BIBLIOTECA
ACCCF

05
VOLUMEN

ACCCF / CONOCIMIENTO APLICADO

Manual de peritaje de celulares y mensajería instantánea

Recepción, aislamiento, adquisición, análisis, contexto y atribución responsable

Examinar comunicaciones móviles sin confundir una captura con la fuente, una extracción con una adquisición completa ni una cuenta con la persona que la utilizó.

Coordinación editorial · Jocsan Laguna

Consejo Americano de Ciberseguridad y Cómputo Forense · 2026

Guía técnica general. Ejemplos y cifras de demostración son ficticios.

Contenido

Índice navegable. Los títulos enlazan a su ubicación dentro del documento.

Presentación: el teléfono no habla por sí solo . . . 4

Capítulo 1. Recepción y estado del dispositivo . . . 4

1.1 Acta que otra persona pueda reconstruir . . . 4

1.2 Riesgos de pérdida y de alteración . . . 5

Capítulo 2. Fuentes por capa . . . 5

2.1 Dispositivo, aplicación y datos asociados . . . 5

2.2 Cuenta, sesiones y dispositivos vinculados . . . 5

2.3 Proveedor y otros participantes . . . 6

Capítulo 3. Aislamiento, alimentación y traslado . . . 6

3.1 Aislamiento real y comprobado . . . 7

3.2 Embalaje, traslado y custodia . . . 7

Capítulo 4. Métodos de adquisición . . . 7

4.1 Documentación manual y captura . . . 7

4.2 Exportación de aplicación y copia de seguridad . . . 8

4.3 Extracción lógica, avanzada y proveedor . . . 8

4.4 Validación de herramienta y de salida . . . 8

Capítulo 5. Examen de conversaciones y contenido . . . 9

5.1 Reconstruir el hilo, no solo la frase . . . 9

5.2 Mensajes editados, eliminados y reenviados . . . 9

5.3 Adjuntos, miniaturas y metadatos . . . 10

Capítulo 6. Atribución y comunicación . . . 10

6.1 Cuenta, dispositivo y persona . . . 10

6.2 Cronología y corroboración . . . 11

6.3 Informe con alcance explícito . . . 11

Anexo A. Formatos operativos . . . 12

A.1 Recepción del dispositivo . . . 12

A.2 Inventario de cuentas y fuentes 12

A.3 Registro de adquisición 13

A.4 Matriz de atribución 13

Anexo B. Marco jurídico y control final 13

Presentación: el teléfono no habla por sí solo

Un celular contiene conversaciones, archivos, sensores, cuentas y restos de actividad, pero también puede ser solo una ventana hacia una nube o hacia otros participantes. La primera pregunta no es qué programa lo abrirá, sino qué afirmación necesita probarse y qué fuentes pueden responderla. Si el objetivo es saber quién escribió un mensaje, una fotografía de la pantalla no basta: se necesitan sesiones, dispositivos, factores, contenido y contexto.

El análisis móvil cambia con el sistema, la aplicación, la versión, el cifrado y el estado del equipo. Una extracción puede obtener bases de datos accesibles; otra puede limitarse a archivos visibles o a una exportación. La palabra “forense” no modifica la cobertura real. El informe debe indicar qué se hizo, qué se obtuvo y qué quedó fuera, sin prometer recuperación de mensajes borrados ni acceso universal.

NIST SP 800-101 Rev. 1 organiza preservación, adquisición, examen, análisis y reporte de dispositivos móviles, con atención a validación y documentación. Es una guía de método, no una lista actualizada de capacidades de cada herramienta. Esas capacidades se comprueban en el modelo y la versión concretos, con datos de prueba y resultados verificables.[1]

> **Primera regla**
>
> No encender, explorar, restablecer ni conectar por curiosidad. Registra el estado y la autoridad, preserva accesorios y decide qué información puede desaparecer antes de cambiar cualquier cosa.

Capítulo 1. Recepción y estado del dispositivo

1.1 Acta que otra persona pueda reconstruir

El acta describe tipo, marca, modelo, identificadores visibles, estado físico, encendido, bloqueo, batería, red visible, fecha y zona, personas, accesorios y acciones previas. No se anota una contraseña en el acta general. Si existe una autorización de desbloqueo, se registra su existencia y el mecanismo seguro para disponer de ella. Las etiquetas anteriores se conservan y se relacionan con el nuevo identificador.

