CIBERPERING
SEGURIDAD, INGENIERÍA, PERICIALES
TECNOLOGICAS Y CIBERSEGURIDAD

CIBERPERING · EL PERITO RESPONDE

Guía rápida de prueba digital

Audio, vídeo, fotografías, documentos y publicaciones en línea: qué conservar, qué comprobar y cuándo pedir una pericial

Edición noviembre 2026

CC BY NC ND

Guía rápida

de prueba digital

Audio, vídeo, fotografías,
documentos y publicaciones en línea:
qué conservar, qué comprobar
y cuándo pedir una pericial

Equipo de peritos de Ciberpering

CIBERPERING
SEGURIDAD, INGENIERÍA, PERICIALES
TECNOLOGICAS Y CIBERSEGURIDAD

Edición noviembre 2026

AVISO

Esta guía ofrece orientación técnica y divulgativa sobre la conservación y la valoración de pruebas digitales. No es un dictamen pericial ni asesoramiento jurídico: aportar, impugnar o proponer una prueba es decisión tuya.

Comprueba en el BOE, el CENDOJ o EUR-Lex cada norma y cada sentencia antes de citarla en un escrito.

Para dudas técnicas concretas, el servicio gratuito **El perito responde** (ciberpering.com/el-perito-responde) ofrece una respuesta orientativa en 48 horas laborables.





Licencia. © 2026 Ciberpering. Esta obra se distribuye bajo la licencia Atribución/Reconocimiento-NoComercial-SinDerivados 4.0 Internacional (CC BY-NC-ND 4.0): https://creativecommons.org/licenses/by-nc-nd/4.0/deed.es. Puedes compartirla citando la autoría, sin fines comerciales y sin modificarla.

CIBERPERING
SEGURIDAD, INGENIERÍA, PERICIALES TECNOLÓGICAS Y CIBERSEGURIDAD

Índice por necesidades

Busca lo que necesitas resolver y ve a la página que lo explica. Los números son los de la página impresa.

1 · Tengo una prueba delante

¿De qué tipo es y qué puedo comprobar?

Me han pasado un audio o una nota de voz	cap. 6 **págs. 36–41**
Tengo un vídeo, una foto o una publicación (ELA, ubicación)	cap. 7 **págs. 42–49**
Es una captura de pantalla o un chat de WhatsApp	cap. 8 **págs. 50–55**
Es un documento, un PDF o una firma	cap. 9 **págs. 56–61**
Sospecho de un deepfake o de una voz clonada	caps. 10, 11 y 12 **págs. 63–66 y 67–73 y 74–79**
Quiero saber qué prueban el hash y los metadatos	cap. 4 **págs. 23–27**
Hay deep web, dark web o criptoactivos de por medio	caps. 13 y 14 **págs. 81–85 y 86–93**

Conviene disponer del original: lo que se pueda comprobar depende de conservarlo bien desde el principio (cap. 2, págs. 12–15).

2 · Tengo que decidir o actuar

Con mi cliente y con la otra parte

¿Qué le digo a mi cliente para que no pierda el original?	caps. 1 y 3 **págs. 7–11 y 16–22**
Voy a aportar una prueba o a impugnar la de la otra parte	cap. 19 **págs. 116–120**
¿Acta notarial, sello de tiempo o certificación en línea?	cap. 5 **págs. 28–34**
¿Qué herramientas cita un informe pericial?	caps. 3 y 6 **págs. 16–22 y 36–41**

Lo que puede desaparecer, como una publicación o unos mensajes temporales, se preserva primero (cap. 5).

3 · Tengo que tratar con un perito o una perito

Encargarlo, preguntarle, leerlo

¿Cuándo encargar una pericial? Plazos y coste orientativo	cap. 15 **págs. 95–98**
¿Cómo formulo la pregunta al perito o a la perito?	cap. 16 y anexo F **págs. 99–103 y 147**
¿Qué mira un perito o una perito y cómo elijo a quien?	cap. 17 **págs. 104–109**
¿Qué puede concluir un perito o una perito y qué no?	cap. 18 **págs. 110–114**
¿Qué pericial necesita mi asunto?	cap. 20 **págs. 121–128**

El perito responde a preguntas técnicas; la valoración de la prueba corresponde al juez o a la jueza (cap. 18).

4 · Para consultar

Checklist	Glosario	Enlaces útiles	Preguntas frecuentes	Plantillas y guion
anexo A **pág. 129**	anexo B **págs. 130–132**	anexo C **págs. 133–135**	anexo D **pág. 136**	anexos E y F **págs. 137–147**

Índice

Cómo usar esta guía 1

Parte I. Cuando llega la prueba **6**

1. Hablar con tu cliente 7
2. La conveniencia de disponer del original 12
3. Cadena de custodia 16
4. Hash y metadatos 23
5. Qué acredita cada mecanismo 28

Parte II. Cada tipo de prueba **35**

6. Audios y notas de voz 36
7. Vídeos, imágenes y publicaciones en línea 42
8. Chats, WhatsApp y capturas 50
9. Documentos y firmas 56

Parte III. Inteligencia artificial **62**

10. Qué ha cambiado 63
11. Inteligencia artificial 67
12. Detectores de IA 74

Parte IV. Deep web y criptoactivos **80**

13. Deep web y dark web 81

14. Criptoactivos 86

Parte V. Cuándo y cómo recurrir a un perito o a una perito **94**

15. Cuándo encargar una pericial 95

16. Cómo pedir una pericial sobre una prueba digital 99

17. Qué mira el perito o la perito 104

18. Qué puede concluir un perito o una perito y qué no 110

Parte VI. En el proceso **115**

19. Si aportas una prueba, si te la aportan 116

20. Asuntos habituales y la pericial que requieren 121

Anexos **128**

A. Checklist 129

B. Glosario 130

C. Enlaces útiles 133

D. Preguntas frecuentes 136

E. Plantillas de trabajo 137

F. Guion de la primera consulta con un perito o una perito 147

Cómo usar esta guía

IDEA CLAVE

Esta guía te da lo técnico que necesitas, como profesional de la abogacía, para decidir qué exigir a tu cliente, qué pedir a un perito o a una perito y qué puedes esperar de una pericial sobre un audio, un vídeo, una fotografía, un documento o una publicación en redes sociales o en una web. No sustituye a un dictamen pericial.



Para quién es. Está escrita para profesionales de la abogacía de familia, penal, civil y laboral. Es un material de consulta, no un tratado. Doy por hecho que dominas el proceso; no te explico cómo se aporta o se impugna una prueba, sino qué hay detrás del archivo que te llega. Los términos técnicos se explican la primera vez que aparecen.

Si eres una persona particular y tienes una prueba en la mano, también te servirá, pero la decisión de cómo usarla corresponde siempre a quien lleva tu asunto.

Quién la firma. La firma el equipo de peritos de Ciberpering. Su enfoque es el análisis técnico de cómo están hechos un audio, un vídeo o una fotografía, además de los documentos, los chats y las publicaciones en redes sociales o en una web.

Qué es. Es una guía técnica con dos límites. Un dictamen pericial parte de un material concreto, con un método y con la firma de un perito o de una perito; queda fuera de esta guía. La decisión de aportar, impugnar o proponer una prueba corresponde a tu criterio jurídico. Lo que sí hago es separar, en cada capítulo, lo que dicen la ley y la jurisprudencia de lo que recomienda un perito o una perito para que una prueba resista un análisis. Lo segundo es voluntario, pero muchas veces determina qué podrá afirmar después el perito o la perito.

Cómo está escrita. Los capítulos siguen el mismo orden: idea clave, explicación, lo que dice la norma y la buena práctica técnica cuando proceden, qué hacer, errores frecuentes y un checklist final. «Qué hacer» recoge lo que puedes pedir a tu cliente y lo que puedes pedir a un perito o a una perito, para que sepas qué instrucciones dar y qué material exigir. Las fotografías e ilustraciones de la guía acompañan al texto; ninguna es una prueba real ni el resultado de un análisis real.

CINCO IDEAS QUE SE REPITEN EN TODA LA GUÍA

1. Pide siempre el archivo original, tal como está en el dispositivo donde se grabó o se recibió. Una copia, un reenvío o una captura de pantalla no valen lo mismo.
2. Desde que tu cliente tiene el archivo, deja por escrito quién lo ha tenido, qué se ha hecho con él y cuándo. Sin ese registro, la otra parte puede dudar de que sea el mismo archivo.
3. Si impugnas una prueba, indica el motivo técnico concreto. Decir que «está manipulada» no basta.
4. Si encargas una pericial, pide un método que otro perito u otra perito pueda repetir.
5. No des por falso un archivo solo porque pueda haberse manipulado, ni por auténtico solo porque lo parezca.

Cómo leerla. Si tienes una prueba digital sobre la mesa y poco tiempo, ve a los capítulos 2, 3, 4 y 19 y al checklist del anexo A. Si vas a encargar una pericial, lee los capítulos 15, 16, 17 y 18. Si el asunto gira en torno a un audio, lee el capítulo 6; si es un vídeo, una fotografía o una publicación en redes sociales o en una web, el 7; si es un documento, el 9. Si te interesa cómo se fabrica un contenido con inteligencia artificial y qué huellas deja, lee el capítulo 11; si la prueba procede de la deep web o de la dark web, el 13; si hay criptoactivos, el 14. Si preparas un caso con prueba digital decisiva, léela entera.

QUÉ HACER

1. Identifica qué prueba tienes, ya sea audio, vídeo, fotografía, documento, chat, publicación en redes sociales o publicación web.
2. Pregunta a tu cliente de dónde sale y qué ha hecho con ella (capítulo 1).
3. Pídele que no la toque hasta que esté preservada (capítulo 3).
4. Decide qué quieres probar o desvirtuar. Esa decisión determina qué pregunta técnica planteas.
5. Si hay una duda técnica concreta, consúltame antes de encargar nada, a través del servicio gratuito **El perito responde**, en el que envías la consulta por formulario y recibes una orientación en 48 horas laborables. Es una orientación, no un dictamen.

ERRORES FRECUENTES

- Leer la guía como si fuera un dictamen sobre tu caso.
- Pedir a tu cliente que «autentique» por su cuenta la prueba con una herramienta gratuita.
- Aceptar una copia sin preguntar por el original.
- Esperar a que la otra parte impugne para empezar a ordenar tu prueba.

MINI CHECKLIST

- ☐ Sé qué prueba tengo y qué pretende acreditar.
- ☐ Sé dónde está el original y quién lo tiene.
- ☐ Tu cliente no ha reenviado, editado ni borrado nada, o sé qué ha hecho.
- ☐ Tengo definida la pregunta técnica, si hace falta una pericial.

*Si tienes dudas, consúltame en **El perito responde** (ciberpering.com/el-perito-responde).*

PARTE I

Cuando llega la prueba

CAPÍTULO 1

Hablar con tu cliente

qué preguntar, qué advertir y qué proteger

IDEA CLAVE

La primera conversación con tu cliente decide si la prueba llegará íntegra o manipulada; pregunta de dónde sale, advierte de lo que no debe hacer y protege lo que puede perderse.



Explicación. Gran parte de lo anterior se decide en la primera conversación con quien trae la prueba. Esa persona suele ser tu cliente; muchas veces ya la ha tocado, porque la ha reenviado o la ha recortado. No lo hace con mala intención, sino porque nadie

le ha explicado qué hay que evitar. Que la haya enseñado a otras personas no altera el archivo. Solo importa si alguna se quedó con una copia o puede confirmar lo que vio. En esta conversación importan sobre todo los datos técnicos. Lo que hagas con la respuesta, incluidas las decisiones sobre qué aportar o cómo, es decisión tuya.

La conversación tiene tres partes: qué preguntar, qué advertir y qué proteger.

Qué preguntar. Empieza por el origen, con preguntas como estas.

- ¿De dónde sale el contenido? ¿Quién lo grabó, lo creó o lo envió?
- ¿Cuándo, dónde y con qué dispositivo o aplicación?
- ¿Tiene el original? ¿En qué dispositivo, nube o cuenta está?
- ¿Lo ha reenviado, recortado, editado o copiado? ¿A quién se lo ha enviado o entregado en copia?
- ¿Hay más contenido antes y después? ¿Existe la conversación o la grabación completa?
- ¿Ha borrado algo? ¿Hay mensajes temporales activados?
- ¿Quién más puede confirmarlo? ¿Lo sabía la otra persona al grabar?
- ¿Ha aportado algo parecido en otro procedimiento?

Qué advertir. A continuación hay que decirle con claridad lo que no debe hacer y lo que puede ocurrir.

- No debe borrar, reenviar, recortar, «mejorar» ni publicar el contenido.
- No debe cambiar de móvil, restaurarlo ni actualizar el sistema sin consultar.
- No debe confrontar a la otra persona con la prueba antes de que esté preservada.
- No debe entregar su único dispositivo sin dejar constancia de su contenido.
- Una pericial puede salir en contra de lo que esperaba; nadie puede prometer un resultado.
- Fabricar o alterar una prueba, o aportarla sabiendo que es falsa, tiene consecuencias legales graves. Debes explicárselas tú.

Qué proteger. Por último, hay que cuidar lo que puede perderse.

- **El dispositivo y las cuentas.** Contraseñas, verificación en dos pasos y copias de seguridad.
- **Los datos de terceras personas y de menores.** No difundirlos y limitar quién accede.
- **El material.** Originales en un solo sitio, con registro de accesos.
- **El secreto profesional.** No enviar material de tu cliente a servicios externos sin valorarlo.
- **El encargo.** Puedes valorar añadir a tu hoja de encargo con tu cliente una cláusula en la que declare que lo que entrega es auténtico y se compromete a conservar los originales. La redacción es jurídica y te corresponde.

LO QUE DICE LA NORMA

Fabricar o aportar a sabiendas una prueba falsa puede tener consecuencias penales y procesales (art. 250.1.7.º y arts. 390 y ss. del Código Penal [CP], art. 247 de la Ley de Enjuiciamiento Civil [LEC]). La obtención de grabaciones o comunicaciones de otras personas tiene sus propios límites (art. 18 de la Constitución Española [CE], art. 197 CP, art. 11.1 de la Ley Orgánica del Poder Judicial [LOPJ]). Valorarlo es tarea tuya.

BUENA PRÁCTICA TÉCNICA

Resume las instrucciones a tu cliente en una sola hoja, con lo que no debe hacer y a quién debe llamar.

QUÉ HACER

1. Haz las preguntas anteriores en orden y anota las respuestas tal cual.
2. Entrega a tu cliente la hoja de advertencias y pídele que la firme o la confirme por escrito.
3. Aplica el capítulo 3, con la ficha de origen, el hash (la huella digital del archivo, capítulo 4) y la copia.
4. Si tu cliente ya ha tocado el material, anótalo sin juzgarlo. Lo que se oculta causa más problemas cuando se descubre.
5. Si dudas de la autenticidad de lo que aporta tu cliente, la decisión profesional es tuya y esta guía no la resuelve.

ERRORES FRECUENTES

- Pedir «mándamelo por WhatsApp».
- Dar por hecho que tu cliente sabe qué no debe hacer.
- Ocultar a tu cliente que la pericial puede no favorecerle.
- No anotar lo que tu cliente ya ha hecho con el contenido.
- No asegurar las cuentas y los dispositivos.

MINI CHECKLIST

- ☐ Preguntas de origen hechas y anotadas.
- ☐ Advertencias entregadas y confirmadas.
- ☐ Original y dispositivo localizados.
- ☐ Cuentas y copias de seguridad aseguradas.
- ☐ Datos de menores y de terceras personas protegidos.
- ☐ Cláusula de encargo valorada.

*Si tienes dudas, consúltame en **El perito responde** (ciberpering.com/el-perito-responde).*

CAPÍTULO 2

La conveniencia de disponer del original

archivo y dispositivo

IDEA CLAVE

Lo que se analiza es el archivo original y el dispositivo que lo creó o lo recibió; una copia reenviada es otra cosa y casi siempre sirve menos. Lo que indiques a tu cliente en la primera conversación decide qué podrá comprobarse después.



Explicación. Una grabación ya no basta por sí sola (capítulo 10). ¿Qué hace falta para comprobarla? Sobre todo, el original. El *original* es el archivo tal como lo creó o lo recibió el dispositivo, sin haber pasado por editores ni por servicios de mensajería. El

dispositivo es el móvil, la grabadora, la cámara o el ordenador donde está. Contiene la aplicación, las bases de datos, los registros y las copias de seguridad; todo ello ayuda a comprobar el origen.

El problema es que, cuando un archivo se reenvía por mensajería o se descarga de una red social, suele recomprimirse y perder parte de sus metadatos (los datos sobre el archivo, véase el capítulo 4). Así se pierden justo las huellas que permiten analizarlo, como la estructura interna, el ruido de fondo o la información del dispositivo. El grado de pérdida depende de cada aplicación y de su versión, por lo que hay que comprobarlo caso por caso.

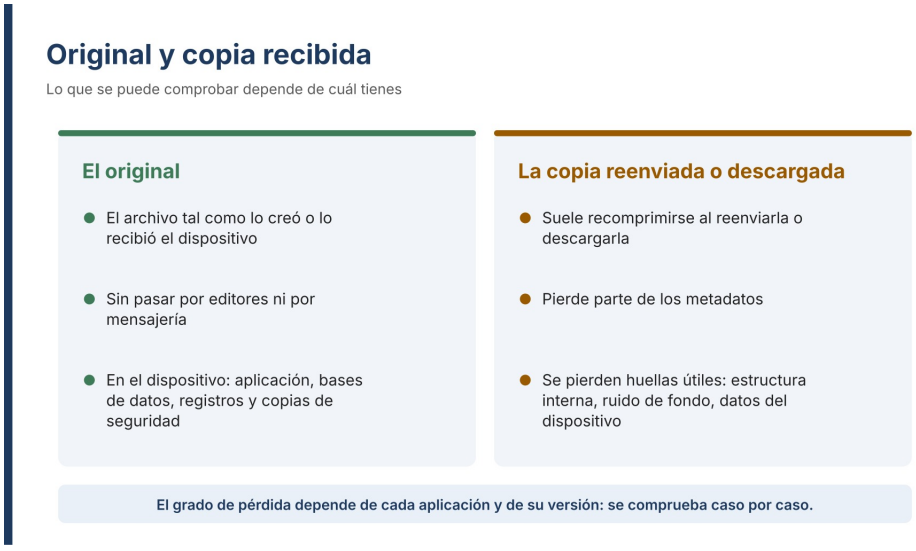

Figura 1. Qué cambia entre el original y la copia recibida. Esquema ilustrativo.

Una nota divulgativa de Fernández Advocats distingue entre prueba digital originaria y derivada. La originaria es el soporte donde se generó o almacenó la información, como el móvil, el ordenador o el servidor. La derivada son las capturas, las impresiones, las copias exportadas y los archivos reenviados. La nota señala que la derivada conserva su valor, pero que cuanto mayor es la distancia respecto del

soporte original, mayor es la necesidad de acreditar su autenticidad, su integridad y su trazabilidad.

De cómo se conserva ese material y se documenta su recorrido trata el capítulo 3.

QUÉ HACER

1. Antes de recibir el material, di a tu cliente que no borre, no reenvíe y no «mejore» el contenido. Que tampoco actualice el sistema, restaure el móvil ni cambie de terminal.
2. Pregúntale dónde está el original (móvil, tarjeta, grabadora, cámara, nube u ordenador).
3. Si el contenido ha llegado por mensajería o por una red social, pide también el archivo de origen, porque la copia recibida suele haber perdido metadatos.
4. Pide que se conserve el dispositivo entero, con su cuenta y sus copias de seguridad, y no solo el archivo. Ahí están la aplicación, las bases de datos y los registros que ayudan a comprobar el origen.
5. Averigua quién ha tenido acceso al dispositivo y a la cuenta desde que se creó o se recibió el contenido, y anótalo (capítulo 3).
6. Si el original está en poder de otra persona o en una cuenta ajena, anótalo y decide cuanto antes cómo asegurarlo (capítulo 3).
7. Si solo existe una copia reenviada o una captura, déjalo por escrito. Sigue siendo prueba, pero cuanto más lejos está del original, más hay que acreditar su autenticidad, su integridad y su trazabilidad.

