BIBLIOTECA
ACCCF

08
VOLUMEN

ACCCF / CONOCIMIENTO APLICADO

Manual de certificación de correos electrónicos, publicaciones y redes sociales

EML, encabezados, URL, archivos, publicaciones, trazabilidad y presentación

Conservar lo que permite revisar un mensaje o una publicación antes de que desaparezca, sin confundir una captura con la fuente ni una fecha de pantalla con una prueba de origen.

Coordinación editorial · Jocsan Laguna

Consejo Americano de Ciberseguridad y Cómputo Forense · 2026

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

Contenido

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

Presentación: conservar antes de que cambie . . . 4

Capítulo 1. Alcance y preparación . . . 4

1.1 Qué afirmación necesita demostrarse . . . 4

1.2 Preparar el entorno de captura . . . 5

Capítulo 2. El mensaje completo . . . 5

2.1 EML: cuerpo, encabezados y adjuntos . . . 5

2.2 Reenvío, descarga y conversión . . . 5

2.3 Adjuntos y entrega de terceros . . . 6

Capítulo 3. Autenticación del canal . . . 7

3.1 Encabezados Received y transporte . . . 7

3.2 DKIM, SPF y DMARC . . . 7

3.3 Fecha, Message-ID y contenido . . . 7

Capítulo 4. Archivos, URLs y publicaciones . . . 8

4.1 Registro completo de una URL . . . 8

4.2 Publicación, hilo y multimedia . . . 8

4.3 Archivo web y fechas de terceros . . . 9

Capítulo 5. Preservación y certificación documentada . . . 9

5.1 Acta de adquisición . . . 10

5.2 Custodia y control de acceso . . . 10

5.3 Certificación pericial, notarial o administrativa . . . 10

Capítulo 6. Retirada, denuncia y daño mediático . . . 10

6.1 Preservar antes de retirar . . . 10

6.2 Daño y alcance . . . 11

6.3 Caso integrado . . . 11

Anexo A. Formatos de preservación . . . 11

A.1 Acta de correo . . . 11

A.2 Registro de publicación 12

A.3 Manifiesto de objetos 12

A.4 Registro de solicitud de retirada 12

Anexo B. Marco jurídico y lista final 12

Presentación: conservar antes de que cambie

Una publicación puede editarse, una cuenta puede cerrarse, un archivo adjunto puede sustituirse y un enlace puede dejar de funcionar. La preservación busca registrar qué existía en un momento, dónde se encontraba, cómo se obtuvo y qué representación quedó. Una captura puede mostrar un fragmento, pero la revisión necesita el objeto completo y su contexto: URL, cuenta, fecha, zona, archivos, respuestas, metadatos y proceso de adquisición.

El correo ofrece un ejemplo claro. Si se conserva solo una imagen del mensaje, se pierden encabezados, estructura y adjuntos. Si se guarda solo el adjunto, se pierde la declaración que explica qué contiene y, en algunos casos, el hash que permite verificarlo. El EML reúne esos componentes y permite relacionarlos. No demuestra que todo lo afirmado sea verdadero ni que una persona concreta escribió el cuerpo.

La palabra “certificación” se usa aquí como proceso documentado, no como garantía universal. Una actuación notarial, una pericial, una constancia de conservación y una captura testiguada pueden tener funciones y efectos distintos. La persona que preserva debe decir qué hizo y qué puede probar; no añadir solemnidad para cubrir una fuente incompleta.

> **Regla de oro**
>
> Conservar contenido y contexto al mismo tiempo. Una imagen nítida de una publicación sin URL ni fecha es una referencia útil, no una reconstrucción completa del objeto.

Capítulo 1. Alcance y preparación

1.1 Qué afirmación necesita demostrarse

No es lo mismo probar que una publicación existió, que una cuenta la publicó, que una persona la escribió, que estaba disponible para el público, que contenía una amenaza o que una entrega ocurrió con un archivo concreto. La afirmación determina la fuente: publicación visible, exportación, EML, registros de plataforma, receptor, administrador o testigo. Si solo se necesita demostrar existencia en una fecha, no se infla el análisis hacia autoría.

Se delimita período, cuentas, URL, palabras clave, participantes, tipos de contenido y datos de terceros. También se define si la preservación se utilizará para una denuncia, una retirada, un proceso, una investigación interna o una constancia de archivo. La urgencia de conservar no elimina la necesidad de autoridad ni la protección de terceros.

