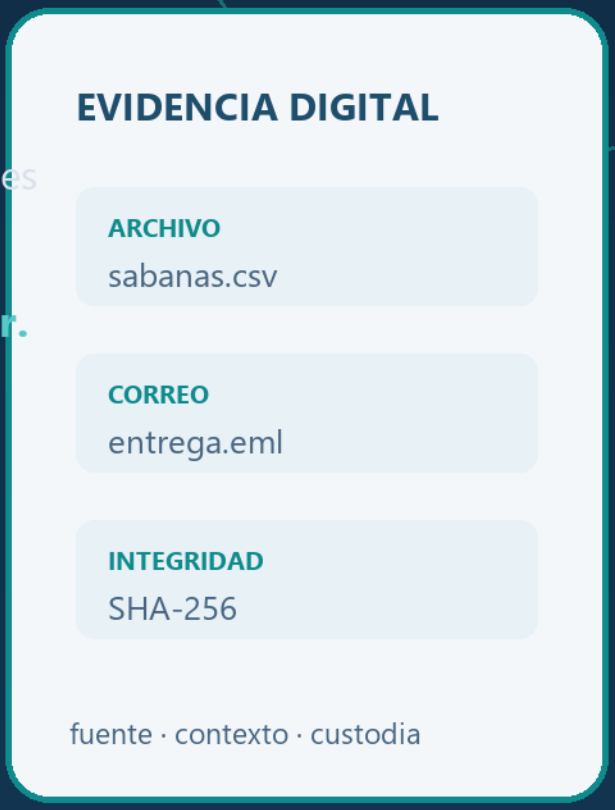
MANUAL DE MANEJO DE

EVIDENCIA DIGITAL

Guía práctica para policía, peritos, abogados y responsables de organizaciones

Preservar. Documentar. Comprender.



Jocsan Laguna
Duriva · ACCCF

Edición 2026 · Ejemplos ficticios y formatos aplicables

Presentación del manual

Este manual explica cómo recibir, preservar, adquirir, trasladar, analizar y presentar evidencia digital con un método que otra persona pueda revisar. Está escrito para policía, peritos, abogados y responsables de organizaciones. No exige ser ingeniero: cada término se explica con una acción y un ejemplo. Tampoco sustituye la autoridad, la legislación ni el criterio profesional que cada caso requiere.

La regla central es sencilla: no se trata de abrir un dispositivo y buscar algo que confirme una sospecha. Se trata de decidir qué debe demostrarse, localizar dónde puede estar la evidencia, elegir el método menos invasivo que sea adecuado y registrar lo realizado. Una conclusión útil no es la más segura de sí misma, sino la que distingue con claridad hechos, inferencias y preguntas abiertas.

Cómo usar este manual

Si eres la primera persona que recibe el caso, ve a los capítulos 1, 3, 5 y 7. Allí encontrarás cómo delimitar el encargo, decidir quién hace qué, elegir una ruta de adquisición y registrar la recepción sin improvisar. Si vas a adquirir o analizar, trabaja los capítulos 4, 6, 8, 9 y 10. Si debes revisar una solicitud, un informe o una presentación, utiliza los capítulos 2, 11 y 12 y los anexos A, K, L y M.

Los ejemplos son ficticios y están completos para mostrar el razonamiento, no para imponer una receta. Los formatos incluyen campos de llenado e instrucciones. La matriz jurídica compara funciones y no afirma que dos artículos sean idénticos. Las fechas y las versiones importan: antes de usar una norma, comprueba que esté vigente y sea aplicable al hecho, al sujeto, al canal y al procedimiento.

Principios rectores

Principio	Aplicación práctica
Mínima alteración	Elegir el método que cambie menos y documentar cualquier cambio inevitable.
Autoridad antes que acceso	Tener permiso no es lo mismo que tener capacidad técnica para entrar. Se necesitan ambos.
Contexto antes que fragmento	Una captura aislada no sustituye el archivo, el mensaje completo o la publicación.
Navaja de Ockham	Empezar por la fuente que mejor discrimina hipótesis, no acumular herramientas.
Decisión sin ego	Si la evidencia contradice la primera versión, se corrige la conclusión, no el original.
Reproducibilidad	Otra persona cualificada debe poder localizar, revisar y repetir el procedimiento.
Límite explícito	Lo no observado o no demostrado se declara, no se rellena con suposiciones.
Protección de personas	Preservar evidencia no autoriza difundir datos ni revictimizar a nadie.

Contenido

Presentación del manual 2
Cómo usar este manual 2
Principios rectores 2
Contenido 3
Capítulo 1. Alcance, preguntas y autoridad 5
1.1 La pregunta que ordena todo el trabajo . . . 5
1.2 Autoridad, proporcionalidad y confidencialidad . . . 6
1.3 Inventario inicial de fuentes . . . 6
1.4 Ejemplo completo: una reclamación por ventas . . . 6
Capítulo 2. Integridad, original y contexto 7
2.1 El original no siempre es el dispositivo . . . 7
2.2 Integridad, autenticidad, atribución y veracidad . . . 8
2.3 El hash como control, no como dogma . . . 8
2.4 Accesibilidad y conservación de contexto . . . 8
Capítulo 3. Roles y responsabilidades 9
3.1 Funciones antes que cargos . . . 9
3.2 Comunicación operativa . . . 10
3.3 Independencia y revisión . . . 10
Capítulo 4. Ciclo de vida y preparación forense 10
4.1 Preparar antes de recibir el caso . . . 10
4.2 Puntos de no retorno . . . 11
4.3 Ciclo documentado . . . 11
Capítulo 5. Árboles de decisión por escenario 12
5.1 Equipo encendido o apagado . . . 12
5.2 Adquisición local, remota o por proveedor . . . 12
5.3 Dispositivos móviles y aislamiento . . . 13
5.4 Cuándo detenerse . . . 13
Capítulo 6. Fuentes modernas y sábanas de llamadas 13
6.1 Nube, SaaS y exportaciones . . . 14
6.2 Correo electrónico y EML . . . 14
6.3 Solicitud y recepción de sábanas de llamadas . . . 14
6.4 Ejemplo de cuerpo de solicitud al proveedor . . . 15
6.5 Virtualización, IoT y contenido sintético . . . 15
6.6 Regulación y vigencia sin ejemplos aislados . . . 15
Capítulo 7. Recepción y preservación inicial 16
7.1 Acta de recepción comprensible . . . 16
7.2 Embalaje y sellado . . . 17
7.3 Etiquetas y relación entre objetos . . . 17
7.4 Recepción de archivos y mensajes . . . 17
Capítulo 8. Adquisición y documentación técnica 18

8.1 Física, lógica, volátil y documental . . . 18
8.2 Herramientas y validación . . . 18
8.3 Exportaciones y consultas reproducibles . . . 19
8.4 Errores e incidencias . . . 19
Capítulo 9. Custodia, traslado y conservación 19
9.1 La cadena que responde preguntas . . . 20
9.2 Transferencias electrónicas . . . 20
9.3 Almacenamiento y acceso posterior . . . 20
Capítulo 10. Examen, análisis e hipótesis 21
10.1 Preguntas antes que herramientas . . . 21
10.2 Cronología y zonas horarias . . . 21
10.3 Lectura de sábanas y registros . . . 22
10.4 Repetibilidad y reproducibilidad . . . 22
Capítulo 11. Informe, presentación y contradicción 22
11.1 Estructura del informe . . . 23
11.2 Lenguaje para público no técnico . . . 23
11.3 Citas y normas . . . 23
11.4 Revisión de contradicción . . . 23
Capítulo 12. Errores frecuentes y mejora continua 24
12.1 Errores que cambian casos . . . 24
12.2 Lecciones aprendidas . . . 24
12.3 Guía mínima para toda la organización . . . 25
Anexo A. Matriz jurídica funcional resumida 25
A.1 Cómo leer la comparación . . . 25
A.2 Método de actualización . . . 26
Anexo B. Ficha de alcance y autoridad 26
B.1 Formato . . . 26
Anexo C. Acta de recepción 27
C.1 Datos mínimos . . . 27
Anexo D. Registro de adquisición 27
D.1 Registro por objeto . . . 27
Anexo E. Cadena de custodia y transferencias 28
E.1 Registro por evento . . . 28
Anexo F. Solicitud a proveedor y entrega EML 28
F.1 Campos de la solicitud . . . 28
F.2 Verificación al recibir . . . 28
Anexo G. Inventario y manifiesto de archivos 29
G.1 Columnas del manifiesto . . . 29
Anexo H. Cronología y zonas horarias 29
H.1 Tabla de correlación . . . 29
Anexo I. Matriz de hipótesis y análisis 29
I.1 Plantilla de razonamiento . . . 29

Anexo J. Revisión de contenido sintético 30
J.1 Expediente mínimo 30
Anexo K. Plantilla de informe técnico 30
K.1 Estructura de redacción 30
Anexo L. Listas de verificación 31
L.1 Recepción y adquisición 31
L.2 Informe y publicación 31
Anexo M. Control de versiones normativas y del manual 31
M.1 Registro de cambios 31
M.2 Cierre de uso 32

Capítulo 1. Alcance, preguntas y autoridad

Decidir qué debe demostrarse antes de tocar la evidencia.

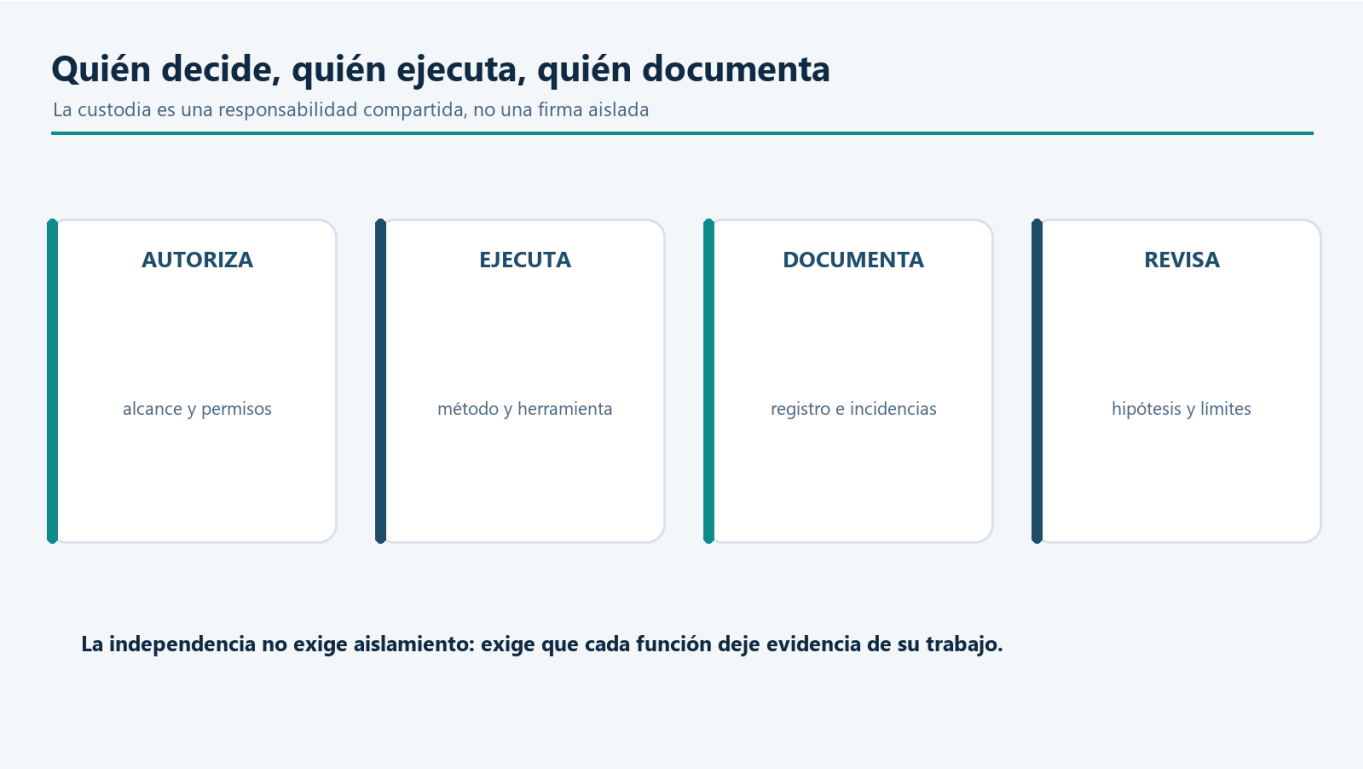


Figura 1. Decidir qué debe demostrarse antes de tocar la evidencia.

