BIBLIOTECA
ACCCF

10
VOLUMEN

ACCCF / CONOCIMIENTO APLICADO

Manual de peritaje financiero y contradicción documental: bancos, XML y SAT

CFDI, estados de cuenta, transferencias, referencias, cronologías y contradicciones

Reconstruir operaciones con documentos y registros verificables, sin confundir una factura con la realidad material, una transferencia con su causa ni una autenticación exitosa con consentimiento.

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: los documentos hablan mejor cuando se les hacen preguntas 4

Capítulo 1. Pregunta, período y fuentes 4

1.1 Afirmaciones separadas y unidad de análisis 4

1.2 Inventario de fuentes y autoridad 5

Capítulo 2. Conciliación 5

2.1 La cadena de correspondencia 5

2.2 Diferencias y explicación documentada 6

2.3 Ejemplo de remesa y abonos 6

Capítulo 3. XML y representaciones 7

3.1 XML como fuente estructurada 7

3.2 Folio, duplicidad y operación material 7

3.3 Metadatos, representaciones y fechas 8

Capítulo 4. Registros bancarios y cronología financiera 8

4.1 El movimiento dentro de su secuencia 9

4.2 Comprobantes y constancias del proveedor 9

4.3 Reglas financieras y su alcance 9

Capítulo 5. Operaciones no reconocidas 10

5.1 Enrolamiento y control de factores 10

5.2 Señales de seguridad y conducta del sistema 10

5.3 Matriz de autenticación y autorización 10

Capítulo 6. Informe de contradicción documental 11

6.1 Separar observación, conciliación e inferencia 11

6.2 Cronología y límites 11

6.3 Revisión independiente 12

Anexo A. Formatos de conciliación y solicitud 12

A.1 Matriz de conciliación 12

A.2 Solicitud de registros financieros 13

A.3 Matriz de operación no reconocida 13

Anexo B. Marco documental comparado y control final 13

Presentación: los documentos hablan mejor cuando se les hacen preguntas

Una factura puede verse perfecta y no bastar para demostrar que el bien se entregó. Una transferencia puede existir y no explicar su causa. Un estado de cuenta puede coincidir con la contabilidad y, aun así, dejar sin respuesta quién autorizó una operación. El análisis financiero no consiste en elegir el documento que parece más oficial, sino en seguir la secuencia entre contrato, comprobante, operación material, movimiento bancario, registros y contabilidad.

El peritaje comienza con una afirmación concreta: operaciones inexistentes, duplicidad, pagos no recibidos, transferencias no reconocidas, saldos que no concuerdan o actividad que no corresponde a la operación declarada. Después identifica qué fuente puede confirmar o debilitar cada afirmación. La coincidencia de importe ayuda a localizar, pero no prueba por sí sola relación ni intención.

El trabajo separa cuatro planos: forma documental, realidad material, ruta del dinero y conducta de los sistemas. En el primero se revisan XML, PDF, sellos, folios y versiones; en el segundo, entrega, personal, activos y evidencia independiente; en el tercero, cuentas, referencias y liquidación; en el cuarto, enrolamiento, factores, alertas y comportamiento. Una conclusión responsable no mezcla esos planos para resolverlos con una sola fecha.

> **Regla rectora**
>
> La existencia de un documento y la verdad de la operación son preguntas relacionadas, pero distintas. Cada una necesita su fuente y su método.

Capítulo 1. Pregunta, período y fuentes

1.1 Afirmaciones separadas y unidad de análisis

Se escribe qué afirma cada parte con fechas, importes, cuentas, referencias y operaciones, sin aceptar la versión como hecho. Un comercio puede reclamar ventas no liquidadas; el procesador puede afirmar que no las recibió; el banco puede mostrar abonos parciales. La unidad de análisis puede ser operación, lote, remesa, factura, transferencia o jornada. Se elige antes de sumar para no mezclar niveles.

Se delimita período y zona, moneda, impuestos, comisiones, devoluciones, contracargos, tipos de cambio y redondeo. Las diferencias pueden deberse a una comisión, a un calendario de liquidación o a un archivo incompleto, no automáticamente a fraude. Las tolerancias se justifican por reglas de negocio y se documentan; no se ajustan hasta que el resultado parezca conveniente.