Objetivo	Fuente prioritaria	Límite a declarar
Existencia de publicación	URL, contenido, página y preservación documentada.	No acredita autoría humana ni totalidad de la cuenta.
Contenido de correo	EML con cuerpo, encabezados y adjuntos.	No prueba veracidad del texto.
Entrega de archivos	Adjuntos, cuerpo, hash, descarga y manifiesto.	No acredita cobertura del sistema de origen.

Objetivo	Fuente prioritaria	Límite a declarar
Alcance público	Visibilidad, audiencia, enlace y evidencia de acceso.	No equivale a número real de lectores.
Autoría o control	Cuenta, sesiones, dispositivos y contexto.	Nombre visible no identifica a la persona.
Secuencia	Fechas, zona, respuestas, ediciones y referencias.	Captura aislada no ordena toda la historia.

1.2 Preparar el entorno de captura

Se utiliza un equipo y una cuenta autorizados, con fecha y zona registradas, navegador conocido y almacenamiento controlado. Se evita iniciar sesión con una cuenta personal que añada datos innecesarios a la evidencia. No se interactúa con la publicación más de lo necesario: responder, denunciar o compartir puede cambiar su alcance y avisar al autor.

Se preparan carpetas de original, copia de trabajo, capturas, exportaciones, registros y manifiesto. El contenido potencialmente ilegal o dañino no se distribuye al equipo entero. Se documenta la presencia y se entrega por canal restringido. Si existe riesgo para una persona, la prioridad es su seguridad y el contacto con los canales competentes, no una demostración técnica adicional.

> **Decisión previa**
>
> Si la publicación puede desaparecer y existe autoridad para conservarla, se registra primero el objeto y su contexto. Después se solicita retirada o revisión. Retirar antes de preservar puede dejar solo una afirmación sin fuente.

Capítulo 2. El mensaje completo

2.1 EML: cuerpo, encabezados y adjuntos

RFC 5322 describe el formato de mensajes de internet, con campos de encabezado y cuerpo. El EML permite conservar una representación del correo con esos componentes y los adjuntos que contenga. Se documenta cómo se obtuvo: exportación del cliente, descarga del servidor o entrega de otra persona. La procedencia cambia la interpretación, no se esconde bajo una extensión conocida.[1]

El archivo se preserva antes de abrirlo con herramientas que puedan modificarlo. Se calcula hash del EML y de los adjuntos por separado y se relaciona en el manifiesto. El cuerpo puede declarar un algoritmo y un valor para un archivo: se comprueba, no se copia en una nota separada. Si hay diferencia, se conserva la primera entrega y se solicita aclaración.

2.2 Reenvío, descarga y conversión

Reenviar un correo puede añadir encabezados y cambiar la relación entre mensaje y archivos. Imprimir a PDF conserva una visualización, no la estructura. Descargar desde webmail puede producir formatos distintos. Se registra cada operación y se conservan las versiones, sin tratar el reenvío como si fuera necesariamente el mensaje original.

Un mensaje reenviado puede seguir siendo evidencia útil de lo recibido por esa persona en esa fecha, pero su contenido anterior se analiza con encabezados y fuentes complementarias. Si el objetivo es

acreditar la entrega de un archivo, el EML original del proveedor es preferible a una captura del reenvío. Si no está disponible, se declara la limitación y se busca el mensaje en otro buzón o servidor.

Representación	Qué conserva	Qué necesita complemento
EML original	Cuerpo, encabezados y adjuntos disponibles.	Procedencia y verificación de contenido.
EML reenviado	Nueva entrega y contenido anterior representado.	Historia del reenvío y origen anterior.
PDF de correo	Diseño y texto legible.	Encabezados, adjuntos y estructura.
Captura	Fragmento mostrado en pantalla.	URL, cuenta, fecha, contexto y archivo.
Adjunto solo	Datos de un archivo.	Mensaje, declaración, relación y proceso.

2.3 Adjuntos y entrega de terceros

El adjunto no se edita ni se convierte para facilitar lectura antes de preservarlo. Se calcula hash, se comprueba si coincide con el valor declarado y se registra apertura y cobertura. Si un CSV abre pero carece de diccionario, se solicita el significado de sus campos. El hash no demuestra que las filas sean completas ni verdaderas: demuestra igualdad entre dos objetos comparados.