ERRORES FRECUENTES

- Aceptar el audio o el vídeo reenviado por mensajería como si fuera el original.
- Sustituir el archivo por una grabación de la pantalla mientras suena el audio o se ve el vídeo.
- Recortar el archivo para quedarse con la parte útil.
- Abrirlo en un editor que lo vuelve a guardar al cerrar.
- Conservar solo el archivo y no el dispositivo, la cuenta ni las copias de seguridad.
- Cambiar de móvil o restaurarlo de fábrica sin copia previa.
- Dar por hecho que la copia recibida conserva los mismos metadatos que el original, cuando hay que comprobarlo caso por caso.

MINI CHECKLIST

- ☐ Sé dónde está el original y quién tiene acceso.
- ☐ Tu cliente no ha borrado, reenviado, editado ni actualizado nada, o consta lo que ha hecho.
- ☐ Tengo el archivo de origen y no solo la copia recibida por mensajería o red social.
- ☐ El dispositivo, la cuenta y las copias de seguridad están localizados y conservados.
- ☐ Nadie ha recortado ni vuelto a guardar el archivo, o consta lo que se hizo.
- ☐ El móvil no se ha restaurado ni cambiado, o consta cuándo y con qué copia previa.
- ☐ Si solo existe una copia derivada, lo he anotado y he valorado qué refuerzo necesita.

*Si tienes dudas, consúltame en **El perito responde** (ciberpering.com/el-perito-responde).*

CAPÍTULO 3

Cadena de custodia

quién ha tenido el material, cuándo y con qué fin

IDEA CLAVE

La cadena de custodia es el registro documentado de quién ha tenido el material, cuándo, con qué fin y qué ha hecho con él; empieza el día en que sabes que el contenido puede importar, no el día en que alguien lo impugna.

Explicación. Una vez localizado el original (capítulo 2), hay que conservarlo y documentar su recorrido. La *cadena de custodia* es el registro documentado de quién ha tenido el material, cuándo, con qué fin y qué ha hecho con él. Empieza el día en que sabes que el contenido puede importar, no el día en que alguien lo impugna. Y casi siempre empieza con tu cliente, antes de que llegue a ti.



Figura 2. La cadena de custodia, de la captura a la sala.

LO QUE DICE LA NORMA

La LEC prevé que los instrumentos de filmación, grabación y semejantes se reproduzcan ante el juez o la jueza y que se conserve el material (arts. 382 a 384 LEC). Lo que no hace es desarrollar un protocolo detallado de custodia digital para la prueba civil. Que un archivo esté íntegro tampoco dice nada sobre si se obtuvo de forma lícita; esa es una cuestión distinta, que tienes que valorar (art. 18 CE y art. 11.1 LOPJ).

Antes de llegar ante el juez o la jueza. La prueba no empieza cuando alguien la presenta, sino cuando se obtiene y se conserva. En el proceso penal, el acceso a un dispositivo tiene reglas propias; la Ley de Enjuiciamiento Criminal (LECrim) exige autorización judicial, con principios como el de especialidad, para las medidas de investigación tecnológica; regula además el registro de dispositivos de almacenamiento masivo y la orden de conservación de datos (arts. 588 bis a y siguientes y 588 sexies a y siguientes LECrim). Conservar bien la prueba desde el principio sigue siendo la mejor defensa. Como buena práctica técnica, la RFC 3227 (Request for Comments, un documento

técnico de referencia sobre cómo recoger evidencias) recomienda recoger primero y analizar después, así como respetar el orden de volatilidad de los datos, es decir, empezar por los que antes se pierden.

Lo que recoge la doctrina penal. Martínez Galindo (2022) señala que la ley procesal penal no desarrolla el procedimiento de la cadena de custodia y que han sido la práctica policial y la jurisprudencia las que han ido estableciendo pautas. Según la misma autora, calcular el hash (un código que identifica el contenido exacto de un archivo, véase el capítulo 4) de la copia forense (una copia exacta del contenido, con comprobación de que coincide con el original) se considera esencial para garantizar la cadena de custodia.

BUENA PRÁCTICA TÉCNICA

La norma ISO/IEC 27037:2012 da directrices para identificar, recoger, adquirir y preservar evidencias digitales. Según Martínez Galindo (2022), parte de que la evidencia se adquiera del modo menos intrusivo posible, con un proceso trazable, auditable y reproducible. La ISO/IEC 27042:2015 da directrices para el análisis y la interpretación de evidencias digitales. La misma autora indica que la Asociación Española de Normalización y Certificación (AENOR) ratificó ambas en diciembre de 2016. La UNE 71506:2013 propone una metodología para su análisis forense. No son normas procesales, pero un perito o una perito las usa como referencia.

Copia forense (clonado forense). Es una copia de un soporte de almacenamiento (disco, tarjeta, memoria) que reproduce todos sus bits, no solo los archivos visibles. El NIST (Instituto Nacional de Normas y Tecnología de EE. UU.) la llama *bit-stream duplicate*, es decir, duplicado bit a bit; define la *imagen* como un archivo a partir del cual puede reconstruirse ese duplicado. Se hace con un *bloqueador de escritura*, un dispositivo que impide enviar al soporte original órdenes que modifiquen sus datos; la especificación del NIST para herramientas de imagen de disco establece que la herramienta no debe alterar el disco original. Para comprobar que la copia es idéntica se calcula el hash del

original y el de la copia (véase el capítulo 4); si coinciden, son idénticas. El análisis se hace sobre la copia y el original se conserva intacto.



Herramientas de adquisición y análisis. Un informe pericial nombra la herramienta con la que se obtuvo el material. Estas son algunas de las más citadas, descritas según sus fabricantes o sus proyectos. Son solo ejemplos.

- UFED (Cellebrite): serie de productos para extraer y analizar datos de dispositivos móviles.
- Magnet AXIOM (Magnet Forensics): plataforma que adquiere y procesa datos de ordenadores, teléfonos y nube en un único fichero de caso.
- Autopsy: plataforma forense digital gratuita y de código abierto, con interfaz gráfica sobre The Sleuth Kit, para investigar lo ocurrido en un ordenador.
- FTK Imager (Exterro): herramienta gratuita de vista previa y de adquisición de imágenes forenses; crea copias sin modificar la evidencia original y genera informes de hash.
- Guymager: adquisidor forense gratuito para Linux que produce imágenes en formato EWF, AFF y dd.

- dd: orden del proyecto GNU coreutils que copia datos de una entrada a una salida con un tamaño de bloque configurable. Quien la emplea documenta la orden exacta y calcula el hash de la copia.
- Clonezilla: programa libre de clonación y de imágenes de discos y particiones. Clona, pero no genera por sí solo una imagen forense, porque es una herramienta de copia y no de adquisición forense. Guarda y restaura solo los bloques usados del disco; en los sistemas de ficheros que no admite, hace una copia sector a sector con dd. Un informe que lo cite indica el modo empleado, porque una copia de bloques usados no contiene el espacio sin asignar.

Nombrar la herramienta no basta. Un informe sólido indica también la versión usada, el tipo de extracción (lógica, de sistema de ficheros o física), el hash del resultado y el registro del proceso. Puedes pedir esos datos en la pregunta pericial (capítulo 16).

En un móvil, la extracción tiene tres niveles, de menos a más datos. La lógica recoge lo que el sistema entrega al preguntarle, como contactos, mensajes y archivos. La de sistema de ficheros añade la estructura de carpetas y archivos, con las bases de datos de las aplicaciones. La física copia la memoria del dispositivo y es el nivel más completo. Esta terminología es la habitual de los fabricantes de herramientas forenses; la guía NIST SP 800-101 Rev. 1 distingue niveles de adquisición de complejidad creciente, entre ellos el lógico y el físico. Antes de extraer, nadie debe borrar datos, actualizar el sistema, restaurar el móvil ni cambiar de terminal. Si hay mensajes temporales, se consulta antes de tocar su configuración.

QUÉ HACER

1. Pide que se rellene una ficha de origen. En ella constará quién creó o recibió el archivo, con qué dispositivo y aplicación, dónde, cuándo y por qué medio llegó a su poder (anexo E).
2. Haz que se calcule el hash del archivo antes de moverlo (capítulo 4) y que se anote con fecha y hora. Si lo hace un perito o una perito, el hash tiene más peso.
3. Después, que se copie el archivo tal cual, sin «guardar como» ni exportar, a un soporte aparte; que se compruebe que el hash de la copia coincide.
4. Que el original se guarde donde no se use y que solo se trabaje con copias.
5. Que se registre cada acceso, es decir, quién, cuándo y para qué (anexo E).
6. Si el contenido está en un servicio que puede desaparecer (mensajes temporales que se borran solos, nube, red social), decide cuanto antes cómo preservarlo (capítulo 5). Conviene saber que, con el paso de los días, ese contenido puede perderse.
7. Si se encarga una extracción o una copia forense, pide que el informe indique la herramienta, la versión, el tipo de extracción y el hash.

ERRORES FRECUENTES

- Recibir el dispositivo sin dejar constancia de lo que contiene.
- No anotar nada y confiar en la memoria.
- Dar por buena una extracción sin saber con qué herramienta ni de qué tipo se hizo.

MINI CHECKLIST

- ☐ Hay una ficha de origen rellenada.
- ☐ Hay un hash calculado y anotado antes de mover el archivo.
- ☐ Se trabaja solo con copias.
- ☐ Cada acceso al material queda registrado.
- ☐ He decidido cómo preservar lo que puede desaparecer.

*Si tienes dudas, consúltame en **El perito responde** (ciberpering.com/el-perito-responde).*

CAPÍTULO 4

Hash y metadatos

qué prueban, qué no y quién debe calcularlos

IDEA CLAVE

El hash prueba que un archivo no ha cambiado desde que se calculó; los metadatos dan pistas, pero se pueden reescribir. Ninguno prueba por sí solo que el contenido sea auténtico.

Explicación. En el capítulo 3 vimos que hay que calcular el hash del original antes de moverlo. Un *hash* es un código que se calcula a partir del contenido de un archivo. Si cambia un solo byte (la unidad mínima de datos de un archivo), el código resultante cambia por completo. El hash SHA-256, por ejemplo, genera 64 caracteres hexadecimales (cifras del 0 al 9 y letras de la a a la f).



Figura 3. Un solo cambio en el archivo transforma por completo el código.

Los algoritmos de hash más habituales. Un algoritmo de hash es el método de cálculo. Cada uno genera un código de longitud fija, sea cual sea el tamaño del archivo. Una *colisión* es un par de archivos distintos que producen el mismo código. Estos son los cuatro que aparecen en los informes:

- MD5: lo describe la RFC 1321 y genera 128 bits (32 caracteres hexadecimales). La RFC 6151 lo declara inaceptable donde se exige resistencia a colisiones, como en las firmas digitales.
- SHA-1: genera 160 bits (40 caracteres). El NIST recomienda migrar a SHA-2 o SHA-3 y propone retirarlo antes del 31 de diciembre de 2030; en 2017 se publicó la primera colisión práctica.
- SHA-256: pertenece a la familia SHA-2, que define la norma FIPS 180-4 del NIST; genera 256 bits (64 caracteres). Es el algoritmo que uso habitualmente en mis periciales.
- SHA-512: pertenece a la misma familia y a la misma norma; genera 512 bits (128 caracteres).

Conviene indicar siempre en el informe qué algoritmo se ha usado.

Calcular MD5 y SHA-1 a la vez sobre una misma evidencia sí tiene valor, porque quien quisiera sustituirla por otro archivo tendría que conseguir el mismo código en los dos algoritmos al mismo tiempo. Ese valor es limitado. Según la teoría (Joux, 2004), unir dos hashes de este tipo añade poca resistencia a las colisiones frente a la del más fuerte de los dos, que aquí es SHA-1. Por eso el cálculo conjunto complementa a SHA-256 y no lo sustituye.

Un hash tiene un alcance limitado. Prueba que el archivo es idéntico al que existía cuando se calculó. En cambio, no prueba que fuera auténtico antes de calcularse. Un audio clonado o un documento falso también tienen un hash perfectamente válido.

Algo parecido ocurre con los *metadatos*, que son datos sobre el archivo, como fecha de creación y de modificación, dispositivo, programa, códec (el programa o formato

que comprime el audio o el vídeo), duración y, a veces, la ubicación. Son un indicio útil que se valora junto con el resto de la prueba. Con programas gratuitos se cambian en un minuto. Además, muchos servicios los eliminan o los reescriben al reenviar el archivo. Si la otra parte te aporta un archivo con metadatos perfectos, eso no te dice nada por sí solo. Que te lo aporten sin metadatos tampoco prueba que sea falso.

Hay otra consecuencia práctica. Según Blázquez Moreno (2023), un mismo contenido puede circular con metadatos distintos. El archivo que ve quien recibe un envío por internet no es el mismo que estaba en el dispositivo de quien lo envió, aunque el contenido coincida. Por eso conviene dejar constancia de cuál es exactamente el archivo que se analiza y de dónde sale, sea el del dispositivo de origen, el recibido por mensajería o una descarga. La misma fuente añade que, con los datos de geolocalización, habría que acreditar además quién tenía el dispositivo en ese momento.

LO QUE DICE LA NORMA

Ninguna norma procesal establece un algoritmo de hash ni obliga a usar uno. Su valor lo aprecia el juez o la jueza según la sana crítica (arts. 382.3 y 384.3 LEC).

BUENA PRÁCTICA TÉCNICA

Lo que importa es quién calcula el hash, cuándo y con qué herramienta. Si lo calcula la propia parte, es solo lo que esa parte afirma. Si lo calcula una tercera parte independiente, como un perito o una perito, tiene más peso; también lo tiene si se vincula a un sello de tiempo cualificado (capítulo 5). El perito o la perito, además, busca incoherencias entre las distintas partes del archivo, como los metadatos del archivo frente a los del propio audio o vídeo que contiene, las fechas frente al contenido, o rastros del programa de edición.

QUÉ HACER

1. Exige que el hash del original se calcule antes de abrirlo, copiarlo o enviarlo; que lo calcule alguien independiente si la prueba es decisiva.
2. Si lo calcula tu cliente, que use una herramienta conocida. En Windows: `Get-FileHash -Algorithm SHA256 archivo` en PowerShell. En Linux: `sha256sum archivo`. En macOS: `shasum -a 256 archivo`.
3. Pide que anoten el valor completo, la fecha y la hora, el nombre y el tamaño del archivo, quién lo calculó y con qué herramienta y versión.
4. Que se repita el cálculo con cada copia y al entregar el material. Los valores deben coincidir.
5. Guarda el valor por escrito en un sitio distinto del archivo. Dónde y cómo hacerlo constar en el procedimiento es decisión tuya.
6. Para ver los metadatos, que se trabaje sobre una copia y se conserve la salida completa de la herramienta, no un resumen.
7. Si los valores no coinciden, que nadie «arregle» nada. Documenta la diferencia y consulta a un perito o a una perito.

ERRORES FRECUENTES

- Usar solo MD5 o solo SHA-1.
- Calcular el hash de una copia, de una captura o de un archivo ya recomprimido y presentarlo como el del original.
- Creer que el hash prueba la autenticidad del contenido.
- «Limpiar» o editar los metadatos «para protegerlos».
- Calcular el hash después de editar el archivo.
- Confundir el hash de un ZIP con el de cada archivo que contiene.

MINI CHECKLIST

☐ Hash SHA-256 calculado sobre el original, no sobre una copia.

☐ Valor, fecha, hora, herramienta y versión anotados.

☐ Hash repetido en cada copia y todos coinciden.

☐ Valor guardado por escrito fuera del propio archivo.

☐ Metadatos extraídos sobre una copia, con la salida completa guardada.

*Si tienes dudas, consúltame en **El perito responde** (ciberpering.com/el-perito-responde).*

CAPÍTULO 5

Qué acredita cada mecanismo

acta notarial, sello de tiempo, cotejo del LAJ, pericial y reconocimiento judicial

IDEA CLAVE

Cada mecanismo acredita una cosa distinta; ninguno, por sí solo, demuestra que un contenido sea auténtico y veraz.

Explicación. Cuando hay que preservar o acreditar un contenido, aparecen el acta, el sello de tiempo, el cotejo y la pericial. Aquí los ordeno. Se suele pedir un acta notarial «para que sea válido». El acta sirve, pero para una cosa concreta; lo mismo pasa con el resto de mecanismos. Elegir entre ellos es una decisión tuya; yo te explico qué acredita cada uno desde el punto de vista técnico. La tabla siguiente resume qué acredita cada uno, qué no acredita, cuándo conviene y quién lo hace (tabla 1).

Mecanismo	Qué acredita	Qué no acredita	Cuándo conviene	Quién lo hace
Acta notarial (presencia o exhibición)	Que la notaría vio o comprobó algo, en esa fecha y lugar, junto con lo que se le mostró. Los documentos públicos hacen prueba plena del hecho, de la fecha y de la identidad de la persona que ejerce la notaría y de quienes intervienen (art. 319 LEC)	Que el contenido sea auténtico, que lo escribiera esa persona o que no estuviera manipulado antes de exhibirlo	Conservar algo que puede desaparecer, como un lugar, una publicación, lo que muestra una pantalla	Notaría
Sello de tiempo cualificado	Que unos datos, por ejemplo un hash, existían en esa fecha y hora y no han cambiado desde entonces. Tiene presunción legal de exactitud (Reglamento (UE, Unión Europea) 910/2014, art. 41; Ley 6/2020)	Ni quién creó el contenido, ni dónde, ni si lo que cuenta es cierto	Fechar y proteger la integridad de un archivo desde el primer momento	Prestador cualificado de servicios de confianza

Mecanismo	Qué acredita	Qué no acredita	Cuándo conviene	Quién lo hace
Cotejo del LAJ	Que lo aportado coincide con el original o con lo que muestra el dispositivo en el acto, con fe pública judicial (art. 453 LOPJ)	Ni el origen del contenido ni su integridad antes del cotejo	Contrastar una impresión o una transcripción con el soporte original	Letrado o Letrada de la Administración de Justicia
Pericial	Origen, identidad e integridad, con método y razonamiento (arts. 335 y ss. LEC)	Ni certezas absolutas ni lo que el material no permite afirmar. El juez o la jueza la valora con sana crítica (art. 348 LEC)	Cuando hay una duda técnica relevante o se impugna la prueba	El perito o la perito
Reconocimiento judicial	El juez o la jueza examina directamente un lugar, un objeto o una persona (art. 353 LEC)	La autenticidad de un archivo digital en sí mismo	Comprobar si un lugar real coincide con lo que muestra un vídeo	Juez o jueza

Tabla 1. Qué acredita, qué no acredita, cuándo conviene y quién realiza cada mecanismo de preservación y acreditación de una prueba digital. Fuente: elaboración propia a partir de los preceptos que cita la tabla.



Figura 4. Escalera de refuerzo: de la captura simple a la pericial.

Qué acredita cada mecanismo

Y qué no acredita

Acta notarial	Sello de tiempo cualificado	Cotejo del LAJ	Pericial	Reconocimiento judicial
ACREDITA Que la notaría vio o comprobó algo, en esa fecha y lugar.	ACREDITA Que unos datos existían en esa fecha y hora y no han cambiado.	ACREDITA Que lo aportado coincide con el original o con lo que muestra el dispositivo.	ACREDITA Origen, identidad e integridad, con método y razonamiento.	ACREDITA El juez o la jueza examina directamente un lugar, un objeto o una persona.
NO ACREDITA Que el contenido sea auténtico, que lo escribiera esa persona o que no estuviera manipulado antes de exhibirlo.	NO ACREDITA Ni quién creó el contenido, ni dónde, ni si lo que cuenta es cierto.	NO ACREDITA Ni el origen del contenido ni su integridad antes del cotejo.	NO ACREDITA Ni certezas absolutas ni lo que el material no permite afirmar.	NO ACREDITA La autenticidad de un archivo digital en sí mismo.

Figura 5. Qué acredita y qué no acredita cada mecanismo.

LO QUE DICE LA NORMA

Cada fila de la tabla indica su base. El valor final de la prueba lo decide el juez o la jueza, de modo que, aunque exista un acta o un cotejo, puede dudar del contenido si hay indicios técnicos de manipulación.

BUENA PRÁCTICA TÉCNICA

Los mecanismos de la tabla se pueden combinar. Una secuencia razonable desde el punto de vista técnico es esta: hash del original, sello de tiempo, extracción o copia forense con cadena de custodia y, si hay impugnación o duda, pericial. El acta o el cotejo documentan el momento y lo que se exhibió. La pericial, en cambio, analiza el contenido. Qué combinación usar y cuándo es decisión tuya.

