BIBLIOTECA
ACCCF

04
VOLUMEN

ACCCF / CONOCIMIENTO APLICADO

# Manual de defensa técnica ante acusaciones basadas en evidencia digital

## Revisión de capturas, conversaciones, archivos, ubicación, informes y razonamiento pericial

Examinar una acusación sin aceptar sus atajos ni fabricar otra versión cómoda: localizar el objeto, comprobar el método y delimitar lo que realmente puede afirmarse.

**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: una imagen nítida puede contar una historia incompleta . . . 4**

**Capítulo 1. La afirmación antes que el archivo . . . 4**

1.1 Descomponer la acusación . . . 4

1.2 El expediente y su cobertura . . . 5

**Capítulo 2. Revisión de la recepción y de la custodia . . . 6**

2.1 Identidad del objeto antes que contenido . . . 6

2.2 Transferencias que faltan en la historia . . . 6

2.3 Autoridad y proporcionalidad . . . 6

**Capítulo 3. Matriz de contradicciones . . . 7**

3.1 Detectar sin escoger solo lo que favorece . . . 7

3.2 Tipos de contradicción y su efecto . . . 7

**Capítulo 4. Capturas, conversaciones y archivos . . . 8**

4.1 La captura como fragmento . . . 8

4.2 Exportación y contexto de mensajería . . . 9

4.3 Metadatos y versiones . . . 9

**Capítulo 5. Razonamiento y revisión independiente . . . 9**

5.1 Premisas y falsa consecuencia . . . 9

5.2 Hipótesis alternativas y prueba de falsación . . . 10

5.3 Revisión que intenta romper el informe . . . 10

**Capítulo 6. Revisión del informe pericial . . . 11**

6.1 Trazabilidad de cada conclusión . . . 11

6.2 Preguntas útiles para contradicción . . . 12

**Capítulo 7. Caso integrado: de la acusación a la conclusión limitada . . . 12**

7.1 Material disponible . . . 12

7.2 Comprobaciones y hallazgos . . . 12

7.3 Informe breve de resultado . . . 12

**Anexo A. Formato de revisión y preguntas . . . . . 13**

A.1 Matriz de afirmaciones . . . . . 13

A.2 Lista de preguntas técnicas . . . . . 13

A.3 Registro de fuentes solicitadas y recibidas . . . . . 13

**Anexo B. Funciones jurídicas para la revisión . . . . . 14**

# Presentación: una imagen nítida puede contar una historia incompleta

Una captura puede parecer concluyente porque contiene un nombre, una frase y una hora. Un video puede parecer suficiente porque muestra un rostro conocido. Una antena puede parecer una dirección cuando se dibuja como un punto en un mapa. La defensa técnica comienza por detener esa traducción automática: qué es exactamente el objeto, quién lo produjo, qué parte de la historia conserva, qué método se aplicó y qué otras explicaciones siguen siendo compatibles.

Contradecir no significa negar todo. Si el hash coincide, se reconoce esa coincidencia; si una fuente es confiable, se explica su alcance; si una conclusión es correcta, no se la combate por deporte. El trabajo consiste en separar lo demostrado de lo inferido. A veces la conclusión acusatoria se mantiene. Otras veces basta una identificación equivocada, una fecha sin zona o una exportación incompleta para mostrar que el razonamiento no se sostiene tal como fue presentado.

La persona acusada no necesita inventar una historia alternativa para demostrar que la primera es débil. El revisor puede concluir que la fuente no acredita la afirmación, que no existe cobertura para descartar otras explicaciones o que el método no permite una identificación humana. La precisión evita convertir una defensa en una segunda acusación sin prueba.

> **Pregunta rectora**
>
> ¿Qué afirmación desaparece si retiro una premisa no comprobada? Esa pregunta guía la revisión de cada captura, informe, registro y conclusión.

# Capítulo 1. La afirmación antes que el archivo

## 1.1 Descomponer la acusación

Se escribe la afirmación completa sin adjetivos: una persona, una acción, un objeto, una fecha, un lugar y una consecuencia. Después se separan sus componentes. “El acusado envió el mensaje desde su casa a las 21:00” contiene al menos cuatro preguntas: existe el mensaje, la cuenta se asoció con él, el dispositivo estaba en una ubicación y él lo utilizó en ese momento. Una misma captura puede no responder ninguna completamente.

