio informático forense (LIF)

4.1. Protocolo de resguardo de evidencias

Objetivo: Establecer pautas y procedimientos para la administración segura y eficiente de dispositivos electrónicos en resguardo del Laboratorio Informático Forense dependiente de Organismo de Investigaciones.

Responsable: Personal del área de administración (s/ la propuesta Secretaría de Gestión) del LIF que se designe para desarrollar las tareas específicas de depósito y archivo de acuerdo con las pautas establecidas en el presente protocolo, las cuales serán las únicas personas autorizadas para el ingreso y la gestión.

Organización: El depósito se encuentra dividido en dos secciones que se corresponden con las etapas del proceso de trabajo del LIF: depósito transitorio y depósito de resguardo

Depósito transitorio: se alojan allí los dispositivos electrónicos ingresados al LIF por Mesa de Entradas que se encuentran a la espera de ser procesados en el área forense.

Depósito de resguardo: se alojan allí los dispositivos electrónicos que fueron procesados por el área de informática forense y se encuentran al resguardo y/o como respaldo de los datos obtenidos hasta la espera de una instrucción de la autoridad fiscal requirente.

4.1.1. Pautas de Trabajo para el personal del Depósito del LIF:

a) **Recepción de Dispositivos Electrónicos:**
   - Registrar en un sistema único la recepción de los dispositivos electrónicos.
   - Establecer criterios de identificación interna para facilitar su seguimiento y ubicación.

b) **Almacenamiento Seguro:**
   - Almacenar los dispositivos electrónicos en un área especialmente designada y segura según su estado (tránsito o resguardo).
   - Cumplir con los requisitos legales y de seguridad, incluyendo medidas de protección contra incendios y acceso no autorizado. Se procurará contar con registros fílmicos del área.
   - Evitar el ingreso a todo personal ajeno a la mencionada área, en caso de ser necesario labores de limpieza y mantenimiento por terceros los mismos deberán ser supervisados por el/la responsable del depósito.

- El Depósito deberá permanecer bajo llave y las mismas se encontrarán en poder de las/los responsables y en caso de ausencia el Jefe/a del Laboratorio Informático Forense designará otra/o responsable.
- Mantener un registro de inventario actualizado con detalles de la ubicación de cada dispositivo.

c) Mantenimiento de la Cadena de Custodia:

- Dejar registro en la cadena de custodia del paso por el depósito (entrada y salida), garantizando la trazabilidad del elemento.

d) Comunicación:

- Mantener una comunicación regular y confidencial entre las áreas del Laboratorio y en caso de ser necesario con la autoridad fiscal requirente.
- Entrega de Dispositivos Electrónicos:
- Registrar y documentar todas las actividades relacionadas con la entrega de dispositivos.

e) Auditorías Internas:

- Realizar auditorías periódicas y revisiones internas para garantizar el cumplimiento de los procedimientos y la integridad de los dispositivos electrónicos almacenados.