1.1 La pregunta que ordena todo el trabajo

Un encargo útil no dice “revisa todo”. Dice qué ocurrió, qué se quiere acreditar, para qué se utilizará el resultado y qué fecha límite existe. La respuesta determina qué fuentes se necesitan y qué nivel de alteración puede justificarse. Una recuperación de archivos para continuidad operativa no es idéntica a una pericial que debe resistir contradicción judicial, aunque compartan herramientas.

Anota los hechos en lenguaje simple: quién reclama, qué afirma, qué niega la otra parte y qué evidencia existe según las primeras declaraciones. Separa lo que alguien vio de lo que alguien supone. Esa distinción evita que una hipótesis inicial se convierta en una instrucción para buscar solo lo que la confirma.

Pregunta	Qué debe quedar escrito	Decisión que evita improvisar
¿Qué afirma cada parte?	Versión separada por persona y por fecha.	No tratar una versión como hecho probado.
¿Qué se necesita demostrar?	Hecho, período, sistema y resultado esperado.	Delimitar fuentes y método.
¿Para qué se usará?	Continuidad, investigación interna, peritaje o proceso.	Definir nivel de documentación.
¿Qué puede salir del alcance?	Datos, dispositivos, cuentas o períodos excluidos.	Reducir exposición innecesaria.

1.2 Autoridad, proporcionalidad y confidencialidad

La autorización debe indicar titular, alcance, acciones permitidas, sistemas, responsables y canal de comunicación. Si se requiere acceder a información de terceros, a una cuenta compartida o a un proveedor, se documenta la vía legítima de obtención. Un perito no se otorga acceso por saber cómo conseguirlo.

La proporcionalidad pregunta si la fuente y el método son necesarios para el objetivo. Si una exportación administrativa responde mejor que una revisión completa del dispositivo, se elige la primera. La confidencialidad no es un añadido: desde la recepción se decide quién puede ver, copiar, transferir y publicar información, especialmente cuando existen datos de terceros o víctimas.

Regla de actuación

Si la autoridad o el alcance no está claro, se detiene la acción y se aclara. “No sabía si podía” no es una custodia defendible. Registra la duda, la respuesta recibida, quién la dio y cuándo.

1.3 Inventario inicial de fuentes

Haz una lista de dispositivos, cuentas, archivos, servidores, proveedores, documentos y personas que pueden aportar contexto. Incluye las fuentes que no están disponibles y el motivo: dispositivo perdido, contraseña desconocida, retención vencida, proveedor sin respuesta o acceso no autorizado. La ausencia también cambia el plan y las conclusiones posibles.

Prioriza por capacidad para resolver hipótesis, volatilidad y riesgo de pérdida. La memoria RAM, una sesión activa, un registro que rota y un enlace que expira pueden exigir acciones distintas. La prioridad no se decide por qué dispositivo parece más importante, sino por qué información puede desaparecer primero y qué pregunta responde.

- Identificador de fuente y custodio actual.
- Tipo de dato, período y formato esperado.
- Relación con el hecho que se quiere demostrar.
- Estado: disponible, restringido, incierto o inaccesible.
- Riesgo de alteración, pérdida o exposición.
- Vía de autorización y siguiente contacto.

1.4 Ejemplo completo: una reclamación por ventas

Una cadena comercial afirma que realizó ventas que no fueron pagadas. El objetivo no es “revisar todas sus computadoras”, sino determinar si las operaciones fueron registradas, transmitidas y liquidadas. Se delimitan fecha, importe, referencia y procesador. Las fuentes prioritarias son reportes del comercio, archivos de remesa, registros del procesador, equipos de interconexión y reportes bancarios.

La autorización se limita a esos sistemas y al período correspondiente. Si las operaciones no aparecen en el archivo de remesa producido por la propia tienda, el hallazgo orienta la investigación, pero no prueba todavía quién causó la inconsistencia. El plan ya evita una revisión invasiva de dispositivos personales y obliga a comparar fuentes independientes.

1. Encargo y versión de las partes redactados por separado.
2. Autorización y exclusiones identificadas.
3. Fuentes priorizadas por pregunta y volatilidad.
4. Datos de terceros y medidas de confidencialidad definidos.
5. Resultado esperado y limitaciones iniciales documentados.

Capítulo 2. Integridad, original y contexto

Comprender qué puede afirmarse del archivo y qué no.

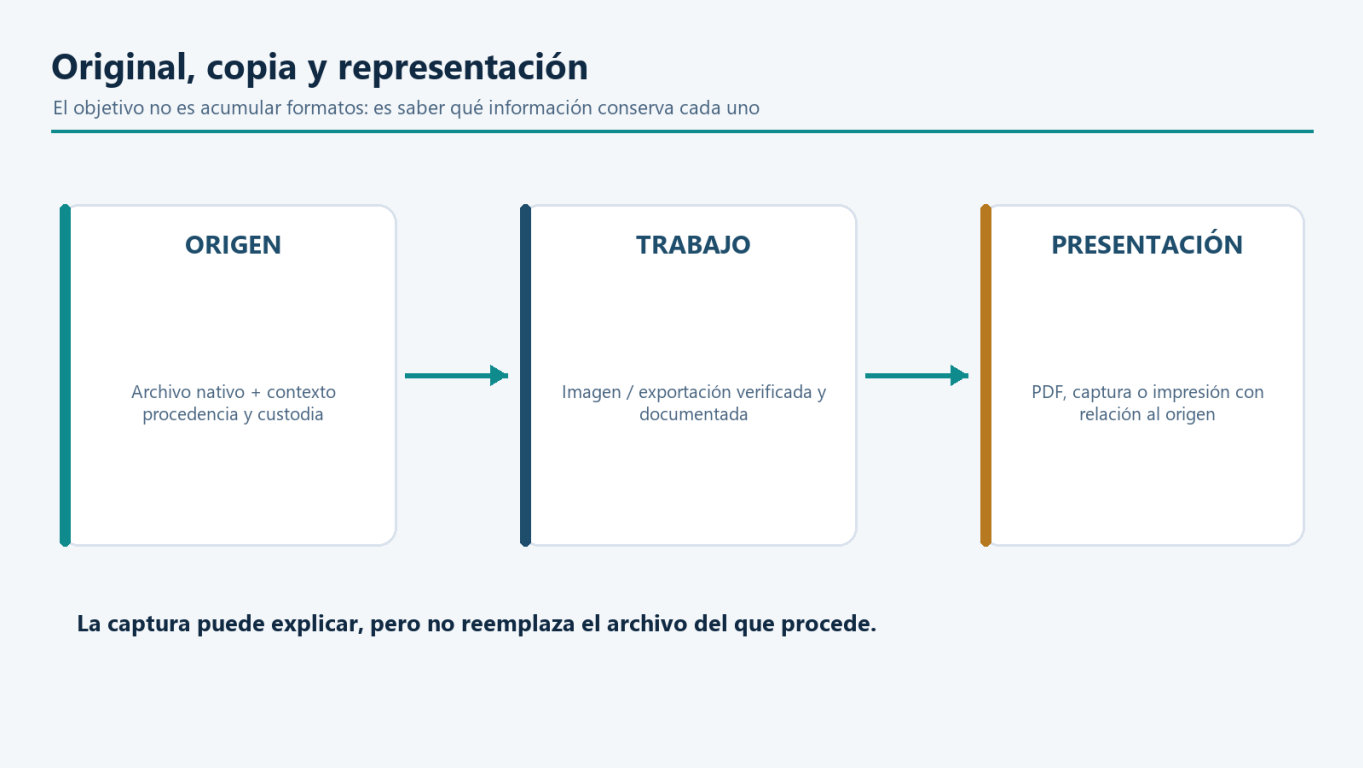


Figura 2. Comprender qué puede afirmarse del archivo y qué no.

2.1 El original no siempre es el dispositivo

En evidencia digital, la noción de original se apoya en integridad desde la forma definitiva y en la posibilidad de consulta posterior, no únicamente en conservar un aparato. Un archivo nativo, una imagen bit a bit, una exportación, una captura y una impresión son representaciones distintas. Cada una puede ser útil si se conoce su relación con el origen y la información que conserva o pierde.

El Código de Comercio mexicano aborda forma escrita, original, integridad y accesibilidad en los artículos 93 y 93 Bis, mientras los artículos 348 a 350 del CNPCF desarrollan una función semejante para información electrónica. Estas reglas no convierten toda copia en original ni todo PDF en una fuente completa. Hay que documentar qué representación se tiene y cómo se obtuvo.[3][4]

[3] Código de Comercio de México, artículos 89–94 y 1205, compilación oficial. [fuente oficial]

[4] Código Nacional de Procedimientos Civiles y Familiares, artículos 348–350, compilación consultada con reforma del 15-01-2026. [fuente oficial]

2.2 Integridad, autenticidad, atribución y veracidad

Integridad se refiere a que el objeto permanece completo e inalterado dentro del alcance declarado. Autenticidad exige sustentar que el objeto es lo que se afirma. Atribución vincula una acción o documento con un origen; veracidad del contenido pregunta si lo narrado ocurrió. Confundirlas produce conclusiones excesivas: un archivo puede estar íntegro y aun así ser falso desde su creación.

Una firma válida puede presumir autoría e integridad en el régimen correspondiente, pero no demuestra que la persona física haya pulsado un botón concreto ni que todo lo afirmado sea verdadero. La revisión debe incluir certificado, vigencia, método, contexto y posibilidad de compromiso de claves, además de corroboración independiente.

Afirmación segura	Qué evidencia requiere	Afirmación que debe evitarse
Los hashes coinciden.	Mismo algoritmo, objeto y momento documentados.	El contenido es verdadero.
El archivo no cambió desde entonces.	Huella calculada en recepción y posterior verificación.	El archivo nunca fue manipulado.
La exportación contiene estos campos.	Método, parámetros y formato del proveedor.	La exportación es completa.
No se observó actividad en el alcance.	Fuentes, filtros, período y consulta reproducible.	La actividad nunca existió.

