ACCCF

CONOCIMIENTO APLICADO · HISPANOAMÉRICA

MANUAL HISPANO DE EVIDENCIA DIGITAL

2026 V1

Preservar, comprobar y explicar la evidencia en Hispanoamérica.



Elaboró y firmó

Jocsan Laguna Romero

Presidente del ACCCF

Emisión institucional del Consejo

CONSEJO DEL ACCCF

EDICIÓN LIBRE · 2026

Contenido

Guía técnica general. No constituye asesoría legal ni dictamen pericial. Los ejemplos son ficticios o anonimizados; las figuras son reconstrucciones editoriales.
La paginación visible corresponde a la edición PDF. Word puede actualizar este índice al abrir el documento; los títulos conservan navegación interna.

Presentación del manual 6
Cómo usar este manual 7
Capítulo 1. Alcance, preguntas y autoridad 8
1.1 La pregunta que ordena el trabajo 8
1.2 Autoridad antes que acceso 8
1.3 Inventario inicial de fuentes 9
1.4 Ejemplo completo: una reclamación por ventas 10
1.5 Fundamento y cierre: el método también protege a las personas 11
Capítulo 2. Integridad, original y contexto 13
2.1 El original no siempre es el dispositivo 13
2.2 Integridad, autenticidad, atribución y veracidad 13
2.3 El hash como control, no como dogma 14
2.4 Metadatos internos y fechas del sistema: una distinción que evita errores 15
2.5 El caso de las fotografías y la banca 16
2.6 Accesibilidad y conservación de contexto 16
Capítulo 3. Roles, responsabilidades y decisiones 18
3.1 Funciones antes que cargos 18
3.2 La primera respuesta sin improvisación 18
3.3 Comunicación operativa 19
3.4 Independencia, privacidad y terceros 20
3.5 Un silogismo de roles 20
Capítulo 4. Ciclo de vida y preparación forense 22
4.1 Preparar antes de recibir el caso 22
4.2 Puntos de no retorno 23
4.3 Ciclo documentado y entregables 25
4.4 Retención y análisis longitudinal 25
4.5 Preparación como responsabilidad social 26
Capítulo 5. Árboles de decisión por escenario 27
5.1 Equipo encendido o apagado 27
5.2 Adquisición local, remota o por proveedor 27
5.3 Dispositivos móviles y aislamiento 28
5.4 Discos ópticos: identificador y formato 29
5.5 Cuándo detenerse 30

5.6 El árbol como razonamiento, no como decoración 31
Capítulo 6. Fuentes modernas y sábanas de llamadas 33
6.1 Nube, SaaS y exportaciones 33
6.2 Correo electrónico y EML 34
6.3 Solicitud y recepción de sábanas de llamadas 35
6.4 Ejemplo de cuerpo de solicitud al proveedor 35
6.5 Virtualización, IoT y contenido sintético 36
6.6 Vigencia: el ejemplo de una reforma derogada 38
6.7 La fuente no vive en un solo lugar 38
Capítulo 7. Recepción y preservación inicial 40
7.1 Acta de recepción comprensible 40
7.2 Embalaje y sellado 41
7.3 Etiquetas y relación entre objetos 42
7.4 Accesorios y conexiones como parte de la recepción 43
7.5 Recepción de archivos y mensajes 44
Capítulo 8. Adquisición y documentación técnica 45
8.1 Física, lógica, volátil y documental 45
8.2 Conexión real: fuente, bloqueador y estación 45
8.3 Medios y adaptadores: NVMe, SATA y discos ópticos 46
8.4 Adquisición lógica y manifiesto 47
8.5 Memoria en vivo y validación de herramientas 48
8.6 Exportaciones y consultas reproducibles 49
8.7 Errores e incidencias 49
Capítulo 9. Custodia, traslado y conservación 51
9.1 La cadena que responde preguntas 51
9.2 Transferencias electrónicas y llaves 51
9.3 Almacenamiento y acceso posterior 52
9.4 Apertura y reemplazo de sello 53
9.5 Accesos, custodia compartida y conflictos 54
Capítulo 10. Examen, cronología e hipótesis alternativas 56
10.1 Examinar no es encontrar un culpable 56
10.2 Metadatos: escuchar al archivo sin creerle todo 56
10.3 Cronología: ordenar relojes antes de ordenar historias 58
10.4 Antenas, cobertura y azimut: geografía sin atajos 59
10.5 Corroboración que sí discrimina 61
10.6 Matriz de hipótesis: permitir que la evidencia contradiga 62
10.7 Repetir, reproducir y saber cuándo parar 63
Capítulo 11. Informe, razonamiento y contradicción 65
11.1 El informe es la ruta de regreso a la fuente 65
11.2 Hecho, resultado, inferencia y opinión 66

11.3 El silogismo y la falsa consecuencia 66
11.4 Explicar contradicciones sin esconderlas 67
11.5 Redactar conclusiones que caben en la evidencia 67
11.6 Contradicción y revisión independiente 68
11.7 Entrega, anexos y acceso posterior 69
Capítulo 12. Errores, aprendizaje y servicio público 71
12.1 El error no se corrige reescribiendo el pasado 71
12.2 Errores de recepción y preservación 71
12.3 Errores de fuente, captura y exportación 72
12.4 Errores de interpretación 73
12.5 Errores jurídicos y de vigencia 74
12.6 Lecciones aprendidas que cambian el procedimiento 75
12.7 La medida final: evitar el próximo abuso 76
Anexo A. Equivalencias jurídicas funcionales 77
Resumen ejecutivo 77
1. Método y límites de la comparación 77
2. Matriz central por función jurídica 78
3. México: base normativa y transición 85
4. Perú: régimen distribuido y actualización financiera 87
5. Chile: firma, fecha y regulación de seguridad 89
6. Argentina: presunciones delimitadas y confiabilidad del soporte 90
7. Colombia: mensajes de datos, conservación y acuses 91
8. Ecuador: equivalencia documental y sistema de pagos 92
9. España y Unión Europea: no discriminación, servicios de confianza y proceso 92
10. Comparación funcional de registros e incidentes financieros 94
11. Estándares metodológicos internacionales 97
12. Reglas para usar la matriz sin cometer falsas equivalencias 98
A.13 Aplicación práctica: seleccionar régimen antes que conclusión 99
A.14 Protección de datos durante la investigación en México 100
Anexo B. Ficha de alcance y autoridad 101
B.1 Contenido del formato 101
Anexo C. Acta de recepción y preservación inicial 103
C.1 Ejemplo de acta física 103
C.2 Recepción de archivos o mensajes 104
Anexo D. Registro de adquisición 105
D.1 Ejemplo completo 105
Anexo E. Cadena de custodia y transferencias 107
E.1 Ejemplo de secuencia 107
E.2 Transferencia electrónica 107
Anexo F. Solicitud y adquisición mediante proveedor 108

F.1 Solicitud modelo 108
F.2 Registro de exportación o API 108
Anexo G. Inventario y manifiesto de objetos 110
G.1 Ejemplo de manifiesto 110
Anexo H. Cronología y zonas horarias 111
H.1 Ejemplo de línea de tiempo 111
H.2 Regla para fechas contradictorias 111
Anexo I. Matriz de hipótesis y corroboración 112
I.1 Ejemplo desarrollado 112
Anexo J. Revisión de contenido sintético 114
J.1 Formato aplicado 114
Anexo K. Estructura de informe y conclusión 115
K.1 Secuencia recomendada 115
K.2 Ejemplo de conclusión completa 116
Anexo L. Listas de verificación operativa 117
L.1 Recepción y adquisición 117
L.2 Análisis, informe y entrega 117
Anexo M. Control de versiones, fuentes y lecciones 119
M.1 Registro normativo y técnico 119
M.2 Lección convertida en mejora 119

Presentación del manual

Preservar evidencia digital no consiste en guardar archivos hasta que parezcan suficientes. Consiste en proteger la posibilidad de que otra persona, con otro criterio y otras herramientas, pueda llegar a una conclusión compatible con los hechos. Un dispositivo no sustituye a un testigo; una captura no sustituye al archivo; una opinión no sustituye al método. El trabajo comienza mucho antes de abrir el primero de ellos: comienza cuando alguien decide qué afirmación necesita demostrar y qué consecuencias tendrá actuar.

Este manual nace de una pregunta incómoda pero necesaria: ¿cuántos abusos podrían evitarse si la primera persona que recibe la evidencia hiciera bien las cosas más simples? Identificar el objeto, fotografiar su estado, delimitar la autorización, pedir el archivo nativo, conservar el mensaje completo, anotar la fecha y la zona, no confundir una antena con una persona, no presentar una intuición como si fuera ciencia. Los cimientos no son ornamentos. Son los que impiden que una acusación se construya sobre una suposición y que una defensa se desmorone por una omisión evitable.

La regla que ordena todo lo demás puede escribirse así: fuente, autoridad, estado, método, registro, verificación y conclusión limitada. Primero se identifica qué puede aportar información. Después se comprueba quién puede autorizar el acceso y en qué condiciones. Se documenta el estado en que el objeto llega, se elige un método adecuado y se deja constancia. Solo entonces se verifica y se concluye dentro de lo que las fuentes permiten. Si una fase falla, la siguiente no se arregla con retórica: se reconoce la limitación y se decide qué puede recuperarse sin fabricar una historia perfecta.

El realismo mágico, aquí, no es adorno literario. Es aceptar que los objetos cotidianos pueden narrar algo extraordinario: una banca puede describir una pausa, un anillo central puede identificar un disco, una bolsa puede dar una falsa sensación de aislamiento, un reloj puede contradecir a otro reloj. Las analogías son puentes para entender, no sustitutos de la prueba. La seriedad está en regresar siempre a la fuente y preguntar qué puede demostrar y qué solamente parece sugerir.

Propósito de esta obra

Ofrecer cimientos para que nadie tenga que aprender evidencia digital a golpes. Compartir un método que pueda ser utilizado por policía, peritos, abogados, ingenieros y responsables de organizaciones, sin ocultar las decisiones difíciles ni las zonas de incertidumbre.

Los ejemplos son ficticios o están anonimizados. Las imágenes son reconstrucciones editoriales: muestran dispositivos y acciones, no constituyen evidencia real de los casos. Las normas se citan con función, artículo, ámbito y fecha de consulta. Cuando una equivalencia entre países es solo parcial o sectorial, se escribe así, porque una frase parecida no produce el mismo efecto jurídico.

Cómo usar este manual

Si eres la primera persona que recibe el caso, empieza por los capítulos 1, 3, 5 y 7. Allí se explica cómo delimitar el encargo, asignar funciones, elegir una ruta según el estado del objeto y registrar la recepción sin improvisar. No necesitas convertirte en analista para evitar los primeros errores: necesitas saber qué preservar y cuándo pedir ayuda.

Si adquieres o analizas, trabaja los capítulos 4, 6, 8, 9 y 10. La parte técnica explica cómo seleccionar fuentes, documentar adquisiciones, comprobar archivos, construir cronologías y evaluar hipótesis alternativas. Si presentas o revisas, utiliza los capítulos 2, 11 y 12 y los anexos jurídicos y operativos. El objetivo no es repetir un procedimiento sino comprender por qué cada decisión deja una traza útil.

Los formatos no son un fin en sí mismos. Un acta vacía con un nombre bonito puede seguir siendo una pseudo custodia, igual que una fotografía sin URL puede ser solo una imagen incompleta. Cada formato debe capturar una decisión o una comprobación: qué se autorizó, qué se recibió, qué cambió, quién lo verificó y qué límites existen. Si un campo no ayuda a responder eso, se elimina.

La lectura debe ser acumulativa. Los conceptos regresan porque cada uno añade una capa: una fuente puede ser original en un sentido limitado, una exportación puede ser mejor fuente que el dispositivo, una antena describe cobertura y no una dirección, una firma puede tener fuerza sin demostrar qué mano pulsó el botón. No avances deprisa hacia los comandos. La velocidad llega cuando el criterio ya es claro.

Capítulo 1. Alcance, preguntas y autoridad

1.1 La pregunta que ordena el trabajo

Un encargo pobremente formulado produce una investigación inflada. “Revisa todo” no indica qué debe demostrarse, para qué se usará el resultado ni qué riesgo de alteración es aceptable. En cambio, una pregunta precisa permite decidir qué fuentes son necesarias y cuáles no deben tocarse: qué operaciones se reclaman, en qué período, de qué sistemas y con qué consecuencia jurídica o empresarial.

Escribe las versiones por separado. Una parte afirma haber realizado ventas no pagadas; la otra sostiene que no recibió esas operaciones. No las mezcles en una sola historia. La primera hipótesis no debe convertirse en una orden de búsqueda solo para encontrar lo que la confirma. La segunda no debe descartarse por resultar incómoda. La función del método es permitir que ambas puedan someterse a prueba, no ayudar a una de ellas a ganar por anticipado.

La recuperación para continuidad operativa no tiene el mismo nivel de exigencia que una pericial destinada a contradicción judicial. En la primera puede bastar una copia controlada que permita volver a trabajar. En la segunda necesitas autoridad, integridad, contexto, trazabilidad, posibilidad de revisión y una explicación que no dependa del prestigio de quien firma. Confundir esos objetivos produce dos errores: hacer demasiado para una recuperación sencilla o hacer demasiado poco para una afirmación que tendrá consecuencias serias.

Pregunta	Qué debe quedar escrito	Decisión que evita improvisar
¿Qué afirma cada parte?	Versión separada por persona, hecho y fecha.	No tratar una versión como hecho probado.
¿Qué se necesita acreditar?	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 quedar fuera?	Datos, dispositivos, cuentas o períodos excluidos.	Reducir exposición innecesaria.

1.2 Autoridad antes que acceso

Poder abrir un archivo no significa poder revisarlo. La autorización debe indicar titular, acciones permitidas, sistemas, responsables, exclusiones y canal de comunicación. Si hace falta acceder a información de terceros, a una cuenta compartida o a un proveedor, se documenta la vía legítima. La capacidad técnica no crea autoridad; solo permite ejecutar lo que la autoridad permite.

La proporcionalidad pregunta si la fuente y el método son necesarios para el objetivo. Una exportación administrativa puede responder mejor que una revisión completa del dispositivo, con menos alteración y menos exposición. Recolectar todo no es exhaustividad: puede ser ruido, exposición de datos y una forma elegante de perder la pregunta. Si existe una fuente con mayor capacidad discriminatoria y menor intrusión, esa es la candidata inicial.
La confidencialidad se decide desde la recepción, no al final del informe. Se determina quién puede ver, copiar, transferir y publicar información, especialmente cuando hay datos de terceros, menores, víctimas o secretos comerciales. En materia de datos personales, el tratamiento debe ser lícito, limitado a finalidades informadas y adecuado a lo necesario, con medidas de seguridad y confidencialidad proporcionadas al riesgo. La nueva ley también obliga a informar de inmediato las vulneraciones significativas para que las personas puedan defenderse.[1]

Regla de actuación
Si la autoridad o el alcance no están claros, se detiene la acción y se aclara. Registra la duda, la respuesta recibida, quién la dio y cuándo. "No sabía si podía" no es una custodia defendible.

1.3 Inventario inicial de fuentes

Haz una lista de dispositivos, cuentas, archivos, servidores, proveedores, documentos y personas que pueden aportar contexto. Incluye lo que no está disponible 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. Un expediente incompleto no debe disfrazarse como un universo completo.
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. La navaja de Ockham empieza por la fuente que mejor discrimina, no por la que acumula más prestigio técnico.

Campo del inventario	Ejemplo de registro útil	Por qué importa
Identificador y custodio	Remesa comercial, procesador, banco y responsable autorizado.	Evita solicitar datos al custodio equivocado.
Tipo, período y formato	Operaciones de una semana, CSV nativo y diccionario de campos.	Permite comparar estructura y significado.

[1]Ley Federal de Protección de Datos Personales en Posesión de los Particulares, nueva ley publicada el 20-03-2025 y reformada el 14-11-2025. Artículos 5–9, 18–20 y 31: principios, seguridad, confidencialidad, vulneraciones y plazos. Fuente oficial en línea

Campo del inventario	Ejemplo de registro útil	Por qué importa
Disponibilidad	Archivo ausente, enlace activo o proveedor pendiente.	Declara límites desde el inicio.
Riesgo	Rotación, borrado remoto, exposición de terceros o pérdida física.	Define prioridad y método.
Autorización y contacto	Titular, canal seguro y suplencia.	Evita accesos dudosos y demoras sin registro.

1.4 Ejemplo completo: una reclamación por ventas

Una cadena comercial afirma que realizó ventas que no fueron pagadas. La pregunta 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. Cada fuente responde una parte distinta de la secuencia.

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. Podría tratarse de operaciones inexistentes, de una remesa incompleta, de otro canal o de una exportación defectuosa. La conclusión responsable empieza por la ausencia documentada en la fuente, no por una acusación dirigida al primer sospechoso disponible.



Figura 1. Delimitar fuentes antes de actuar: qué puede revisarse y qué queda fuera. Reconstrucción editorial; no constituye evidencia real.

Lo que el ejemplo enseña
Una pregunta bien delimitada evita una revisión invasiva de dispositivos personales y obliga a comparar fuentes independientes. La evidencia no se acumula por volumen: se selecciona por su capacidad para resolver una afirmación.

1.5 Fundamento y cierre: el método también protege a las personas

La identificación, recolección, adquisición y preservación no son solo operaciones técnicas. ISO/IEC 27037 las presenta como decisiones que deben documentarse para permitir revisión posterior. La fuente y la autoridad condicionan el método; no hay acceso legítimo solo porque alguien tenga una contraseña o un dispositivo en la mano. Esta secuencia también evita que una investigación se convierta en una segunda lesión para las personas afectadas.[2]

En México, la información electrónica puede admitirse como prueba cuando se acredita la fiabilidad del método, la atribución, la accesibilidad y la integridad. Esa exigencia no se

[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

satisface con una captura aislada ni con la afirmación de que un perito vio algo en una pantalla. Debe poder explicarse cómo se generó, comunicó, recibió o archivó la información y cómo se mantuvo íntegra desde su generación. La precisión delimita lo que puede afirmarse después.[3][4]

Conclusión limitada

Antes de tocar evidencia debes poder responder qué afirmación se investiga, quién autoriza, qué fuentes discriminan mejor, qué exclusiones protegen a terceros y qué resultado esperas. Si alguna respuesta falta, el primer entregable no es una adquisición: es una aclaración documentada.

[3]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

[4]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

Capítulo 2. Integridad, original y contexto

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. La pregunta no es solamente "¿tengo el objeto?", sino "¿qué puedo demostrar con esta representación?".

Una imagen bit a bit del medio puede conservar sectores asignados y no asignados; una exportación lógica puede conservar solo ciertos archivos; una captura puede mostrar una visualización sin conservar estructura ni metadatos; una impresión puede legibilizar el contenido sin ofrecer el archivo original. Ninguna es universalmente superior. La elección depende de la pregunta y de la necesidad de revisión. No destruyas el objeto de origen para producir una representación que luego resulte insuficiente.

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.[56]

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. Incluso una secuencia criptográficamente correcta puede necesitar una explicación sobre quién controlaba la clave y el dispositivo en ese momento.

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

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

Afirmación segura	Evidencia requerida	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. Un hash recién calculado solo acredita integridad desde el momento en que se calcula.

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.”



Figura 2. El hash compara objetos; no certifica autoría ni veracidad del contenido. Reconstrucción editorial; no constituye evidencia real.

2.4 Metadatos internos y fechas del sistema: una distinción que evita errores

Las propiedades que muestra el sistema operativo pueden reflejar cuándo un archivo fue copiado, descargado o modificado en ese equipo, no cuándo fue creado originalmente. Esas fechas no son inútiles: ayudan a reconstruir la historia de ese objeto en ese sistema. El error consiste en presentarlas como si fueran la fecha de captura original sin ninguna otra comprobación. Hay que leer qué significa cada campo, en qué sistema y para qué afirmación. Los metadatos internos de una fotografía pueden incluir fecha de captura, modelo de dispositivo y coordenadas cuando estaban habilitadas. Herramientas como ExifTool permiten leerlos. Pero tampoco son inmutables ni prueban por sí solos que la escena ocurrió tal como se describe. Un archivo puede ser editado, sus metadatos pueden cambiar y un dispositivo puede tener una hora incorrecta. La fecha de captura es una fuente que debe corroborarse con otras: contenido, registros de aplicación, respaldos, ubicaciones, secuencia y testimonios. La NOM-151 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. La fecha visible es solo el comienzo de una pregunta más rigurosa.[7]

2.5 El caso de las fotografías y la banca

En un caso analizado por el autor, un juego de fotografías aportaba fecha y coordenadas compatibles con una ubicación diferente a la señalada por una acusación. El acelerómetro del teléfono mostraba además una pausa compatible con el momento en que una persona dijo haberse sentado en una banca. La importancia no estaba en la banca como objeto, sino en la pausa: un patrón cotidiano que ayudaba a revisar una versión sin recurrir a una interpretación dramática.

