



Ministerio  
del Interior

Dirección Nacional  
de Políticas de Género



# Guía de buenas prácticas para el manejo de evidencia digital en delitos de violencia de género facilitada por la tecnología (VBGFT)



Naciones Unidas  
Oficina contra  
la Droga y el Delito

# **Guía de buenas prácticas para el manejo de evidencia digital en delitos de violencia de género facilitada por la tecnología**

Montevideo, 2026  
© Ministerio del Interior  
© PNUD Uruguay  
ISBN: 978-92-95114-89-0

La “Guía de buenas prácticas para el manejo de evidencia digital en delitos de violencia de género facilitada por la tecnología” fue realizada en el marco del proyecto “Violencia basada en género en el ámbito digital” que está siendo ejecutado por la Fiscalía General de la Nación y el Ministerio del Interior, con apoyo del Programa de las Naciones Unidas para el Desarrollo (PNUD) y la financiación de la República de Corea a través de su Agencia Nacional de Policía.

Esta Guía tiene como finalidad fortalecer las capacidades institucionales para el manejo de la evidencia digital en investigaciones de delitos sexuales, especialmente en casos de violencia de género facilitada por la tecnología (VBGFT).

---

Este documento es para distribución general del Ministerio del Interior.

Se reservan los derechos de autoría y se autorizan las reproducciones y traducciones siempre que se cite la fuente.

Queda prohibido todo uso de esta obra, de sus reproducciones o de sus traducciones con fines comerciales.

---

Los puntos de vista, las designaciones y las recomendaciones presentadas en este informe no reflejan necesariamente la postura oficial del PNUD. Se agradece la difusión y reproducción en cualquier medio, con indicación de la fuente.

El uso genérico del masculino que se utiliza en esta publicación responde a la intención de simplificar la redacción y disminuir la sobrecarga en la lectura. Por lo tanto, de ninguna manera pretende constituir una discriminación entre mujeres y varones, lo cual es una preocupación para este equipo de trabajo.

# **Guía de buenas prácticas para el manejo de evidencia digital en delitos de violencia de género facilitada por la tecnología (VBGFT)**

## **Autoridades del Ministerio del Interior**

### **Ministro del Interior**

Dr. Carlos Negro

### **Subsecretaria**

Cra. Gabriela Valverde

### **Director General de Secretaría**

Dr. Gerardo Siri

### **Subdirector General de Secretaría**

Crio. Gral. (PT) (R) Dr. Ruben Amato

### **Director de la Policía Nacional**

Crio. General (R) José Azambuya

### **Subdirector de la Policía Nacional**

Crio. Gral. (R) Julio Sena

---

## **Autoridades de la Dirección Nacional de Políticas de Género**

### **Encargada de la Dirección Nacional de Políticas de Género**

Cria. Mayor (PE) Lic. July Zabaleta

### **Subdirectora Nacional de Políticas de Género**

Cria. Mayor (PT) Esc./Lic. Cecilia Erhardt Ayala

---

## **Autoridades de la Dirección Nacional de Policía Científica**

### **Director Nacional de Policía Científica**

Crio. Gral. Fernando Noble

### **Subdirector Nacional de Policía Científica**

Crio. Mayor Edgar Duarte

## **Autoridades de la Dirección de Investigaciones de la Policía Nacional**

### **Director General de Ciberdelitos**

Crio. Gral. Paulo Rocha

### **Subdirector de Ciberdelitos**

Crio. Mayor Winston Rodríguez

---

## **Autoridades de organismos de cooperación internacional**

### **Programa de las Naciones Unidas para el Desarrollo (PNUD) Representante Residente**

Stefano Pettinato

**Oficina de las Naciones Unidas  
contra la Droga y el Delito (UNODC)  
Jefa de Oficina de UNODC en  
Uruguay y Coordinadora Regional  
de Ciberdelito para Sudamérica**  
Mariana Kiefer

Para la elaboración de esta guía se conformó un grupo de trabajo integrado por actores clave de distintas instituciones. Agradecemos especialmente los aportes y la colaboración de las siguientes personas e instituciones:

**Dirección Nacional de Políticas de Género**

**Coordinación Técnica Especializada**

Cria. Dra. Laura Labarfois.

**Departamento de Cooperación y Gestión de Programas y Proyectos**

Subcomisaria (PE) T/A Mercedes Arzúa, Encargada del Departamento.

Cabo (PA) Romina Fleitas.

Agente (PA) Diego Meneses.

**Dirección General de Ciberdelitos**

Of. Ayte. Alexandra Rodríguez, Encargada del Departamento de Delitos contra Niños, Niñas y Adolescentes.

Sargento Richard Terán.

**Dirección Nacional de Policía Científica**

Crio. Mayor Lic. EEP. Ivor Álvarez, coordinador ejecutivo de la Dirección Nacional de Policía Científica.

**Unidad de Víctimas y Testigos de la Fiscalía General de la Nación**

Lic. Manuela Reguera, directora.

Lic. Cecilia Capozzoli, subdirectora.

**Oficina de las Naciones Unidas contra la Droga y el Delito (UNODC)**

Mariana Kiefer, Jefa de Oficina de UNODC en Uruguay y Coordinadora Regional de Ciberdelito para Sudamérica.

Carla Cohen, Especialista en investigaciones en entornos digitales.

Agostina Miquelarena, Experta en criptomonedas y blockchain.

**Programa de las Naciones Unidas para el Desarrollo (PNUD)**

Mariela Sorari, Analista especializada en Estado de Derecho y Derechos Humanos.



Ministerio  
del Interior

Expte. N° 2026-4-1-0008167

Montevideo, **15 OCT. 2026**

VISTO: el proyecto de “Guía de buenas prácticas para el manejo de evidencia digital en delitos de violencia de género facilitada por la tecnología (VGFT)”;

RESULTANDO: I) que el referido proyecto está dirigido al personal de primera respuesta en casos de violencia de género facilitada por la tecnología – operadores de la Fiscalía General de la Nación y de la Policía Nacional, así como otros actores del sistema de justicia que intervengan en investigaciones de delitos sexuales con componentes digitales;

II) que la referida Guía, posee como objetivo establecer buenas prácticas aplicables a la fase preliminar de la investigación policial en el ámbito penal, abarcando desde la recepción de la denuncia hasta la preservación y documentación primaria de elementos digitales, contribuyendo así a la integridad probatoria y a la conservación de datos de interés;

III) que a fojas 60 del informe de la Subdirectora de la Dirección Nacional de Políticas de Género surge que las autoridades de la Dirección General de Ciberdelitos y la Dirección Nacional de Policía Científica avalan el mencionado proyecto;

CONSIDERANDO: I) que la Asesoría Letrada del señor Ministro, el 13 de octubre de 2026, informa, que la mencionada Guía es un instrumento de orientación técnica con la finalidad de fortalecer la actuación policial en las

etapas iniciales de la investigación (especialmente en la recepción de denuncias y preservación de evidencia digital, procurando garantizar su integridad y evitar la revictimización);-----

II) que en virtud de lo expuesto, no existiendo objeciones jurídicas, corresponde aprobar la Guía referida, en razón de su evidente utilidad;-----

ATENTO: a lo expuesto y a lo dispuesto por la Asesoría Letrada del señor Ministro;-----

EL MINISTRO DEL INTERIOR

RESUELVE:

- 1º) APRUÉBASE el proyecto de “Guía de buenas prácticas para el manejo de evidencia digital en delitos de violencia de género facilitada por la tecnología (VGFT)”;-----
- 2º) PASE por su orden a la Dirección Nacional de Políticas de Género, Dirección General de Ciberdelitos y Dirección Nacional de Policía Científica para conocimiento y demás efectos pertinentes. Oportunamente, archívese.-----

DPN/RC

  
Dr. CARLOS NEGRO FERNÁNDEZ  
Ministro del Interior

# Índice

|    |                                                                               |
|----|-------------------------------------------------------------------------------|
| 10 | <b>01. Presentación, alcance y objetivos</b>                                  |
| 12 | <b>02. Contexto tecnológico y naturaleza de la evidencia digital</b>          |
| 14 | <b>03. Recepción de la denuncia</b>                                           |
| 14 | Sobre la participación de la víctima en los procedimientos técnicos           |
| 16 | <b>04. Evidencia digital en poder de la víctima</b>                           |
| 17 | A. Información almacenada en dispositivos de la víctima                       |
| 18 | B. Conversaciones en plataformas de mensajería                                |
| 18 | C. Información asociada a cuentas de redes sociales                           |
| 19 | D. Correos electrónicos y servicios en la nube                                |
| 20 | <b>05. Consideraciones técnicas para la preservación de evidencia digital</b> |
| 20 | Buenas prácticas recomendadas                                                 |
| 21 | A. Hash: garantía técnica de inalterabilidad                                  |
| 23 | B. Consideración especial: archivos de texto plano (.TXT)                     |
| 24 | C. Contenido recomendado en el informe de procedimiento                       |
| 27 | <b>06. Métodos de preservación según el tipo de evidencia</b>                 |
| 27 | A. Evidencia almacenada en la memoria del dispositivo                         |
| 29 | B. Evidencia almacenada en servicios de nube                                  |

|           |                                                                                                                                                                    |
|-----------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>33</b> | <b>07. Casos especiales y situaciones particulares</b>                                                                                                             |
| <b>33</b> | A. Dispositivos iOS sin funcionalidad de exportación nativa                                                                                                        |
| <b>34</b> | B. Mensajes o archivos eliminados                                                                                                                                  |
| <b>34</b> | C. Aplicaciones con cifrado de extremo a extremo                                                                                                                   |
| <b>35</b> | D. Mensajería efímera o con autodestrucción                                                                                                                        |
| <b>36</b> | E. Múltiples dispositivos vinculados                                                                                                                               |
| <b>37</b> | F. Autenticación de dos factores                                                                                                                                   |
| <b>38</b> | <b>08. Cadena de custodia</b>                                                                                                                                      |
| <b>39</b> | <b>09. Consideraciones finales</b>                                                                                                                                 |
| <b>41</b> | <b>10. Glosario</b>                                                                                                                                                |
| <b>45</b> | <b>11. Bibliografía</b>                                                                                                                                            |
| <b>48</b> | <b>Anexo I. Modelo de formulario de cadena de custodia</b>                                                                                                         |
| <b>54</b> | <b>Anexo II. Procedimiento establecido por la Dirección Nacional de Policía Científica para la colección de indicios y evidencias de dispositivos informáticos</b> |

# 01. Presentación, alcance y objetivos

Esta guía busca fortalecer las capacidades institucionales para el manejo de la evidencia digital en investigaciones de delitos sexuales, especialmente en casos de violencia de género facilitada por la tecnología (VBGFT).