Servicios de certificación en línea. Existen servicios privados, a veces llamados «testigos online», que capturan una web, una publicación, un correo o un archivo y entregan un justificante con fecha y hora. Dos ejemplos son Safe Stamper y eGarante. Según su documentación, Safe Stamper certifica páginas web, redes sociales y chats, correos, fotografías y vídeos geolocalizados y archivos. Declara apoyarse en un sello de tiempo cualificado emitido por un prestador independiente, en una firma de inalterabilidad y en el registro diario del hash en una cadena de bloques (blockchain). eGarante ofrece, según su web, certificación de páginas web y redes sociales, de correos y de documentos; afirma que su prueba electrónica tiene capacidad probatoria en un proceso judicial. Antes de contratar uno, comprueba qué sello de tiempo usa (si no es cualificado, no tiene la presunción de exactitud de la tabla), qué certifica exactamente, qué archivo entrega y durante cuánto tiempo lo conserva. Son empresas privadas que actúan como terceras partes de confianza; certifican lo que su sistema capturó en ese momento, es decir, el contenido, la fecha y la hora. La Organización de Consumidores y Usuarios (OCU) los describe como un «notario digital». El Instituto Nacional de Ciberseguridad (INCIBE) los describe como servicios que «permiten certificar evidencias digitales en una fecha y hora determinada», basados en firmas

digitales y en una tercera parte de confianza; no cita ninguno en concreto. La autoría de la publicación y la veracidad de su contenido se acreditan con otros medios; el juez o la jueza valora el conjunto.

QUÉ HACER

1. Formula la pregunta que quieres responder: ¿qué existió en esa fecha?, ¿qué se vio en esa pantalla?, ¿el archivo es íntegro?, ¿quién lo creó?
2. Elige el mecanismo según la pregunta, no según lo que «se suele pedir».
3. Averigua cuándo hay que actuar. Lo que puede desaparecer (una publicación, mensajes temporales) va primero.
4. Si usas un acta, entrega a la notaría el original o el acceso al dispositivo; pide que conste el hash y el procedimiento seguido.
5. Si usas un sello de tiempo, comprueba que lo emite un prestador cualificado y guarda el justificante y el hash.
6. Si la prueba es decisiva, valora combinar varios mecanismos.
7. Si usas un servicio privado de certificación en línea, guarda el archivo y el justificante que entrega; anota qué sello de tiempo declara usar.

ERRORES FRECUENTES

- Pensar que un acta notarial de una captura prueba la autenticidad del mensaje.
- Creer que un sello de tiempo prueba que el contenido sea verdadero.
- Llegar tarde, cuando el contenido ya no está.
- Entregar a la notaría una copia en lugar del original.
- Usar un servicio de fechado que no sea cualificado y presentarlo como tal.
- Dar por válido un servicio de certificación solo por lo que afirma el propio servicio.

MINI CHECKLIST

- ☐ Sé qué pregunta quiero responder.
- ☐ He elegido el mecanismo que la responde.
- ☐ Lo que puede desaparecer está preservado.
- ☐ El hash consta en el acta o en el justificante.
- ☐ La combinación elegida cubre lo decisivo.

*Si tienes dudas, consúltame en **El perito responde** (ciberpering.com/el-perito-responde).*

PARTE II

Cada tipo de prueba

CAPÍTULO 6

Audios y notas de voz

manipulaciones habituales y qué se puede comprobar

IDEA CLAVE

Un audio se puede cortar, tapar, reordenar o clonar sin que el oído lo note; hay comprobaciones técnicas sobre el sonido grabado, pero casi todas exigen el original.

Explicación. Ya sabes qué es el original y por qué importa su hash. Empiezo por las manipulaciones más habituales de un audio. Te sirven para formular una duda concreta cuando impugnas un audio y para saber qué te pueden alegar cuando aportas uno.

La manipulación más simple son los cortes y empalmes, en los que se quitan palabras o se unen frases de momentos distintos. Parecida es la inserción de una frase grabada aparte. También se puede superponer ruido o música para tapar un fragmento y que no se entienda, o cambiar la velocidad o el tono para alterar el ritmo o el carácter de la voz. Más reciente es la voz clonada o sintetizada, en la que una IA genera una voz que imita a una persona real. Hay también audios auténticos mal atribuidos o sacados de contexto. Aquí no hay montaje, pero el audio se presenta de forma que dice otra cosa.

¿Qué puede comprobar un perito o una perito de audio? Entre otras cosas, lo siguiente.

Primero, el contenedor (el tipo de archivo que agrupa el sonido y sus datos) y el códec (el sistema que comprime el sonido). Las notas de voz de las aplicaciones de

mensajería suelen usar formatos comprimidos como Opus. Una doble compresión (el audio se comprimió, se editó y se volvió a comprimir), o un formato extraño para el dispositivo que se dice que lo grabó, es un indicio de posible edición.

Después, el espectrograma, que es una imagen del sonido con tiempo, frecuencia e intensidad. Los cortes y los empalmes suelen dejar saltos bruscos en el ruido de fondo o en el abanico de sonidos graves y agudos que contiene el audio.

También se revisa la coherencia acústica, es decir, la reverberación (el eco de la sala), el ruido de la sala y la respuesta del micrófono deberían ser constantes dentro de una misma grabación.

Otra herramienta es la frecuencia de red (ENF). La red eléctrica oscila en torno a 50 Hz en Europa y a veces deja huella en la grabación. Cuando existe, ayuda a comprobar la continuidad. No siempre es aplicable, porque una grabación a batería puede no tenerla.

También hay que tener en cuenta la voz sintética. Los indicios clásicos (respiración, entonación plana, ruido incoherente con el lugar) son cada vez menos fiables al oído. Por eso se combinan con el análisis técnico del sonido y con el contexto.

No hay que mezclar esto con otra tarea. Identificar *quién* habla es otra disciplina, la fonética forense. Comparar una voz con muestras indubitadas (grabaciones cuya autoría nadie discute) no es lo mismo que comprobar que el audio no ha sido alterado (capítulo 17). Si tu asunto depende de quién habla, necesitas ese perfil, no uno de audio y vídeo.



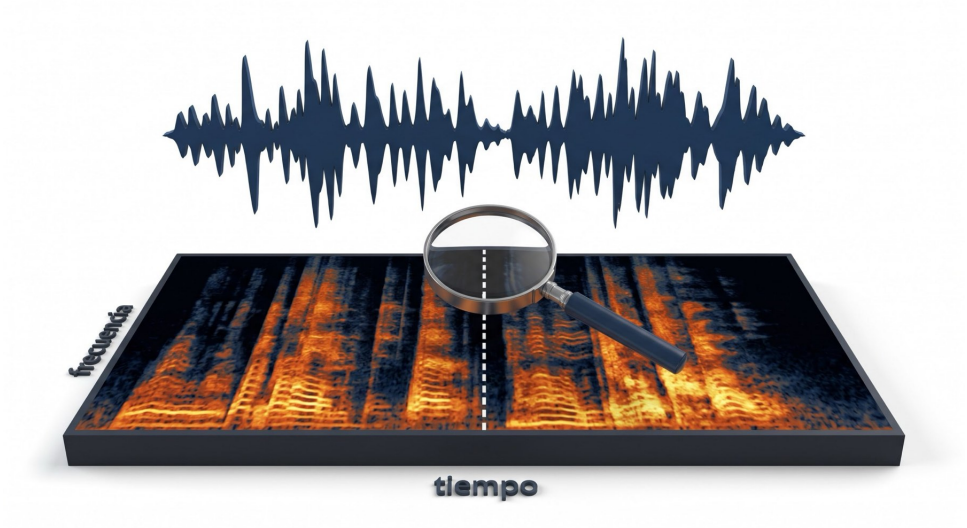

Figura 6. Lo que muestra un espectrograma: el audio visto como imagen.

LO QUE DICE LA NORMA

El audio se aporta como medio de reproducción de palabra y sonido (art. 382 LEC) y se valora conforme a la sana crítica (art. 382.3 LEC). Si se impugna, la jurisprudencia sobre conversaciones digitales apunta a la necesidad de acreditar

origen, identidad e integridad (sentencia del Tribunal Supremo [STS] 300/2015, de 19 de mayo).

BUENA PRÁCTICA TÉCNICA

Cuanto más cerca del original, más se puede comprobar. Un audio reenviado y recomprimido limita el análisis. Aun así, un perito o una perito puede dar una opinión razonada sobre lo que sí se puede afirmar y lo que no. Para ver el espectrograma existen editores de audio como Audacity, un editor y grabador multipista gratuito y de código abierto que incluye un modo espectrograma y una ventana de análisis de espectro. Su uso aquí es de visualización y se hace sobre una copia (capítulo 3).

QUÉ HACER

1. Exige el original y el dispositivo (capítulo 2).
2. Pide a tu cliente que anote quién grabó, con qué, dónde, cuándo y qué se oye antes y después.
3. Pide la grabación completa, no un fragmento.
4. Que conserve el contexto, es decir, el chat donde llegó, la fecha de recepción y quién la envió.
5. Que nadie limpie el audio ni aplique reducción de ruido o normalización sobre el original.
6. Si el audio es de la otra parte, pide a tu cliente que lo escuche con auriculares, sobre una copia; que anote las marcas de tiempo de cualquier salto, cambio de ruido o expresión extraña. Son notas para el perito o la perito, no conclusiones.
7. Pregunta a otras personas si estaban allí, si la persona habla así y si reconocen el momento.
8. Decide si procede encargar una pericial (capítulos 15 y 16).

ERRORES FRECUENTES

- Transcribir el audio y perder o no guardar el archivo.
- «Mejorarlo» para que se entienda.
- Creer que una voz clonada se nota de oído.
- Pensar que, si no se ve un corte en un editor, el audio es íntegro.
- Dar por hecho que un audio auténtico está bien atribuido a quien habla.

MINI CHECKLIST

- ☐ Tengo el archivo original y el dispositivo.
- ☐ Tengo la grabación completa y su contexto.
- ☐ Nadie ha procesado ni mejorado el audio.
- ☐ Hay marcas de tiempo de lo que llama la atención.
- ☐ Sé quién puede confirmar el momento y el lugar.

*Si tienes dudas, consúltame en **El perito responde** (ciberpering.com/el-perito-responde).*

CAPÍTULO 7

Vídeos, imágenes y publicaciones en línea

montajes, contexto manipulado y contraste con el lugar real

> **IDEA CLAVE**
>
> *Una imagen puede ser auténtica y engañar por su contexto, o ser falsa y parecer auténtica; hay que comprobar el archivo y también el lugar.*

Explicación. En imagen y vídeo la manipulación toma otras formas. Las más comunes son cinco. La primera es el montaje, en el que se pega, se clona o se borra una parte de la imagen. La segunda es la imagen sintética, en la que una IA genera una foto o un vídeo de algo que no ocurrió. La tercera es el cambio de rostro o de sincronía labial, en el que se sustituye una cara o se hace decir a alguien lo que no dijo. La cuarta es la edición temporal, en la que se recortan, se ralentizan o se reordenan las escenas. La quinta, que a veces es la más difícil de detectar, es el contexto manipulado, en el que una imagen real se presenta con otra fecha, otro lugar u otras personas.

Para comprobar todo esto, el perito o la perito dispone de varias técnicas. Empieza por los metadatos y la estructura del archivo, donde busca incoherencias entre el dispositivo declarado, las fechas y la forma en que está construido el archivo. Sigue con las huellas de recompresión; el análisis del nivel de error (ELA) puede señalar zonas con una compresión distinta, aunque es un indicio y admite falsos positivos. A continuación puede estudiar el ruido del sensor (PRNU). Cada sensor de cámara

deja un patrón de ruido propio; eso permite vincular una foto a un dispositivo si se dispone del original y de imágenes de referencia de ese dispositivo.

En vídeo se analizan además los fotogramas, que son las imágenes sueltas que forman el vídeo; se buscan cortes, fotogramas repetidos y cambios en el número de imágenes por segundo. También se comprueba que la luz, las sombras, los reflejos y el audio sean coherentes con la escena. Y se revisa la sincronía entre imagen y sonido, porque un desajuste entre ambos puede ser un indicio de montaje.

Los modelos de IA que generan imágenes, audio y vídeo mejoran deprisa. Los defectos de hace poco (dedos, parpadeo, bordes del rostro) ya no aparecen siempre. Por eso la valoración a simple vista es insuficiente, tanto para fiarte de un vídeo como para descartarlo.

Queda el contraste con el lugar real. Un vídeo puede mostrar una escena que no ocurrió en el sitio que dice. Para comprobarlo se localiza el lugar, se verifica que existe y se compara con lo que muestra el vídeo en cuanto a su distribución, sus ventanas, su orientación, su luz y su sonido ambiente. Esa comparación se documenta mejor mediante un acta notarial, que recoge lo que la notaría comprobó en el lugar y en esa fecha. Lo que importa técnicamente es que los lugares cambian y conviene documentarlos pronto.

Por último están las publicaciones en redes sociales y en páginas web. Una publicación puede cambiar o desaparecer; una captura solo muestra lo que había en una pantalla (capítulo 8). Conviene conservar la publicación con su enlace, su fecha y sus comentarios antes de que se borre, además de valorar un acta notarial o un sello de tiempo cualificado que dejen constancia de lo que se vio en ese momento (capítulo 5). Esas vías dejan constancia de lo que se exhibió; no prueban quién publicó ni que lo publicado sea cierto. También existen servicios privados de certificación en línea, como Safe Stamper o eGarante, que certifican publicaciones web y, en el caso de Safe Stamper, fotografías y vídeos (capítulo 5).

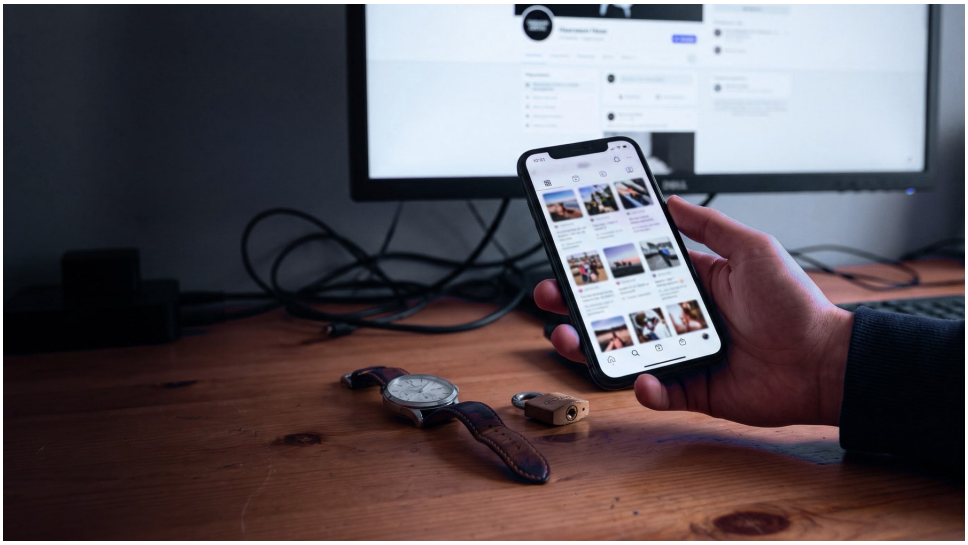



Figura 7. Qué se contrasta en un vídeo: imagen, sonido y metadatos.

El análisis del nivel de error (ELA). El ELA (del inglés *error level analysis*) es una técnica que se aplica a imágenes JPEG. Este formato comprime con pérdida; cada vez que se guarda la imagen, se pierde algo de información. El análisis guarda de nuevo la imagen con una calidad conocida y mide, zona por zona, cuánto difiere el resultado del original. Esa diferencia es el nivel de error, que se representa como un mapa en el que las zonas

con más diferencia aparecen más claras. Una imagen guardada una sola vez tiende a mostrar un nivel de error parecido en toda su superficie. Una zona pegada o retocada puede mostrar un nivel distinto del resto. La técnica se describe en un documento técnico de Neal Krawetz (2007).

La lectura exige cautela. Una zona clara indica dónde mirar; no prueba que haya un retoque. Los bordes, los contrastes fuertes y las texturas ricas dan niveles de error altos incluso en imágenes sin tocar. La técnica solo sirve con imágenes con pérdida. Una imagen guardada muchas veces muestra un nivel de error bajo y uniforme. Un nivel uniforme tampoco garantiza que la imagen sea auténtica. Por eso el ELA no se usa como prueba única, sino que se contrasta con los metadatos, con el ruido del sensor (PRNU) y con la coherencia de las luces y las sombras. Si la otra parte aporta un mapa ELA, pregunta sobre qué archivo se calculó (el original o una copia recomprimida), con qué herramienta, con qué calidad y con qué otras comprobaciones se acompaña.



Figura 8. Ejemplo ilustrativo: imagen original, imagen con una persona añadida y mapa ELA simulado. No es el resultado de un análisis real.

Reforzar el lugar con Google Earth y Street View. Si la fotografía o el vídeo conservan las coordenadas GPS en los metadatos, esas coordenadas permiten comprobar el lugar con cuatro pasos.

1. Lee las coordenadas en los metadatos de la imagen o del vídeo, si existen.
2. Localiza en Google Earth el punto que indican los metadatos.
3. Compara lo que muestra la imagen o el vídeo con ese lugar en Street View, como edificios, calles, rótulos, relieve y sombras según la hora.
4. Guarda lo consultado, con fecha y hora, para el informe.

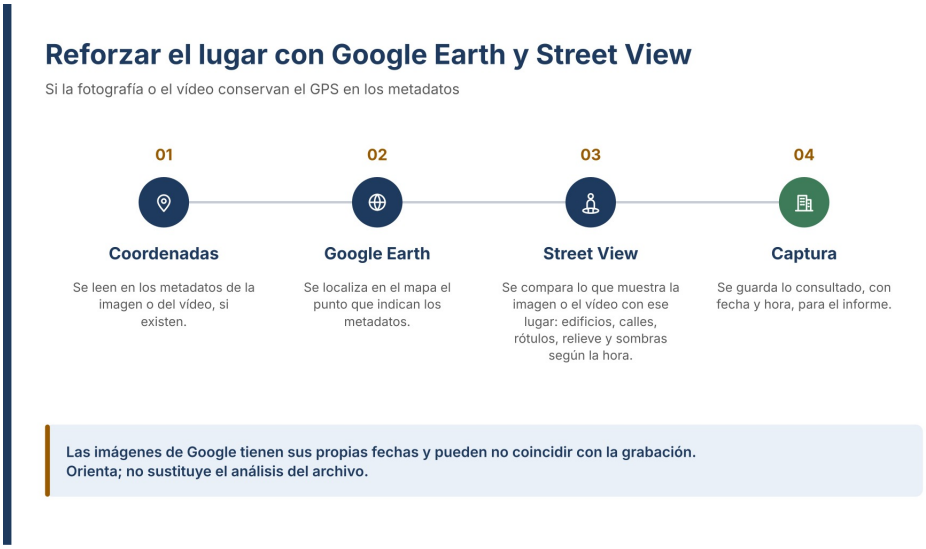

Figura 9. Pasos para verificar el lugar con las coordenadas de los metadatos.

Esta comprobación tiene límites. Las coordenadas pueden no existir o haberse modificado. Las imágenes de Google tienen sus propias fechas: Street View indica el mes y el año de la captura. Google Earth permite ver imágenes históricas. Ninguna tiene por qué coincidir con la fecha de la grabación. Unas obras, un rótulo nuevo o un edificio demolido explican las diferencias sin que haya montaje. Es una vía de orientación; no sustituye al análisis de la integridad del archivo ni al acta notarial del

lugar (capítulo 5). Si el entorno coincide, se refuerza que se grabó donde indican los metadatos.



Figura 10. Coordenadas, vista de calle y fotografía contrastadas en pantalla.

LO QUE DICE LA NORMA

La imagen y el vídeo se aportan como medios de reproducción (art. 382 LEC) y se valoran conforme a la sana crítica. El reconocimiento judicial es el examen directo por el juez o la jueza de lugares y objetos (art. 353 LEC).

BUENA PRÁCTICA TÉCNICA

Documenta el lugar real cuanto antes y con fecha cierta, porque los lugares cambian; se mueven muebles, se cambia una ventana, se reforma.

