2023

-

Protocolo para la identificación, recolección, preservación, procesamiento y presentación de evidencia digital

Argentina

Ministerio Público Fiscal

Ministerio de Seguridad

El crecimiento exponencial y el carácter dinámico que reviste el ciberdelito, hace necesario actualizar las prácticas de intervención por parte de los cuerpos forenses para la realización de la labor científico pericial; han tornado fundamental la preservación de la evidencia digital para que luego se conviertan en prueba dentro de un proceso legal en el cual se deben aplicar técnicas científicas y analíticas especializadas que permiten identificar, preservar, analizar y presentar los datos e información obtenida de los dispositivos analizados

En este contexto es necesario complementar, actualizar y fortalecer los protocolos de actuación ya existentes como premisa básica para la mejora continua de los procedimientos de las fuerzas de ley.

En este contexto, el Ministerio de Seguridad, sancionó mediante la Resolución Nº 75/22 el "Plan Federal de Prevención de Delitos Tecnológicos (2021 - 2024)" el cual posee como una de sus líneas de acción prioritaria la elaboración y actualización de protocolos en técnicas de detección, investigación, preservación de pruebas, cadena de custodia y forense.

Asimismo, mediante la Resolución N° 86/22 se creó en el ámbito de la UNIDAD DE GABINETE DE ASESORES del MINISTERIO DE SEGURIDAD, el "PROGRAMA DE FORTALECIMIENTO EN CIBERSEGURIDAD Y EN INVESTIGACION DEL CIBERCRIMEN (FORCIC)" el cual tiene entre sus objetivos el incremento de las capacidades de prevención, detección y análisis de incidentes cibernéticos, de las capacidades de prevención, detección e investigación del ciberdelito y el incremento de la capacidad de respuesta en el marco de las actividades de investigación de las áreas específicas de ciberdelito dependientes de las fuerzas de seguridad y policiales.

Por estas razones, la DIRECCIÓN DE INVESTIGACIONES DEL CIBERDELITO del **MINISTERIO DE SEGURIDAD**, elaboró, en forma conjunta con las áreas específicas de la POLICIA FEDERAL ARGENTINA, la GENDARMERÍA NACIONAL ARGENTINA, la PREFECTURA NAVAL ARGENTINA y la POLICÍA DE SEGURIDAD AEROPORTUARIA - y personal del **MINISTERIO PUBLICO FISCAL DE LA NACION**, conformado por LA SECRETARÍA DE COORDINACIÓN INSTITUCIONAL, la DIRECCIÓN DE APOYO TECNOLÓGICO A LA INVESTIGACIÓN PENAL -DATIP- y la UNIDAD FISCAL ESPECIALIZADA EN CIBERDELINCUENCIA -UFECI-,un protocolo único de actuación, para la identificación, recolección, preservación, procesamiento y presentación de evidencia digital, a fin de lograr una metodología de intervención adecuada y uniforme en aquellos casos donde existan elementos que pudieran contener potenciales elementos probatorios (PEP) digitales, complementario del "PROTOCOLO DE ACTUACIÓN PARA LA INVESTIGACIÓN CIENTÍFICA EN EL LUGAR DEL HECHO"; cuya aplicación resulta obligatoria para los procedimientos policiales que lleven a cabo las Fuerzas Policiales y de Seguridad Federales aprobado por la Resolución N° 528/21 del MINISTERIO DE SEGURIDAD.

El Protocolo para la identificación, recolección, preservación, procesamiento y presentación de evidencia digital:

- ✓ Define de las pautas y procedimientos al que deberán atenerse los miembros de las Fuerzas Federales Policiales y de Seguridad al momento del proceso de identificación, recolección, preservación, procesamiento y presentación de evidencia digital asociada a cualquier delito y, en particular, los ciberdelitos (delitos ciberasistidos y ciberdependientes),
- ✓ Detalla los procedimientos específicos de secuestro para el primer interviniente clasificados por tipo de dispositivo electrónico tales como celulares, notebooks, equipos de escritorio, servidores, equipos de imagen de video, criptoactivos, rigs de minería y redes informáticas.
- ✓ Incluye los flujogramas de los procedimientos de secuestro para su consulta rápida en el campo.
- ✓ Detalla también los lineamientos para la intervención técnica-forense por parte del personal especialista en el laboratorio

INDICE

TÍTULO I - PARTE GENERAL DISPOSICIONES DE APLICACIÓN GENERAL

CAPÍTULO I - REGLAS GENERALES

1.1 **Objeto:** El presente PROTOCOLO GENERAL DE ACTUACIÓN (en adelante "PGA") tiene por objeto establecer las pautas y el procedimiento al que deberán atenerse los miembros de las Fuerzas Federales Policiales y de Seguridad al momento del proceso de identificación, recolección, preservación, procesamiento y presentación de evidencia digital asociada a cualquier delito y, en particular, los ciberdelitos (delitos ciberasistidos y ciberdependientes), en cumplimiento de los objetivos establecidos en la Resolución N° 86/2022 del Ministerio de Seguridad de la Nación en el marco del PROGRAMA DE FORTALECIMIENTO EN CIBERSEGURIDAD Y EN INVESTIGACIÓN DEL CIBERCRIMEN (ForCIC).

1.2 **Alcance y Aplicación:** El presente PGA es de aplicación obligatoria en todo el país para todo el personal de POLICÍA FEDERAL ARGENTINA, GENDARMERÍA NACIONAL ARGENTINA, POLICÍA DE SEGURIDAD AEROPORTUARIA, PREFECTURA NAVAL ARGENTINA debiéndose tener en cuenta que su accionar debe ajustarse en un todo a la Constitución Nacional, las leyes penales, las pautas procesales y los protocolos vigentes.

1.3 **Complementariedad:** Estos preceptos serán de aplicación complementaria a las medidas establecidas en el código de procedimiento que rija la materia y a las disposiciones emanadas de la autoridad judicial a cargo de la investigación, siempre que no se oponga a las mismas y resulte lo más conveniente para el mejor abordaje posible del caso concreto. Particularmente, se deberán tener en cuenta las pautas establecidas por el "PROTOCOLO DE ACTUACIÓN PARA LA INVESTIGACIÓN CIENTÍFICA EN EL LUGAR DEL HECHO"– Resolución MS N° 528/21.

CAPÍTULO II - CONCEPTOS Y GLOSARIO

2.1 **AFU** (After the first unlock - Después del primer desbloqueo): es el estado del dispositivo una vez que se ha ingresado el código de acceso por primera vez.

2.2 **BFU** (Before the first unlock - Antes del primer desbloqueo): es el estado inicial cuando se enciende el dispositivo.

2.3 **Blockchain:** Libro de contabilidad digital distribuido de transacciones firmadas criptográficamente que se agrupan en bloques. Cada bloque se vincula criptográficamente con el anterior después de su validación y de someterse a una decisión consensuada. A medida que se añaden nuevos bloques, los más antiguos se vuelven más difíciles de modificar (creando una resistencia a la manipulación). Los nuevos bloques se replican en las copias del libro mayor dentro de la red, y cualquier conflicto se resuelve automáticamente utilizando las reglas establecidas (NISTIR 8202).

2.4 **Cadena de Custodia:** se entiende como toda aquella documentación que registre cronológicamente la trazabilidad del elemento desde su secuestro y durante todo el proceso judicial. En el proceso se identifican todas las personas que hayan tomado contacto con esos elementos y las observaciones

sobre modificaciones en su estado, siendo responsables los funcionarios públicos y particulares intervinientes.

2.5 **Caliente (AFU)/ Frío (BFU)**: términos utilizados para describir el estado de la seguridad del dispositivo

2.6 **Ciberdelito:** se encuentra comprendido por los delitos ciberasistidos, entendido como aquellas conductas que ya se encuentra tipificadas en nuestro ordenamiento y cuya planificación, organización, ejecución o resultado se encuentran utilizando el ciberespacio para lograr su fin ilícito, y los delitos ciberdependientes, como aquellos delitos realizados únicamente por medio y/o a través de las tecnologías de la información y comunicación (TIC´s) haciendo que éstos necesiten del ciberespacio para su existencia.

2.7 **Copia Forense de Archivos:** copia de archivos la cual, a diferencia de una Imagen Forense (2.14) no conforma la totalidad de los datos incluidos en un medio de almacenamiento a ser presentados como PEP Digitales. Existen herramientas forenses que se refieren a la copia como “Reproducción”, “Extracción”, “Archivos de Evidencias” o “Imagen customizada”. El cálculo de sus HASH permite verificar su integridad.