La pantalla visible se fotografía sin interactuar cuando es posible: hora, iconos de red, batería, notificaciones y estado. La fotografía demuestra cómo se encontraba en ese instante, no todo el contenido. Si alguien ya abrió aplicaciones o intentó una extracción, se registra. La recepción imperfecta se documenta; no se reescribe como si el objeto hubiera llegado intacto.

Campo	Ejemplo ficticio	Decisión que facilita
Dispositivo	Teléfono DEMO-MBL-003, modelo y serie visibles.	Identificar y comparar con actas.
Estado	Encendido, bloqueado, 43 %, red móvil visible.	Priorizar preservación y aislamiento.
Accesorios	Cable, cargador, SIM y funda etiquetados por separado.	Conservar rutas de acceso y contexto.
Historia declarada	Titular intentó exportar una conversación antes de entregar.	Separar acciones previas del análisis.

Campo	Ejemplo ficticio	Decisión que facilita
Autoridad	Revisión de una conversación y cuentas especificadas.	Limitar acceso a terceros y otras aplicaciones.
Decisión	Preservar estado y contactar especialista.	Evitar cambios no autorizados.

1.2 Riesgos de pérdida y de alteración

Un equipo puede recibir mensajes, sincronizar, borrar remotamente, bloquear por inactividad o perder batería. También puede contener sesiones y claves que se pierden al apagar. Se identifica qué riesgo es más urgente y qué conocimiento técnico existe para enfrentarlo. Apagar no es siempre preservar; mantener encendido no es siempre analizar. El registro debe explicar la opción elegida.

Si la prioridad es una conversación disponible en otro participante o en el proveedor, puede ser menos intrusivo solicitar esa fuente antes que intervenir el dispositivo. Si la prioridad es actividad volátil o una clave de cifrado, puede ser necesaria una adquisición en vivo autorizada. La navaja de Ockham selecciona la fuente con mejor capacidad discriminatoria y menor alteración, no la herramienta más sofisticada.

Cuándo detenerse

Falta de autoridad, riesgo de borrado, herramienta no validada, cifrado no comprendido o peligro para una persona exigen pausar y escalar. Explorar para ver qué aparece puede cambiar la evidencia y ampliar el alcance sin permiso.

Capítulo 2. Fuentes por capa

2.1 Dispositivo, aplicación y datos asociados

La memoria del dispositivo puede contener bases de aplicaciones, archivos, miniaturas, registros, credenciales protegidas, cachés y datos de sensores. Su disponibilidad depende del estado y el acceso. Una carpeta de imágenes no equivale a toda la fototeca si existe sincronización. Un mensaje eliminado localmente puede seguir en otro participante o en una copia, y también puede ser irrecuperable. El análisis no garantiza ninguno de los dos extremos.

Los accesorios importan: SIM o eSIM, memoria, cargador, cables, adaptadores, funda, documentación y otros dispositivos sincronizados. Un reloj, una tableta o una computadora puede contener notificaciones o sesiones con información distinta. Se inventarían sin ampliar automáticamente la autoridad: que un objeto esté conectado no significa que todo su contenido esté dentro del encargo.

2.2 Cuenta, sesiones y dispositivos vinculados

La aplicación puede permitir varias sesiones, clientes de escritorio, respaldos, recuperación por correo o por operador. Se solicita lista de dispositivos vinculados, altas y bajas, factores, fechas, cambios de recuperación y actividad de sesiones cuando esté disponible. El nombre de la cuenta describe una asociación lógica; la identidad física necesita más elementos.

Una dirección IP puede aportar una pista de red, pero no domicilio ni persona. Un número de teléfono puede estar reciclado o asociado a otra persona durante el período. Un IMEI identifica un equipo o

configuración en su contexto, no necesariamente al portador. La atribución se construye con convergencia y alternativas: préstamo, uso compartido, acceso remoto, robo de sesión o administración por otra persona.

2.3 Proveedor y otros participantes

El proveedor puede conservar metadatos, registros de conexión o información de cuenta sin conservar contenido cifrado. Otros participantes pueden tener el mensaje con una representación distinta y adjuntos originales. La solicitud identifica cuenta, período, campos, formato nativo, zona y proceso. No se promete que una plataforma entregará contenido solo porque se le pida; se registra su capacidad y su respuesta.