QUÉ HACER

1. Exige el original y el dispositivo.
2. Pide que se anote cuándo, dónde y quién lo grabó o lo fotografió.
3. Pide la secuencia completa, con lo que ocurre antes y después.
4. Si viene de una red social o de una página web, decide cómo preservar la publicación original con su enlace, fecha y comentarios antes de que se borre.
5. Que nadie aplique filtros, recorte ni cambie el formato del original.
6. Si hay duda sobre el lugar, que se fotografíe el espacio real desde los mismos ángulos y con fecha; valora además un acta notarial.
7. Pregunta a quien conoce el lugar o a las personas implicadas si la escena es posible.
8. Si el archivo conserva coordenadas GPS, contrástalas con Google Earth y Street View y guarda las capturas con fecha y hora.
9. Si se usa o se aporta un análisis ELA, anota el archivo analizado, la herramienta y la calidad. Contrástalo con otras comprobaciones.

ERRORES FRECUENTES

- Fiarse de la vista: «no se ve nada raro, será verdadero».
- Guardar una captura de la publicación y no el contenido original.
- Recortar el vídeo para mostrar solo el fragmento relevante.
- Comparar con fotos antiguas del lugar sin fecha fiable.
- Dar por hecho que, sin IA, no puede haber montaje.
- Tomar una zona clara de un mapa ELA como prueba de montaje.
- Dar por buena la ubicación porque la vista de calle se parece, sin comparar las fechas de las imágenes de Google.

MINI CHECKLIST

- ☐ Original y dispositivo localizados.
- ☐ Secuencia completa guardada.
- ☐ Cuándo, dónde y quién anotados.
- ☐ Publicación de origen preservada, si procede.
- ☐ Lugar real documentado, si hay duda.
- ☐ Ubicación contrastada con Google Earth y Street View, si hay coordenadas.

*Si tienes dudas, consúltame en **El perito responde** (ciberpering.com/el-perito-responde).*

CAPÍTULO 8

Chats, WhatsApp y capturas

por qué una captura no basta y qué la refuerza

IDEA CLAVE

Una captura muestra lo que había en una pantalla, no que la conversación existiera ni quién escribió; se refuerza con el dispositivo, la copia de seguridad y el móvil de la otra persona.

Explicación. Los chats son una prueba muy frecuente y también muy frágil. Una captura de pantalla es, al fin y al cabo, una imagen. Se puede fabricar con generadores gratuitos de conversaciones falsas, con un editor de imágenes o simplemente recortando. No lleva los datos internos de la aplicación y no acredita que el número sea de quien se dice. Tampoco muestra lo que se borró o se editó. Además, algunas aplicaciones permiten editar o eliminar mensajes durante un tiempo, así que hay que comprobar las funciones de la versión concreta que se usaba.



Figura 11. Lo que ve el juez o la jueza en un mensaje y los datos que lo acompañan. Esquema ilustrativo.

¿Qué refuerza una conversación digital? Lo más sólido es el dispositivo; una extracción forense del móvil, o una exportación de la conversación con sus adjuntos, conserva fechas, estados y archivos. Después viene la copia de seguridad, que permite contrastar el contenido con otra fuente. También cuenta tener la conversación completa, porque un extracto se puede descontextualizar.

Otra vía es el móvil de la otra persona. Si esa persona aporta su móvil o permite cotejarlo, se comprueba la coincidencia. En la misma línea están los datos que guarda el proveedor o el operador, a los que la parte no tiene acceso directo. Esos datos pueden desaparecer pronto; Delgado Martín recoge un informe de la Comisión Europea de 2025 según el cual los proveedores pueden eliminar datos en un plazo de días.



Un acta notarial o el cotejo del LAJ (Letrado o Letrada de la Administración de Justicia) dejan constancia de lo que se exhibió en ese momento. Eso sí, no prueban por sí solos que el mensaje se enviara desde ese teléfono ni que lo escribiera esa persona (capítulo 5).



Figura 12. Captura de pantalla frente a extracción completa del dispositivo.

LO QUE DICE LA NORMA

La conversación digital entra como instrumento que archiva y permite conocer datos (art. 384 LEC); la impresión de una captura suele tratarse como documento privado (art. 326 LEC). Si se impugna su autenticidad, quien la aporta puede proponer una prueba pericial u otra prueba útil (art. 326.2 LEC). El Tribunal Supremo se ha pronunciado sobre la impugnación de conversaciones en redes sociales y ha apuntado a la necesidad de una pericial sobre origen, identidad e integridad (STS 300/2015, de 19 de mayo).

BUENA PRÁCTICA TÉCNICA

Conviene conservar el móvil y la cuenta, no solo la imagen. Cuanto antes se haga una extracción o exportación, menos riesgo hay de que cambie algo. Para chats que se ven en una web, Safe Stamper declara certificar chats, entre otros contenidos (capítulo 5). La forma de aportar el resultado la decides tú.

Para conservar un chat hay dos vías, según lo que se necesite. La extracción completa del móvil, con herramientas como UFED o Magnet AXIOM, la hace un perito o una perito y clona el teléfono con todas sus conversaciones y adjuntos, no solo lo que se ve en pantalla. Safe Stamper declara grabar y certificar una o varias conversaciones concretas vistas en WhatsApp Web, con sello de tiempo y hash. Certifica lo capturado, es decir, que se escribió desde ese número de teléfono; no certifica lo que no se vio. Por eso la primera abarca todo el dispositivo y la segunda solo las conversaciones que se graban. A diferencia de la extracción completa, Safe Stamper no permite capturar audios ni vídeos.

QUÉ HACER

1. Indica a tu cliente que no borre la conversación, no salga del grupo y no cambie de móvil sin copia previa.
2. Pide la conversación completa, desde el primer mensaje relevante hasta el último.
3. Que anote el número o la cuenta, el nombre con que figura el contacto y cómo sabe quién es.
4. Los mensajes temporales son un riesgo; si están activados, lo que desaparezca no se podrá recuperar. Antes de cambiar su configuración, consulta a un perito o a una perito, porque cambiarla puede alterar la conversación en curso.
5. Encarga a un perito o a una perito una extracción o exportación con hash; valora además si añades un acta notarial.
6. Si hay una captura, pide también el archivo original de la imagen con sus metadatos.
7. Si los mensajes pueden confirmarse con la otra persona o con otro dispositivo, tenlo en cuenta al decidir cómo probarlo.

ERRORES FRECUENTES

- Aportar solo recortes de la conversación.
- Capturas sin fecha, sin hora o sin número visible.
- Pasar el chat a un documento de texto y perder el original.
- Borrar el chat para no ver los mensajes de la otra persona.
- Pensar que un acta notarial de la captura demuestra quién escribió.
- Fiarse de un chat sin comprobar si hay mensajes eliminados o marcados como «editado». En WhatsApp, quien recibe un mensaje no puede editarlo; solo puede hacerlo quien lo envió, durante los quince minutos siguientes, y el chat lo marca.

MINI CHECKLIST

- ☐ Conversación completa, no recortes.
- ☐ Móvil y cuenta conservados.
- ☐ Número o cuenta y nombre de contacto anotados.
- ☐ Capturas originales guardadas con sus metadatos.
- ☐ Decidido si se hace extracción, exportación o acta.

*Si tienes dudas, consúltame en **El perito responde** (ciberpering.com/el-perito-responde).*

CAPÍTULO 9

Documentos y firmas

tipos de firma, PDF con metadatos incoherentes y pedir siempre el original

IDEA CLAVE

Pide siempre el original; un PDF dice mucho de sí mismo y una firma válida no demuestra por sí sola quién la puso.

Explicación. Un documento digital puede estar bien presentado y tener una historia que no coincide con la que se cuenta. Esa historia está en el archivo; por eso hay que pedirlo. Antes de ver qué revisa un perito o una perito, hay que distinguir los tipos de firma, porque no todas prueban lo mismo.

La firma manuscrita en papel es la más clásica. La pericial caligráfica trabaja mejor con el original en papel y con muestras indubitadas; sobre una fotocopia o un escaneo se pierde información y se limitan las conclusiones. En el otro extremo está la imagen de una firma, que es un dibujo que se puede copiar y pegar en otro documento. No identifica a nadie por sí misma.

Además de esas dos, existen las firmas electrónicas. La simple, la avanzada y la cualificada se diferencian por las garantías técnicas y de identificación. La cualificada tiene el efecto jurídico de una firma manuscrita (Reglamento (UE) 910/2014, art. 25; Ley 6/2020). Algo distinto es la firma digital con certificado, que permite comprobar si el documento se modificó después de firmarlo. Eso sí, no excluye que otra persona usara el certificado, las credenciales o el dispositivo de la persona titular.

Cuando un perito o una perito revisa un PDF u otro documento, empieza por las fechas de creación y de modificación. Una fecha de creación posterior a la que aparece en el texto es una señal de alerta. Mira luego el programa que lo generó; una versión de programa que no existía cuando se dice que se redactó el documento es otra señal. También examina el historial de revisiones, porque algunos PDF conservan los cambios añadidos al final del archivo sin borrar lo anterior (modificaciones incrementales); eso se puede estudiar. Revisa los tipos de letra, las capas y las imágenes incrustadas, que pueden delatar un pegado posterior. Y, por último, comprueba la coherencia interna, como autor, formato, numeración y estilo frente a otros documentos del mismo origen.



Figura 13. Los metadatos de un PDF mostrados con ExifTool. Los datos de la pantalla son ficticios.

Hay que ser prudente. Un metadato incoherente es un indicio, no una prueba de falsedad, porque algunos programas reescriben fechas al guardar. Por eso se compara con el resto.

Correo electrónico y cabeceras. Un correo contiene, además del mensaje, las cabeceras, que son datos técnicos que no se ven al leerlo, como la persona remitente,

las personas destinatarias, la fecha, el identificador del mensaje y el recorrido por los servidores. Una impresión o una captura del correo no los muestra. Por eso se pide el correo original, en el formato que exporta el programa de correo (por ejemplo .eml o .msg), junto con el acceso a la cuenta o al dispositivo donde está. El perito o la perito comprueba si las fechas, los servidores y las direcciones de las cabeceras son coherentes entre sí y con el contenido. Una cabecera incoherente es un indicio, no una prueba de falsedad. Un archivo exportado puede haberse editado, así que se calcula su hash y se conserva el original (capítulo 3). Un correo puede desaparecer del servidor. Decide cómo preservarlo (capítulo 5).

En un informe sobre un correo se citan a menudo tres comprobaciones técnicas. SPF comprueba si el servidor que envió el mensaje estaba autorizado por el dominio del remitente (RFC 7208). DKIM comprueba si el mensaje lleva la firma del dominio y no ha cambiado por el camino (RFC 6376). DMARC comprueba si al menos una de las dos anteriores se ha superado y corresponde al dominio del remitente visible (RFC 9989). Una cabecera puede alterarse, así que lo que se comprueba en ella se contrasta con el servidor y con la cuenta de origen.

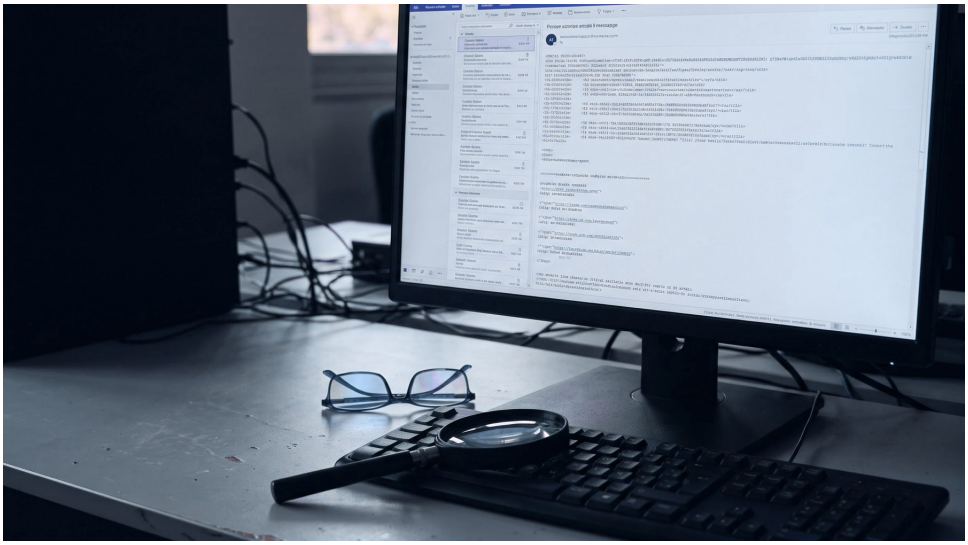

Figura 14. Las cabeceras de un correo electrónico contienen datos técnicos que no se ven al leerlo.

LO QUE DICE LA NORMA

Un documento privado se aporta con las reglas de los arts. 324 y siguientes LEC. Si se impugna su autenticidad, quien lo presentó puede pedir un cotejo pericial de letras o proponer cualquier otra prueba útil y pertinente (art. 326.2 LEC). Si el documento es electrónico y se impugna su autenticidad, su integridad o su fecha y hora, el art. 326.3 LEC remite a ese mismo procedimiento cuando el servicio de confianza empleado no es cualificado. Si se empleó un servicio cualificado, el art. 326.4 LEC presume que el documento reúne la característica cuestionada, siempre que el prestador figure en la lista de confianza; la carga de comprobarlo recae en quien impugna. El documento público tiene su propio régimen (art. 319 LEC). La pericial se rige por los arts. 335 y siguientes LEC.

BUENA PRÁCTICA TÉCNICA

Pide el original en papel y el archivo nativo, es decir, el archivo tal como lo creó el programa (por ejemplo, el PDF o el Word original). No hay que abrirlo en un editor para guardarlo después, porque eso puede cambiar la fecha de modificación. El hash se calcula antes de nada (capítulo 4). Para un documento digital, eGarante declara certificar su envío y su entrega; Safe Stamper, la existencia y la integridad de un archivo en una fecha concreta (capítulo 5).

QUÉ HACER

1. Pide el original, es decir, el documento en papel y el archivo tal como se creó o se recibió.
2. Que se calcule y se anote el hash del archivo antes de abrirlo.
3. Que se preserve una copia sin modificar y se trabaje sobre otra.
4. Si el documento lleva firma electrónica, que se valide con una herramienta fiable, como los validadores de las administraciones públicas (por ejemplo, VALIDe); que se guarde el informe de validación.
5. Si hay firmas manuscritas en discusión, que no se destruya el papel ni se reescanee sin conservar el original. Que se reserven muestras indubitadas de la misma época.
6. Pide la historia del documento, es decir, quién lo redactó, con qué programa, cuándo y cómo llegó a manos de tu cliente.
7. Compara la fecha que dice el documento con los metadatos y con el contexto.
8. Si es un correo, pide el original con sus cabeceras, no una impresión ni una captura.
9. Si algo no encaja, que nadie lo corrija. Consulta a un perito o a una perito.

ERRORES FRECUENTES

- Aceptar un PDF como original sin ver el archivo.
- Encargar una pericial de firma sobre fotocopias.
- Abrir el PDF en un editor y guardarlo.
- Creer que una firma electrónica válida significa que la pulsó la persona titular.
- Pensar que, si los metadatos parecen normales, el contenido no pudo cambiarse.
- Reescanear el documento y destruir el papel.
- Dar un correo por válido a partir de una impresión, sin sus cabeceras.

MINI CHECKLIST

- ☐ Tengo el papel original y el archivo nativo.
- ☐ Hash del archivo calculado y anotado.
- ☐ Copia sin modificar preservada.
- ☐ Firma electrónica validada y el informe guardado, si procede.
- ☐ Historia del documento anotada.
- ☐ Fechas del texto y de los metadatos comparadas.
- ☐ Correo original con sus cabeceras, si procede.

*Si tienes dudas, consúltame en **El perito responde** (ciberpering.com/el-perito-responde).*

PARTE III

Inteligencia artificial

CAPÍTULO 10

Qué ha cambiado

deepfakes, cheapfakes y por qué una grabación ya no basta por sí sola

IDEA CLAVE

Una grabación o una captura ya no se sostiene por sí sola como prueba; antes de apoyarte en ella, o de atacarla, hay que poder comprobar de dónde viene, quién aparece y si ha cambiado.

Explicación. Durante décadas, una foto o un audio se daban por fieles salvo prueba en contrario. Hoy ya no ocurre así, porque cualquiera puede crear o alterar contenido con herramientas gratuitas. Para ti, como profesional de la abogacía, eso significa que tanto la prueba que aportas como la que te aportan pueden ser cuestionadas con argumentos técnicos. Conviene distinguir dos tipos de falsificación.

El primero es el *deepfake* (ultrasuplantación). Se trata de audio, imagen o vídeo generado o alterado con inteligencia artificial que parece auténtico. Una voz clonada, una cara colocada sobre otro cuerpo o la foto de algo que nunca ocurrió son ejemplos típicos.

El segundo es el *cheapfake*, una alteración sencilla y sin IA. Se corta, se reordena, se cambia la velocidad, se tapa una palabra con ruido o se saca una frase de su contexto. Para hacerlo basta un editor gratuito y unos minutos.

El riesgo no está solo en la IA. Una grabación auténtica puede engañar por su contexto; una falsa puede colarse simplemente porque nadie pidió el original.

Existe además el efecto contrario. Si todo puede ser falso, se puede negar lo verdadero con un simple «eso es una IA». La doctrina lo ha llamado el «dividendo del mentiroso» (Chesney y Citron, 2019). De ahí que esta guía insista en dos cosas a la vez: no fabricar pruebas y no negar sin motivo las que aporta la otra parte.



Figura 15. Deepfake y cheapfake: dos vías para alterar una grabación.

LO QUE DICE LA NORMA

La ley no establece que una grabación sea fiable o no lo sea; deja su valoración en manos del juez o la jueza. Esa persona valora los medios de reproducción de palabra, sonido e imagen y los instrumentos de archivo de datos según las reglas de la sana crítica (arts. 382.3 y 384.3 LEC). Cuando se impugna una conversación digital, la jurisprudencia ha exigido garantías sobre su origen, la identidad de las personas que intervienen en la conversación y su integridad (STS 300/2015, de 19 de mayo). Esas tres preguntas ordenan toda la guía.

BUENA PRÁCTICA TÉCNICA

Trata cualquier prueba digital, tanto la tuya como la ajena, como si fuera a ponerse en duda. Así la preparas, o la analizas, con el mismo cuidado.

QUÉ HACER

1. Clasifica el contenido como audio, vídeo, fotografía, documento, chat, publicación en redes sociales o publicación web.
2. Plantéate las tres preguntas: ¿de qué dispositivo y aplicación procede (origen)? ¿quién habla, aparece o escribe (identidad)? ¿ha cambiado desde que se creó (integridad)?
3. Separa lo que sabes de lo que das por supuesto. Pide a tu cliente que haga lo mismo; una cosa es lo que ha visto y otra lo que supone.
4. Antes de nada, localiza el original y el dispositivo (capítulo 2).
5. No aceptes un «es real» o un «es falso» que se apoye solo en cómo suena o cómo se ve; pide comprobaciones.
6. Si el contenido es decisivo, plantea pronto una consulta técnica.

ERRORES FRECUENTES

- Dar por buena una prueba porque «se nota a simple vista». Los modelos actuales ya no dejan los defectos apreciables de hace unos años.
- Pensar que sin IA no hay montaje. Los cortes y las mezclas siguen sirviendo para falsear.
- Aceptar una prueba porque parece natural.
- Alegar «es una IA» sin señalar un solo indicio concreto.
- Fiarse de un detector gratuito como si fuera un veredicto (capítulo 12).

MINI CHECKLIST

☐ Sé si el contenido es audio, vídeo, fotografía, documento, chat, publicación en redes sociales o publicación web.

☐ Tengo anotados origen, identidad e integridad, es decir, qué se sabe y qué se supone.

☐ Sé dónde está el original.

☐ No he sacado conclusiones solo «de oído» o «de vista».

*Si tienes dudas, consúltame en **El perito responde** (ciberpering.com/el-perito-responde).*

CAPÍTULO 11

Inteligencia artificial

cómo se fabrica una prueba y qué huellas deja

IDEA CLAVE

La inteligencia artificial permite fabricar voz, imagen y vídeo verosímiles; cada fabricación puede dejar huellas que se buscan con métodos distintos, aunque ninguna prueba basta por sí sola; lo que da peso es la convergencia de indicios independientes.

Explicación. Los capítulos 10 y 12 explican por qué una grabación ya no basta y qué límites tienen los detectores. Este capítulo mira el otro lado, es decir, cómo se fabrica un contenido sintético y qué rastros puede dejar. Entender el proceso ayuda a formular mejor la pregunta al perito o a la perito (capítulo 16). Los generadores de imagen y de vídeo suelen basarse en redes generativas antagónicas o en modelos de difusión. Los de voz parten de una muestra de la persona.