2.8 **Criptoactivos:** Representación digital de valor que se puede comercializar o transferir digitalmente y se puede utilizar con fines de pago o inversión. Los activos virtuales no incluyen representaciones digitales de monedas fiduciarias. (GAFI2021)

2.9 **Dirección IP Pública:** es un identificador único e irrepetible con el cual se puede identificar el acceso a internet de cualquier dispositivo con conectividad.

2.10 **Equipo Servidor:** equipo informático cuyo propósito es proveer y gestionar datos de algún tipo de forma a fin de que estén disponibles para otras máquinas que se conecten a él.

2.11 **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.). Técnicamente, 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. Tiene valor probatorio en un proceso judicial.

2.12 **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.

2.13 **ICCID (Integrated circuit card identifier):** Es un número de serie único que tiene cada una de las tarjetas SIMs. Este número está incluido dentro de la SIM y también aparece impreso en el propio chip de la SIM. Se usa para identificar el chip de la SIM.

2.14 **Imagen Forense:** réplica en forma completa (por sector, bit a bit) de la estructura y contenido de un dispositivo de almacenamiento. Puede realizarse por medio de un copiador de hardware o un software con licencia (libre o propietaria). El cálculo de sus valores HASH permite verificar su integridad.

2.15 **IMEI (International Mobile Station Equipment Identity):** Es un código de 15 dígitos programado por

el fabricante para identificar cada equipo móvil a nivel mundial. Está compuesto por un código de identificación de marca y modelo otorgado a los fabricantes por la GSMA (Global System Mobile Association).

2.16 **IMSI (International Mobile Subscriber Identitiy):** Es un número único para identificar a un abonado móvil.

2.17 **Jalibreak/Rooting**. proceso utilizado para la obtención de mayores privilegios en el sistema operativo del dispositivo electrónico para superar las limitaciones definidas por el fabricante. En algunos casos, este proceso puede facilitar la obtención de los PEP digitales.

2.18 **Memoria RAM:** memoria de acceso aleatorio (RAM) es el almacenamiento en memoria a corto plazo. En los dispositivos, el sistema operativo utiliza la memoria RAM para almacenar de forma temporal los programas y procesos de ejecución. En la RAM se cargan todas las instrucciones que ejecuta la unidad central de procesamiento (CPU) y otras unidades del ordenador, además de contener los datos que manipulan los distintos programas. Una vez apagado el dispositivo, la RAM deja de recibir energía y se pierde la información almacenada en ella.

2.19 **Personal Especialista:** personal idóneo con conocimientos especializados en evidencia digital perteneciente a las Fuerzas Policiales y de Seguridad y con las capacidades para hacer adquisiciones en el lugar del hecho, procesar la información y producir la potencial evidencia digital.

2.20 **Personal interviniente/ primer interviniente:** personal de las Fuerzas Policiales y de Seguridad, capacitado y/o autorizado para actuar primero en el lugar del hecho al realizar el correcto secuestro de los PEPs.

2.21 **Potencial Elemento de Prueba (PEP):** Se consideran Potenciales Elementos de Prueba (PEP) aquellos dispositivos susceptibles de contener información (representación física), los cuales almacenan potencial evidencia digital (representación lógica).

2.22 **Potencial Elemento de Prueba digital (PEP digital)**: cualquier dato (registro y/o archivo) que puede ser generado, transmitido o almacenado por equipos de tecnología informática y que está constituido por campos magnéticos y pulsos electrónicos, los cuales pueden ser recolectados y analizados con herramientas y/o técnicas especiales. Los efectos contendores primarios y secundarios (PEP) son indispensables para el acceso a los datos.

2.23 **Procesamiento de PEP digitales:** medidas técnicas realizadas sobre los PEP tendientes a satisfacer lo requerido por el objeto de investigación.

2.24 **Rig de Minería:** conjunto de elementos de hardware instalados y configurados para el minado de criptoactivos.

2.25 **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.

2.26 **Triage:** proceso de selección de dispositivos o filtrado de información ordenado por la autoridad judicial, quien aporta los criterios de evaluación sobre los dispositivos electrónicos en el lugar del hecho, susceptibles a ser secuestrados para llevar a cabo un posterior análisis forense. Este proceso puede traer aparejada la alteración de datos informáticos por lo que resulta necesario tomar recaudos y precauciones, analizar los riesgos inherentes a esta clase de intervenciones e informar a la autoridad judicial sobre los mismos, así como documentar adecuadamente las tareas realizadas. El proceso del Triage servirá para sustentar la decisión judicial de secuestro o no de los elementos, realización de imágenes o copias forenses, detenciones, entre otras posibles medidas procesales. El proceso de Triage deberá ser liderado por Personal Especialista.

2.27 **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.

2.28 **Wallet/billetera electrónica:** dispositivo electrónico, servicio de banca móvil o aplicación móvil que permite a una parte realizar transacciones electrónicas con otra parte que intercambia unidades de moneda digital por bienes y/o servicios.

CAPÍTULO III - PRINCIPIOS GENERALES DE INTERVENCIÓN

3.1 **Personal interviniente/ primer interviniente:** Es el responsable de la exploración, localización, valoración y/o recolección de PEPs que pudieran contener evidencia digital y se encuentren asociados al hecho investigado y que sea de interés para el análisis pericial en el laboratorio de la especialidad, procurando la relevancia, suficiencia, validez legal y confiabilidad durante el proceso de identificación, recolección y adquisición de los mismos.

3.2 **Recolección, Aseguramiento y Transporte.** Los procesos de recolección, aseguramiento y transporte de la prueba priorizarán la no modificación de los PEP digitales. Si por cuestiones de metodología esto no pudiera evitarse, los procesos deberán quedar debidamente documentados.

3.3 **Procesamiento por Especialista.** Los efectos que pudieran contener PEPs digitales sólo deben ser procesados por personal idóneo, entrenado y capacitado (2.19) para la generación de reportes que respondan al objeto de investigación.

3.4 **Documentación de las Actuaciones.** Todo lo actuado durante la recolección, transporte, almacenamiento y procesamiento de los efectos que pudieran PEPs digitales debe estar completamente documentado, preservado y disponible para un posterior examen.

CAPÍTULO IV - INTERVENCIÓN INICIAL, EXPLORACIÓN, LOCALIZACIÓN, VALORACIÓN Y RECOLECCIÓN DE EFECTOS QUE PUDIERAN CONTENER PEPs DIGITALES

4.1 En el caso de un allanamiento u orden de presentación, previamente a llevar a cabo el procedimiento, se recomienda coordinar con la autoridad judicial 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, inspección manual de dispositivos, volcados de memoria RAM, claves de accesos, acceso a datos de la nube, capacidades del personal a interviniente, insumos, etc.

4.2 En caso de que el personal interviniente verifique la presencia de PEPs que pudiesen contener potencial evidencia digital en el lugar del hecho , procurará en el acta prevista labrada con las formalidades legales vigentes, 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 policial, el estado en que éstos fueron hallados (encendido/apagado), incluyendo las características identificativas de cada dispositivo (por ejemplo, daños, inscripciones, modelo, número de serie y cualquier marca de identificación). Cuando sea necesario y las circunstancias del hecho lo ameriten, se procurará que la fijación narrativa se complemente con fotografías, filmaciones, planos del lugar y del sitio de ubicación de cada efecto, esquema o croquis de disposición de cables y conexiones entre dispositivos. Todo ello a fin de asegurar que el procedimiento pueda ser reconstruido, en caso de ser solicitado por la autoridad judicial.

4.3 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 interviniente el procedimiento 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.

4.4 En caso de considerarlo pertinente, el personal interviniente podrá realizar la consulta remota con el área especializada de la fuerza a la que pertenece, 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 bajo el liderazgo personal especialista, debiéndose en todos los casos documentar el proceso realizado.

4.5 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 judicial interviniente. Dicho triage deberá ser liderado por personal especialista.

4.6 Se deberá poner especial atención en intentar determinar quién o quiénes son los usuarios de los dispositivos. De la misma manera, al momento del allanamiento, 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.

CAPÍTULO V - PROCEDIMIENTOS ESPECÍFICOSPOR TIPO DE DISPOSITIVO ELECTRÓNICO

DISPOSITIVOS MÓVILES Y CELULARES

5.1 Se debe priorizar aislar el dispositivo y, en consecuencia, impedir su conexión a la red móvil de telefonía y/o wifi para así evitar su posible adulteración o borrado remoto.