En México, la Ley en Materia de Telecomunicaciones y Radiodifusión de 2025 contiene reglas de conservación y entrega de datos para sus destinatarios y autoridades. El análisis debe comprobar si la solicitud se encuentra dentro de ese régimen y si el registro es de telecomunicaciones, de una aplicación o de otro proveedor. No se trata una plataforma de mensajería como si toda su información fuera una sábana telefónica.[2]

Fuente independiente

Una captura y una impresión de esa captura no son dos pruebas independientes. Un mensaje recibido por otra persona, una exportación de aplicación y un registro de sesión pueden tener orígenes y errores distintos.



Figura 1. El teléfono es una capa, no todo el caso. Una conversación puede existir en objetos distintos Reconstrucción editorial; no constituye evidencia real.

Capítulo 3. Aislamiento, alimentación y traslado

3.1 Aislamiento real y comprobado

El aislamiento busca controlar cambios remotos y nuevas comunicaciones. Se evalúa celular, Wi-Fi, Bluetooth, NFC, cables y sincronización. Activar modo avión requiere tocar el dispositivo y puede modificar registros; apagar puede perder sesiones; un contenedor de aislamiento puede ser ineficaz si no se valida o si el equipo intenta reconectar. Se documenta qué se hizo y qué efecto tuvo.

Una bolsa antiestática protege de descargas, no necesariamente de radiofrecuencia. Llamarla Faraday no cambia su función. La solución de aislamiento debe probarse con métodos seguros y en condiciones similares: tipos de señal, cierre, materiales, distancia y estado del dispositivo. La comprobación no consiste en hacer una llamada al número de una persona sin autorización; se utiliza equipo de prueba.

Opción	Riesgo principal	Registro necesario
Modo avión	Interacción, cambios de registro y conexiones restantes.	Pantalla, acciones, hora y conexiones verificadas.
Apagar	Pérdida de memoria, sesión o acceso por cifrado.	Justificación, estado y capacidad de adquisición.
Contenedor RF	Aislamiento insuficiente o no validado.	Prueba, cierre, materiales y condiciones.
Mantener conectado	Sincronización, mensajes o borrado remoto.	Necesidad, control y observación.
Alimentación	Calor, actividad o alteración de estado.	Cargador, cable y propósito documentados.

3.2 Embalaje, traslado y custodia

El embalaje se elige por función física y lógica: protege de golpes, electricidad estática, humedad y acceso, y conserva la decisión de aislamiento adoptada. Los accesorios se embalan y relacionan. El sello incluye identificador, fecha y responsable; cada apertura o cambio se documenta. No se transporta un equipo activo sin control de batería y conectividad cuando eso puede cambiar datos.

La cadena registra quién entrega, quién recibe, para qué, dónde, en qué estado y con qué verificación. En una transferencia electrónica se registran permisos, canal, versión, descarga y hash del objeto correspondiente. Si se comparte la extracción con un revisor, se entrega una copia controlada y se restringen datos de terceros fuera del alcance.

> **Regla práctica**
>
> El embalaje no repara una mala decisión, pero evita nuevas alteraciones. El sello tampoco demuestra que el contenido sea verdadero: demuestra una condición de cierre dentro de una secuencia documentada.

Capítulo 4. Métodos de adquisición

4.1 Documentación manual y captura

La revisión manual puede ser útil cuando la pregunta se limita a una conversación o cuando otras fuentes no están disponibles. Se registra aplicación, versión, dispositivo, fecha y zona, operador, recorrido y contenido mostrado. La grabación de pantalla aporta continuidad visual, pero sigue siendo una selección de lo que la interfaz permite ver. No demuestra la totalidad de la base ni los eventos no visibles.

Antes de capturar se define el alcance y se evita exponer otros chats, fotos o notificaciones. Si se produce una exportación desde la aplicación, se conservan formato, filtros, adjuntos, nombre original y fecha. El archivo se calcula como objeto nuevo y se relaciona con el dispositivo. No se renombra la fuente antes de preservarla.

4.2 Exportación de aplicación y copia de seguridad

La exportación de chat puede incluir texto y adjuntos con una estructura elegida por la aplicación. Debe comprobarse si incluye mensajes editados, eliminados, reacciones, citas, respuestas o referencias, y cómo representa fechas y participantes. Una copia de seguridad puede contener una instantánea distinta y estar cifrada con una clave separada. Se registra la capacidad disponible sin afirmar equivalencia con una extracción física.