Se registran las versiones por separado, sin convertirlas en hechos. La acusación afirma una secuencia; la defensa puede negarla, reconocer parte o desconocerla. El objetivo no es mezclarlas para obtener una versión intermedia, sino identificar qué fuentes pueden confirmar o debilitar cada elemento. El primer documento de trabajo es un mapa de afirmaciones y fuentes necesarias.

| Componente | Pregunta de revisión | Fuente que puede discriminar |
|---|---|---|
| Existencia | ¿Existe el mensaje, archivo, publicación o registro? | Nativo, proveedor, receptor, copia verificada. |
| Integridad | ¿Qué representación se recibió y cómo cambió? | Original, exportación, EML, manifiesto y hash. |

| Componente | Pregunta de revisión | Fuente que puede discriminar |
|---|---|---|
| Atribución | ¿Cuenta, dispositivo o persona? ¿Con qué evidencia? | Sesiones, factores, enrolamiento, contexto y uso. |
| Tiempo | ¿Qué reloj, zona y evento representa la fecha? | Registro literal, sincronización y fuentes independientes. |
| Lugar | ¿Es coordenada, celda, inferencia o testimonio? | Precisión, azimut, mapa, sensores y corroboración. |
| Significado | ¿El contenido prueba lo narrado o solo lo visible? | Hilo, secuencia, original y explicación alternativa. |

## 1.2 El expediente y su cobertura

Se inventaría el material recibido y el faltante: imágenes, archivos nativos, discos, oficios, informes, anexos, exportaciones, videos, audios, sábanas, registros y declaraciones. Cada objeto recibe un identificador sin alterar su nombre original. Si una pericial cita un anexo que no está disponible, esa ausencia se registra antes de evaluar su conclusión. No se revisa un informe como si sus anexos existieran por referencia.

La cobertura describe período, sistemas, filtros y objetos no incluidos. “Se analizó el teléfono” no indica si se revisó toda la memoria, una partición, una aplicación o algunas capturas. “Se examinaron las comunicaciones” tampoco dice si se excluyeron mensajes posteriores que cambian el sentido. La defensa necesita la consulta y el universo examinado, no solamente el resultado favorable a una parte.

### Regla de trabajo

No discutas primero la reputación del perito. Comprueba el objeto, la cobertura y el método. Una crítica de credenciales no repara una fuente que no has revisado.

### Qué conserva cada representación

ACCCF · RECONSTRUCCIÓN EDITORIAL · DATOS FICTICIOS

Una buena imagen puede ser una fuente incompleta

| Objeto | Conserva | No acredita por sí solo |
|---|---|---|
| Captura | Fragmento visible y diseño de pantalla. | URL, fecha, cuenta, hilo o integridad. |
| Exportación | Campos y secuencia elegidos por el proveedor. | Cobertura total o significado de vacíos. |
| Archivo nativo | Estructura y metadatos disponibles. | Autoría humana o verdad del contenido. |
| Registro de servidor | Eventos del sistema y su contexto. | Identidad física ni ausencia de otros canales. |

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

*Figura 1. Qué conserva cada representación. Una buena imagen puede ser una fuente incompleta Reconstrucción editorial; no constituye evidencia real.*

# Capítulo 2. Revisión de la recepción y de la custodia

## 2.1 Identidad del objeto antes que contenido

El acta debe permitir reconocer el objeto exacto: tipo, marca, modelo, serie o identificadores disponibles, estado, accesorios, embalaje, sello, fecha y personas. Un disco genérico, una memoria sin etiqueta o un teléfono descrito de manera distinta en dos actuaciones exige una aclaración. La defensa pregunta qué objeto llegó, cuál se adquirió y cuál aparece en cada fotografía, sin asumir que una diferencia es automáticamente una manipulación maliciosa.

Cuando hay una inconsistencia de identificación, no se construye una conclusión hasta aclararla. Puede existir un error de transcripción, una representación distinta o un objeto realmente diferente. Se comparan actas, oficios, fotografías, capacidad, formato, etiquetas, sellos y códigos del anillo central en discos ópticos. La duda se dirige a la fuente antes que a la persona.