2.3 El hash como control, no como dogma

Una función hash produce un valor que permite comparar objetos. Si dos archivos tienen el mismo valor con el mismo algoritmo, hay coincidencia en su contenido bit a bit dentro de la comparación realizada. Si un archivo cambia, el valor cambia. Esto ayuda a detectar sustituciones o diferencias, pero no explica por qué ocurrieron ni certifica origen, fecha, autoría o veracidad.

Registra algoritmo, operador, fecha y zona horaria, objeto exacto, ubicación y relación con la evidencia. SHA-256 es una opción común para control de integridad, no una palabra mágica. Dos representaciones distintas de la misma información pueden tener valores diferentes sin que ello demuestre falsedad; una conversión de formato puede cambiar el archivo aunque el contenido visible sea semejante.

Frase correcta para el informe

“El archivo recibido presentó SHA-256 [valor] calculado el [fecha y zona]. La verificación posterior coincidió. Esto acredita que el objeto no cambió entre ambas comprobaciones, no que sea auténtico ni esté completo desde su origen.”

2.4 Accesibilidad y conservación de contexto

Un objeto inaccesible no permite ejercer revisión. Conservar exige saber abrir, leer, interpretar y relacionar la información con su contexto. Un archivo propietario puede necesitar versión del software, documentación del formato o una exportación complementaria. Una copia visual ayuda a presentar, pero no debe eliminar el archivo nativo ni los datos necesarios para comprobarlo.

La NOM-151-SCFI-2016 desarrolla requisitos de conservación y digitalización en México. No sustituye el método del caso ni certifica la veracidad del contenido. La conservación debe incluir condiciones de acceso, integridad, relación con original, metadatos disponibles, responsables y cualquier constancia o tercero involucrado.[5]

[5] NOM-151-SCFI-2016, conservación y digitalización de mensajes de datos. [fuente oficial]

Capítulo 3. Roles y responsabilidades

Saber quién decide, quién ejecuta, quién documenta y quién revisa.

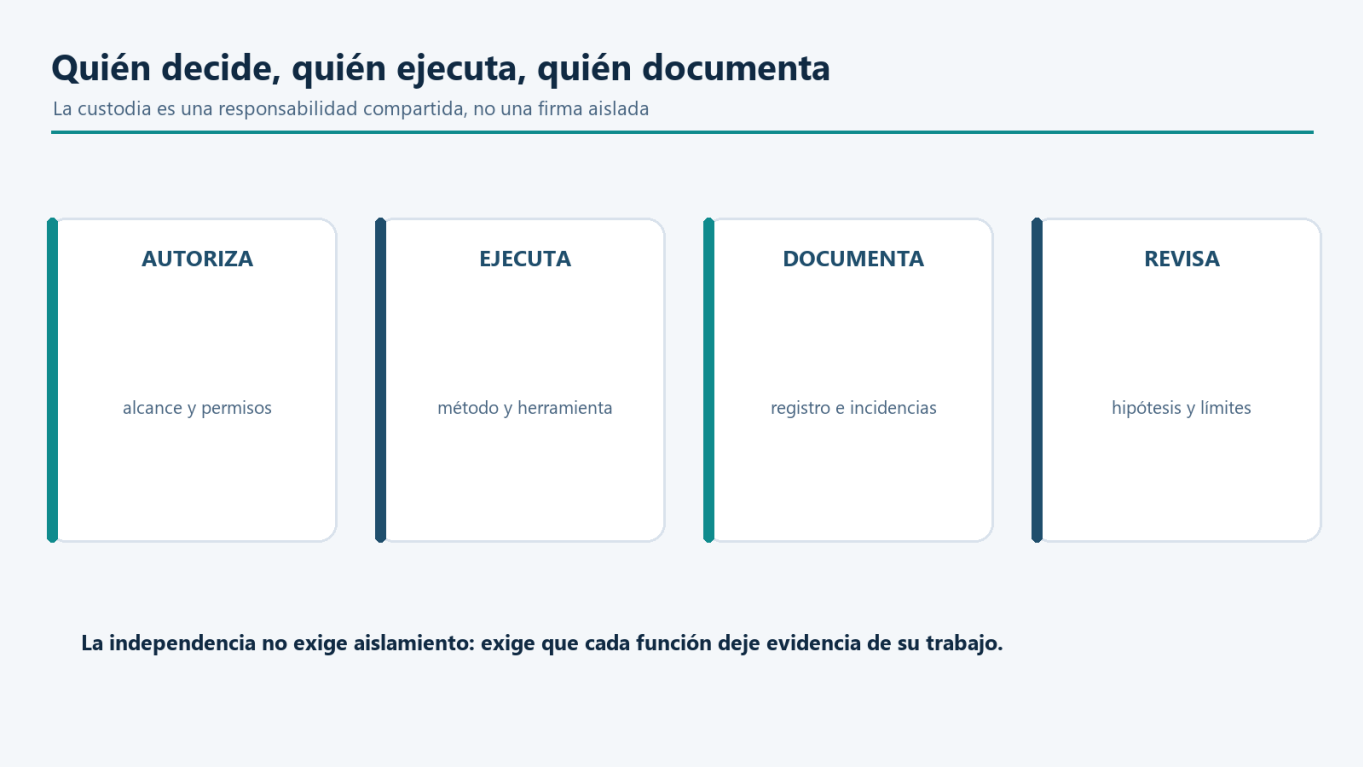


Figura 3. Saber quién decide, quién ejecuta, quién documenta y quién revisa.

3.1 Funciones antes que cargos

Una misma persona puede cumplir varias funciones si el caso lo permite, pero cada actuación debe quedar asociada a una función concreta. Autorizar, ejecutar, documentar, custodiar, revisar y comunicar no son lo mismo. El director no necesariamente adquiere evidencia; el técnico no decide por sí solo qué se publica; el abogado no sustituye la verificación técnica.

Para una fuerza de orden, esta distinción permite que personal sin formación de ingeniería pueda recibir y proteger el caso sin convertirse en analista improvisado. La primera persona respondedora registra estado y riesgo, protege el objeto y solicita apoyo. El especialista decide el método con base en esa recepción y no con una descripción telefónica incompleta.

Función	Responsabilidad principal	Registro esperado
Autoridad del encargo	Define alcance, permisos y exclusiones.	Autorización y cambios aprobados.
Primera respuesta	Identifica estado, evita pérdida y solicita apoyo.	Acta inicial y fotografías.
Especialista	Selecciona y ejecuta el método.	Adquisición, herramienta e incidencias.
Custodio	Controla acceso, ubicación y transferencias.	Cadena de custodia.
Revisor	Contrasta método, hallazgos y límites.	Observaciones y resolución.

3.2 Comunicación operativa

Antes de actuar se establece quién puede responder preguntas técnicas, jurídicas y de custodia. El directorio incluye nombre, función, canal, disponibilidad y suplencia. Las decisiones urgentes se registran con fecha y justificación; una llamada informal no debe quedar como la única constancia de una acción irreversible.

Cuando se entrega material a un proveedor, la conversación se conserva en un formato que permita reconstruirla. Si el proveedor envía archivos por correo, se guarda el EML con cuerpo, encabezados y adjuntos. Si se acuerda una exclusión o una nueva exportación, se incorpora a la autorización y al registro de cambios.

3.3 Independencia y revisión

La revisión independiente busca errores, no culpables. Comprueba si el objeto es el correcto, si el método responde al encargo, si las fechas son coherentes y si la conclusión excede los hallazgos. El revisor puede pedir repetir una consulta o añadir una fuente, pero no altera el original para hacerlo coincidir con la versión preliminar.

El ego se controla documentando hipótesis y resultados adversos. Una revisión que solo busca confirmar lo que el analista ya escribió no es independiente. El informe debe permitir que otra persona entienda qué se encontró, qué se descartó y qué sigue abierto, aunque la respuesta no favorezca al cliente.

Capítulo 4. Ciclo de vida y preparación forense

Evitar pérdidas antes de que ocurra el incidente.



Figura 4. Evitar pérdidas antes de que ocurra el incidente.

4.1 Preparar antes de recibir el caso

La preparación forense consiste en saber qué activos existen, qué registros produce cada uno, quién puede exportarlos, cuánto se conservan y cómo se solicita ayuda. Una organización preparada no registra todo para siempre: identifica fuentes relevantes, define retención proporcional y comprueba que los registros puedan recuperarse con su contexto.

También prepara formatos, credenciales de emergencia, contactos de proveedores, sincronización horaria y procedimientos de preservación. La primera respuesta no debería depender de buscar en internet cómo sellar un dispositivo o averiguar quién administra una cuenta.

- Inventario de activos y propietarios actualizado.
- Fuentes de registros, formato y período de retención.
- Contactos técnicos, jurídicos y de proveedores con suplencia.
- Zona horaria y sincronización documentadas.
- Procedimiento de adquisición, sellado y transferencia disponible.
- Ejercicios periódicos con evidencia ficticia.

4.2 Puntos de no retorno

Algunas acciones pueden impedir el análisis posterior: restablecer un teléfono, reinstalar el sistema, cifrar sin conservar claves, eliminar una cuenta, permitir rotación de registros o sustituir un enlace sin guardar la versión anterior. La contención debe evaluar estas consecuencias y no ejecutarse por reflejo.

Cuando una acción irreversible es necesaria para proteger personas o continuidad, se registra quién la autorizó, por qué era imprescindible, qué evidencia se preservó antes y qué capacidad de análisis se perdió. La buena intención no recupera los datos eliminados.

Decisión urgente	Riesgo probatorio	Actuación previa recomendada
Apagar o reiniciar	Pérdida de memoria y sesiones.	Evaluar adquisición en vivo y documentar estado.
Suspender cuenta	Pérdida de acceso a registros o contenido.	Exportar registros y solicitar preservación al proveedor.
Bloquear dispositivo	Cifrado o borrado remoto potencial.	Confirmar claves y método de acceso autorizado.
Cambiar servidor	Sobrescritura o pérdida de bitácoras.	Preservar imágenes, registros y configuración.

4.3 Ciclo documentado

El ciclo se organiza en autoridad, identificación, preservación inicial, adquisición, custodia, examen, análisis, informe y conservación. Cada fase produce un entregable que alimenta la siguiente. Si una fase carece de registro, la siguiente recibe una suposición y no una base verificable.

ISO/IEC 27037 orienta identificación, recolección, adquisición y preservación; NIST SP 800-86 organiza recolección, examen, análisis e informe. Son referencias metodológicas, no leyes ni garantías de validez. El manual los traduce en acciones comprensibles y formatos que permiten demostrar el trabajo.[1][2]

[1] ISO/IEC 27037:2012. Directrices para identificación, recolección, adquisición y preservación de evidencia digital. [fuente oficial]

[2] NIST SP 800-86. Guide to Integrating Forensic Techniques into Incident Response. [fuente oficial]

Capítulo 5. Árboles de decisión por escenario

Elegir una ruta según estado, objetivo y riesgo, no por costumbre.