Cuando el objetivo es preservar la conversación, se complementa la exportación con captura del contexto y con fuentes de otros participantes. Cuando el objetivo es analizar eventos no incluidos, se evalúa una extracción autorizada. Una diferencia entre exportaciones puede deberse a filtros o versiones, no automáticamente a manipulación. Ambos objetos se conservan con identificadores relacionados.

4.3 Extracción lógica, avanzada y proveedor

La extracción lógica obtiene archivos o bases accesibles mediante herramienta compatible. Una adquisición avanzada puede tener mayor cobertura cuando el dispositivo y el método lo permiten, pero exige capacitación, autoridad y validación. El informe debe evitar la etiqueta genérica “extracción total” si solo cubrió particiones o aplicaciones determinadas. Los errores, objetos no descifrados y exclusiones se conservan.

La adquisición por proveedor puede ofrecer información de cuenta o registros que no están en el teléfono. Se solicitan campos, zona, formato nativo, proceso y diccionario. El archivo recibido se relaciona con el EML y la declaración de integridad cuando exista. El proveedor puede no tener contenido cifrado o puede aplicar otra retención; la respuesta no se presenta como una sábana telefónica universal.[34]

4.4 Validación de herramienta y de salida

Se utiliza un dispositivo o conjunto ficticio con datos conocidos para comprobar que la herramienta produce los objetos esperados, interpreta fechas, participantes y adjuntos, y no modifica la fuente fuera de lo documentado. Se registra nombre, versión, entorno, licencia, configuración y resultado. Una actualización puede cambiar el comportamiento y exige nueva validación.

La salida debe abrirse y compararse con una fuente visible seleccionada: una conversación de control, un archivo, una fecha o una secuencia. Los objetos no decodificados se marcan, no se ocultan. Si una segunda herramienta produce otra representación, se documenta la diferencia y se evalúa cuál responde mejor a la pregunta. La herramienta no se convierte en testigo; es un componente del método.

Criterio de aceptación

Una adquisición termina cuando la salida puede abrirse, relacionarse con el dispositivo, describir su cobertura, conservar incidencias y permitir una revisión compatible. No termina cuando el programa muestra “100 %”.

Captura, exportación y extracción no son sinónimos ACCCF · RECONSTRUCCIÓN EDITORIAL · DATOS FICTICIOS

La elección depende de la pregunta y de la cobertura

Método	Cobertura posible	Límite que se declara
Captura manual	Lo que la interfaz permite ver.	Selección humana y ausencia de estructura.
Exportación de app	Conversación elegida y adjuntos según función.	Filtros, formato y eventos no incluidos.
Extracción lógica	Archivos y bases accesibles por la herramienta.	Cifrado, compatibilidad y permisos.
Extracción avanzada	Mayor cobertura si está soportada y autorizada.	No prometer recuperación ni acceso universal.

La figura explica decisiones y relaciones; no representa evidencia de un caso real.

Figura 2. Captura, exportación y extracción no son sinónimos. La elección depende de la pregunta y de la cobertura Reconstrucción editorial; no constituye evidencia real.

Capítulo 5. Examen de conversaciones y contenido

5.1 Reconstruir el hilo, no solo la frase

Se analizan participantes, identificadores, mensajes citados, respuestas, adjuntos, reacciones, edición, eliminación, fecha de envío, recepción y lectura cuando la fuente los contiene. Una captura puede ocultar el mensaje al que se respondía. La secuencia se documenta con identificadores de la fuente, no con una numeración inventada que sugiera una continuidad no probada.

La conversación se compara con el contexto: llamadas, archivos, contactos, actividad de aplicación, ubicación aproximada, correo y testimonios. La interpretación de una frase requiere lengua, relación, eventos y secuencia. Un “sí” puede responder una pregunta distinta si se pierde el mensaje citado. El análisis no debe completar el sentido con imaginación.

5.2 Mensajes editados, eliminados y reenviados

Una etiqueta “editado” indica una condición visible, no qué contenido tenía antes. La etiqueta “eliminado” no demuestra que todos los rastros hayan desaparecido ni que el motivo fuera ocultar. Un reenvío puede añadir una capa de origen distinta. Se revisan registros disponibles, copias, otros participantes y respaldos, sin prometer que se recuperará el texto anterior.