Cómo se clona una voz. Una voz clonada se fabrica en cuatro fases consecutivas, que se describen a continuación.

1. **Muestra.** Se reúne audio de la persona. ElevenLabs recomienda aproximadamente entre uno y dos minutos de audio limpio para su clonado instantáneo.
2. **Extracción de rasgos.** El sistema obtiene del audio los rasgos que caracterizan la voz.

3. **Generación del habla.** El sistema produce una representación del sonido, como un espectrograma, para el texto que se quiere hacer decir.
4. **Conversión a audio.** Un componente llamado *vocoder* transforma esa representación en una señal sonora.

Cada fase puede dejar rastro en el espectrograma, en la forma de onda, en las huellas del *vocoder*, en la prosodia (la entonación y el ritmo) o en las transiciones entre sonidos. Estos rastros se buscan con análisis espectral y fonético (capítulo 6).

Un servicio comercial como ElevenLabs ofrece dos opciones, y la diferencia importa al valorar un audio. El clonado instantáneo no entrena un modelo propio, sino que parte de un modelo ya entrenado; su documentación indica entre uno y dos minutos de audio de buena calidad. El clonado profesional, de pago, entrena un modelo dedicado y su documentación recomienda como mínimo 30 minutos de audio de buena calidad. Según mi criterio, la calidad del instantáneo es media y la del profesional es casi perfecta. Es un ejemplo ilustrativo, no una recomendación ni una valoración del servicio.



Figura 16. Las cuatro fases de la clonación de una voz.



Huellas en imagen y vídeo. Las huellas se agrupan en familias. La tabla resume qué se mira en cada una y qué límite tiene (tabla 2).

Familia	Qué se mira	Límite
Espaciales	Manos, dientes, texto, reflejos, simetrías y fondos incoherentes	Los generadores mejoran; una imagen sin fallos visibles puede ser sintética
De frecuencia	Regularidades en el espectro de la imagen asociadas a las redes generativas antagónicas y a los modelos de difusión	Pueden alterarse al comprimir o al cambiar el tamaño
De ruido (PRNU)	El patrón de ruido de la imagen frente al del sensor de la cámara a la que se atribuye	Exige material de referencia de esa cámara
De metadatos	Datos de creación y de edición del archivo	Pueden faltar o editarse
De compresión	Rastros de guardados sucesivos (capítulo 7)	Solo en formatos con pérdida

Tabla 2. Familias de huellas que se examinan en una imagen o un vídeo, con lo que se mira en cada una y su límite. Fuente: elaboración propia.



Procedencia y marcas de agua. Dos vías buscan certificar el origen del contenido en lugar de analizar el contenido. La primera es la de la C2PA (Coalition for Content Provenance and Authenticity), que define un formato para incrustar en el archivo metadatos firmados criptográficamente, llamados credenciales de contenido. Indican qué dispositivo o programa produjo el archivo y qué ediciones sufrió. Dicen cómo se hizo el archivo; no dicen que lo que muestra sea verdadero. Pueden eliminarse al guardar de nuevo o al convertir el archivo. La segunda vía es SynthID, una marca de agua invisible que Google incorpora en contenido generado con sus modelos. Su detección depende de las herramientas de Google. Solo la incorporan algunos generadores, así que su ausencia no prueba que el contenido sea auténtico.



Límites de la detección. Un resultado de detección es un indicio. Un método entrenado con unos generadores puede fallar con otros nuevos. La compresión y el cambio de tamaño degradan las huellas. Atribuir un contenido a un generador concreto es más difícil que decir si parece sintético. La ausencia de huella tampoco garantiza la autenticidad. Por eso se acumulan indicios independientes, como los del archivo, los del contenido, los del contexto y los de la procedencia. Varios indicios débiles que apuntan en la misma dirección pesan más que uno solo.

Un caso documentado (Arup, 2024). Según la prensa, un empleado en Hong Kong de la multinacional Arup participó en una videollamada con quienes parecían ser su director financiero y otras personas de la empresa. Eran imitaciones hechas con inteligencia artificial. Se hicieron 15 transferencias por unos 200 millones de dólares de Hong Kong, unos 25,6 millones de dólares estadounidenses. Arup confirmó que era la víctima. El caso muestra el valor de confirmar por un segundo canal las órdenes de pago recibidas por voz o por vídeo. Las fuentes figuran en el anexo C.

El efecto contrario. Si todo puede ser falso, también se puede negar lo verdadero. Es el efecto descrito en el capítulo 10; el capítulo 19 explica cómo se impugna con motivos.

LO QUE DICE LA NORMA

Este capítulo no añade normas a las ya citadas. Ninguna norma procesal otorga a un detector valor de prueba (capítulo 12).

BUENA PRÁCTICA TÉCNICA

Conserva el original y calcula su hash antes de cualquier análisis (capítulo 3). Pregunta al perito o a la perito por varios métodos independientes, no por un porcentaje. Pide que el informe declare las limitaciones. Confirma por un segundo canal las órdenes de pago o las instrucciones recibidas por voz o por vídeo.

QUÉ HACER

1. Conserva el archivo original y calcula su hash antes de analizar nada.
2. Pregunta al perito o a la perito qué métodos independientes aplicará, en lugar de pedir un porcentaje de «probabilidad de IA».
3. Pide que el informe indique el método, la herramienta con su versión y las limitaciones.
4. Reúne el contexto, es decir, quién envió el archivo, cuándo, por qué canal y qué más se dijo.
5. Si el archivo trae credenciales de contenido, consérvalo tal como llegó, porque guardarlo de nuevo puede eliminarlas.
6. Ante una orden de pago o una instrucción recibida por voz o por vídeo, confirma por un segundo canal.

ERRORES FRECUENTES

- Tratar un detector como un veredicto.
- Dar por auténtico un archivo porque no muestra fallos visibles.
- Dar por falso un archivo porque no tiene credenciales de contenido ni marca de agua.
- Analizar una copia recomprimida como si fuera el original.
- Buscar una sola huella en lugar de varios indicios independientes.

MINI CHECKLIST

☐ Original conservado y hash calculado.

☐ Varios métodos independientes previstos.

☐ Método, herramienta y limitaciones en el informe.

☐ Contexto del archivo reunido.

*Si tienes dudas, consúltame en **El perito responde** (ciberpering.com/el-perito-responde).*

CAPÍTULO 12

Detectores de IA

qué son, sus límites, cautelas de privacidad y comprobación en cinco minutos

IDEA CLAVE

Un detector de IA devuelve una probabilidad, no un veredicto; sirve para decidir si merece la pena una pericial, no para sustituirla.

Explicación. Ante una duda, mucha gente pasa el archivo por un detector. Hay que saber qué hace exactamente. Un detector es un programa que estima si un audio, una imagen o un vídeo ha sido generado o alterado con IA. Funciona de dos maneras. Los clasificadores son modelos entrenados con ejemplos reales y sintéticos que calculan una probabilidad. Los lectores de marcas, por su parte, buscan una marca de agua o unos metadatos de procedencia que algunos generadores incrustan en sus resultados.

Los detectores tienen varios límites. El primero son los falsos positivos y los falsos negativos; un detector puede marcar como sintético algo real y dejar pasar algo falso. Además, depende del entrenamiento, ya que reconoce mejor lo que se parece a sus datos y los modelos nuevos pueden pasar sin ser detectados. A eso se suma la degradación por compresión, porque un audio recomprimido o reenviado reduce la fiabilidad.

Tampoco hay que fiarse de la marca de agua. Solo existe si el generador la puso. Su ausencia no demuestra que el contenido sea auténtico, porque quien falsifica no suele marcar. Además, dos detectores pueden dar resultados opuestos sobre el mismo

archivo. Y muchos son opacos; no explican por qué dan ese resultado, así que no se puede comprobar si es acertado.

Las publicaciones técnicas dan cifras de acierto muy altas, pero hay que leerlas con cuidado. Blázquez Moreno (2023) recoge, para distintos métodos, porcentajes que van del 75 % al 99,1 %; los atribuye a quienes proponen cada método. Son resultados de experimentos con conjuntos de datos concretos. No son la tasa de acierto que tendrá un detector con el archivo de tu cliente, recomprimido y de origen incierto. La misma fuente advierte de que los métodos de generación se sofistican y de que las técnicas de detección deben actualizarse al mismo ritmo.

Antes de usar un detector, lee las condiciones y los avisos que publique el propio servicio.

Cautelas de privacidad. Subir un audio o una imagen a un servicio externo es ceder datos personales a una tercera parte. Los servidores pueden estar fuera de la UE. Si la voz o la imagen es de una persona menor, la cautela es máxima. Hay que valorar la normativa de protección de datos (el Reglamento General de Protección de Datos [RGPD] y la Ley Orgánica de Protección de Datos Personales y garantía de los derechos digitales [LOPDGDD]), el consentimiento de quien aporta el material y, para ti, el deber de secreto profesional. Esta valoración es jurídica y te corresponde.

Cautelas de cadena de custodia. Trabaja siempre sobre una copia, nunca sobre el original. Calcula el hash antes y anota la herramienta, la versión, la fecha y el resultado. Manipular el original fuera de un procedimiento controlado puede servir a la otra parte para cuestionar la cadena de custodia.



LO QUE DICE LA NORMA

Ninguna norma procesal otorga a un detector valor de prueba. En su caso, el resultado entraría como un indicio, valorado con sana crítica, o como parte de una pericial.

BUENA PRÁCTICA TÉCNICA

Si aun así quieres hacer una comprobación rápida para decidir si encargar una pericial, puedes seguir seis pasos en unos cinco minutos.



Figura 17. Comprobación rápida con un detector de IA, en seis pasos.

1. **Consulta de privacidad.** Antes de subir nada, comprueba que puedes hacerlo, por privacidad y secreto profesional.
2. **Preservación.** Trabaja con una copia, calcula su hash y deja el original intacto.
3. **Varios análisis.** Pasa la copia por más de una herramienta, porque cada una se entrena con datos distintos. Guarda una captura de cada resultado.
4. **Lectura prudente.** Anota el porcentaje y el aviso del propio servicio. Es un indicio, no un «sí» o un «no».
5. **Cruce de datos.** Compara el resultado con los metadatos, el contexto y las personas que pueden confirmarlo.
6. **Siguiente paso.** Si hay indicios, plantea una pericial. Si no los hay, no concluyas que el contenido sea auténtico.

QUÉ HACER

1. Antes de subir nada, valora si procede por privacidad y secreto profesional.
2. Sube siempre una copia con su hash calculado, nunca el original.
3. Si procede, sigue los seis pasos.
4. Guarda un registro con herramienta, versión, fecha, hash y capturas.
5. Si el resultado es dudoso, consulta a un perito o a una perito.
6. No cites el porcentaje como una certeza ante nadie.

ERRORES FRECUENTES

- Subir el original o una copia sin hash.
- Usar una sola herramienta y tomarla como veredicto.
- Subir la voz de un menor a un servicio gratuito sin valorarlo.
- Interpretar la ausencia de marca como prueba de autenticidad.
- No guardar qué se hizo y con qué versión.

MINI CHECKLIST

- ☐ Consulta de privacidad hecha.
- ☐ Copia con hash, original intacto.
- ☐ Dos o tres herramientas probadas.
- ☐ Resultados y avisos guardados.
- ☐ Contrastado con contexto y metadatos.
- ☐ Decisión tomada sobre la pericial.

*Si tienes dudas, consúltame en **El perito responde** (ciberpering.com/el-perito-responde).*

PARTE IV

Deep web y criptoactivos

CAPÍTULO 13

Deep web y dark web

qué son, qué cambia para la prueba y cómo se preserva lo que se encuentra

> **IDEA CLAVE**
>
> *La deep web y la dark web no son lo mismo; lo que se encuentra en ellas es volátil y se preserva cuanto antes, con las mismas garantías que cualquier contenido en línea.*

Explicación. Según INCIBE, la deep web agrupa los contenidos a los que no llegan los buscadores habituales. Su existencia no es ilegal por sí misma. La dark web es una capa más oculta, a la que se accede con herramientas específicas como el navegador Tor y con direcciones que terminan en .onion. INCIBE señala que puede alojar actividad legítima y también riesgos importantes.

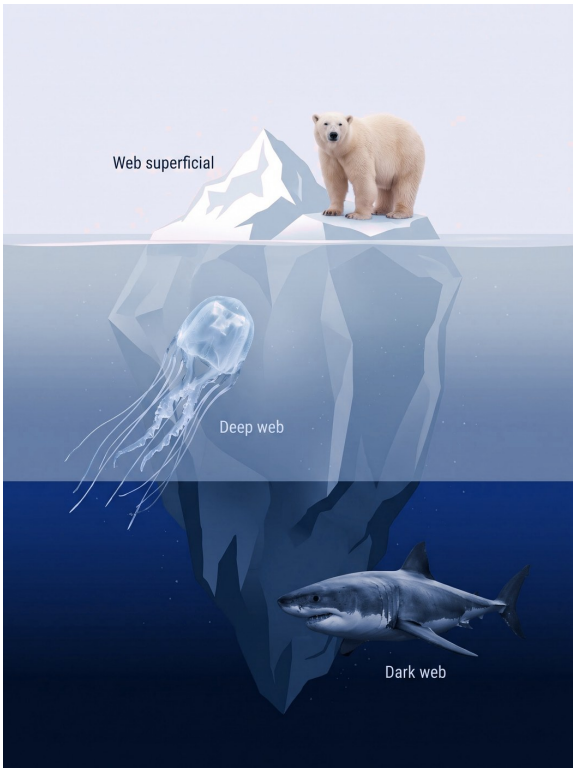

Figura 18. Capas de la web: superficial, profunda y oscura. Esquema ilustrativo; las proporciones no son reales.

Según el Proyecto Tor, los servicios onion protegen la dirección IP del servicio, de modo que no consta dónde está el servidor ni quién lo opera. Para la prueba eso tiene tres consecuencias.

1. **Volatilidad.** Los sitios pueden dejar de estar disponibles. Europol comunica en su sala de prensa operaciones contra mercados de la dark web.
2. **Autoría.** La página no suele mostrar quién opera el sitio. Atribuirlo a una persona exige otros indicios, ajenos a lo que muestra la página.
3. **Captura insuficiente.** Una captura o un enlace no bastan (capítulo 8), porque el contenido puede cambiar o desaparecer. Una dirección .onion se abre con Tor.

Cómo se preserva lo hallado. Se documenta la ruta de acceso (fecha y hora, equipo, navegador y dirección). El contenido se conserva con un servicio de certificación en línea, un acta notarial u otro mecanismo de los del capítulo 5. Si se piensa en un servicio de certificación en línea, hay que preguntarle a ese servicio si puede acceder a direcciones .onion; esta guía no lo afirma de ninguno. Todo archivo descargado se abre solo en un equipo dedicado a ese fin y aislado del equipo de trabajo habitual. Puede ser una máquina virtual, que es un ordenador simulado que funciona dentro del tuyo, como una ventana con su propio sistema y sus propios archivos, o un ordenador físico reservado solo para esto. Si lo descargado trae un virus, el problema se limita a ese equipo y no pasa a tus documentos ni a los de tu cliente.



Figura 19. Pasos para preservar un contenido hallado en la dark web.

LO QUE DICE LA NORMA

Esta guía no analiza qué conductas son delito en la dark web ni si el mero acceso tiene consecuencias legales. Es una cuestión jurídica que corresponde a la persona letrada. La preservación de la prueba sigue las reglas del capítulo 5.

BUENA PRÁCTICA TÉCNICA

Quien accede se limita a observar y documentar. Trabaja desde un equipo dedicado, ya sea una máquina virtual aislada de tu equipo principal o un ordenador físico reservado solo para esto, con registro de lo que se hace y con el hash de lo que se descarga (capítulo 3).

QUÉ HACER

1. Anota cómo llegó la dirección .onion a tu cliente y quién se la facilitó.
2. Pide que se conserve el contenido cuanto antes, porque puede desaparecer.
3. Decide con antelación el mecanismo de preservación (capítulo 5).
4. Limita el acceso a observar y documentar. Cualquier interacción con otras personas (registrarse, comprar, contactar) la decide antes la persona letrada.
5. Abre los archivos descargados solo en un equipo dedicado y aislado, ya sea una máquina virtual o un ordenador físico reservado para ello.
6. Pregunta al perito o a la perito si tiene medios para acceder y preservar contenido en la dark web, y si lo hace desde un equipo dedicado y aislado, antes de encargárselo.

ERRORES FRECUENTES

- Confundir deep web con dark web.
- Guardar solo el enlace .onion.
- Esperar a que el contenido siga disponible.
- Abrir archivos descargados en el equipo de trabajo habitual.
- Atribuir un sitio a una persona solo por lo que dice la página.

MINI CHECKLIST

- ☐ Origen de la dirección anotado.
- ☐ Mecanismo de preservación decidido.
- ☐ Ruta de acceso documentada con fecha y hora.
- ☐ Archivos descargados abiertos solo en un equipo dedicado y aislado.
- ☐ Consulta jurídica hecha antes de cualquier interacción.

*Si tienes dudas, consúltame en **El perito responde** (ciberpering.com/el-perito-responde).*

CAPÍTULO 14

Criptoactivos

qué muestra la cadena de bloques, qué no y cómo se preserva

IDEA CLAVE

La cadena de bloques es un registro público de transacciones, pero identifica direcciones, no personas; vincular una dirección con alguien exige pruebas ajenas al registro.

Explicación. Los criptoactivos son, según la definición del Reglamento (UE) 2023/1114 (MiCA) que recogen las autoridades europeas, representaciones digitales de un valor o un derecho que pueden transferirse y almacenarse electrónicamente mediante tecnología de registro distribuido o una tecnología similar. Bitcoin y Ethereum son los ejemplos más conocidos. En Bitcoin, cada transferencia queda anotada en la cadena de bloques, un registro público que cualquiera puede consultar. Cada transacción tiene un identificador propio (el hash de la transacción, o TXID), de 64 caracteres hexadecimales. En Ethereum y en las cadenas de su familia el hash de la transacción también es de 64 caracteres hexadecimales, pero se escribe con el prefijo 0x.

El control de los fondos depende de las claves privadas. Un monedero (wallet) es, en esencia, un conjunto de claves privadas; quien dispone de ellas puede autorizar transferencias. Para la prueba hay una consecuencia directa. El registro muestra qué

dirección envió fondos a qué otra y cuándo, pero no dice quién está detrás de cada dirección.



Figura 20. Qué se puede leer en la cadena de bloques y qué requiere otras pruebas. Esquema ilustrativo.

Se distinguen así dos planos

1. **Lo que consta en el registro.** Direcciones, importes, fechas y horas de los bloques, identificadores de transacción.
2. **Lo que no consta.** La identidad de quien controla una dirección, el motivo de la transferencia y si dos direcciones pertenecen a la misma persona.

Cómo se lee una transacción. En Bitcoin, una transacción gasta salidas de transacciones anteriores, que se identifican por su TXID y por un número de salida. Eso permite seguir el recorrido de los fondos de una transacción a la siguiente. A partir del TXID, un explorador de bloques muestra si la transacción está confirmada, qué direcciones y qué importes intervienen, qué comisión se pagó y cuántas confirmaciones tiene. Una transacción pendiente todavía no está incluida en ningún bloque. El hash de una transacción no es una dirección, aunque ambos sean cadenas de caracteres.

La fecha y la hora. Cada transacción lleva la hora del bloque que la incluye, y esa hora no es exacta. En Bitcoin, la hora de un bloque solo tiene que ser posterior a la mediana de los once bloques anteriores y no superar en más de dos horas la hora que calcula la red. Sirve para ordenar los hechos de forma aproximada, no para establecer una hora exacta. La fecha y la hora de tu propia consulta sí se pueden establecer con los medios del capítulo 5.

Existen programas de análisis que agrupan direcciones por patrones de uso y las etiquetan con nombres de servicios. Se basan en reglas como suponer que las direcciones que se gastan juntas en una misma transacción pertenecen a la misma persona. Meiklejohn y otros (2013) usaron reglas de este tipo para agrupar direcciones de Bitcoin. Estudios posteriores muestran sus límites. Kappos y otros (2022) documentan agrupaciones erróneas por transacciones CoinJoin, en las que participan varias personas, y Möser y Narayanan (2021) indican que las técnicas

habituales descansan en reglas que no se habían evaluado con rigor. Son indicios, no identificación; las agrupaciones se basan en suposiciones que pueden fallar. Las etiquetas también pueden ser erróneas. Una conclusión que descanse solo en una agrupación automática debe presentarse como hipótesis.