En particular, el documento busca brindar buenas prácticas aplicables en la recepción de la denuncia por parte de la víctima o denunciante. Está dirigido a los primeros respondientes para la preservación y documentación inicial de la evidencia digital, y su aplicación está prevista para aquellos casos en los que no se cuente con otras herramientas forenses inmediatas, contribuyendo así a reducir riesgos probatorios y a evitar la pérdida o alteración de información relevante.

El documento está dirigido a los primeros respondientes en casos de violencia de género facilitado por la tecnología, circunscribiendo su aplicación a las etapas iniciales de la investigación, específicamente cuando las víctimas o denunciantes se acercan a centros de denuncia que no cuentan con herramientas forenses.

De acuerdo con los desafíos advertidos en Uruguay, el objetivo es asegurar la preservación inicial de la evidencia aportada al sistema de justicia. Todo esto se establece sin perjuicio de la implementación de otras medidas de preservación que puedan ejecutarse posteriormente, ya sea a través de herramientas forenses especializadas o mediante solicitudes formales a los proveedores de servicios electrónicos.

Las recomendaciones en esta guía se basan en lineamientos técnicos reconocidos y la experiencia práctica acumulada en investigaciones de ciberdelitos y delitos sexuales, con especial énfasis en un enfoque centrado en la víctima, la protección de derechos fundamentales y la correcta preservación de la cadena de custodia de la evidencia digital.

## 02. Contexto tecnológico y naturaleza de la evidencia digital

Las conductas en estudio pueden desarrollarse a través de diversos medios tecnológicos, tales como plataformas de mensajería instantánea, correos electrónicos, salas de chat de juegos en red, redes sociales, plataformas de streaming y otros servicios digitales.

En este marco, los hechos denunciados pueden abarcar situaciones diversas: conversaciones o intercambios realizados a través de aplicaciones de mensajería, contenido publicado o distribuido en redes sociales, material íntimo compartido sin consentimiento, imágenes o videos alojados en sitios web, y en algunos casos, contenido generado o modificado mediante herramientas digitales. En todos estos supuestos, los principios de preservación descritos en esta guía resultan aplicables, aunque los métodos concretos pueden variar según el entorno en que se encuentre la evidencia.

De acuerdo con los estándares internacionales, un sistema informático comprende todo dispositivo o conjunto de dispositivos interconectados cuya función sea el procesamiento automatizado de datos, incluyendo los medios de almacenamiento y comunicación asociados<sup>1</sup>. Esto incluye computadoras, laptops, teléfonos móviles, tablets y servicios basados en la nube.

---

1. Artículo 1, inciso a), del Convenio sobre la Ciberdelincuencia (Consejo de Europa, 2001).

Esta diversidad tecnológica implica que la evidencia digital relevante puede encontrarse:

- en la memoria interna de un dispositivo,
- en servicios de almacenamiento en la nube,
- o distribuida entre ambos entornos.

A diferencia de la evidencia física, la evidencia digital presenta características particulares que inciden directamente en su manejo, tales como su volatilidad, la posibilidad de modificación o eliminación, presencial o remota, como así también la posibilidad de que cuente con metadatos<sup>2</sup> y se pueda duplicar, entre otras.

En muchos casos, la persona que realiza la denuncia mantiene acceso directo y legítimo a la información vinculada a los hechos denunciados, ya sea a través de sus dispositivos personales o mediante sus credenciales de acceso a plataformas y servicios digitales.

Esta situación puede resultar especialmente relevante en las etapas iniciales del proceso, dado que la información puede perderse, alterarse o eliminarse si no se adoptan medidas oportunas de identificación y preservación.

En este contexto, el adecuado manejo de la evidencia digital desde el primer contacto institucional puede resultar de suma importancia para contribuir a preservar su integridad, autenticidad y utilidad probatoria en etapas posteriores del proceso.

---

2. El metadato refiere a la información adicional que no está directamente relacionada con el objeto preservado. Por ejemplo, en un documento de texto, donde el dato es el texto redactado en sí mismo y un metadato puede ser la fecha en la que el documento fue creado o el autor del mismo (Presman, G. 2018, p. 305).

## 03. Recepción de la denuncia

La recepción de la denuncia suele constituir una etapa relevante en este tipo de investigaciones, en tanto suele ser el primer contacto institucional de la víctima y el punto de partida para la adopción de medidas urgentes de investigación.

En este tipo de casos, el factor tiempo puede adquirir una especial consideración, ya que por las características inherentes de la evidencia digital mencionadas con anterioridad, la misma puede eliminarse, modificarse o alterarse, ya sea por el funcionamiento propio de las plataformas, por acciones de terceros o por el uso cotidiano de los dispositivos involucrados.

La manera en que se recibe la denuncia puede permitir la identificación temprana de evidencia digital de interés para la investigación, facilitar la orientación de las primeras decisiones investigativas y contribuir a reducir la necesidad de realizar ampliaciones posteriores con la víctima, evitando reiteraciones innecesarias del relato y posibles situaciones de revictimización.

### **Sobre la participación de la víctima en los procedimientos técnicos:**

Una consideración particular de este tipo de investigaciones es que, en muchos casos, la preservación de evidencia digital requiere la intervención activa de la propia víctima: acceder a su dispositivo personal, ingresar sus credenciales en plataformas y ejecutar pasos técnicos bajo supervisión del funcionario actuante, entendi-

do por tal a quien lleva adelante la preservación y no a un superior jerárquico. Esta necesidad puede entrar en tensión con el principio de minimizar la carga sobre la víctima durante las etapas iniciales del proceso.

En este sentido, se recomienda que el funcionario explique con anticipación y en lenguaje claro cuáles serán los pasos del procedimiento, qué información se va a preservar y cuál es el propósito de cada acción. La víctima debe comprender que mantiene el control de sus credenciales y dispositivos en todo momento: el funcionario no solicita ni almacena contraseñas o códigos de verificación, siendo la propia víctima quien los ingresa cuando el sistema los requiere.

Cuando la situación de la víctima lo justifique —por ejemplo, en casos de alto impacto emocional, dificultades para manejar los procedimientos técnicos, o cuando la víctima prefiera no quedar expuesta directamente al contenido que se está preservando— puede considerarse la participación de un representante de confianza, como un familiar, una persona de apoyo designada o un profesional legal, quien pueda acompañar o incluso ejecutar algunos de los pasos bajo la supervisión del funcionario, dentro del marco legal aplicable y con la autorización expresa de la víctima. En los casos en que la víctima sea menor de edad, la presencia de un adulto responsable es siempre requerida.

El objetivo de estas consideraciones es que la víctima pueda atravesar el proceso de preservación sin que ello implique una carga innecesaria o una exposición adicional a los hechos denunciados, contribuyendo a reducir el riesgo de revictimización desde el primer contacto institucional.

## 04. Evidencia digital en poder de la víctima

Las víctimas pueden presentarse ante las autoridades con uno o más dispositivos tecnológicos, como teléfonos móviles, computadoras u otros equipos. Estos dispositivos pueden contener evidencia digital almacenada en su memoria interna. Alternativamente, la víctima puede tener acceso a información alojada en servicios de almacenamiento en la nube vinculados a plataformas de mensajería, redes sociales, correo electrónico u otros servicios en línea, sin que necesariamente exista una copia de esta información en la memoria del dispositivo.

Por ejemplo, una conversación de WhatsApp puede estar almacenada en la memoria del teléfono de la víctima, pero las imágenes asociadas a esa conversación pueden estar únicamente en los servidores de la empresa (Meta), es decir en la nube. En otros casos, como con Instagram Direct, los mensajes pueden existir solo en la nube y no tener copia local en el dispositivo.

Tradicionalmente, una de las medidas más utilizadas para resguardar este tipo de evidencia ha sido y sigue siendo el secuestro del soporte físico (hardware), método que puede presentar dificultades cuando su adopción supone el secuestro de un número importante de dispositivos, los datos están alojados en un servidor de una oficina o empresa o se trata -como es lógico suponer—de uno o más dispositivos de la víctima que resultan de uso habitual y permanente para las distintas actividades de su vida.

