TEQUILA SO

TECNOLOGÍA EXPLICADA CON MÉTODO

Manejo de Evidencia Digital

Preservar, adquirir, analizar y presentar con método

GUÍA PRÁCTICA ILUSTRADA · EDICIÓN 2026



Jocsan Laguna

Edición 2026 · Texto, ejercicios y diagramas en español claro

Fotografía de reconstrucción editorial; no representa un caso real.

MANEJO DE EVIDENCIA DIGITAL · GUÍA DE LECTURA

Cómo usar este manual

Este manual explica cómo recibir, preservar, adquirir, trasladar, analizar y presentar evidencia digital con un método que otra persona pueda revisar. Está dirigido a primera respuesta, peritos, abogados, responsables de organizaciones y estudiantes. Cada término se traduce en una acción, un registro y un límite.

> **Regla central**
> No se trata de abrir un dispositivo para confirmar una sospecha. Se trata de decidir qué debe demostrarse, localizar dónde puede constar, elegir el método adecuado con menor alteración y documentar lo realizado, incluidos errores y resultados adversos.

Qué contiene cada recurso

Recurso	Lectura correcta
Fotografía nueva	Reconstrucción editorial hiperrealista de un entorno de trabajo; no documenta un caso real.
Diagrama propio	Explicación visual de decisiones, roles, objetos o razonamiento; no representa mediciones.
Laboratorio ficticio	Archivos creados para aprendizaje, con hashes reales de esos archivos, pero sin hechos reales detrás.
Ejercicio	Simulación con resultado esperado y criterio de evaluación; no afirma ejecuciones no realizadas.

Relación con la guía breve

La guía corta publicada como introducción al manual 01 conserva su función de lectura inicial. Este volumen desarrolla el procedimiento completo, los ejercicios y los formularios; no compite con esa introducción ni la sustituye como orientación rápida.

- Para recibir un caso: estudia los apartados 1, 3, 4 y 8.
- Para adquirir y analizar: trabaja los apartados 5, 6, 7, 9 y 10.
- Para informar y responder preguntas: utiliza los apartados 11, 12 y 18.

Autor: Jocsan Laguna · Proyecto: Tequila SO · Revisión editorial y visual: 16 de noviembre de 2026.

MAPA DEL MANUAL

Contenido y recorrido de aprendizaje

Cómo usar este manual 2
Contenido y recorrido de aprendizaje 3
1. Alcance, preguntas y autoridad 4
2. Original, copia, representación e integridad 5
3. Roles, responsabilidades y ciclo de vida 6
4. Recepción, embalaje y documentación 7
5. Adquisición local, remota y por proveedor 8
6. Registro técnico, incidencias y validación 9
7. Correo, EML, nube y sábanas de llamadas 10
8. Custodia, transferencias y conservación 11
9. Análisis, hipótesis y contradicciones 12
10. Cronología, zonas horarias y contexto 14
11. Informe, presentación y revisión independiente 15
12. Explicar a la autoridad sin falsa certeza 16
13. Errores frecuentes y mejora continua 17
14. Laboratorio ficticio y recorrido guiado 18
15. Ejercicios con resultados esperados 19
15. Ejercicios con resultados esperados (continuación) 20
16. Plantillas de alcance y recepción 21
17. Plantillas de adquisición e incidencias 22
18. Plantillas de custodia, informe y manifiesto 23
19. Fuentes metodológicas y marco de consulta 23
20. Créditos visuales y control editorial 24

Al terminar podrás

- Delimitar hecho, fuente, autoridad, método y entregable antes de actuar.
- Distinguir original, copia, representación, integridad, autenticidad, atribución y veracidad.
- Documentar recepción, adquisición, custodia, transferencias, incidencias y conservación.
- Preservar correo, archivos nativos, registros de proveedor y contexto temporal.
- Analizar hipótesis y contradicciones sin convertir una herramienta en veredicto.
- Explicar el trabajo a una autoridad en lenguaje claro, con límites comprensibles.
- Resolver seis ejercicios y utilizar formularios sin inventar datos faltantes.

HECHO · FUENTE · PERMISO · ENTREGABLE

1. Alcance, preguntas y autoridad

Un encargo útil no dice “revisa todo”. Indica qué ocurrió, qué afirma y qué niega cada parte, qué se necesita acreditar, para qué se utilizará el resultado y qué fecha límite existe. La respuesta determina fuentes, nivel de documentación y alteración justificable. Recuperar archivos para continuidad operativa no es idéntico a una pericial que será contradicha en un proceso.



Figura 1. Cuatro respuestas que ordenan el trabajo antes de acceder a la fuente. Diagrama propio.

Autoridad antes que acceso

La autorización debe identificar titular, sistemas, acciones permitidas, exclusiones, responsables y canal de comunicación. Si intervienen terceros, cuentas compartidas o proveedores, se documenta la vía legítima de obtención. Saber cómo acceder no concede permiso para hacerlo.

Pregunta inicial	Registro que evita improvisar
¿Qué afirma cada parte?	Versiones separadas por persona y fecha; ninguna se trata como hecho probado.
¿Qué se necesita demostrar?	Hecho, período, sistema, preguntas alternativas y resultado esperado.
¿Qué queda fuera?	Datos, dispositivos, cuentas y períodos excluidos; datos de terceros y confidencialidad.
¿Qué fuentes pueden desaparecer?	Volatilidad, retención, enlaces que expiran, sesiones y registros que rotan.
Cuándo detenerse	

Pregunta inicial	Registro que evita improvisar

> Si la autoridad o el alcance no están claros, si existe riesgo para personas o si continuar puede destruir evidencia, se pausa y se escala. Registra motivo, estado del objeto, acciones previas y siguiente responsable.