Los sensores no registraron la tristeza ni la intención, y tampoco convirtieron los datos en una certeza metafísica. Pudieron ser consistentes con una secuencia, pero la conclusión necesitaba corroboración: fotografías, mensajes, desplazamientos, fuentes de nube, testimonios y revisión de si los datos fueron generados por sensores o introducidos manualmente. La ciencia no se expresa como “el celular dijo la verdad”, sino como “estas fuentes, por su origen y comportamiento, resultan compatibles con esta secuencia y no con la otra”.[8]

Lección de método
Una fuente no se vuelve verdadera por ser abundante ni por ser sofisticada. Los metadatos ayudan cuando se comprende qué son, cuándo se generaron, qué alteración es posible y con qué otras fuentes coinciden. La confianza nace de la convergencia, no del adjetivo.

2.6 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. Un informe bonito que no permite localizar la fuente es una presentación, no una investigación completa.

[7]NOM-151-SCFI-2016, conservación y digitalización de mensajes de datos, publicada el 30-03-2017. Requisitos de constancia, integridad, accesibilidad y huella digital electrónica. Fuente oficial en línea
[8]Jocsan Laguna. Libro abogados, capítulo 1. Material narrativo de investigación proporcionado por el autor. Nombres modificados en el manual para proteger identidades.



Figura 3. Fuente, exportación, copia de trabajo e impresión: representaciones con distinta cobertura. Reconstrucción editorial; no constituye evidencia real.

Conclusión limitada
Integridad no equivale a autenticidad, atribución no equivale a identidad física y fecha no equivale a acontecimiento. Documenta cada concepto por separado para no convertir una herramienta de control en una conclusión absoluta.

Capítulo 3. Roles, responsabilidades y decisiones

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; el custodio no altera la fuente para facilitar el análisis.

Para una fuerza de orden, esta distinción permite que personal sin formación de ingeniería reciba y proteja 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. El revisor independiente comprueba si la afirmación y la evidencia se relacionan, sin depender de quién presentó el informe.

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 La primera respuesta sin improvisación

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. La recepción debe decir qué ocurrió antes de llegar, no la versión que conviene para aparentar una secuencia ideal.

Una inspección ocular puede orientar, pero no se convierte en pericia por añadir una tabla, una captura o una conclusión. El perito en informática debe explicar el método, la fuente, la herramienta, los parámetros, las verificaciones y las limitaciones. Cuando alguien sin esa

materia presenta una percepción como si fuera un análisis científico, el problema no es de vocabulario: es de autoridad metodológica y de posibilidad de revisión.



Figura 4. La revisión independiente contrasta fuente, método y conclusión; no solo corrige estilo. Reconstrucción editorial; no constituye evidencia real.

3.3 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. La comunicación es parte de la evidencia de la decisión y no una nota administrativa separada.

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. Si la respuesta llega por enlace, se documenta quién lo abrió, con qué permisos, en qué fecha y qué versión descargó.

Registro mínimo de comunicación
Quién solicitó, a quién, qué autorizó, por qué canal, con qué fecha, qué cambios produjo y qué comprobación posterior existe. La conversación no es contexto opcional: explica por qué se tomó una decisión.

3.4 Independencia, privacidad y terceros

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. Una revisión que solo busca confirmar lo que el analista ya escribió no es independiente.

La privacidad exige separar la finalidad de la investigación de la exposición innecesaria. Los datos de terceros deben revisarse con criterio de proporcionalidad, seguridad y confidencialidad. El aviso de privacidad no es un documento ritual: explica qué datos se tratan, para qué, quién puede accederlos y cómo se ejercen derechos. Si el caso involucra datos personales, el responsable debe adoptar medidas necesarias y suficientes, sin convertir la pericia en una transferencia pública de información.[9]

Desde 2025, la autoridad federal en protección de datos personales es la Secretaría Anticorrupción y Buen Gobierno, no el INAI. Ese cambio no elimina las obligaciones de protección ni convierte toda investigación en una excepción: exige actualizar a quién se presenta una solicitud o reclamación cuando corresponda y evitar citar al instituto histórico como si siguiera siendo la autoridad actual.[10]

3.5 Un silogismo de roles

Premisa mayor: una pericia exige materia, método y posibilidad de revisión. Premisa menor: una inspección visual sin identificación de fuente, parámetros ni verificación no ofrece ninguna de las tres. Conclusión: la apariencia de análisis no basta para convertir una percepción en pericia. La respuesta no es despedir a quien hizo la inspección, sino asignar correctamente las funciones y conservar lo que sí puede acreditarse.

La primera respuesta puede documentar estado y custodia sin necesidad de presentarse como análisis. El especialista puede adquirir después con método. El revisor puede comprobar qué se hizo y qué no. Así se evita que una buena intención se convierta en una afirmación indefendible, y se permite que cada persona aporte lo que su función realmente puede sostener.[11][12]

[9]Ley Federal de Protección de Datos Personales en Posesión de los Particulares, nueva ley publicada el 20-03-2025 y reformada el 14-11-2025. Artículos 5–9, 18–20 y 31: principios, seguridad, confidencialidad, vulneraciones y plazos. Fuente oficial en línea

[10]Secretaría Anticorrupción y Buen Gobierno. Comunicado 011, 21-03-2025: transición de funciones de protección de datos personales del INAI a la Secretaría. Fuente oficial en línea

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

[12]Jocsan Laguna. Sinaloa. Desarrollo y conclusiones de opinión técnica en materia de informática forense. Material proporcionado por el autor; se generalizan errores sin exponer datos personales.

Conclusión limitada
La competencia se demuestra por función y método, no por cargo. Si una persona no puede explicar la fuente, el procedimiento y la comprobación, su intervención debe presentarse como lo que es: recepción, orientación o inspección, no como dictamen técnico.

Capítulo 4. Ciclo de vida y preparación forense

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. La retención no es acumulación sin límite; es decidir qué información puede ser necesaria y por cuánto tiempo.

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. El contacto correcto, la autorización de emergencia y una copia del acta deben existir antes del incidente, no descubrirse mientras la evidencia rota o se pierde acceso.

Preparación mínima	Qué debe comprobarse	Error que previene
Inventario de activos y propietarios	Responsable, fuente, formato y ubicación actualizados.	Solicitar registros al custodio equivocado.
Retención y formato	Período disponible, campos, zona y proceso de exportación.	Descubrir tarde que el dato ya no existe o no se entiende.
Directorio y suplencia	Contactos técnicos, jurídicos, custodios y proveedores con reemplazo.	Depender de una sola persona.
Sincronización horaria	Fuente temporal, desfase y revisión periódica.	Construir una cronología falsa por relojes incompatibles.
Ejercicios	Evidencia ficticia, recepción, adquisición, transferencia y revisión.	Improvisar el procedimiento durante la crisis.

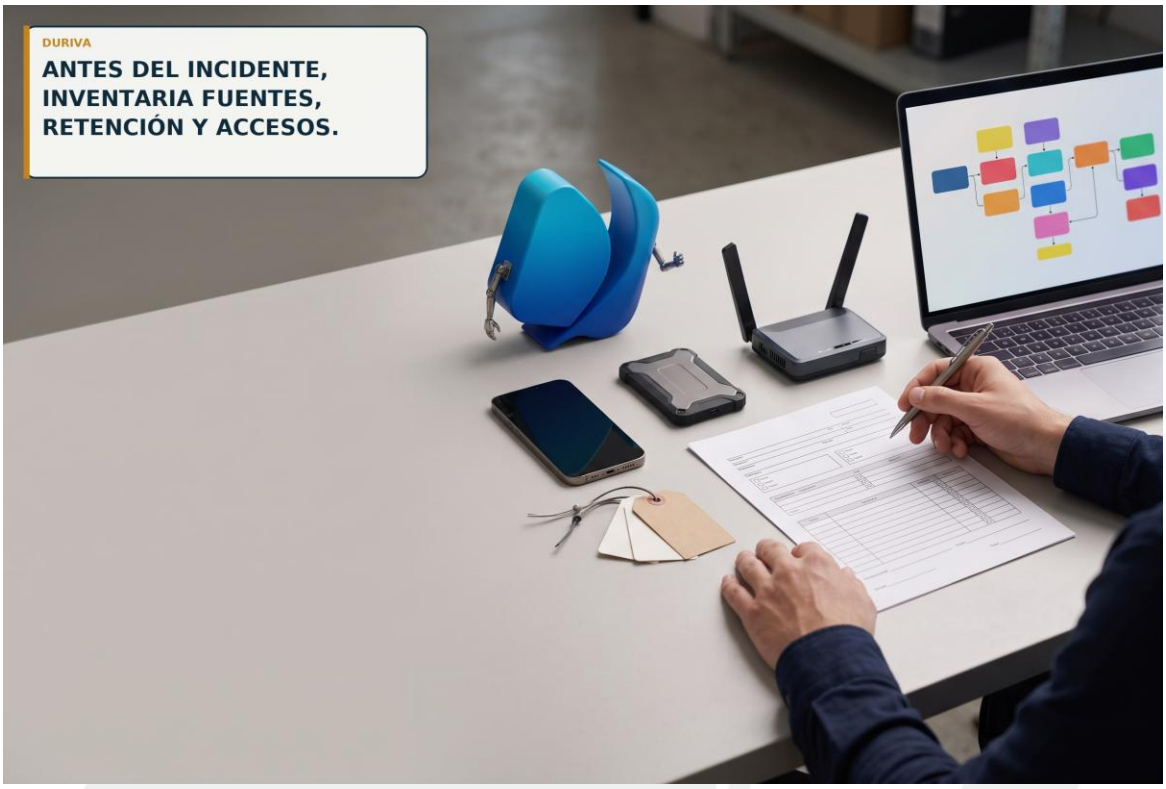


Figura 5. Preparación antes del incidente: inventario de fuentes, retención y accesos. Reconstrucción editorial; no constituye evidencia real.

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. Apagar puede preservar un estado o destruir memoria y sesiones; suspender una cuenta puede detener actividad o eliminar el acceso a la única exportación disponible.

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. La contención no se juzga solo por el daño evitado, sino también por la posibilidad de explicar qué se hizo, por qué y con qué costo probatorio.

Decisión urgente	Riesgo probatorio	Actuación previa recomendada
Apagar o reiniciar	Pérdida de memoria y sesiones.	Evaluar adquisición en vivo y documentar estado.

Decisión urgente	Riesgo probatorio	Actuación previa recomendada
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.
Eliminar enlace	Pérdida de la versión o del canal de descarga.	Conservar URL, permisos, versión, fecha y archivo recibido.



Figura 6. Puntos de no retorno: acciones que pueden impedir el análisis posterior. Reconstrucción editorial; no constituye evidencia real.

4.3 Ciclo documentado y entregables

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. La cadena no se sostiene con una carpeta que solo contiene una conclusión.
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 sin convertir la metodología en una certificación automática del contenido.[13][14]

Fase	Entregable mínimo	Pregunta de aceptación
Autoridad	Alcance, permisos, exclusiones y responsables.	¿Podemos hacer esto, con este objetivo y este alcance?
Identificación	Objeto, estado, custodio, identificadores y fotografías.	¿Sabemos exactamente qué tenemos y cómo llegó?
Adquisición	Método, herramienta, parámetros, salida e incidencias.	¿Otra persona puede repetirlo y relacionarlo con el objeto?
Custodia	Transferencias, accesos, sellos y verificaciones.	¿Podemos reconstruir quién accedió y por qué?
Análisis	Hipótesis, fuentes, resultados y alternativas.	¿Buscamos también lo que contradice la primera versión?
Informe y conservación	Conclusión, límites, anexos y acceso posterior.	¿Se puede revisar, abrir y comprender en el futuro?

4.4 Retención y análisis longitudinal

Un evento aislado puede parecer anómalo solo porque se desconoce la rutina. La actividad de un día debe compararse con períodos anteriores y posteriores cuando la pregunta sea si hubo comportamiento inusual, preparación o repetición. Un acceso breve puede ser la etapa final de una preparación larga; muchos accesos pequeños pueden indicar una conducta distribuida. El análisis longitudinal evita convertir una fotografía del incidente en una explicación completa del pasado.

[13]ISO/IEC 27037:2012. Directrices para identificación, recolección, adquisición y preservación de evidencia digital. Edición confirmada por ISO como vigente. Fuente oficial en línea
[14]NIST SP 800-86. Guide to Integrating Forensic Techniques into Incident Response. Guía metodológica, no legislación ni garantía de admisibilidad. Fuente oficial en línea

La retención de registros no es infinita ni uniforme. En México, la Ley en Materia de Telecomunicaciones y Radiodifusión distingue un primer período de doce meses en sistemas que permitan consulta y entrega en tiempo real a las autoridades competentes, y otros doce meses en sistemas de almacenamiento electrónico, cuya entrega se realiza dentro de las cuarenta y ocho horas siguientes a la notificación de la solicitud. El punto no es memorizar el plazo: es solicitar la fuente antes de que la retención y la cobertura cambien la posibilidad de análisis.[15]

Decisión de preservación
No esperes al vencimiento mínimo de retención para pedir los registros. La retención regulatoria no garantiza disponibilidad indefinida ni cobertura de todos los eventos. Preserva pronto, documenta el período y compara patrones antes de declarar que algo fue inusual.

4.5 Preparación como responsabilidad social

La preparación evita que una emergencia se convierta en una decisión arbitraria. Una organización que sabe quién responde, qué conserva, cómo exportar y qué no debe tocar tiene menos probabilidades de destruir evidencia útil o exponer datos de terceros. La preparación también democratiza el trabajo: una primera persona respondedora puede actuar con orden aunque no sea ingeniera, porque el procedimiento y los contactos ya existen.

Conclusión limitada
La preparación no consiste en registrar todo, sino en poder recuperar lo relevante con su contexto. Si una fuente crítica no tiene responsable, retención conocida, formato documentado o acceso autorizado, esa es una debilidad que debe resolverse antes del incidente.

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

Capítulo 5. Árboles de decisión por escenario

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 en una costumbre heredada.

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. La primera decisión no es elegir una herramienta: es comprender qué se pierde con cada opción.

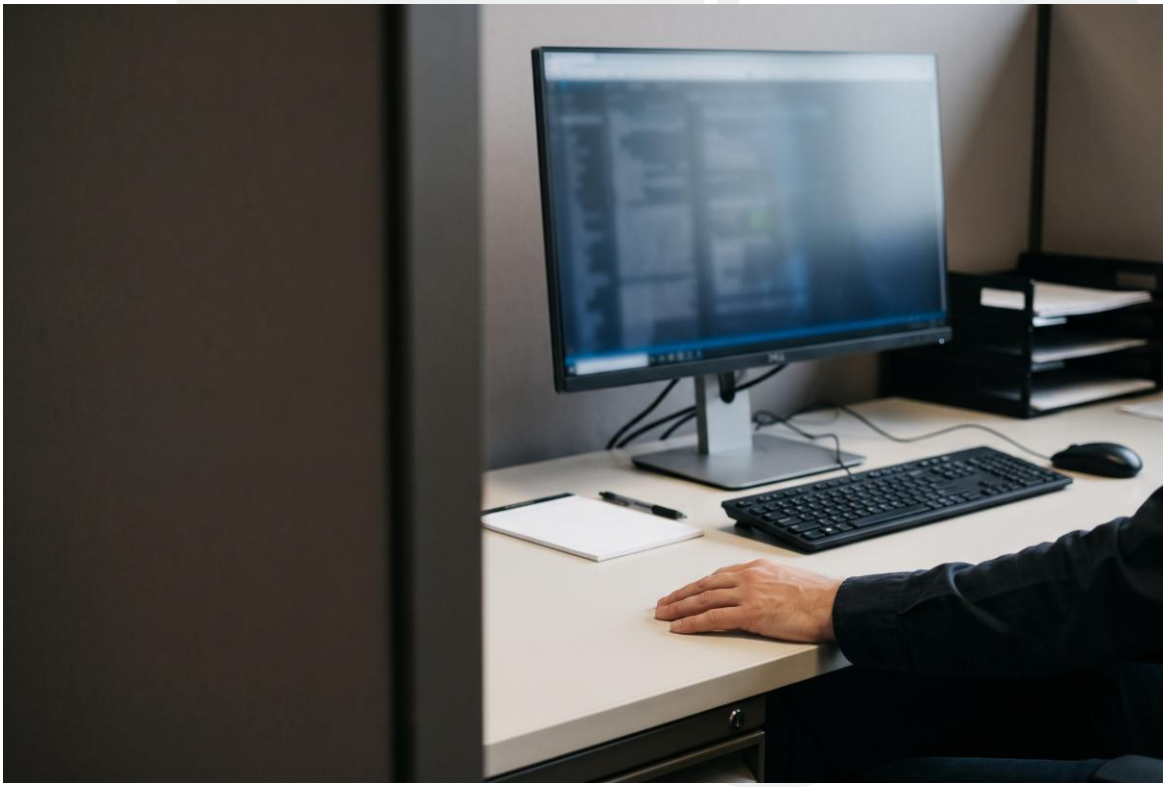


Figura 7. Equipo encendido: registrar estado y actividad antes de decidir. Reconstrucción editorial; no constituye evidencia real.

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. La pregunta no es dónde está el archivo visible, sino dónde está la fuente con mayor cobertura y menor alteración. 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. Un archivo nativo del proveedor puede ser mejor evidencia que una impresión del mismo archivo hecha por otra persona.

Condición	Ruta preferida	Registro indispensable
Memoria o sesiones necesarias	Adquisición en vivo si está autorizada y validada.	Estado, proceso, salida, hora y alteración inevitable.
Equipo apagado y estable	Imagen o adquisición lógica según objetivo.	Fuente, conexión, método, cobertura e incidencias.
Eventos en plataforma o terceros	Exportación administrativa o proveedor.	Rol, filtros, zona, formato, campos y entrega EML.
Acceso limitado o herramienta no validada	Detener y escalar sin alterar estado.	Motivo, estado, riesgo y siguiente responsable.

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 conectividad puede ser necesaria para exportar o preservar una cuenta, por lo que aislar no siempre es la primera respuesta.

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. La etiqueta “Faraday” no basta si el embalaje no cumple la función ni se comprueba su eficacia en el escenario concreto.



Figura 8. Antiestático y aislamiento de radiofrecuencia no son la misma función. Reconstrucción editorial; no constituye evidencia real.

5.4 Discos ópticos: identificador y formato

Un disco óptico exige identificación precisa. No basta anotar “un CD” o “un DVD” cuando la etiqueta, el oficio y la inspección no coinciden. Debe registrarse el tipo de soporte, marca y modelo si existen, capacidad, estado, lectores disponibles y cualquier identificador visible. El anillo central puede contener un código o identificador de fabricación; se revisa sin tocar la superficie de datos y se fotografía con contexto.

No todos los discos presentan el mismo identificador único ni todos los códigos visibles son un número de serie probatorio. La instrucción correcta es revisar el anillo central y registrar exactamente lo que aparece, sin inventarlo cuando no existe. También se diferencia soporte reescribible de soporte de solo lectura: un DVD-RW no es una simple variación estética, porque cambia las posibilidades de reescritura y debe documentarse como tal.



Figura 9. Revisión del anillo central: identificadores y códigos que pueden identificar el disco. Reconstrucción editorial; no constituye evidencia real.

Identificador antes que conclusión
Si no puedes identificar el soporte, no puedes afirmar que analizaste el objeto correcto. La pseudo custodia comienza con "hay un disco"; la custodia comienza con identificadores, estado, formato, fotografías y relación con el acta.

5.5 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. La detención documentada no es fracaso: conserva la posibilidad de análisis y evita una actuación indefendible.

El registro de detención incluye motivo, estado en que quedó el objeto, acciones previas, riesgos identificados y siguiente responsable. Si la duda se resuelve después, se incorpora quién respondió y con qué método. La pausa no reescribe el pasado: explica por qué se eligió no empeorar el caso.