Asimismo, la expansión de los servicios de computación en la nube ha modificado los escenarios de investigación, en tanto parte significativa de la información de interés puede no encontrarse en la

memoria interna del dispositivo, sino en servidores externos administrados por terceros proveedores de servicios digitales.

En este contexto, puede resultar pertinente considerar alternativas de preservación de la evidencia digital que permitan resguardar la información de interés para la investigación, sin recurrir de manera automática, en el caso que sea posible, a medidas que puedan resultar gravosas para la víctima, y siempre dentro del marco legal aplicable y las competencias de cada actor interviniente, evitando la revictimización.

Es por lo descripto con antelación, que la preservación o resguardo de evidencia digital contenida en el dispositivo, en la nube o en sitios web, requiere de la implementación de procedimientos que permitan documentar adecuadamente la autenticidad de la información obtenida, y contribuir a verificar su inalterabilidad.

A continuación, se describen tipos de información que, según el caso, pueden ser objeto de preservación inicial, atendiendo a su naturaleza y al entorno en el que se encuentran alojados, siempre que se adopten medidas adecuadas de documentación y resguardo de la integridad, las cuales serán detalladas en próximas secciones.

#### **A. Información almacenada en dispositivos de la víctima**

En los dispositivos móviles o computadoras de la víctima puede encontrarse evidencia digital relevante, como conversaciones, archivos multimedia o registros de actividad, vinculados a los hechos denunciados.

Dado que estos dispositivos suelen ser de uso cotidiano y permanente, se recomienda que la adopción de medidas de preservación pondere la protección de los derechos de la víctima, evitando prácticas invasivas o innecesarias, como el secuestro prolongado del dispositivo, cuando existan alternativas menos gravosas.

## **B. Conversaciones en plataformas de mensajería**

Las aplicaciones de mensajería instantánea suelen constituir una de las principales fuentes de evidencia digital en investigaciones de delitos sexuales.

En aquellos supuestos en que la plataforma lo permita<sup>3</sup>, es posible preservar conversaciones completas, ya sea desde la versión web o desde la aplicación del dispositivo móvil<sup>4</sup>, incluyendo conversaciones, mensajes de audios, imágenes y otros archivos adjuntos, a través de las funcionalidades disponibles en la propia aplicación, sin realizar intervenciones adicionales sobre el dispositivo.

Estas opciones de exportación permiten compartir dichos archivos exportados a otro contacto a través de plataformas de mensajería instantánea, correo electrónico, y opciones de almacenamiento en la nube, entre otros. En estos casos, el producto de la exportación debe ser compartido a un contacto institucional, preferentemente un correo electrónico.

## **C. Información asociada a cuentas de redes sociales**

Las redes sociales y plataformas digitales suelen contar con herramientas que permiten a los usuarios de las mismas acceder y descargar información vinculada a sus cuentas, como mensajes, comentarios y reacciones, publicaciones, interacciones u otros datos de actividad, y exportar una copia de la misma a un servicio externo o al propio dispositivo del usuario, tales como los servicios de la empresa Meta (Instagram y Facebook)<sup>5</sup>.

---

3. Dupuy y Neme (2023), pp. 257 - 260.

4. WhatsApp. (s. f.).

5. Meta. (s. f.).

Estas funcionalidades pueden resultar útiles para preservar evidencia digital en etapas tempranas de la investigación, como así también poder identificar de manera inequívoca a las cuentas que mantuvieron contacto con la víctima, a través de indicadores como el ID o URL completa del perfil.

La utilización de estas herramientas no sustituye los requerimientos formales que puedan realizarse posteriormente a los proveedores de servicios electrónicos, pero puede contribuir a asegurar información relevante que, de otro modo, podría perderse.

#### **D. Correos electrónicos y servicios en la nube**

Los correos electrónicos y los servicios de almacenamiento en la nube (Google Drive, Dropbox, OneDrive) pueden contener información relevante no solo en el contenido visible (mensajes, archivos), sino también en los metadatos asociados a la cabecera del mismo: fecha y hora de creación, dirección IP<sup>6</sup> desde donde se envió, destinatarios ocultos, historial de modificaciones de documentos, entre otros datos técnicos.

Identificados los principales tipos de información digital que pueden ser objeto de preservación inicial, las siguientes secciones detallan las consideraciones técnicas y los métodos procedimentales para llevarla a cabo.

---

4. La IP o Internet Protocol, es un conjunto de números y/o letras, dependiendo de la versión, que identifican a una interfaz de un dispositivo dentro de una red que utilice el protocolo IP. Existen dos tipos, la pública y la privada. La primera de ellas es la que tiene asignada cualquier equipo o dispositivo conectado de forma directa a Internet, siendo siempre únicas. La segunda de ellas se utiliza para identificar equipos o dispositivos dentro de una red doméstica o privada (Giaccaglia, Lamperti y Nuñez, 2017, p. 194). Por ejemplo, la dirección IP pública es la que normalmente queda registrada en los servidores de plataformas o proveedores de servicios cuando un usuario se conecta, lo que permite asociar esa conexión a un proveedor de Internet determinado, y eventualmente, a un domicilio o titular del servicio mediante el requerimiento correspondiente.

## 05. Consideraciones técnicas para la preservación de evidencia digital

Cabe destacar que estas medidas están pensadas para la actuación de los primeros respondientes en los momentos iniciales del caso, cuando no se dispone con herramientas forenses disponibles para realizar una preservación inmediata. Ello no obsta a que la evidencia sea posteriormente preservada mediante las herramientas tecnológicas disponibles en la Policía Nacional y/o la Fiscalía General.

Dentro de este marco, se recomienda que toda acción de obtención o preservación de evidencia digital se realice con la autorización expresa de la víctima, dentro de los límites de dicha autorización, y se documente adecuadamente. Asimismo, en caso de que la víctima sea menor de edad, resulta necesario contar con la presencia de un adulto responsable del/la menor. Esta documentación contribuye a respaldar la autenticidad, integridad y trazabilidad de la información preservada en etapas posteriores del proceso, conforme al marco legal aplicable en cada jurisdicción.

### **Buenas prácticas recomendadas**

La adecuada preservación de evidencia digital se beneficia del cumplimiento de tres buenas prácticas identificadas en la materia, que podrán ser aplicadas por el órgano de investigación que corresponda -Fiscalía o Policía-.

En primer lugar, se recomienda obtener la autorización y consentimiento de la víctima. Esto implica contar con una autorización expresa y documentada de la misma, estableciendo una delimitación clara del alcance del acceso permitido. Es fundamental respetar la privacidad de la persona, accediendo únicamente a información relacionada con los hechos denunciados.

En segundo lugar, se considera una buena práctica la documentación completa del procedimiento. Esta documentación puede materializarse en un informe detallado que cumpla con las formalidades establecidas en la legislación aplicable, incluyendo una descripción clara y secuencial de cada paso realizado durante el proceso de preservación. Asimismo, resulta conveniente que quede registro de todas las personas que intervinieron en el procedimiento.

En tercer lugar, se recomienda que tanto la Fiscalía como la policía pueda implementar mecanismos que contribuyan a documentar la inalterabilidad de la evidencia obtenida. Para ello, existen métodos técnicos que permiten verificar que la evidencia no fue modificada desde su obtención hasta su eventual análisis o presentación. Estos métodos facilitan el mantenimiento de la cadena de custodia desde el momento mismo de la obtención de la evidencia.

La implementación conjunta de estos tres principios constituye una práctica recomendada para la preservación de evidencia digital. La valoración de la evidencia así preservada corresponderá a las autoridades competentes de cada jurisdicción, conforme a su marco legal y procesal aplicable.

#### **A. Hash: garantía técnica de inalterabilidad**

El hash es el método técnico ampliamente reconocido para verificar que una evidencia digital no ha sido alterada. Consiste en aplicar un algoritmo matemático que genera una cadena alfanumérica única para cada archivo.

El algoritmo más utilizado hoy día, debido a su seguridad y a estándares internacionales, es el SHA- 256<sup>7</sup>.

Otra de las particularidades de este método es que es unidireccional, esto significa que con el valor hash obtenido no puede reconstruirse el archivo o documento original que dio origen al valor<sup>8</sup>.

El hash funciona como una “huella digital” del archivo. Su principal característica es que cualquier modificación, por mínima que sea, genera un hash completamente diferente. Esto permite verificar la integridad del archivo en cualquier etapa posterior del proceso, simplemente recalculando el hash y comparándolo con el valor original registrado en la documentación. Si ambos valores coinciden, se garantiza que el archivo no ha sufrido cambio alguno desde su preservación inicial<sup>9</sup>.

Para ilustrar el funcionamiento del hash, puede presentarse el siguiente ejemplo práctico. Si tomamos un archivo llamado “conversacion\_whatsapp.txt” con su contenido original, el algoritmo SHA-256 generará un valor como:

**a3f5c8b2e1d4f6a8c9b7e2d1f4a6c8b5e3d7f9a2c4b6e8d1f3a5c7b9e2d4f6a8.**

Si modificamos el archivo, aunque sea agregando un simple punto al final del texto, el hash resultante será completamente diferente:

**f7e2d4c9a6b8e1f3d5a7c9b2e4f6a8d1c3b5e7f9a2d4c6b8e1f3a5c7b9e2d4f6.**

Esta diferencia en el resultado hace que cualquier alteración sea inmediatamente detectable.