La captura no basta. Una captura de un explorador de bloques es una página web más; vale lo que vale cualquier captura (capítulo 8). Se preserva como cualquier contenido en línea (capítulo 5) y se anota la dirección, el TXID, el explorador consultado y la fecha y hora de la consulta. Conviene conservar también la propia pantalla del monedero o de la plataforma de donde procede el dato, con su contexto.

Cómo se obtiene la información. El procedimiento sigue estos pasos.

1. **Datos de partida.** Se reúnen las direcciones, los TXID, las fechas, los importes y la plataforma o el monedero que aporta la persona cliente.
2. **Consulta del registro.** Se consulta cada TXID en más de un explorador de bloques, o en un nodo propio, y se comprueba que consta, que está confirmado y que coincide con las direcciones y los importes que se indican.
3. **Conservación de la consulta.** Se guarda lo consultado con el TXID, el explorador, la fecha y la hora, por alguno de los medios del capítulo 5, y se calcula el hash de lo guardado (capítulo 4).
4. **Recorrido de los fondos.** Se sigue la transacción hacia delante o hacia atrás hasta donde el registro lo permite. Se anota aparte lo que se lee del registro y lo que se supone.
5. **Plataforma.** Si los fondos llegan a una dirección de una plataforma, el registro público termina ahí. Lo que hay detrás de esa dirección lo conoce, en su caso, la plataforma. Hay que pedírselo (véase más abajo).
6. **Monedero propio.** Si los fondos están en un monedero de la persona cliente, se documenta en su dispositivo, con ella presente, qué direcciones y qué

transacciones muestra el monedero, y se contrasta cada una con el registro público. No se accede a las claves privadas.

Cómo se pide la información a la plataforma. Hay vías distintas según quién la pida y de quién sean los datos. Si la persona cliente tiene cuenta en la plataforma, puede ejercer el derecho de acceso del artículo 15 del RGPD y pedir una copia de los datos personales que la plataforma trata sobre ella. El plazo de respuesta es de un mes. La plataforma puede ampliarlo en los casos que prevé el reglamento. También puede descargar los historiales que la propia plataforma ofrezca en su cuenta, sin modificarlos. Si la información corresponde a otra persona o está en poder de un tercero, no basta con pedirla. La LEC prevé las diligencias preliminares (art. 256, con una lista cerrada de supuestos), la exhibición de documentos entre las partes (art. 328) y la exhibición de documentos por terceros que no son parte (art. 330). Los proveedores de servicios de criptoactivos están obligados a conservar registros de sus servicios, órdenes y operaciones (art. 68 del Reglamento (UE) 2023/1114, desarrollado por el Reglamento Delegado (UE) 2025/1140). Esta guía no indica cuánto tiempo conserva cada plataforma esos datos; se le pregunta a la propia plataforma.

Dónde se custodian los fondos. Si la persona cliente opera con una plataforma, la entidad que presta servicios con criptoactivos guarda los datos de la cuenta y de las operaciones. Desde el 1 de julio de 2026, según la Comisión Nacional del Mercado de Valores (CNMV), solo pueden operar en España proveedores autorizados por la CNMV u otras autoridades europeas. El propio organismo remite a los registros de la Autoridad Europea de Valores y Mercados (ESMA) y de la CNMV para comprobarlo. Con el Reglamento (UE) 2023/1113, aplicable desde el 30 de diciembre de 2024, las transferencias de criptoactivos entre estos proveedores llevan información sobre quien las ordena y quien las recibe. Si los fondos están en un monedero que controla la propia persona cliente, esa información no existe y la prueba es la que aporte la persona cliente con sus claves y su dispositivo.

LO QUE DICE LA NORMA

Esta guía no analiza la calificación jurídica de los criptoactivos ni cómo se embargan o se recuperan, cuestiones que corresponden a la persona letrada. Sí conviene saber que la Sala Segunda del Tribunal Supremo se pronunció en la sentencia 326/2019, de 20 de junio de 2019, sobre un caso de bitcoins; la persona letrada debe leerla antes de plantear la pretensión.

BUENA PRÁCTICA TÉCNICA

Quien analiza una transacción parte del TXID, no de un enlace ni de una imagen. Consulta más de un explorador, deja constancia de las fechas de consulta y separa lo que lee del registro de lo que interpreta. No pide ni custodia claves privadas ni frases de recuperación de la persona cliente; si el trabajo exige acceder a un monedero, se decide antes con la persona letrada y con la persona cliente cómo se hará y con qué garantías.

QUÉ HACER

1. Pide a tu cliente las direcciones, los TXID, las fechas, los importes y la plataforma o el monedero utilizado. Pregunta si los fondos estaban en una plataforma o en un monedero propio y qué dispositivo lo contiene.
2. Verifica en los registros de ESMA y de la CNMV si el proveedor está autorizado.
3. Pide que se conserve cuanto antes la documentación de la cuenta y las comunicaciones con la plataforma (capítulo 5).
4. Si tu cliente tiene cuenta, pídele que solicite a la plataforma una copia de sus datos y que descargue los historiales disponibles sin modificarlos. Anota la fecha y calcula su hash (capítulo 4).
5. Conserva cada consulta a un explorador de bloques con el TXID, el explorador, la fecha y la hora (capítulo 5).
6. Contrasta cada TXID en más de un explorador y comprueba que está confirmado y que coincide con las direcciones y los importes que cuenta tu cliente.
7. Si necesitas información de otra persona o de una plataforma ajena a tu cliente, anota qué datos faltan y por qué vía pueden pedirse.
8. Trata las agrupaciones y etiquetas de direcciones como indicios y pide que se explique cómo se obtuvieron.
9. Nunca pidas a tu cliente claves privadas ni frases de recuperación por correo ni por mensajería.
10. Pregunta al perito o a la perito qué puede concluir y qué no (capítulo 18) antes de encargar el análisis.

ERRORES FRECUENTES

- Dar por hecho que una dirección identifica a una persona.
- Presentar como prueba la captura de un explorador sin TXID ni fecha de consulta.
- Consultar un solo explorador y no anotar cuál.
- Dar por exacta la hora que muestra el explorador.
- Tratar como confirmada una transacción que aparece pendiente.
- Confundir el hash de una transacción con una dirección.
- Aceptar una etiqueta o una agrupación de direcciones sin saber cómo se obtuvo.
- Compartir claves privadas o frases de recuperación.
- Dejar pasar el tiempo sin pedir a la plataforma que conserve los datos.

MINI CHECKLIST

- ☐ Direcciones y TXID anotados.
- ☐ Plataforma o monedero identificados.
- ☐ Autorización del proveedor comprobada en los registros.
- ☐ Consulta al explorador documentada con fecha y hora.
- ☐ TXID contrastado en más de un explorador.
- ☐ Estado confirmado de la transacción comprobado.
- ☐ Hora del bloque tratada como aproximada.
- ☐ Copia de los datos y documentación de la cuenta solicitadas a la plataforma.
- ☐ Agrupaciones y etiquetas tratadas como indicios.
- ☐ Ninguna clave privada compartida.

*Si tienes dudas, consúltame en **El perito responde** (ciberpering.com/el-perito-responde).*

PARTE V

Cuándo y cómo recurrir a un perito o a una perito

CAPÍTULO 15

Cuándo encargar una pericial

señales de alerta, plazos y coste orientativo

IDEA CLAVE

Encarga la pericial cuando la prueba sea decisiva y haya una duda técnica concreta. Hazlo pronto, porque el análisis necesita tiempo y material íntegro.



Explicación. Hay que decidir si hace falta un perito o una perito. No hace falta una pericial para cada audio o cada captura. Hace falta cuando el contenido puede inclinar el resultado y hay motivos para dudar de su origen, su identidad o su integridad. También sirve para reforzar tu propia prueba antes de que alguien la impugne.

Señales de alerta. ¿Cómo saber si hay motivos para dudar? Estas son las señales más habituales.

- No existe el original o solo hay una copia reenviada.
- La otra parte no entrega el original ni el dispositivo.
- El archivo tiene metadatos incoherentes, un formato inesperado o falta de metadatos.
- Se oyen o se ven saltos, cambios de ruido de fondo, cortes o ediciones.
- La voz o la imagen resulta «demasiado limpia» o no encaja con el lugar.
- El contenido es decisivo y fácil de fabricar.
- Solo se aporta un extracto de una conversación o de una grabación.
- Quien lo aporta no sabe explicar cómo lo obtuvo.

Ninguna de estas señales prueba una manipulación. Son motivos para mirar con método.

> **LO QUE DICE LA NORMA**
>
> El dictamen pericial se aporta con la demanda o la contestación, o se anuncia si no es posible; en ciertos casos puede presentarse más tarde (arts. 336 a 338 LEC). El perito o la perito puede ser llamado a ratificarlo (art. 347 LEC). Los momentos procesales concretos los gestionas tú.

> **BUENA PRÁCTICA TÉCNICA**
>
> Antes de encargar nada hay tres cuestiones prácticas.

- **Plazos.** Dependen del número de archivos, de si hay que extraer un dispositivo, de la duración del audio o vídeo y del grado de detalle exigido. Pide siempre al perito o a la perito un plazo estimado tras ver el material. No existe un plazo estándar fiable.
- **Coste.** Depende de los mismos factores, de la urgencia y de si hay que ratificar el informe en sala. Pide un presupuesto por escrito con el alcance definido.

- **Consulta previa.** En El perito responde puedes obtener una orientación sobre qué se podría analizar antes de encargar nada. Es una orientación previa; el dictamen es otro documento.

QUÉ HACER

1. Escribe el objetivo que persigues con la pericial, en una frase (capítulo 17).
2. Reúne el material (originales, dispositivos, contexto y la ficha de origen, con hash).
3. Haz una consulta orientativa para saber qué es posible y qué no.
4. Pide presupuesto, alcance y plazo por escrito.
5. Formaliza el encargo con la hoja de encargo pericial (anexo E4).
6. Entrega el material con justificante de recepción (anexo E3) y hash.
7. Pregunta si el perito o la perito podrá ratificar el informe y cuándo.
8. Comprueba que el plazo del encargo es compatible con los plazos procesales.

ERRORES FRECUENTES

- Esperar a que la otra parte impugne para empezar.
- Encargar sin tener el original.
- Pedir un informe «favorable».
- Tomar la consulta orientativa por el dictamen.
- Elegir solo por precio o por rapidez.
- No prever la ratificación en la vista o el juicio.

MINI CHECKLIST

- ☐ La prueba es decisiva y hay una duda técnica concreta.
- ☐ Objetivo de la pericial escrito en una frase.
- ☐ Material original reunido, con hash.
- ☐ Presupuesto, alcance y plazo por escrito.
- ☐ Plazo del encargo compatible con los plazos procesales.
- ☐ Ratificación prevista.

*Si tienes dudas, consúltame en **El perito responde** (ciberpering.com/el-perito-responde).*

CAPÍTULO 16

Cómo pedir una pericial sobre una prueba digital

preguntas que sí se pueden responder

IDEA CLAVE

Una pericial vale lo que vale su pregunta; si preguntas «¿es auténtico?», casi nunca habrá una respuesta técnica; si preguntas por algo comprobable, sí.



Explicación. Casi toda pericial gira en torno al origen, la identidad y la integridad (capítulo 17). Aquí vemos cómo traducir una necesidad, la de probar la autenticidad de

una evidencia digital, en preguntas cuyas conclusiones un perito o una perito pueda avalar en su informe.

El fallo más habitual es preguntar por el significado de la prueba en lugar de por el propio archivo. «¿Es verdad lo que dice el audio?» y «¿es falso este vídeo?» son preguntas sobre el significado de la prueba. La veracidad de una conversación, de una escena o de una publicación la valora el juez o la jueza. Un perito o una perito responde sobre lo técnico, es decir, qué contiene el archivo, cómo está construido y si hay indicios de que se haya alterado.

Una buena pregunta tiene tres rasgos. Se refiere a un archivo concreto, con su hash. Nombra algo observable, como un corte, un empalme, una recompresión o una incoherencia entre fecha y contenido. Y admite varias respuestas: «sí», «no» o «con este material no se puede saber».

La tabla siguiente muestra cómo reformular preguntas habituales. Son ejemplos de redacción, no fórmulas cerradas (tabla 3).

En lugar de preguntar...	Pregunta mejor...	Por qué
¿Es auténtico este audio?	¿Presenta el archivo indicios de cortes, empalmes o inserciones? Si los hay, ¿en qué instantes?	La autenticidad en sentido amplio no se mide; los indicios en el propio archivo, sí
¿Es falso este vídeo?	¿Muestra el archivo señales de edición, recompresión o generación sintética? ¿Son compatibles sus metadatos con el dispositivo que se declara?	Se pide lo observable y se deja la valoración al juez o a la jueza
¿Es esta la voz de la persona que se indica?	¿Puede compararse esta voz con muestras indubitadas de esa persona?	Es otra disciplina, la fonética forense (capítulo 6)

En lugar de preguntar...	Pregunta mejor...	Por qué
¿Se ha manipulado el chat?	¿Constan estos mensajes, con la misma fecha, la misma persona emisora y el mismo texto, en el dispositivo del que proceden?	Se pide comprobar el origen sobre el dispositivo, no sobre la captura
¿Es válido este PDF?	¿Tiene el archivo versiones, metadatos o estructura que contradigan la fecha o la autoría que se le atribuyen?	La validez jurídica no es una cuestión técnica

Tabla 3. Preguntas habituales sobre una prueba digital y su reformulación en preguntas que un perito o una perito puede contestar. Fuente: elaboración propia.

Qué necesita el perito o la perito para responder. Cuanto más completo el material, más podrá afirmar. Para cualquier archivo, lo habitual es lo siguiente (tabla 4).

Material	Para qué sirve
Archivo original, sin reenviar, con su hash	Es la base de cualquier análisis; sin él, muchas comprobaciones no son posibles
Dispositivo o aplicación de origen	Permite comprobar origen, bases de datos y registros
Grabación o secuencia completa	Los cortes se buscan también en lo que falta, no solo en lo que se oye
Contexto (quién, cuándo, dónde, con qué)	Permite contrastar el archivo con lo declarado
Muestras de referencia, si existen	Otras grabaciones del mismo dispositivo o de la misma persona, para comparar
La pregunta y lo que se pretende acreditar	Define el alcance y evita un análisis sin rumbo

Tabla 4. Material que necesita el perito o la perito para responder y para qué sirve cada elemento. Fuente: elaboración propia.

BUENA PRÁCTICA TÉCNICA

Habla con el perito o la perito antes de entregar nada. En esa conversación se comprueba si la pregunta se puede responder con el material disponible. A veces la respuesta honesta es que no. Saberlo pronto es útil. Si hay varias preguntas, es preferible separarlas, porque cada una puede requerir un método y un perfil distintos (capítulo 17).

QUÉ HACER

1. Escribe qué necesitas probar, en una frase y sin adjetivos.
2. Pásala a una pregunta sobre algo observable en el archivo.
3. Comprueba que nombra un archivo concreto, con su hash.
4. Añade lo que necesitas saber si la respuesta es «no hay indicios».
5. Reúne el material de la tabla y anota lo que falte.
6. Consulta con el perito o la perito si la pregunta se puede responder antes de encargar el análisis (capítulo 15).
7. Si hay dos preguntas de naturaleza distinta, sepáralas.

ERRORES FRECUENTES

- Preguntar si algo «es verdad», «es auténtico» o «es falso».
- Pedir identificar a quien habla a un perito o a una perito de audio y vídeo.
- Dar al perito o a la perito solo la transcripción o la captura.
- Escribir la pregunta con la conclusión dentro («demuestre que se cortó»).
- Entregar solo el fragmento que interesa.
- No decir qué se quiere acreditar.

MINI CHECKLIST

- ☐ La pregunta se refiere a un archivo concreto, con su hash.
- ☐ Nombra algo observable.
- ☐ Admite «no se puede saber» como respuesta.
- ☐ El material entregado es original y completo.
- ☐ He dicho qué pretendo acreditar.

*Si tienes dudas, consúltame en **El perito responde** (ciberpering.com/el-perito-responde).*

CAPÍTULO 17

Qué mira el perito o la perito

origen, identidad, integridad y elección del perito o de la perito según la pregunta

---

IDEA CLAVE

Un perito o una perito competente responde a una pregunta concreta con un método que otra persona profesional pueda repetir; elegir bien depende de qué quieres saber, no de qué título suena mejor.

Explicación. Si se encarga una pericial, hay que decidir quién analiza el contenido. Casi toda pericial sobre prueba digital se ordena alrededor de tres preguntas. La primera es el origen: ¿de qué dispositivo, aplicación o cuenta procede? La segunda es la identidad: ¿quién habla, aparece o escribe? La tercera es la integridad: ¿ha cambiado desde que se creó o se recibió?

A ellas se suma una cuarta cuestión que no es técnica, la veracidad del contenido, es decir, si lo que muestra ocurrió realmente. El perito o la perito puede aportar indicios, pero la valoración final es del juez o de la jueza.

Como no todos los peritos ni todas las peritos responden a las mismas preguntas, la tabla siguiente orienta sobre el perfil que encaja con cada una. Ten en cuenta que puede haber solapamientos (tabla 5).

Si la pregunta es...	Perfil que encaja	Qué suele hacer
¿El audio o el vídeo ha sido cortado, empalmado o procesado? ¿Cómo se grabó y se transmitió?	Perito tecnológico	Análisis técnico del audio y del vídeo, códecs, contenedor, espectrograma, ruido, redes y telefonía
¿Qué contiene este móvil u ordenador? ¿Este chat o documento es íntegro y de dónde sale?	Perito tecnológico	Extracción, copias forenses, bases de datos de aplicaciones, registros, metadatos, hash
¿Es esta la voz de esta persona? ¿Qué se dice exactamente en un audio difícil?	Fonética forense	Comparación de voces, análisis del habla, transcripción
¿Esta firma o este manuscrito es de esta persona?	Grafoscopia o documentoscopia	Comparación con muestras indubitadas, análisis del soporte y la tinta

Tabla 5. Perfil profesional que encaja con cada tipo de pregunta y lo que suele hacer. Fuente: elaboración propia.

Mi perfil es el de perito tecnológico, que corresponde a las dos primeras filas. Si tu pregunta corresponde a otra fila, necesitas a esa persona especialista; te lo diré sin problema desde **El perito responde**. Además, hay asuntos que requieren dos perfiles.



LO QUE DICE LA NORMA

Los peritos y las peritos deben poseer el título oficial correspondiente a la materia y, si esta no tiene título oficial, ser personas entendidas en ella (art. 340 LEC). Prometen actuar con la mayor objetividad (art. 335.2 LEC). El dictamen puede aportarse con la demanda o la contestación y el perito o la perito puede ser llamado a ratificarlo en el juicio o la vista (arts. 336 y 347 LEC).

BUENA PRÁCTICA TÉCNICA

Un informe pericial sólido suele incluir seis apartados, que debes reconocer cuando lo recibas.

1. **Objeto:** qué se pregunta.
2. **Material recibido:** qué se recibió, de quién y con qué hash.
3. **Método:** técnicas y herramientas, con versión.
4. **Resultados:** lo observado, con capturas y datos.
5. **Conclusiones:** cada una con su grado de certeza, separando lo que se puede afirmar de lo que no.

6. **Limitaciones:** lo que el material no permitía comprobar.

La UNE 197001:2019, «Criterios generales para la elaboración de informes periciales», establece la estructura mínima de un informe pericial, a saber, título, identificación, paginación, declaración de tachas, juramento o promesa cuando proceda, índice, cuerpo del informe y anejos. Dice que el cuerpo recoge objeto, alcance, antecedentes, consideraciones preliminares, documentos de referencia, terminología, desarrollo del estudio y conclusiones. Añade que un informe, una vez emitido, no debe alterarse. Se limita a la forma del informe; los métodos de la pericial y las reglas procesales se rigen por otras normas. En cuanto al método, Martínez Galindo (2022) recoge que la ISO/IEC 27037 exige un proceso reproducible, comprensible y verificable, con herramientas contrastadas.