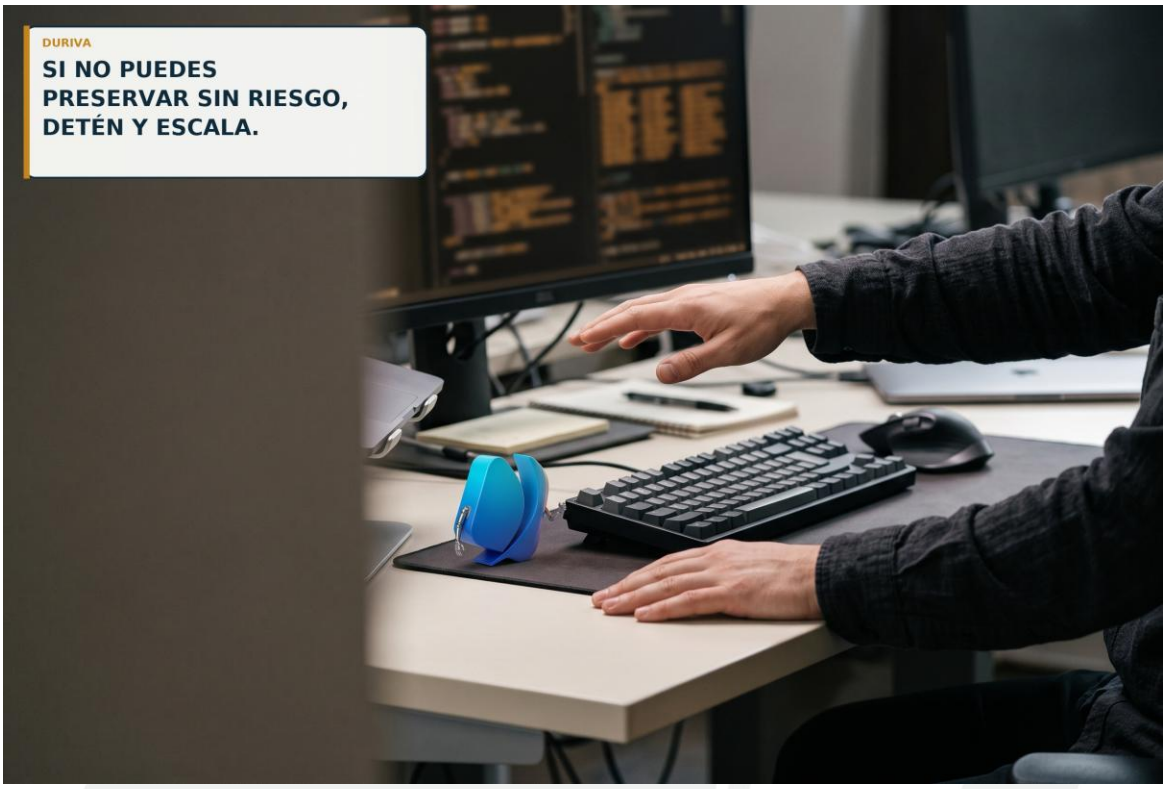


Figura 10. Detener y escalar: cuando continuar puede destruir más evidencia de la que aporta. Reconstrucción editorial; no constituye evidencia real.

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.

5.6 El árbol como razonamiento, no como decoración

Un árbol de decisión es útil cuando obliga a responder condiciones de entrada, acciones y registros, no cuando presenta una secuencia de iconos que nadie sigue. Cada rama debe terminar en una acción justificada, una justificación y un registro. Si la condición cambia, la ruta cambia. Un equipo cifrado, un teléfono conectado o un proveedor con una exportación mejor no deben conducir a la misma operación por defecto.

Conclusión limitada
La ruta correcta depende de estado, objetivo, autoridad y riesgo. Si la decisión solo se justifica por costumbre, el árbol está mal construido o mal aplicado. Registrar la condición que llevó a una ruta es tan importante como registrar la acción final.

Capítulo 6. Fuentes modernas y sábanas de llamadas

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. Descargar una interfaz no equivale a adquirir el historial completo de la cuenta.

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. La salida debe permitir comprobar qué consulta se hizo y qué cobertura tuvo.



Figura 11. Exportación por proveedor o API: filtros, campos, zona, formato y entrega. Reconstrucción editorial; no constituye evidencia real.

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. Guardar solo el adjunto rompe el vínculo entre el archivo y la declaración de integridad.

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. La autenticidad del canal se revisa con encabezados, servidor y contexto, no con una captura de la pantalla de correo.

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.



Figura 12. El EML conserva cuerpo, encabezados y adjuntos; una captura no los sustituye. Reconstrucción editorial; no constituye evidencia real.

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.

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.
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.

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.

Ejemplo de solicitud
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: una cámara no es toda la evidencia, y un router no es toda la red.



Figura 13. Virtualización: host, invitados, instantáneas y almacenamiento compartido. Reconstrucción editorial; no constituye evidencia real.

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.

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.[16][17]

[16]México. Código Penal Federal, artículos 199 Octies y 199 Nonies, compilación con reforma del 13-03-2026: determinadas conductas de contenido íntimo sexual sin consentimiento, incluso si el material no corresponde a la persona identificada. Fuente oficial en línea

[17]Reglamento (UE) 2024/1689 de inteligencia artificial, artículo 50, texto consolidado al 27-07-2026: transparencia de determinadas ultrafalsificaciones y adaptación para obras creativas, satíricas, artísticas o de ficción. Fuente oficial en línea

6.6 Vigencia: el ejemplo de una reforma derogada

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.[18]

Regla de actualización
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.

6.7 La fuente no vive en un solo lugar



Figura 14. Dispositivo, aplicación, cuenta y proveedor: capas de evidencia moderna. Reconstrucción editorial; no constituye evidencia real.

[18]San Luis Potosí. Gaceta Parlamentaria, 30-07-2026: derogación del 187 Ter y del capítulo con 272 Bis y 272 Ter. Antecedente histórico, no regla vigente. Fuente oficial en línea

Conclusión limitada
La vista del usuario no agota la fuente. La exportación correcta puede vivir en el proveedor, en una nube, en un historial de versiones o en un correo de entrega. Identifica la capa y conserva su contexto antes de analizar el contenido.

Capítulo 7. Recepción y preservación inicial

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. Si hay un disco, se indica soporte, capacidad, formato y código del anillo central cuando sea visible.
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. El objetivo no es fabricar una recepción impecable, sino documentar qué condiciones existían al inicio.

Campo	Qué debe contener	Ejemplo ficticio
Objeto e identificador	Tipo, marca, modelo, serie, capacidad y código asignado.	SSD 2.5 pulgadas, 512 GB, serie demo-003.
Entrega y recepción	Nombre, función, fecha, hora, zona y lugar.	Custodio A entrega a analista B, 09 nov, 14:32 −06.
Estado	Encendido, bloqueo, red, daño y accesorios.	Apagado, sin daño visible, cable SATA y fuente.
Sello y embalaje	Tipo, identificador, condición y fotografías.	Sello 01 íntegro, caja rígida y bolsa antiestática.
Acciones previas	Aperturas, conexiones, copias, cambios o desconocidos.	Se desconoce si se encendió antes de la entrega.
Decisión inicial	Preservar, escalar, adquirir o solicitar aclaración y responsable.	Preservar estado y solicitar especialista.



Figura 15. Fotografiar el estado inicial del objeto y sus accesorios antes de analizar. Reconstrucción editorial; no constituye evidencia real.

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. La apertura y el reemplazo son eventos de custodia, no una nota al margen.

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. El material se elige por la función que necesita la evidencia, no por la apariencia profesional del contenedor.



Figura 16. Recepción y embalaje: protección física, sello, etiqueta y relación entre objetos. Reconstrucción editorial; no constituye evidencia real.

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. La etiqueta física y el acta deben coincidir con el inventario digital y con el informe final.

Una convención posible es ED-AAAAMMDD-CASO-FUENTE-SECUENCIA-VERSION. Si la organización ya tiene otra, se mantiene si es única y consistente. El identificador no sustituye el objeto original: una exportación distinta de la misma fuente recibe identificador relacionado y una nota de relación. El identificador debe permitir localizar sin revelar cliente, titular ni información sensible.

Ejemplo ficticio de identificador
ED-20261109-DEMO-MBL-003-A00

ED = evidencia digital
20261109 = recepción
DEMO = caso ficticio
MBL = fuente móvil

003 = tercer objeto
A00 = adquisición inicial



Figura 17. Etiquetar objeto, estado, fecha, custodio e identificador. Reconstrucción editorial; no constituye evidencia real.

7.4 Accesorios y conexiones como parte de la recepción

Un cable, un adaptador, una tarjeta SIM, una memoria SD o una fuente de alimentación pueden explicar cómo se accedió a la información o qué conexiones eran posibles. Se registran como objetos relacionados, no como accesorios invisibles. Fotografiar solo el teléfono puede omitir la evidencia necesaria para adquirir o interpretar el dato. El inventario debe incluir cada elemento recibido y su relación con el dispositivo principal.



Figura 18. Accesorios y conexiones: parte de la recepción y de la posibilidad de adquisición. Reconstrucción editorial; no constituye evidencia real.

7.5 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. La descarga es un evento de recepción, no una acción invisible.

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. El orden se crea mediante inventario, no mediante alterar el objeto recibido.

Conclusión limitada
La recepción es la primera prueba de método. Si el objeto, el estado, los identificadores y las acciones previas no quedan claros, cualquier afirmación posterior empieza con una incertidumbre evitable.

Capítulo 8. Adquisición y documentación técnica

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. Cada método responde una necesidad distinta y produce límites distintos.
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. La frase “adquisición forense” no describe por sí sola qué se hizo ni qué cobertura tuvo.

Método	Cuándo puede ser adecuado	Límite que debe declararse
Imagen física	Se necesita el medio completo, incluido espacio no asignado.	No garantiza análisis de cada archivo ni de cada plataforma.
Adquisición lógica	Se requieren archivos o fuentes seleccionadas.	La selección y el filtro determinan cobertura.
Memoria volátil	Sesiones, claves, procesos o estado temporal son relevantes.	Justificación, autoridad y pérdida potencial al cambiar estado.
Exportación oficial	La mejor fuente está en proveedor o plataforma.	Parámetros, formato y cobertura del proveedor.
Documental	No hay otra representación disponible y debe mostrarse la visualización.	No conserva todas las propiedades del original.

8.2 Conexión real: fuente, bloqueador y estación

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. La fuente se conecta al bloqueador, la estación de trabajo al otro extremo. La configuración debe coincidir con lo que realmente se hizo, no con la imagen ideal de un manual.

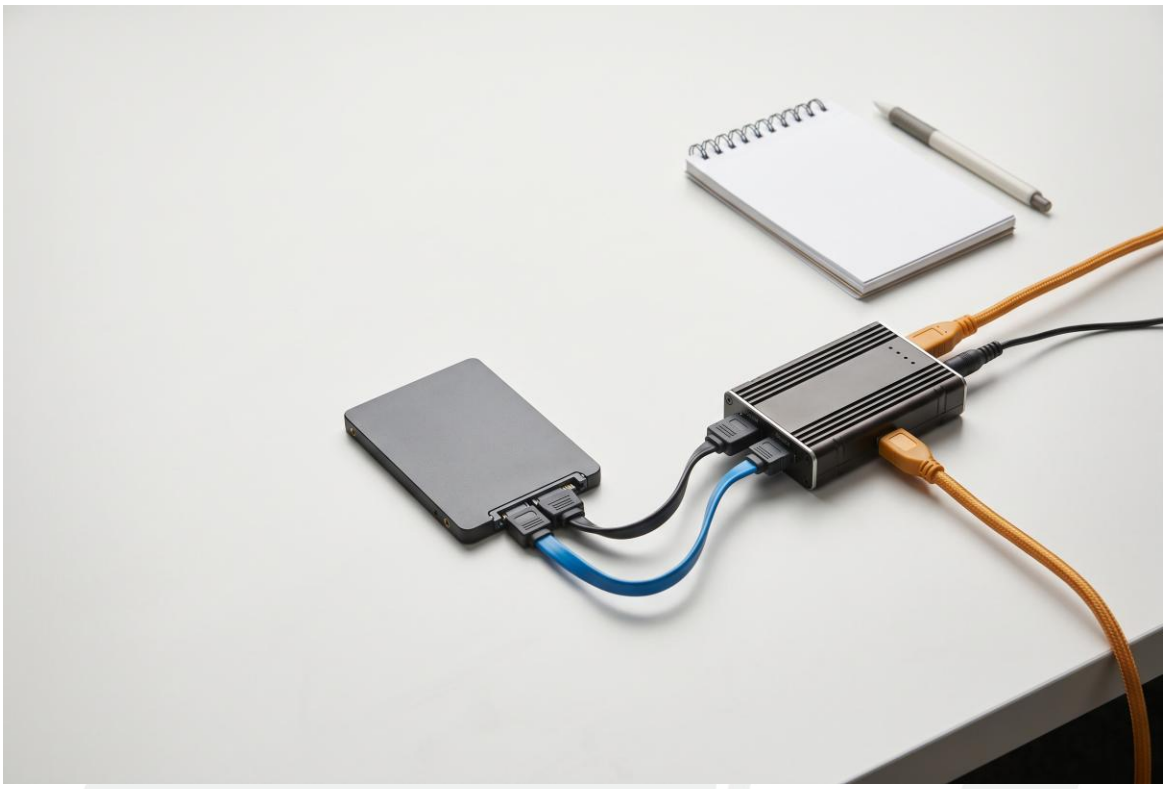


Figura 19. Fuente, bloqueador y estación de trabajo: la conexión también es evidencia. Reconstrucción editorial; no constituye evidencia real.

Registra el modelo y número de serie del bloqueador cuando estén disponibles, los puertos usados, los cables, la alimentación, el estado de los indicadores y cualquier incidencia. Si la herramienta produce un error, se conserva el mensaje y se evalúa su efecto en vez de ocultarlo. La protección se demuestra por configuración y verificación, no por afirmar que existía un dispositivo con ese nombre.

8.3 Medios y adaptadores: NVMe, SATA y discos ópticos

La forma del medio cambia la adquisición. Un M.2 NVMe no se conecta como un SATA 2.5, y un 3.5 SATA requiere alimentación distinta. El adaptador debe ser compatible y quedar documentado. Una foto del adaptador ayuda a explicar la ruta, pero el registro debe incluir modelo, interfaz, alimentación y verificación de que el medio se reconoce correctamente en la estación.



Figura 20. Medios y adaptadores: forma, conector y procedimiento de adquisición. Reconstrucción editorial; no constituye evidencia real.

Para un disco óptico se documenta lector, formato, capacidad, método de lectura, sectores ilegibles y relación con el soporte recibido. No se afirma adquisición de un DVD si las imágenes muestran una carpeta en el equipo y no el disco. Si la lectura falla, se conserva el error y se evalúa una segunda unidad o método, sin reemplazar el problema por una afirmación genérica.

8.4 Adquisición lógica y manifiesto

Una adquisición lógica obtiene archivos o fuentes seleccionadas. Antes de ejecutarla se delimitan carpetas, tipos de archivo, fechas, filtros y exclusiones. La salida se acompaña de un manifiesto que relaciona identificador, nombre, ruta, tipo de objeto, origen, método, tamaño, formato, hash y observaciones. Sin manifiesto, una carpeta llena de archivos puede ser volumen, pero no necesariamente evidencia organizada.

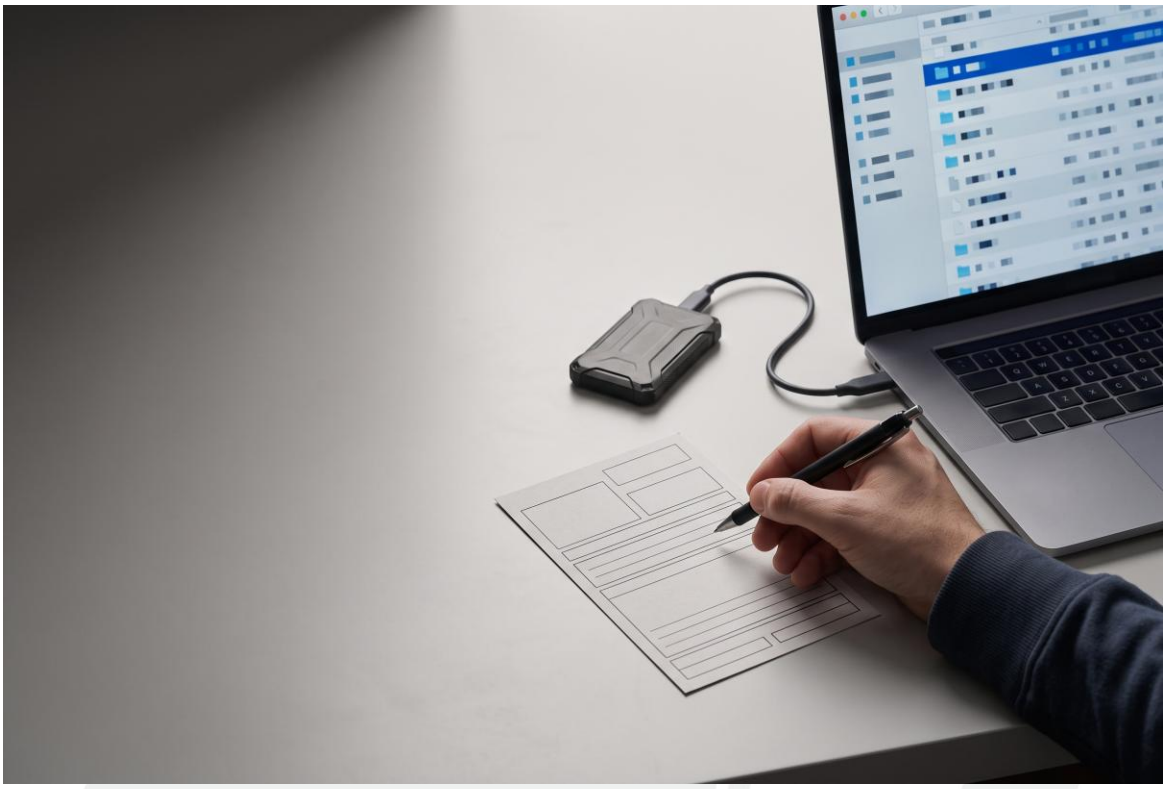


Figura 21. Manifiesto de archivos: origen, derivados, formato e integridad por objeto. Reconstrucción editorial; no constituye evidencia real.

Regla de manifiesto
El manifiesto no publica secretos ni datos sensibles innecesarios. La ruta puede abreviarse en la versión pública si revela información protegida, pero debe conservar la relación suficiente para localizar el objeto en el expediente controlado.

8.5 Memoria en vivo y validación de herramientas

La adquisición en vivo se justifica cuando memoria, sesiones, claves o procesos son relevantes y existe autoridad y capacidad para ejecutarla. Se documenta estado, herramienta, versión, parámetros, alteración inevitable y salida. Si no se dispone de esas condiciones, se escala. No se realiza una adquisición invasiva solo porque una exportación sería más difícil de solicitar.
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.



Figura 22. Validar herramienta antes de usarla: datos ficticios, salida legible y objeto esperado. Reconstrucción editorial; no constituye evidencia real.

8.6 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. La repetibilidad depende de condiciones documentadas, no de memoria.

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. Una ausencia puede ser significativa, pero solo dentro de la cobertura comprobada.

8.7 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. Repetir no elimina el primer intento; crea otro objeto relacionado con otra historia. 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. Un expediente perfecto solo en apariencia es menos defendible que uno que declara la incidencia y su tratamiento.

Conclusión limitada

La adquisición no termina con un archivo. Termina con una salida que puede abrirse, relacionarse con el objeto, verificarse y repetirse bajo condiciones documentadas. Si algo falla, queda dentro del registro, no fuera de la narrativa.

Capítulo 9. Custodia, traslado y conservación

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. 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. Un sello puede estar intacto al recibir y aun así desconocerse quién lo abrió antes. La cadena responde eventos: recepción, apertura, copia, acceso, traslado, verificación y devolución. Cada evento tiene responsable y propósito; no solo nombre y fecha.



Figura 23. Transferencia de custodia: objeto, responsables, sello y verificación. Reconstrucción editorial; no constituye evidencia real.

9.2 Transferencias electrónicas y llaves

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. Compartir un enlace sin saber quién puede abrirlo no es custodia controlada.
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. Si cambia la llave o el destinatario, también se registra.



Figura 24. Cifrado y llaves: proteger contenido sin perder control de recepción. Reconstrucción editorial; no constituye evidencia real.

Regla de llaves
Cifrar no basta: registra quién tiene la llave, por qué canal separado se entregó y cómo se verificó la recepción. Las claves no se escriben en el acta ni en el cuerpo del correo.

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 conservación incluye legibilidad futura, documentación de formato y claves disponibles.

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. La primera copia de trabajo no se confunde con el embalaje original; cualquier apertura, reemplazo de sello o transferencia queda registrada.



Figura 25. Respaldo y migración: conservar original, copia de trabajo y acceso posterior. Reconstrucción editorial; no constituye evidencia real.

9.4 Apertura y reemplazo de sello

Abrir un contenedor para trabajar no borra el sello ni la historia. Se registra quién abrió, por qué, con qué autoridad, qué condición tenía el sello y qué objeto contenía. Al terminar, se repone con un nuevo identificador de sello y se conserva el anterior cuando el procedimiento lo exija. La cadena se fortalece con acciones verificables, no con la afirmación genérica de que el paquete estaba cerrado.



Figura 26. Apertura y reemplazo de sello: una transferencia que también debe quedar documentada. Reconstrucción editorial; no constituye evidencia real.

9.5 Accesos, custodia compartida y conflictos

El acceso posterior necesita registro de consultas, propósito y autorización. Si una persona revisa, exporta o comparte, la acción debe quedar asociada a su función. Compartir custodia no elimina responsabilidad: define quién decide, quién ejecuta y quién verifica. Los conflictos de interés se declaran y se separan cuando la independencia lo requiere.



Figura 27. Registro de accesos: quién puede abrir, consultar y transferir con autorización. Reconstrucción editorial; no constituye evidencia real.

Conclusión limitada
La custodia no termina cuando el objeto se guarda. Termina cuando se puede reconstruir cada acceso, transferencia y verificación, incluida la forma en que se conserva la posibilidad de abrirlo en el futuro.

Capítulo 10. Examen, cronología e hipótesis alternativas

10.1 Examinar no es encontrar un culpable

El examen comienza cuando la fuente ya fue identificada, adquirida y relacionada con el encargo. Su finalidad no es buscar el archivo que haga parecer acertada la primera impresión, sino convertir una masa de datos en observaciones que puedan comprobarse. El analista abre la copia de trabajo, documenta las herramientas y formula preguntas pequeñas: qué archivo existe, qué fecha muestra, qué campo significa, qué cambio ocurrió, qué sistema produjo el registro y qué otra fuente podría contradecirlo. La respuesta a cada pregunta debe regresar a un objeto concreto del manifiesto.