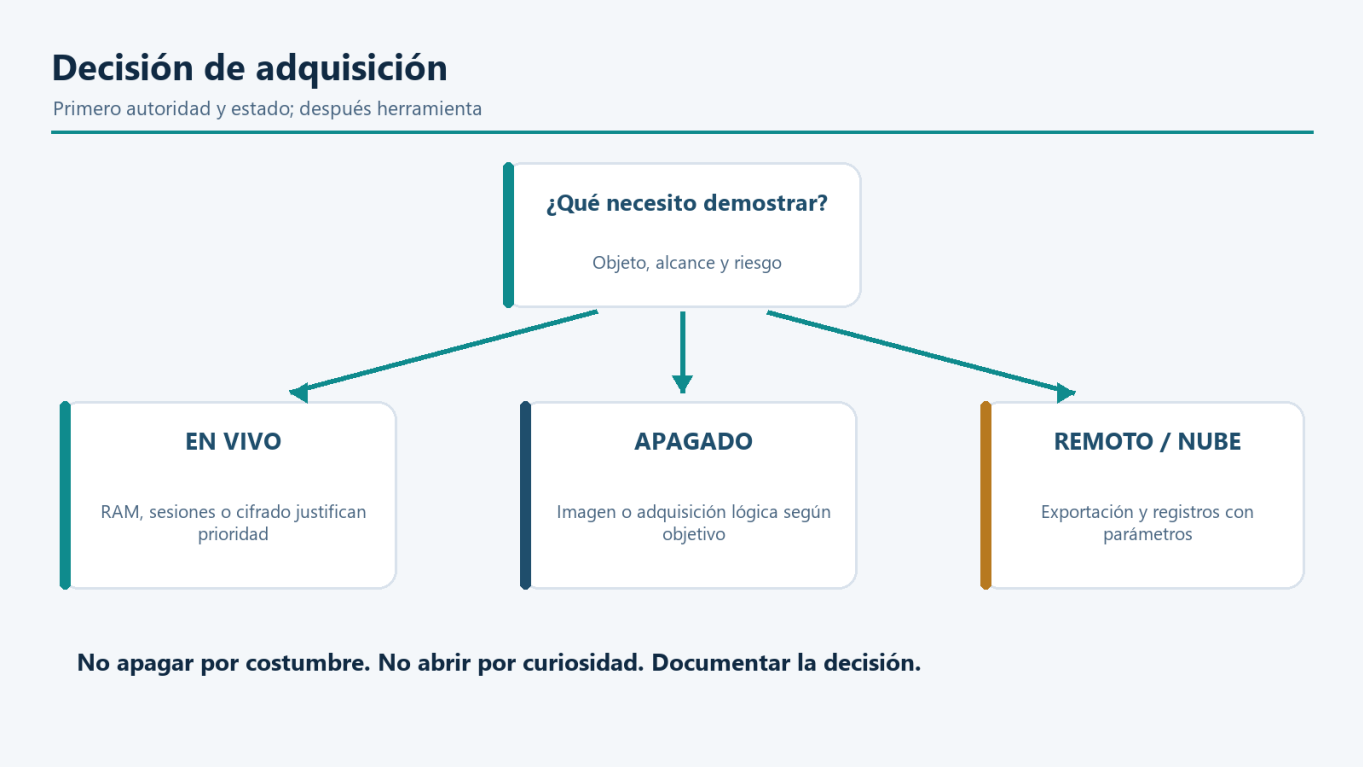


Figura 5. Elegir una ruta según estado, objetivo y riesgo, no por costumbre.

5.1 Equipo encendido o apagado

Un equipo encendido puede contener memoria volátil, sesiones, claves, conexiones y procesos que desaparecen al apagarlo. También puede seguir modificando datos mientras se observa. Un equipo apagado puede ser más estable para una imagen, pero el cifrado y el estado de hibernación cambian las opciones. La decisión se toma con base en la pregunta y en la capacidad disponible.

No se apaga por regla universal ni se conserva encendido por ansiedad. Se registra estado, actividad visible, cifrado conocido, conexiones, autoridad y necesidad de memoria. Si no existe capacidad para adquirir en vivo con seguridad, se documenta y se solicita apoyo antes de cambiar el estado.

5.2 Adquisición local, remota o por proveedor

La adquisición local permite observar dispositivo y contexto, pero no siempre es la mejor fuente. Una exportación administrativa puede conservar eventos que el dispositivo no almacena o que ya fueron eliminados localmente. La vía remota exige registrar identidad de quien ejecuta, parámetros, fecha, zona, formato y canal de transferencia.

Al proveedor se le solicita la fuente adecuada, no “toda la información”. La petición delimita período, cuenta, campos, formato, significado de columnas y proceso de generación. Si existe un portal oficial, se documenta quién lo utiliza, con qué rol y qué filtros aplica. Si el proveedor entrega un archivo sin explicar cómo se creó, esa limitación queda escrita.

5.3 Dispositivos móviles y aislamiento

En un teléfono se evalúan encendido, bloqueo, cifrado, red, sincronización, borrado remoto y batería. Aislar puede evitar cambios remotos, pero también impedir adquisición legítima o activar bloqueos. Retirar batería no es una instrucción universal y muchos equipos no permiten hacerlo sin daño o alteración.

La solución de aislamiento debe ser real y comprobada. Una bolsa antiestática no equivale a jaula de Faraday. Se documenta qué tecnología se usó, cómo se verificó, qué conexiones quedaron activas y qué riesgos se aceptaron. Si no hay condiciones para decidir con seguridad, se preserva el estado y se escala.

5.4 Cuándo detenerse

Detenerse también es una decisión profesional. Falta de autoridad, riesgo para personas, imposibilidad de preservar, ausencia de herramienta validada o peligro de destrucción de evidencia exigen pausar y escalar. Continuar para “ver si aparece algo” puede producir más daño que información.

El registro de detención incluye motivo, estado en que quedó el objeto, acciones previas, riesgos identificados y siguiente responsable. No se presenta como fracaso: es una medida para conservar la posibilidad de análisis y evitar una actuación indefendible.

Regla de seguridad

No ejecutar muestras desconocidas en equipos personales o redes de producción. Usar entorno aislado y copias controladas, con autorización y objetivo definido. La curiosidad no justifica exponer a terceros.

Capítulo 6. Fuentes modernas y sábanas de llamadas

Trabajar nube, correo, proveedores, registros y contenido sintético con contexto.



Figura 6. Trabajar nube, correo, proveedores, registros y contenido sintético con contexto.

6.1 Nube, SaaS y exportaciones

La vista del usuario es solo una capa. Una plataforma puede tener historial de versiones, registros de acceso, roles, tokens, direcciones IP, actividad administrativa, enlaces compartidos, notificaciones y respaldos en otras capas. La exportación debe indicar quién la generó, con qué rol, filtros, zona horaria, formato, período y limitaciones.

Una descarga en PDF puede ser útil para leer, pero insuficiente para analizar estructura y metadatos. Solicita formatos nativos cuando existan, junto con documentación de campos y proceso de generación. Si la plataforma ofrece API, registra endpoint, versión, parámetros, paginación, límites y respuesta, sin incluir secretos en el informe.

6.2 Correo electrónico y EML

El EML conserva cuerpo, adjuntos y encabezados del mensaje, elementos que una captura no reúne por completo. Es especialmente importante cuando el cuerpo contiene una referencia, una explicación de campos o un valor hash para los archivos adjuntos. El EML permite revisar qué se afirmó en la entrega y relacionar cada archivo con esa declaración.

Preserva el mensaje original y registra cómo se obtuvo: exportación del cliente, descarga del servidor o entrega de otra persona. Calcula huellas del EML y de los adjuntos por separado y documenta su relación. El EML acredita el contenido del mensaje recibido, no que todo lo que el remitente afirma sea verdadero ni que la identidad física del remitente esté probada.

> **No confundir objetos**
>
> El hash del EML no es el hash del adjunto y el hash del adjunto no es el hash del sistema que produjo los datos. Cada valor identifica un objeto distinto y debe registrarse con nombre, algoritmo, fecha y relación.

6.3 Solicitud y recepción de sábanas de llamadas

Una sábana de llamadas es una exportación de registros de telecomunicaciones. Para interpretarla no basta una tabla con números: se necesita saber período, zona horaria, tipo de evento, dirección, duración, identificadores, celdas, tecnología, campos vacíos y método de extracción. La solicitud debe pedir formatos nativos disponibles, documentación de columnas y constancia del sistema que produjo el archivo.

En el cuerpo del correo de entrega, el proveedor debe incluir el valor hash correspondiente a cada archivo entregado y el algoritmo utilizado. Ese valor permite comprobar que el adjunto recibido coincide con el archivo al que el proveedor se refiere. Además, se debe presentar y conservar el EML que contiene ese cuerpo, sus encabezados y sus adjuntos. No basta copiar el hash en una nota separada ni guardar solo la tabla.

Al recibir, se verifica que el valor del cuerpo coincida con el adjunto. Si coincide, se documenta; si no, se registra la diferencia y se solicita aclaración sin editar el archivo. Si el proveedor no entrega hash, se anota esa ausencia y se calcula uno al momento de recepción, dejando claro que solo acredita integridad desde ese instante. Ningún hash demuestra por sí solo la veracidad de las llamadas ni la identidad de quien utilizó el teléfono.[16]

Elemento de la solicitud	Qué se pide al proveedor	Qué se revisa al recibir
Período y zona	Inicio, fin, zona horaria y horario de verano.	Eventos dentro del período y conversiones coherentes.
Formato y campos	CSV/XLSX/PDF disponibles, diccionario y proceso de extracción.	Archivo nativo, columnas, vacíos y unidades.
Integridad	Hash de cada archivo y algoritmo en el cuerpo del correo.	Cálculo local, coincidencia o discrepancia documentada.

Elemento de la solicitud	Qué se pide al proveedor	Qué se revisa al recibir
Entrega	EML con cuerpo, encabezados y adjuntos.	EML completo y archivos relacionados, sin separar objetos.
Contexto	Tipo de red, eventos, roaming, celdas e identificadores disponibles.	Qué puede y qué no puede inferirse de cada campo.

[16] México. Disposiciones de carácter general aplicables a las instituciones de crédito, artículos 316 Bis y serie. [fuente oficial]

6.4 Ejemplo de cuerpo de solicitud al proveedor

El siguiente ejemplo es ficticio y puede adaptarse sin incluir datos sensibles en un canal ordinario. La autorización y el expediente se remiten por el canal seguro correspondiente. La finalidad es que la respuesta llegue con suficiente contexto para analizarla y con objetos cuya integridad pueda verificarse.

```
Asunto: EXP-DEMO-2026-001 · Solicitud de registros y constancia de integridad

Estimado equipo de custodia:

Por medio del canal seguro ya autorizado, solicito los registros comprendidos entre el 1 y el 3 de
noviembre de 2026, con indicación expresa de zona horaria y horario de verano aplicable. Agradezco
incluir, cuando estén disponibles, fecha y hora de inicio, duración, tipo de evento, dirección,
identificadores de línea y equipo, celda, tecnología y explicación de campos vacíos.

Solicito los archivos en su formato nativo disponible (CSV y/o XLSX), una copia PDF de consulta, el
diccionario de campos y una descripción del proceso y fecha de extracción. Para cada archivo, agradezco
indicar en el cuerpo de la respuesta el algoritmo y el valor hash correspondiente.

La entrega debe conservar este correo en formato EML, incluidos cuerpo, encabezados y adjuntos. Cualquier
limitación de formato, retención o cobertura debe quedar expresamente señalada.

Atentamente,
Responsable técnico autorizado · EXP-DEMO-2026-001
```

6.5 Virtualización, IoT y contenido sintético

En virtualización se distinguen host, invitado, instantáneas, almacenamiento compartido y registros de administración. En IoT se separan dispositivo, aplicación, hub, nube, firmware y sincronización. La presencia de un dato en una pantalla no indica dónde se generó ni cuántas copias existen. La adquisición debe nombrar la capa y no solo el producto.