## 2.2 Transferencias que faltan en la historia

La cadena de custodia debe reconstruir accesos y cambios de responsabilidad: recepción, apertura, copia, análisis, traslado, descarga y devolución. Si solo existe la firma de entrega final, hay un período sin trazabilidad. Eso no prueba alteración, pero limita lo que puede afirmarse sobre quién pudo cambiar el objeto y bajo qué condiciones.

Para archivos digitales se conserva el canal completo: EML, encabezados, cuerpo, adjuntos, enlace, permisos, versión y descarga. Un hash calculado al recibir controla integridad desde ese momento, no retroactivamente desde la creación. Si el proveedor escribe el hash en el cuerpo, se verifica y se conserva la relación. Si el informe solo copia un valor sin objeto, algoritmo ni fecha, su significado es limitado.

| Pregunta de custodia | Evidencia esperada | Conclusión que no debe adelantarse |
|---|---|---|
| ¿Es el mismo objeto? | Identificadores, fotografías, sellos y actas coincidentes. | “El acta dice lo mismo, entonces todo es válido.” |
| ¿Quién pudo acceder? | Eventos, roles, ubicación, propósito y fecha. | “Solo el perito tuvo contacto.” |
| ¿Qué copia se analizó? | Relación original, imagen, exportación y trabajo. | “La copia es bit a bit porque lo afirma el informe.” |
| ¿Qué cambió al exportar? | Filtros, zona, formato, campos y limitaciones. | “El PDF equivale a la base completa.” |
| ¿Qué no se sabe? | Períodos, acciones y fuentes ausentes. | “La ausencia de registro demuestra falsificación.” |

## 2.3 Autoridad y proporcionalidad

La defensa revisa quién autorizó el acceso, qué acciones permitía y si existían exclusiones. Una contraseña entregada voluntariamente puede autorizar una consulta concreta, no una copia indiscriminada de toda la vida digital. Un dispositivo de empresa puede contener información personal o de terceros. La capacidad de abrir un archivo no demuestra por sí sola permiso para usarlo con cualquier finalidad.

La revisión no invita a repetir una intrusión. Si el expediente no permite acceder a una fuente, se solicita por la vía correspondiente. La persona defensora no debe ingresar a cuentas ajenas para

“verificar” ni instalar herramientas en dispositivos ajenos. La defensa técnica también protege contra una segunda lesión a la privacidad.

**Resultado de esta etapa**

Una tabla con objeto, estado, identidad, autoridad, transferencias, representaciones y huecos. La siguiente etapa analiza contradicciones sobre esa base, no sobre una historia recordada.

# Capítulo 3. Matriz de contradicciones

## 3.1 Detectar sin escoger solo lo que favorece

La matriz incluye hechos compatibles con la acusación y con otras explicaciones. Cada fila contiene afirmación, objeto, valor literal, método, contradicción, explicación posible y prueba pendiente. No se marca una contradicción como “falso” antes de revisar relojes, formatos, campos, cobertura, representaciones y transcripción. Algunas diferencias son explicables; otras impiden la conclusión.

Un resultado puede confirmar una parte y debilitar otra. Un EML puede demostrar que el adjunto recibido coincide con el declarado por el proveedor, pero no que el contenido del adjunto sea verdadero. Un video puede ser técnicamente original y mostrar una escena preparada. Una fecha puede ser coherente y aun así no corresponder al evento alegado. La revisión conserva esas diferencias.

| Afirmación | Comprobación | Resultado posible |
|---|---|---|
| “El archivo nunca cambió” | Hash, algoritmo, momento y relación con fuente. | Coincide desde recepción; historia anterior desconocida. |
| “La conversación está completa” | Exportación, hilo, participantes y filtros. | Fragmento visible; cobertura por acreditar. |
| “La foto fue a las 20:42” | Metadatos, reloj, zona y secuencia. | Fecha interna compatible con otra hora o incierta. |
| “La antena ubica al acusado” | Celda, tecnología, cobertura y terminal. | Asociación de red; no persona ni domicilio. |
| “El peritaje demuestra autoría” | Fuentes, método, alternativas y premisas. | Cuenta asociada; identidad física pendiente. |

## 3.2 Tipos de contradicción y su efecto

Una contradicción de identidad pregunta si se habla del mismo objeto; una de fuente, si la representación permite la afirmación; una de método, si la consulta puede producir ese resultado; una de tiempo, si los relojes y zonas son compatibles; una de inferencia, si la conclusión sigue a las premisas. No todas tienen el mismo peso ni todas invalidan el expediente. El informe explica el efecto concreto en cada afirmación.