La diferencia entre examen y análisis es semejante a la diferencia entre leer las piezas de un reloj y explicar por qué se detuvo. En el examen se observan engranes, desgaste y posición; en el análisis se contrastan explicaciones: falta de energía, daño mecánico, manipulación o una lectura equivocada. Si se salta directamente a la explicación preferida, cualquier pieza parece confirmarla. La disciplina consiste en describir antes de interpretar y conservar también lo que no encaja.[19]

Regla de trabajo
Toda afirmación del análisis debe poder seguirse hacia atrás: de la conclusión al hallazgo, de ahí a la consulta, al objeto analizado, a la adquisición y finalmente a la fuente. Si uno de esos eslabones no puede mostrarse, la conclusión necesita reformularse o necesita otra fuente.

10.2 Metadatos: escuchar al archivo sin creerle todo

Un metadato es información sobre un objeto, no una confesión espontánea del acontecimiento. La fecha de creación en un sistema de archivos puede corresponder a la copia en ese medio; la fecha interna de una fotografía puede depender del reloj de la cámara; una etiqueta de autor puede ser un nombre de cuenta configurado por cualquier persona. Cada campo tiene un productor, un mecanismo y una posibilidad de alteración. Leerlo bien exige saber quién lo escribió, cuándo, bajo qué condiciones y si el análisis lo modificó.

El nombre de un archivo también puede orientar sin demostrar por sí solo. Una secuencia IMG_0041, IMG_0042 e IMG_0043 sugiere un orden de generación dentro de una cámara o aplicación, pero no impide copias, renombrados, reinicios de numeración o archivos importados. El análisis prudente pregunta si los identificadores internos, miniaturas, fechas, registros de la aplicación y respaldos mantienen esa secuencia. El nombre es una pista de investigación, no un sello cronológico.

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

Supongamos que una imagen muestra las 18:42 y una acusación sostiene que fue capturada a las 20:42. La primera tentación es declarar que la prueba fue falsificada. La segunda, igual de peligrosa, es aceptar las 18:42 como hora absoluta. El método correcto conserva el archivo nativo, extrae los campos sin alterarlo, comprueba la zona, revisa el reloj del dispositivo, compara la secuencia anterior y posterior y busca otra fuente independiente: mensaje de envío, copia en nube, recibo de una compra, video de otra cámara o registro de actividad. Solo entonces puede explicarse si existe una diferencia de zona, un reloj mal configurado, una conversión o una inconsistencia mayor.



Figura 28. Los metadatos necesitan productor, significado, contexto y corroboración; no son testimonios infalibles. Reconstrucción editorial; no constituye evidencia real.

Dato observado	Pregunta técnica	Conclusión que todavía no puede darse
Fecha de sistema	¿Qué evento representa en este sistema de archivos?	Es la fecha original del hecho.
Fecha EXIF	¿Cómo estaba configurado el reloj y la zona?	La escena ocurrió necesariamente a esa hora.
Autor o cuenta	¿Quién podía configurar o usar esa cuenta?	La persona física quedó identificada.

Dato observado	Pregunta técnica	Conclusión que todavía no puede darse
Nombre consecutivo	¿La secuencia se conserva en otras fuentes?	No hubo copias, importaciones ni renombrado.
Coordenadas	¿Qué precisión y origen tiene la posición?	La persona estaba en un punto exacto.

10.3 Cronología: ordenar relojes antes de ordenar historias

Una cronología útil no es una columna de fechas ordenadas. Es una reconciliación entre relojes que pueden estar en zonas distintas, sincronizarse con servidores diferentes o conservar errores humanos. Primero se registra el valor literal de la fuente; después, su zona declarada o inferida, la conversión aplicada y la precisión disponible. El dato original nunca se sustituye por la conversión. Si un proveedor usa UTC y un teléfono registra hora local, el informe debe mostrar ambos y explicar cómo se compararon.

La precisión importa tanto como la fecha. Un registro que solo contiene día no puede colocarse a las 14:32 por comodidad visual. Un archivo con segundos no necesariamente tiene exactitud de segundos. Si el reloj presenta un desfase conocido, se documenta cómo se midió y a qué fuentes afecta. Cuando no hay forma de resolverlo, se utiliza una ventana temporal o se declara la incertidumbre. Esa honestidad evita que una secuencia visualmente perfecta convierta dos eventos incompatibles en una relación causal.

La secuencia debe conservar también acontecimientos negativos y períodos sin datos. Un corte de registros puede deberse a inactividad, rotación, pérdida de conectividad, configuración o borrado; la línea de tiempo no debe escoger una explicación sin prueba. Conviene marcar cada evento como observado, calculado, declarado por una persona o inferido. Mezclar esas cuatro clases como si fueran idénticas es una forma sutil de fabricar certeza.



Figura 29. La cronología conserva el tiempo original, la zona, la conversión y la incertidumbre de cada fuente. Reconstrucción editorial; no constituye evidencia real.

Ejemplo de normalización cronológica
Objeto: ED-20261109-DEMO-SRV-001-A00
Valor literal: 2026-11-03 20:14:07
Zona declarada por el proveedor: UTC
Conversión de trabajo: 2026-11-03 14:14:07 -06:00
Precisión disponible: segundos; sincronización del servidor no acreditada
Relación: evento anterior al correo recibido a las 14:20:11 -06:00
Límite: la proximidad temporal no demuestra quién realizó la acción ni que un evento haya causado el otro.

10.4 Antenas, cobertura y azimut: geografía sin atajos

Una sábana puede indicar que una línea se comunicó mediante una celda. Ese dato no convierte la antena en una persona ni demuestra que el portador estuviera debajo de ella. La celda describe una relación radioeléctrica dentro de condiciones de red, cobertura, congestión, tecnología y configuración. El análisis necesita ubicación de la celda, orientación o azimut cuando exista, tipo de tecnología, fecha, potencia o mediciones disponibles y una comprensión

real del área. Un punto en un mapa es una representación del equipamiento, no una fotografía del usuario.

El azimut orienta el sector hacia el cual la antena está dirigida; no es una línea láser que termine en una casa. La cobertura depende de propagación, obstáculos, frecuencia, relieve, interferencia, potencia y decisiones de la red. Una llamada puede ser servida por una celda que no es la más cercana. Tampoco la ausencia de otra celda en una exportación demuestra que no existiera cobertura alternativa: puede significar que no fue utilizada, que no se entregó el dato o que el sistema no lo conservó.

En un expediente anonimizado revisado por el autor, una localización fue tratada como si describiera el trayecto de una persona, aunque la fuente solo permitía hablar de cobertura. Otros elementos complicaban la versión: un video aportaba una secuencia que no concordaba con la interpretación afirmada y testigos describían hechos de manera inconsistente. El valor del análisis no estaba en sustituir una historia por otra igual de absoluta, sino en mostrar que la conclusión no se derivaba necesariamente de la fuente. La antena seguía siendo una antena; la identidad del portador necesitaba otra prueba.[20]



Figura 30. Una antena aporta cobertura potencial; no una dirección exacta ni la identidad del portador. Reconstrucción editorial; no constituye evidencia real.

[20]Jocsan Laguna. Sinaloa. Desarrollo y conclusiones de opinión técnica en materia de informática forense. Material proporcionado por el autor; se generalizan errores sin exponer datos personales.

Forma defendible de concluir
“El registro entregado asocia el evento con la celda identificada. En ausencia de mediciones y parámetros adicionales, ese dato no permite fijar una ubicación puntual ni atribuir el uso del terminal a una persona física.”

10.5 Corroboración que sí discrimina

Dos archivos que dicen lo mismo no siempre son dos fuentes independientes. Una captura y una impresión de la misma captura solo repiten una representación. En cambio, un registro de servidor, un mensaje recibido por un tercero y una secuencia de sensores pueden tener orígenes distintos y errores distintos. La corroboración gana fuerza cuando las fuentes no comparten la misma dependencia y cada una podría haber contradicho la versión.
La convergencia no se cuenta por número de páginas. Se evalúa por independencia, proximidad al hecho, capacidad de error y poder para distinguir hipótesis. Un centenar de capturas sin origen puede pesar menos que un EML completo con encabezados, adjunto verificable y registros del servidor. La navaja de Ockham no ordena elegir la explicación más cómoda: invita a no multiplicar causas si una secuencia sencilla explica los datos sin ignorar sus contradicciones.

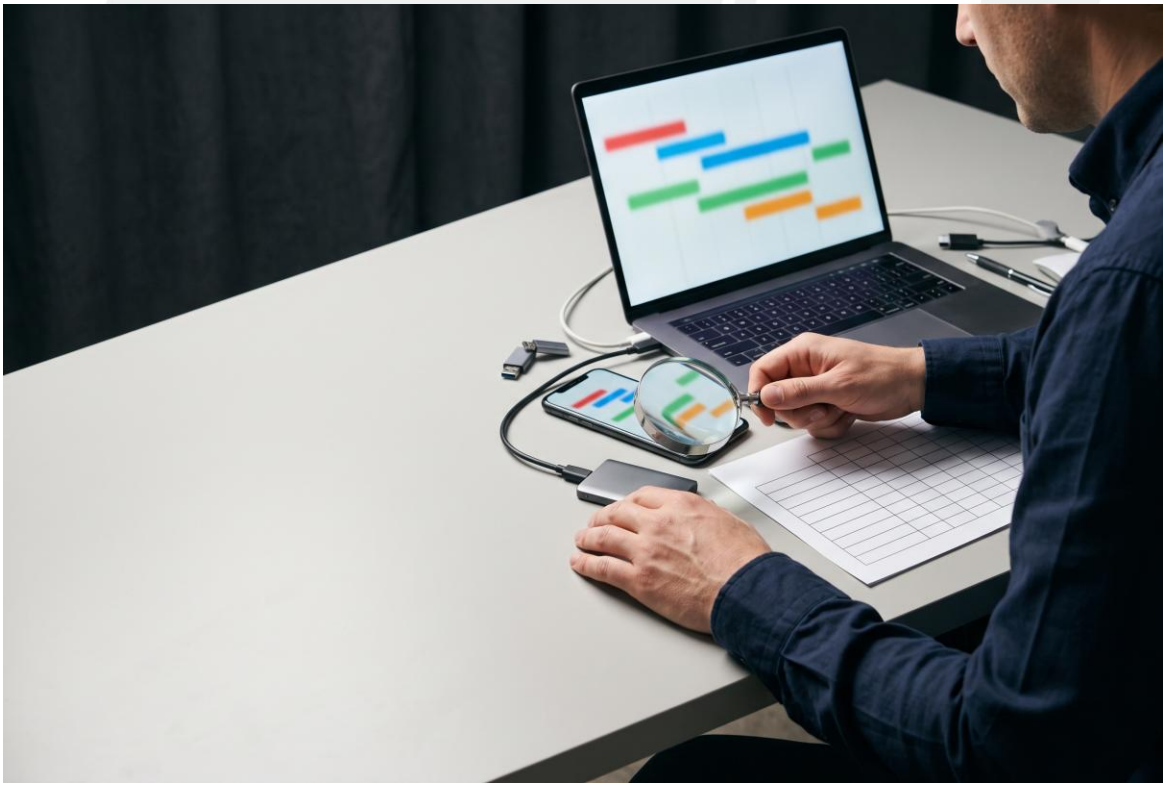


Figura 31. Corroborar es comparar fuentes con origen y errores distintos, no repetir la misma captura. Reconstrucción editorial; no constituye evidencia real.

10.6 Matriz de hipótesis: permitir que la evidencia contradiga

Antes de analizar conviene escribir al menos dos explicaciones plausibles y una condición que las distinga. Si una empresa sostiene que un archivo fue creado por un empleado el día de su salida, las hipótesis podrían ser: creación en esa fecha por la cuenta asignada; copia posterior de un archivo previo; modificación de metadatos; o uso de la cuenta por otra persona. No todas tienen que ser igualmente probables, pero todas deben enfrentarse a una comprobación concreta.

El resultado puede ser positivo, negativo o inconcluso. Un negativo documentado no es un fracaso: puede eliminar una explicación y evitar una acusación injusta. Un inconcluso tampoco debe disfrazarse de confirmación. Cuando la fuente no permite distinguir, la respuesta correcta es solicitar otra fuente, cambiar el alcance o declarar el límite. El analista no recibe puntos por mantener una hipótesis equivocada; recibe confianza por abandonarla cuando los datos lo exigen.

Hipótesis	Comprobación	Resultado ficticio	Lectura limitada
El documento se creó el 3 de noviembre.	Metadatos internos, historial de versión y registro de nube.	Historial muestra versión previa del 28 de octubre.	La fecha visible no acredita creación inicial.
La cuenta fue utilizada por su titular.	Sesiones, segundo factor, dispositivos y actividad concurrente.	Hay una sesión desde dispositivo no registrado.	La atribución de cuenta no identifica aún a la persona.
La imagen pertenece al mismo evento.	Secuencia, miniaturas, respaldo y otros archivos próximos.	Respaldo contiene secuencia coherente.	Es compatible con el evento; requiere contexto para su significado.
No existieron otros accesos.	Consulta completa, retención, filtros y errores.	Exportación cubre solo siete días.	No se observaron en el período consultado; no puede afirmarse inexistencia total.



Figura 32. Buscar también lo que contradice la primera hipótesis evita convertir el análisis en confirmación. Reconstrucción editorial; no constituye evidencia real.

10.7 Repetir, reproducir y saber cuándo parar

Una consulta repetible puede ejecutarse de nuevo bajo condiciones documentadas y producir un resultado compatible sobre el mismo objeto. La reproducibilidad exige además que otra persona cualificada pueda comprender y evaluar el procedimiento con independencia suficiente. Guardar solo una captura del resultado no satisface ninguna de las dos si se desconoce el archivo, la versión de herramienta, los filtros o la consulta. El objetivo es que la revisión pueda disentir con datos, no que deba confiar en la memoria del analista.[21]

El análisis se detiene cuando las preguntas del encargo fueron respondidas dentro del alcance, cuando una fuente adicional ya no discrimina o cuando continuar implicaría una intrusión desproporcionada. También se detiene para pedir autoridad ante una fuente nueva. La exhaustividad no consiste en abrir cada carpeta posible, sino en no dejar sin examinar una hipótesis razonable que la evidencia disponible sí puede resolver.

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

Entregable del capítulo
Una matriz de análisis con afirmación, fuente, consulta, hallazgo literal, hipótesis compatible, hipótesis debilitada, límite y acción adicional. La conclusión nace de esa matriz; no se escribe antes para llenarla después.

Capítulo 11. Informe, razonamiento y contradicción

11.1 El informe es la ruta de regreso a la fuente

Un informe pericial no debe impresionar por su grosor ni por la cantidad de términos en inglés. Debe permitir que una persona con otro criterio localice el objeto, comprenda qué se hizo y examine si la conclusión se deriva de los hallazgos. La estructura es una ruta: encargo, alcance, autoridad, fuentes, método, resultados, análisis, conclusión, límites y anexos. Si una afirmación no puede recorrer esa ruta en sentido inverso, el informe se convierte en literatura de autoridad.

El lector principal no siempre es ingeniero. Una jueza, un abogado, un directivo o una persona acusada necesita comprender el razonamiento sin aprender antes un lenguaje secreto. Escribir claro no reduce la ciencia: la expone. Por eso cada término especializado se explica la primera vez y cada captura se acompaña del objeto original o de una razón por la que no está disponible. La sencillez de la explicación debe ser proporcional al rigor del trabajo, no a su ausencia.



Figura 33. El informe permite verificar fuente, método, hallazgo y conclusión; no depende del prestigio de quien firma. Reconstrucción editorial; no constituye evidencia real.

11.2 Hecho, resultado, inferencia y opinión

El texto debe distinguir cuatro planos. Un hecho documental es lo que consta en la recepción: el archivo llegó con determinado nombre y tamaño. Un resultado técnico es lo que produce la comprobación: el hash calculado coincide con otro valor. Una inferencia es la lectura razonada de varios resultados: el adjunto recibido coincide con el que el proveedor declaró. Una opinión es la conclusión profesional dentro del encargo: la entrega conserva un mecanismo verificable de integridad desde ese momento. Mezclar los planos permite que una opinión parezca un dato observado.

También deben separarse las cuestiones jurídicas de las técnicas. El perito puede describir cómo se obtuvo un registro, qué campos contiene y qué inconsistencias presenta. No necesita declarar que una persona es culpable, que una conducta constituye un delito o que una parte debe ganar. Esa contención no disminuye la utilidad del informe; evita que una conclusión de competencia distinta contamine la fuerza de los hallazgos reales.

Plano	Ejemplo correcto	Exceso que debe evitarse
Recepción	“Se recibió adjunto.csv dentro del EML identificado como EV-04.”	“El banco entregó la verdad completa.”
Resultado	“El SHA-256 calculado coincide con el valor escrito en el cuerpo.”	“El contenido nunca fue alterado desde su origen.”
Análisis	“La coincidencia vincula el adjunto con la declaración del proveedor.”	“La llamada fue realizada por el titular.”
Conclusión	“Existe verificación de integridad entre entrega y recepción.”	“La prueba es irrefutable y concluyente.”

11.3 El silogismo y la falsa consecuencia

Un silogismo ordena premisas y conclusión. En el trabajo pericial sirve para detectar saltos que el entusiasmo suele ocultar. Premisa mayor: una celda registra una relación entre la red y un terminal dentro de condiciones de cobertura. Premisa menor: el registro analizado asocia una comunicación con la celda A. Conclusión válida: existe una asociación documentada entre esa comunicación y la celda A. Lo que no se deriva es que una persona concreta estuviera en una dirección concreta. Para sostener eso faltan premisas sobre ubicación, terminal y usuario.

La falsa consecuencia aparece cuando una afirmación verdadera se utiliza como pasaporte para otra que no la sigue. El archivo contiene una dirección IP; por tanto, el sospechoso escribió el mensaje. La firma verifica; por tanto, todo lo dicho ocurrió. El video muestra un reloj; por tanto, la grabación completa es auténtica. El disco está sellado; por tanto, la copia

analizada proviene de él. Cada conclusión exige una premisa adicional y una comprobación distinta. El razonamiento no se fortalece omitiendo esos pasos, sino haciéndolos visibles.
En materia de soporte físico, una contradicción de identificación puede bastar para impedir una inferencia. Si el acta describe un tipo de disco y las imágenes o capacidades corresponden a otro, no se resuelve diciendo que fue un error menor. Primero se aclara qué objeto se recibió, cuál se adquirió y cuál aparece en cada actuación. La conclusión se suspende hasta que la identidad de la fuente esté resuelta. No hay análisis excelente sobre un objeto equivocado.[22]

Prueba del "por tanto"
Después de cada "por tanto", escribe la premisa que hace necesaria la conclusión. Si esa premisa es solo costumbre, intuición o prestigio, sustituye la consecuencia absoluta por una observación limitada o realiza la comprobación que falta.

11.4 Explicar contradicciones sin esconderlas

Una contradicción no siempre significa falsedad. Puede revelar zona horaria, reloj desfasado, exportaciones con filtros distintos, dos objetos homónimos, interpretaciones de campo o una fuente realmente incompatible. El informe debe presentar la diferencia con sus valores literales y analizar las explicaciones posibles. Ocultarla porque debilita una versión es abandonar la función científica; explotarla sin investigarla es el error contrario.
Supongamos que un video tiene una fecha imposible, una sábana contiene un número que no corresponde al formato esperado y dos testigos describen posiciones incompatibles. No hay que escoger cuál molestia ignorar. Se revisa si el video conserva contador o fecha de sistema no inicializada, si el número fue transcrito o exportado incorrectamente y si los testimonios observaron el mismo evento desde lugares distintos. Si la explicación no se sostiene, queda como inconsistencia no resuelta. Su efecto en la conclusión se declara con precisión.
El caso de las fotografías y la banca enseña el lado constructivo: fuentes cotidianas pueden ofrecer una explicación compatible con la versión de una persona que parecía improbable. El caso de la antena enseña el lado preventivo: una fuente técnica puede ser invocada para sostener lo que no demuestra. En ambos, el método es el mismo: preservar, comprender, comparar y limitar. La evidencia no se usa para adornar una acusación ni una defensa, sino para acercarse a una secuencia que resista revisión.[23][24]

11.5 Redactar conclusiones que caben en la evidencia

Una conclusión fuerte no es necesariamente una conclusión absoluta. "No se observaron eventos en la exportación comprendida entre estas fechas, con estos filtros y esta cobertura"

[22] Jocsan Laguna. Sinaloa. Desarrollo y conclusiones de opinión técnica en materia de informática forense. Material proporcionado por el autor; se generalizan errores sin exponer datos personales.
[23] Jocsan Laguna. Libro abogados, capítulo 1. Material narrativo de investigación proporcionado por el autor. Nombres modificados en el manual para proteger identidades.
[24] Jocsan Laguna. Sinaloa. Desarrollo y conclusiones de opinión técnica en materia de informática forense. Material proporcionado por el autor; se generalizan errores sin exponer datos personales.

es más fuerte que “nunca ocurrieron”, porque puede comprobarse y sobrevive a una pregunta hostil. Del mismo modo, “los datos revisados son compatibles con la secuencia A y presentan estas inconsistencias con B” explica mejor el peso del análisis que “A quedó plenamente demostrado”.