Para contenido generado o manipulado con IA se separan generación, edición, conversión y publicación. Se conserva original, historial, herramienta y versión cuando estén disponibles, junto con autorizaciones y revisión humana. Un detector aporta indicios, no veredicto. El análisis jurídico revisa consentimiento, identidad, conducta, uso y vigencia; no convierte “IA” en una categoría penal universal.[7]

[7] Reglamento (UE) 2024/1689 de inteligencia artificial, artículo 50, texto consolidado al 27-07-2026. [fuente oficial]

6.6 Regulación y vigencia sin ejemplos aislados

El Código Penal Federal mexicano regula en los artículos 199 Octies y 199 Nonies determinadas conductas de contenido íntimo sexual sin consentimiento, incluido el supuesto en que el material no corresponde con la persona identificada. El Reglamento europeo de IA, en el artículo 50, aborda transparencia de ultrafalsificaciones y adapta ciertas obligaciones para obras creativas y revisión editorial. Son regímenes diferentes y no deben fundirse en una supuesta prohibición mundial de IA.

San Luis Potosí muestra por qué se verifica la vigencia: la reforma aprobada en noviembre de 2025 adicionó figuras específicas sobre IA, pero los artículos 187 Ter, 272 Bis y 272 Ter fueron derogados el 30 de julio de 2026. El ejemplo es

solo un antecedente local, no una regla universal ni una autorización general. La conducta debe analizarse con la norma vigente y con otras figuras que puedan aplicar.[6][7][8][9]

[6] Código Penal Federal, artículos 199 Octies y 199 Nonies, compilación con reforma del 13-03-2026. [fuente oficial]

[7] Reglamento (UE) 2024/1689 de inteligencia artificial, artículo 50, texto consolidado al 27-07-2026. [fuente oficial]

[8] Congreso de San Luis Potosí. Aprobación de reforma sobre uso indebido de IA, 14-11-2025. [fuente oficial]

[9] Gaceta Parlamentaria de San Luis Potosí. Derogación del 187 Ter y del capítulo con 272 Bis y 272 Ter, publicada el 30-07-2026. [fuente oficial]

Capítulo 7. Recepción y preservación inicial

Registrar el objeto y su estado antes de cualquier análisis.

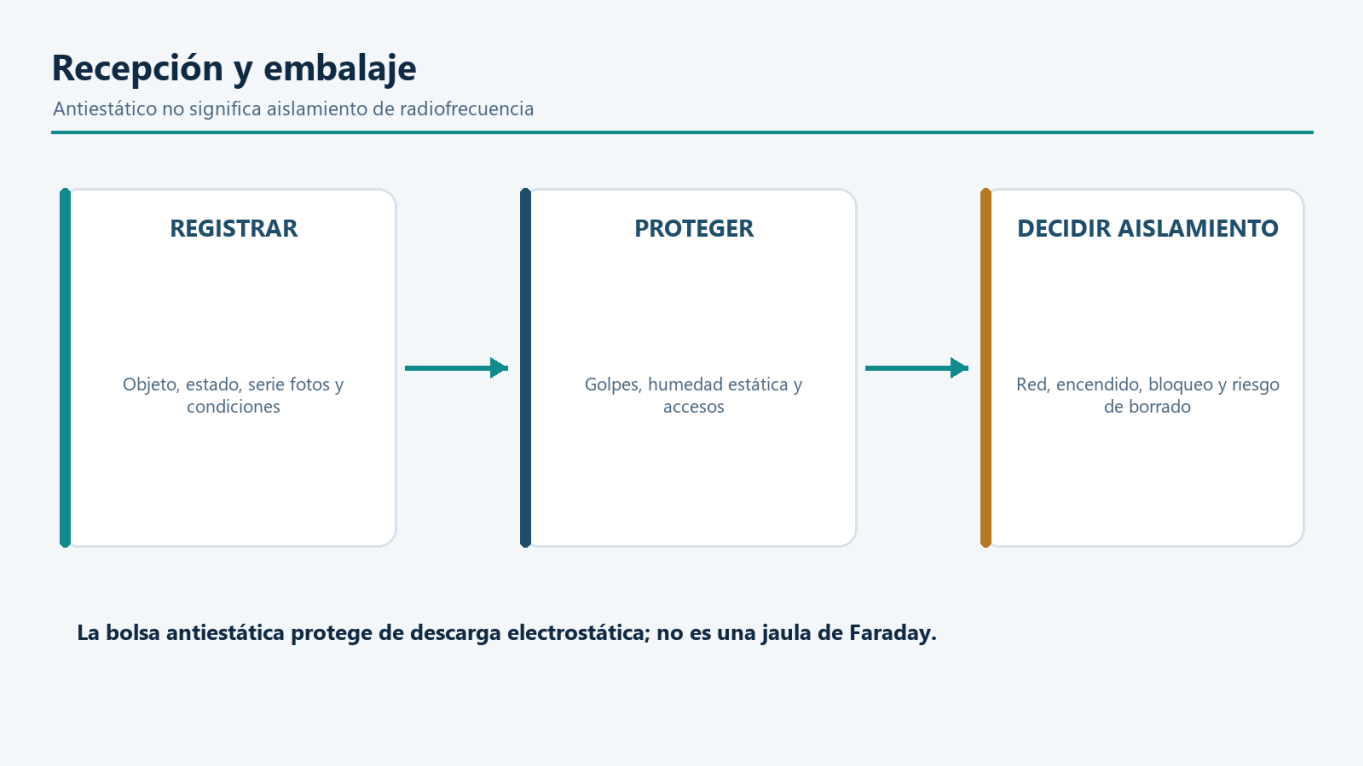


Figura 7. Registrar el objeto y su estado antes de cualquier análisis.

7.1 Acta de recepción comprensible

El acta responde qué llegó, cómo llegó, quién lo entregó, quién recibió, cuándo, dónde y en qué estado. Incluye identificadores disponibles, accesorios, sellos, fotografías y observaciones. No se limita a escribir “una computadora” o “una USB”: registra marca, modelo, número de serie cuando exista, capacidad, estado físico y cualquier etiqueta previa.

La primera persona respondedora no necesita saber adquisición forense para hacerlo bien. Debe evitar encender, explorar o conectar sin autorización, fotografiar el estado, anotar lo visible y pedir apoyo. Si alguien ya abrió archivos, también se registra; no se oculta para que el acta parezca perfecta.

- Identificador único del caso y del objeto.
- Fecha, hora, zona, lugar, entrega y recepción.
- Descripción física, serie, capacidad y accesorios.
- Estado de encendido, bloqueo, red y daños visibles.
- Fotografías generales y de identificadores.
- Acciones previas conocidas y riesgos inmediatos.

7.2 Embalaje y sellado

El embalaje evita daño físico, electrostático, humedad, acceso no autorizado y sustitución. Se selecciona según el objeto y el estado. El sello incluye identificador, fecha, responsable y condiciones que permitan detectar apertura. Si se rompe para trabajar, se documenta y se repone según procedimiento, sin borrar el historial.

Antiestático y aislamiento de radiofrecuencia no son equivalentes. La primera función protege componentes de descargas; la segunda busca impedir comunicaciones inalámbricas y debe validarse. Un embalaje correcto no repara una mala decisión previa, pero evita nuevas alteraciones y permite reconstruir quién accedió al objeto.

7.3 Etiquetas y relación entre objetos

Cada objeto recibe un identificador estable y sin nombre de cliente. Los derivados se relacionan con el original mediante un campo de procedencia. No se reutiliza el identificador para una exportación distinta: se crea un objeto relacionado con su propia fecha, método y huella. Esto evita comparar archivos que solo comparten nombre.

Una convención posible es ED-AAAAMMDD-CASO-FUENTE-SECUENCIA-VERSION. Si la organización ya tiene otra, se mantiene si es única y consistente. La etiqueta física y el acta deben coincidir con el inventario digital y con el informe final.

```
Ejemplo ficticio:
ED-20261109-DEMO-MBL-003-A00

ED = evidencia digital
20261109 = recepción
DEMO = caso ficticio
MBL = fuente móvil
003 = tercer objeto
A00 = adquisición inicial
```

7.4 Recepción de archivos y mensajes

La recepción digital registra origen, canal, fecha, remitente aparente, destinatario, nombres, tamaños y formatos. Los archivos se guardan sin modificarlos y se calculan huellas a la llegada. Si el proveedor entrega valores en el cuerpo, se comprueban y se conserva el EML. Si se recibe por enlace, se documenta quién lo abrió, permisos, fecha de descarga y versión.

Nunca se edita el nombre original para “ordenar” antes de preservar. La relación entre original y copia de trabajo se hace en el manifiesto. Cuando el archivo fue previamente renombrado o convertido por otra persona, se anota esa historia y se conservan todas las versiones disponibles.

Capítulo 8. Adquisición y documentación técnica

Obtener datos con método, validación y trazabilidad.

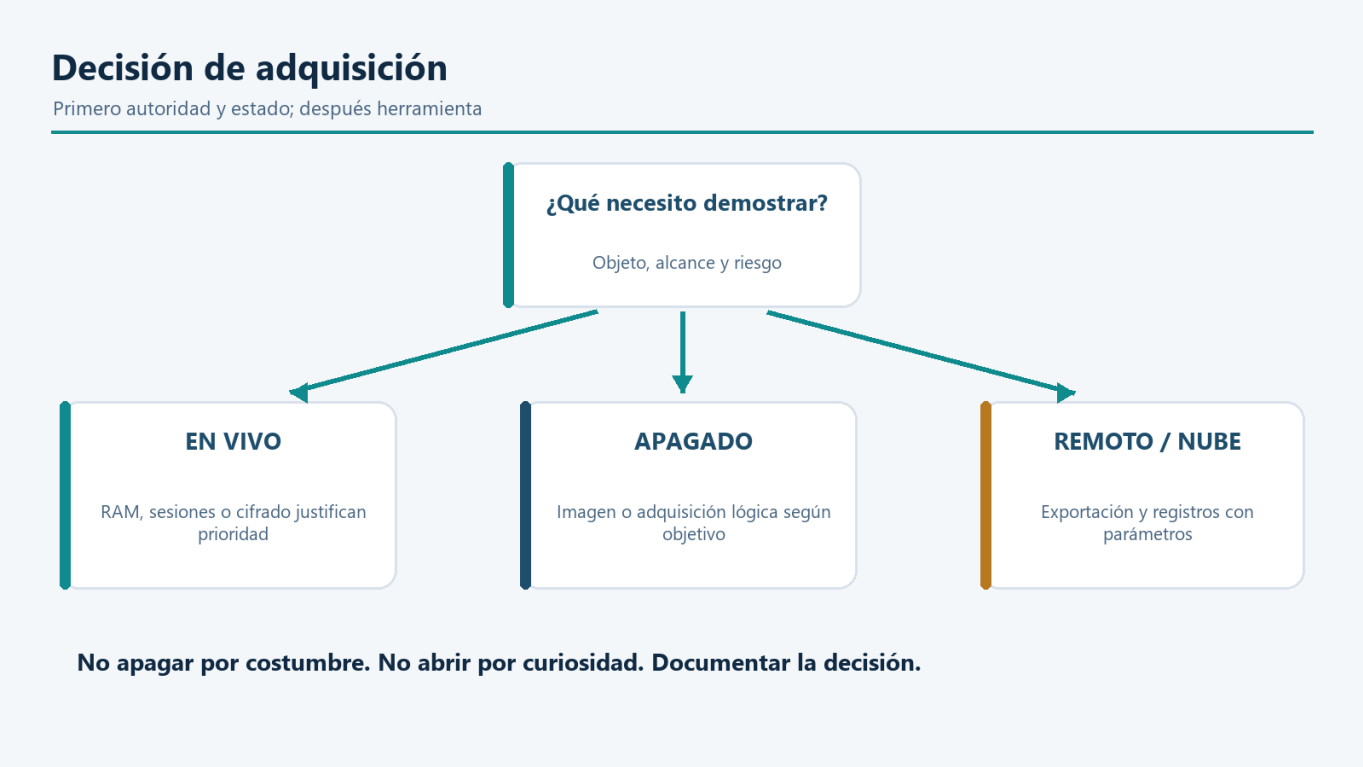


Figura 8. Obtener datos con método, validación y trazabilidad.