Observación	Qué puede significar	Qué se necesita para concluir más
Editado	Cambio posterior en la aplicación.	Versiones, registros o participantes con contenido anterior.
Eliminado para todos	Visualización de eliminación en el cliente.	Cobertura de la eliminación y copias disponibles.
Reenviado	Contenido transmitido desde otro mensaje.	Origen y fecha inicial si están disponibles.
Sin archivo adjunto	Adjunto no descargado, expirado o no incluido.	Registro, enlace, otro participante o copia.
Hora distinta	Zona, reloj, conversión o edición.	Valor literal y configuración de la fuente.

5.3 Adjuntos, miniaturas y metadatos

El archivo adjunto se preserva por separado y se relaciona con el mensaje. Su miniatura puede corresponder a una versión distinta; su nombre puede cambiar al descargarlo. Se revisan metadatos internos, contenido, tamaño, formato y fecha del sistema, sin convertir esos campos en prueba automática de origen. La copia en otro participante puede conservar mejor calidad o información adicional.

Un documento, una imagen o un audio puede requerir análisis específico de originalidad y contenido. El peritaje móvil demuestra que el archivo se encontró asociado a un mensaje o carpeta, no que su escena sea verdadera ni que su autor sea el remitente. Esa separación evita que una buena adquisición se utilice para justificar una conclusión excesiva sobre el contenido.

Caso ficticio

Una conversación contiene una amenaza seguida de un mensaje eliminado. Otro participante conserva el mensaje posterior, que era una aclaración enviada por el mismo autor. La defensa y la acusación deben analizar ambos. La recuperación del contexto no prueba inocencia ni culpabilidad; evita interpretar una frase aislada como si fuera toda la comunicación.

Capítulo 6. Atribución y comunicación

6.1 Cuenta, dispositivo y persona

La atribución se organiza en preguntas: qué cuenta produjo o recibió el mensaje, qué dispositivo tenía la sesión, quién podía desbloquearlo, quién controlaba los factores, qué otra persona tenía acceso y qué actividad muestra la secuencia. La titularidad contractual de una línea puede aportar contexto, pero no prueba por sí sola el uso en el momento.

Se consideran préstamo, uso compartido, delegación, robo de credenciales, sesión persistente, acceso remoto y administración por terceros. La defensa no necesita demostrar una de esas alternativas para señalar que la atribución es insuficiente; la acusación necesita la premisa que la descarte con evidencia. Si existe convergencia fuerte, se describe su alcance sin saltar a certeza absoluta.

6.2 Cronología y corroboración

Se conserva el valor literal de cada fecha, su zona y precisión. Envío, recepción, lectura, edición y captura son eventos distintos. La fecha de una exportación no es la fecha del mensaje. La hora de una notificación puede depender de otra capa. Las diferencias se analizan con diccionario y reloj antes de presentarlas como falsificación.

La corroboración puede venir de otro participante, un registro de sesión, una copia, un recibo, una cámara o una secuencia de sensores. No se cuenta el número de capturas como si fueran fuentes independientes. La pregunta es qué error podría tener cada fuente y si esa convergencia permite descartar explicaciones alternativas.

6.3 Informe con alcance explícito

Nivel	Redacción defendible	No afirmar
Objeto	Se recibió el dispositivo con estos identificadores y accesorios.	“Era el teléfono del acusado” solo por apariencia.
Adquisición	La herramienta obtuvo estos archivos y bases en el alcance descrito.	“Se extrajo todo lo que existía.”
Contenido	El mensaje figura con esta fecha y participantes en la fuente.	“El titular lo escribió” sin evidencia de uso.
Análisis	Las fuentes son compatibles con esta secuencia y presentan estos límites.	“No hay ninguna otra explicación.”
Ausencia	No se observó el evento en la cobertura y filtros.	“Nunca existió.”

Cierre del análisis

La persona no se deduce de una sola etiqueta. La atribución se fortalece cuando fuentes independientes podrían haberla contradicho y no lo hacen; se debilita cuando una de ellas demuestra otra posibilidad.



Figura 3. De una cuenta a una persona: faltan premisas. La atribución se fortalece con independencia, no con adjetivos Reconstrucción editorial; no constituye evidencia real.