El grado de afirmación debe corresponder al poder discriminatorio del método. Cuando solo hay una representación visual, se describe lo visible y se pide el nativo. Cuando existen varias fuentes independientes, se explica su convergencia y también sus límites. Cuando hay una fuente determinante ausente, no se compensa con adjetivos. El lector debe saber qué se afirmó, con qué base, qué quedó fuera y qué nueva información podría cambiar la respuesta.

Situación	Redacción defendible	Información que podría cambiarla
Hash coincidente	El objeto permaneció igual entre las dos verificaciones documentadas.	Error de identificación del objeto o del algoritmo registrado.
Cuenta atribuida	Los eventos se asociaron con la cuenta; el usuario físico no queda identificado solo por ello.	Registros de segundo factor, dispositivo, control de credenciales y corroboración.
Metadatos de fecha	La fecha interna es compatible con el período investigado, sujeta a reloj y zona.	Respaldo independiente, secuencia nativa y sincronización.
Consulta sin resultados	No se observaron registros dentro de la cobertura y filtros declarados.	Exportación ampliada, corrección de filtros o recuperación de retención.

11.6 Contradicción y revisión independiente

Antes de entregar, otra persona debe intentar romper el razonamiento sin alterar los objetos. Revisa si el identificador coincide con el acta, si la copia deriva de la fuente, si la consulta produce el mismo resultado y si la conclusión excede los datos. No se limita a corregir comas. Una revisión que solo embellece el informe deja intacto el error que podía cambiar el caso.

En una comparecencia, la respuesta profesional no consiste en defender cada palabra como si fuera una propiedad personal. Si señalan una fecha equivocada, se corrige; si una fuente no estaba disponible, se declara; si el método no permite una afirmación, se retira. La autoridad del perito está en la calidad del método y en su disposición a ser revisado, no en negarse a reconocer un límite. La contradicción es una prueba del sistema, no un insulto.



Figura 34. La revisión independiente intenta localizar fallas de fuente, método e inferencia antes de la entrega. Reconstrucción editorial; no constituye evidencia real.

Preguntas de contradicción
¿Puedo localizar el objeto exacto? ¿Puedo repetir la consulta? ¿La fuente es independiente de la versión que se evalúa? ¿Existe otra explicación compatible? ¿Qué no se revisó? ¿Qué afirmación desaparece si retiro una premisa?

11.7 Entrega, anexos y acceso posterior

El paquete de entrega contiene informe, manifiesto, anexos referenciados y copias controladas cuando corresponda. Los anexos se nombran igual en el texto y en los archivos. Si se entrega una versión pública, se separan datos personales y secretos sin destruir la versión completa preservada. El informe no publica contraseñas, claves privadas ni información que facilite un nuevo daño.

Se comprueba que el archivo abre, que las imágenes son legibles, que los enlaces internos funcionan y que los anexos citados existen. La entrega electrónica utiliza canal autorizado, cifrado cuando proceda y verificación de recepción. La huella del informe permite controlar versiones, pero no convierte su contenido en verdadero. El objeto entregado debe poder revisarse años después, con formato y contexto disponibles.

Entregable del capítulo
Un informe que responde cada pregunta del encargo, identifica sus fuentes, separa observación e inferencia, conserva contradicciones, declara límites y entrega anexos suficientes para una revisión independiente.

Capítulo 12. Errores, aprendizaje y servicio público

12.1 El error no se corrige reescribiendo el pasado

Todo procedimiento real contiene decisiones imperfectas: alguien conectó antes de fotografiar, olvidó la zona horaria, recibió una impresión en vez del archivo o usó un nombre ambiguo. La respuesta profesional no es borrar el evento y crear un acta ideal. Se conserva lo ocurrido, se registra su alcance y se determina si puede recuperarse la información mediante otra fuente. La mejora empieza por la verdad del expediente, no por su apariencia.

Una corrección posterior puede reducir daño, pero no fabrica custodia retrospectiva. Si hoy se calcula un hash de un archivo recibido hace un mes, el valor controla desde hoy; no acredita que el objeto haya permanecido intacto durante el mes anterior. Si se solicita una segunda exportación, se conserva como nuevo objeto con su propia recepción y se compara con la primera. Reconocer la diferencia protege tanto la investigación como a las personas.



Figura 35. El original se preserva; el análisis se realiza sobre copia controlada. Las excepciones se justifican y registran. Reconstrucción editorial; no constituye evidencia real.

12.2 Errores de recepción y preservación

Apagar por costumbre puede destruir memoria y sesiones; mantener encendido sin control puede seguir modificando datos. Trabajar sobre el original puede impedir demostrar qué cambios fueron propios del análisis. Guardar un teléfono en una bolsa antiestática y llamarla

Faraday confunde dos funciones. Embalar sin identificador impide saber si el objeto devuelto es el mismo. Estas fallas no se resuelven comprando más herramientas: se previenen con estado, autoridad, función y registro.
También es un error tratar los accesorios como irrelevantes. Un cable o adaptador explica la conexión; una memoria adicional puede contener la fuente; una fuente de poder permite conservar un estado mientras se decide. La recepción debe mirar el conjunto sin tocar por curiosidad. Fotografiar, identificar, relacionar y pedir apoyo son acciones sencillas que evitan explicaciones imposibles años después.



Figura 36. La protección electrostática y el aislamiento de radiofrecuencia cumplen funciones distintas. Reconstrucción editorial; no constituye evidencia real.

12.3 Errores de fuente, captura y exportación

Una captura sin URL, fecha, cuenta ni contexto es como una fotografía de una página arrancada: permite leer un fragmento, pero impide conocer el libro. Debe conservarse la fuente nativa cuando exista, acompañar la captura con ruta y momento, y documentar quién la obtuvo. Si solo existe la visualización, se dice eso y no se afirma que se revisó el historial completo. La imagen puede ser útil sin fingir que es el universo.
Exportar sin filtros, zona, rol ni diccionario de campos produce un archivo que puede ser correcto y aun así incomprensible. El mismo problema aparece cuando se recibe solo un PDF de una sábana y se descarta el correo con su declaración de integridad. El procedimiento

robusto pide formato nativo, parámetros, proceso, campos, limitaciones, hash en el cuerpo y EML de entrega. No es burocracia: es la información necesaria para saber qué se tiene.



Figura 37. Sin URL, fecha, cuenta y contexto, una captura queda incompleta aunque la imagen sea nítida. Reconstrucción editorial; no constituye evidencia real.

12.4 Errores de interpretación

Asignar una IP a una persona sin revisar asignación, sesión, dispositivo, compartición y contexto convierte un dato de red en identidad física. Interpretar una antena como domicilio convierte cobertura en presencia. Tratar una fecha como inmutable o como completamente inútil son dos versiones del mismo problema: no preguntar qué produjo el campo. El análisis serio no oscila entre credulidad y desprecio; evalúa cada fuente según su mecanismo y corroboración.

Los detectores de contenido sintético merecen la misma prudencia. Un porcentaje no identifica por sí solo autoría, herramienta ni conducta. Compresión, recorte, regrabación y entrenamiento del detector pueden alterar el resultado. Se conserva archivo, versión, publicación, historial y contexto; se comparan métodos y se explican falsos positivos y negativos. Un indicio puede orientar una solicitud de fuente, pero no sustituirla.



Figura 38. Un detector de IA aporta indicios con límites; no sustituye archivo, historial, contexto y corroboración. Reconstrucción editorial; no constituye evidencia real.

12.5 Errores jurídicos y de vigencia

Una equivalencia por parecido de palabras puede ser más peligrosa que no citar ninguna norma. La firma simple, avanzada, digital y cualificada no produce idénticos efectos en todos los países. Una regla bancaria no se aplica a toda empresa. Una norma archivística no resuelve cualquier controversia privada. Una iniciativa no es un decreto. La cita útil lleva instrumento, artículo, función, ámbito, versión y fuente oficial; si una parte no está comprobada, se declara. La transición del CNPCF ejemplifica la necesidad de revisar declaratorias y reformas antes de escoger el régimen. La derogación en San Luis Potosí de disposiciones específicas sobre IA muestra que una reforma muy comentada puede dejar de ser vigente. El manual no intenta congelar el derecho: enseña a actualizarlo sin perder el método. La versión jurídica se revisa al momento del caso y se registra en el control de cambios.[25][26]

[25]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

[26]San Luis Potosí. Gaceta Parlamentaria, 30-07-2026: derogación del 187 Ter y del capítulo con 272 Bis y 272 Ter. Antecedente histórico, no regla vigente. Fuente oficial en línea



Figura 39. Verificar vigencia, ámbito y reforma evita convertir una cita histórica en fundamento actual. Reconstrucción editorial; no constituye evidencia real.

12.6 Lecciones aprendidas que cambian el procedimiento

Una lección aprendida debe terminar en un cambio observable. Si una exportación llegó sin zona, se modifica la solicitud para exigirla. Si dos objetos fueron confundidos, se revisa el identificador y la fotografía. Si una herramienta cambió el formato, se actualiza la validación y el ejemplo. Añadir una frase a una carpeta de incidencias sin cambiar el procedimiento solo acumula arrepentimiento documentado.

La revisión se programa por riesgo y por cambios de entorno, no por calendario vacío. Se comprueban fuentes oficiales, versiones de herramientas, formatos de proveedores y condiciones de almacenamiento. Cuando se actualiza el manual, se sustituye el contenido aplicable y se conserva el historial, en lugar de apilar notas que se contradicen. Las actas históricas no se modifican; el procedimiento vigente sí mejora.

Incidencia ficticia	Consecuencia	Cambio verificable
Adjunto sin EML	Se pierde la declaración de hash y el contexto de entrega.	La lista de recepción exige EML, adjuntos y comparación.
Fecha sin zona	La cronología puede desplazar eventos.	Plantilla con valor literal, zona, conversión e incertidumbre.

Incidencia ficticia	Consecuencia	Cambio verificable
Sello cambiado sin registro	No puede reconstruirse la apertura.	Evento obligatorio de apertura y reposición.
Conclusión superior al hallazgo	La inferencia no resiste contradicción.	Revisión de premisas y tabla de afirmaciones permitidas.
Norma desactualizada	Se aplica un efecto que ya no corresponde.	Control de vigencia con fuente y fecha de consulta.

12.7 La medida final: evitar el próximo abuso

El propósito de este manual no es formar personas capaces de producir más papel técnico. Es ayudar a que una recepción correcta impida una acusación construida sobre un objeto equivocado; a que una cronología honesta impida una condena basada en relojes incompatibles; a que una empresa preserve los registros que pueden demostrar qué pasó; a que una persona comprenda por qué una captura no basta y qué puede solicitar. La técnica se vuelve servicio cuando reduce la arbitrariedad.

Dar con las manos abiertas no significa publicar secretos ni entregar una receta para dañar. Significa compartir los fundamentos que permiten trabajar con dignidad: identificar, proteger, preguntar, verificar, reconocer límites y corregir. El conocimiento no se guarda como un puño cerrado. Se entrega con método para que otra persona pueda hacerlo mejor y para que ninguna autoridad —humana o técnica— tenga que pedir fe donde debería ofrecer comprobación.

Cierre del manual

Preservar la evidencia es preservar la posibilidad de verdad. El método no promete ganar: promete que la afirmación podrá ser revisada, que el error podrá reconocerse y que la conclusión no será más grande que los hechos.

Anexo A. Equivalencias jurídicas funcionales

Jurisdicciones estudiadas: México, Perú, Chile, Argentina, Colombia, Ecuador y España/Unión Europea. Revisión documental: 9 de noviembre de 2026. El criterio rector es la equivalencia funcional, no la identidad normativa.

Resumen ejecutivo

Esta matriz responde a una pregunta operativa: qué norma cumple, en cada jurisdicción, la función que el manual necesita documentar. No parte de buscar un artículo con el mismo número ni una frase parecida. La equivalencia funcional permite comparar el reconocimiento jurídico del documento electrónico, la escritura, la atribución, la integridad, la noción de original, la accesibilidad, la conservación, la admisibilidad, la valoración y la carga probatoria, así como las obligaciones sectoriales de registros e incidentes. Dos disposiciones pueden perseguir la misma finalidad con presunciones, destinatarios, plazos y consecuencias distintos; por eso una concordancia temática nunca debe traducirse en la afirmación de que producen idénticos efectos procesales.

El resultado muestra una estructura compartida, pero no uniforme. México, Colombia y Ecuador contienen reglas especialmente claras sobre mensajes de datos, escrito, original, integridad y conservación. Chile y Argentina distinguen con precisión los efectos de las distintas clases de firma. Perú distribuye el régimen entre la Ley 27269, su Reglamento, el Código Procesal Civil, las normas archivísticas y la regulación SBS. España combina eIDAS, legislación procesal y normativa de servicios de pago. En todos los casos, la forma electrónica no basta para demostrar autoría, integridad o veracidad del contenido. El manual debe pedir fuente, método, contexto, continuidad y posibilidad de verificación; el hash ayuda a comparar objetos, pero no demuestra por sí solo quién creó un archivo ni si lo narrado ocurrió.

1. Método y límites de la comparación

Se utilizaron textos oficiales, compilaciones legislativas, diarios oficiales y documentos de reguladores. Cada entrada registra el instrumento y los artículos que efectivamente fueron localizados. “Directa” significa que la función está expresamente cubierta con una estructura semejante; “parcial” indica que solo cubre un aspecto o depende de otra norma; “sectorial” delimita la regla a archivos, firmas, pagos o entidades supervisadas; “no acreditada” señala que la investigación no localizó una regla general suficientemente comprobada. Esta última categoría no afirma que el derecho del país carezca de regulación, sino que no debe inventarse una equivalencia con la evidencia disponible.

La consulta tiene tres límites prácticos. Primero, una compilación puede incorporar reformas en fechas distintas y cada caso exige revisar la versión aplicable al hecho y al procedimiento. Segundo, las reglas civiles, mercantiles, penales, administrativas, archivísticas y financieras no son intercambiables por semejanza terminológica. Tercero, la admisibilidad, la autenticidad, la valoración y la carga de la prueba son preguntas diferentes: una norma puede permitir presentar un documento sin concederle plena prueba ni invertir la carga probatoria. En

consecuencia, esta matriz orienta la documentación técnica y la localización de normas, pero no sustituye el análisis jurídico del expediente ni una conclusión judicial.

Nivel	Significado operativo	Regla para citarlo en el manual
Directa	La función está reconocida expresamente y con una estructura comparable.	Explicar requisitos, excepciones y efectos; no copiar solo el enunciado.
Parcial	La norma cubre una parte de la función o exige complemento procesal.	Citar el instrumento complementario y delimitar qué queda fuera.
Sectorial	La regla se limita a archivo, certificación, pagos o entidades vigiladas.	No extenderla a toda evidencia digital ni a todos los sujetos.
No acreditada	No se localizó una equivalencia suficientemente verificada.	Escribir “no acreditada en esta revisión”, nunca “inexistente”.

2. Matriz central por función jurídica

La tabla concentra las funciones de reconocimiento y forma. Las citas se encuentran dentro de las celdas para mantener unida cada proposición con su fuente. Las categorías no puntúan la calidad del sistema jurídico: describen su utilidad para el manual y el grado de correspondencia comprobado. En particular, la noción de “original” no siempre exige conservar un dispositivo físico; varias legislaciones la abordan mediante integridad desde la forma definitiva y accesibilidad posterior. El manual debe evitar tanto la superstición del soporte como la idea de que una captura conserva todas las propiedades del archivo del que procede.

Cuando una celda combina normas, la función está distribuida y no debe atribuirse íntegramente al primer instrumento mencionado. El caso peruano es especialmente instructivo: la Ley 27269 regula firmas y certificados digitales; no contiene, por sí sola, un régimen general de original y conservación de mensajes de datos. La admisión de documentos firmados digitalmente aparece en su Reglamento y la conservación de microformas tiene un régimen archivístico específico. Separar esas fuentes evita construir una equivalencia elegante pero falsa.

Reconocimiento del documento electrónico

Jurisdicción	Regla, alcance y límite
México	CCom 89 y 89 Bis: neutralidad y no rechazo por mensaje de datos.

Jurisdicción	Regla, alcance y límite
Perú	Ley 27269, arts. 1–2, para firma electrónica; alcance específico, no régimen documental completo.
Chile	Ley 19.799, arts. 1–3: equivalencia del soporte y validez, con exclusiones.
Argentina	Ley 25.506, arts. 1, 3 y 6, para firma y documento digital.
Colombia	Ley 527, art. 5: no se niegan efectos por ser mensaje de datos.
Ecuador	Ley 67, art. 2: igual valor jurídico que documentos escritos, sujeto a la ley y reglamento.
España / UE	eIDAS 46: no se niegan efectos ni admisibilidad solo por formato electrónico.

Fuentes de la tabla: [27][28][29][30][31][32][33]

Forma escrita y accesibilidad posterior

Jurisdicción	Regla, alcance y límite
México	CCom 93 y 93 Bis; CNPCF 349 exige accesibilidad.
Perú	Reglamento 052-2008-PCM, art. 3, para exigencia de firma; accesibilidad archivística se regula aparte.
Chile	Ley 19.799, art. 2.d exige almacenamiento idóneo para uso posterior; art. 3, forma escrita.
Argentina	Ley 25.506, art. 6: documento digital satisface escritura; Decreto 182/2019, conservación.

[27]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
[28]Perú. Ley 27269 de Firmas y Certificados Digitales y Reglamento DS 052-2008-PCM. Régimen específico de firma y admisión de documentos firmados digitalmente. Fuente oficial en línea
[29]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
[30]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
[31]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
[32]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
[33]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

Jurisdicción	Regla, alcance y límite
Colombia	Ley 527, art. 6: mensaje accesible para posterior consulta.
Ecuador	Ley 67, art. 6: información accesible para posterior consulta.
España / UE	eIDAS no formula una regla general idéntica al 93 Bis; LSSI y normas sectoriales complementan. Parcial, no forzar equivalencia.

Fuentes de la tabla: [343536373839]

Atribución y firma

Jurisdicción	Regla, alcance y límite
México	CCom 90–92; CNPCF 349; presunción según método fiable y atribuible.
Perú	Ley 27269, art. 3, y Reglamento 3–4; firma digital en IOFE y admisión de documentos firmados.
Chile	Ley 19.799, arts. 2.f–g y 4–5: firma simple y avanzada no tienen idénticos efectos.
Argentina	Ley 25.506, arts. 5, 7–9: carga al invocar firma electrónica desconocida; presunciones para firma digital válida.
Colombia	Ley 527, arts. 7, 16–17 y 28: método confiable, atribución y atributos de firma digital.
Ecuador	Ley 67, arts. 10, 13–16: procedencia, identidad y efectos de firma electrónica.

[34]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
[35]Perú. Reglamento de la IOFE, DS 052-2008-PCM, artículos 3 y 4: exigencia y admisión de documentos electrónicos firmados digitalmente. Fuente oficial en línea
[36]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
[37]Argentina. Decreto 182/2019: conservación digital y copias autenticadas en los plazos y condiciones previstos. Fuente oficial en línea
[38]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
[39]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

Jurisdicción	Regla, alcance y límite
España / UE	eIDAS 25–26: no discriminación de firma simple; equivalencia a manuscrita para cualificada; requisitos de avanzada.

Fuentes de la tabla: [40][41][42][43][44][45][46]

Original e integridad desde forma definitiva

Jurisdicción	Regla, alcance y límite
México	CCom 93 Bis y CNPCF 350: integridad desde generación definitiva y accesibilidad; regla especial de cadena pública en el 350.
Perú	No acreditada como regla general en la Ley 27269. Microformas e integridad archivística tienen régimen específico en DL 681 y DS 001-2000-JUS.
Chile	Ley 19.799, art. 2.g detecta modificaciones en firma avanzada; art. 5 asigna valor según clase de documento. Parcial.
Argentina	Ley 25.506, art. 8: presunción de integridad si verificación digital verdadera. Directa para firma digital, no universal para todo archivo.
Colombia	Ley 527, arts. 8–9: garantía confiable de integridad desde la forma definitiva y exhibición.
Ecuador	Ley 67, art. 7: comprobación de integridad desde forma definitiva; Reglamento, art. 6.

[40]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
[41]Perú. Reglamento de la IOFE, DS 052-2008-PCM, artículos 3 y 4: exigencia y admisión de documentos electrónicos firmados digitalmente. Fuente oficial en línea
[42]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
[43]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
[44]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
[45]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
[46]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

Jurisdicción	Regla, alcance y límite
España / UE	eIDAS 26.d vincula datos para detectar modificaciones; LEC 326 regula impugnación de autenticidad e integridad. Parcial y procesal.