8.1 Física, lógica, volátil y documental

La adquisición física copia el medio completo y puede incluir espacio no asignado; la lógica obtiene archivos o fuentes seleccionadas. La volátil recoge memoria y estados temporales cuando está justificada. La documental registra una visualización cuando las demás no están disponibles, sin presentarla como si conservara todas las propiedades del original.

La elección depende de la pregunta, no del prestigio de la herramienta. Para reconstruir actividad eliminada puede ser adecuada una imagen; para obtener registros de una plataforma puede bastar una exportación oficial. El método se explica con prerrequisitos, autoridad, herramienta, versión, parámetros, salida y errores.

8.2 Herramientas y validación

Una herramienta debe conocerse y validarse para el uso previsto. Se registra nombre, versión, entorno, configuración y resultado de prueba. Una actualización puede cambiar formato o comportamiento; no se copia un comando antiguo sin comprobarlo. La validación usa datos ficticios y demuestra que la salida puede abrirse y relacionarse con el objeto esperado.

Los bloqueadores de escritura y otras protecciones se emplean cuando corresponda, pero no se invocan como garantía absoluta. Se documenta el flujo real: dispositivo, conexión, estado, error y verificación. Si una herramienta produce una incidencia, se conserva el mensaje y se evalúa su efecto en vez de ocultarlo.

Campo de adquisición	Ejemplo ficticio	Qué demuestra
Fuente	Disco DEMO-SSD-003	Objeto exacto y custodio.
Método	Imagen bit a bit sobre copia controlada	Tipo de cobertura.

Campo de adquisición	Ejemplo ficticio	Qué demuestra
Herramienta	Nombre y versión validados en laboratorio	Condiciones de ejecución.
Fecha y zona	2026-11-09T14:32:07-06:00	Secuencia temporal.
Integridad	SHA-256 del objeto adquirido	Objeto al que corresponde el valor.
Incidencias	Sector ilegible documentado	Alcance y límite del resultado.

8.3 Exportaciones y consultas reproducibles

Una consulta debe poder repetirse con los mismos parámetros. Registra sistema, cuenta, rol, filtros, zona, formato, campos, fecha, operador y resultado. Si la plataforma cambia su interfaz, conserva versión o evidencia de la ruta utilizada. Una captura puede mostrar la configuración, pero no sustituye la salida nativa.

Cuando la consulta devuelve cero registros, no se concluye inexistencia sin revisar filtros, cobertura, zona, retención y errores. El informe describe qué se consultó y qué respuesta se obtuvo. Esa forma de negativo documentado es más defendible que una afirmación absoluta.

8.4 Errores e incidencias

Las incidencias no se borran del expediente: sectores ilegibles, archivos dañados, contraseñas ausentes, interrupciones de red, diferencias de hash y cambios de proveedor se registran. Se evalúa si afectan cobertura, autenticidad o análisis y se solicita una segunda entrega cuando sea posible.

Si hay que repetir una adquisición, se conservan ambos objetos con identificadores distintos y se explica el motivo. No se elimina el primer archivo para evitar una explicación incómoda. La trazabilidad incluye decisiones que salieron mal y cómo se corrigieron.

Capítulo 9. Custodia, traslado y conservación

Mantener la relación entre objeto, responsable, ubicación y verificación.



Figura 9. Mantener la relación entre objeto, responsable, ubicación y verificación.

9.1 La cadena que responde preguntas

La cadena de custodia permite saber qué objeto existía, dónde estaba, quién podía acceder, para qué se movió y cómo se verificó. No es una lista de firmas sin identificadores. Cada transferencia incluye objeto, entrega, recepción, fecha, zona, propósito, condición del sello y verificación de integridad cuando proceda.

La cadena también registra accesos legítimos sin traslado físico: apertura del contenedor, copia de trabajo, préstamo temporal, cambio de ubicación o descarga remota. Documentar solo la entrega final deja huecos que impiden reconstruir la historia.

9.2 Transferencias electrónicas

Una transferencia por enlace necesita destinatario, permisos, canal, fecha, versión y verificación de descarga. El cifrado protege contenido, pero la gestión de claves debe hacerse por un canal separado y sin incluir secretos en el acta. El receptor confirma objeto y hash antes de continuar.

Si el proveedor incluye el hash en el cuerpo del correo, se conserva el EML completo y los adjuntos. El cuerpo vincula la declaración con la entrega; el archivo recibido se verifica localmente. Si el proveedor cambia el archivo, debe quedar nueva entrega y nueva huella, sin reemplazar silenciosamente el anterior.

9.3 Almacenamiento y acceso posterior

Se mantienen original preservado y copia de trabajo según política. Los respaldos se cifran, se verifican y se prueba su recuperación. Un respaldo que nadie puede abrir no es conservación útil. La migración a otro formato se documenta y no elimina el original.

La retención regulatoria, la política empresarial y la conservación probatoria no tienen el mismo fin ni plazo. No se usa una cifra universal. Se define por norma, caso y necesidad, con acceso restringido y registro de consultas. La conservación incluye legibilidad futura, documentación de formato y claves disponibles.

Capítulo 10. Examen, análisis e hipótesis

Convertir artefactos en explicaciones sin saltos de fe.

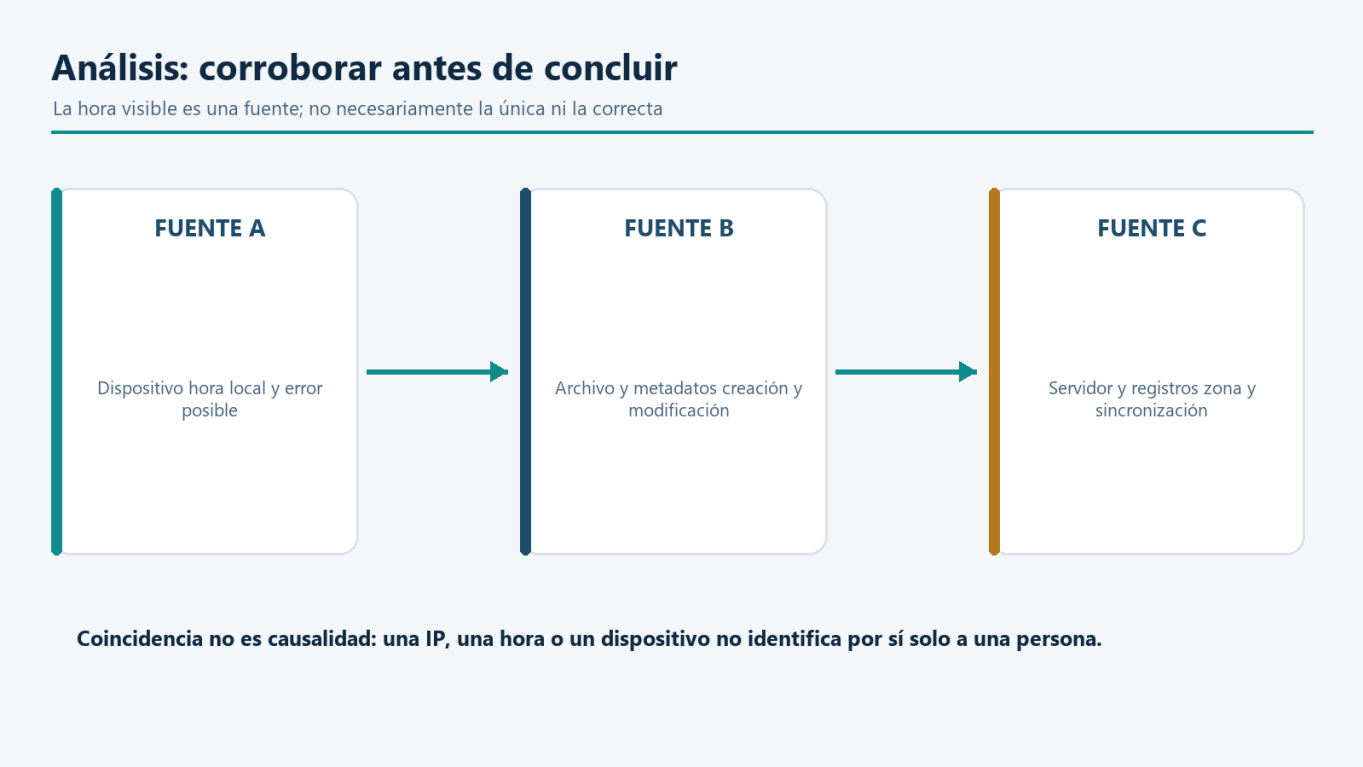


Figura 10. Convertir artefactos en explicaciones sin saltos de fe.

10.1 Preguntas antes que herramientas

El análisis comienza con afirmaciones que pueden ser confirmadas o debilitadas. Cada una se vincula con fuentes y pruebas. El objetivo no es encontrar una coincidencia y detenerse, sino buscar también explicaciones alternativas y resultados que puedan contradecir la primera versión.

Una matriz de hipótesis registra afirmación, fuente, método, hallazgo, alternativa y límite. Esta práctica reduce el riesgo de elegir artefactos por intuición y permite explicar por qué una conclusión cambió. La ausencia de evidencia en una fuente puede ser importante, pero se interpreta dentro de su cobertura.

Afirmación	Fuente y prueba	Alternativa	Resultado limitado
El video es una sola grabación continua.	Nombres, fechas, capítulos y continuidad.	Selección o conversión posterior.	La secuencia no sostiene continuidad en el alcance revisado.
La operación salió del dispositivo del titular.	Registros de acceso, dispositivo y sesión.	Credenciales usadas por otra persona.	Se acredita uso de credenciales, no identidad física.
No existió exfiltración.	Registros de red y transferencias.	Cobertura incompleta o canal cifrado.	No se observó en las fuentes revisadas.