OBJETO · PROCEDENCIA · CONTROL · CONTEXTO

2. Original, copia, representación e integridad

El original no siempre es el aparato. Un archivo nativo, una imagen bit a bit, una exportación, una captura, una impresión y una traducción son representaciones distintas. Cada una puede ser útil si se conoce su relación con el origen y qué información conserva, transforma o pierde. La noción jurídica aplicable depende del régimen y del caso; técnicamente, la obligación es describir sin ambigüedad qué se recibió.

Cuatro preguntas que no son intercambiables

Concepto	Pregunta que responde	Error que debe evitarse
Integridad	¿El objeto permanece completo e inalterado dentro del alcance y las comprobaciones declaradas?	“El contenido es verdadero”.
Autenticidad	¿Hay base para sostener que el objeto es lo que se afirma?	“Coincide el hash; por tanto, es auténtico desde su origen”.
Atribución	¿Qué relación existe entre una acción o documento y un origen, cuenta o persona?	“La cuenta fue usada; por tanto, esta persona física actuó”.
Veracidad	¿Lo narrado ocurrió realmente?	“El archivo no cambió; por tanto, los hechos que relata son ciertos”.

El hash como control, no como dogma

Una función hash permite comparar objetos. Registra algoritmo, objeto exacto, ubicación, fecha, zona, operador y relación con la evidencia. Dos representaciones distintas pueden tener hashes diferentes sin que ello demuestre falsedad; una conversión cambia los bits aunque el contenido visible parezca equivalente.

> **Frase defendible**
> “El archivo recibido presentó un SHA-256 calculado en recepción y la verificación posterior coincidió. Esto demuestra que el objeto no cambió entre ambas comprobaciones; no demuestra por sí solo autoría, autenticidad de origen, totalidad ni veracidad del contenido”.

Conservación y accesibilidad

Conservar exige poder abrir, leer y relacionar el objeto con su contexto. Una copia visual ayuda a presentar, pero no elimina el archivo nativo ni sus metadatos disponibles. En México, el Código de Comercio aborda mensajes de datos, forma escrita, original e integridad; el CNPCF contiene reglas sobre información electrónica y su aplicación es gradual; la NOM-151-SCFI-2016 trata conservación y digitalización. Ninguna de estas referencias convierte toda copia en original ni certifica veracidad.

Código de Comercio: compilación oficial, artículos 89–94 y 1205

Código Nacional de Procedimientos Civiles y Familiares: artículos 348–350 y transitorios

NOM-151-SCFI-2016: publicación en el Diario Oficial de la Federación

FUNCIÓN · RESPONSABLE · CONTINUIDAD

3. Roles, responsabilidades y ciclo de vida

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



Figura 2. Funciones y ciclo documentado: cada etapa entrega registros a la siguiente. Diagrama propio.

Función	Responsabilidad y evidencia de trabajo
Autoridad del encargo	Define alcance, permisos, exclusiones y cambios aprobados.
Primera respuesta	Registra estado, acciones previas, riesgos, fotografías y necesidad de apoyo.
Especialista	Selecciona y ejecuta método; conserva parámetros, salidas, errores y verificación.
Custodio	Controla ubicación, accesos, transferencias, sellos y almacenamiento.

Función	Responsabilidad y evidencia de trabajo
Revisor	Contrasta identidad, cobertura, método, fechas, alternativas, conclusiones y límites.

Preparación antes del incidente

- Inventario de activos, propietarios, registros, formatos y períodos de retención.
- Contactos técnicos, jurídicos y de proveedores, con suplencia y canal seguro.
- Sincronización horaria y zona documentadas; formatos y procedimientos disponibles.
- Ejercicios con material ficticio y criterios de detención antes de una contingencia real.

> **Puntos de no retorno**
> Apagar, restablecer, reinstalar, suspender cuentas, cambiar servidores o cifrar sin conservar claves puede eliminar capacidad de análisis. Si una acción urgente es imprescindible, registra quién la autorizó, por qué, qué se preservó antes y qué se perdió.

ESTADO · IDENTIDAD · SELLO · PROCEDENCIA

4. Recepción, embalaje y documentación

El acta de recepción responde qué llegó, cómo llegó, quién entregó, quién recibió, cuándo, dónde y en qué estado. Incluye identificadores disponibles, accesorios, sellos, fotografías y observaciones. Si alguien ya abrió archivos o conectó el dispositivo, se registra: no se reescribe la historia para aparentar una recepción perfecta.