Fuentes de la tabla: [47]4848950515253

Conservación y contexto de origen/destino/fecha

Jurisdicción	Regla, alcance y límite
México	NOM-151 para conservación y digitalización; CCom 93 Bis para accesibilidad.
Perú	DS 001-2000-JUS para microformas; Reglamento IOFE para firma y certificados. Sectorial.
Chile	Ley 19.799, arts. 2.d y 5: uso posterior y fechado acreditado para fecha de instrumento privado con firma avanzada.
Argentina	Decreto 182/2019, art. 5: conservación digital durante plazos específicos y copias autenticadas.
Colombia	Ley 527, arts. 12–13: formato, reproducción exacta, origen, destino, fecha y hora; terceros.
Ecuador	Ley 67, art. 8: accesibilidad, formato, origen, destino, fechas, horas e integridad; terceros.
España / UE	Normas sectoriales y de conservación; no acreditada una cláusula general única equivalente a Ley 527.12 en esta revisión.

[47]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
[48]Perú. DL 681 y DS 001-2000-JUS: tecnologías avanzadas, microformas, autenticidad, integridad y conservación archivística. Ámbito sectorial. Fuente oficial en línea
[49]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
[50]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
[51]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
[52]Ecuador. Reglamento a la Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos: incorporación de anexos, desmaterialización, integridad y verificación. Fuente oficial publicada por la Función Judicial. Fuente oficial en línea
[53]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

Fuentes de la tabla: [545556575859]

Admisibilidad y valoración probatoria

Jurisdicción	Regla, alcance y límite
México	CCom 1205 admite mensajes de datos; CFPC 210-A y CNPCF 348–350 fijan fiabilidad, atribución, accesibilidad e integridad.
Perú	CPC 188–197: finalidad, legalidad, medios típicos/atípicos y carga; Reglamento 4 para documentos firmados digitalmente.
Chile	Ley 19.799, art. 5: plena prueba en casos previstos; demás documentos según reglas generales.
Argentina	CCyC 318–319: correspondencia por cualquier medio y ponderación de confiabilidad de soportes/procedimientos.
Colombia	Ley 527, arts. 10–11: admisibilidad, sana crítica, generación, archivo, comunicación, integridad e iniciador.
Ecuador	Ley 67, art. 14: firma electrónica admitida como prueba; arts. 2 y 7 sujetan eficacia y original a requisitos.
España / UE	eIDAS 46 y LEC 326/384: admisión, impugnación, servicios de confianza y sana crítica.

[54]NOM-151-SCFI-2016, conservación y digitalización de mensajes de datos, publicada el 30-03-2017. Requisitos de constancia, integridad, accesibilidad y huella digital electrónica. Fuente oficial en línea
[55]Perú. DL 681 y DS 001-2000-JUS: tecnologías avanzadas, microformas, autenticidad, integridad y conservación archivística. Ámbito sectorial. Fuente oficial en línea
[56]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
[57]Argentina. Decreto 182/2019: conservación digital y copias autenticadas en los plazos y condiciones previstos. Fuente oficial en línea
[58]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
[59]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

Fuentes de la tabla: [60]

Carga probatoria y presunciones

Jurisdicción	Regla, alcance y límite
México	No hay una presunción universal de autoría por existir un archivo; se acredita el método y su atribución.
Perú	CPC 196: carga a quien afirma hechos de su pretensión o contradice alegando nuevos hechos, salvo regla distinta.
Chile	Valor según clase de instrumento y firma; fecha privada exige atención al fechado acreditado.
Argentina	Ley 25.506, arts. 5 y 7–8: carga al invocar firma electrónica desconocida; presunciones solo en su régimen.
Colombia	Ley 527, arts. 17, 21 y 28: presunciones delimitadas de origen, recepción e intención de firma.
Ecuador	Ley 67, art. 10: presunción de procedencia salvo prueba en contrario y excepciones; no autoría humana automática.
España / UE	LEC 326.4: presunción de característica cuestionada y correcta prestación si hay servicio cualificado, en sus términos.

[60]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
[61]Perú. Código Procesal Civil, artículos 188–197 y 245.5: finalidad, legalidad, medios, carga, valoración y fecha por medios técnicos. Fuente oficial en línea
[62]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
[63]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
[64]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
[65]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
[66]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

Fuentes de la tabla: [6768697071]

3. México: base normativa y transición

México ofrece una secuencia completa para el manual, pero exige distinguir el régimen mercantil vigente, el CFPC histórico y la entrada gradual del CNPCF. El artículo 210-A del CFPC reconoce la información generada o comunicada por medios electrónicos, ópticos u otra tecnología como prueba y exige ponderar la fiabilidad del método, la atribución y la accesibilidad; su original se apoya en integridad desde la forma definitiva. El Código de Comercio contiene la arquitectura sustantiva de comercio electrónico: 89 y 89 Bis, neutralidad y no discriminación; 90–92, atribución, envío, recepción y acuses; 93 y 93 Bis, escrito, original, integridad y accesibilidad; 94, lugar de expedición y recepción. El artículo 1205 fue verificado directamente en la compilación oficial y admite, entre otros medios, fotografías, videos, sonido y mensajes de datos.[72]

El CNPCF, cuya compilación oficial consultada indica última reforma del 15 de enero de 2026, contiene en los artículos 348–350 una estructura semejante y añade tecnologías como cadena de bloques. El artículo 350 también contiene una regla probatoria especial para registros de cadena pública, condicionada a que no acrediten vulneración o falta de confiabilidad; no debe transformarse en una afirmación general de que cualquier registro distribuido es auténtico. La transición es gradual y depende de declaratorias. La compilación consultada conserva el límite general del 1 de abril de 2027; una iniciativa publicada en Gaceta Parlamentaria el 29 de abril de 2026 propuso sustituirlo por el 31 de enero de 2030, pero una iniciativa no es un decreto publicado. Antes de aplicar esa transición a un caso real debe comprobarse si existió una reforma posterior en el DOF y qué declaratoria corresponde al órgano jurisdiccional.[73][74]

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

[68]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

[69]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

[70]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

[71]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

[72]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

[73]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

[74]Cámara de Diputados. Gaceta Parlamentaria, 29-04-2026. Iniciativa que propone modificar el plazo de entrada en vigor del CNPCF al 31-01-2030. Es una iniciativa, no un decreto publicado. Fuente oficial en línea

Instrumento	Función verificada	Precisión que debe conservar el manual
CFPC 210-A	Información electrónica como prueba; fiabilidad, atribución, accesibilidad e integridad.	Es la base histórica de la transición, no un artículo que simplemente "cambia de número".
CNPCF 348–350	Reconocimiento, fiabilidad, original, accesibilidad y regla de cadena pública.	Entrada gradual; revisar declaratoria y reformas al momento del asunto.
CCom 89–94	Neutralidad, efectos, atribución, envío/recepción, escrito, original y lugar.	No confundir acuse de recepción con veracidad del contenido ni con consentimiento válido en todo contexto.
CCom 1205	Admisibilidad expresa de mensajes de datos y otros medios.	Admisibilidad no equivale a plena prueba ni elimina contradicción y peritaje.
NOM-151-SCFI-2016	Conservación, digitalización, PSC acreditado, huella, RFC 3161, constancias y accesibilidad.	Es requisito técnico de conservación/digitalización en su ámbito, no certificado mágico de autoría o veracidad.
CNBV 316 Bis y serie	Comprobantes, notificaciones, cifrado, accesos, incidentes, incidencias, bitácoras y revisiones.	Cada artículo tiene destinatarios, objetos y plazos distintos; no citar "el 316 Bis" como si fuera una sola obligación.

Fuentes de la tabla: [7576777879]

La NOM-151 merece un tratamiento técnico separado de las reglas procesales. Su utilidad está en la preservación y constatación de mensajes de datos y en las condiciones de

[75]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

[76]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

[77]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

[78]NOM-151-SCFI-2016, conservación y digitalización de mensajes de datos, publicada el 30-03-2017. Requisitos de constancia, integridad, accesibilidad y huella digital electrónica. Fuente oficial en línea

[79]Disposiciones de carácter general aplicables a las instituciones de crédito, artículos 316 Bis, 316 Bis 1, 316 Bis 10 a 17: comprobantes, cifrado, acceso, incidentes, incidencias, bitácoras y revisiones. Fuente oficial en línea

digitalización, no en declarar que todo lo almacenado es verdadero. La página de normalización de la Secretaría de Economía la identifica como vigente, mientras el texto del DOF desarrolla los requisitos de constancia, integridad y accesibilidad. El manual debe registrar herramienta, versión, algoritmo, fecha y zona horaria, identidad del operador y relación entre original, copia y constancia. No debe prometer que un sello de tiempo o una constancia resuelve por sí solo la autoría humana, la legalidad de la obtención o la totalidad de una conversación.[8081]

La regulación CNBV se desglosa así: 316 Bis, comprobantes; 316 Bis 1, notificaciones; 316 Bis 10, cifrado y protección; 316 Bis 11, control de acceso; 316 Bis 12, investigación y notificación de incidentes, con información a la Comisión dentro de cinco días naturales; 316 Bis 14, incidencias y operaciones no reconocidas con conservación de cinco años; 316 Bis 15, bitácoras con conservación segura por 180 días y atención a solicitudes del usuario dentro de diez días hábiles; 316 Bis 17, revisiones de seguridad al menos anuales. Estos plazos no se exportan a otros países ni a todo tipo de empresa. Para un peritaje se solicitan los registros vinculados con la operación y el período pertinente, no “todos los servidores” como fórmula indiscriminada.[82]

4. Perú: régimen distribuido y actualización financiera

Perú exige abandonar la idea de una única ley de mensajes de datos. La Ley 27269, modificada por la Ley 27310, regula firmas y certificados digitales y consta de 16 artículos en el texto oficial revisado. Su artículo 1 reconoce la firma electrónica; el 2 delimita su ámbito; el 3 define la firma digital mediante criptografía asimétrica. El Reglamento aprobado por DS 052-2008-PCM desarrolla la IOFE y, en sus artículos 3 y 4, regula la equivalencia de la firma digital generada en esa infraestructura y la admisión de documentos electrónicos firmados digitalmente como prueba. La propia norma reconoce variedad de firmas electrónicas y no permite tratar cualquier símbolo o imagen insertada como firma digital acreditada.[8384]

En materia procesal, el Código Procesal Civil contiene las reglas generales en los artículos 188–197: finalidad, oportunidad, pertinencia, legalidad, medios típicos y atípicos, prueba de oficio, carga y valoración. El artículo 192 enumera declaración de parte, testigos, documentos, pericia e inspección judicial; el 193 admite auxilios técnicos o científicos como medios atípicos; el 196 distribuye la carga salvo disposición diferente. El artículo 245.5 permite al juez considerar fecha cierta la determinada por medios técnicos que le produzcan convicción. Para archivo, el DL 681 y el DS 001-2000-JUS cubren tecnologías y microformas, autenticidad,

[80]NOM-151-SCFI-2016, conservación y digitalización de mensajes de datos, publicada el 30-03-2017. Requisitos de constancia, integridad, accesibilidad y huella digital electrónica. Fuente oficial en línea

[81]Secretaría de Economía. PLATIICA. Ficha de la NOM-151-SCFI-2016, conservación y digitalización de mensajes de datos. Consulta de vigencia y referencia complementaria al texto del DOF. Fuente oficial en línea

[82]Disposiciones de carácter general aplicables a las instituciones de crédito, artículos 316 Bis, 316 Bis 1, 316 Bis 10 a 17: comprobantes, cifrado, acceso, incidentes, incidencias, bitácoras y revisiones. Fuente oficial en línea

[83]Perú. Ley 27269 de Firmas y Certificados Digitales y Reglamento DS 052-2008-PCM. Régimen específico de firma y admisión de documentos firmados digitalmente. Fuente oficial en línea

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

integridad y conservación; su alcance no debe confundirse con una regla universal de original para cualquier archivo privado.[8586]

Tema peruano	Regla útil	Advertencia operativa
SBS 504-2021, art. 12.6.g	Preservar evidencias para investigaciones forenses tras incidentes.	Convertirlo en procedimiento documentado, no en recolección indiscriminada.
SBS 504-2021, art. 15	Reporte de incidentes significativos y análisis forense a disposición de la Superintendencia.	El informe debe contener resumen ejecutivo y detalle técnico.
SBS 504-2021, art. 17.3–17.4	Mantener y proteger registros de enrolamiento, intentos de autenticación y operaciones; monitorear transacciones.	Son registros especialmente relevantes para reconstruir secuencia y autenticación, no prueba automática de identidad física.
SBS 2286-2024, nuevo 20.3	Responsabilidad empresarial por determinadas operaciones no reconocidas, salvo que acredite responsabilidad del usuario.	Es la modificatoria correcta de la 504-2021; no citar una numeración errónea ni el texto anterior como si siguiera intacto.

Fuentes de la tabla: [8788]

La comparación financiera debe reflejar esta actualización de 2024. El párrafo 20.3 modificado abarca operaciones no reconocidas por canal digital sin el requisito de autenticación reforzada, en ciertos supuestos de exención o después de que el usuario reportó robo o pérdida de credenciales, salvo acreditación de responsabilidad del usuario. Esto es distinto de afirmar que el banco siempre responde o que el uso de credenciales siempre prueba autorización. El peritaje debe examinar factores, enrolamiento, registros, alertas, contexto de dispositivo y secuencia, conectando los hechos técnicos con la regla vigente al momento de la operación.[89]

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

[86]Perú. DL 681 y DS 001-2000-JUS: tecnologías avanzadas, microformas, autenticidad, integridad y conservación archivística. Ámbito sectorial. Fuente oficial en línea

[87]Perú. SBS 504-2021, artículos 12.6.g, 15 y 17.3–17.4: preservación, reporte y análisis forense, registros de enrolamiento, autenticación y operaciones. Fuente oficial en línea

[88]Perú. SBS 2286-2024: modificación del artículo 20.3 sobre determinadas operaciones no reconocidas y responsabilidad, salvo acreditación de responsabilidad del usuario. Fuente oficial en línea

[89]Perú. SBS 2286-2024: modificación del artículo 20.3 sobre determinadas operaciones no reconocidas y responsabilidad, salvo acreditación de responsabilidad del usuario. Fuente oficial en línea

5. Chile: firma, fecha y regulación de seguridad

La Ley 19.799 vigente en la compilación de la Biblioteca del Congreso Nacional regula documentos electrónicos y sus efectos. El artículo 1 consagra equivalencia del soporte, el 2 define documento y firmas, el 3 reconoce forma y efectos con exclusiones, el 4 exige firma electrónica avanzada para instrumento público y el 5 diferencia el valor probatorio. Los instrumentos privados con firma avanzada comparten el régimen de plena prueba indicado por la ley, pero no hacen fe respecto de su fecha salvo fechado electrónico otorgado por prestador acreditado. Los documentos con firma electrónica no avanzada se valoran conforme a reglas generales. Esta diferencia evita dos errores: negar todo valor a una firma simple y concederle automáticamente el de una avanzada.[90]

En el frente bancario, la Recopilación Actualizada de Normas distingue el capítulo 20-10, Gestión de Seguridad de la Información y Ciberseguridad, del 20-9 sobre continuidad. El 20-7 regula externalización y exige condiciones de confidencialidad, integridad, trazabilidad y disponibilidad, además de acceso oportuno a registros e información requerida por autoridades. El 20-8 se refiere a información de incidentes operacionales. Para el manual, la equivalencia funcional se formula por controles y evidencia disponible, no por afirmar que un capítulo reproduce el 316 Bis. Debe solicitarse la norma vigente y el alcance de la entidad antes de fijar plazos o contenido mínimo.[91]

Necesidad del caso	Fuente funcional chilena	Precaución
Atribuir documento y firma	Ley 19.799, arts. 2–5.	Separar identificación formal, firma avanzada y eficacia probatoria.
Probar fecha de instrumento privado	Ley 19.799, art. 5.2.	La firma avanzada no basta por sí sola para hacer fe de la fecha.
Revisar proveedor/nube y registros	RAN 20-7 y 20-10; incidentes, 20-8.	No confundir continuidad, externalización y ciberseguridad.

Fuentes de la tabla: [92][93]

[90]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

[91]Chile. Recopilación Actualizada de Normas, capítulos 20-7, 20-8 y 20-10: externalización, incidentes operacionales, seguridad de la información y ciberseguridad. Fuente oficial en línea

[92]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

[93]Chile. Recopilación Actualizada de Normas, capítulos 20-7, 20-8 y 20-10: externalización, incidentes operacionales, seguridad de la información y ciberseguridad. Fuente oficial en línea

6. Argentina: presunciones delimitadas y confiabilidad del soporte

La Ley 25.506 reconoce firma electrónica y digital con efectos diferentes. El artículo 5 define la firma electrónica que carece de alguno de los requisitos de firma digital y, si se desconoce, impone a quien la invoca acreditar su validez. Los artículos 7 y 8 presumen autoría e integridad para firma digital en las condiciones legales; el 9 determina validez y el 6 reconoce escritura. El Decreto 182/2019 regula conservación y copias autenticadas. La Ley 27.446 derogó el antiguo artículo 4 de la Ley 25.506 y sustituyó otras disposiciones; por ello el anexo no debe reproducir exclusiones históricas como si fueran el texto vigente.[949596]

El Código Civil y Comercial aporta las reglas probatorias transversales. El artículo 318 permite presentar correspondencia cualquiera que sea el medio de creación o transmisión, con límites para correspondencia confidencial. El 319 ordena valorar los instrumentos particulares ponderando, entre otras pautas, congruencia, claridad técnica, usos, relaciones precedentes y confiabilidad de soportes y procedimientos técnicos. El manual puede traducir esas pautas en preguntas concretas: qué sistema generó el registro, quién administraba las claves, qué cambios podía realizar, cómo se exportó, si la secuencia es congruente y si existe corroboración independiente. La presunción de integridad criptográfica no contesta por sí sola esas preguntas de contexto.[97]

Regulación BCRA	Función	Diferencia frente a México
Comunicación A 7783	Registros de transacciones disponibles en formato digital al menos 90 días; registro en tiempo real para determinados servicios de mensajería; monitoreo.	Plazo y alcance propios; no sustituirlo por 180 días mexicanos.
Comunicación A 8280	Respuesta y recuperación ante ciberincidentes; reporte final dentro de cinco días corridos posteriormente a contención, recuperación y resolución.	El cómputo depende del evento descrito por la norma; no es idéntico al aviso CNBV.

Fuentes de la tabla: [9899]

[94]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

[95]Argentina. Ley 27.446: derogación del antiguo artículo 4 de la Ley 25.506 y sustitución de otras disposiciones. Impide citar como vigente el texto histórico. Fuente oficial en línea

[96]Argentina. Decreto 182/2019: conservación digital y copias autenticadas en los plazos y condiciones previstos. Fuente oficial en línea

[97]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

[98]Argentina. BCRA Comunicación A 7783: registros de transacciones digitales disponibles al menos 90 días y monitoreo de eventos de seguridad. Fuente oficial en línea

[99]Argentina. BCRA Comunicación A 8280: respuesta y recuperación ante ciberincidentes; reporte final dentro de cinco días corridos posteriormente a contención, recuperación y resolución. Fuente oficial en línea

7. Colombia: mensajes de datos, conservación y acuses

La Ley 527 de 1999 ofrece una correspondencia funcional muy clara con el modelo mexicano. El artículo 5 evita negar efectos por la forma electrónica; 6 cubre escrito y accesibilidad; 7, firma mediante método confiable y apropiado; 8–9, original e integridad; 10–11, admisibilidad y valoración; 12–13, conservación directa o por terceros; 16–25, atribución, envío, recepción, acuses, duplicados, tiempo y lugar. El artículo 28 establece atributos de firma digital. El artículo 12 exige conservar información que permita determinar origen, destino, fecha y hora, elemento que debe incorporarse a los formatos de exportación y custodia.[100]

El CPACA aporta reglas para actuaciones administrativas. Los artículos 57–58 exigen autenticidad, integridad y disponibilidad de actos y archivo electrónico; el 61 exige control de documentos recibidos, fecha y hora, seguridad y acuse; el 62 regula prueba de envío/recepción y constancia de fallas del servicio. Estas disposiciones no sustituyen la Ley 527: responden al procedimiento administrativo. Para el sector financiero se localizó la Circular Externa 033 de 2020 como instrumento de instrucciones en seguridad y ciberseguridad, pero las fuentes recuperadas no permitieron fijar con seguridad todos sus numerales operativos. La matriz, por rigor, no le atribuye plazos ni requisitos textuales no leídos.[101][102]

Aplicación	Regla documental	Registro mínimo sugerido
Mensaje original	Ley 527, arts. 8–9.	Objeto en formato nativo, integridad, proceso de generación y forma de exhibición.
Conservación	Ley 527, arts. 12–13.	Formato, origen, destino, fecha, hora, custodio y tercero involucrado.
Recepción administrativa	CPACA 61–62.	Radicado, acuse, fecha/hora y constancia verificable de cualquier falla.
Ciberseguridad financiera	CE 033 de 2020 identificada por SFC.	Confirmar numerales y versión oficial antes de imponer obligaciones específicas.