10.2 Cronología y zonas horarias

Una cronología registra fecha, zona, fuente temporal y precisión. La hora del dispositivo puede estar mal configurada; la del archivo puede indicar creación, modificación o descarga; la del servidor puede seguir otra zona. Se conserva el valor original y la conversión, sin mezclarlos como si fueran el mismo evento.

Una secuencia de nombres puede orientar capítulos y continuidad, como ocurre en determinadas cámaras, pero no prueba por sí sola que el video sea completo. Se compara nomenclatura, fechas, estructura, contenido y procedencia. La ausencia de un capítulo es una pregunta, no una conclusión automática de edición maliciosa.

10.3 Lectura de sábanas y registros

En sábanas se revisan tipo de evento, inicio, duración, dirección, participantes, celdas y campos vacíos. Una llamada entrante no es lo mismo que una saliente, y una celda puede cambiar durante el evento. Los identificadores técnicos no equivalen automáticamente a personas. La lectura compara período y contexto, no solo coincidencias de número.

La ubicación de una celda no prueba la ubicación exacta de una persona. Requiere documentación de cobertura, tecnología, tiempo y otras fuentes. Si se afirma recorrido, se presentan niveles de precisión y alternativas. El análisis evita convertir un mapa atractivo en una certeza inexistente.

10.4 Repetibilidad y reproducibilidad

Repetibilidad busca el mismo resultado en el mismo entorno; reproducibilidad, en otro entorno documentado. ISO/IEC 27037 distingue ambas propiedades. El informe indica qué condiciones pueden cambiar: herramienta, versión, sistema, filtros o fuente. Una coincidencia entre herramientas no elimina una hipótesis común compartida.

El análisis registra resultados positivos, negativos e inconclusos. No se promete repetir lo que depende de un proveedor o de una fuente volátil. Se conservan consultas y salidas relevantes para que otra persona pueda comprobar el razonamiento y señalar errores.[1]

[1] ISO/IEC 27037:2012. Directrices para identificación, recolección, adquisición y preservación de evidencia digital. [fuente oficial]

Capítulo 11. Informe, presentación y contradicción

Explicar el trabajo con claridad y sin sobreactuar certeza.



Figura 11. Explicar el trabajo con claridad y sin sobreactuar certeza.

11.1 Estructura del informe

El informe comienza con encargo y alcance, identifica fuentes y objetos, explica método, presenta hallazgos, analiza alternativas, concluye dentro del alcance y declara límites. Los anexos contienen actas, manifiestos, hashes, registros y figuras. La conclusión responde las preguntas sin incluir nuevas acusaciones ni consejos jurídicos no solicitados.

La escritura distingue hechos observados, resultados de herramienta, inferencias y valoración jurídica. El lector debe saber de dónde sale cada afirmación. Una figura resume una secuencia o contradicción; no se utiliza para hacer que un informe parezca más técnico de lo que realmente es.

- Encargo, alcance y exclusiones.
- Objetos, procedencia y custodia.
- Herramientas, versiones y parámetros.
- Hallazgos con ubicación verificable.
- Hipótesis alternativas y resultados negativos.
- Conclusión, límites y anexos completos.

11.2 Lenguaje para público no técnico

Una explicación técnica puede ser precisa sin ser inaccesible. En lugar de “se efectuó la adquisición forense de evidencias”, se escribe “se creó una copia controlada del disco y se registró su integridad”. Los términos necesarios se definen una vez y se usan de forma consistente. Las siglas no sustituyen la explicación.

La presentación ejecutiva resume qué se revisó, qué se encontró y qué decisión puede tomarse. El detalle técnico queda disponible sin obligar al directivo a interpretarlo. La policía y el abogado deben poder seguir la secuencia sin conocer comandos; el especialista debe poder repetirla con los anexos.

11.3 Citas y normas

Una cita incluye instrumento, artículo, función, versión y fuente oficial. No se cita una ley por similitud de nombre ni se presenta una iniciativa como decreto. La equivalencia comparada se limita a función y alcance; no implica mismos efectos procesales. Cuando una norma fue derogada, se explica como antecedente histórico y no como regla vigente.

La revisión comprueba que la afirmación técnica y la cita hablan de lo mismo. Una regla de comprobantes no acredita toda autoría; una regla de conservación no certifica veracidad; una norma de incidentes no demuestra una transferencia concreta. La fuente no se usa como adorno de una conclusión que ya existía.

11.4 Revisión de contradicción

Antes de entregar, se pregunta si otra persona puede localizar el objeto, repetir la consulta, comprender el salto inferencial y encontrar las limitaciones. Las preguntas difíciles se responden con expediente, no con autoridad personal. Si algo no está documentado, se reconoce y se corrige el alcance.

La revisión incluye títulos, texto, anexos, imágenes y metadatos del archivo de entrega. No se afirma validación visual sin abrir el resultado final. Se calcula SHA-256 del archivo entregado y se conserva un manifiesto para que origen y destino puedan compararse sin confundirlo con la prueba del contenido.

Capítulo 12. Errores frecuentes y mejora continua

Evitar fallas conocidas y actualizar sin fabricar certeza.



Figura 12. Evitar fallas conocidas y actualizar sin fabricar certeza.

12.1 Errores que cambian casos

Los errores más costosos suelen ser sencillos: abrir por curiosidad, apagar por costumbre, capturar sin URL, exportar sin zona, confundir original con impresión, asignar una IP a una persona, presentar un hash como prueba total y citar una norma derogada. La prevención comienza con procedimientos claros y una primera respuesta entrenada.

Cuando el error ya ocurrió, se documenta sin inventar una cadena perfecta. Se evalúa qué cambió, qué puede verificarse todavía y qué conclusión debe limitarse. Reescribir actas anteriores para ocultarlo destruye confianza y puede afectar el expediente más que la falla original.

Error	Consecuencia	Respuesta correcta
Apagar por regla universal	Pérdida de memoria o sesiones.	Evaluar estado antes de decidir.
Antiestático como Faraday	Falsa sensación de aislamiento.	Usar y verificar aislamiento real.
Copiar hash en nota separada	Se pierde vínculo con la entrega.	Conservar EML, cuerpo y adjuntos.
Confiar en detector de IA	Falsa conclusión de origen o falsedad.	Corroborar con fuente, método y contexto.
Citar reforma antigua	Se afirma una norma inexistente.	Revisar vigencia y derogaciones.

12.2 Lecciones aprendidas

Una revisión posterior identifica qué falló en fuentes, decisiones, herramientas, comunicación y presentación. Las mejoras se asignan a responsables y se comprueban con ejercicios. No se fabrica evidencia de cumplimiento anterior: se registra cuándo entró en vigor la nueva práctica.

Una versión nueva del manual conserva historial y motivo del cambio. Si una plataforma modifica su exportación, se actualiza el capítulo 6 o 8; si cambia una ley, se actualiza el anexo A y el registro M. Las notas contradictorias no se apilan sin revisar el cuerpo principal.

12.3 Guía mínima para toda la organización

La organización debe poder responder cinco preguntas sin depender de una sola persona: quién autoriza, dónde está la evidencia, cómo se obtuvo, quién la ha tocado y qué puede afirmarse. Si alguna no tiene respuesta, el plan indica cómo recuperarla o cómo limitar la conclusión.

El manual se usa como punto de partida, no como manuscrito inmutable. La práctica se adapta al caso, se documenta y se revisa. La meta es que cualquier equipo pueda trabajar con orden, compartir conocimiento y sostener una explicación, incluso cuando el resultado no sea el esperado.

Anexo A. Matriz jurídica funcional resumida

Localizar la función sin inventar equivalencias entre países.

A.1 Cómo leer la comparación

Equiparable significa equivalencia funcional, no identidad de contenido, presunciones, sujetos, plazos o efectos procesales. La matriz completa se entrega como archivo independiente para poder actualizarla sin rehacer el manual. Antes de aplicar una regla se comprueba instrumento, artículo, ámbito subjetivo, canal, materia y versión al momento del hecho.

La tabla resume instrumentos de partida, no un catálogo exhaustivo. Si una función no quedó acreditada en la investigación, se marca así y no se rellena por analogía. Las reglas civiles, penales, administrativas, archivísticas y financieras no son intercambiables.[3][4][10][11][12][13][14][15][16]

Jurisdicción	Base funcional de partida	Advertencia principal
México	CCom 89–94 y 1205; CNPCF 348–350; NOM-151; CNBV 316 Bis y serie.	Transición gradual; cada artículo CNBV tiene objeto y plazo distintos.
Perú	Ley 27269 y Reglamento; CPC 188–197; régimen archivístico; SBS 504-2021 y 2286-2024.	El régimen está distribuido; no atribuir todo a la Ley 27269.
Chile	Ley 19.799; RAN 20-7, 20-8 y 20-10.	Firma avanzada y fecha no son la misma cuestión.
Argentina	Ley 25.506; CCyC 318–319; BCRA A 7783 y A 8280.	Presunciones solo en su régimen; revisar derogaciones.
Colombia	Ley 527; CPACA; instrucciones SFC aplicables.	Conservar origen, destino, fecha y hora; confirmar numerales SFC.
Ecuador	Ley 67; Resolución JPRM-2025-006-M para pagos.	El sistema de pagos no reproduce toda la CNBV.
España / UE	eIDAS; LEC 326 y 384; RD-ley 19/2018, 45, 66 y 67.	Firma simple, avanzada y cualificada no tienen idénticos efectos.

[3] Código de Comercio de México, artículos 89–94 y 1205, compilación oficial. [fuente oficial]

[4] Código Nacional de Procedimientos Civiles y Familiares, artículos 348–350, compilación consultada con reforma del 15-01-2026. [fuente oficial]

[10] Perú. Ley 27269 y Reglamento de Firmas y Certificados Digitales. [fuente oficial]

[11] Chile. Ley 19.799 sobre documentos electrónicos y firma electrónica. [fuente oficial]

[12] Argentina. Ley 25.506 de Firma Digital. [fuente oficial]

[13] Colombia. Ley 527 de 1999 sobre mensajes de datos y comercio electrónico. [fuente oficial]

[14] Ecuador. Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos. [fuente oficial]

[15] España. Ley de Enjuiciamiento Civil, artículos 326 y 384, texto consolidado. [fuente oficial]

[16] México. Disposiciones de carácter general aplicables a las instituciones de crédito, artículos 316 Bis y serie. [fuente oficial]

A.2 Método de actualización

La actualización registra fuente oficial, fecha de consulta, artículo leído y cambio operativo. No se sustituye una norma por una noticia ni una iniciativa por un decreto. La matriz completa conserva citas para reconocimiento, escritura, atribución, integridad, original, accesibilidad, conservación, admisibilidad, carga probatoria y regulación financiera.

ISO/IEC 27037 y NIST SP 800-86 se citan como metodología, no como legislación nacional. La función del anexo es orientar qué preservar, solicitar, verificar y limitar, no resolver un expediente con una tabla de frases similares.[1][2]

[1] ISO/IEC 27037:2012. Directrices para identificación, recolección, adquisición y preservación de evidencia digital. [fuente oficial]

[2] NIST SP 800-86. Guide to Integrating Forensic Techniques into Incident Response. [fuente oficial]

Anexo B. Ficha de alcance y autoridad

Formulario inicial para delimitar el trabajo.