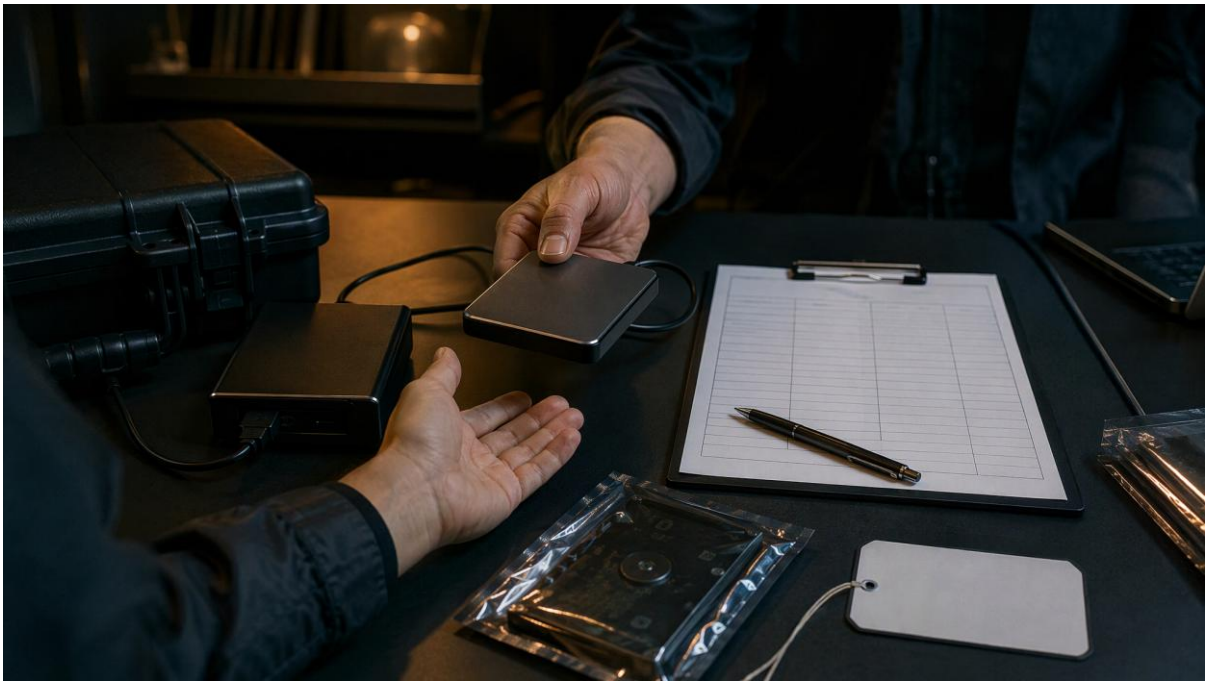


Figura 3. Entrega documentada de un dispositivo, con acta, identificadores y material de resguardo. Reconstrucción editorial hiperrealista; no es un caso real.

Datos mínimos de primera respuesta

- Identificador único de caso y objeto; convención estable y sin nombre de cliente.
- Fecha, hora, zona, lugar, entrega, recepción y función de cada participante.
- Marca, modelo, serie, capacidad, estado físico, accesorios y etiquetas previas.
- Encendido, bloqueo, red, batería, daños visibles y acciones previas conocidas.
- Fotografías generales y de identificadores, relacionadas con el objeto correcto.
- Riesgos de volatilidad, borrado remoto, exposición de terceros y decisión inicial.

Embalaje y sellado

El embalaje se elige según objeto y estado para reducir daño físico, electrostático, humedad, acceso no autorizado y sustitución. El sello incluye identificador, fecha y responsable. Si se abre para trabajar, se documenta y se repone según procedimiento, sin borrar el historial.

> **Antiestático no significa Faraday**
> La protección contra descargas y el aislamiento de radiofrecuencia cumplen funciones distintas. Documenta qué tecnología se usó, cómo se comprobó y qué conexiones quedaron activas.

COBERTURA · MENOR ALTERACIÓN · VALIDACIÓN

5. Adquisición local, remota y por proveedor

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 no existe otra vía. Ninguna debe presentarse como si conservara todas las propiedades de otra.



Figura 4. Rutas de adquisición y datos que deben quedar documentados. Diagrama propio.

Decisiones por escenario

Escenario	Decisión responsable	Límite que debe declararse
Equipo encendido	Evaluar memoria, sesiones, claves, conexiones, cifrado y alteración en curso antes de cambiar estado.	No hay regla universal de apagar o conservar encendido.
Teléfono	Valorar bloqueo, cifrado, red, sincronización, borrado remoto, batería y aislamiento real.	Una bolsa antiestática no equivale a aislamiento de radiofrecuencia.
Plataforma o nube	Solicitar exportación oficial, rol, filtros, período, zona, formato, campos y proceso.	La vista del usuario no cubre historial, registros administrativos ni todas las capas.
Visualización como última vía	Conservar URL, fecha, contexto, secuencia y método de captura.	No llamarla imagen completa, archivo nativo o exportación del proveedor.

Seguridad de personas y sistemas

No ejecutes muestras desconocidas en equipos personales o redes de producción. Usa entorno aislado, autorización y copias controladas; la curiosidad no justifica exponer a terceros.

HERRAMIENTA · PARÁMETROS · SALIDA · ERROR

6. Registro técnico, incidencias y validación

Una herramienta debe conocerse y validarse para el uso previsto. Registra nombre, versión, entorno, configuración, comando o parámetros, salida y prueba realizada. Una actualización puede cambiar comportamiento o formato; no se copia un procedimiento antiguo sin comprobarlo. La validación utiliza datos ficticios y demuestra que la salida puede abrirse y relacionarse con la fuente esperada.

Registro de adquisición por objeto

Campo	Qué debe quedar documentado
Fuente y custodio	Identificador exacto, tipo, estado, procedencia y persona que la conserva.
Método y justificación	Físico, lógico, volátil, remoto, proveedor o documental; relación con la pregunta.
Herramienta y validación	Nombre, versión, entorno, protección contra escritura y prueba para ese uso.
Parámetros	Filtros, campos, comandos, configuración, fecha, zona y operador.
Destino y salida	Ubicación separada, nombre, ruta, formato, tamaño y relación original/copia.
Integridad	Algoritmo, valor, momento y objeto cubierto por cada comprobación.
Verificación	Apertura, comparación, repetición cuando proceda, cobertura y revisor.

Campo	Qué debe quedar documentado
Incidencias	Errores, omisiones, sectores, accesos, interrupciones y efecto en el alcance.

Consultas que devuelven cero registros

Antes de concluir inexistencia, revisa filtros, cobertura, zona, retención, permisos, formato y errores. El informe describe qué se consultó y qué respuesta se obtuvo: “no se observó en este alcance” es más defendible que “nunca existió”.