Pregunta	Fuentes prioritarias	No confundir con
¿La operación fue registrada?	Sistema comercial, CFDI, pedido y contabilidad.	Existencia material del bien o servicio.
¿Fue entregada?	Recepción, logística, ejecución y evidencia independiente.	Folio fiscal o descripción escrita.
¿Fue transmitida?	Remesa, procesador, interfaz y registros.	Captura del reporte final.

Pregunta	Fuentes prioritarias	No confundir con
¿Fue liquidada?	Banco, referencia, lote y calendario.	Mismo importe como identidad única.
¿Fue autorizada?	Factores, sesiones, alertas, contrato y contexto.	Un “sí” del sistema como consentimiento humano.
¿Qué quedó fuera?	Filtros, período, canales y documentos ausentes.	Ausencia en un archivo como inexistencia universal.

1.2 Inventario de fuentes y autoridad

El inventario incluye contratos, pedidos, XML y PDF, representaciones de estados de cuenta, archivos bancarios, registros del procesador, interfaces, contabilidad, inventarios, logística, comunicaciones y personal. Cada fuente tiene custodio, formato, período, cobertura y autoridad. La solicitud de información personal o financiera se limita a la operación relevante y utiliza canal seguro.

No se solicita “todo el banco” ni “todo el SAT”. Se piden operaciones por referencia y período, formato nativo disponible, diccionario, proceso de extracción, filtros y constancia de cobertura. La entrega se conserva con EML y adjuntos. Si un proveedor declara hash, se verifica; si no lo declara, se calcula al recibir y se limita su alcance.

> **Condición de inicio**
>
> Antes de sumar, verifica qué operación representa cada fila y qué documento corresponde a cada afirmación. La contabilidad no se reconcilia con una suma de totales sin identidad ni cobertura.

Capítulo 2. Conciliación

2.1 La cadena de correspondencia

Se crea una fila por operación y se relacionan pedido, CFDI, entrega, remesa, procesador, banco y asiento. Los campos ausentes no se rellenan con suposiciones. Si una factura no tiene banco asociado, se marca como pendiente; si hay dos movimientos candidatos, se describen las alternativas y la evidencia necesaria. El objetivo es mostrar dónde se rompe la secuencia, no obligar a que todas las filas concuerden.

La relación puede ser uno a uno, uno a muchos o muchos a uno. Un lote puede agrupar ventas; una transferencia puede cubrir varias facturas; una devolución puede afectar solo parte. El método declara cómo se reparte una operación y evita asignar importes dos veces. El total de cada nivel se compara con su fuente para detectar duplicidad o pérdida de registros.

2.2 Diferencias y explicación documentada

Diferencia ficticia	Comprobaciones	Conclusión provisional
Mismo importe en dos fechas	Referencia, ordenante, cuenta, canal y concepto.	Candidato posible, no identidad confirmada.
Factura sin abono	Calendario, lote, comisiones, devolución y otra cuenta.	Pendiente o explicado según fuente.
Abono sin factura	Cargo anterior, anticipo, relación posterior o error.	No asignarlo para equilibrar.
Remesa corta	Filtros, transmisión, lote duplicado y corte horario.	Cobertura antes que acusación.
Saldo distinto	Moneda, impuestos, redondeo y comisiones.	Diferencia cuantificada y explicada.
Documento repetido	UUID, folio, archivo, hash y representación.	Duplicidad real o dos copias del mismo objeto.

2.3 Ejemplo de remesa y abonos

Una tienda ficticia declara 18,420 operaciones en tres días. Su archivo contiene ese número de filas, pero una remesa tiene solo 17,900. La primera pregunta no es quién robó, sino si el corte horario, los filtros o el canal dejaron fuera eventos. Se comparan archivos de origen, transmisión, procesador y banco con zona y calendario. Un abono posterior puede corresponder a un lote distinto; no se usa para cerrar la diferencia sin relación.