Caso ficticio

Un proveedor entrega un CSV y un PDF con un hash para cada uno en el cuerpo del correo. El CSV coincide y el PDF no. Se conserva todo, se pide nueva entrega del PDF y se registra que el CSV coincide con la declaración, sin afirmar que el contenido del proveedor sea completo. La segunda entrega recibe otro identificador; no sustituye la primera.

EML, adjuntos y declaración: objetos relacionados ACCCF · RECONSTRUCCIÓN EDITORIAL · DATOS FICTICIOS

Cada integridad corresponde a un objeto distinto



El hash del EML no es el hash del adjunto. El adjunto coincidente no prueba la verdad de lo que el proveedor afirma.

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

Figura 1. EML, adjuntos y declaración: objetos relacionados. Cada integridad corresponde a un objeto distinto Reconstrucción editorial; no constituye evidencia real.

Capítulo 3. Autenticación del canal

3.1 Encabezados Received y transporte

Los campos Received aportan una secuencia declarada de servidores, fechas y datos de transporte. Se revisan en el orden definido por la estructura del mensaje, sin asumir que todos son necesariamente confiables ni que el primero visible corresponde al origen humano. Algunos campos pueden ser añadidos por sistemas intermedios. El análisis compara servidores, tiempos, dominios y otros resultados de autenticación.

La dirección From visible puede no coincidir con el dominio autenticado ni con el servidor de envío. Una IP en un encabezado puede identificar infraestructura, no a la persona. La fecha puede depender de relojes distintos. El análisis no convierte un encabezado complejo en una prueba mágica; explica qué componentes son verificables y cuáles dependen de confianza.

3.2 DKIM, SPF y DMARC

DKIM asocia un dominio con el mensaje mediante firma criptográfica y permite verificar los componentes firmados. SPF publica qué hosts están autorizados para un dominio en el contexto del protocolo; DMARC aporta alineación y política del dominio. Estos mecanismos ayudan a evaluar canal y dominio, pero no prueban quién redactó el texto ni su veracidad. Un fallo también puede requerir revisión de reenvío, configuración o transformaciones.[23]

El informe registra dominio, selector, campos firmados, resultado, fecha y fuente de consulta cuando están disponibles. No basta escribir “DKIM pass” como si fuera una identificación personal. Tampoco “SPF fail” demuestra por sí solo suplantación maliciosa: se revisa el trayecto y la configuración. El análisis técnico conserva el mensaje original para que otra persona pueda comprobarlo.

3.3 Fecha, Message-ID y contenido

Message-ID puede ayudar a relacionar mensajes y sistemas, pero su unicidad y estructura dependen del generador. Las fechas se conservan literalmente con su zona y se comparan con registros del servidor y eventos de recepción. La fecha de descarga no es la fecha de envío. La fecha de un archivo adjunto es otra capa distinta.

Afirmación	Qué puede comprobarse	Qué no se deriva
Dominio autenticado	Firma, alineación y configuración del canal.	La persona física escribió el mensaje.
Fecha de envío	Encabezados y registros coherentes.	El texto fue creado en ese mismo instante.
Mensaje recibido	Buzón, EML y registros de servidor.	La persona lo leyó o comprendió.
Contenido verdadero	Fuentes independientes del hecho narrado.	DKIM o hash prueban el hecho.
Cuenta comprometida	Sesiones, recuperación y actividad anómala.	Una dirección distinta prueba por sí sola robo.

Regla de lectura

El encabezado se analiza como evidencia de transporte y dominio, no como una confesión de la persona. La autoría necesita corroboración adicional.

Leer encabezados sin convertirlos en una identificación humana
ACCCF · RECONSTRUCCIÓN EDITORIAL · DATOS FICTICIOS

Pistas de transporte, dominio y contenido

Elemento	Qué puede aportar	Límite
Received	Saltos declarados por servidores.	Puede haber entradas añadidas o reinterpretadas.
DKIM	Dominio responsable y partes firmadas.	No identifica a quien escribió.
From visible	Dirección mostrada al destinatario.	Puede diferir del dominio autenticado.
Fecha y Message-ID	Referencias temporales y del mensaje.	Relojes y unicidad dependen del sistema.