5.2 Se recuerda que no se debe interactuar innecesariamente ni buscar información en los dispositivos móviles, excepto cuando así lo requiera la autoridad judicial, debiéndose siempre documentar el proceso realizado. Esto se debe a que los dispositivos registran todas las interacciones realizadas y, por lo tanto, al momento de practicarse en el laboratorio la obtención de datos, el equipo especializado reportará las mismas.

5.3 El primer interviniente, al observar si el dispositivo se encuentra encendido (CALIENTE-AFU), no debe apagarlo, procurando realizar los procedimientos recomendados para garantizar la preservación y la correcta identificación detallados a continuación, los cuales deben ser volcados en el acta del procedimiento:

a. Realizar la extracción de la tarjeta SIM para prevenir el acceso o modificación remota a través de la red de telefonía celular (3G, 4G, 5G, etc.)

b. Registrar la numeración y logo visibles en el exterior de la tarjeta SIM (ICCID).

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

d. Adherir la o las tarjetas SIM con cinta transparente a la carcasa del equipo.

e. De ser posible, identificar el IMEI del dispositivo telefónico. En el caso de que no se visualice, registrar “IMEI no visible / ilegible”. Por ningún motivo se deberá manipular el equipo con la intención de obtener número de serie/IMEI con métodos tales como ingresando el código “*#06#” en el teclado o ingresando a su menú de configuración

f. De ser posible, activar el modo avión del dispositivo.

g. De ser posible, desactivar la opción de WIFI.

h. De ser posible, identificar y registrar marca o inscripción visible (se puede observar en la carcasa del dispositivo o impreso en la etiqueta de datos). En el caso que no se visualice, registrar “Marca o Inscripción No visible”.

i. De ser posible, identificar y registrar modelo técnico (se puede observar en la carcasa del dispositivo o impreso en la etiqueta de datos). En el caso que no se visualice, registrar “Modelo Técnico No visible”.

j. De ser posible, identificar Número de Serie (se puede observar en la carcasa del dispositivo, impreso en la etiqueta de datos ubicada generalmente bajo la batería cuando la misma sea accesible). En caso de no observarse, por ningún motivo se deberá manipular el equipo con la intención de obtener el número de serie con métodos tales como ingresando el código “*#06#” en el teclado o ingresando a su menú de configuración.

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

l. Registrar el estado de conservación a simple vista del dispositivo (Bueno, Regular, Malo) incluyendo descripción de detalles. Por ejemplo, cuando posea un faltante de partes o pantalla fracturada se considerará un estado de conservación malo.

m. Finalizados los pasos anteriores, colocar el dispositivo en una bolsa Faraday o desplegar otro método no invasivo que se valga del mismo principio para lograr un aislamiento electromagnético de toda señal (Ej. papel aluminio. Utilizar como mínimo 5 vueltas sobre el dispositivo).

5.4 En casos que la autoridad judicial lo disponga, con la disponibilidad de los medios necesarios, se procurará mantener el dispositivo encendido (CALIENTE-AFU) manteniendo la carga del mismo conectándolo a un powerbank (batería portátil) utilizando el método de aislamiento electromagnético antes mencionado, a los efectos de ser remitido a las oficinas especializadas/laboratorio, evitando que el mismo se apague.

5.5 En el caso de que la autoridad judicial solicite un triage de dispositivos móviles, el mismo será liderado por personal especialista (presencial o asesoramiento remoto) y consistirá en un examen manual (sin herramientas forenses) usando las funciones propias del dispositivo con las limitaciones del caso. Dichas interacciones quedarán registradas en el dispositivo por lo cual deberán quedar correctamente documentadas.

5.6 Si el dispositivo está apagado (FRIO-BFU), mantenerlo en ese estado, procediendo a realizar los siguientes pasos:

a. Realizar la extracción de la tarjeta SIM para prevenir el acceso o modificación remota a través de la red de telefonía celular (3G, 4G, 5G, etc.)

b. Registrar la numeración y logo visibles en el exterior de la tarjeta SIM (ICCID).

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

d. Adherir la o las tarjetas SIM con cinta transparente a la carcasa del equipo.

e. De ser posible, identificar el IMEI del dispositivo telefónico. En el caso de que no se visualice, registrar “IMEI no visible / ilegible”.

f. De ser posible, identificar y registrar marca o inscripción visible (se puede observar en la carcasa del dispositivo o impreso en la etiqueta de datos). En el caso que no se visualice, registrar “Marca o Inscripción No visible”.

g. De ser posible, identificar y registrar modelo técnico (se puede observar en la carcasa del dispositivo o impreso en la etiqueta de datos). En el caso que no se visualice, registrar “Modelo Técnico No visible”.

h. De ser posible, identificar Número de Serie (se puede observar en la carcasa del dispositivo, impreso en la etiqueta de datos ubicada generalmente bajo la batería cuando la misma sea accesible). En caso de no observarse, por ningún motivo se deberá manipular el equipo con la intención de obtener el número de serie con métodos tales como ingresando el código “*#06#” en el teclado o ingresando a su menú de configuración.

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

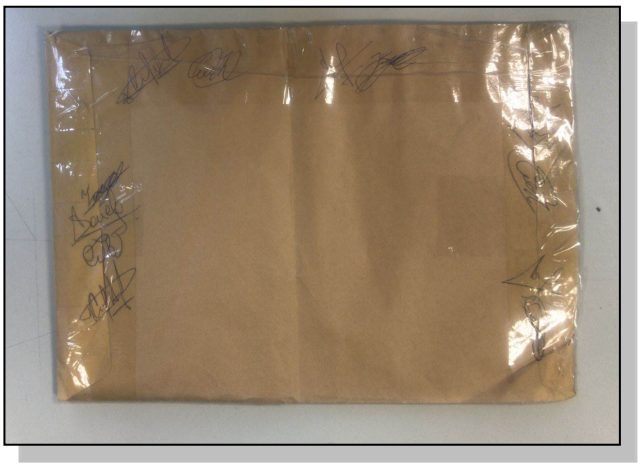
j. Registrar el estado de conservación a simple vista del dispositivo (Bueno, Regular, Malo) incluyendo descripción de detalles. Por ejemplo, cuando posea un faltante de partes o pantalla fracturada se considerará un estado de conservación malo.

k. Finalizados los pasos anteriores, colocar el dispositivo en una bolsa Faraday o el desplegar otro método no invasivo que se valga del mismo principio para lograr un aislamiento electromagnético de toda señal (Ej. papel aluminio. Utilizar como mínimo 5 vueltas sobre el dispositivo).

5.7 Tanto para equipos encendidos o apagados, cuando sea posible, secuestrar cargador y cables de datos de los dispositivos.

5.8 Previa coordinación y de acuerdo a lo que disponga la autoridad judicial, si al momento del secuestro, en conocimiento de sus derechos, algún usuario deseara informar, de forma espontánea y voluntaria, la/s clave/s de su dispositivo para evitar el entorpecimiento de la etapa de análisis forense, las mismas deberán ser plasmadas en el acta labrada oportunamente. Todo uso de las claves aportadas deberá ser acordado con la autoridad judicial y debidamente documentado.

5.9 Una vez acondicionado técnicamente el dispositivo (bolsa de Faraday, papel aluminio, etc.) el mismo deberá ser preservado de forma individual en un sobre, caja u otro elemento contenedor que el primer interviniente disponga que garantice la medida. Es importante remarcar que se deben incorporar firmas de los intervinientes (quienes figuran en el acta, en especial los testigos) en los cierres y pliegues del sobre, de forma tal de no generar dudas sobre un posible acceso al dispositivo. Una vez finalizado el embalaje se procederá a la confección de una planilla de cadena de custodia para cada dispositivo en particular.



EQUIPO INFORMÁTICO DE ESCRITORIO

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

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

b. 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.

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

d. Si el equipo informático está encendido, pero el monitor apagado, encenderlo y registrar fotográficamente lo que se visualiza.

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

f. De acuerdo a lo acordado y dispuesto formalmente por la autoridad judicial, el primer interviniente evaluará si la situación en particular y especial requiere la participación de personal especialista, para que éste, con la autorización de la autoridad judicial, proceda a la realización de la adquisición de memoria RAM, imagen forense o descarga de información en la nube. Al momento de realizar estas tareas deberán quedar registros de las características de los dispositivos que sean de interés para la causa. La obtención de los valores de algoritmo HASH de los PEPs digitales adquiridos deberán ser plasmados en el acta de procedimiento.

g. Una vez finalizada todas las medidas recomendadas y/o llevadas a cabo por el personal especialista, se procederá a desconectar el cable de alimentación (cable power).

h. Se procederá al embalaje, rotulado y preservación del dispositivo y a la confección de la planilla de cadena de custodia para cada efecto en particular.

i. El embalaje del mismo 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 primer interviniente disponga, y que asegure tal medida. Se deberá prestar atención también a no dejar posibles accesos con tornillos.