Si una exportación confirma que las referencias faltantes no fueron transmitidas por la tienda, el hallazgo orienta la investigación hacia su proceso de generación. Aún no identifica causa ni responsable. Puede existir operación no registrada, filtro, fallo o duplicidad. El informe separa ausencia en la remesa, existencia en el punto de venta y abono bancario, y propone la siguiente fuente capaz de distinguir esas hipótesis.

> **Resultado de conciliación**
>
> Una matriz que muestra correspondencia, diferencias, duplicidades, ausencias y preguntas pendientes. La suma es una comprobación; la explicación es el análisis.

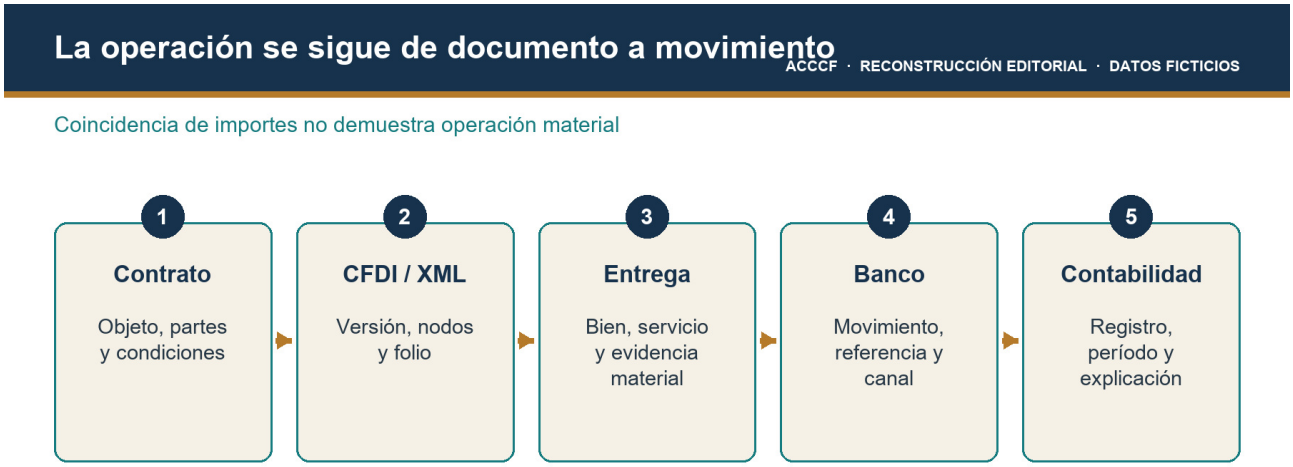


Figura 1. La operación se sigue de documento a movimiento. Coincidencia de importes no demuestra operación material Reconstrucción editorial; no constituye evidencia real.

Capítulo 3. XML y representaciones

3.1 XML como fuente estructurada

El XML conserva nodos, atributos y relaciones que una representación PDF puede no mostrar. Se preserva el archivo original con su nombre, tamaño, fecha de recepción y hash, y se analiza una copia. Se revisan versión, emisor, receptor, folio, tipo, moneda, conceptos, impuestos, complementos y documentos relacionados según el encargo. No se modifica el archivo para “ver si valida”.

El material oficial del SAT ofrece guías de llenado para CFDI 4.0 y complementos. La guía elegida debe corresponder al tipo de comprobante y a la fecha. Un atributo puede cambiar entre versiones; no se compara un XML histórico con un ejemplo de otra versión como si fueran idénticos. El PDF sirve para leer; el XML permite analizar la estructura.[1]

3.2 Folio, duplicidad y operación material

El UUID ayuda a identificar un comprobante, pero la duplicidad se revisa con archivo, estructura, emisor, folio, importe y contexto. Dos archivos idénticos pueden ser copias del mismo objeto; dos XML distintos con el mismo UUID requieren aclaración. La existencia de sello o timbre no demuestra por sí sola entrega de un bien o prestación de un servicio.