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

Figura 2. Leer encabezados sin convertirlos en una identificación humana. Pistas de transporte, dominio y contenido Reconstrucción editorial; no constituye evidencia real.

Capítulo 4. Archivos, URLs y publicaciones

4.1 Registro completo de una URL

Se conserva URL completa, parámetros, dominio, fecha y zona, cuenta visible, tipo de acceso, rol, idioma, versión de navegador y estado de la página. Se registra si hubo redirección, inicio de sesión, restricción geográfica o error. La URL puede cambiar de contenido sin cambiar de dirección; por eso se conserva el objeto y el proceso de obtención.

La captura debe incluir contexto suficiente para reconocer la página, pero no exponer datos innecesarios. Se acompaña del archivo HTML cuando sea útil y lícito, de recursos multimedia, de exportación nativa y de una descripción de lo que no se pudo obtener. Una página dinámica puede mostrar contenido distinto a cada visitante; el informe no la generaliza como vista universal.

4.2 Publicación, hilo y multimedia

Se preserva el texto, autor aparente, identificador de publicación, fecha visible, URL, respuestas relevantes, citas, reenvíos, reacciones y multimedia. El orden de respuestas puede cambiar con algoritmos o moderación. Si se captura un hilo, se registra cómo se desplazó y hasta dónde llegó la cobertura. Una sola respuesta fuera de contexto puede distorsionar la conversación.

El archivo de imagen o video se descarga cuando está autorizado y se calcula hash por separado. La publicación se relaciona con el archivo en el manifiesto. Si se investiga autenticidad del contenido, se aplica el volumen específico de análisis multimedia; la preservación solo demuestra que esa versión estaba disponible en esa fuente y momento.

4.3 Archivo web y fechas de terceros

Un archivo de terceros puede conservar una instantánea útil, pero su fecha pertenece a su captura, no necesariamente a la primera publicación. Se registra quién lo archivó, qué versión capturó, qué recursos faltan y cómo se consultó. Una fecha en el contenido puede ser editada por el autor o mostrar otra zona. La corroboración busca publicaciones, notificaciones, enlaces y registros de fecha cercanos.

Elemento	Registro necesario	Límite
URL y redirecciones	Dirección completa y secuencia de acceso.	Contenido cambiante o personalizado.
Publicación y hilo	Identificador, texto, respuestas y alcance capturado.	No toda la conversación si la cobertura fue limitada.
Multimedia	Archivo, calidad, hash y procedencia.	No autenticidad de escena ni autoría.
Archivo externo	Custodio, instantánea, fecha y recursos ausentes.	No primera publicación ni contenido completo.
Acceso	Cuenta, rol, visibilidad y restricciones.	No todos los usuarios vieron lo mismo.

Regla de presentación

No uses un archivo web para afirmar “siempre estuvo así” ni una captura para afirmar “esto es todo”. Describe la versión, la fecha y la cobertura que realmente puedes demostrar.

Una publicación se conserva con su entorno

ACCCF · RECONSTRUCCIÓN EDITORIAL · DATOS FICTICIOS

La captura es una representación, no el universo

Campo	Ejemplo ficticio	Utilidad
URL completa	https://ejemplo.invalid/estado/001	Localizar el objeto y parámetros.
Cuenta y visible	@demostracion · público	Contexto de autoría aparente y alcance.
Fecha y zona	2026-11-10 10:42 −06	Secuencia de adquisición, no creación automática.
Contenido asociado	Respuestas, multimedia y versión	Evitar fragmento sin sentido.
Preservación	HTML, archivo, video y manifiesto	Relación entre visualización y fuente.

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

Figura 3. Una publicación se conserva con su entorno. La captura es una representación, no el universo Reconstrucción editorial; no constituye evidencia real.

Capítulo 5. Preservación y certificación documentada

5.1 Acta de adquisición

El acta identifica caso, operador, autoridad, lugar, fecha y zona, equipo, navegador o herramienta, cuenta y rol, objetos adquiridos, acciones, formatos, incidencias y hash. Si se captura pantalla, se indica recorrido y filtros. Si se exporta, se indican parámetros y salida. Si se utiliza proveedor, se conserva respuesta y canal. El acta describe lo realizado, no un procedimiento ideal que no ocurrió.