5.11 En caso que el equipo se encuentre encendido, y la orden judicial ordena la ejecución de un triage, el personal especialista realizará la copia de información requerida, en una unidad de almacenamiento extraíble aportada por la autoridad judicial requirente, obteniéndose los valores de algoritmo HASH, los cuales deben ser plasmados en el acta de intervención correspondiente. Al momento de realizar estas tareas deberán quedar registros de las características de los dispositivos que sean de interés para la causa. Posterior a ello, se procederá al embalaje, rotulado y confección de planilla de cadena de custodia del dispositivo de almacenamiento destino.

5.12 Si el dispositivo está apagado se procederá a realizar los siguientes pasos:

a. Proceder a desconectar el cable de alimentación (cable power) y proceder al embalaje, rotulado y preservación del dispositivo y a la confección de la planilla de cadena de custodia por cada efecto en particular.

b. El embalaje del mismo 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 primer interviniente disponga, y que asegure tal medida. Se deberá prestar atención también a no dejar posibles accesos con tornillos.

5.13 En el caso de embalarse algún elemento en sobres, se deberán incorporar firmas de los intervinientes (quienes figuran en el acta, en especial los testigos) en los cierres y pliegues del mismo, de forma tal de no generar dudas sobre un posible acceso al dispositivo. Lo mismo aplica a fajas o clausuras aplicadas a puertos y aberturas.

5.14 Para todos los casos, una vez finalizado el embalaje se procederá a la confección de una planilla de cadena de custodia para cada dispositivo en particular.

`

LAPTOP O COMPUTADORA PORTÁTIL:

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

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

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

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

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

e. De acuerdo a lo acordado y dispuesto formalmente por la autoridad judicial, el primer interviniente evaluará si la situación en particular y especial requiere la participación de personal especialista, para que este, con la autorización de la autoridad judicial, proceda a la realización de la adquisición de memoria RAM, imagen forense o descarga de información en la nube. La obtención de los valores de algoritmo HASH de los PEPs digitales adquiridos deberán ser plasmados en el acta de procedimiento.

f. El proceso de secuestro se realizará desenchufando el cable de energía y extrayendo su batería. En el caso que no sea posible la extracción de la batería, se procederá a apagar el equipo presionando el botón de encendido por DIEZ (10) segundos.

g. De ser posible, identificar y registrar las características del equipo: marca visible, el modelo, número de serie, y el estado de conservación del mismo. Así mismo se describirán todas otras aquellas características que lo puedan llegar a identificar e individualizar, como stickers, rupturas, etc.

h. Proceder al embalaje, rotulado y preservación del dispositivo y a la confección de una planilla de cadena de custodia para cada efecto en particular.

i. El embalaje del mismo se realizará fajando o clausurando todos los puertos por donde pueda ingresar o egresar información, y energía, con cintas adhesivas, papel adhesivo, o elementos que el primer interviniente disponga, y que asegure tal medida. Se deberá prestar especial atención a los posibles accesos con tornillos, tales como tapas de acceso al disco de almacenamiento de información del dispositivo. De estar disponibles, se deberá secuestrar los cargadores de los equipos.

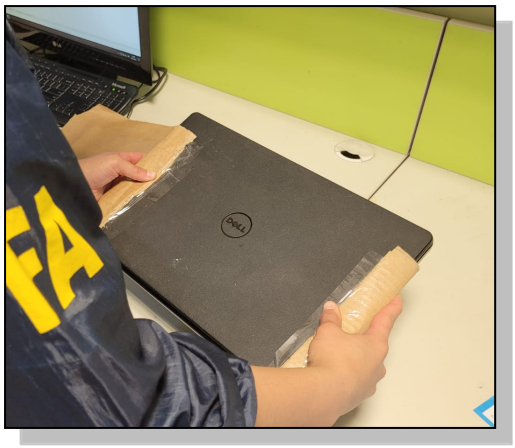
5.16 Si el dispositivo está apagado proceder a realizar los siguientes pasos:

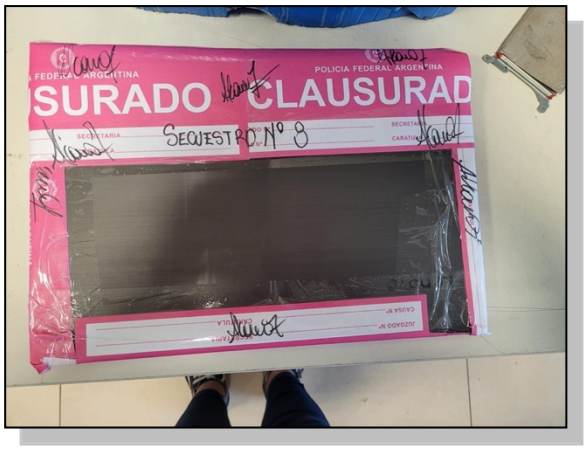
a. El proceso de secuestro se realizará desenchufando el cable de energía y extrayendo su batería cuando sea posible.

b. Documentar el equipo, describiendo: la marca visible, el modelo, número de serie, y el estado de conservación del mismo. Así mismo se describirán todas aquellas características que lo puedan llegar a identificar e individualizar, como stickers, rupturas, etc.

c. Proceder al embalaje, rotulado y preservación del dispositivo y a la confección de la planilla de cadena de custodia por cada efecto en particular.

d. El embalaje del mismo se realizará fajando o clausurando todos los puertos por donde pueda ingresar o egresar información, y energía, con cintas adhesivas, papel adhesivo, o elementos que el primer interviniente disponga, y que asegure tal medida. Se deberá prestar especial atención a los posibles accesos con tornillos, tales como tapas de acceso al disco de almacenamiento de información del dispositivo. De estar disponibles, se deberá secuestrar los cargadores de los equipos.





5.17 Todo lo que pertenezca a una misma computadora será identificado (etiquetado), embalado y transportado en su conjunto, para evitar que se mezcle con las partes de otros dispositivos y poder luego reconfigurar el sistema.

5.18 Una vez finalizado el embalaje se procederá a la confección de la planilla de cadena de custodia por cada computadora en particular.

5.19 En el caso que la orden judicial disponga u ordene la realización de un triage, el personal especialista procederá a realizar el mismo en presencia de los testigos, siguiendo la orientación y lineamientos emanados por la autoridad judicial, documentando toda la medida y plasmándola en el acta de procedimiento. Al momento de realizar estas tareas deberán quedar registros de las características de los dispositivos que sean de interés para la causa.

5.20 En caso que el equipo se encuentre encendido, y la orden judicial sea la copia de información específica, el personal especialista procederá a la copia de información solicitada, en una unidad de almacenamiento extraíble aportada por la autoridad judicial requirente. La unidad de almacenamiento deberá ser previamente tratada con un borrado seguro para evitar cualquier tipo de contaminación previa al a copia. Posteriormente, procederá al embalaje y confección de planilla de cadena de custodia del

dispositivo de almacenamiento destino. A los archivos obtenidos se les realizarán dos cálculos de HASH para poder verificar su integridad, los cuales deben estar plasmados en el acta de procedimiento.

EQUIPOS SERVIDORES

5.21 En caso que el equipo se encuentre encendido, y la orden judicial sea secuestro, se procederá de igual forma que un equipo informático de escritorio. Es recomendable evaluar previamente si los servicios que corren en los servidores a secuestrar son críticos y que posibles consecuencias puede generar su indisponibilidad, debiendo informarse esto a la autoridad judicial.

5.22 En caso que el equipo se encuentre apagado, y la orden judicial sea secuestro, se procederá al embalaje, rotulado y confección de cadena de custodia, de igual forma que un equipo informático de escritorio.

5.23 En caso que el equipo se encuentre encendido, y la orden judicial sea la copia de información específica, el personal especialista procederá junto al administrador del equipo servidor, a la copia de información solicitada, en una unidad de almacenamiento extraíble aportada por la autoridad judicial requirente. La unidad de almacenamiento deberá ser previamente tratada con un borrado seguro para evitar cualquier tipo de contaminación previa al a copia. Posteriormente, procederá al embalaje y confección de planilla de cadena de custodia del dispositivo de almacenamiento destino. A los archivos obtenidos se les realizarán dos cálculos de HASH para poder verificar su integridad, los cuales deben estar plasmados en el acta de procedimiento.