La operación material se revisa con contrato, pedido, inventarios, entrega, ejecución, personal, comunicaciones, registros de acceso y evidencia independiente. La pregunta no es solo si el CFDI es formalmente correcto, sino si la actividad descrita tiene soporte. El análisis no declara automáticamente delito o simulación: señala qué documentos coinciden, qué hechos faltan y qué contradicciones existen.

3.3 Metadatos, representaciones y fechas

La fecha de emisión del CFDI no es necesariamente la de entrega, pago o registro contable. La fecha del archivo en el sistema puede corresponder a descarga. La representación PDF puede mostrar una versión distinta si fue generada de otro XML. Se relacionan objetos y se conservan todas las versiones. El hash acredita integridad desde recepción, no la realidad de la operación.

Objeto	Qué demuestra	Qué necesita otra fuente
XML recibido	Estructura y contenido del archivo en esa entrega.	Autenticidad de la operación y cobertura total.
PDF asociado	Representación visual declarada.	Que procede del mismo XML sin comparación.
UUID	Identificador del comprobante.	Que no haya error, duplicidad o simulación.
Entrega	Evidencia de bien o servicio.	Que todas las facturas sean materiales.
Hash	Igualdad entre objetos y momento.	Fecha, autoría y verdad económica.

Caso ficticio

Dos XML tienen el mismo UUID y distinta descripción. No se elige el que favorece a una parte: se preservan ambos, se solicita registro del emisor, historial y comprobación pertinente, y se compara con entrega y contabilidad. La diferencia de contenido exige una explicación antes de atribuir una operación.

El PDF ayuda a leer; el XML permite analizar estructura

ACCCF · RECONSTRUCCIÓN EDITORIAL · DATOS FICTICIOS

La versión y los catálogos aplicables forman parte del caso

Elemento	Qué revisar	No confundir con
Versión y nodos	CFDI 4.0, atributos y complementos.	Texto extraído de una representación PDF.
UUID y relaciones	Folio, documentos relacionados y duplicidad.	Número escrito manualmente en una nota.
Sellos y validación	Estructura, referencia y verificación pertinente.	Prueba automática de operación material.
Cronología	Emisión, entrega, pago y registro contable.	Una única fecha como toda la operación.

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

Figura 2. El PDF ayuda a leer; el XML permite analizar estructura. La versión y los catálogos aplicables forman parte del caso Reconstrucción editorial; no constituye evidencia real.

Capítulo 4. Registros bancarios y cronología financiera

4.1 El movimiento dentro de su secuencia

El estado de cuenta identifica fecha, hora cuando existe, importe, moneda, referencia, ordenante, beneficiario, canal y saldo. Se solicitan campos y diccionario. Una transferencia puede tener fecha de instrucción, ejecución, compensación y disponibilidad distintas. La cronología no las mezcla en una sola columna. La existencia del abono no prueba qué contrato lo originó ni quién lo ordenó.

Se reconstruye la secuencia desde instrucción hasta liquidación con comprobantes, alertas, rechazos, devoluciones, contracargos y registros de canal. Si una cuenta está bloqueada o congelada, se solicita el acto, alcance, fecha y operaciones relacionadas por la vía legal; no se intenta acceder por medios alternativos. La falta de movimiento en una cuenta no prueba ausencia en otras.

4.2 Comprobantes y constancias del proveedor

El comprobante visual debe relacionarse con el registro del proveedor y no con una captura aislada. Se solicitan exportación nativa, diccionario, proceso y cobertura. Si hay una referencia o folio, se usa para vincular, no para sustituir la validación. Una imagen de “transferencia exitosa” puede indicar instrucción, no recepción final ni autenticidad de cuenta.

El EML de entrega del proveedor conserva la declaración de integridad y los adjuntos. El hash del EML, del reporte y del sistema son objetos distintos. Si el proveedor entrega solo PDF, se solicita CSV o formato nativo para analizar estructura; si no existe, se declara el límite y se trabaja con la representación recibida sin presentarla como base completa.