Una constancia de conservación puede complementar la prueba de integridad y accesibilidad. En México, la NOM-151 tiene requisitos específicos para conservación y digitalización de mensajes de datos en su ámbito; no certifica la veracidad del contenido ni sustituye la adquisición del mensaje completo. Un sello de tiempo o hash no prueba autoría humana ni licitud de obtención.[45]

5.2 Custodia y control de acceso

La fuente se separa de la copia de trabajo y se restringe el acceso. Las transferencias electrónicas incluyen destinatario, permisos, fecha, versión, canal de entrega de llaves y verificación de descarga. El informe no contiene contraseñas, tokens ni cookies. Si se preserva una página autenticada, se documenta el rol sin exponer la sesión.

La copia de trabajo se utiliza para análisis, anonimización y presentación. La versión pública se revisa para evitar datos personales, imágenes íntimas, domicilios y terceros no relacionados. La versión completa preservada no se destruye por crear una versión redactada; se limita su acceso y uso posterior.

5.3 Certificación pericial, notarial o administrativa

La elección depende de la jurisdicción, el objeto y la finalidad. Una actuación notarial puede documentar una visualización; una pericial puede analizar origen, estructura, autenticidad, relaciones y contexto; una constancia administrativa puede acreditar una actuación en su ámbito. Ninguna transforma un fragmento en prueba completa. Se solicita la forma adecuada antes de iniciar para no repetir acciones sobre una página que puede cambiar.

> **Criterio de calidad**
>
> La mejor certificación no es la que tiene más sellos, sino la que permite a otra persona comprender qué se vio, dónde, cuándo, con qué método y qué quedó fuera.

Capítulo 6. Retirada, denuncia y daño mediático

6.1 Preservar antes de retirar

Antes de solicitar la retirada de contenido se conserva URL, identificador, publicación, cuenta, multimedia, respuestas y fecha de acceso. También se registran las versiones que ya cambiaron y los enlaces de referencia. Si existe amenaza inmediata, se prioriza seguridad y canales de emergencia; la preservación no se convierte en demora peligrosa.

El reporte a plataforma debe ser específico: objeto, URL, motivo, evidencia, fecha y petición. No incluye más datos personales de los necesarios ni envía el archivo dañino a canales no destinados. Se conserva número de reporte, contenido, fecha y respuestas. La retirada de un enlace no demuestra que

todas las copias desaparecieron ni que el daño dejó de existir.

6.2 Daño y alcance

El análisis separa contenido, republicación, alcance visible, reacciones y consecuencias declaradas. Los contadores de plataforma pueden significar cosas distintas y no prueban lectores individuales ni impacto total. Se conservan métricas con fecha y significado cuando se conocen. No se calcula daño económico por multiplicar impresiones sin fundamento.

La evaluación de daño mediático puede necesitar testimonios, documentos laborales, contratos, comunicaciones y otras fuentes no digitales. La preservación técnica demuestra contenido y secuencia, no todo el daño. El informe no inventa titulares de cuentas anónimas ni les asigna una intención por el tono de una publicación.

6.3 Caso integrado

Una publicación ficticia contiene una acusación y varias respuestas. Se preserva el hilo disponible, los archivos y las métricas con fecha. Después la cuenta cambia el texto y elimina una respuesta. La primera versión se conserva con sus límites y la nueva como objeto relacionado. El análisis compara cambios sin borrar la historia. La solicitud de retirada se registra, pero el informe no afirma que el contenido dejó de circular en otras cuentas.

> **Lección**
>
> La evidencia de daño mediático se construye con versiones y contexto. Una captura final puede mostrar menos que la primera, pero la primera tampoco prueba todo el recorrido.

Anexo A. Formatos de preservación

A.1 Acta de correo

Registro ficticio

```
Caso / objeto: EXP-DEMO-2026-008 / EML-001-R00
Fuente: [buzón, servidor, cliente o tercero]
Obtención: [exportación, descarga o entrega]
Remitente aparente y destinatarios: [registro]
Fecha y zona del mensaje: [literal]
Fecha y zona de adquisición: [literal]
Cuerpo y declaraciones: [referencia, algoritmo y hash]
Encabezados: [archivo completo]
Adjuntos: [nombres, tamaños, formatos y hashes]
Autenticación: [DKIM / SPF / DMARC si se revisa]
Verificación: [coincidencias y diferencias]
Incidencias: [formato, ausencia, error o límite]
Custodia: [original, copia de trabajo y acceso]
```