B.1 Formato

Se completa antes de actuar. Si un dato no está disponible, se escribe el motivo y la persona que debe confirmarlo. No se dejan vacíos críticos para completar después de la adquisición.

Campo	Contenido que se registra	Ejemplo ficticio
Identificador	Código único del encargo.	EXP-DEMO-2026-001
Pregunta	Hecho que se necesita acreditar.	Determinar si las ventas fueron transmitidas y liquidadas.
Período	Inicio, fin y zona horaria.	1–3 nov 2026, UTC−06:00.
Fuentes incluidas	Sistemas, archivos y custodios autorizados.	Remesa, procesador y reportes bancarios.
Exclusiones	Datos o dispositivos fuera del mandato.	Dispositivos personales no relacionados.
Autorización	Titular, acciones y canal.	Dirección autorizada; canal seguro registrado.
Entregable	Tipo de informe y anexos.	Informe técnico, manifiesto y actas.
Riesgos	Alteración, pérdida y confidencialidad.	Rotación de registros y datos de terceros.

Anexo C. Acta de recepción

Documentar el estado antes de cualquier análisis.

C.1 Datos mínimos

El acta se acompaña de fotografías generales y de identificadores. Las acciones previas se registran incluso si fueron incorrectas; no se corrige retrospectivamente para aparentar una recepción ideal.

Campo	Contenido requerido
Objeto e identificador	Tipo, marca, modelo, serie, capacidad y código asignado.
Entrega y recepción	Nombre, función, fecha, hora, zona y lugar.
Estado	Encendido, bloqueo, red, daño y accesorios.
Sello y embalaje	Tipo, identificador, condición y fotografías.
Acciones previas	Aperturas, conexiones, copias, cambios o desconocidos.
Riesgos	Volatilidad, borrado remoto, datos de terceros y prioridad.
Decisión inicial	Preservar, escalar, adquirir o solicitar aclaración y responsable.

Anexo D. Registro de adquisición

Relacionar fuente, método, salida y verificación.

D.1 Registro por objeto

Cada adquisición tiene un registro propio. Si se repite, se asigna un nuevo identificador relacionado y se explica el motivo sin eliminar el primer intento.

Campo	Contenido requerido
Fuente y custodio	Identificador exacto y persona que la conserva.
Método y justificación	Físico, lógico, volátil, remoto o documental y razón.
Herramienta	Nombre, versión, entorno y validación.
Parámetros	Filtros, campos, fecha, zona y configuración.
Salida	Nombre, ruta, formato, tamaño y relación original/copia.
Integridad	Algoritmo, valor, fecha y objeto cubierto.
Incidencias	Errores, omisiones, sectores, accesos y efecto en el alcance.
Verificación	Apertura, comparación, repetición y revisor.

Anexo E. Cadena de custodia y transferencias

Reconstruir cada acceso y movimiento.

E.1 Registro por evento

Se registra también la apertura de un contenedor, la descarga remota y la copia de trabajo. La transferencia no termina hasta confirmar recepción y condición del objeto.

Fecha y zona	Objeto	Entrega	Recepción	Propósito	Sello/integridad
09 nov 14:32 −06	ED-DEMO-003	Custodio A	Analista B	Adquisición	Sello 01 íntegro
09 nov 16:05 −06	ED-DEMO-003-A00	Analista B	Custodio C	Resguardo	Hash coincidente
10 nov 09:10 −06	ED-DEMO-003-A01	Custodio C	Revisor D	Revisión	Acceso registrado

Anexo F. Solicitud a proveedor y entrega EML

Asegurar formato, contexto e integridad en registros remotos.

F.1 Campos de la solicitud

La solicitud se adapta al proveedor y al canal autorizado. La contraseña o credencial no se escribe en el acta ni en el cuerpo. El canal seguro se identifica por referencia, no por secretos.

Elemento	Contenido que debe constar
Expediente y autorización	Código, titular y referencia al canal seguro.
Cuenta y alcance	Identificadores autorizados, período, zona y exclusiones.
Formato	Nativo disponible y copia de consulta, diccionario y proceso de extracción.
Integridad	Algoritmo y hash de cada archivo en el cuerpo de la respuesta.
Entrega	EML con cuerpo, encabezados y adjuntos; enlace y permisos si aplica.
Limitaciones	Retención, campos ausentes, cobertura, errores y aclaraciones.

F.2 Verificación al recibir

Se guarda el EML antes de trabajar con adjuntos. Se calculan hashes de EML y archivos por separado y se comparan con el cuerpo. Las diferencias se registran y solicitan aclaración. La ausencia de hash del proveedor se anota y se calcula uno local sin atribuirlo al proveedor.

1. EML completo preservado y legible.
2. Archivos nativos recibidos y relacionados con el cuerpo.
3. Algoritmo y valores comparados y registrados.
4. Campos, unidades, zona y proceso de extracción comprendidos.
5. Limitaciones y discrepancias documentadas.

Anexo G. Inventario y manifiesto de archivos

Mantener relación entre origen, derivados y entregables.

G.1 Columnas del manifiesto

El manifiesto reúne identificador, nombre, ruta, tipo de objeto, origen, método, tamaño, formato, hash y observaciones. No publica datos sensibles ni secretos. La ruta puede abreviarse en la versión pública si revela información protegida.

Identificador	Relación	Archivo	Formato	Integridad
ED-DEMO-003	Original recibido	sabanas.csv	CSV	SHA-256 calculado en recepción
ED-DEMO-003-A00	Entrega relacionada	entrega.eml	EML	Objeto independiente del CSV
ED-DEMO-003-A01	Copia de trabajo	sabanas_trabajo.csv	CSV	Hash distinto si cambia estructura
ED-DEMO-003-R01	Presentación	informe.pdf	PDF	Hash del archivo entregado

Anexo H. Cronología y zonas horarias

Evitar conversiones ocultas y falsas coincidencias.

H.1 Tabla de correlación

Se conserva el valor original de cada fuente y se añade la conversión sin sustituirlo. Si la hora del dispositivo no es fiable, se indica el desfase conocido o la incertidumbre.

Evento	Fuente temporal	Valor original	Zona	Conversión y límite
Captura de video	Reloj del dispositivo	06:04:16	Desconocida	No asumir UTC; comparar con otra fuente.
Exportación	Servidor	2026-11-01T12:04:16Z	UTC	06:04:16 en UTC−06; registrar horario de verano.
Recepción EML	Cliente de correo	09 nov 07:05	UTC−06	Hora de recepción, no del hecho investigado.

Anexo I. Matriz de hipótesis y análisis

Documentar confirmación, alternativa y límite.

I.1 Plantilla de razonamiento

Cada afirmación se somete a fuentes capaces de confirmarla o debilitarla. El revisor añade alternativas que el analista no había considerado y se registra cómo cambia la conclusión.

Afirmación	Fuente/prueba	Alternativa	Resultado
El archivo es original.	Procedencia, metadatos y custodia.	Exportación o edición previa.	Se acredita solo la representación recibida.
El usuario autorizó la operación.	Autenticación, dispositivo y sesión.	Credenciales comprometidas.	Uso de credenciales no equivale a identidad física.

Afirmación	Fuente/prueba	Alternativa	Resultado
No existen otros archivos.	Consulta y cobertura documentadas.	Filtro, retención o formato.	No se observaron en el alcance consultado.

Anexo J. Revisión de contenido sintético

Separar generación, edición, conversión y publicación.

J.1 Expediente mínimo

El objetivo no es declarar “deepfake” por apariencia. Se registra cada transformación conocida, su evidencia y sus límites. El detector se identifica con versión y error conocido cuando esté disponible; no se usa como única prueba.

1. Archivo original recibido y procedencia.
2. Herramienta, versión e historial de generación/edición disponibles.
3. Códec, compresión, metadatos y versiones comparados.
4. URL, publicación, etiqueta, audiencia y contexto.
5. Consentimiento, identidad, finalidad y norma vigente revisados.
6. Detectores y corroboración con límites explícitos.

Anexo K. Plantilla de informe técnico

Presentar hallazgos sin mezclar hechos e inferencias.

K.1 Estructura de redacción

El informe final incluye portada, identificación del encargo, índice, resumen ejecutivo, alcance, fuentes, método, hallazgos, análisis, conclusión, límites y anexos. Cada afirmación tiene una ubicación de evidencia y una formulación acorde con su fuerza.

Apartado	Contenido que debe responder
Encargo	Qué se solicitó, para qué y con qué exclusiones.
Fuentes	Qué se recibió, de quién y en qué representación.
Método	Qué se hizo, con qué herramienta y parámetros.
Hallazgos	Qué se observó y dónde puede localizarse.
Análisis	Qué explicaciones son compatibles o quedan debilitadas.
Conclusión	Qué puede afirmarse dentro del alcance.
Límites	Qué no se demostró y qué fuentes faltan.
Anexos	Actas, manifiesto, hashes, registros y figuras.

Anexo L. Listas de verificación

Comprobar el trabajo antes de cada entrega.

L.1 Recepción y adquisición

La lista se marca con evidencia, no con intención. Si un punto no aplica, se escribe el motivo y su aprobación. No se deja un criterio crítico sin respuesta.

1. Autoridad, alcance y exclusiones documentados.
2. Objeto, estado, fotografías y responsables identificados.
3. Método justificado por fuente y riesgo.
4. Herramienta, versión y parámetros registrados.
5. Hashes, EML y archivos relacionados preservados.
6. Incidencias y límites incluidos en el expediente.

L.2 Informe y publicación

La revisión final se hace sobre el archivo abierto, no sobre el borrador de trabajo. Las imágenes se revisan en tamaño completo y miniatura cuando se utilicen para publicación.

1. Conclusión coherente con fuentes y alcance.
2. Citas vigentes, artículos y funciones verificados.
3. Sin nombres de clientes, credenciales ni datos innecesarios.
4. Índice, figuras, tablas y anexos legibles.
5. Archivos finales abiertos y revisados visualmente.
6. SHA-256 de origen y destino coincidentes y manifiesto conservado.

Anexo M. Control de versiones normativas y del manual

Actualizar sin acumular contradicciones.

M.1 Registro de cambios

Cada cambio normativo o metodológico registra fuente, fecha, capítulo afectado, decisión editorial y revisor. Si una norma es derogada, se modifica el texto principal y las preguntas frecuentes, no solo se añade una nota al final.

Fecha	Fuente	Cambio	Acción editorial	Revisión
30 jul 2026	Gaceta SLP	187 Ter, 272 Bis y 272 Ter derogados.	Explicar como antecedente histórico; actualizar posts y anexo A.	Completa
27 jul 2026	EUR-Lex	Texto consolidado del Reglamento de IA consultado.	Citar artículo 50 con ámbito y excepciones correctas.	Completa
09 nov 2026	Manual	Revisión de lenguaje y formatos.	Incorporar EML, sábanas y listas para primera respuesta.	Completa

M.2 Cierre de uso

Este manual es una guía general. No constituye asesoría legal ni dictamen pericial sobre un caso concreto. La aplicación exige analizar autoridad, jurisdicción, hechos, canal y norma vigente. La versión se entrega con recursos y matriz independiente para que las actualizaciones puedan revisarse sin perder el diseño del volumen.