También se distingue ausencia de evidencia y evidencia de ausencia. Que un registro no aparezca en una exportación puede ser significativo si la fuente es completa para el período y los filtros, pero no demuestra que el hecho no existió en otros canales. Esta distinción evita convertir una limitación del proveedor en una prueba absoluta de defensa o de acusación.

**Prueba de revisión**

¿La contradicción cambia la identidad del objeto, la cobertura, la cronología o la conclusión? Si no cambia ninguna, quizá sea una diferencia de presentación. Si cambia una, se formula la pregunta técnica que la resuelve.

**Una contradicción necesita explicación, no un veredicto**

ACCCF · RECONSTRUCCIÓN EDITORIAL · DATOS FICTICIOS

Ejemplo de matriz para revisar fuente, método e inferencia

| Afirmación | Comprobación | Lectura permitida |
|---|---|---|
| “La captura es toda la conversación” | Solicitar exportación, hilo y participantes. | La imagen contiene un fragmento; cobertura desconocida. |
| “El video ocurrió a esa hora” | Revisar contador, zona, reloj y publicación. | Fecha compatible o incierta según fuente. |
| “La antena prueba presencia” | Solicitar celda, azimut, tecnología y cobertura. | Relación con una celda; no domicilio. |
| “El titular escribió el mensaje” | Sesiones, dispositivo, 2FA y contexto. | Cuenta asociada; persona no acreditada. |

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

*Figura 2. Una contradicción necesita explicación, no un veredicto. Ejemplo de matriz para revisar fuente, método e inferencia*
*Reconstrucción editorial; no constituye evidencia real.*

# Capítulo 4. Capturas, conversaciones y archivos

## 4.1 La captura como fragmento

Se describe exactamente lo visible y lo ausente: URL, aplicación, versión, cuenta, fecha, zona, dispositivo, participantes, mensajes anteriores y posteriores, adjuntos y reacciones. Una captura puede ser útil para mostrar un fragmento, pero no demuestra por sí sola totalidad, fecha de creación o autoría. La solicitud se orienta al archivo nativo, la exportación de la aplicación, el mensaje en otro participante o el registro del proveedor.

Cuando solo existe la captura, se limita la conclusión. No se afirma que fue fabricada porque exista una diferencia de alineación, compresión o formato: esos indicios pueden venir de la aplicación o de la captura. Se busca una fuente anterior y se documenta quién la produjo, cuándo y con qué herramienta. Si no hay acceso, la incertidumbre permanece.

### 4.2 Exportación y contexto de mensajería

Una exportación puede contener texto y archivos elegidos por el usuario o por la función de la aplicación. No equivale necesariamente a la base de datos ni a todos los eventos: edición, borrado, reacciones, bloqueos y dispositivos vinculados pueden tener cobertura distinta. Se solicita diccionario, versión, fecha y filtros. Si el mensaje depende de cifrado de extremo a extremo, el proveedor puede no conservar su contenido; eso no impide revisar otras capas.

La secuencia se compara con mensajes recibidos por otros participantes y con registros de dispositivos vinculados. Una reacción o un mensaje posterior puede cambiar el sentido de una frase sin demostrar que la anterior es falsa. La defensa no recorta la conversación para producir el efecto contrario: solicita el contexto suficiente y explica qué parte sigue siendo ambigua.