A.2 Registro de publicación

Campo	Contenido mínimo	Control
URL e identificador	Dirección completa, parámetros y redirecciones.	Objeto localizable.
Cuenta y visibilidad	Autor aparente, rol, acceso y audiencia visible.	No atribución automática.
Fechas	Visible, adquisición, zona y precisión.	No confundir publicación y descarga.
Contenido	Texto, respuestas, reacciones, multimedia y versión.	Cobertura del hilo.
Proceso	Herramienta, versión, filtros y acciones.	Repetibilidad.
Archivos	HTML, imagen, video, exportación y hash.	Relación original / derivado.
Incidencias	Error, acceso, contenido ausente y limitación.	No ocultar cobertura.

A.3 Manifiesto de objetos

Inventario de entrega

```
ID / nombre original / tipo de objeto
Fuente y relación: [original, exportación, derivado]
Fecha y zona de recepción
Método y herramienta / versión
Tamaño y formato
Algoritmo y hash del objeto
Objeto padre y objetos relacionados
Apertura y verificación
Datos sensibles y restricciones
Ubicación preservada y copia de trabajo
Transferencias y receptor
Límites y pendientes
```

A.4 Registro de solicitud de retirada

Formato ficticio

```
Plataforma y canal: [oficial]
URL / publicación / cuenta: [objeto específico]
Motivo y evidencia adjunta: [identificadores]
Solicitud: [retirada, revisión, preservación]
Fecha y zona: [envío]
Número de reporte: [referencia]
Respuesta: [fecha, contenido y acción]
Otras copias conocidas: [URL y estado]
Comunicación con afectados: [canal y versión]
Pendientes: [cobertura y siguiente revisión]
```

Anexo B. Marco jurídico y lista final

México reconoce mensajes de datos en CCom 89–94 y 1205; CFPC/CNPCF desarrolla fiabilidad, atribución e integridad según transición; NOM-151 regula conservación en su ámbito. Perú distribuye firma, proceso y archivo; Chile diferencia firma y fecha; Argentina pondera confiabilidad; Colombia y Ecuador exigen conservar formato, origen, destino y fechas; España combina eIDAS, LEC y servicios de confianza. Ninguna regla hace verdadero un mensaje por ser electrónico.[6789101112131415 16]

La preservación también se limita por privacidad y derechos de terceros. Se restringen roles, acceso y difusión; se separan versiones de trabajo y públicas; se evita publicar contenido íntimo, datos de

menores, secretos o credenciales. La prueba se entrega por el canal autorizado y con manifiesto, no como una colección pública de archivos.[17][18][19]

Control final	Pregunta de aceptación
Objeto	¿EML, URL, archivo y contexto disponibles?
Proceso	¿Se registró quién obtuvo, con qué rol, filtros y fecha?
Integridad	¿Cada hash corresponde a un objeto y momento?
Canal	¿DKIM / SPF / DMARC se interpretaron con límites?
Cobertura	¿Hilo, respuestas y ausencias quedaron declarados?
Atribución	¿Cuenta y persona no se confundieron?
Privacidad	¿La entrega evita exposición innecesaria?

Cierre

Preservar es dejar una ruta verificable de lo que existió en un momento. No es coleccionar capturas hasta que parezca suficiente.

Referencias citadas

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

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

[2] RFC Editor. RFC 6376, DomainKeys Identified Mail (DKIM) Signatures: responsabilidad de un dominio y verificación criptográfica de los componentes firmados. No acredita por sí sola quién escribió el texto ni la verdad del contenido. Fuente oficial en línea

[3] RFC Editor. RFC 8616 y referencias técnicas SPF RFC7208, DKIM RFC6376 y DMARC RFC7489: autorización de hosts, firma de dominio, alineación y política. Ayudan a evaluar el canal; no acreditan por sí solos identidad humana ni veracidad del contenido. Fuente oficial en línea

[4] 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

[5] 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

[6] 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

[7] 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

[8] 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

[9] 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

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

[11] 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

[12] 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

[13] 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

[14] 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

[15] 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

[16] 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

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

[18] Colombia. Ley Estatutaria 1581 de 2012, artículos 4, 8, 12, 17–18 y 26: principios, derechos, información, deberes de responsables y encargados, y transferencia a terceros países. Fuente oficial en línea

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

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