Las incidencias también son expediente

Sectores ilegibles, archivos dañados, contraseñas ausentes, interrupciones de red, diferencias de hash y cambios de proveedor se conservan. Si repites una adquisición, asigna un nuevo identificador relacionado y explica el motivo; no elimines el primer intento para evitar una explicación incómoda.

> **Validación no es infalibilidad**
> Una prueba controlada demuestra comportamiento bajo condiciones conocidas. No garantiza que toda fuente, versión o caso producirá el mismo resultado.

MENSAJE · ADJUNTOS · CAMPOS · PROCEDENCIA

7. Correo, EML, nube y sábanas de llamadas

Un archivo EML suele conservar el mensaje con cuerpo, encabezados y adjuntos cuando existen, elementos que una captura aislada no reúne por completo. RFC 5322 especifica el formato de mensajes de Internet y distingue la sección de encabezados del cuerpo; MIME extiende el contenido. Esa estructura permite revisar qué se declaró en una entrega y relacionar archivos con esa declaración, no probar automáticamente la identidad física del remitente ni la veracidad del texto.



Figura 5. La entrega útil conserva mensaje, archivos y diccionario de campos como objetos relacionados. Diagrama propio.

Solicitud y recepción de sábanas de llamadas

Una sábana es una exportación de registros de telecomunicaciones. Para interpretarla se necesita período, zona, tipo de evento, dirección, duración, identificadores, celdas, tecnología, campos vacíos y método de extracción. Solicita formatos nativos disponibles, copia de consulta, diccionario y descripción del sistema o proceso que produjo el archivo.

Elemento	Qué solicitar y qué revisar al recibir
Período y zona	Inicio, fin, zona y horario de verano; coherencia de eventos y conversiones.
Formato y campos	CSV/XLSX/PDF disponibles, unidades, columnas, vacíos y proceso de extracción.
Integridad	Algoritmo y hash de cada archivo en el cuerpo de la respuesta cuando sea posible; cálculo local y comparación.
Entrega	EML con cuerpo, encabezados y adjuntos; enlace, permisos, versión y fecha si aplica.
Contexto	Tipo de evento, red, roaming, celdas e identificadores; alcance de cada campo.

Si el proveedor no entrega hash, se anota esa ausencia y se calcula uno local al recibir, dejando claro que solo acredita integridad desde ese instante. Si hay discrepancia, se conserva el archivo y se solicita aclaración sin editarlo. Una celda no demuestra ubicación exacta de una persona y un identificador técnico no equivale automáticamente a un usuario físico.

> **Buena práctica, no obligación universal**
> Esta guía propone solicitar hash en el cuerpo y conservar el EML para mantener el vínculo de la entrega. No afirma que todo proveedor esté obligado a hacerlo: la obligación concreta depende de norma, autoridad, canal y procedimiento aplicables.

RFC 5322: Internet Message Format, estructura de encabezados y cuerpo

OBJETO · RESPONSABLE · UBICACIÓN · VERIFICACIÓN

8. Custodia, transferencias y conservación

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.



Figura 6. La custodia se sostiene con relaciones verificables entre autoridad, preservación, análisis y presentación. Diagrama propio.

Movimientos que también deben registrarse

- Apertura de un contenedor o cambio de sello, aunque no haya traslado físico.
- Creación y ubicación de copias de trabajo, exportaciones y derivados.
- Préstamo temporal, cambio de ubicación, acceso remoto y descarga.
- Entrega incompleta, discrepancia, objeto no recibido y aclaración posterior.

Transferencias electrónicas

Un enlace necesita destinatario, permisos, canal, fecha, versión y verificación de descarga. El cifrado protege contenido; las claves se gestionan por canal separado y no se escriben en el acta. Si el proveedor cambia un archivo, debe existir nueva entrega y nueva huella, sin reemplazar silenciosamente el anterior.

Conservación útil

Original preservado y copia de trabajo se mantienen según política. Los respaldos se cifran, verifican y se prueba su recuperación. La migración documenta formato y relación, sin eliminar el original. La retención regulatoria, la política empresarial y la conservación probatoria no tienen el mismo fin ni plazo: se define por norma, caso y necesidad.

> **Acceso posterior**
> Un respaldo que nadie puede abrir no es conservación útil. Preserva documentación de formato, software necesario, claves autorizadas y contexto, con acceso restringido y registro de consultas.

OBSERVACIÓN · INFERENCIA · PREGUNTA ABIERTA

9. Análisis, hipótesis y contradicciones

El análisis comienza con afirmaciones que pueden confirmarse o debilitarse. Cada una se vincula con fuentes y pruebas capaces de discriminar explicaciones. El objetivo no es encontrar una

coincidencia y detenerse, sino buscar alternativas, resultados adversos y condiciones que cambiarían la conclusión.



Figura 7. Separar observación, inferencia y pregunta abierta evita convertir una interpretación en un hecho. Diagrama propio.

Matriz de razonamiento

Afirmación	Fuente y prueba	Alternativa	Resultado limitado
El archivo es original.	Procedencia, metadatos, formato y custodia.	Exportación, renombrado o edición previa.	Se acredita la representación recibida y su historia conocida.
El titular autorizó la operación.	Autenticación, dispositivo, sesión y registros.	Credenciales comprometidas o sesión compartida.	Se acredita uso de credenciales, no identidad física.
No existen otros archivos.	Consulta, filtros, cobertura y retención.	Filtro incorrecto, formato incompatible o fuente ausente.	No se observaron en el alcance consultado.
El video es continuo.	Nombres, estructura, fechas, capítulos y contenido.	Selección, conversión o reinicio de grabación.	La secuencia revisada no prueba por sí sola continuidad.