Anexo A. Formatos operativos

A.1 Recepción del dispositivo

Acta ficticia

```
Caso: EXP-DEMO-2026-005
Dispositivo / ID: DEMO-MBL-003
Marca, modelo e identificadores visibles: [registro]
Estado: [encendido, bloqueo, batería, red, daño]
Accesorios: [cable, SIM, memoria, funda, otros]
Entrega / recepción: [funciones, fecha, zona, lugar]
Acciones previas: [observadas y declaradas por separado]
Autoridad: [aplicaciones, cuentas, período, exclusiones]
Riesgos: [volatilidad, borrado, batería, privacidad]
Decisión inicial: [aislamiento, alimentación, escalamiento]
Fotografías y sellos: [identificadores y relación]
Observaciones: [sin claves ni datos innecesarios]
```

A.2 Inventario de cuentas y fuentes

Capa	Cuenta / fuente	Disponibilidad y autoridad	Límite
Dispositivo	[Aplicación y versión]	[Estado, acceso y alcance]	[Cifrado, cobertura]
Cuenta	[Identificador]	[Sesiones, factores y permiso]	[Uso por terceros]
Participantes	[Contacto autorizado]	[Fuente disponible]	[Representación distinta]
Proveedor	[Servicio y custodio]	[Solicitud y respuesta]	[Contenido o retención]
Respaldo	[Fecha y ubicación]	[Clave y acceso]	[Instantánea y cobertura]

A.3 Registro de adquisición

Bitácora de salida

```
Fuente y autoridad: DEMO-MBL-003 / [alcance]
Método: [manual, exportación, lógica, avanzada, proveedor]
Dispositivo, sistema y aplicación: [versiones]
Herramienta, versión y validación: [prueba ficticia]
Fecha de inicio / fin y zona: [literales]
Acciones sobre el dispositivo: [interacciones y cambios]
Objetos obtenidos: [archivos, bases, exportaciones]
Filtros y cobertura: [período, cuentas, exclusiones]
Hash y manifiesto: [por objeto]
Incidencias: [errores, no decodificado, ausencias]
Verificación: [apertura, muestra y revisión]
Custodia posterior: [copia de trabajo y acceso]
```

A.4 Matriz de atribución

Afirmación	Fuente favorable	Alternativa	Resultado limitado
La cuenta envió el mensaje	[Registro]	[Otra sesión posible]	[ ]
El dispositivo estaba activo	[Pantalla, registros]	[Fecha o sesión distinta]	[ ]
La persona lo usó	[Factores, contexto]	[Préstamo, robo, delegación]	[ ]
La conversación está completa	[Exportación]	[Filtros y otras capas]	[ ]
El archivo pertenece al evento	[Mensaje, metadatos]	[Reenvío o edición previa]	[ ]

Anexo B. Marco jurídico y control final

El reconocimiento del documento electrónico no supone que toda captura sea auténtica ni que una cuenta identifique a una persona. En México se revisan CCom 89–94 y 1205, el régimen CFPC/CNPCF según transición y la LMTR para el ámbito correspondiente. Perú distribuye firma, proceso y archivo; Chile diferencia firmas y fecha; Argentina pondera confiabilidad; Colombia y Ecuador detallan conservación; España combina eIDAS y LEC. La aplicación se revisa con versión, materia y jurisdicción.[5][6][7][8][9][10][11][12][13][14]

La protección de datos acompaña todo el procedimiento: se limitan aplicaciones, período, cuentas y datos de terceros; se separan versiones de trabajo y entrega; se conserva evidencia de autoridad y acceso. Un informe no publica contraseñas, claves privadas, números completos ni información que pueda facilitar otro daño.[15][16][17]

Control final	Pregunta de aceptación
Identidad	¿Dispositivo, accesorios y actas coinciden?
Estado	¿Se documentó la decisión de aislamiento y alimentación?
Cobertura	¿La extracción declara filtros, límites y errores?
Contexto	¿La conversación conserva hilo, adjuntos y otras capas?
Atribución	¿Cuenta, dispositivo y persona están separados?

Control final	Pregunta de aceptación
Privacidad	¿Se excluyeron datos ajenos al encargo?
Revisión	¿Otra persona puede localizar y comprobar el objeto?

Cierre

El teléfono puede guardar una parte decisiva de los hechos. El método decide si esa parte puede comprenderse sin convertir una pantalla en una acusación.

Referencias citadas

Cada número remite a la fuente consultada en el cuerpo. La fecha general de revisión documental es el 10 de noviembre de 2026; el uso en un expediente exige comprobar la versión aplicable al hecho, materia, sujeto y jurisdicción.