EQUIPOS DE IMAGEN Y VIDEO

5.24 El primer 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).

5.25 En el caso que el dispositivo se encuentre encendido, proceder a desconectar el cable de alimentación de energía, y proceder a su secuestro.

5.26 En caso de ser un DVR, introducirlo en una caja, bolsa o sobre, fajada y firmada por el primer interviniente y los testigos.

5.27 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 primer interviniente disponga, a fin de asegurar la medida.

5.28 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 primer interviniente y los testigos.

5.29 Se debe documentar el mismo describiendo: la marca visible, el modelo, número de serie y el estado de conservación del mismo. Asimismo, se describirán todas aquellas características que lo puedan llegar a identificar e individualizar, como stickers, rupturas, etc.

5.30 Una vez finalizado el embalaje se procederá a la confección de una planilla de cadena de custodia para cada dispositivo en particular.

5.31 En casos que la autoridad judicial lo ordene, el personal especialista procederá al volcado “en caliente” de los videos solicitados, almacenándolos en una unidad de almacenamiento extraíble aportada por la autoridad judicial requirente. Posteriormente, procederá al embalaje y confección de planilla de cadena de custodia del dispositivo de almacenamiento destino. La unidad de almacenamiento deberá ser previamente tratada con un borrado seguro para evitar cualquier tipo de contaminación previa al a copia.

REDES INFORMÁTICAS

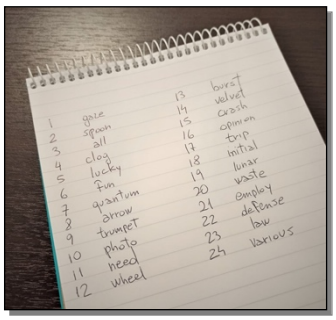
5.32 A fin de minimizar posibles daños, tales como interrupciones en servicios críticos, se recomienda realizar un relevamiento de las conexiones críticas ligadas a la arquitectura de la red. Dicha labor debe ser realizada por personal especialista.

5.33 Si durante el procedimiento fuera de interés de la autoridad judicial identificar datos relevantes de las redes informáticas (IP Privada, IP Pública, arquitectura de red, etc.), dicha labor debe ser realizada por personal especialista.

5.34 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 primer interviniente.

CRIPTOACTIVOS

5.35 Al momento del allanamiento se deberá prestar atención a la presencia de billeteras frías (aspecto similar a un pendrive), como así a anotaciones con palabras claves (semillas), códigos QR, etc., que puedan estar asociadas a wallets.



5.36 Ante la presencia de indicadores o identificadores propios de actividades ligadas a los criptoactivos se deberá realizar consulta con la autoridad judicial, quién determinará el criterio a adoptar.

RIG DE MINERIA

5.37 Los rigs de minería pueden presentar distintos aspectos de acuerdo a su tecnología. 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 judicial para la evaluación de su secuestro.

5.38 En caso de encontrarse en un allanamiento con equipos de minería (rig de minería), el primer interviniente coordinará con la autoridad judicial y con el personal especialista de criptoactivos como proceder.

5.39 En los casos en los que la autoridad judicial ordene el secuestro, se procederá de igual forma que con un equipo informático encendido.

CAPITULO VI - CADENA DE CUSTODIA: EMBALAJE, ROTULADO Y REMISIÓN DE EFECTOS QUE PUDIERAN CONTENER PEPs DIGITALES

6.1 El registro de la cadena de custodia es un documento o una serie de documentos (actas de secuestro, actas de entrega y recepción, actas apertura o desintervención y formulario de cadena de custodia) relacionados que detallan la trazabilidad, registrando quién fue responsable de resguardar y trasladar los PEP desde su secuestro hasta su disposición final definida por la autoridad judicial. En el anexo 3 de este documento se encuentra el instructivo para completar el formulario de cadena de custodia.

CAPITULO VII - INTERVENCIÓN DEL PERSONAL ESPECIALISTA (OFICINA ESPECIALIZADA)

INCUMBENCIAS DE LA OFICINA ESPECIALIZADA

7.1 La oficina especializada en actividades forenses de cada institución realizará tareas técnico-periciales idóneas a su función en relación a los PEP digitales.

7.2 Debido a las particularidades de cada tipo de tecnología, los procedimientos aplicables pueden presentar diferencias del mismo. A modo de ejemplo, no son iguales las tareas para la extracción de datos de un teléfono o de un equipo informático u otro dispositivo electrónico.

7.3 Se procederá únicamente a la creación de imágenes forenses o extracción, categorización (decodificación) de datos, generación de los reportes pertinentes junto con el informe técnico y actas de estilo, quedando expresamente excluida la realización de tareas de análisis respecto de la información extraída. En relación a la información extraída, la misma será enviada al área de análisis correspondiente tales como la autoridad judicial, la dependencia preventora o quien tenga conocimiento de los pormenores de la investigación, de acuerdo a lo dispuesto por la autoridad judicial.

ASIGNACIÓN DE TURNOS Y RECEPCIÓN DE EFECTOS QUE PUDIERAN CONTENER PEP DIGITALES

7.4 La oficina especializada en actividades forenses de cada institución otorgará turnos para aquellas solicitudes de labores periciales que tengan su origen en oficios judiciales y/o mandas judiciales expresas en el marco de las causas que se sustancien y que provengan de la autoridad judicial.

7.5 Una vez asignado e informado el turno pericial otorgado, la unidad requirente o la instancia judicial correspondiente deberá indicar si requiere las imágenes forenses y/o las extracciones de datos, como así también brindará los medios técnicos (dispositivos de almacenamiento externos, etc.) suficientes para remitir tal información.

7.6 De no contarse con un recinto transitorio de evidencia, solo se recibirán los elementos ofrecidos para su estudio y/o extracción en el día correspondiente al turno pericial. En ambos casos, se suscribirá un acta de recepción de los elementos, consignando el estado en que ellos se encuentran (inscripción/modelo/estado de conservación/etc.), firmada por los intervinientes. Cuando se requiera la presencia de testigos (desintervención), se deberá confeccionar el acta de apertura y entrega dejando constancia de ello, acompañado a la misma de todos aquellos anexos que se consideren pertinentes.

7.7 En caso que el elemento no tuviera planilla de cadena de custodia, se creará una, la cual acompañará al elemento en todo momento, dejando constancia del faltante de la misma en el acta labrada a tal fin.

7.8 En caso que sea un sobre o bolsa, y la misma se encuentre rota o dañada, se procederá a la apertura y control de los elementos alojados en su interior, todo esto en presencia de la persona que entrega los elementos quedando esto documentando debidamente.

INTERVENCIÓN TÉCNICA-FORENSE

7.9 Para los PEP digitales, la oficina especializada en actividades forenses procederá únicamente a la copia forense y categorización (decodificación) de datos. El procesamiento de información estará dirigido únicamente para dar respuesta a los objetos de pericia o investigación.

7.10 Con respecto a los dispositivos móviles (teléfonos, tablets, etc.), la extracción y procesamiento/decodificación de información, se realizará mediante software debiendo dejar claramente documentada la versión utilizada. Dentro de las herramientas, existen varios tipos de extracciones disponibles para los dispositivos móviles, las cuales dependerán de los sistemas operativos (versiones/actualizaciones/parches de seguridad), de los componentes electrónicos variables (chipset), como así de las medidas de seguridad existentes en los mismos (bloqueo de acceso por el usuario, etc.), y del nivel de acceso a los datos de usuario (rooteado, jailbreak). Se podrán realizar técnicas o métodos a los efectos de adquirir datos del usuario escalando privilegios en el sistema operativo del dispositivo (root, jalibreak) para facilitar la obtención de los PEP digitales mediante extracciones de datos del usuario manteniendo la integridad de los mismos. Ante una eventual aplicación de una técnica o método de extracción que conlleve a procedimientos de escalamiento de los permisos del sistema operativo para la obtención de datos del usuario, la misma deberá ser autorizada previamente por la autoridad judicial, debiéndose informar los posibles riesgos y beneficios que conllevan tales prácticas.

7.11 En el caso de trabajar con computadoras, se recomienda realizar primero una imagen forense del disco duro. La misma puede realizarse por medio de un duplicador de hardware o un software. Para este procedimiento se deberá:

a. Utilizar un bloqueador de escritura al momento de realizar la imagen forense. Esto permite operar el dispositivo asegurando que no se modifique la información.

b. Una vez finalizada la imagen forense, el agente deberá realizar los cálculos de hash de la misma.

7.12 Los únicos autorizados a presenciar la intervención técnico-forense y presentación de resultados, serán los autorizados expresamente por la autoridad judicial.