Repetibilidad y reproducibilidad

Documenta qué condiciones pueden cambiar: herramienta, versión, sistema, fuente, filtros y proveedor. Una coincidencia entre herramientas no elimina una hipótesis común compartida. Registra resultados positivos, negativos e inconclusos; no prometas repetir lo que depende de una fuente volátil.

Contenido sintético

Para material generado o manipulado con IA, separa generación, edición, conversión y publicación. Conserva original, historial, herramienta y versión cuando existan. Un detector aporta indicios con límites; no emite un veredicto universal de falsedad.

VALOR ORIGINAL · CONVERSIÓN · CORROBORACIÓN

10. Cronología, zonas horarias y contexto

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



Figura 8. La conversión nunca sustituye el valor original ni elimina la incertidumbre del reloj. Diagrama propio.

Tabla de correlación temporal

Evento ficticio	Valor original	Zona y fuente	Conversión y límite
Primera nota del laboratorio	2026-11-12T15:30:00Z	UTC; valor escrito en 01_notas.txt	09:30 en UTC−06:00; fecha inventada para práctica.
Segunda nota del laboratorio	2026-11-12T16:05:00Z	UTC; mismo archivo y contexto	10:05 en UTC−06:00; no prueba actividad real.
Revisión de imagen	2026-11-12T10:05:00−06:00	Nota manual de history-demo.txt	Coincide en formato con la segunda nota; no demuestra mismo actor ni causalidad.
Fecha sin zona	Hora visible sin sufijo	Reloj o fuente no documentada	No asumir UTC ni hora local; registrar la

Evento ficticio	Valor original	Zona y fuente	Conversión y límite
			ausencia y buscar contexto.

Una secuencia de nombres puede orientar capítulos o continuidad, pero no prueba por sí sola que un video esté completo. La ausencia de un capítulo es una pregunta, no una conclusión automática de edición maliciosa.

> **Precisión no es exactitud**
> Una fecha puede incluir segundos y seguir siendo incorrecta. La proximidad temporal tampoco demuestra causalidad, intención o identidad.

MÉTODO · HALLAZGO · LÍMITE · CONTRADICCIÓN

11. Informe, presentación y revisión independiente

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



Figura 9. Revisión independiente de informe, objetos y registros antes de la entrega. Reconstrucción editorial hiperrealista; no es un caso real.

Recorrido de revisión

1. Comprueba que caso, objeto, representación, origen y destino sean los correctos.
2. Repite o revisa consultas críticas con fuente, versión, parámetros, fecha y zona documentados.
3. Contrasta cada conclusión con hallazgos, alternativas, resultados negativos y fuentes ausentes.
4. Abre el archivo final, revisa texto, tablas, figuras, enlaces y anexos; calcula hash del entregable y conserva manifiesto.

Qué busca una revisión independiente

Busca errores, no culpables. Puede pedir repetir una consulta o añadir una fuente, pero no altera el original para hacerlo coincidir con el borrador. Una revisión que solo confirma lo que el analista ya escribió no es independiente.

> **Expediente antes que autoridad personal**
> Las preguntas difíciles se responden mostrando objeto, método y razonamiento. Si algo no está documentado, se reconoce y se corrige el alcance; no se rellena con memoria o seguridad personal.

LENGUAJE CLARO · PRUEBA LOCALIZABLE · LÍMITES

12. Explicar a la autoridad sin falsa certeza

Una explicación técnica puede ser precisa sin ser inaccesible. En lugar de “se efectuó la adquisición forense de evidencias”, escribe “se creó una copia controlada del disco y se registró su integridad”. La persona que decide debe seguir qué se recibió, qué se hizo, qué se observó y qué no puede concluirse.



Figura 10. Cuatro preguntas para explicar el trabajo a una autoridad sin fabricar certeza. Diagrama propio.

Ejemplo de explicación oral

> **Guion breve y defendible**
> “Recibí este archivo con este identificador y calculé su SHA-256. Después trabajé sobre una copia y volví a comprobarlo: los valores coinciden. Eso significa que el archivo no cambió entre esas dos comprobaciones. En su contenido observé estos campos y esta fecha. No significa que el hash demuestre quién lo creó, que lo que dice sea verdadero o que el archivo esté completo desde su origen. Para eso revisé —o falta revisar— estas otras fuentes”.

Lenguaje que evita sobreactuación

Evita	Escribe o explica en su lugar
“La evidencia es auténtica porque el hash coincide”.	“El objeto no cambió entre estas dos verificaciones documentadas”.
“No existía actividad”.	“No observé actividad en esta fuente, período, filtros y cobertura”.
“La IP identifica a la persona”.	“El registro asocia un evento con una dirección IP en ese momento; hace falta contexto y corroboración”.
“El detector confirmó que es falso”.	“El detector aporta un indicio que debe compararse con original, historial y otras señales”.
“Sin falsa evidencia”.	“Sin afirmar hechos, ejecuciones, capturas o resultados que no puedo demostrar”.

La presentación ejecutiva resume qué se revisó, qué se encontró y qué decisión puede tomarse. El detalle técnico queda en anexos para que otra persona cualificada pueda repetirlo. La valoración jurídica corresponde a la autoridad y al marco aplicable, no a una frase automática del informe.

PREVENCIÓN · INCIDENCIA · CORRECCIÓN · APRENDIZAJE

13. Errores frecuentes y mejora continua

Los errores más costosos suelen ser sencillos: abrir por curiosidad, apagar por costumbre, capturar sin URL, exportar sin zona, confundir original con impresión, asignar una IP a una persona, presentar un hash como prueba total o citar una norma derogada. Cuando el error ya ocurrió, se documenta sin inventar una cadena perfecta.