Blázquez Moreno (2023) describe la UNE 71506:2013 como un proceso en fases, que son preservación de la evidencia original, adquisición mediante una copia que no modifica los metadatos, documentación cronológica de los pasos y de las herramientas, análisis y presentación del informe. Puedes usar esa secuencia como guion; pide al perito o a la perito que te indique en qué fase hizo cada cosa y dónde consta.

QUÉ HACER

1. Escribe qué necesitas probar y las preguntas técnicas que se derivan de ello. Si las preguntas requieren perfiles distintos (tabla 5), puede hacer falta más de un perito o una perito.
2. Elige el perfil por las preguntas técnicas.
3. Pregunta por la titulación, la experiencia en ese tipo de análisis y las herramientas que usa.
4. Pregunta si trabaja sobre copia y si conserva evidencias y registros.
5. Pide el alcance por escrito: qué analizará, qué entregará y en qué plazo.
6. Entrega el material con su hash y pide un justificante de recepción.
7. Lee el informe como lo leerá el juez o la jueza: ¿se entiende?, ¿se puede repetir?, ¿las conclusiones están respaldadas?

ERRORES FRECUENTES

- Encargar una «pericial de IA» sin saber qué necesitas probar.
- Elegir solo por precio.
- Entregar al perito o a la perito copias y no los originales.
- Pedir una conclusión favorable en lugar de una respuesta.
- Aceptar un informe sin método ni limitaciones.
- Confundir la comprobación del archivo con la identificación de quien habla.

MINI CHECKLIST

- ☐ Tengo claro qué necesito probar y qué preguntas técnicas se derivan.
- ☐ El perfil encaja con la pregunta.
- ☐ Sé qué herramientas y método se usarán.
- ☐ Alcance, entregable y plazo por escrito.
- ☐ Material entregado con hash y justificante de recepción.

*Si tienes dudas, consúltame en **El perito responde** (ciberpering.com/el-perito-responde).*

CAPÍTULO 18

Qué puede concluir un perito o una perito y qué no

IDEA CLAVE

Un buen informe separa lo que se puede afirmar con seguridad, lo que solo se puede afirmar con reservas y lo que el material no permite decir; desconfía de un informe que los mezcle.



Explicación. Quien encarga una pericial espera una respuesta. Quien la lee, a veces, entiende que el informe dice más de lo que dice. Este capítulo establece, por tipo de prueba, qué suele poder concluirse y qué no. Es una guía general; en cada caso manda

el material recibido; un archivo recomprimido o incompleto reduce lo que se puede afirmar.

Para leer la tabla, ten en cuenta tres niveles. **Afirmable** es lo que se comprueba de forma directa y repetible. **Con reservas** es lo que ofrece indicios que dependen del material, del método y del estado del archivo. **No afirmable** es lo que queda fuera del alcance de un análisis técnico del archivo (tabla 6).

Prueba	Afirmable	Con reservas	No afirmable
Cualquier archivo	Su hash, tamaño, formato, contenedor y códec; si dos archivos son idénticos o no	Que no ha cambiado desde una fecha anterior, solo si existe un hash o un sello de tiempo de esa fecha	Que su contenido sea auténtico solo porque el hash sea correcto
Audio	Qué contiene y cómo está codificado; saltos o discontinuidades observables y su instante	Ausencia de edición, sobre todo si está recomprimido; continuidad por la frecuencia de red cuando existe; indicios de voz sintética	Quién habla (fonética forense); que lo dicho sea verdad; el momento real de la grabación solo a partir de los metadatos
Vídeo e imagen	Estructura del archivo, fotogramas repetidos o cortes observables, incoherencias entre metadatos y contenido	Indicios de montaje o generación sintética; vínculo con un dispositivo por el ruido del sensor si hay original y referencias	Que la escena ocurrió; que el lugar es el declarado sin contraste con el lugar real
Chat o captura	Que el archivo es una imagen con ciertas características y metadatos	Que un mensaje consta en el dispositivo de origen, si se ha podido examinar	Quién tecleó realmente cada mensaje; que la cuenta pertenezca a una persona concreta

Prueba	Afirmable	Con reservas	No afirmable
Publicación en redes sociales o web	Qué muestra la copia conservada de la publicación (archivo o captura), con su hash y sus metadatos	Que la copia coincide con lo que había en línea en ese momento, solo si consta un acta o un sello de tiempo hecho al conservarla	Quién publicó el contenido; que lo publicado sea verdadero
Documento o PDF	Metadatos, estructura, versiones y posibles incoherencias de fechas o programas	La fecha real de creación, no solo a partir de los metadatos	Autoría de una firma manuscrita (grafoscopia); validez jurídica de la firma
Detector de IA	Qué probabilidad devolvió la herramienta, con su versión y la fecha	Como indicio para decidir si merece una pericial	Que algo sea o no sea sintético solo por su resultado (capítulo 12)

Tabla 6. Lo que un análisis técnico permite afirmar, afirmar con reservas o no afirmar, según el tipo de prueba.

Fuente: elaboración propia a partir de los capítulos 6 a 12.

Cómo redacta un buen informe. Un informe sólido se expresa con fórmulas como «se observa», «no se observa», «es compatible con» o «con este material no puede determinarse». Dice qué se comprobó, con qué método y con qué herramienta y versión, así como qué no pudo comprobarse. Y deja constancia de que la valoración de la prueba corresponde al juez o a la jueza.

BUENA PRÁCTICA TÉCNICA

Según Martínez Galindo (2022), la norma ISO/IEC 27037 pide que las herramientas forenses estén probadas y que se indique su margen de error. Una conclusión que indica su grado de certeza es una conclusión sólida; resiste el informe de otro perito u otra perito que la contradiga. Si un perito o una perito

> y otro perito u otra perito aplican el mismo método al mismo material, deberían llegar a lo mismo. Por eso el informe debe describir el método con suficiente detalle para repetirse (capítulo 17).

Blázquez Moreno (2023) recuerda una limitación más. Que un análisis concluya que un archivo no ha sido generado con IA no verifica que no haya sido manipulado con edición audiovisual convencional. Son dos preguntas distintas y conviene formularlas por separado.

QUÉ HACER

1. Antes de encargar, mira en la tabla qué se puede esperar de tu tipo de prueba.
2. Al recibir el informe, localiza qué conclusiones son afirmables y cuáles van con reservas.
3. Comprueba que las reservas coinciden con las limitaciones que el perito o la perito dice tener.
4. Busca las expresiones absolutas («es falso», «es auténtico») y pregunta en qué se apoyan.
5. Si necesitas una respuesta que el informe no da, pregunta si con otro material sería posible.
6. Valora qué peso puede tener cada conclusión.

ERRORES FRECUENTES

- Esperar una respuesta absoluta sobre autenticidad.
- Leer «no se observan indicios» como «es auténtico».
- Citar solo la conclusión que interesa y omitir las reservas.
- Aceptar un informe sin limitaciones.
- Pedir al perito o a la perito que opine sobre quién tiene razón.
- Tomar el resultado de un detector como una pericial.

MINI CHECKLIST

☐ Sé qué se puede afirmar de mi tipo de prueba.

☐ El informe separa lo afirmable de lo que va con reservas.

☐ No hay conclusiones absolutas sin apoyo.

☐ Las limitaciones están escritas.

☐ He valorado el peso de cada conclusión.

*Si tienes dudas, consúltame en **El perito responde** (ciberpering.com/el-perito-responde).*

PARTE VI

En el proceso

CAPÍTULO 19

Si aportas una prueba, si te la aportan

dos checklists e impugnación motivada frente a genérica

IDEA CLAVE

La prueba que aportas debe poder resistir una impugnación; la que te aportan debe cuestionarse con motivos técnicos concretos, no con una negación genérica.

Explicación. Hay dos posiciones, aportar la prueba o recibir la ajena. Una es el reverso de la otra. Quien aporta debe poder demostrar de dónde sale su prueba. Quien recibe una prueba ajena debe poder señalar qué le hace dudar.

Esa es la diferencia entre impugnar con motivos y sin ellos. Una impugnación genérica dice «se impugna la grabación sin más» o «podría ser una IA». No señala ningún indicio concreto y suele tener poco recorrido. Una impugnación motivada, en cambio, señala hechos comprobables. La tabla siguiente lo muestra con un ejemplo (tabla 7).

	Impugnación genérica	Impugnación motivada
Qué dice	«No se reconoce el audio»	«El archivo aportado es una copia recomprimida, sin metadatos de origen y con un cambio brusco del ruido de fondo en el minuto 1:12»
En qué se apoya	En la mera posibilidad de manipulación	En indicios técnicos o de contexto concretos

	Impugnación genérica	Impugnación motivada
Qué pide	Nada concreto	El original, el dispositivo, la grabación completa y, en su caso, una pericial

Tabla 7. Comparación entre una impugnación genérica y una impugnación motivada, con un ejemplo. Fuente: elaboración propia.

Que una impugnación sea genérica o motivada influye en el peso que le da el juez o la jueza. La doctrina penal lo dice igual para la cadena de custodia; Martínez Galindo (2022) sostiene que quien la cuestiona debe argumentarlo de forma suficiente y fundada, sin limitarse a una impugnación genérica. El momento, la forma y el contenido de la impugnación son decisiones procesales tuyas. Esta guía solo te ayuda a identificar los motivos técnicos.

Para ordenar el análisis de un archivo, propio o ajeno, la nota divulgativa de Fernández Advocats (citada en el capítulo 2) propone cinco preguntas: si se obtuvo lícitamente, si es auténtico, si está íntegro, si se ha conservado correctamente y si queda corroborado por el resto de la prueba. Advierte de que son problemas distintos; un archivo puede ser auténtico y haberse obtenido de forma ilícita, o ser lícito y estar incompleto. Un perito o una perito puede aportar datos sobre la autenticidad, la integridad y la conservación. La licitud y la corroboración son valoraciones jurídicas y probatorias que te corresponden a ti.

LO QUE DICE LA NORMA

Si se impugna la autenticidad de un documento privado, quien lo presentó puede pedir el cotejo pericial o proponer otra prueba útil (art. 326.2 LEC). Los medios de reproducción y los instrumentos de archivo se valoran con sana crítica (arts. 382.3 y 384.3 LEC). La mala fe procesal tiene consecuencias (art. 247 LEC).

BUENA PRÁCTICA TÉCNICA

Reúne los indicios técnicos antes de redactar. Un perito o una perito puede ayudarte a formularlos de manera comprobable.



Para ordenar el trabajo, usa el checklist que corresponda a tu situación, es decir, el A si eres tú quien aporta la prueba; el B, si te la aporta la otra parte.

CHECKLIST A. SI APORTAS UNA PRUEBA

- ☐ Conservo el original y el dispositivo.
- ☐ Hash SHA-256 calculado y anotado, con el nombre de quien lo calculó.
- ☐ Ficha de origen (quién, cómo, cuándo, con qué).
- ☐ Contenido completo, no solo el fragmento favorable.
- ☐ Fecha cierta o preservación valorada (sello de tiempo, acta u otra vía).
- ☐ Sé que se puede impugnar y he valorado una pericial preventiva.
- ☐ He comprobado que la obtención es lícita.
- ☐ Todo lo que aporto es auténtico y lo he comprobado.

CHECKLIST B. SI TE APORTAN UNA PRUEBA

- ☐ ¿Es el original o una copia? ¿Con qué hash?
- ☐ ¿Se aporta el dispositivo o solo el archivo?
- ☐ ¿Está completo o es un extracto?
- ☐ ¿Hay indicios técnicos concretos? Cortes, cambios de fondo, metadatos incoherentes, formato inesperado.
- ☐ ¿Hay indicios de contexto? Lugar, hora, personas, lenguaje.
- ☐ He anotado los indicios con marcas de tiempo o referencias.
- ☐ He decidido si pedir el original y una pericial.
- ☐ No niego sin motivo lo que puede ser auténtico.

QUÉ HACER

1. Elige el checklist que corresponda.
2. Complétalo antes de decidir nada.
3. Si a tu propia prueba le falta algo, complétala ya.
4. Si te aportan una prueba, apunta cada indicio de forma verificable.
5. Reúne los indicios por escrito y consulta con un perito o una perito si hay dudas técnicas.

ERRORES FRECUENTES

- Impugnar siempre, sin haber leído la prueba.
- Impugnar sin indicios y esperar que el juez o la jueza los busque.
- Aportar solo el fragmento favorable.
- Creer que, si la otra parte no impugna, la prueba es auténtica.
- Redactar la impugnación sin consultar el material original.

MINI CHECKLIST

☐ He completado el checklist A o el B, según mi caso.

☐ Cada indicio que señalo está anotado de forma verificable.

☐ He decidido si pedir el original y consultar a un perito o a una perito.

*Si tienes dudas, consúltame en **El perito responde** (ciberpering.com/el-perito-responde).*

CAPÍTULO 20

Asuntos habituales y la pericial que requieren

IDEA CLAVE

Estos son veintisiete asuntos con prueba digital, con la pericial que corresponde a cada uno y las evidencias que conviene tener a mano.

Explicación. Busca el asunto que se parezca al tuyo. Cada tarjeta indica qué perfil de perito o de perita hace falta, qué evidencias debes poder aportar y en qué capítulo se explica. Las evidencias son las que la guía defiende para ese tipo de prueba; el perito o la perita puede pedir más tras ver el material. Los asuntos de la última franja no tienen capítulo propio salvo que se indique. Para ellos la guía solo defiende lo común a toda prueba digital, que es conservar sin tocar el dispositivo o la cuenta y documentar quién ha tenido el material (capítulos 2 y 3). Un mismo asunto puede requerir más de un perfil (capítulo 17).

PERITO TECNOLÓGICO

1 Amenazas o reconocimiento de deuda por chat

PERICIAL

Pericial sobre el chat y su origen, con extracción del móvil.

EVIDENCIAS QUE DEBES APORTAR

El móvil con la conversación completa, sin borrar, con el número o la cuenta del contacto.

Cap. 8

2 Captura de pantalla que la otra parte dice que está trucada

PERICIAL

Comprobar si los mensajes constan en el dispositivo y si el archivo de la captura es coherente.

EVIDENCIAS QUE DEBES APORTAR

El archivo original de la imagen con sus metadatos y el móvil donde se recibió.

Cap. 8

3 Audio o nota de voz que podría estar editado

PERICIAL

Comprobar la integridad del archivo.

EVIDENCIAS QUE DEBES APORTAR

El archivo original, el dispositivo que lo grabó o lo recibió y el chat donde llegó.

Cap. 6

4 Llamada o reunión grabada

PERICIAL

Comprobar la integridad de la grabación y si hay saltos o cortes.

EVIDENCIAS QUE DEBES APORTAR

La grabación completa, no un fragmento, con los datos de quién grabó, con qué, dónde y cuándo.

Cap. 6

5 Vídeo de una cámara de seguridad reenviado por mensajería

PERICIAL

Comprobar la integridad del archivo y la coherencia de la hora.

EVIDENCIAS QUE DEBES APORTAR

El archivo de origen y no el reenviado, junto con el dispositivo que lo grabó.

Cap. 7

6 Foto con fecha y ubicación para acreditar presencia

PERICIAL

Comprobar la coherencia entre los metadatos y el archivo.

EVIDENCIAS QUE DEBES APORTAR

El archivo original con sus metadatos y el dispositivo que la tomó.

Cap. 7

7 Imagen o vídeo que podría ser un montaje

PERICIAL

Buscar indicios de manipulación y contrastar la escena con el lugar real.

EVIDENCIAS QUE DEBES APORTAR

El archivo original, la secuencia completa y fotografías del lugar real con fecha.

Cap. 7

8 Correo electrónico con fecha o contenido dudoso

PERICIAL

Analizar las cabeceras y los metadatos.

EVIDENCIAS QUE DEBES APORTAR

El correo original (.eml o .msg) y el acceso a la cuenta o al dispositivo donde está, no una impresión.

Cap. 9

9 PDF o contrato con metadatos incoherentes

PERICIAL

Analizar metadatos y estructura del archivo.

EVIDENCIAS QUE DEBES APORTAR

El archivo tal como se creó o se recibió, su hash calculado antes de abrirlo y la historia del documento.

Cap. 9

10 Documento con firma electrónica

PERICIAL

Validar la firma y comprobar el documento.

EVIDENCIAS QUE DEBES APORTAR

El archivo firmado original y el informe de validación.

Cap. 9

11 Sospecha de deepfake o de voz clonada

PERICIAL

Buscar indicios técnicos de síntesis, con las reservas del capítulo 12.

EVIDENCIAS QUE DEBES APORTAR

El archivo original, dónde y cómo apareció y, si es voz, muestras indubitadas.

Caps. 10 a 12

12 Informe de un detector de IA aportado como prueba

PERICIAL

Valorar el resultado y sus límites.

EVIDENCIAS QUE DEBES APORTAR

El informe, el archivo analizado, la herramienta con su versión y la fecha.

Cap. 12

13 Contenido de la deep web o de la dark web

PERICIAL

Preservar lo encontrado.

EVIDENCIAS QUE DEBES APORTAR

La dirección .onion, cómo llegó a tu cliente y quién se la facilitó.

Cap. 13

14 Operaciones con criptoactivos

PERICIAL

Explicar qué muestra la cadena de bloques y qué no.

EVIDENCIAS QUE DEBES APORTAR

Direcciones, TXID, fechas, importes y la plataforma o el monedero utilizado. Nunca claves privadas.

Cap. 14

OTRO PERFIL

15 ¿Es esta la voz de esta persona?

PERICIAL

Fonética forense.

EVIDENCIAS QUE DEBES APORTAR

La grabación original y muestras indubitadas de la voz.

Cap. 17

16 ¿Esta firma es de esta persona?

PERICIAL

Grafoscopia o documentoscopia.

EVIDENCIAS QUE DEBES APORTAR

El documento original en papel, sin reescanear, con muestras indubitadas de la misma época.

Caps. 9 y 17

DOS PERFILES

17 Audio de una amenaza

PERICIAL

Perito tecnológico para el origen y la integridad del audio. Fonética forense para la voz.

EVIDENCIAS QUE DEBES APORTAR

El original y el dispositivo, la grabación completa y muestras indubitadas de la voz.

Caps. 6 y 17

18 Documento en papel, escaneado, con firma y fecha dudosas

PERICIAL

Grafoscopia para la firma y perito tecnológico para el archivo.

EVIDENCIAS QUE DEBES APORTAR

El papel original, el archivo escaneado y muestras indubitadas de la misma época.

Caps. 9 y 17

OTROS ASUNTOS HABITUALES

19 Fuga de información, filtración o espionaje industrial

PERICIAL

Análisis forense de los equipos y las cuentas implicados.

EVIDENCIAS QUE DEBES APORTAR

Los equipos y las cuentas sin tocar y el registro de quién los ha tenido.

Caps. 2 y 3

20 Competencia desleal

PERICIAL

Análisis forense de los dispositivos implicados, con cadena de custodia.

EVIDENCIAS QUE DEBES APORTAR

Los dispositivos y las cuentas sin tocar y el registro de quién los ha tenido.

Caps. 2 y 3

21 Incumplimiento de un contrato de desarrollo o implantación de software

PERICIAL

Evaluar lo entregado frente a lo pactado en el contrato.

EVIDENCIAS QUE DEBES APORTAR

El contrato, la documentación del proyecto y lo entregado tal como se recibió.

Caps. 2 y 3

22 Uso indebido de los equipos de la empresa y despido

PERICIAL

Analizar la actividad que queda en los equipos.

EVIDENCIAS QUE DEBES APORTAR

Los equipos sin tocar. Consulta antes de acceder a nada, por la intimidad y el secreto de las comunicaciones.

Caps. 2 y 3

23 Reseñas falsas, publicaciones injuriosas o noticias falsas

PERICIAL

Preservar y analizar la publicación.

EVIDENCIAS QUE DEBES APORTAR

El enlace, la fecha, los comentarios y el dispositivo o la cuenta donde se vio, antes de que se borre.

Cap. 7

24 Suplantación de identidad en redes sociales

PERICIAL

Preservar y analizar el perfil falso y sus publicaciones.

EVIDENCIAS QUE DEBES APORTAR

El enlace del perfil, la fecha y el dispositivo donde se vio, antes de que se borre.

Cap. 7

25 Ciberacoso

PERICIAL

Preservar y analizar los mensajes y las publicaciones.

EVIDENCIAS QUE DEBES APORTAR

El dispositivo con las conversaciones completas, sin borrar, con el número o la cuenta de origen.

Cap. 8

26 Fraude del CEO o estafa por correo

PERICIAL

Analizar el correo y sus cabeceras.