### 4.3 Metadatos y versiones

Los campos de fecha, autor, aplicación o dispositivo tienen productores y significados distintos. La fecha de creación del sistema puede ser la de copia; el autor puede ser una configuración; el modelo puede proceder de una aplicación que reescribió el archivo. Se comparan metadatos internos, propiedades del sistema, miniaturas, historial de versiones, copia en nube y secuencia de nombres. Un metadato es una pista verificable, no un testimonio infalible.

| Dato | Hipótesis inicial | Alternativa que debe probarse |
|---|---|---|
| Autor de documento | La persona nombrada lo escribió. | Cuenta compartida, plantilla, otro editor o configuración. |
| Fecha de creación | El archivo nació en ese momento. | Copia, descarga, conversión o reloj distinto. |
| IMG_0042 | Pertenece a una secuencia continua. | Importación, renombrado, reinicio o archivos faltantes. |
| Cuenta de correo | El titular escribió el texto. | Sesión, delegación, robo o redacción por tercero. |
| Ubicación EXIF | La persona estuvo en el punto exacto. | Precisión, edición, herencia o sincronización. |

**Caso ficticio**

Una captura muestra una amenaza a las 21:03. El archivo nativo y el mensaje recibido por otro participante muestran 20:03 UTC, que corresponde a otra hora local. La diferencia no demuestra falsificación: revela una conversión omitida en la acusación. La revisión corrige la cronología y conserva el contenido para analizarlo con su contexto.

## Capítulo 5. Razonamiento y revisión independiente

### 5.1 Premisas y falsa consecuencia

El silogismo ayuda a mostrar qué falta. Premisa mayor: un registro de celda acredita una relación de red en determinadas condiciones. Premisa menor: el registro asocia un evento con la celda A. Conclusión válida: existe esa asociación documentada. No se deriva que el titular estuviera en una dirección ni que llevara el teléfono. Para eso se necesitan premisas sobre ubicación, terminal y uso.

La falsa consecuencia aparece cuando una verdad pequeña se utiliza como pasaporte para otra mayor: la firma verifica, por tanto todo el contenido es verdadero; la cuenta pertenece a una persona, por tanto ella escribió; el archivo está íntegro, por tanto es original desde su nacimiento; el perito es reconocido, por tanto su conclusión es científica. Cada salto exige una premisa adicional y una comprobación.

## 5.2 Hipótesis alternativas y prueba de falsación

Se formulan al menos dos explicaciones plausibles y una comprobación capaz de debilitarlas. Si se afirma creación nueva de un archivo, se revisan historial y respaldos; si se afirma uso por el titular, se revisan sesiones y segundo factor; si se afirma manipulación, se comparan original y referencias. La alternativa no se adopta por ser conveniente: se evalúa con el mismo estándar que la acusación.

| Hipótesis A | Hipótesis B | Comprobación que las distingue |
|---|---|---|
| Documento creado el día de salida | Documento anterior copiado o editado después. | Historial de versiones, respaldo y actividad. |
| Cuenta usada por titular | Cuenta usada por otra persona o sesión persistente. | Factores, dispositivo, acceso concurrente y control. |
| Video editado | Video original de una escena preparada. | Estructura, referencias y circunstancias de grabación. |
| Ubicación contradictoria | Fuentes con precisión o zona distinta. | Metadatos, celda, reloj y sensores independientes. |

## 5.3 Revisión que intenta romper el informe

El revisor independiente no solo corrige estilo. Localiza cada objeto, repite consultas, compara valores, busca anexos ausentes y trata de encontrar una explicación que el analista no consideró. También revisa lo favorable a la acusación para no crear una defensa sesgada. Las observaciones se contestan con fuente y cambio, no con autoridad personal.

NIST SP 800-86 y ISO/IEC 27037 aportan marcos para recolección, preservación, examen, análisis y reporte. No garantizan que una conclusión sea verdadera: permiten preguntar si la ruta fue documentada y si otra persona puede reproducirla. El prestigio no sustituye la posibilidad de revisión.[12]

> **Regla de independencia**
>
> El mejor momento para localizar una premisa débil es antes de entregar. Si el informe necesita esconder una fuente o una alternativa para sostenerse, necesita otro análisis, no una mejor defensa retórica.