[100]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

[101]Colombia. CPACA, artículos 57–58, 61 y 62: autenticidad e integridad de actos y archivo electrónico, acuse y constancia de fallas del servicio. Fuente oficial en línea

[102]Colombia. Superintendencia Financiera. Circular Externa 033 de 2020, identificada como instrucción de seguridad y ciberseguridad; sus numerales deben confirmarse antes de imponer obligaciones específicas. Fuente oficial en línea

8. Ecuador: equivalencia documental y sistema de pagos

La Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos —Ley 67— regula de forma expresa las funciones centrales. El artículo 2 reconoce igual valor jurídico a los mensajes de datos conforme a la ley y reglamento; 6 cubre información escrita accesible; 7, original e integridad; 8, conservación con formato, accesibilidad, origen, destino, fechas, horas e integridad; 10, procedencia e identidad con presunción y excepciones; 11, envío y recepción; 13–14, definición y efectos de firma electrónica. El Reglamento desarrolla incorporación de anexos, desmaterialización, integridad y verificación. La presunción del artículo 10 no autoriza a identificar automáticamente a la persona física que pulsó un dispositivo: exige analizar verificación, avisos y diligencia del destinatario.[103][104]

En materia financiera, la Resolución JPRM-2025-006-M, publicada en el Registro Oficial Suplemento 104 del 18 de agosto de 2025, regula sistemas de pago. Sus artículos 77–79 abordan operación, validez, compensación y liquidación; el 82 exige individualizar fondos y movimientos de billeteras y disponibilidad continua; disposiciones posteriores desarrollan participantes y supervisión. Es una fuente útil para comprender registros y confirmación del sistema de pagos, pero no acredita las mismas obligaciones de bitácoras, conservación e incidentes de la CNBV. El manual debe marcar esta equivalencia como sectorial y parcial y solicitar el régimen de la entidad y del canal antes de inferir responsabilidades.[105]

Necesidad	Fuente ecuatoriana	Límite
Conservar mensaje y metadatos	Ley 67, art. 8.	No basta un PDF de visualización si se pierde el formato y los datos de origen.
Atribuir mensaje	Ley 67, arts. 10 y 13–14.	Firma y procedencia no identifican por sí solas a la persona física ni prueban todos los hechos.
Reconstruir pago electrónico	Resolución JPRM-2025-006-M.	Régimen de sistemas de pago, no equivalente general de todas las obligaciones CNBV.

9. España y Unión Europea: no discriminación, servicios de confianza y proceso

España requiere combinar derecho europeo y procesal. eIDAS, artículo 25, impide negar efectos o admisibilidad a una firma por ser electrónica o no cualificada; la firma cualificada

[103]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
[104]Ecuador. Reglamento a la Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos: incorporación de anexos, desmaterialización, integridad y verificación. Fuente oficial publicada por la Función Judicial. Fuente oficial en línea
[105]Ecuador. Resolución JPRM-2025-006-M, Registro Oficial Suplemento 104, 18-08-2025: operación, validez, compensación, liquidación y disponibilidad de fondos en sistemas de pago. Fuente oficial en línea

tiene efecto equivalente a la manuscrita; el 26 define requisitos de firma avanzada; el 46 impide negar efectos y admisibilidad al documento por su formato. La Ley 6/2020 regula determinados servicios electrónicos de confianza y derogó la Ley 59/2003 y el artículo 25 de la LSSI. Por tanto, citar la antigua Ley de Firma Electrónica como vigente sería un error de actualización. La equivalencia funcional se concentra en no discriminación, niveles de firma y servicios de confianza, no en copiar la estructura mexicana.[106][107]

La LEC consolidada, actualizada el 7 de octubre de 2026, distingue autenticidad y valoración. El artículo 326 regula documentos privados y su impugnación; sus apartados 3 y 4 tratan documentos electrónicos y servicios de confianza no cualificados y cualificados, con presunciones en el caso previsto. El 384 regula instrumentos para archivar, conocer o reproducir datos: examen con participación de las partes, documentación y custodia, y valoración conforme a sana crítica. La propia ley permite cuestionar autenticidad, integridad, precisión de fecha y hora u otras características. Así, presentar un documento electrónico no cierra el debate técnico; lo abre con un objeto verificable y contradictorio.[108]

Servicios de pago	Regla española	Aplicación técnica
RD-ley 19/2018, art. 45	Restitución por operación no autorizada con las condiciones y excepciones previstas, incluida la sospecha razonada de fraude comunicada por escrito.	Distinguir ausencia de autorización jurídica de simple discrepancia sobre dispositivo o credenciales.
Art. 66	Marco de gestión de riesgos, controles y procedimientos de gestión/clasificación de incidentes; evaluación al menos anual.	Solicitar evaluaciones y controles pertinentes, no asumir que acreditan una operación concreta.
Art. 67	Notificación inmediata al Banco de España de incidentes graves; información a usuarios sin dilación indebida cuando afecte o pueda afectar sus intereses.	Preservar cronología de detección, clasificación, aviso y medidas de mitigación.

Fuentes de la tabla: [109]

[106]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
[107]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
[108]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
[109]España. Real Decreto-ley 19/2018, artículos 45, 66 y 67: restitución por operaciones no autorizadas, gestión de riesgos y notificación inmediata de incidentes graves. Fuente oficial en línea

10. Comparación funcional de registros e incidentes financieros

La tabla siguiente evita una simplificación frecuente: presentar cualquier norma de ciberseguridad como “el equivalente” de los artículos 316 Bis y siguientes. En realidad hay varias funciones: emitir comprobantes, notificar al usuario, controlar acceso, registrar autenticación, conservar bitácoras, investigar incidentes, informar al regulador y asignar responsabilidad por operaciones no reconocidas. Una jurisdicción puede cubrir esas funciones en instrumentos separados. El peritaje debe construir una lista de datos necesarios y solo después localizar su fundamento, no comenzar con una petición genérica de “todos los registros que existan”.

Los plazos que aparecen son deliberadamente pocos y están vinculados al texto leído. No se traslada el plazo mexicano de 180 días a Argentina ni el de cinco días naturales de la CNBV a Perú o España. Cuando no se verificó un plazo, la celda no lo inventa. Para conservación probatoria, el manual puede recomendar preservar inmediatamente una copia y solicitar el dato al custodio sin esperar al vencimiento mínimo de retención, porque la retención regulatoria no garantiza disponibilidad indefinida ni cobertura de todos los eventos relevantes.

México

Jurisdicción	Regla, alcance y límite
Registros/autenticación	CNBV 316 Bis 11 y 15: acceso y bitácoras.
Incidentes	316 Bis 12: investigación y aviso.
Operaciones no reconocidas	316 Bis 14: incidencias y operaciones no reconocidas.
Plazo verificado y alcance	180 días para bitácoras del 316 Bis 15; cinco años para 316 Bis 14; aviso de cinco días naturales del 316 Bis 12, en sus respectivos ámbitos.

Fuentes de la tabla: [110]

Perú

Jurisdicción	Regla, alcance y límite
Registros/autenticación	SBS 504-2021, 17.3–17.4: enrolamiento, intentos y operaciones; monitoreo.
Incidentes	12.6.g y 15: preservación, reporte y análisis forense.

[110] Disposiciones de carácter general aplicables a las instituciones de crédito, artículos 316 Bis, 316 Bis 1, 316 Bis 10 a 17: comprobantes, cifrado, acceso, incidentes, incidencias, bitácoras y revisiones. Fuente oficial en línea

Jurisdicción	Regla, alcance y límite
Operaciones no reconocidas	SBS 2286-2024 modifica 20.3 y responsabilidad salvo prueba de responsabilidad del usuario.
Plazo verificado y alcance	No se extrapola un plazo único; leer regla y modificatorias aplicables.

Fuentes de la tabla: [111]

Chile

Jurisdicción	Regla, alcance y límite
Registros/autenticación	RAN 20-10; externalización y registros en 20-7.
Incidentes	RAN 20-8.
Operaciones no reconocidas	Requiere norma específica del producto y canal.
Plazo verificado y alcance	No se atribuyen plazos no verificados.

Fuentes de la tabla: [112]

Argentina

Jurisdicción	Regla, alcance y límite
Registros/autenticación	BCRA A 7783: transacciones y eventos de seguridad.
Incidentes	BCRA A 8280: respuesta, recuperación y reporte final.
Operaciones no reconocidas	Reglas por canal y normativa de usuario; no inferirlas solo de autenticación.
Plazo verificado y alcance	Registros digitales al menos 90 días en A 7783; reporte final dentro de cinco días corridos en el supuesto de A 8280.

[111]Perú. SBS 2286-2024: modificación del artículo 20.3 sobre determinadas operaciones no reconocidas y responsabilidad, salvo acreditación de responsabilidad del usuario. Fuente oficial en línea
[112]Chile. Recopilación Actualizada de Normas, capítulos 20-7, 20-8 y 20-10: externalización, incidentes operacionales, seguridad de la información y ciberseguridad. Fuente oficial en línea

Fuentes de la tabla: [113]

Colombia

Jurisdicción	Regla, alcance y límite
Registros/autenticación	Ley 527 para conservación general; SFC para supervisión.
Incidentes	CE 033 de 2020 identificada como instrucción en la materia.
Operaciones no reconocidas	No acreditada una regla textual suficiente en esta revisión.
Plazo verificado y alcance	Confirmar numerales y texto oficial antes de usar plazos o campos obligatorios.

Fuentes de la tabla: [114]

Ecuador

Jurisdicción	Regla, alcance y límite
Registros/autenticación	Ley 67.8 para mensaje; JPRM-2025-006-M para sistema de pagos.
Incidentes	No acreditada equivalencia integral con CNBV.
Operaciones no reconocidas	Requiere régimen específico de entidad y canal.
Plazo verificado y alcance	No se inventa plazo de bitácora o incidente.

Fuentes de la tabla: [115]

España

Jurisdicción	Regla, alcance y límite
Registros/autenticación	RD-ley 19/2018, 66: riesgos y controles.

[113]Argentina. BCRA Comunicación A 7783: registros de transacciones digitales disponibles al menos 90 días y monitoreo de eventos de seguridad. Fuente oficial en línea
[114]Colombia. Superintendencia Financiera. Circular Externa 033 de 2020, identificada como instrucción de seguridad y ciberseguridad; sus numerales deben confirmarse antes de imponer obligaciones específicas. Fuente oficial en línea
[115]Ecuador. Resolución JPRM-2025-006-M, Registro Oficial Suplemento 104, 18-08-2025: operación, validez, compensación, liquidación y disponibilidad de fondos en sistemas de pago. Fuente oficial en línea

Jurisdicción	Regla, alcance y límite
Incidentes	Art. 67: incidentes graves y aviso a usuarios.
Operaciones no reconocidas	Art. 45: restitución bajo condiciones y excepciones.
Plazo verificado y alcance	Incidente grave: inmediato; evaluación de riesgos al menos anual; datos estadísticos al menos anuales.

Fuentes de la tabla: [116]

11. Estándares metodológicos internacionales

ISO/IEC 27037:2012 proporciona directrices para identificación, recolección, adquisición y preservación de evidencia digital potencial. La ficha oficial de ISO indica que la edición fue revisada y confirmada en 2018 y permanece vigente. Sus definiciones permiten precisar identificación, preservación, imagen bit a bit, repetibilidad y reproducibilidad. El estándar sirve para construir procedimientos y controles, no para declarar que un documento es auténtico o admisible por haber usado una herramienta concreta. Tampoco sustituye las reglas de cada jurisdicción ni la valoración judicial.[117]

NIST SP 800-86 organiza el proceso en recolección, examen, análisis e informe y conecta archivos, sistemas operativos, tráfico y aplicaciones con la respuesta a incidentes. La guía advierte que no es un procedimiento universal ni asesoría jurídica. Para el manual, su aporte es estructurar fuentes y documentación; para los anexos jurídicos, su condición es guía técnica. Una buena práctica consiste en mapear cada fase con evidencia de trabajo: identificación de fuente y autoridad, adquisición documentada, verificación, hallazgos, hipótesis alternativas y conclusiones delimitadas. La meta no es fabricar certeza, sino hacer visible qué se hizo, qué puede repetirse y qué sigue sin demostrarse.[118]

Fase del manual	Referencia metodológica	Evidencia de calidad exigible
Identificación	ISO/IEC 27037	Fuente, custodio, estado, autoridad, riesgo de alteración y prioridad.
Adquisición	ISO/IEC 27037 y NIST SP 800-86	Método, herramienta/versión, fecha y zona, hash cuando proceda, incidencias y relación original/copia.

[116]España. Real Decreto-ley 19/2018, artículos 45, 66 y 67: restitución por operaciones no autorizadas, gestión de riesgos y notificación inmediata de incidentes graves. Fuente oficial en línea
[117]ISO/IEC 27037:2012. Directrices para identificación, recolección, adquisición y preservación de evidencia digital. Edición confirmada por ISO como vigente. Fuente oficial en línea
[118]NIST SP 800-86. Guide to Integrating Forensic Techniques into Incident Response. Guía metodológica, no legislación ni garantía de admisibilidad. Fuente oficial en línea

Fase del manual	Referencia metodológica	Evidencia de calidad exigible
Examen y análisis	NIST SP 800-86	Copia de trabajo, hipótesis, pruebas, resultados negativos y reproducibilidad.
Informe	NIST SP 800-86 y norma procesal local	Hechos, método, hallazgos, límites, anexos y contradicción posible.

12. Reglas para usar la matriz sin cometer falsas equivalencias

La primera regla es citar función + instrumento + artículo + ámbito + versión, no “la ley equivalente”. La segunda es conservar las diferencias: firma simple, avanzada, digital o cualificada; original electrónico y copia impresa; presunción de integridad y prueba de autoría; conservación archivística y custodia forense; registro de autenticación y consentimiento; admisibilidad y fuerza probatoria. La tercera es registrar la fecha de consulta y revisar reformas posteriores cuando el expediente lo requiera. La cuarta es no utilizar una norma bancaria para justificar cualquier investigación privada fuera de su ámbito subjetivo, ni una regla administrativa para resolver todo proceso civil o penal.

La segunda comprobación es material. Antes de cerrar el anexo del manual debe verificarse que cada enlace abra la fuente, que el artículo exista en el texto descargado, que no se haya atribuido a Perú un régimen general inexistente en la Ley 27269, que la modificatoria peruana sea SBS 2286-2024, que Argentina no reproduzca como vigente el artículo derogado por Ley 27.446 y que España no cite como vigente la Ley 59/2003. La transición mexicana debe mantener separadas la compilación CNPCF, la iniciativa de prórroga a 2030 y cualquier decreto efectivamente publicado. La regulación de IA de San Luis Potosí se documenta en un expediente independiente porque contiene reforma y derogación posterior, no una regla de custodia.

Control editorial	Pregunta de aceptación	Acción si falla
Identidad	¿El instrumento y el artículo aparecen literalmente en la fuente?	Retirar la cita o marcarla como no verificada.
Función	¿La norma regula realmente la función descrita?	Reclasificar como parcial/sectorial y explicar el límite.
Vigencia	¿La versión y las reformas son las aplicables al hecho?	Registrar fecha y realizar revisión específica en diario oficial.

Control editorial	Pregunta de aceptación	Acción si falla
Ámbito	¿Sujeto, canal y procedimiento están comprendidos?	No extender la regla; solicitar el régimen especial.
Efecto	¿Se distingue admisión, autenticidad, valor y carga probatoria?	Reescribir la conclusión sin presunciones automáticas.
Prueba técnica	¿El formato permite verificar lo que la norma exige?	Preservar nativo, contexto, metadatos y proceso de exportación.

Conclusión operativa: el manual no necesita una tabla de frases parecidas, sino una guía para demostrar el mismo problema con reglas distintas. La equivalencia funcional útil es la que permite decidir qué preservar, qué solicitar, qué verificar y qué límite declarar. Todo lo que no pueda sostenerse con fuente y alcance comprobados debe quedar fuera o marcado expresamente como no acreditado.

Alcance del estudio
Aviso jurídico: este documento es material general de investigación y diseño editorial. No constituye asesoría legal, dictamen pericial ni opinión sobre un caso concreto. La aplicación a un expediente exige revisar la norma vigente al momento de los hechos, la jurisdicción, la materia, el canal y las reglas procesales correspondientes.

A.13 Aplicación práctica: seleccionar régimen antes que conclusión

Un expediente puede tocar varios países sin que todas sus normas se apliquen a todos los hechos. Una cuenta administrada en México, un proveedor en Chile y una operación cuestionada en España exigen separar lugar del hecho, sujeto regulado, canal, contrato, proceso y versión temporal. El primer paso no es traducir el artículo 210-A, sino identificar qué función se necesita: conservar el mensaje, acreditar atribución, obtener bitácoras, reconstruir autenticación o revisar una obligación de incidente. Después se localiza la norma que cumple esa función para ese sujeto y ese procedimiento.

Paso	Pregunta aplicada	Resultado documentado
Delimitar	¿Qué hecho, sujeto, canal y proceso se analiza?	Mapa de jurisdicción y alcance.
Localizar	¿Qué norma cubre la función en esa materia?	Instrumento, artículo, versión y fuente oficial.

Paso	Pregunta aplicada	Resultado documentado
Clasificar	¿La equivalencia es directa, parcial o sectorial?	Límite expreso y normas complementarias.
Preservar	¿Qué objeto permite comprobar el requisito?	Nativo, contexto, metadatos, exportación y custodia.
Concluir	¿Qué efecto está probado y cuál no?	Afirmación limitada, sin importar presunciones ajenas.

A.14 Protección de datos durante la investigación en México

La custodia forense no es una excepción general a la protección de datos. El tratamiento debe mantener finalidad, proporcionalidad, seguridad y confidencialidad; el expediente no se comparte completo solo porque sea más cómodo. Se separan versiones de trabajo y difusión, se restringen accesos y se evita conservar datos de terceros que no responden al encargo. Las vulneraciones significativas deben tratarse con la diligencia prevista por la legislación, incluida la información a las personas afectadas para que puedan defender sus derechos. La autoridad federal actual es la Secretaría Anticorrupción y Buen Gobierno, conforme a la transición iniciada en marzo de 2025.[119][120]

Regla comparada
La equivalencia jurídica útil termina en una decisión verificable: qué conservar, qué solicitar, qué comprobar y qué no afirmar. Si el análisis no cambia ninguna de esas respuestas, la cita es decorativa.

[119]Ley Federal de Protección de Datos Personales en Posesión de los Particulares, nueva ley publicada el 20-03-2025 y reformada el 14-11-2025. Artículos 5–9, 18–20 y 31: principios, seguridad, confidencialidad, vulneraciones y plazos. Fuente oficial en línea

[120]Secretaría Anticorrupción y Buen Gobierno. Comunicado 011, 21-03-2025: transición de funciones de protección de datos personales del INAI a la Secretaría. Fuente oficial en línea

Anexo B. Ficha de alcance y autoridad

Esta ficha se completa antes de acceder a la fuente. Su función es impedir que el encargo crezca por impulso o que una capacidad técnica se confunda con permiso. Si cambia el objeto, el período o la finalidad, se crea una versión nueva y se conserva la anterior. Todo campo no disponible debe explicar el motivo y la persona que puede resolverlo.

B.1 Contenido del formato

Campo	Contenido requerido	Ejemplo ficticio completo
Identificador	Código del caso sin nombre de cliente ni datos sensibles.	EXP-DEMO-2026-001.
Finalidad	Uso previsto: continuidad, investigación interna, peritaje o proceso.	Determinar registro, transmisión y liquidación de ventas reclamadas.
Versiones separadas	Qué afirma cada parte, sin presentarlo como hecho probado.	Comercio: ventas no pagadas. Procesador: operaciones no recibidas.
Período	Inicio, fin, zona y precisión necesaria.	1 al 3 de noviembre de 2026, hora local −06:00.
Fuentes incluidas	Sistemas, archivos, cuentas y dispositivos autorizados.	Remesas, reportes de procesador y abonos bancarios de tres referencias.
Exclusiones	Qué no se revisará y por qué.	Dispositivos personales y correos fuera de las referencias del caso.
Autoridad	Titular que autoriza, instrumento, acciones permitidas y vigencia.	Representante autorizado; consulta y exportación administrativa documentada.
Riesgos	Volatilidad, privacidad, continuidad, terceros y puntos de no retorno.	Rotación de registros y datos personales de compradores no relacionados.
Entregable	Producto, formato, destinatarios, canal y revisión.	Informe técnico, manifiesto y exportaciones; entrega cifrada al responsable.

Campo	Contenido requerido	Ejemplo ficticio completo
Control de cambios	Versión, fecha, solicitante, autorizador y efecto en fuentes.	A01: se agrega diccionario de campos del procesador, sin ampliar dispositivos.

Condición de inicio
No se ejecuta la adquisición hasta que alcance, autoridad y exclusiones puedan responderse. Si una urgencia obliga a actuar, se registra la decisión excepcional, su fundamento y el límite de lo realizado.

Anexo C. Acta de recepción y preservación inicial

El acta se llena al recibir el objeto, no al terminar el análisis. Describe lo observado y lo declarado por quien entrega por separado. La fotografía se relaciona con el identificador, pero no sustituye la descripción. Si se desconoce una acción previa, se escribe “se desconoce” con su explicación; no se sustituye por una suposición tranquilizadora.