Error	Consecuencia	Respuesta correcta
Apagar por regla universal	Pérdida de memoria, sesiones o claves.	Evaluar estado, autoridad y pregunta antes de decidir.
Antiestático como Faraday	Falsa sensación de aislamiento.	Usar tecnología adecuada y verificar el aislamiento real.
Renombrar antes de preservar	Se pierde relación con el objeto recibido.	Conservar nombre original y relacionar copias en manifiesto.
Copiar hash en nota separada	Se pierde vínculo con entrega y declaración.	Conservar EML, cuerpo, encabezados y adjuntos relacionados.
Eliminar primer intento fallido	Desaparece trazabilidad de la incidencia.	Conservar ambos objetos con identificadores y motivo.
Confiar en detector de IA	Conclusión falsa de origen o falsedad.	Corroborar fuente, método, historial y contexto.

Error	Consecuencia	Respuesta correcta
Citar norma sin vigencia	Se afirma una regla inaplicable o inexistente.	Revisar fuente oficial, transitorios, ámbito y fecha del hecho.
Ocultar resultados adversos	El informe deja de ser revisable.	Incluir contradicciones, ausencias, errores y preguntas abiertas.

Mejora continua comprobable

- Asigna cada mejora a responsable, fecha, evidencia de implementación y ejercicio de comprobación.
- Actualiza cuerpo, formularios y preguntas frecuentes; no acumules notas contradictorias al final.
- Registra versión de herramienta, plataforma, norma y manual que motivó cada cambio.
- No fabriques cumplimiento anterior: indica desde cuándo entra en vigor la nueva práctica.

Cinco preguntas para toda la organización
Quién autoriza, dónde está la evidencia, cómo se obtuvo, quién ha accedido y qué puede afirmarse. Si alguna respuesta falta, el plan debe recuperarla o limitar la conclusión.

ARCHIVOS REALES DEL PAQUETE · HECHOS INVENTADOS

14. Laboratorio ficticio y recorrido guiado

Laboratorio_Forense_Jocsan.zip acompaña esta edición. Contiene documentos creados para enseñar, no una captura de sistema, una conversación real ni un caso judicial. Los hashes de SHA256SUMS.txt sí corresponden a los archivos del paquete; las fechas y actividades narradas son ficticias. Conserva el ZIP sin cambios y trabaja sobre una copia descomprimida.

Archivo	Uso correcto en la práctica
00_LEEME.txt	Alcance, advertencias y contenido del paquete.
01_notas.txt	Palabra “lavanda” y dos fechas UTC para integridad y conversión.
02_correo_demo.eml	Mensaje ficticio, sin envío, con dominios .invalid y sin adjuntos.
03_imagen_demo.png	Composición gráfica ficticia; no una fotografía real.
04_documentos/datos-inventario.txt	Identificadores y relaciones para practicar manifiesto.
05_navegador/history-demo.txt	Notas para cronología manual; no es base de navegador.
metadatos-demo.json	Declaración del paquete, finalidad educativa y ausencia de memoria.
SHA256SUMS.txt	Valores para comprobar cada archivo antes del ejercicio.

Recorrido de preparación

1. Crea un registro de recepción para el ZIP con origen, fecha, zona, operador y finalidad educativa.
2. Calcula el hash del ZIP y conserva ese valor como comprobación del paquete recibido.
3. Descomprime una copia y verifica los archivos contra SHA256SUMS.txt.
4. Relaciona EML, documentos, imagen y notas en un manifiesto sin cambiar sus nombres.
5. Convierte las fechas en campos separados y registra las incertidumbres.
6. Redacta una salida con fuente, método, observación, límite y siguiente comprobación.

Lo que el laboratorio no contiene
No incluye memoria, binarios de sistema, base real de navegador, datos de clientes ni adjuntos en el EML. No afirmes que existen ni ejecutes procedimientos que requieren esas fuentes.

PRÁCTICA 1–3 · RECEPCIÓN, INTEGRIDAD Y CORREO

15. Ejercicios con resultados esperados

Ejercicio 1 · Delimitar antes de abrir

Consigna: recibes el laboratorio y una petición de “revisar todo para encontrar quién actuó”. Redacta alcance, fuentes, exclusiones y entregable sin prometer atribución.

Resultado esperado
El alcance es aprender recepción, integridad, correo, cronología e informe con archivos ficticios. Se excluyen discos personales, cuentas y fuentes no incluidas. El entregable es un registro de método y observaciones; no se promete identificar a una persona.

Criterio: 1 punto por alcance, 1 por fuentes y exclusiones, 1 por entregable limitado. “Revisar todo” no obtiene puntuación de método.

Ejercicio 2 · Integridad con objeto exacto

Consigna: verifica 01_notas.txt contra SHA256SUMS.txt y explica qué demuestra el resultado.

Resultado esperado
El SHA-256 calculado debe coincidir con 2a46845be1431df9ff506f876322d286e0e7cab52d5d0c199a470429a1ae7596 para el archivo distribuido en este paquete. La coincidencia vincula el objeto comprobado con el valor del manifiesto; no prueba que las notas sean hechos reales ni identifica autoría.

Criterio: 2 puntos por algoritmo y objeto correctos; 1 por explicar el límite. No se premia decir “hash válido = contenido verdadero”.

Ejercicio 3 · Leer el EML sin inventar entrega

Consigna: revisa 02_correo_demo.eml e identifica remitente aparente, destinatario, asunto, fecha, cuerpo y adjuntos.

Resultado esperado

From: remitente@example.invalid; To: analista@example.invalid; Subject: Revisión autorizada de ejemplo; Date: Thu, 12 Nov 2026 09:30:00 -0600. El cuerpo declara que es ficticio y no fue enviado ni recibido. No contiene adjuntos ni hash de adjuntos. Se conserva el EML completo y no se afirma envío real.