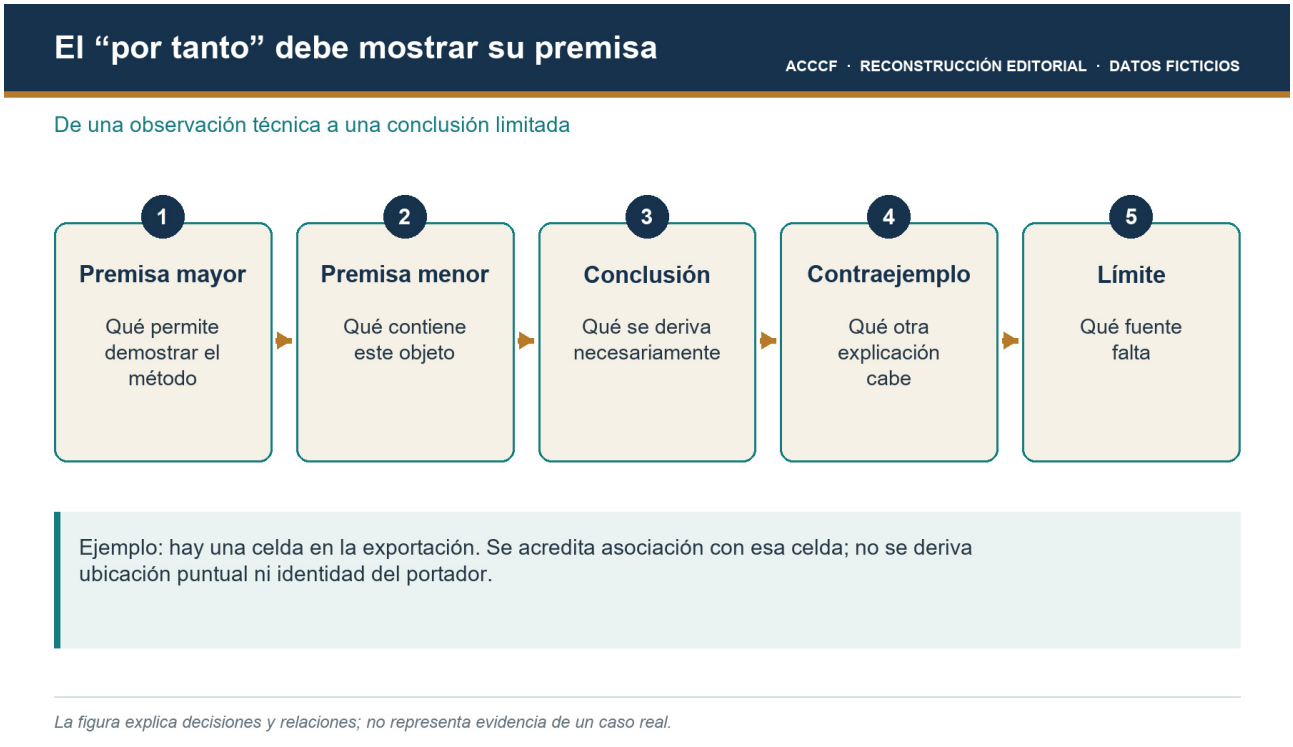



*Figura 3. El “por tanto” debe mostrar su premisa. De una observación técnica a una conclusión limitada Reconstrucción editorial; no constituye evidencia real.*

# Capítulo 6. Revisión del informe pericial

## 6.1 Trazabilidad de cada conclusión

Se toma cada conclusión y se sigue hacia atrás: conclusión ☐ hallazgo ☐ consulta ☐ objeto ☐ adquisición ☐ fuente ☐ autoridad. Si un eslabón falta, se identifica qué afirmación debe limitarse. Las páginas de bibliografía no sustituyen esa ruta. Una norma técnica puede ser verdadera y no demostrar que se aplicó al objeto correcto.

Se distinguen hechos documentales, resultados técnicos, inferencias y opiniones jurídicas. El perito puede explicar qué hizo y qué observó; no necesita declarar culpabilidad ni el resultado del proceso. Una opinión sobre derecho se separa de los hallazgos para que su evaluación no contamine la revisión técnica.

| Plano del texto | Ejemplo de revisión | Pregunta pendiente |
|---|---|---|
| Recepción | El EML llegó con dos adjuntos. | ¿Se conserva completo y con identificadores? |
| Resultado | El adjunto coincide con hash declarado. | ¿Qué prueba eso sobre contenido y origen? |
| Inferencia | La entrega conserva verificación de integridad. | ¿Desde qué momento y con qué límite? |
| Conclusión | El registro es compatible con una entrega verificable. | ¿Puede afirmarse identidad o verdad? |
| Opinión jurídica | La parte es responsable. | ¿Corresponde al perito y qué premisas usa? |

### 6.2 Preguntas útiles para contradicción

Las preguntas se formulan para obtener una comprobación, no para ofrecer un discurso: qué objeto produjo el dato, qué versión de herramienta se usó, qué filtros se aplicaron, qué campos vacíos existen, qué zona horaria se utilizó, qué fuente descartó una hipótesis, qué limitaciones impiden atribuir una acción a una persona. Si la respuesta es “la experiencia del perito”, se pide el registro concreto.