---

7. National Institute of Standards and Technology (NIST). (s. f.-a).

8. National Institute of Standards and Technology (NIST). (s. f.-b).

9. Guttman, White & Walraven (2022), p. 7.

Existen diversas herramientas gratuitas y confiables para calcular valores hash<sup>10</sup>, disponibles para los distintos sistemas operativos. Su utilización no requiere conocimientos técnicos avanzados, y el proceso es igualmente válido independientemente de la herramienta o software que se emplee, siempre que se registre en la documentación del procedimiento cuál fue utilizada y cuál es el valor hash obtenido. Esta información contribuye a la trazabilidad de la evidencia en etapas posteriores del proceso.

## **B. Consideración especial: archivos de texto plano (.TXT)**

Los archivos de texto plano, identificados por la extensión .TXT, como los generados por WhatsApp al exportar conversaciones, presentan una particularidad técnica que merece especial atención. Estos archivos son técnicamente modificables entre el momento de su exportación y el cálculo del hash.

Esta característica técnica plantea la necesidad de implementar resguardos procedimentales complementarios que refuercen la confiabilidad de la evidencia preservada. Dentro de los mismos podrían implementarse los siguientes:

- Presencia y certificación del funcionario actuante. Como fedatario público, el funcionario certifica mediante su firma que presenció el procedimiento completo, garantizando que se siguieron todos los pasos establecidos sin que se produjera alteración alguna entre el momento de la exportación y el cálculo del hash. Esta función de fe pública es reconocida en los sistemas procesales como un mecanismo de certificación de actuaciones.
- Informe detallado del procedimiento. Se trata de un documento que cumple con las formalidades establecidas en la legisla-

---

10. Tanto en sistemas operativos Window, como MacOS y Linux, se pueden utilizar herramientas nativas ejecutadas a través de comandos o herramientas descargables.

ción aplicable y que describe cronológicamente cada paso del proceso de preservación. Este informe debe ser firmado por el funcionario actuante y por la víctima que aportó el dispositivo, quedando constancia documental de todo lo actuado.

- Respaldo audiovisual continuo del procedimiento. Esto implica la filmación sin cortes ni edición de todo el procedimiento, desde el momento mismo de la exportación hasta el cálculo del hash. Este registro audiovisual constituye un elemento adicional de documentación que puede ser posteriormente examinado. El propio archivo de video también debe ser hashado para garantizar su inalterabilidad.

La combinación de estos tres resguardos suele utilizarse en la práctica observada de los actores del proceso penal, para abordar la particularidad técnica de los archivos de texto plano, con el fin de fortalecer la documentación del procedimiento de preservación, quedando un registro completo que evidencie la continuidad y trazabilidad de todas las actuaciones realizadas. La evaluación de la suficiencia de estos resguardos para los efectos probatorios corresponderá a las autoridades competentes de cada jurisdicción, conforme a su marco legal aplicable.

### **C. Contenido recomendado en el informe de procedimiento**

Se considera una buena práctica que toda preservación de evidencia digital quede documentada en un informe que permita la trazabilidad del procedimiento. A continuación, se describen los elementos que se recomienda incluir en dicha documentación, mínimamente:

#### **1. Datos de identificación**

- Fecha, hora de inicio y finalización de la medida, y lugar del procedimiento
- Número de expediente o caso (si ya estuviera asignado)

- Oficina actuante (comisaría, fiscalía)
- Identificación completa del funcionario actuante (nombre, cargo, credencial)

## **2. Identificación de la víctima/aportante**

- Nombre completo
- Cédula de identidad
- Datos de contacto

## **3. Testigos**

- Identificación de testigos presentes (si los hubiere)

## **4. Descripción del dispositivo**

- Tipo de dispositivo (teléfono móvil, tablet, computadora)
- Marca y modelo
- Sistema operativo y versión
- Número de serie
- IMEI o identificador único (en dispositivos móviles)
- Estado del dispositivo

## **5. Descripción del procedimiento**

- Plataforma o servicio del cual se extrae información (WhatsApp<sup>11</sup>, Facebook, Instagram, etc.). De ser posible dejar indicada la URL o ID de la cuenta de la víctima.
- Método de extracción utilizado (exportación nativa, descarga de nube, etc.)
- Pasos realizados, descritos de manera clara y secuencial:  
Ejemplo: “1) Se ingresó a la aplicación WhatsApp;  
2) Se abrió la conversación del contacto identificado como ‘Juan Pérez’; 3) Se seleccionó la opción ‘Exportar chat’;  
4) Se eligió la opción ‘Con archivos incluidos’;  
5) Se compartió vía correo electrónico a [dirección]...”
- Archivos obtenidos y sus formatos

---

11. WhatsApp. (s. f.).

## 6. Valores hash

- Algoritmo utilizado (preferentemente SHA-256)
- Valor hash de cada archivo preservado
- Software o herramienta utilizada para el cálculo
- Ejemplo:

**Archivo:** conversacion\_contacto\_juan.txt

**Algoritmo:** SHA-256

**Hash:**

**a3f5c8b2e1d4f6a8c9b7e2d1f4a6c8b5e3d7f9a2c4b6e8df3a5c7b9e2d4f6a8**

**Herramienta:** se deberá indicar el software utilizado

## 7. Respaldo audiovisual (cuando corresponda)

- Descripción del material (video o fotografías)
- Formato del archivo (MP4, AVI, JPG, etc.)
- Duración (en caso de video)
- Valor hash del archivo audiovisual
- Descripción de lo que documenta el video/fotos

## 8. Firmas

- Firma del funcionario actuante
- Firma de la víctima/aportante
- Firma de testigos (si los hubiere)

La inclusión de estos elementos en el informe contribuye a documentar de manera integral el proceso de preservación, facilitando su trazabilidad y posterior evaluación por las autoridades competentes.

## 06. Métodos de preservación según el tipo de evidencia

La estrategia de preservación varía según dónde se encuentre almacenada la información. A continuación, se describen los principales métodos identificados como buenas prácticas para diferentes escenarios.

### A. Evidencia almacenada en la memoria del dispositivo

Cuando la información se encuentra almacenada localmente en el dispositivo de la víctima, existen diferentes métodos de preservación según las características del dispositivo y las funcionalidades disponibles en las aplicaciones involucradas.

#### Método 1: Exportación nativa de aplicaciones

Este método resulta aplicable cuando la aplicación ofrece funcionalidad propia de exportación. Un ejemplo representativo es WhatsApp, que permite exportar conversaciones completas desde la propia aplicación.

El procedimiento general varía ligeramente según el sistema operativo del dispositivo. En dispositivos iOS, se accede a la conversación deseada, se ingresa a la información del contacto, y se selecciona la opción “Exportar chat” disponible al final de la pantalla. En dispositivos Android, se accede a la conversación, se utiliza el menú de opciones (tres puntos verticales), y se selecciona “Más” seguido de “Exportar chat”.

En ambos sistemas operativos, la aplicación ofrece la posibilidad de exportar la conversación sin archivos adjuntos (solo texto) o con archivos adjuntos (incluyendo imágenes, videos y audios). Una vez seleccionada la opción deseada, el archivo puede compartirse mediante diversos métodos.

El producto de la exportación consiste en un archivo de texto plano (.TXT) que contiene la conversación completa. Cuando se incluyen archivos adjuntos, estos se exportan en sus formatos originales junto con el archivo de texto. Es importante tener en cuenta que algunas aplicaciones presentan limitaciones en la cantidad de mensajes o el tamaño de archivos que pueden exportarse.

El procedimiento completo de preservación mediante este método implica que la víctima realice la exportación bajo supervisión del funcionario, quien posteriormente descarga los archivos en su computadora o dispositivo a disposición y calcula el hash de cada archivo inmediatamente después de recibirlos. Se recomienda documentar todo el proceso mediante registro audiovisual cuando sea posible, desde la exportación hasta el cálculo del hash.

## Método 2: Registro de llamadas

Este tipo de información puede ser resguardada de manera manual ingresando al registro de llamadas entrantes y salientes, y documentando dicho listado mediante fotografías tomadas con una cámara externa, para su posterior asiento e incorporación al informe.

De la misma manera es posible acceder a la aplicación de mensajería de WhatsApp y realizar el mismo procedimiento para preservar las llamadas entrantes y salientes de dicha plataforma.

Luego, el órgano encargado de investigar podrá corroborar dichos abonados mediante requerimiento formal a la empresa prestataria de telefonía.

## **B. Evidencia almacenada en servicios de nube**

Cuando la información se encuentra almacenada en servidores de las plataformas digitales y no necesariamente en la memoria local del dispositivo, pueden utilizarse las funcionalidades de descarga que ofrecen las propias plataformas. Este tipo de evidencia es común en redes sociales, servicios de correo electrónico y sistemas de almacenamiento en línea.

Diversas plataformas digitales ofrecen a sus usuarios herramientas para descargar la información asociada a sus cuentas. Estas funcionalidades, generalmente ubicadas en las secciones de configuración o privacidad, permiten exportar datos como mensajes, publicaciones, archivos multimedia, contactos, y otros tipos de información almacenada en la nube. A continuación se describen dos ejemplos representativos de este tipo de herramientas.

### **Método 1: Descarga desde plataformas Meta (Facebook e Instagram)**

Facebook e Instagram son ejemplos de plataformas que ofrecen funcionalidades de descarga de información. El procedimiento general implica que la víctima inicie sesión en su cuenta y acceda a las opciones de configuración y privacidad. Dentro de estas opciones, ambas plataformas presentan una sección denominada “Exporta tu información” o similar. Esta funcionalidad ofrece la posibilidad de elegir entre una descarga completa que incluye toda la información disponible en la cuenta, o una descarga personalizada que permite seleccionar tipos específicos de información.