Criterio: 1 punto por campos, 1 por ausencia de adjuntos y 1 por límite de identidad y envío.

PRÁCTICA 4–6 · TIEMPO, INCIDENCIAS E INFORME

15. Ejercicios con resultados esperados (continuación)

Ejercicio 4 · Conversión y corroboración

Consigna: convierte las dos fechas de 01_notas.txt a UTC−06:00 y compáralas con history-demo.txt.

Resultado esperado

2026-11-12T15:30:00Z corresponde a 09:30 en UTC−06:00 y 2026-11-12T16:05:00Z a 10:05. La primera coincide en formato con la lectura inicial del historial ficticio y la segunda con la revisión de imagen. Se conservan valores originales y conversiones; la coincidencia no prueba mismo actor, causalidad ni hechos reales.

Criterio: 2 puntos por conversiones, 1 por conservar originales y 1 por límite interpretativo.

Ejercicio 5 · Discrepancia de hash

Consigna: en una copia de práctica cambias un carácter de 01_notas.txt y el hash deja de coincidir. Explica qué haces con original, copia e incidencia.

Resultado esperado

No se edita el archivo preservado. Se conservan original y copia modificada con identificadores distintos, se registra quién cambió qué, cuándo y con qué finalidad, y se documenta la diferencia de hash. No se reescribe SHA256SUMS.txt para ocultar la discrepancia.

Criterio: 2 puntos por preservar y relacionar objetos; 1 por incidencia; 1 por no alterar el manifiesto original.

Ejercicio 6 · Explicación para autoridad

Consigna: redacta una explicación de cinco líneas con fuente, método, observación, límite y siguiente comprobación.

Modelo de respuesta

Fuente: laboratorio ficticio identificado. Método: recepción, copia de trabajo, SHA-256, lectura de EML y conversión documentada. Observación: campos del mensaje y dos fechas convertidas. Límite: no hay envío real, memoria, adjuntos ni hechos reales. Siguiente comprobación: revisión independiente de manifiesto, hashes, cronología e informe final.

Criterio: 1 punto por cada línea clara y limitada. Una respuesta extensa que oculta ausencias no obtiene puntuación completa.

FORMULARIOS · CAMPOS OBLIGATORIOS · DECISIONES

16. Plantillas de alcance y recepción

Completa los campos antes de actuar. Si un dato crítico no está disponible, registra el motivo y quién debe confirmarlo; no lo completes retrospectivamente como si hubiera existido desde el inicio.

A. Ficha de alcance y autoridad

Campo	Contenido requerido
Identificador del encargo	Código único, versión y fecha de apertura.
Pregunta y finalidad	Hecho que debe acreditarse, uso del resultado y preguntas alternativas.
Período y zona	Inicio, fin, zona horaria y regla de conversión.
Fuentes incluidas	Sistemas, objetos, cuentas, custodios y representaciones autorizadas.
Exclusiones	Datos, dispositivos, personas, cuentas y períodos fuera del mandato.
Autorización	Titular, acciones permitidas, canal, responsables y cambios aprobados.
Entregable	Informe, anexos, destinatarios, confidencialidad y fecha límite.
Riesgos	Volatilidad, alteración, pérdida, datos de terceros y medidas de control.

B. Acta de recepción

Campo	Contenido requerido
Objeto e identificador	Tipo, marca, modelo, serie, capacidad, formato y código asignado.
Entrega y recepción	Nombre, función, fecha, hora, zona, lugar y canal.
Estado y accesorios	Encendido, bloqueo, red, daño, batería, etiquetas y accesorios.
Sello y embalaje	Tipo, identificador, condición y fotografías relacionadas.
Acciones previas	Aperturas, conexiones, copias, cambios o historia desconocida.
Decisión inicial	Preservar, escalar, adquirir o solicitar aclaración; responsable y motivo.

FUENTE · MÉTODO · SALIDA · EFECTO EN EL ALCANCE

17. Plantillas de adquisición e incidencias

C. Registro de adquisición

Campo	Contenido requerido
Fuente y custodio	Identificador exacto, procedencia, estado y persona que la conserva.
Método y justificación	Físico, lógico, volátil, remoto, proveedor o documental; relación con la pregunta.
Herramienta	Nombre, versión, entorno, configuración y validación para el uso previsto.
Parámetros	Comandos, filtros, campos, fecha, zona, operador y protección aplicada.
Salida y destino	Nombre, ruta, formato, tamaño, ubicación separada y relación original/copia.
Integridad	Algoritmo, valor, fecha, zona y objeto cubierto por cada valor.
Verificación	Apertura, comparación, repetición cuando proceda y revisor.
Cobertura	Qué incluye, qué excluye y qué fuentes o propiedades no conserva.

D. Registro de incidencias

Campo	Contenido requerido
Incidencia y objeto	Qué ocurrió, mensaje observado, objeto afectado, fecha y responsable.
Acciones previas	Qué se hizo antes y después; comandos, parámetros y decisiones.
Efecto	Impacto en integridad, cobertura, autenticidad, análisis o confidencialidad.
Respuesta	Aclaración, segunda entrega, nueva adquisición, limitación o detención.
Trazabilidad	Identificadores de objetos conservados, hashes y resolución del revisor.

Regla de conservación

Nunca elimines un intento fallido ni reescribas el registro para que el procedimiento parezca ideal. La corrección debe añadir trazabilidad, no borrarla.