7.13 PRESENTACIÓN: Las presentaciones de los resultados serán documentadas correctamente a través de:

a. Informe Técnico-forense con las formalidades legales vigentes.

b. PEP digitales procesados que soportan el informe. Para su almacenamiento se adoptará algún método de comprobación para asegurar su integridad, tales como el cálculo de HASH al archivo individual, HASH de archivos comprimidos, uso de blockchain Federal, etc.

7.14 Una vez concluidas las labores encomendadas, se procederá a la devolución de los objetos de estudio, se practicará el borrado seguro de la totalidad de los datos tratados, cumpliendo el debido resguardo de los derechos y garantías que correspondan. Salvo disposición judicial en contrario, la oficina especializada, no realizará resguardo de datos obtenidos en la intervención técnico-forense ni de elementos por tiempo indeterminado, de lo que dará cuenta a la autoridad judicial requirente. El resguardo de información es de carácter transitorio exclusivamente ceñido a la práctica pericial y de acuerdo a la capacidad de almacenamiento de los servidores de la institución asignados.

7.15 Solamente se resguardarán las diligencias administrativas confeccionadas, informes técnicos-forenses, y aquellas diligencias que den cuenta de la efectiva entrega de lo actuado y de los PEP digitales ofrecidos, según las políticas de seguridad de la información de cada Institución.

7.16 Finalmente, se procederá a embalar debidamente los efectos que contengan los PEP digitales, confeccionándose su correspondiente planilla de cadena de custodia.

ANEXO 1 – ETIQUETA IDENTIFICADORA DE PEP

POTENCIAL ELEMENTO DE PRUEBA (PEP)

PEP: ..... **Formulario de cadena de custodia n° :** .....

Causa/Sumario: .....

Carátula: .....

Dependencia Preventora: .....

Autoridad Judicial: .....

Lugar de Recolección: .....

.....Fecha:.....Hora:.....

Detalle/Observaciones: .....

.....

Argentina
Ministerio Público Fiscal
Ministerio de Seguridad

ANEXO 2 – FORMULARIO DE CADENA DE CUSTODIA

Argentina unida Ministerio de Seguridad Argentina

FORMULARIO DE CADENA DE CUSTODIA N°

FECHA		HORA	
CARÁTULA (preventiva)			
SUMARIO	Nº		
JUZGADO/FISCALIA	Nº		
SECRETARÍA	Nº		
LUGAR DE RECOLECCIÓN			
Otra información de utilidad			
Identificación del Material			

Breve descripción del Material:*

*La descripción completa se encuentra en el acta que corresponda (secuestro, allanamiento, levantamiento, entre otras) o en la pericia perteneciente a este material.

Modo de conservación	Medio ambiente		Conservadora refrigerada				Otros		
Tipo de embalaje / elemento contenedor	Sobres de papel		Bolsas Plásticas		Cajas		Frascos		Otros

RESPONSABLE DEL LEVANTAMIENTO (FIRMA)	DNI LEGAJO APELLIDO y NOMBRE	DEPENDENCIA	FECHA	HORA
1.				

Observaciones:

	DNI LEGAJO APELLIDO y NOMBRE	DEPENDENCIA		HORA
2.				

Observaciones:

	DNI LEGAJO APELLIDO y NOMBRE	DEPENDENCIA		HORA
3.				

Observaciones:

Gendarmería Nacional

Argentina unida Ministerio de Seguridad Argentina

FORMULARIO DE CADENA DE CUSTODIA N°

	DNI LEGAJO APELLIDO y NOMBRE	DEPENDENCIA	FECHA	HORA
4.				
Observaciones:				
	DNI LEGAJO APELLIDO y NOMBRE	DEPENDENCIA	FECHA	HORA
5.				
Observaciones:				
	DNI LEGAJO APELLIDO y NOMBRE	DEPENDENCIA	FECHA	HORA
6.				
Observaciones:				
7.	DNI LEGAJO APELLIDO y NOMBRE	DEPENDENCIA	FECHA	HORA
Observaciones:				

Observaciones:

Gendarmería Nacional

ANEXO 3 - INSTRUCTIVO PARA EL LLENADO DEL FORMULARIO DE CADENA DE CUSTODIA

PARÁMETROS GENERALES

1. Llenar cada uno de los espacios correspondientes a los datos requeridos de manera clara y precisa.
2. Si luego de llenar un espacio, queda parte de este sin utilizar, se deberá pasar una línea para inutilizar el espacio restante.
3. Se podrá utilizar tinta de color negro y de color azul para el llenado de la planilla.
4. La planilla podrá ser llenada de forma manuscrita con letra imprenta y clara o impresa.
5. La firma siempre deberá ser de forma manuscrita.

FORMULARIO DE CADENA DE CUSTODIA

- **Formulario de cadena de custodia N°….:** Espacio para registrar el número del formulario que debe coincidir con el rotulo/s asignado/s al Potencial Elemento de Prueba.
- **Fecha y hora:** Día, mes, año y hora de obtención de los Potenciales Elementos de Prueba (PEP) , separados con una barra diagonal (/) en el formato: DD/ MM/ AAAA. Ejemplo 16/08/2022 y la hora en formato 24 hrs. Ejemplo: 19 hrs.
- **Caratula (preventiva):** Espacio para registrar la caratula del expediente o causa asignado, al momento de iniciar la investigación; es el asignado por el organismo actuante o el Ministerio Público.
- **Sumario:** Espacio para registrar el número de sumario asignado al momento de iniciar el procedimiento y dependencia preventora; es el asignado por LAS FUERZAS POLICIALES Y DE SEGURIDAD FEDERALES actuantes.
- **Juzgado/ Fiscalía:** Nombre de la dependencia a la que pertenece el magistrado que instruye la investigación vinculada con el Potencial Elemento de Prueba (PEP) que será descripto.
- **Secretaria:** Nombre de la dependencia a la que pertenece el secretario que instruye la investigación vinculada con el Potencial Elemento de Prueba (PEP) que será descripto.
- **Lugar de recolección:** Provincia, ciudad, municipio, zona, sector, avenida, calle, entre otros, donde se obtuvieron los Potenciales Elemento de Prueba (PEP).

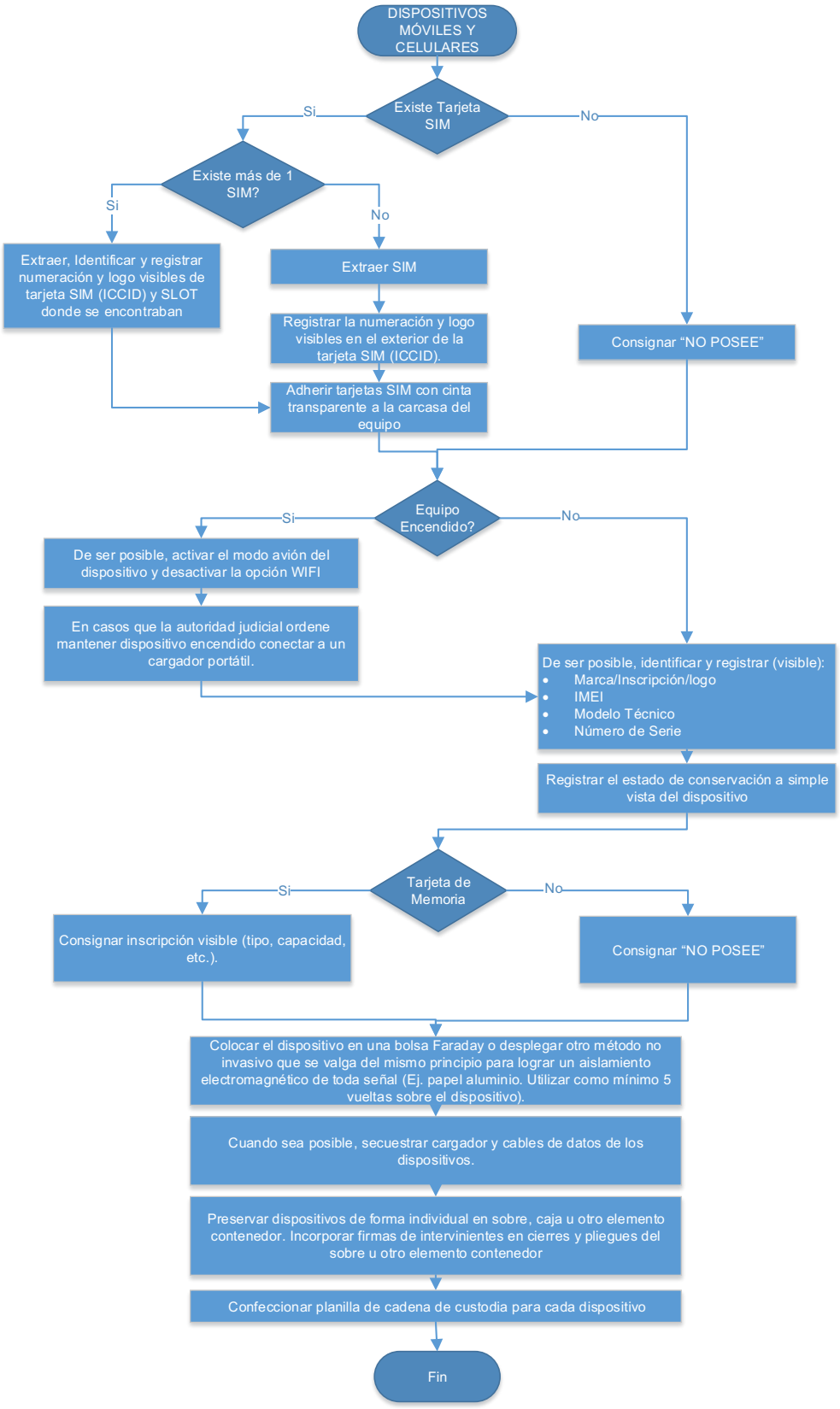
- **Otra información de utilidad:** información de las partes, datos del imputado, damnificado o cualquier otro dato que crea de utilidad.