Adicionalmente, puede configurarse el intervalo de fechas deseado, el formato de exportación (HTML facilita la visualización) y la calidad del contenido multimedia. Una vez configurada la solicitud, la plataforma procesa la información, lo que puede demorar desde minutos hasta varios días según el volumen de datos.

La víctima recibe notificaciones por correo electrónico, primero confirmando la solicitud y posteriormente cuando el archivo está listo para descargar. El producto final es un archivo ZIP que, al descomprimirse, contiene un archivo `index.html` que permite navegar por toda la información descargada de manera estructurada mediante cualquier navegador web.

Este producto puede enviarse al correo institucional de la fiscalía o policía. El cálculo del hash del archivo ZIP inmediatamente después de completarse la descarga y antes de descomprimirlo permite documentar la integridad del archivo, registrando este valor en la documentación del procedimiento.

## Método 2: Google Takeout (Gmail, Drive, Photos y otros servicios)

Google Takeout<sup>12</sup> es otro ejemplo de herramienta que centraliza la exportación de datos de múltiples servicios. El procedimiento implica que la víctima acceda al sitio <https://takeout.google.com> con sus credenciales. La herramienta presenta por defecto todos los servicios de Google seleccionados, permitiendo al usuario mantener esta selección completa o elegir únicamente los servicios que resulten relevantes para la investigación, tales como Gmail, Drive, Google Photos, Contactos, Calendario, entre otros.

Posteriormente, se configura el método de entrega, la frecuencia de exportación, y el formato y tamaño de los archivos. Una vez creada la exportación, el proceso de preparación puede demorar desde horas hasta días según el volumen de información involucrado.

Cuando la exportación está lista, la víctima recibe un correo electrónico con el enlace de descarga. Es importante considerar que estos enlaces suelen tener fecha de vencimiento, por lo que resulta conveniente gestionarlos dentro del plazo establecido. Este producto puede enviarse al correo institucional de la fiscalía o policía.

---

12. Google. (s. f.)

El cálculo del hash de los archivos descargados inmediatamente después de completarse la descarga permite documentar su integridad, registrándose este valor en la documentación del procedimiento.

### **Método 3: Resguardo de correos electrónicos**

En el caso de los correos electrónicos, es posible resguardar no solamente el remitente sino también el contenido del mensaje y sus metadatos. El producto de descarga es un archivo con extensión .eml<sup>13</sup>, el cual puede abrirse sin conexión a Internet, ya que es un archivo local que contiene el mensaje completo, incluyendo texto, cabeceras y archivos adjuntos, almacenado en formato de texto.

Algunos servicios como Gmail permiten en el correo recibido, en la opción de más, descargar el mensaje seleccionado y en la opción de mostrar original, poder acceder a los metadatos del mismo, pudiendo copiarlos en un archivo aparte.

### **Consideraciones generales para métodos de descarga desde la nube**

Aunque las plataformas específicas pueden variar en sus interfaces y opciones, los principios generales de estos procedimientos son similares. Se considera una buena práctica planificar estos procedimientos con anticipación, teniendo en cuenta que los tiempos de preparación pueden extenderse varios días según el volumen de información. Los enlaces de descarga generalmente tienen vigencia limitada, por lo que conviene gestionarlos oportunamente para evitar su vencimiento. Los archivos resultantes pueden ser de gran tamaño, requiriendo espacio suficiente en disco y considerando los tiempos de descarga según la conexión a Internet disponible.

---

13. National Institute of Justice (2008), pg. 66.

En cuanto a aspectos de seguridad y privacidad, se recomienda que la víctima mantenga control de sus credenciales en todo momento. Se sugiere que el funcionario no solicite ni almacene contraseñas de las cuentas de la víctima. Una práctica recomendada consiste en que la víctima realice las descargas bajo supervisión del funcionario, pero ejecutando ella misma los pasos necesarios desde su propia sesión autenticada, manteniendo así el control sobre sus accesos y contraseñas.

## 07. Casos especiales y situaciones particulares

En el desarrollo de las investigaciones pueden presentarse situaciones que requieren consideraciones específicas. A continuación, se describen algunos escenarios que pueden requerir adaptaciones en los procedimientos de preservación.

### A. Dispositivos iOS sin funcionalidad de exportación nativa

Cuando una aplicación en dispositivos iPhone o iPad no ofrece opción de exportación, puede utilizarse la funcionalidad nativa de grabación de pantalla que incorporan estos sistemas operativos. Esta función permite grabar todo lo que se visualiza en la pantalla del dispositivo mientras la víctima navega por la aplicación mostrando la información relevante.

La grabación de pantalla se activa desde el Centro de control del dispositivo mediante un botón específico. Una vez iniciada la grabación, la víctima puede navegar por la aplicación, abrir conversaciones, mostrar perfiles u otra información pertinente. Al finalizar, la grabación se detiene y el video resultante se guarda automáticamente en la aplicación Fotos del dispositivo, desde donde puede compartirse con el funcionario actuante. El funcionario calcula el hash del archivo de video recibido y lo registra en la documentación del procedimiento.

Alternativamente, puede optarse por registrar la pantalla mediante un dispositivo externo, como una cámara o un segundo teléfono. En este caso, el video queda almacenado directamente en ese dispositivo y el funcionario calcula el hash sobre ese archivo, siguiendo el mismo procedimiento de documentación.

## **B. Mensajes o archivos eliminados**

La recuperación de información eliminada de dispositivos digitales constituye un procedimiento técnico especializado que excede el alcance de las actuaciones iniciales de preservación. Cuando se identifica que información relevante ha sido eliminada, se sugiere evitar intentos de recuperación sin personal especializado, ya que acciones inadecuadas pueden comprometer la posibilidad de recuperación posterior.

En estos casos, resulta conveniente documentar inmediatamente qué tipo de información fue eliminada, cuando ocurrió la eliminación según conocimiento de la víctima, y si la información se eliminó solo localmente del dispositivo o también de servicios de nube asociados. Adicionalmente, puede preservarse el dispositivo indicando a la víctima que limite su uso en la medida de lo posible, ya que cada uso nuevo puede sobrescribir el espacio donde estaban almacenados los datos eliminados. En algunos casos, puede considerarse activar el modo avión del dispositivo para evitar sincronizaciones automáticas que pudieran sobrescribir información.

Una vez documentada la situación, se debe contactar al personal especializado en análisis forense digital para evaluar la viabilidad de recuperación mediante herramientas y procedimientos técnicos específicos.

## **C. Aplicaciones con cifrado de extremo a extremo**

Diversas aplicaciones de mensajería, como WhatsApp, Signal, Telegram (en sus chats secretos) e iMessage, implementan cifrado de extremo a extremo. Este tipo de cifrado implica que únicamente el emisor y el receptor pueden leer el contenido de los mensajes, quedando cifrado incluso para la propia plataforma que proporciona el servicio.

Esta característica técnica tiene implicaciones importantes para la preservación de evidencia. Si la víctima ha eliminado la conversación de su dispositivo y no cuenta con respaldo o back up, la información no puede recuperarse desde los servidores de la plataforma, dado que esta no tiene acceso al contenido cifrado. Un requerimiento formal a la empresa proveedora del servicio puede permitir obtener, dependiendo el caso, metadatos asociados, como fechas de mensajes, números o identificadores de cuentas involucradas, direcciones IP de conexión, entre otros, pero no el contenido de las conversaciones cifradas.

Ante esta situación, resulta conveniente verificar si la víctima tiene activados sistemas de respaldo o back up. WhatsApp, por ejemplo, puede configurarse para realizar copias de seguridad en Google Drive (dispositivos Android) o iCloud (dispositivos iOS). Si existe un back up disponible, puede evaluarse la posibilidad de restaurarlo en un dispositivo para luego proceder a la exportación mediante los métodos descritos anteriormente. Este punto deberá ser realizado por personal técnico para evitar alteraciones de la evidencia digital.

Si no existe back up y la información fue eliminada del dispositivo, puede considerarse la posibilidad de recuperación forense del dispositivo según lo indicado en el apartado anterior.

#### **D. Mensajería efímera o con autodestrucción**

Algunas aplicaciones ofrecen funcionalidades de mensajería efímera, donde los mensajes se eliminan automáticamente después de ser visualizados o transcurrido un tiempo determinado. Ejemplos de estas funcionalidades se encuentran en

Snapchat, Instagram (mensajes que desaparecen), Telegram (mensajes auto destruibles) y WhatsApp (mensajes temporales). Estas aplicaciones están diseñadas específicamente para no dejar rastro de las comunicaciones. Cuando los mensajes aún no han desaparecido, resulta fundamental actuar con celeridad.

Si bien se contemplan opciones de grabación de pantalla nativa en dispositivos iOS o Android para registrar la información mientras está visible, se sugiere prioritariamente realizar la documentación fotográfica o filmica del dispositivo y de la información a relevar utilizando un dispositivo externo independiente, como una cámara fotográfica o un segundo teléfono celular. Este método presenta dos ventajas técnicas.

Por un lado, evita alertar a la otra parte: en diversas aplicaciones, la captura de pantalla nativa genera una notificación automática al emisor del mensaje indicando que se ha registrado la pantalla.

Por otro lado, reduce la interacción directa con el software y la configuración interna del dispositivo, minimizando el riesgo de alteración involuntaria de la evidencia.