TRANSFERENCIA · ESTRUCTURA · RELACIÓN DE OBJETOS

18. Plantillas de custodia, informe y manifiesto

E. Cadena de custodia por evento

Campo	Contenido requerido
Fecha, hora y zona	Momento del evento y regla temporal utilizada.
Objeto y relación	Identificador, original, copia, derivado o entregable y procedencia.
Entrega y recepción	Nombre, función y confirmación de ambas partes.
Propósito y ubicación	Razón del movimiento o acceso y destino del objeto.
Sello e integridad	Condición del sello, algoritmo, valor y resultado cuando proceda.
Incidencia	Diferencia, objeto no recibido, apertura o condición extraordinaria.

F. Estructura del informe técnico

Apartado	Pregunta que debe responder
Encargo y alcance	Qué se solicitó, para qué y con qué exclusiones.
Fuentes y custodia	Qué se recibió, de quién, en qué representación y con qué historia.
Método	Qué se hizo, con qué herramienta, versión, parámetros, fecha y zona.
Hallazgos	Qué se observó y dónde puede localizarse en los objetos.
Análisis	Qué explicaciones son compatibles, se debilitan o quedan abiertas.
Conclusión y límites	Qué puede afirmarse y qué no se demostró dentro del alcance.
Anexos	Actas, manifiestos, hashes, consultas, incidencias y figuras.

G. Columnas del manifiesto

Identificador · nombre original · ruta · tipo de objeto · relación con origen · método de obtención · tamaño · formato · algoritmo · hash · fecha y zona · responsable · ubicación · incidencias · destino y observaciones. La versión pública omite datos sensibles sin alterar el objeto preservado.

DOCUMENTACIÓN · VIGENCIA · ALCANCE DE LAS CITAS

19. Fuentes metodológicas y marco de consulta

Metodología y formatos

1. NIST SP 800-86: recolección, examen, análisis e informe; trabajo sobre copias e integridad.

2. ISO/IEC 27037: identificación, recolección, adquisición y preservación de evidencia digital.

3. RFC 5322: formato de mensajes de Internet, encabezados y cuerpo.

4. RFC 2045: formato MIME y estructura de contenido de mensajes.

Fuentes oficiales mexicanas de consulta

5. Código de Comercio: mensajes de datos, original, integridad y conservación.

6. Código Nacional de Procedimientos Civiles y Familiares y sus transitorios.

7. NOM-151-SCFI-2016: conservación de mensajes de datos y digitalización.

Cómo se utilizan

NIST e ISO son referencias metodológicas, no leyes ni garantías de validez. RFC describe formato, no autenticidad ni identidad física. Las normas jurídicas se consultan por función y ámbito; no se intercambian como si produjeran los mismos efectos en todo caso.

La compilación del Código de Comercio consultada muestra última reforma DOF 14-11-2025 y cantidades actualizadas mediante Acuerdo DOF 18-02-2026. La del CNPCF muestra última reforma DOF 15-01-2026 y transitorios de entrada en vigor gradual. La NOM-151 enlazada fue publicada el 30-03-2017. Antes de aplicar cualquier regla se comprueba nuevamente vigencia, declaratoria, jurisdicción, fecha del hecho y procedimiento.

> **Citas que no decoran conclusiones**
> Una regla de comprobantes no acredita toda autoría; una regla de conservación no certifica veracidad; una norma de incidentes no demuestra una transferencia concreta. La cita debe hablar exactamente de la afirmación que acompaña.

IMÁGENES · FUENTES · CIERRE

20. Créditos visuales y control editorial

Recurso	Procedencia y uso
Portada y figuras 3 y 9	Fotografías hiperrealistas nuevas creadas con apoyo de IA y revisadas visualmente. Reconstrucciones editoriales; no documentan casos reales.
Figuras 1, 2 y 4–8, 10	Diagramas propios creados para explicar alcance, funciones, adquisición, correo, custodia, análisis, tiempo y presentación. No representan mediciones.
Laboratorio	Archivos ficticios de Jocsan Laguna para práctica. Los valores de SHA256SUMS.txt corresponden a esos archivos; no convierten las narraciones en hechos reales.
Identidad Tequila SO	Escudo original aportado para esta línea editorial. No implica aval institucional adicional.
Tipografías	Manrope, Source Serif 4 e IBM Plex Mono, utilizadas en la línea editorial del proyecto.

Recurso	Procedencia y uso
Texto y ejercicios	Reorganización y ampliación del manual de Jocsan Laguna, con seis ejercicios, formularios y explicación en español claro.

Control editorial de esta edición

- Se conservó el contenido útil del original: recepción, adquisición, custodia, EML, sábanas, cronología, análisis e informe.
- Se añadieron diez figuras, seis ejercicios y formularios de alcance, recepción, adquisición, incidencias, custodia, informe y manifiesto.
- Se explicó el hash como control entre comprobaciones y se evitó presentarlo como prueba total.
- Se distinguió la solicitud de hash y EML como buena práctica, no como obligación universal de todo proveedor.
- Se revisó el material real del laboratorio y se evitaron ejecuciones, capturas o resultados inexistentes.
- Las traducciones y la serie 01–13 de otra línea editorial no forman parte de este trabajo.

Antes de un caso real
Comprueba autoridad, jurisdicción, norma vigente, herramienta, cobertura y revisión profesional. Esta guía es educativa; no constituye dictamen pericial ni asesoría jurídica sobre un caso concreto.

La idea que debe quedar

La evidencia digital se vuelve más comprensible cuando cada objeto tiene procedencia, cada acción tiene registro y cada conclusión tiene un límite. El método no consiste en parecer infalible, sino en permitir que otra persona compruebe el trabajo y entienda exactamente hasta dónde llega.

Tequila SO · Jocsan Laguna · Edición 2026.