- **Identificación del material:** Breve descripción de la apariencia e individualización del Potencial Elemento de Prueba (PEP) resguardado. En casos especiales, en este apartado se pueden agregar agrupamientos de elementos de la misma locación y misma especie (ej.: Formulario de Cadena Custodia No 1: 10 pendrives ubicados en la oficina 1; Formulario de Cadena Custodia 2: 20 DVDs ubicados en la habitación 2).

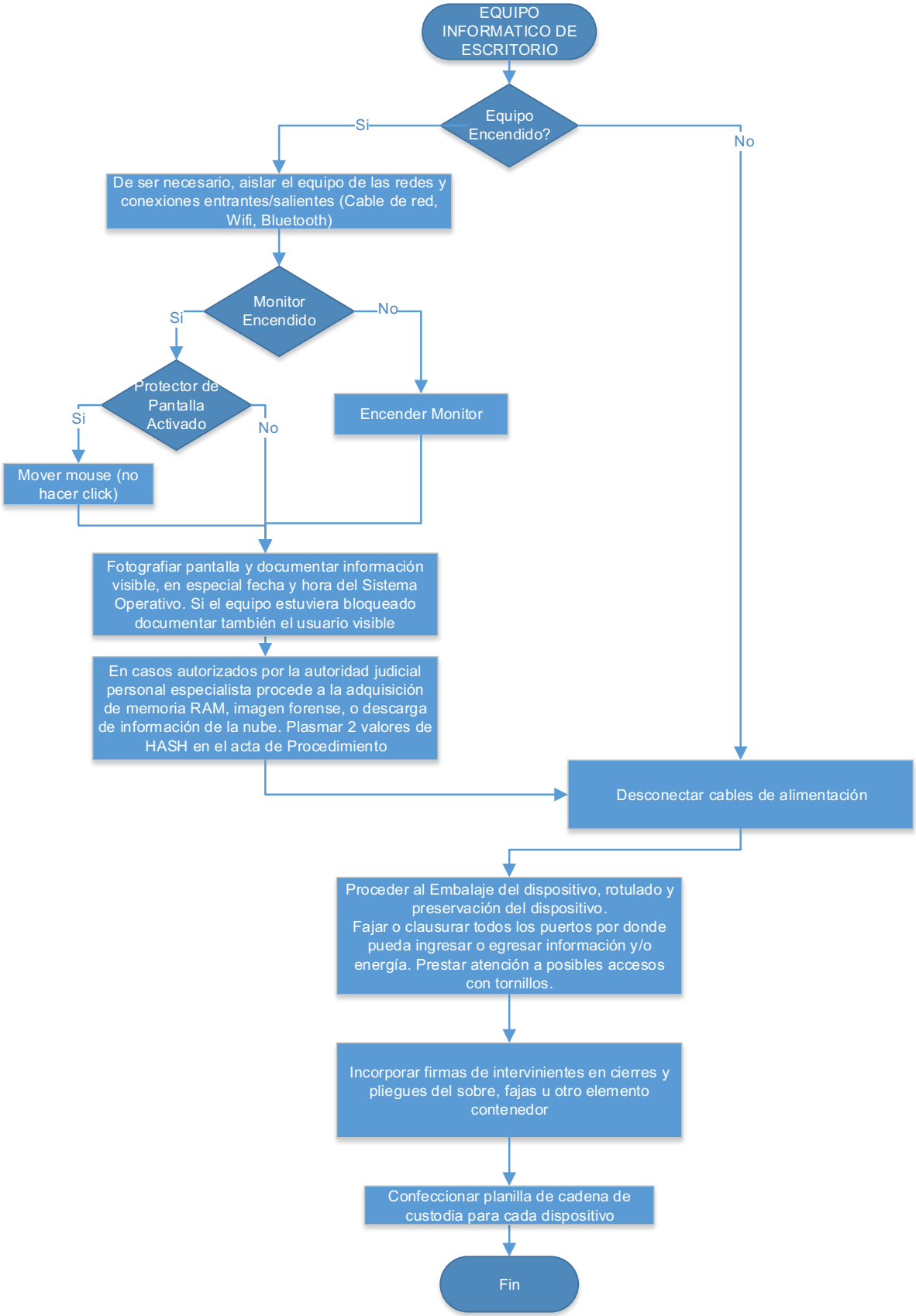
- En el caso particular de telefonía celular se recomienda hacer un formulario por cada teléfono celular por usuario.