En caso de utilizar este método de registro externo, se recomienda calcular el valor hash SHA-256 del archivo de video o imagen resultante y registrar ese valor junto con las características del dispositivo externo utilizado.

## **E. Múltiples dispositivos vinculados**

En ocasiones, un usuario tiene su cuenta activa en varios dispositivos simultáneamente. Por ejemplo, WhatsApp puede estar activo en un celular, una tablet y una computadora, o Instagram puede estar abierto en un celular y una computadora al mismo tiempo.

En estos casos, la información puede estar accesible desde cualquiera de esos dispositivos, aunque las sincronizaciones pueden variar entre ellos. Resulta conveniente consultar a la víctima cuántos dispositivos tiene vinculados a la cuenta en cuestión, identificar en cuál de ellos está disponible la información más completa o reciente, y preservar desde ese dispositivo. Asimismo, conviene documentar en el informe la existencia de los otros dispositivos vinculados.

La mayoría de las plataformas permiten verificar qué dispositivos tienen sesiones activas.

## **F. Autenticación de dos factores**

Cuando una cuenta tiene activada la verificación en dos pasos o autenticación de dos factores (2FA), el acceso a la cuenta requiere no solo la contraseña sino también un segundo factor de autenticación, que puede ser un código enviado por SMS, un código generado por una aplicación autenticadora, una huella digital, reconocimiento fácil u otro método.

Durante los procedimientos de preservación que requieran acceso a la cuenta, la víctima necesitará tener disponible este segundo factor de autenticación. Por ejemplo, si el segundo factor es un código SMS, deberá tener acceso a su teléfono para recibir dicho código. Si utiliza una aplicación autenticadora, deberá tener acceso a esa aplicación en su dispositivo.

Es conveniente informar a la víctima previamente que durante el procedimiento es probable que reciba solicitudes de códigos de verificación, y que será necesario ingresarlos para completar el acceso a la información. El funcionario no solicita ni almacena estos códigos de verificación, siendo la víctima quien los ingresa directamente cuando el sistema los requiere.

## 08. Cadena de custodia

Las medidas de preservación descritas en esta guía están orientadas a resguardar la evidencia digital sin necesidad de secuestrar el dispositivo de la víctima. Sin embargo, cuando las circunstancias del caso lo requieran, según lo descrito en el presente documento, puede resultar necesario el envío del dispositivo al Laboratorio Forense correspondiente.

En ese supuesto, el resguardo y traslado deberá realizarse utilizando el modelo de formulario de cadena de custodia adjunto como Anexo I y conforme al procedimiento establecido por la Dirección Nacional de Policía Científica para la colección de indicios y evidencias de dispositivos informáticos, el cual se adjunta como Anexo II.

## 09. Consideraciones finales

La preservación adecuada de evidencia digital constituye un eslabón fundamental dentro de un proceso más amplio de respuesta institucional a los delitos de violencia de género en entornos digitales. Sin embargo, la responsabilidad del primer respondiente no concluye con el cálculo del hash y la suscripción del informe: abarca también garantizar que la víctima comprenda qué sucedió durante el procedimiento, qué pasos siguen a continuación y a qué recursos puede acceder.

En este sentido, se consideran buenas prácticas al cierre de la actuación inicial las siguientes:

**Explicar los pasos siguientes.** La víctima debe conocer, en términos accesibles, qué ocurrirá con la evidencia preservada, quiénes tendrán acceso a ella y en qué etapas del proceso será utilizada. Esta información contribuye a reducir la incertidumbre y a fortalecer la confianza institucional.

**Informar sobre los derechos de la víctima.** El funcionario actuante debe asegurarse de que la víctima conozca sus derechos fundamentales en el proceso, incluyendo el derecho a ser informada sobre el avance de la investigación, a recibir asistencia legal y psicológica, y a no ser expuesta innecesariamente al contenido de la evidencia preservada en etapas posteriores.

**Activar la cadena de derivación.** La preservación de evidencia es solo una dimensión de la respuesta institucional. En paralelo o de manera inmediata, corresponde orientar a la víctima hacia los recursos de apoyo disponibles: asistencia psicológica, asesoramiento legal, servicios de salud. La articulación entre los distintos

actores del sistema —fiscalía, policía, servicios de salud, organizaciones de apoyo— es condición necesaria para una respuesta integral y centrada en la víctima.

**Resguardar la confidencialidad.** Toda la información obtenida durante el procedimiento, incluyendo los datos personales de la víctima, las credenciales utilizadas, el contenido de la evidencia preservada y los datos del caso, debe ser tratada con estricta confidencialidad, accediendo a ella únicamente el personal con competencia directa en la investigación.

La aplicación consistente de las buenas prácticas descritas en esta guía contribuye no solo a preservar la integridad probatoria de la evidencia digital, sino también a garantizar que el primer contacto institucional represente para la víctima un punto de inicio hacia la reparación, y no una fuente adicional de daño.

## 10. Glosario

**1. ALGORITMO DE HASH SHA-256:** SHA-256 (Algoritmo Hashing Seguro de 256 bits) es una función hash creada por la NSA y completada por el NIST en 2001. Toma datos de cualquier longitud y genera un hash de 256 bits (32 bytes), que suele mostrarse como una cadena hexadecimal de 64 caracteres. SHA-256 ofrece una función unidireccional, lo que significa que los datos introducidos no se pueden revertir ni descifrar.

**2. ARCHIVO EML:** La extensión de archivo EML es un acrónimo de E-mail. Un archivo EML es un correo electrónico que se almacena para poder mantener el formato y las cabeceras HTML originales. La estructura del archivo EML es estándar y está compuesta por dos partes, el encabezado y el cuerpo.

**3. AUTENTICACIÓN DE DOS FACTORES (2FA):** Mecanismo de seguridad que requiere que el usuario verifique su identidad mediante dos elementos distintos para acceder a una cuenta: habitualmente, una contraseña y un segundo factor como un código enviado por SMS, un código generado por una aplicación autenticadora, o un dato biométrico como huella digital o reconocimiento facial. Su activación implica que, durante procedimientos de preservación que requieran acceso a la cuenta de la víctima, esta deberá tener disponible ese segundo factor de autenticación.

**4. BACK UP (COPIA DE SEGURIDAD):** Copia de los datos almacenados en un dispositivo o plataforma, generada de forma automática o manual, con el propósito de poder restaurar la información en caso de pérdida, eliminación o daño. Aplicaciones como WhatsApp pueden configurarse para realizar copias de seguridad periódicas en servicios de almacenamiento en la nube como Google Drive o iCloud.

**5. CABECERA DE CORREO ELECTRÓNICO:** Un encabezado de internet de mensaje de correo electrónico proporciona una lista de detalles técnicos sobre el mensaje, como quién lo envió, el software usado para redactarlo y los servidores de correo electrónico por los que se ha transmitido hasta llegar al destinatario.

**6. CADENA DE CUSTODIA:** Registro documentado y cronológico que da cuenta de todas las personas que tuvieron acceso o contacto con la evidencia desde el momento de su obtención hasta su presentación en el proceso judicial. Su mantenimiento tiene por finalidad garantizar la autenticidad e integridad de la evidencia, demostrando que no fue alterada, sustituida o manipulada en ninguna etapa del proceso.

**7. CIFRADO DE EXTREMO A EXTREMO:** Sistema de comunicación mediante el cual únicamente el emisor y el receptor pueden leer el contenido de los mensajes intercambiados. La información viaja cifrada a través de los servidores de la plataforma, sin que esta tenga acceso al contenido. Esta característica implica que, si la víctima ha eliminado una conversación de su dispositivo y no cuenta con un back up, la información no puede recuperarse desde los servidores del proveedor del servicio.

**8. DIRECCIÓN DE IP:** La IP o Internet Protocol, es un conjunto de números y/o letras, dependiendo de la versión, que identifican a una interfaz de un dispositivo dentro de una red que utilice el protocolo IP. Existen dos tipos, la pública y la privada. La primera de ellas es la que tiene asignada cualquier equipo o dispositivo conectado de forma directa a Internet, siendo siempre únicas. La segunda de ellas se utiliza para identificar equipos o dispositivos dentro de una red doméstica o privada.

**9. EVIDENCIA DIGITAL:** Cualquier registro generado por o almacenado en un sistema computacional que puede ser utilizado como evidencia en un proceso legal. La evidencia electrónica es el elemento material de un sistema informático o hardware y la evidencia digital es la información en ellos contenida.

**10. FUNCIÓN HASH:** Una función que asigna una cadena de bits de longitud arbitraria a una cadena de bits de longitud fija. Se espera que las funciones hash aprobadas cumplan las siguientes propiedades: 1. Unidireccional: es computacionalmente inviable encontrar una entrada que se asigne a una salida preespecificada, y 2. Resistente a colisiones: es computacionalmente inviable encontrar dos entradas distintas que se asigne a la misma salida.

**11. ID (IDENTIFICADOR DE USUARIO):** Número o código de identificación única que una plataforma digital asigna a cada cuenta de usuario para identificarla de manera inequívoca, con independencia de los cambios que puedan realizarse en el nombre de usuario o en otros datos visibles del perfil. Junto con la URL completa del perfil, el ID constituye un indicador relevante para identificar de forma precisa las cuentas que mantuvieron contacto con la víctima.