4.3 Reglas financieras y su alcance

En México, las disposiciones CNBV comprenden comprobantes, notificaciones, acceso, incidentes, incidencias, bitácoras y revisiones para instituciones de crédito. En Perú, la SBS 504-2021 regula preservación y análisis forense en entidades supervisadas y la 2286-2024 modifica determinados supuestos de operaciones no reconocidas. En España, el RD-ley 19/2018 regula restitución con condiciones y excepciones. Estas reglas no significan que toda autenticación pruebe autorización ni que todo banco responda igual.[2345]

Jurisdicción	Fuente sectorial útil	Precaución
México	CNBV 316 Bis 11, 14, 15 y 17 para acceso, incidencias, bitácoras y revisión.	Ámbito y plazos distintos por artículo.
Perú	SBS 504-2021 y 2286-2024 para preservación, registros y determinadas operaciones.	Leer supuestos y excepciones, no generalizar responsabilidad.
Argentina	BCRA A 7783 y A 8280 para registros e incidentes.	90 días de registros digitales y reporte en su régimen, no universal.
Chile	RAN 20-7, 20-8 y 20-10 para externalización, incidentes y ciberseguridad.	No confundir funciones ni sujetos.
España	RD-ley 19/2018, 45, 66 y 67.	Restitución condicionada y gestión/notificación de incidentes.

Regla de interpretación

El registro bancario prueba lo que el sistema registró. La autorización jurídica y la identidad del ordenante necesitan análisis adicional.

Capítulo 5. Operaciones no reconocidas

5.1 Enrolamiento y control de factores

Se revisa quién registró el dispositivo o factor, con qué método, fecha, canal y evidencia; cambios posteriores; recuperación; baja; alertas y accesos. Un segundo factor puede reducir riesgo, pero no prueba que el titular aprobó cada operación si el enrolamiento fue comprometido o si la recuperación fue la vía de ataque. La secuencia empieza antes de la transferencia.

NIST SP 800-63B-4 diferencia niveles de garantía y trata autenticación resistente al phishing. La guía no autoriza a concluir que cualquier MFA es equivalente ni que la recuperación es un detalle secundario. El análisis considera canal, vínculo con dominio, dispositivo, sesión y posibilidad de phishing. La afirmación técnica se limita a lo que la fuente acredita.[6]

5.2 Señales de seguridad y conducta del sistema

Se revisan alertas, reglas, dispositivo nuevo, cambio de beneficiario, ubicación aproximada, monto, frecuencia, comportamiento previo y respuesta del banco. Una operación puede haber sido bloqueada por el sistema y luego permitida por un canal alterno. La ausencia de alerta no prueba que fuera normal; puede deberse a configuración o cobertura.

Se comparan operaciones reconocidas y no reconocidas sin sesgo. Si las primeras comparten dispositivo y patrón con las segundas, la atribución puede ser compatible con uso habitual o con una cuenta comprometida de forma persistente. Si hay cambio de factor minutos antes, se investiga su origen. La conclusión no se decide por la frase “el sistema validó correctamente”.

5.3 Matriz de autenticación y autorización

Elemento	Qué acredita	Pregunta pendiente
Enrolamiento	Registro de factor y fecha.	¿Quién lo inició y con qué control?
Autenticación	El sistema aceptó factores en un evento.	¿Eran del titular y cómo se recuperaron?
Alerta	El sistema clasificó una condición.	¿Qué acción tomó y con qué resultado?
Operación	Instrucción y resultado en el canal.	¿Hubo consentimiento y qué contrato aplica?
Titular	Cuenta y relación contractual.	¿Quién usó el canal en ese momento?
Responsabilidad	Regla y hechos acreditados.	¿Qué supuesto y excepción corresponde?

Caso ficticio

Una transferencia no reconocida sigue a un cambio de correo de recuperación y al alta de un dispositivo. El banco registró autenticación válida, pero esa secuencia exige revisar el cambio previo. El análisis no afirma fraude del titular ni responsabilidad automática del banco: documenta los eventos y la regla aplicable.