[1] NIST SP 800-101 Rev. 1. Guía de análisis forense de dispositivos móviles: preservación, adquisición, examen, análisis, validación y reporte. La tecnología y las capacidades concretas deben comprobarse en el dispositivo y herramienta actuales. Fuente oficial en línea

[2] Ley en Materia de Telecomunicaciones y Radiodifusión, publicada el 16-07-2025. Artículos 182 y 183: requerimientos y conservación de datos, consulta en tiempo real y entrega dentro de 48 horas según el tramo. Fuente oficial en línea

[3] RFC Editor. RFC 5322, Internet Message Format: estructura del mensaje, encabezados y cuerpo. Es una referencia técnica para preservar y comprender correo electrónico, no una prueba automática de identidad humana. Fuente oficial en línea

[4] NIST SP 800-101 Rev. 1. Guía de análisis forense de dispositivos móviles: preservación, adquisición, examen, análisis, validación y reporte. La tecnología y las capacidades concretas deben comprobarse en el dispositivo y herramienta actuales. Fuente oficial en línea

[5] Código de Comercio de México, artículos 89–94 y 1205: neutralidad, atribución, escrito, original, integridad, accesibilidad y admisión de mensajes de datos. Compilación oficial. Fuente oficial en línea

[6] Código Nacional de Procedimientos Civiles y Familiares, artículos 348–350. Compilación con reforma del 15-01-2026. La aplicación es gradual y depende de declaratorias. Fuente oficial en línea

[7] Ley en Materia de Telecomunicaciones y Radiodifusión, publicada el 16-07-2025. Artículos 182 y 183: requerimientos y conservación de datos, consulta en tiempo real y entrega dentro de 48 horas según el tramo. Fuente oficial en línea

[8] Perú. Reglamento de la IOFE, DS 052-2008-PCM, artículos 3 y 4: exigencia y admisión de documentos electrónicos firmados digitalmente. Fuente oficial en línea

[9] Perú. Código Procesal Civil, artículos 188–197 y 245.5: finalidad, legalidad, medios, carga, valoración y fecha por medios técnicos. Fuente oficial en línea

[10] Chile. Ley 19.799 sobre documentos electrónicos y firma electrónica, artículos 1–5: equivalencia, escrito, firma simple/avanzada, fecha y valor probatorio. Fuente oficial en línea

[11] Argentina. Código Civil y Comercial, artículos 318–319: correspondencia por cualquier medio y ponderación de confiabilidad de soportes y procedimientos técnicos. Fuente oficial en línea

[12] Colombia. Ley 527 de 1999, artículos 5–13, 16–25 y 28: mensajes de datos, escrito, original, integridad, admisibilidad, conservación, envío, recepción y firma digital. Fuente oficial en línea

[13] Ecuador. Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos, Ley 67, artículos 2, 6–8, 10–16: equivalencia, escrito, original, conservación, procedencia, envío, recepción y firma electrónica. Fuente oficial en línea

[14] España. Ley de Enjuiciamiento Civil, artículos 326 y 384: documentos privados, impugnación, instrumentos para archivar, conocer o reproducir datos, examen, custodia y sana crítica. Fuente oficial en línea

[15] México. Ley Federal de Protección de Datos Personales en Posesión de los Particulares, texto publicado el 20-03-2025 y reforma del 14-11-2025. Artículos 5–9, 18–20 y 31: principios, seguridad, confidencialidad, vulneraciones y atención de derechos. La autoridad federal actual es la Secretaría Anticorrupción y Buen Gobierno. Fuente oficial en línea

[16] Ecuador. Ley Orgánica de Protección de Datos Personales, Registro Oficial Suplemento 459 de 26-05-2021. Artículos 10, 37–44: principios, medidas de seguridad, protección desde el diseño, riesgos y tratamiento ante incidentes. Fuente oficial en línea

[17] Unión Europea. Reglamento (UE) 2016/679, artículos 5, 25, 28 y 32–34: principios, protección desde el diseño, encargados, seguridad y notificación/comunicación de violaciones de seguridad. España exige revisar además la legislación nacional y sectorial aplicable. Fuente oficial en línea

Aviso editorial: guía técnica general y material educativo. No constituye asesoría legal, dictamen pericial ni autorización para acceder a sistemas o información. Los ejemplos y cifras de demostración son ficticios; las figuras son reconstrucciones editoriales.