**12. IMEI:** Acrónimo de International Mobile Equipment Identity (Identidad Internacional de Equipos Móviles). Es un código numérico único de 15 dígitos que identifica de manera individual a cada dispositivo móvil a nivel mundial, con independencia de la tarjeta SIM utilizada. Su registro en el informe de procedimiento permite identificar con precisión el dispositivo interviniente en la investigación.

**13. METADATOS:** Información adicional asociada a un archivo o comunicación digital que no forma parte de su contenido principal, pero describe sus características o su historial. Por ejemplo, en un documento de texto, el metadato puede ser la fecha de creación, el autor o el historial de modificaciones.

**14. SISTEMA INFORMÁTICO:** Todo dispositivo o conjunto de dispositivos interconectados cuya función sea el procesamiento automatizado de datos, incluyendo los medios de almacenamiento y comunicación asociados.

**15. URL (LOCALIZADOR UNIFORME DE RECURSOS):** Es la dirección virtual de cualquier recurso único en Internet. Este recurso puede ser una página web, una imagen, un video o incluso un docu-

mento. Normalmente, una URL consta de diferentes partes, como un protocolo, un nombre de dominio, una extensión y una ruta.

**16. VALOR HASH:** Resultado de aplicar una función hash criptográfica a datos. Los valores hash representan grandes cantidades de datos como valores numéricos mucho más pequeños, por lo que se utilizan como firmas digitales para identificar de forma única cada archivo electrónico. Los valores hash se representan típicamente como un número hexadecimal y su longitud depende del tipo de algoritmo hash utilizado.

# 11. Bibliografía

- Consejo de Europa. (2001). *Convenio sobre la Ciberdelincuencia*. Serie de Tratados Europeos, n.º 185. <https://www.coe.int/en/web/conventions/full-list?module=treaty-detail&treaty-num=185>
- Dupuy, D., & Neme, C. F. (2023). ABC de la investigación de cara al juicio. En D. Dupuy (Dir.) y C. F. Neme (Coord.), *Acosos en la red a mujeres* (pp. 249-304). Hammurabi.
- Giaccaglia, M., Lamperti, S. y Nuñez, L. (2017). Investigación criminal y penal. En A.H. Di Iorio (Dir), *El rastro digital del delito* (pp. 159-202). Universidad FASTA.
- Google. (s. f.). *Cómo descargar tus datos de Google*. Google Account Help. <https://support.google.com/accounts/answer/3024190?hl=en>
- Guttman, B., White, D. R., & Walraven, T. (2022). *Digital evidence preservation: Considerations for evidence handlers* (NIST IR 8387). National Institute of Standards and Technology. <https://doi.org/10.6028/NIST.IR.8387>
- International Organization for Standardization & International Electrotechnical Commission. (2012). *Information technology – Security techniques – Guidelines for identification, collection, acquisition and preservation of digital evidence* (ISO/IEC 27037:2012). ISO. <https://www.iso.org/standard/44381.html>
- Meta. (s. f.). *Acceder a tu información y descargarla*. Facebook Help Center. <https://www.facebook.com/help/1701730696756992>

National Institute of Justice. (2008). *Electronic crime scene investigation: A guide for first responders* (2.<sup>a</sup> ed., NCJ 219941). U.S. Department of Justice. <https://www.ojp.gov/pdffiles1/nij/219941.pdf>

National Institute of Standards and Technology (NIST). (s. f.). Hash value. En *Glossary*. Computer Security Resource Center. [https://csrc.nist.gov/glossary/term/hash value](https://csrc.nist.gov/glossary/term/hash%20value)

National Institute of Standards and Technology (NIST). (s. f.). SHA-256. En *Glossary*. Computer Security Resource Center. [https://csrc.nist.gov/glossary/term/sha 256](https://csrc.nist.gov/glossary/term/sha%20256)

Presman, G. (2018). La cadena de custodia en la evidencia digital. En D. Dupuy (Dir.) y M. Kieffer (Coord.), *Ciberdelitos II* (pp. 303-312). IB de F.

WhatsApp. (s. f.). *Cómo exportar tu historial de chats*. WhatsApp Help Center. <https://faq.whatsapp.com/196737011380816>



## **Anexo I**

### **Modelo de formulario de cadena de custodia**

**MINISTERIO DEL INTERIOR**  
**Dirección Nacional de Policía Científica**

**REGISTRO DE CADENA DE CUSTODIA DE EVIDENCIAS FÍSICAS**

|                |           |                     |  |
|----------------|-----------|---------------------|--|
| N° DE CASO     |           | N° DE REGISTRO      |  |
| FECHA: _/ _/ _ | HORA: _:_ | Unidad Solicitante: |  |
| Dirección:     |           |                     |  |
| Víctima:       |           |                     |  |

**IDENTIFICACION DE PARTICIPANTES EN LA ESCENA**

|                | Nombre y Apellido | Documento Identidad | Firma |
|----------------|-------------------|---------------------|-------|
| Fijación       |                   |                     |       |
| Fotógrafo      |                   |                     |       |
| Planimétrico   |                   |                     |       |
| Colección      |                   |                     |       |
| Embalaje       |                   |                     |       |
| Etiquetado     |                   |                     |       |
| Preservación   |                   |                     |       |
| Observaciones: |                   |                     |       |

**EVIDENCIAS FÍSICAS O INDICIOS COLECTADOS**

| Cant. | Descripción | Cant. | Descripción |
|-------|-------------|-------|-------------|
|       |             |       |             |
|       |             |       |             |
|       |             |       |             |
|       |             |       |             |
|       |             |       |             |
|       |             |       |             |
|       |             |       |             |
|       |             |       |             |
|       |             |       |             |
|       |             |       |             |
|       |             |       |             |
|       |             |       |             |
|       |             |       |             |
|       |             |       |             |
|       |             |       |             |

|                                      |    |            |                     |
|--------------------------------------|----|------------|---------------------|
| FUNCIONARIO DE CUSTODIA DE LA ESCENA |    | FIRMA      |                     |
|                                      |    | ACLARACIÓN |                     |
| REGISTRO DE CONTINUIDAD              | SI | NO         | CANTIDAD DE PAGINAS |
|                                      |    |            |                     |

**AREA DE RESGUARDO Y CUSTODIA A CARGO DE LAS EVIDENCIAS FÍSICAS**

|                        |              |
|------------------------|--------------|
| FUNCIONARIO QUE RECIBE | DEPARTAMENTO |
| GRADO Y NOMBRE         | FIRMA        |

MINISTERIO DEL INTERIOR  
Dirección Nacional de Policía Científica

|                        |   |   |      |               |  |
|------------------------|---|---|------|---------------|--|
| FUNCIONARIO QUE RECIBE |   |   |      | DEPARTAMENTO  |  |
| GRADO Y NOMBRE         |   |   |      | FIRMA         |  |
|                        |   |   |      |               |  |
| FECHA                  | / | / | HORA | Nº Referencia |  |
| Observaciones:         |   |   |      |               |  |
|                        |   |   |      |               |  |
|                        |   |   |      |               |  |
|                        |   |   |      |               |  |
|                        |   |   |      |               |  |
|                        |   |   |      |               |  |
| FUNCIONARIO QUE RECIBE |   |   |      | DEPARTAMENTO  |  |
| GRADO Y NOMBRE         |   |   |      | FIRMA         |  |
|                        |   |   |      |               |  |
| FECHA                  | / | / | HORA | Nº Referencia |  |
| Observaciones:         |   |   |      |               |  |
|                        |   |   |      |               |  |
|                        |   |   |      |               |  |
|                        |   |   |      |               |  |
|                        |   |   |      |               |  |
|                        |   |   |      |               |  |
| FUNCIONARIO QUE RECIBE |   |   |      | DEPARTAMENTO  |  |
| GRADO Y NOMBRE         |   |   |      | FIRMA         |  |
|                        |   |   |      |               |  |
| FECHA                  | / | / | HORA | Nº Referencia |  |
| Observaciones:         |   |   |      |               |  |
|                        |   |   |      |               |  |
|                        |   |   |      |               |  |
|                        |   |   |      |               |  |
|                        |   |   |      |               |  |
|                        |   |   |      |               |  |
| FUNCIONARIO QUE RECIBE |   |   |      | DEPARTAMENTO  |  |
| GRADO Y NOMBRE         |   |   |      | FIRMA         |  |
|                        |   |   |      |               |  |
| FECHA                  | / | / | HORA | Nº Referencia |  |
| Observaciones:         |   |   |      |               |  |
|                        |   |   |      |               |  |
|                        |   |   |      |               |  |
|                        |   |   |      |               |  |
|                        |   |   |      |               |  |
|                        |   |   |      |               |  |
| FUNCIONARIO QUE RECIBE |   |   |      | DEPARTAMENTO  |  |
| GRADO Y NOMBRE         |   |   |      | FIRMA         |  |
|                        |   |   |      |               |  |
| FECHA                  | / | / | HORA | Nº Referencia |  |
| Observaciones:         |   |   |      |               |  |
|                        |   |   |      |               |  |
|                        |   |   |      |               |  |
|                        |   |   |      |               |  |
|                        |   |   |      |               |  |
|                        |   |   |      |               |  |