C.1 Ejemplo de acta física

Campo	Registro ficticio
Caso y evidencia	EXP-DEMO-2026-001 · ED-20261109-DEMO-SSD-003-R00.
Objeto	Unidad SSD SATA de 2.5 pulgadas, capacidad declarada 512 GB; número de serie visible DEMO-003.
Entrega	Custodio A, responsable administrativo autorizado; 9 de noviembre de 2026, 14:32 −06:00.
Recepción	Analista B, especialista asignado; laboratorio de recepción.
Estado observado	Apagado y desconectado; carcasa sin deformación visible; conector sin residuo aparente.
Accesorios	Cable SATA y fuente registrados como objetos relacionados ACC-003-01 y ACC-003-02.
Historia declarada	La unidad fue retirada por personal de sistemas; se desconoce si fue conectada después del incidente.
Fotografías	FOT-003-01 general; FOT-003-02 serie; FOT-003-03 conectores y accesorios.
Embalaje y sello	Bolsa antiestática dentro de contenedor rígido; sello SL-DEMO-003 íntegro.
Decisión inicial	Preservar, validar bloqueador y preparar adquisición física autorizada.
Observaciones	No se encendió ni exploró durante recepción. Sin contraseñas escritas en el acta.

C.2 Recepción de archivos o mensajes

Para recepción electrónica se sustituyen los campos de estado físico por canal, cuenta, remitente aparente, URL o mensaje, permisos, nombres originales, tamaños y fecha de descarga. El archivo se preserva antes de renombrar o convertir. Si proviene de correo, se conserva el EML y se calculan huellas separadas para mensaje y adjuntos. Si proviene de enlace, se registra quién accedió y qué versión estaba disponible.

Control	Ejemplo ficticio
Canal y mensaje	Correo del proveedor recibido el 9 de noviembre de 2026, 15:02 −06:00.
Objeto completo	entrega_001.eml preservado con cuerpo, encabezados y dos adjuntos.
Adjuntos	registros.csv y diccionario.pdf; nombres originales conservados en el manifiesto.
Declaración del proveedor	El cuerpo declara algoritmo SHA-256 y un valor para cada adjunto.
Verificación	Cálculo local documentado: registros.csv coincide; diccionario.pdf no coincide.
Tratamiento	No se edita ningún adjunto; se solicita aclaración y segunda entrega del PDF.
Límite	La coincidencia del CSV acredita igualdad con la entrega, no veracidad ni cobertura completa.

Anexo D. Registro de adquisición

El registro debe permitir comprender qué se copió, con qué cobertura y bajo qué condiciones. La herramienta no se cita como una marca de confianza: se acompaña de versión, configuración, validación y resultado. Los errores se conservan junto con la salida. Si se repite la adquisición, se crea un nuevo identificador y se explica la relación.

D.1 Ejemplo completo

Campo	Registro ficticio
Caso y adquisición	EXP-DEMO-2026-001 · ED-20261109-DEMO-SSD-003-A01.
Fuente relacionada	ED-20261109-DEMO-SSD-003-R00, identificada en acta de recepción.
Objetivo y cobertura	Imagen física del medio completo, incluido espacio no asignado, para examen posterior.
Autoridad	Ficha A01; alcance limitado al SSD recibido y al incidente delimitado.
Conexión	Fuente conectada al bloqueador de escritura y este a la estación; modelo y puertos anotados en bitácora.
Herramienta	Herramienta validada para imagen de prueba; nombre, versión y configuración en registro técnico.
Fecha y zona	Inicio 2026-11-09T15:21:08−06:00; fin 2026-11-09T16:47:52−06:00.
Salida	ssd003_A01.e01 y archivo de registro; copia de trabajo separada del original preservado.
Integridad	Algoritmo SHA-256; valor asociado al archivo de imagen en el manifiesto controlado.
Incidencias	Doce sectores ilegibles documentados; no se oculta el mensaje ni se declara adquisición perfecta.
Verificación	La salida abre, el tamaño es coherente con el medio y el valor de verificación coincide.

Campo	Registro ficticio
Cierre	Original resellado con nuevo identificador; sello anterior y apertura registrados en custodia.

Criterio de aceptación
No basta que el archivo exista. Debe abrirse, relacionarse con la fuente, describir su cobertura y conservar incidencias. Si una etapa no puede comprobarse, se anota antes de continuar.

Anexo E. Cadena de custodia y transferencias

La bitácora registra eventos, no solamente traslados. Abrir un sello, crear una copia, descargar un archivo o consultar un contenedor también puede cambiar quién responde y qué debe verificarse. Cada fila relaciona objeto, responsables, propósito, ubicación, sello e integridad. Las claves nunca se escriben en este formato.

E.1 Ejemplo de secuencia

Evento	Responsables y propósito	Verificación y resultado
Recepción 09-11 14:32 −06	Custodio A entrega SSD-003 a analista B para preservación.	Serie y fotografías coinciden; sello SL-003 íntegro.
Apertura 09-11 15:18 −06	Analista B abre contenedor para adquisición autorizada.	Se conserva sello previo y motivo; no hay cambio de objeto.
Adquisición 09-11 15:21 −06	Analista B genera A01 sobre estación validada.	Salida, incidencias y hash quedan en registro D.
Resello 09-11 16:55 −06	Analista B devuelve fuente a contenedor.	Nuevo sello SL-003-B; original separado de copia de trabajo.
Transferencia 10-11 09:10 −06	Custodio C entrega copia A01 a revisor D mediante canal cifrado.	Destinatario, permisos, descarga y verificación hash confirmados.
Consulta 10-11 11:42 −06	Revisor D abre copia para revisar matriz de hipótesis.	Acceso registrado; ninguna modificación al original.

E.2 Transferencia electrónica

Una transferencia por enlace incluye emisor, destinatario, permisos, fecha de expiración, versión, canal de entrega de la llave y comprobación de descarga. La recepción no se presume porque el sistema diga “enviado”. El receptor confirma identidad del objeto, tamaño y hash cuando proceda. Si el enlace se sustituye, se conserva el historial de ambas entregas.

Anexo F. Solicitud y adquisición mediante proveedor

Este formato evita pedir “toda la información” y recibir una tabla sin contexto. La solicitud define la pregunta, los campos y la forma de entrega. La autorización se envía por canal seguro; el ejemplo no contiene datos reales. Si el proveedor no puede cumplir un punto, debe declararlo en la respuesta para que la limitación viaje con la evidencia.

F.1 Solicitud modelo

Solicitud ficticia de registros y entrega verificable
Asunto: EXP-DEMO-2026-001 · Registros del 1 al 3 de noviembre de 2026

Por el canal seguro autorizado, solicito los eventos asociados con las referencias incluidas en el expediente, comprendidos entre 2026-11-01T00:00:00−06:00 y 2026-11-03T23:59:59−06:00. Agradezco indicar zona usada por el sistema, horario de verano y regla de conversión.

Solicito, cuando estén disponibles: fecha/hora, tipo de evento, dirección, duración, identificadores, celda, tecnología, resultado y explicación de campos vacíos. Incluir formato nativo CSV/XLSX, copia PDF de consulta, diccionario de campos, proceso y fecha de extracción, filtros, cobertura y limitaciones de retención.

En el cuerpo de la respuesta, indicar para cada archivo el algoritmo y valor hash. Conservar la entrega en formato EML con cuerpo, encabezados y adjuntos. No remitir claves ni credenciales en ese correo.

Responsable técnico autorizado · EXP-DEMO-2026-001

F.2 Registro de exportación o API

Campo	Ejemplo ficticio
Cuenta y rol	Cuenta administrativa DEMO; rol de solo lectura y exportación.
Sistema y versión	Portal de proveedor; versión o fecha de interfaz documentada.
Consulta	Período, referencias y tipos de evento; filtros guardados en bitácora.

Campo	Ejemplo ficticio
Zona y formato	UTC declarado; CSV nativo y diccionario de campos.
API, si aplica	Endpoint, versión, parámetros, paginación y límites; sin secretos en el informe.
Resultado	Dos archivos, número de filas y errores de exportación registrados.
Entrega	EML completo, URL o canal controlado y fecha de descarga.
Verificación	Hash de cada objeto y relación con la declaración del proveedor.
Cobertura y límite	Retención disponible, datos ausentes y período no cubierto.

Anexo G. Inventario y manifiesto de objetos

El manifiesto relaciona objetos y evita que una carpeta se convierta en una colección sin procedencia. Cada fila corresponde a un archivo, imagen, exportación, visualización o informe. La ruta y el tamaño ayudan a identificarlo; el hash controla ese objeto específico. Los datos sensibles se omiten en versiones públicas sin destruir la versión completa de trabajo.

G.1 Ejemplo de manifiesto

Identificador	Relación y objeto	Control
DEMO-EML-001-R00	Correo original recibido; cuerpo, encabezados y adjuntos.	Nombre, tamaño, fecha de recepción y SHA-256 en registro controlado.
DEMO-CSV-001-R00	Adjunto registros.csv extraído sin modificación del EML.	Coincide con hash declarado en cuerpo; 18,420 filas.
DEMO-PDF-001-R00	Adjunto diccionario.pdf de la primera entrega.	Hash no coincide; conservado para comparación y aclaración.
DEMO-PDF-001-R01	Segunda entrega del diccionario; objeto distinto relacionado.	Nueva fecha y nuevo hash; no sustituye silenciosamente R00.
DEMO-CSV-001-W01	Copia de trabajo del CSV para consulta.	Derivada de R00; cambios de análisis se guardan aparte.
DEMO-INF-001-V10	Informe versión 1.0 y anexos referenciados.	Entrega cifrada; hash de distribución y receptor documentados.

Regla de nombres
El nombre operativo no borra el original. El manifiesto conserva el nombre recibido y añade el identificador interno, de modo que ordenar nunca signifique alterar la fuente.

Anexo H. Cronología y zonas horarias

La cronología separa lo que la fuente dice de la conversión que el analista realiza. Nunca se reemplaza el valor original por una fecha “corregida”. La precisión se expresa con la granularidad disponible: día, minuto, segundo o ventana. Si la sincronización no está acreditada, se registra como límite en lugar de convertir la hora en una certeza ficticia.

H.1 Ejemplo de línea de tiempo

Fuente y valor literal	Normalización	Lectura permitida
Servidor: 2026-11-03 20:14:07 UTC	2026-11-03 14:14:07 −06:00; precisión de segundos.	Evento observado en servidor; autoría física no demostrada.
Correo: 03 nov 2026 14:20:11 −06:00	Sin conversión; encabezado conservado en EML.	Recepción seis minutos después; proximidad no prueba causalidad.
Fotografía: 2026:11:03 14:16:00	Zona no declarada; reloj del dispositivo pendiente.	Compatible solo si se confirma zona y reloj; no se ordena como certeza.
Testimonio: “después de comer”	Ventana aproximada; no se asigna hora exacta.	Contexto declarado por persona, no registro técnico.
Exportación: del 1 al 3 de noviembre	Cobertura limitada; fuera de ese período no hay consulta.	La ausencia de eventos fuera del alcance no puede afirmarse.

H.2 Regla para fechas contradictorias

Primero se comprueba si los eventos pertenecen al mismo objeto y significado; después, zona, reloj, conversión, formato y proceso de exportación. Solo entonces se evalúa manipulación. La contradicción se conserva con ambos valores y su explicación posible. Una línea de tiempo útil muestra dónde está la duda en vez de ocultarla bajo una celda ordenada.

Anexo I. Matriz de hipótesis y corroboración

La matriz se formula antes de escribir las conclusiones. Debe incluir una comprobación capaz de debilitar cada hipótesis, no solo datos que la favorezcan. Cuando dos fuentes proceden del mismo archivo, se marca su dependencia; contarlas como corroboración independiente inflaría artificialmente el peso de la evidencia.

I.1 Ejemplo desarrollado

Elemento	Desarrollo ficticio
Afirmación	El archivo se creó por primera vez el 3 de noviembre en la cuenta del ex empleado.
Hipótesis A	Creación nueva en esa fecha mediante la cuenta asignada.
Hipótesis B	Copia o modificación posterior de un documento previo.
Hipótesis C	Uso de la cuenta por otra persona o sesión no controlada.
Fuentes	Archivo nativo, historial de nube, sesiones, segundo factor, respaldo anterior.
Comprobación	Comparar versión, autor de aplicación, sesión y dispositivo; revisar secuencia anterior.
Hallazgo	Versión previa del 28 de octubre y sesión desde dispositivo no registrado.
Efecto	Debilita creación nueva y atribución automática al titular.
Límite	No identifica todavía quién controlaba el dispositivo ni la intención.
Acción adicional	Solicitar registros de enrolamiento y actividad del dispositivo dentro del alcance autorizado.
Conclusión provisional	La fecha visible no acredita creación inicial; la cuenta no identifica por sí sola a la persona.

Decisión sin ego
Si el hallazgo contradice la hipótesis inicial, se cambia la hipótesis o la conclusión. No se cambia el objeto ni se omite el hallazgo para conservar una versión cómoda.

Anexo J. Revisión de contenido sintético

El objetivo no es obtener un porcentaje de “IA”, sino documentar origen, transformaciones y publicación. Generación, edición, transcodificación y regrabación son eventos distintos. El detector, si se utiliza, se registra con nombre, versión, configuración y limitaciones. Un resultado positivo o negativo no sustituye el archivo ni el contexto.

J.1 Formato aplicado

Campo	Ejemplo ficticio
Objeto recibido	video_publicado.mp4; enlace, cuenta, fecha y copia preservada.
Fuente anterior	Se desconoce archivo de generación; se solicita a titular y plataforma.
Historial	Publicación, descarga y conversión documentadas como eventos separados.
Herramienta declarada	No hay declaración del publicador; no se presume una herramienta concreta.
Análisis técnico	Codificación, fotogramas, audio, continuidad y metadatos disponibles.
Detector	Resultado orientativo; versión y límites documentados, sin veredicto automático.
Corroboración	Original de cámara, historial de edición y publicación temprana solicitados.
Contexto jurídico	Consentimiento, identidad, uso, conducta, fecha y norma vigente por separado.
Conclusión permitida	El archivo presenta transformaciones compatibles con edición; origen y autor no acreditados.
Fuente que cambiaría el resultado	Archivo original con historial verificable o registros del servicio de generación.

Anexo K. Estructura de informe y conclusión

La plantilla ordena el contenido, pero no reemplaza el razonamiento. Cada capítulo del informe responde una pregunta del lector y remite a anexos concretos. Los datos personales se limitan a lo necesario. El informe ejecutivo y el técnico pueden separarse para permitir lectura directiva y revisión especializada sin perder la relación entre ellos.

K.1 Secuencia recomendada

Sección	Pregunta que responde	Contenido mínimo
Encargo y alcance	¿Qué se pidió y qué quedó fuera?	Preguntas, finalidad, jurisdicción, período y exclusiones.
Autoridad y roles	¿Quién permitió y quién ejecutó?	Autorizaciones, funciones, comunicaciones y conflictos declarados.
Fuentes	¿Qué objetos se recibieron o adquirieron?	Manifiesto, identificadores, estados, representaciones y ausencias.
Método	¿Cómo se examinó y con qué cobertura?	Herramientas, versiones, parámetros, fechas, consultas e incidencias.
Hallazgos	¿Qué se observó?	Resultados positivos, negativos e inconclusos con referencia al objeto.
Análisis	¿Qué explicaciones se compararon?	Hipótesis, corroboración, contradicciones y falsas consecuencias evitadas.
Conclusiones	¿Qué puede afirmarse dentro del alcance?	Respuesta por pregunta, grado de afirmación y fundamento.
Limitaciones	¿Qué no se demostró?	Fuentes ausentes, cobertura, reloj, formatos, errores y acceso.

Sección	Pregunta que responde	Contenido mínimo
Anexos y entrega	¿Cómo se revisa?	Actas, adquisiciones, manifiesto, cronología, consultas y control de versión.

K.2 Ejemplo de conclusión completa

Conclusión ficticia

El archivo registros.csv recibido como adjunto del mensaje DEMO-EML-001-R00 presentó coincidencia SHA-256 con el valor declarado por el proveedor en el cuerpo del correo. Esto acredita igualdad entre el adjunto recibido y el archivo al que se refiere esa declaración. La exportación contiene 18,420 filas comprendidas entre el 1 y el 3 de noviembre de 2026, expresadas en UTC según el diccionario entregado. No se observaron eventos con las tres referencias consultadas dentro de esa cobertura. Este resultado no demuestra inexistencia de operaciones fuera del período, en otros canales o en registros no entregados, ni identifica a la persona que pudo realizarlas.

La conclusión anterior no necesita la frase “fehacientemente” ni una promesa de éxito judicial. Su fuerza está en que cada componente puede localizarse: mensaje, archivo, hash, filas, período, referencias y límite. Si la contraparte encuentra otra fuente, el análisis puede ampliarse sin destruir el trabajo anterior.

Anexo L. Listas de verificación operativa

Las listas se usan como control de salida, no como sustituto del juicio profesional. Cada respuesta afirmativa necesita evidencia localizable. “No aplica” requiere motivo. Si un control falla, se registra quién decide continuar, por qué y con qué limitación. Las preguntas pueden imprimirse y adaptarse al procedimiento sin convertirse en una declaración retrospectiva de acciones no realizadas.

L.1 Recepción y adquisición

Control	Evidencia esperada	Si falla
¿El alcance y la autoridad están documentados?	Ficha firmada o autorización verificable.	Detener y aclarar; registrar la excepción si existe.
¿El objeto tiene identificador y estado?	Acta, serie, fotografías y accesorios.	No analizar hasta resolver identidad o declarar límite.
¿La fuente y la copia están separadas?	Relación original/derivado y ubicación.	Crear copia controlada sin reescribir la recepción.
¿El método y la cobertura son claros?	Registro de adquisición, filtros y formato.	Completar bitácora con lo realmente ejecutado.
¿La salida abre y se verifica?	Prueba de apertura, manifiesto y hash pertinente.	Repetir como nuevo objeto y conservar incidencia.
¿Se registraron errores y exclusiones?	Incidencias, filtros, campos ausentes y motivo.	No declarar exhaustividad; limitar conclusión.

L.2 Análisis, informe y entrega

Control	Pregunta de revisión	Resultado exigido
Trazabilidad	¿Cada conclusión regresa a hallazgo y fuente?	Ruta completa y anexos coincidentes.

Control	Pregunta de revisión	Resultado exigido
Cronología	¿Se conservan valores literales, zonas y precisiones?	Conversión explicada e incertidumbre visible.
Hipótesis	¿Se buscó lo que contradice la versión inicial?	Alternativas, resultados negativos e inconclusos.
Lenguaje	¿Integridad, autoría y veracidad están separadas?	Sin absolutos ni falsas consecuencias.
Contradicción	¿Otra persona intentó localizar fallas?	Observaciones, respuesta y cambios registrados.
Vigencia	¿Las normas corresponden a sujeto, materia y fecha?	Fuente oficial, versión, función y ámbito.
Entrega	¿Abre, se lee y contiene los anexos citados?	Paquete verificado, canal y recepción confirmados.
Privacidad	¿La versión difundida evita exposición innecesaria?	Acceso, minimización y versiones controladas.

Anexo M. Control de versiones, fuentes y lecciones

El control de versiones distingue el expediente histórico del procedimiento vigente. Una acta pasada no se modifica para parecer actualizada; una guía sí se corrige cuando cambia la norma o la herramienta. Cada cambio indica razón, fuente, responsable, fecha y efecto. Las fuentes no verificadas no se presentan como si lo estuvieran.

M.1 Registro normativo y técnico

Elemento	Qué registrar	Ejemplo
Instrumento o herramienta	Nombre completo, materia, jurisdicción o versión.	CNPCF, artículos 348–350; herramienta y versión de validación.
Fuente y consulta	URL oficial, fecha, compilación y responsable.	Portal de Cámara de Diputados, consulta documentada.
Cambio detectado	Reforma, derogación, declaratoria o cambio de comportamiento.	Iniciativa separada de decreto; nueva versión de exportación.
Efecto funcional	Qué requisito o decisión cambia y para quién.	Actualizar régimen de transición o diccionario de campos.
Acción editorial	Capítulo, tabla o formato modificado.	Sustituir texto vigente y conservar historial.
Revisión	Persona, fecha, prueba y siguiente revisión por riesgo.	Comprobar artículo en fuente y probar ejemplo ficticio.

M.2 Lección convertida en mejora

Campo	Ejemplo ficticio
Incidencia	Se recibió una exportación sin zona horaria ni diccionario.
Impacto	No podía construirse una cronología fiable ni interpretar campos vacíos.
Causa	La solicitud anterior pedía “reporte completo” sin formato ni contexto.

Campo	Ejemplo ficticio
Corrección del caso	Se solicitó nueva entrega, conservando la primera y su limitación.
Cambio preventivo	El anexo F exige zona, diccionario, filtros, nativo, hash y EML.
Verificación	Ejercicio con proveedor ficticio: todos los campos llegan y pueden abrirse.
Responsable y versión	Revisor metodológico; formato F pasa de 1.0 a 1.1 con fecha y motivo.

Regla de continuidad
Una nueva versión no esconde la anterior. Permite saber qué se creía, qué cambió, con qué fuente y cómo afecta a los casos futuros, sin alterar los expedientes ya cerrados.