También se pregunta qué cambiaría la conclusión. Si no existe ninguna fuente capaz de modificarla, el método puede estar cerrado a falsación. Un informe robusto indica qué datos apoyan su conclusión y cuáles podrían debilitarla. Eso no lo hace menos firme; lo hace comprobable.

**Pregunta central**

¿Puede otra persona, sin compartir la versión inicial, localizar el objeto, repetir el método y llegar a un resultado compatible? Si no, la conclusión depende de una explicación que el expediente no permite revisar.

## Capítulo 7. Caso integrado: de la acusación a la conclusión limitada

### 7.1 Material disponible

Un caso ficticio contiene una captura de conversación, un video descargado de una plataforma, una sábana en PDF y un informe que afirma presencia y autoría. La persona acusada reconoce la cuenta, pero niega haber escrito el mensaje y señala otra ubicación. No existe todavía archivo nativo del video ni EML de la sábana. El primer resultado no es una contrapericial extensa: es un inventario de fuentes faltantes.

### 7.2 Comprobaciones y hallazgos

La exportación de la conversación muestra mensajes posteriores que cambian el sentido del fragmento, sin eliminar el mensaje inicial. El video presenta una conversión de plataforma y se solicita el original de cámara para evaluar continuidad. El EML de la sábana permite verificar el adjunto, pero el diccionario indica que la celda es una relación de red, no una coordenada del usuario. El informe de acusación había unido tres afirmaciones distintas en una sola.

La revisión no concluye que todo es falso. Concluye que el mensaje existe, que el contexto inicial estaba incompleto, que el video aún no permite una afirmación de originalidad y que la sábana no demuestra domicilio ni portador. Esas conclusiones son útiles porque delimitan qué puede discutirse con fundamento y qué necesita otra fuente.

### 7.3 Informe breve de resultado

#### Ejemplo de conclusión técnica

```
1. La captura EV-01 contiene el fragmento visible del mensaje, pero no acredita totalidad, autoría física ni fecha de generación

2. El archivo EV-02 es una descarga de plataforma. Su estructura puede ser compatible con una conversión legítima; sin el origin

3. La sábana EV-03 asocia el evento con la celda DEMO-A17. El diccionario no contiene mediciones que permitan ubicación puntual.

4. La afirmación de autoría física requiere evidencia adicional de sesión, dispositivo, factores y contexto. El resultado no dem
```

**Lección**

La defensa técnica puede ser precisa sin prometer absolución. Su fuerza está en mostrar exactamente qué parte de una acusación no nace de la fuente.

# Anexo A. Formato de revisión y preguntas

## A.1 Matriz de afirmaciones

| Campo | Contenido requerido | Ejemplo ficticio |
|---|---|---|
| Afirmación literal | Texto sin interpretación ni adjetivos. | “La persona escribió a las 21:03.” |
| Objeto y fuente | Identificador, representación y procedencia. | Captura EV-01; nativo pendiente. |
| Premisas usadas | Qué debe ser verdadero para sostenerla. | Cuenta = persona; hora mostrada = local. |
| Comprobación | Método, filtros, herramienta y cobertura. | Exportación, sesiones y diccionario. |
| Contradicción | Valor literal que no encaja y posibles causas. | Mensaje con zona UTC distinta. |
| Conclusión limitada | Qué queda demostrado y qué no. | Mensaje existe; autoría física no acreditada. |
| Fuente pendiente | Qué puede cambiar el resultado y cómo se solicita. | Registros de sesión y participantes. |

## A.2 Lista de preguntas técnicas

### Guía para formular revisión

1. ¿Cuál es el objeto exacto y dónde está su representación nativa?
2. ¿Qué consulta produjo el hallazgo y qué cobertura tuvo?
3. ¿Qué campos fueron excluidos, filtrados o quedaron vacíos?
4. ¿Qué significan la fecha, la zona y la precisión?
5. ¿Qué otra explicación es compatible con el mismo hallazgo?
6. ¿Qué fuente podría debilitar la hipótesis principal?
7. ¿La corroboración es independiente o repite el mismo archivo?
8. ¿Qué premisa permite pasar de cuenta a persona?
9. ¿Qué parte de la conclusión es técnica y cuál jurídica?
10. ¿Qué limitaciones impiden afirmar más?