| AREA DE RESGUARDO Y CUSTODIA A CARGO DE LAS EVIDENCIAS FÍSICAS |     |  |      |  |               |  |  |  |  |
|----------------------------------------------------------------|-----|--|------|--|---------------|--|--|--|--|
| FUNCIONARIO QUE RECIBE                                         |     |  |      |  | DEPARTAMENTO  |  |  |  |  |
| GRADO Y NOMBRE                                                 |     |  |      |  | FIRMA         |  |  |  |  |
|                                                                |     |  |      |  |               |  |  |  |  |
| FECHA                                                          | / / |  | HORA |  | N° Referencia |  |  |  |  |
| Observaciones:                                                 |     |  |      |  |               |  |  |  |  |
|                                                                |     |  |      |  |               |  |  |  |  |
|                                                                |     |  |      |  |               |  |  |  |  |
|                                                                |     |  |      |  |               |  |  |  |  |
|                                                                |     |  |      |  |               |  |  |  |  |
|                                                                |     |  |      |  |               |  |  |  |  |
| FUNCIONARIO QUE RECIBE                                         |     |  |      |  | DEPARTAMENTO  |  |  |  |  |
| GRADO Y NOMBRE                                                 |     |  |      |  | FIRMA         |  |  |  |  |
|                                                                |     |  |      |  |               |  |  |  |  |
| FECHA                                                          | / / |  | HORA |  | N° Referencia |  |  |  |  |
| Observaciones:                                                 |     |  |      |  |               |  |  |  |  |
|                                                                |     |  |      |  |               |  |  |  |  |
|                                                                |     |  |      |  |               |  |  |  |  |
|                                                                |     |  |      |  |               |  |  |  |  |
|                                                                |     |  |      |  |               |  |  |  |  |
|                                                                |     |  |      |  |               |  |  |  |  |
| FUNCIONARIO QUE RECIBE                                         |     |  |      |  | DEPARTAMENTO  |  |  |  |  |
| GRADO Y NOMBRE                                                 |     |  |      |  | FIRMA         |  |  |  |  |
|                                                                |     |  |      |  |               |  |  |  |  |
| FECHA                                                          | / / |  | HORA |  | N° Referencia |  |  |  |  |
| Observaciones:                                                 |     |  |      |  |               |  |  |  |  |
|                                                                |     |  |      |  |               |  |  |  |  |
|                                                                |     |  |      |  |               |  |  |  |  |
|                                                                |     |  |      |  |               |  |  |  |  |
|                                                                |     |  |      |  |               |  |  |  |  |
|                                                                |     |  |      |  |               |  |  |  |  |
| FUNCIONARIO QUE RECIBE                                         |     |  |      |  | DEPARTAMENTO  |  |  |  |  |
| GRADO Y NOMBRE                                                 |     |  |      |  | FIRMA         |  |  |  |  |
|                                                                |     |  |      |  |               |  |  |  |  |
| FECHA                                                          | / / |  | HORA |  | N° Referencia |  |  |  |  |
| Observaciones:                                                 |     |  |      |  |               |  |  |  |  |
|                                                                |     |  |      |  |               |  |  |  |  |
|                                                                |     |  |      |  |               |  |  |  |  |
|                                                                |     |  |      |  |               |  |  |  |  |
|                                                                |     |  |      |  |               |  |  |  |  |
|                                                                |     |  |      |  |               |  |  |  |  |

|                        |     |      |  |               |  |
|------------------------|-----|------|--|---------------|--|
| FUNCIONARIO QUE RECIBE |     |      |  | DEPARTAMENTO  |  |
| GRADO Y NOMBRE         |     |      |  | FIRMA         |  |
|                        |     |      |  |               |  |
| FECHA                  | / / | HORA |  | N° Referencia |  |
| Observaciones:         |     |      |  |               |  |
|                        |     |      |  |               |  |
|                        |     |      |  |               |  |
|                        |     |      |  |               |  |
|                        |     |      |  |               |  |
|                        |     |      |  |               |  |

  

|                        |     |      |  |               |  |
|------------------------|-----|------|--|---------------|--|
| FUNCIONARIO QUE RECIBE |     |      |  | DEPARTAMENTO  |  |
| GRADO Y NOMBRE         |     |      |  | FIRMA         |  |
|                        |     |      |  |               |  |
| FECHA                  | / / | HORA |  | N° Referencia |  |
| Observaciones:         |     |      |  |               |  |
|                        |     |      |  |               |  |
|                        |     |      |  |               |  |
|                        |     |      |  |               |  |
|                        |     |      |  |               |  |
|                        |     |      |  |               |  |

  

|                        |     |      |  |               |  |
|------------------------|-----|------|--|---------------|--|
| FUNCIONARIO QUE RECIBE |     |      |  | DEPARTAMENTO  |  |
| GRADO Y NOMBRE         |     |      |  | FIRMA         |  |
|                        |     |      |  |               |  |
| FECHA                  | / / | HORA |  | N° Referencia |  |
| Observaciones:         |     |      |  |               |  |
|                        |     |      |  |               |  |
|                        |     |      |  |               |  |
|                        |     |      |  |               |  |
|                        |     |      |  |               |  |
|                        |     |      |  |               |  |

  

|                        |     |      |  |               |  |
|------------------------|-----|------|--|---------------|--|
| FUNCIONARIO QUE RECIBE |     |      |  | DEPARTAMENTO  |  |
| GRADO Y NOMBRE         |     |      |  | FIRMA         |  |
|                        |     |      |  |               |  |
| FECHA                  | / / | HORA |  | N° Referencia |  |
| Observaciones:         |     |      |  |               |  |
|                        |     |      |  |               |  |
|                        |     |      |  |               |  |
|                        |     |      |  |               |  |
|                        |     |      |  |               |  |
|                        |     |      |  |               |  |



## **Anexo II**

Procedimiento establecido por la Dirección Nacional de Policía Científica para la colección de indicios y evidencias de dispositivos informáticos



## PROTOCOLO PARA LA COLECCIÓN DE INDICIOS Y EVIDENCIAS DE DISPOSITIVOS INFORMÁTICOS

LAI 01-01  
Pág. 1 de 2

**Fecha de entrada en vigencia:**

**27/09/2024**

### 1. Objetivos

Unificar criterios en cuanto al procedimiento correcto de recolección de indicios informáticos y su descripción en la cadena de custodia

### 2. Alcance

Todas la Unidades y Organismos externos cuyas tareas supongan la colección, custodia y/o traslado de indicios y/o evidencias de índole informática.

### 3. Responsabilidades

Todo el personal **de las Unidades y Organismos** externos que tomen intervención en presuntos hechos delictivos o que requieran de su intervención por la naturaleza de los mismos.

### 4. Descripción

Se establece como indicio informático todo objeto material o virtual que se halle en la escena del hecho y que requiere de análisis para ser presentado como evidencia. La evidencia digital tiene por características la volatilidad de la información, alterabilidad y facilidad de eliminación. Por tanto, surge la necesidad de establecer un protocolo unificado de actuación para la colección, custodia y/o traslado de indicios y/o evidencias de índole informática.

#### A) Dispositivos celulares:

1. En la colección de dispositivos celulares, es importante que los mismos no sean manipulados a fin de encenderlos en caso de estar apagados en la escena del hecho, o en caso contrario de apagarlos para transportarlos de "forma segura". A la hora de recolectar un dispositivo celular, solo se debe verificar su estado para simplemente interrumpir su conexión al servicio de telefonía e internet mediante la opción de modo avión, la cual imposibilita todo tipo de comunicación. Esto último en caso de que el dispositivo se encuentre encendido, en caso contrario, nunca debe encenderse, debe mantenerse apagado hasta su entrega a este laboratorio.



## PROTOCOLO PARA LA COLECCIÓN DE INDICIOS Y EVIDENCIAS DE DISPOSITIVOS INFORMÁTICOS

LAI 01-01  
Pág. 2 de 2

### Control de emisión

| Elaborado por:                                                                                                                                                                               | Revisado por: | Aprobado por: |
|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------|---------------|
| Sgto. Alvaro MACEDO.<br><br>ALVARO<br>ANDRES<br>MACEDO<br>REYES<br><br><small>Firmado digitalmente<br/>por ALVARO ANDRES<br/>MACEDO REYES<br/>Fecha: 2024.09.27<br/>11:25:02 -03'00'</small> |               |               |

- Los dispositivos celulares deben ser descriptos en la cadena de custodia en base a lo observable a simple vista por quien efectúa la recolección en la escena del hecho, no deben ser abiertos, encendidos y/o desarmados para verificar si cuentan con tarjetas SIM y/o tarjetas microSD, o para verificar información técnica que pueda surgir de su configuración.
- La descripción más conveniente consta de su marca de fabricante (en caso de que sea apreciable), color, posibles daños presentes y protección con la que cuente (funda, estuche, etc.). No es necesario aportar datos técnicos que impliquen la manipulación de los dispositivos como ser número de IMEI, modelo, etc., dicha información será agregada a la cadena de custodia a posterior por el Laboratorio de Análisis Informático de la D.N.P. Científica.
- En caso de no ser posible interrumpir la comunicación de un dispositivo mediante la opción modo avión, se recomienda cubrir el mismo con papel aluminio, creando siete (7) capas de papel alrededor del dispositivo.

#### B) Computadoras, laptops y DVRs y otros dispositivos informáticos:

- La recomendación para este tipo de equipos informáticos es apagarlos encaso de hallarse encendidos, previo a su colección
- Proteger los puertos de conexión con cinta.
- Embalar con cartón y cinta.

### 5. Referencias

Protocolo de actuación conjunta del ministerio público y de la policía nacional en materia de procedimiento penal

| Versión | Fecha de elaboración | Modificaciones    |
|---------|----------------------|-------------------|
| 01      | 09/24                | • Primera versión |