ANEXO 4 – DIAGRAMAS DE FLUJO

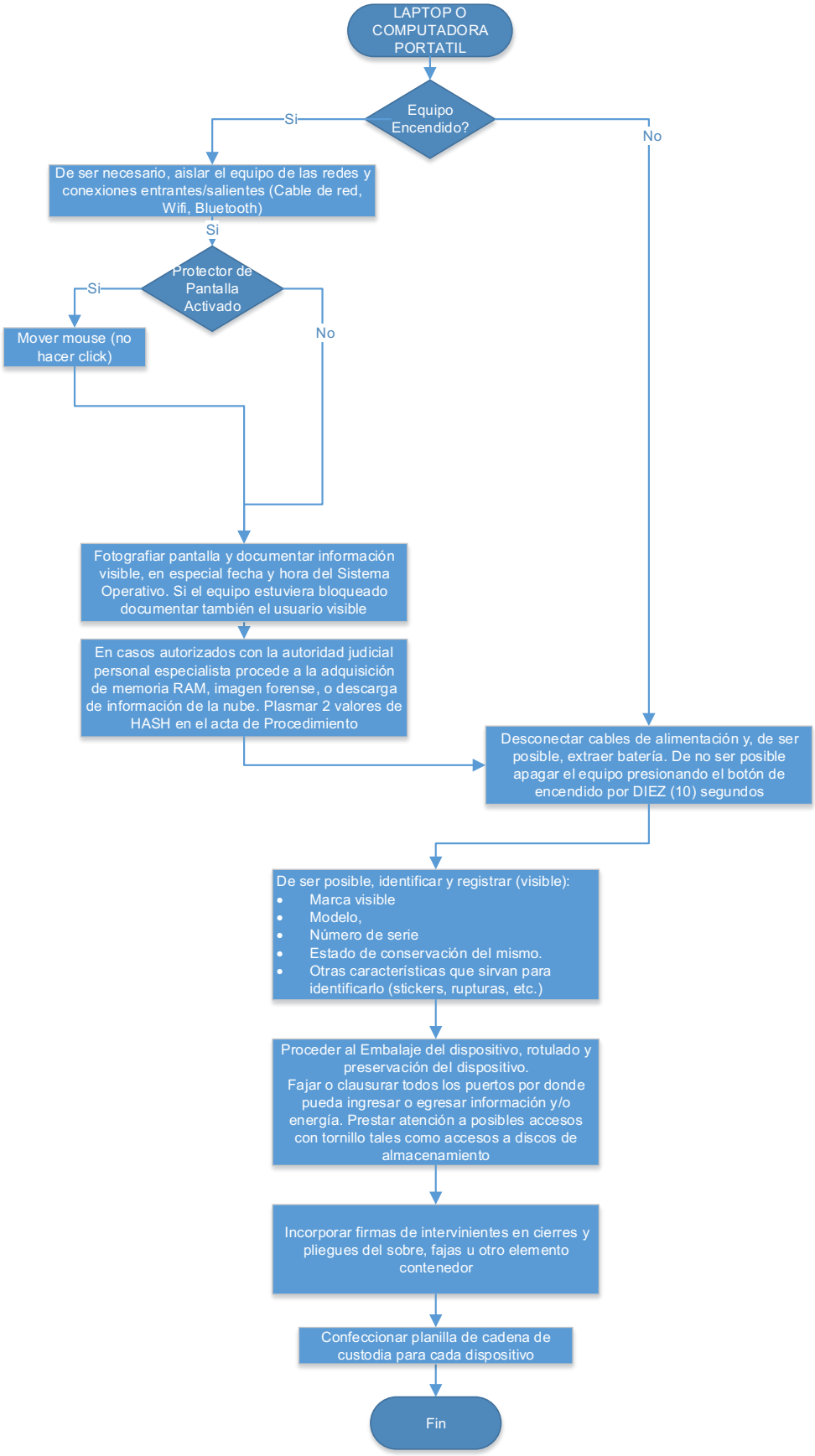
PRIMERA INTERVENCION – DISPOSITIVOS MÓVILES Y CELULARES



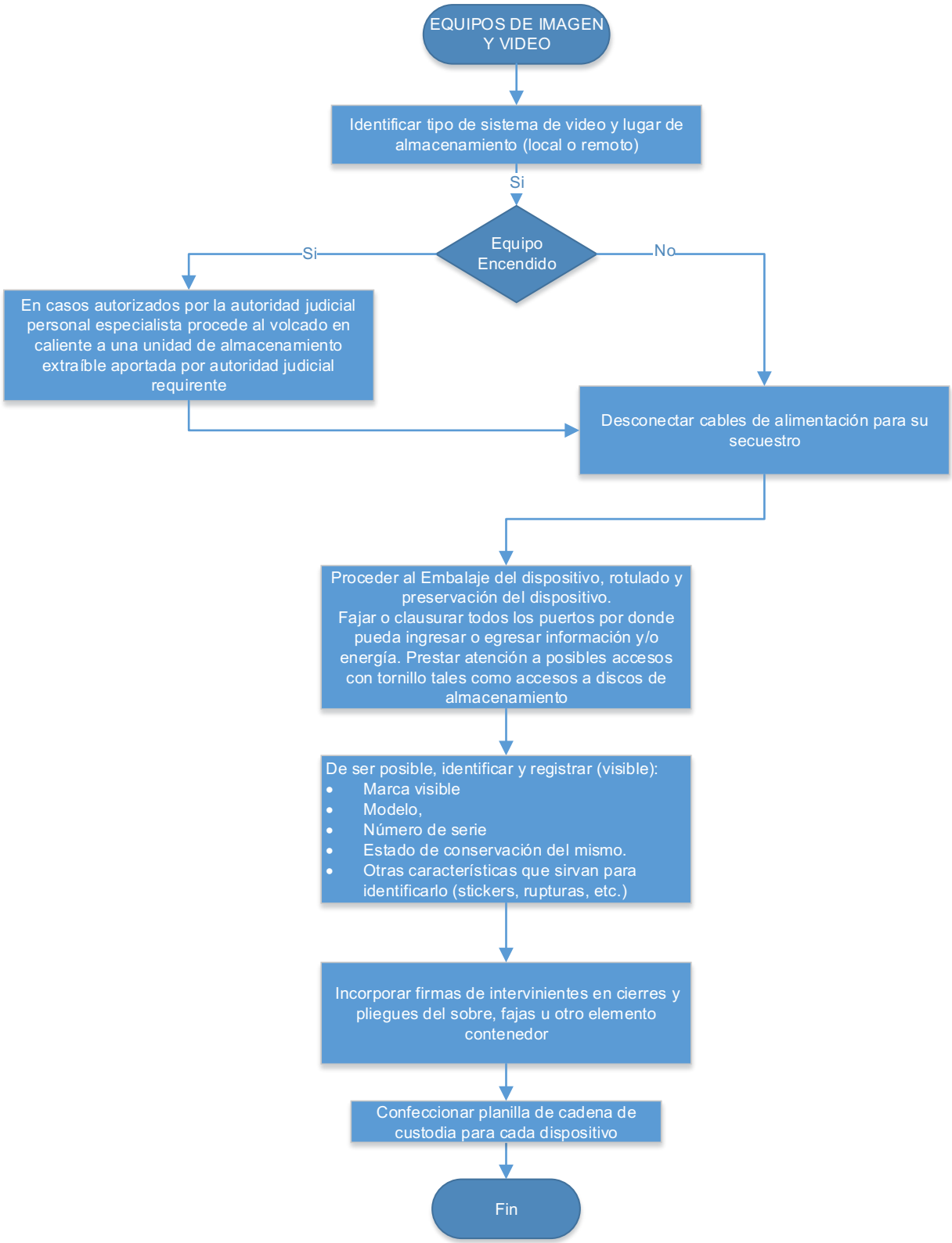
PRIMERA INTERVENCION – EQUIPOS INFORMÁTICO DE ESCRITORIO



PRIMERA INTERVENCION – LAPTOPS O COMPUTADORA PORTATIL



PRIMERA INTERVENCION – EQUIPOS DE IMAGEN Y VIDEO



APARTADO BIBLIOGRAFIA DE CONSULTA

- “Protocolo de Actuación para la Investigación Científica en el Lugar del Hecho” – Ministerio de Seguridad de la Nación Argentina - 2021
- “Tecnología de la información. Técnicas de seguridad. Guías para la identificación, la recolección, la adquisición y la preservación de la evidencia digital” - IRAM-ISO-IEC – Norma 27037:2022
- “Guía sobre Aspectos Relevantes y Pasos Apropiados para la Investigación, Identificación, Incautación y Decomiso de Activos Virtuales” – GAFILAT, diciembre 2021.
- “Guía actualizada para un enfoque basado en el riesgo. Activos virtuales y Proveedores de Servicios de Activos Virtuales”- GAFI, 2021

MIEMBROS DEL EQUIPO DE TRABAJO

MINISTERIO DE SEGURIDAD DE LA NACION ARGENTINA

Pedro JANICES, Director de Investigaciones del Ciberdelito

Alejandro Alberto CORVETTO, Dirección de Investigaciones del Ciberdelito

POLICÍA FEDERAL ARGENTINA

Comisario Víctor AQUINO, Jefe de la División Pericias Informáticas y Electrónicas.

Sargento Primero Walter Pedro NUÑEZ, División Pericias Telefónicas. Profesor de la Escuela de Inteligencia Criminal

Sargento Cristian Fabián GIMENEZ, División Pericias Telefónicas

GENDARMERÍA NACIONAL ARGENTINA

Comandante Bruno DIAZ, Jefe de la división Informática Forense

Primer Alférez Gustavo ALEGRE, Auxiliar División Informática Forense

Alférez Marcio Maximiliano BASILOFF, Instructor e Investigador de la Subdirección de Investigación de Delitos Tecnológicos

Cabo Primero Fabricio Ezequiel REVOLERO, Investigador de la Subdirección de Investigación de Delitos Tecnológicos

POLICÍA DE SEGURIDAD AEROPORTUARIA

Carolina Belén PALACIO, Directora de Delitos Complejos.

Oficial Principal Camila Dafne SEREN, Auxiliar de la Oficina de Criminalística -Informática Forense.

PREFECTURA NAVAL ARGENTINA

Subprefecto Rubén Darío GALEANO, Segundo Jefe de la División Pericias Informáticas y Telefónicas

Cabo Segundo Martín PIROTTI, Auxiliar de la División Pericias Informáticas.

MINISTERIO PUBLICO FISCAL DE LA NACIÓN

Juan DOLLERA, Coordinación Institucional

Ezequiel AURTENECHEA, Subsecretario administrativo DATIP

Nicolás SANGUINETI, Subsecretario administrativo DATIP

Matías GRONDONA, Subsecretario Administrativo UFECI

Christian MANSILLA, Auxiliar Fiscal UFECI

Antonio Javier MAZA, Oficial Mayor UFECI

Horacio AZZOLIN, Titular de la Unidad Fiscal Especializada en Ciberdelincuencia

Romina DEL BUONO, Titular de la Dirección General de Investigaciones y apoyo Tecnológico a la investigación penal