## A.3 Registro de fuentes solicitadas y recibidas

| Solicitud | Recepción y control | Estado |
|---|---|---|
| Nativo y exportación de conversación | EML, adjuntos, hash, filtros y diccionario. | [ Pendiente / recibido / limitado ] |
| Archivo original y referencias de video | Objeto, herramienta, versión, fecha y método. | [ ] |
| Sábana nativa y diccionario | Campos, zona, celda, cobertura y EML. | [ ] |
| Sesiones y factores de cuenta | Enrolamiento, dispositivos, acceso y recuperación. | [ ] |
| Anexos del informe cuestionado | Relación con citas y consultas reproducibles. | [ ] |

# Anexo B. Funciones jurídicas para la revisión

La revisión técnica se conecta con reglas de reconocimiento, integridad, original, atribución y valoración. La admisión no equivale a plena prueba y una presunción de firma no acredita todos los hechos. La fuente debe analizarse en su jurisdicción, materia y versión; esta guía no sustituye el estudio procesal de la defensa.

| Jurisdicción | Función documental relevante | Aplicación a la defensa |
|---|---|---|
| México | CCom 89–94 y 1205; CFPC 210-A / CNPCF 348–350 según transición. | Fiabilidad del método, atribución, integridad y accesibilidad; revisar régimen vigente. |
| Perú | Reglamento IOFE; CPC 188–197 y 245.5; normas archivísticas sectoriales. | Carga, legalidad, medios típicos/atípicos y fecha por medios técnicos. |
| Chile | Ley 19.799, arts. 1–5. | Clases de firma, fecha y valor probatorio diferenciados. |
| Argentina | Ley 25.506; CCyC 318–319; Decreto 182/2019. | Confiabilidad de soportes, correspondencia y presunciones limitadas. |
| Colombia | Ley 527, arts. 5–13, 16–25 y 28; CPACA cuando aplique. | Original, conservación, contexto, admisibilidad y valoración. |
| Ecuador | Ley 67, arts. 2, 6–8, 10–16 y Reglamento. | Integridad, conservación, procedencia y efectos de firma. |
| España / UE | eIDAS 25–26 y 46; LEC 326 y 384; Ley 6/2020. | Impugnación, custodia, examen y valoración; no citar Ley 59/2003 como vigente. |

Fuentes de la tabla: [34567891011121314]

### Cierre

Revisar no es fabricar duda. Es exigir que la afirmación tenga una fuente, un método y una conclusión que no exceda lo demostrado.

# 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 800-86. Guide to Integrating Forensic Techniques into Incident Response. Guía metodológica, no legislación ni garantía de admisibilidad. Fuente oficial en línea

[2] ISO/IEC 27037:2012. Directrices para identificación, recolección, adquisición y preservación de evidencia digital. Edición confirmada por ISO como vigente. Fuente oficial en línea

[3] 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

[4] Código Federal de Procedimientos Civiles, artículo 210-A: fiabilidad del método, atribución, accesibilidad e integridad de la información electrónica. Código abrogado por decreto de 07-06-2023, sujeto al régimen gradual de transición. Fuente oficial en línea

[5] 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

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

[7] 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

[8] 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

[9] Argentina. Ley 25.506 de Firma Digital, artículos 1 y 5–9: documento digital, carga al invocar firma electrónica desconocida y presunciones delimitadas. Fuente oficial en línea

[10] 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

[11] 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

[12] Reglamento (UE) 910/2014 eIDAS, artículos 25–26 y 46: no discriminación de firmas electrónicas y documentos por su formato, firma avanzada y efectos de firma cualificada. Fuente oficial en línea

[13] 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

[14] España. Ley 6/2020 de servicios electrónicos de confianza: derogación de la Ley 59/2003 y del artículo 25 de la LSSI; no se cita el régimen anterior como vigente. 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.