EVIDENCIAS QUE DEBES APORTAR

El correo original con sus cabeceras y el acceso a la cuenta o al dispositivo donde está.

Cap. 9

27 Ciberataque o software malicioso en una empresa

PERICIAL

Análisis forense de los equipos y los registros afectados.

EVIDENCIAS QUE DEBES APORTAR

Los equipos y los registros afectados sin tocar y el registro de quién ha accedido a ellos.

Caps. 2 y 3

QUÉ HACER

1. Identifica a qué asunto se parece el tuyo.
2. Mira el perfil que le corresponde (tabla 5, capítulo 17).
3. Si tu asunto tiene varias preguntas con perfiles distintos, puede hacer falta más de un perito o una perita.
4. Si dudas, consulta antes de encargar nada (capítulo 15).

ERRORES FRECUENTES

- Encargar la pericial a un perfil que no responde a esa pregunta.
- Pedir una sola pericial para preguntas que requieren perfiles distintos.
- Pedir que «autentique» una prueba sin decir qué hay que comprobar.

MINI CHECKLIST

☐ Sé a qué asunto se parece el mío.

☐ Sé qué perfil necesito.

☐ He separado las preguntas que requieren perfiles distintos.

*Si tienes dudas, consúltame en **El perito responde** (ciberpering.com/el-perito-responde).*

Anexos

ANEXO **A**

Checklist

Para cualquier prueba digital que te llegue, antes de que nadie la toque

- ☐ Tengo claro si es audio, vídeo, fotografía, documento, chat, publicación en redes sociales o publicación web.
- ☐ Sé dónde está el original y en qué dispositivo o cuenta.
- ☐ Nadie ha borrado, reenviado, recortado, editado ni actualizado nada, o consta lo que se hizo.
- ☐ Se ha calculado el hash SHA-256 del original y consta con fecha y hora.
- ☐ Hay una copia sin modificar y se trabaja solo con ella.
- ☐ Hay una ficha de origen (quién, cuándo, dónde, con qué y cómo llegó a tu cliente).
- ☐ Tengo el contenido completo y su contexto, no solo un fragmento.
- ☐ Sé quién puede confirmar el momento, el lugar y la identidad.
- ☐ He identificado lo que puede desaparecer y he decidido cómo preservarlo.
- ☐ Hay anotado lo que llama la atención, con marcas de tiempo, sin sacar conclusiones.
- ☐ He decidido si hay que preservarlo, aportarlo o consultar a un perito o a una perito.

ANEXO B

Glosario

Término	Significado
Autenticidad	Que el contenido procede de quien se dice y de la fuente que se dice
Blockchain (cadena de bloques)	Registro de transacciones compartido, formado por bloques enlazados con hashes
Bloqueador de escritura	Dispositivo que impide modificar el soporte original al copiarlo
C2PA	Coalición y formato técnico para incrustar en los archivos metadatos firmados sobre su origen y sus ediciones
Cadena de custodia	Registro documentado de quién ha manejado el material, cuándo y para qué
Cheapfake	Alteración sencilla, sin IA, como cortes, cambios de velocidad, descontextualización
Clave privada	Dato secreto que permite autorizar transferencias de criptoactivos
Códec	Programa o formato que comprime y descomprime audio o vídeo
Colisión	Par de archivos distintos que producen el mismo hash
Contenedor	Archivo que agrupa audio, vídeo y datos con su estructura (por ejemplo, MP4 u OGG)
Copia forense	Copia bit a bit de un soporte, con comprobación por hash de que coincide con el original

Término	Significado
Cotejo	Comprobación de que una copia o una impresión coincide con el original
Credenciales de contenido	Metadatos firmados (C2PA) que indican qué dispositivo o programa produjo un archivo y qué ediciones sufrió
Criptoactivo	Representación digital de un valor o un derecho que puede transferirse y almacenarse electrónicamente mediante tecnología de registro distribuido
Dark web	Capa de internet a la que se accede con herramientas específicas como Tor, con direcciones .onion
Deepfake (ultrasuplantación)	Contenido de audio, imagen o vídeo generado o alterado con IA que parece auténtico
Deep web	Contenidos de internet a los que no llegan los buscadores habituales; no es ilegal por sí misma
ELA	Análisis del nivel de error de una imagen para detectar zonas con compresión distinta
ENF	Frecuencia de la red eléctrica que puede quedar registrada en una grabación
Espectrograma	Imagen del sonido con tiempo, frecuencia e intensidad
Extracción forense	Obtención de datos de un dispositivo con métodos que preservan su integridad
Fonética forense	Disciplina que compara voces y analiza el habla con fines periciales
Hash	Código calculado a partir del contenido de un archivo; cambia si el archivo cambia
Integridad	Que el archivo no ha cambiado desde un momento dado
Marca de agua	Señal incrustada en un contenido para identificar su origen
MD5	Algoritmo de hash de 128 bits (32 caracteres hexadecimales)

Término	Significado
Metadatos	Datos sobre el archivo, como fechas, dispositivo, programa, ubicación
Monedero (wallet)	Programa o dispositivo que gestiona las claves de quien controla unos criptoactivos
PRNU	Patrón de ruido propio de cada sensor de cámara
Sello de tiempo cualificado	Servicio de confianza que certifica que unos datos existían en una fecha y hora
SHA-1	Algoritmo de hash de 160 bits (40 caracteres hexadecimales)
SHA-256	Algoritmo de hash de la familia SHA-2, que genera un código de 64 caracteres hexadecimales
SHA-512	Algoritmo de hash de la familia SHA-2, que genera un código de 128 caracteres hexadecimales
SynthID	Marca de agua invisible que Google incorpora en contenido generado con sus modelos
Testigo online	Tercero de confianza privado que captura un contenido en línea y entrega un justificante con fecha y hora
Tor	Red y navegador que protegen la ubicación de quien navega y de los servicios con direcciones .onion
TXID	Identificador de una transacción, que es un hash de 64 caracteres hexadecimales en Bitcoin
Veracidad	Que lo que muestra el contenido ocurrió realmente

Tabla 8. Términos técnicos y jurídicos usados en la guía y su significado. Fuente: elaboración propia.

ANEXO C

Enlaces útiles

- BOE: legislación consolidada (LEC, LOPJ, Código Penal, Ley 6/2020).
- Consejo General del Poder Judicial: acceso al buscador de jurisprudencia CENDOJ (buscador).
- EUR-Lex: Reglamentos (UE) 910/2014 y 2024/1689.
- Agencia Española de Protección de Datos: RGPD y LOPDGDD.
- UNE e ISO: catálogo de normas técnicas (UNE 71506, UNE 197001, ISO/IEC 27037).
- RFC 3227: directrices para recoger y archivar evidencias.
- NIST SP 800-86: técnicas forenses en la respuesta a incidentes.
- SWGDE: guías de buenas prácticas en evidencia digital, audio y vídeo.
- Herramientas citadas en los capítulos 3 y 6 como ejemplo: Audacity, Clonezilla, UFED (Cellebrite), Magnet AXIOM, Autopsy, FTK Imager (Exterro), Guymager y dd (GNU coreutils).
- Fuentes de hash y copia forense (capítulos 3 y 4): FIPS 180-4 (NIST), RFC 1321, RFC 6151, NIST retira SHA-1, Joux (2004), «Multicollisions in Iterated Hash Functions» y Disk Imaging Tool Specification (NIST CFTT).
- Criptoactivos (capítulo 14): Reglamento (UE) 2023/1114 (MiCA), CNMV: regulación de criptoactivos, Banco de España: cierre del registro de proveedores, ESAs: ficha sobre criptoactivos, Reglamento (UE) 2023/1113, Bitcoin Developer Guide: wallets y Blockstream: TXID.

- Safe Stamper (y su artículo sobre cómo grabar y certificar una conversación de WhatsApp) y eGarante: páginas de los servicios citados en el capítulo 5 como ejemplo.
- Criptoactivos (capítulo 14): documentación para desarrolladores de Bitcoin (transacciones y TXID), Bitcoin Wiki, «Block timestamp», Meiklejohn y otros, «A Fistful of Bitcoins», Möser y Narayanan, «Resurrecting Address Clustering in Bitcoin» y Kappos y otros, USENIX Security 2022.
- INCIBE: artículo sobre testigos online para recoger pruebas digitales (capítulo 5).
- Deep web y dark web (capítulo 13): INCIBE, «Deep web y dark web: descubre qué son y en qué se diferencian», INCIBE, «Navegadores y deep web: profundicemos en el tema», Proyecto Tor, servicios onion y Europol, sala de prensa.
- Inteligencia artificial (capítulo 11): C2PA, especificación 2.2, Google DeepMind, SynthID, ElevenLabs, clonado instantáneo de voz, ElevenLabs, clonado profesional de voz, South China Morning Post sobre Arup y Fortune sobre Arup.
- Correo electrónico (capítulo 9): RFC 5322, RFC 7208, RFC 6376 y RFC 9989.
- Extracción en móviles (capítulo 3): NIST SP 800-101 Rev. 1, guía de forense de dispositivos móviles.
- Imagen y ubicación (capítulo 7): Krawetz, N. (2007), «A Picture's Worth», ayuda de Google Earth, imágenes históricas en Google Earth, ayuda de Street View y etiquetas GPS de ExifTool.
- Blázquez Moreno, R. (2023). «Deepfakes en el procedimiento probatorio». *Revista Vasca de Derecho Procesal y Arbitraje*, 3 (Premios IVADP, XIII ed.).
- Chesney, R. y Citron, D. (2019). «Deep Fakes: A Looming Challenge for Privacy, Democracy, and National Security». *California Law Review*, 107, p. 1753.
- Delgado Martín, J. *Kit avanzado para la obtención y práctica de la prueba digital* (colección Temas; extracto consultado).

- Fernández Advocats. «La prueba digital en el proceso penal» (nota divulgativa, sin fecha).
- Martínez Galindo, G. (2022). «Problemática jurídica de la prueba digital y sus implicaciones en los principios penales». *Revista Electrónica de Ciencia Penal y Criminología*, 24-23, pp. 1-38.
- El perito responde (Ciberpering): servicio gratuito de consulta.

ANEXO D

Preguntas frecuentes

¿Puede mi cliente grabar una conversación en la que participa? Es una cuestión jurídica que depende de las circunstancias y que tienes que valorar (art. 18 CE y art. 197 CP).

¿Sirve una captura de pantalla? Puede aportarse, pero si se impugna necesitará refuerzo, como el dispositivo, la conversación completa, una extracción o el cotejo con el móvil de la otra persona (capítulo 8).

¿Basta un acta notarial? Deja constancia de lo que se exhibió ante la notaría. No prueba por sí sola que el contenido sea auténtico (capítulo 5).

¿Puedo usar un detector de IA gratuito? Como orientación, con cautelas de privacidad y sobre una copia. No como prueba (capítulo 12).

¿Qué pasa si el original ya no existe? Hay que documentar lo que sí existe y cómo se perdió. Un perito o una perito puede indicar qué se puede y qué no se puede comprobar con lo que queda. La estrategia es tuya.

¿Alguien puede decir «es una IA» para librarse de una prueba? Puede alegarlo. Una alegación genérica no analiza el archivo concreto. Lo que se examina son los indicios técnicos, tarea propia de la pericial.

¿Cuánto tarda una pericial? Depende del material y del alcance. Pide un plazo estimado tras ver los archivos (capítulo 15).

¿Una respuesta de El perito responde es un dictamen? No. Es una orientación técnica gratuita sobre tu consulta, con respuesta en 48 horas laborables.

ANEXO E

Plantillas de trabajo

Cinco hojas para imprimir o copiar. Rellénalas con bolígrafo o en un documento; guárdalas junto al material.

Ficha de origen

Formulario E1 Expediente n.º _____ Fecha _____

1. Descripción del archivo

○ Audio ○ Vídeo ○ Fotografía

○ Documento ○ Chat ○ Publicación en redes sociales o web

Nombre del archivo

_____

2. Quién lo creó o lo grabó

Nombre y relación con el asunto

_____

3. Con qué dispositivo y aplicación

Marca, modelo y aplicación, con versión si se conoce

_____

4. Dónde y cuándo

Lugar, fecha y hora, indicando si son aproximadas

5. Cómo llegó a quien lo aporta

Medio, cuenta de origen, fecha y hora de recepción

6. Dónde está el original

Dispositivo, tarjeta, nube o ubicación

7. Quién ha tenido acceso

Personas y fechas

8. Hash SHA-256 del original

Valor completo, fecha, hora y herramienta con versión

9. Qué se pretende acreditar

Una frase

10. Observaciones

Lo que llama la atención, con marcas de tiempo, sin conclusiones

Tabla 9. Campos de la ficha de origen de una prueba digital, plantilla E1. Fuente: elaboración propia.

Registro de custodia

Formulario E2 Expediente n.º _____ Fecha _____

Registro 1

Fecha y hora | *Quién* | *Qué hizo*

Con qué finalidad | *Hash antes y después*

Registro 2

Fecha y hora | *Quién* | *Qué hizo*

Con qué finalidad | *Hash antes y después*

Registro 3

Fecha y hora | *Quién* | *Qué hizo*

Con qué finalidad | *Hash antes y después*

Registro 4

Fecha y hora | *Quién* | *Qué hizo*

Con qué finalidad | *Hash antes y después*

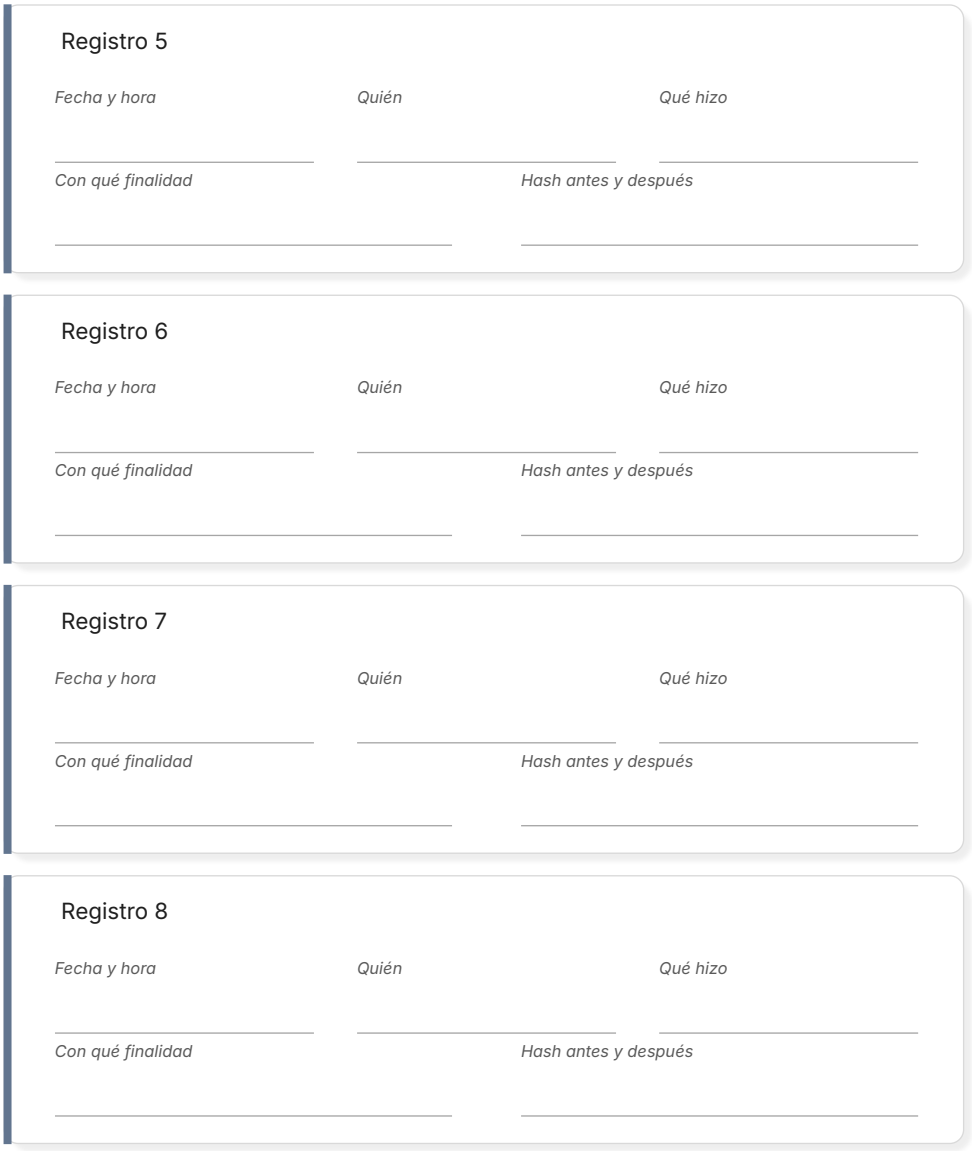

Tabla 10. Campos del registro de custodia, plantilla E2. Fuente: elaboración propia.

Una línea por cada vez que el material cambia de manos, se copia, se abre o se traslada. Nada de abreviaturas que otra persona no entienda.

Justificante de recepción de material

Formulario E3 Expediente n.º _____ Fecha _____

1. Quien entrega

Nombre y relación con el asunto

_____

2. Quien recibe

Nombre y cargo

_____

3. Fecha y hora de entrega

Fecha *Hora*

_____ _____

4. Material entregado

Descripción de cada elemento, con su hash

_____

_____

5. Estado del material

Observaciones sobre el soporte, la carga o daños visibles

_____

_____

6. Forma de entrega

○ En mano ○ Por mensajería certificada ○ Por enlace con clave

7. Compromiso de custodia

Dónde se guarda y quién tiene acceso

8. Firmas

De quien entrega *De quien recibe*

Tabla 11. Campos del justificante de recepción de material, plantilla E3. Fuente: elaboración propia.

Hoja de encargo pericial

Formulario E4 Expediente n.º _____ Fecha _____

1. Quién encarga

Nombre y datos de contacto

_____

2. Asunto

Identificación del asunto, sin datos que no sean necesarios

_____

3. Pregunta o preguntas

Una por cada comprobación (capítulo 16)

_____

_____

4. Material que se entrega

Lista con hash (E3)

_____

_____

5. Alcance

Qué se analizará y qué queda fuera

_____

_____

6. Entregable

○ Informe ○ Dictamen ○ Orientación escrita

7. Plazo estimado

Tras ver el material, no antes

8. Presupuesto

Por escrito, con el alcance definido

9. Ratificación

Si se prevé y en qué condiciones

10. Confidencialidad

Quién puede ver el material y el informe

Tabla 12. Campos de la hoja de encargo pericial, plantilla E4. Fuente: elaboración propia.

Lista para leer un informe pericial recibido

Formulario E5 Expediente n.º _____ Fecha _____

Criterios

	Sí	No
El objeto coincide con la pregunta que se hizo.	○	○
Indica el material recibido, con hash.	○	○
Describe el método y las herramientas, con versión.	○	○
Separa los resultados de las conclusiones.	○	○
Cada conclusión indica su grado de certeza (capítulo 18).	○	○
Recoge las limitaciones.	○	○
No usa «es falso» ni «es auténtico» sin apoyo.	○	○
Una persona con la misma formación podría repetir el análisis.	○	○
Tiene estructura reconocible (capítulo 17).	○	○

ANEXO F

Guion de la primera consulta con un perito o una perito

Para llevar escrito antes de la llamada o de rellenar el formulario de El perito responde.

1. **Qué tengo.** Tipo de prueba y cuántos archivos hay.
2. **De dónde viene.** Quién lo creó, con qué dispositivo y cómo llegó a mí.
3. **Dónde está el original.** Y si ha pasado por mensajería o redes.
4. **Qué he hecho con él.** Si lo he abierto, copiado, reenviado o editado.
5. **Qué necesito comprobar.** En una frase y sin adjetivos.
6. **Qué quiero acreditar.** Qué hecho quiero probar con el resultado.
7. **Qué plazos hay.** Fecha de vista, de juicio o de un trámite.
8. **Qué puede desaparecer.** Mensajes temporales, nube, un dispositivo que se va a cambiar.

PREGUNTAS QUE CONVIENE HACER AL PERITO O A LA PERITO

- ¿Qué puede comprobarse con este material y qué no?
- ¿Necesita el original o el dispositivo?
- ¿Cuál sería el alcance y el entregable?
- ¿Qué plazo estimado y qué presupuesto, una vez visto el material?
- ¿Podrá ratificar el informe si se pide?
- ¿Qué método y qué herramientas usará?