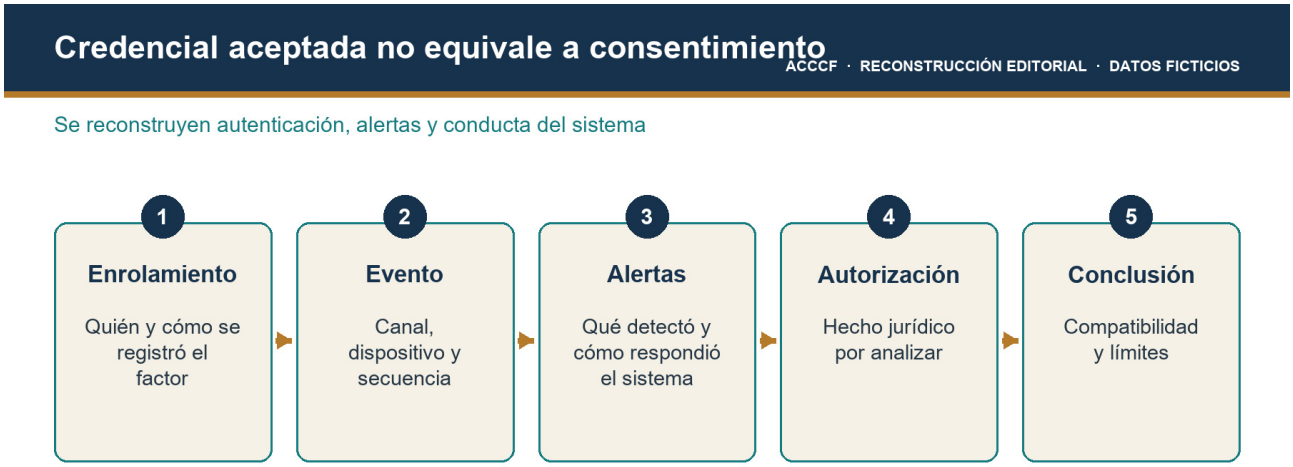


Figura 3. Credencial aceptada no equivale a consentimiento. Se reconstruyen autenticación, alertas y conducta del sistema Reconstrucción editorial; no constituye evidencia real.

Capítulo 6. Informe de contradicción documental

6.1 Separar observación, conciliación e inferencia

El informe distingue lo que el archivo contiene, lo que la conciliación produce y lo que el analista interpreta. “El XML contiene este importe” es observación; “el movimiento candidato coincide en importe y referencia” es conciliación; “es compatible con la operación declarada” es inferencia. La responsabilidad o legalidad es otra pregunta que no debe ocultarse entre las sumas.

Cada diferencia tiene una sección con valores literales, fuentes, explicaciones alternativas, resultado y necesidad pendiente. No se elimina porque dificulta el relato. Si una operación no puede vincularse, se declara no determinada. Si una fuente nueva cambia la relación, se actualiza la matriz y se conserva la versión anterior.

6.2 Cronología y límites

La cronología conserva emisión, entrega, transmisión, instrucción, liquidación, registro contable y comunicación, con zona y precisión. La proximidad de dos eventos no prueba causalidad. La ausencia de eventos fuera de la exportación no se utiliza para afirmar inexistencia. El informe identifica los canales y cuentas no revisados.

Afirmación	Redacción defendible	Límite
Coincidencia de importe	Candidato compatible por importe, referencia y período.	No identidad única sin otras fuentes.

Afirmación	Redacción defendible	Límite
Factura sin operación	No se localizó evidencia material en el alcance revisado.	No afirmar simulación total sin cobertura.
Transferencia no reconocida	Se documentó instrucción y autenticación en el canal.	No consentimiento humano automático.
Documento duplicado	Los objetos comparten UUID y presentan estas diferencias.	No borrar ninguno ni escoger por conveniencia.
Saldo conciliado	La matriz reconcilia los movimientos dentro de cobertura.	No prueba legalidad ni realidad de todas las operaciones.

6.3 Revisión independiente

El revisor repite sumas y relaciones, comprueba duplicados, zona, filtros, versiones y correspondencia con fuentes. También intenta explicar la diferencia desde otra hipótesis: comisión, lote, devolución, error de fecha, otro canal o documento faltante. Una conclusión que solo funciona ocultando una fila no resiste revisión.

Cierre

El informe financiero fuerte no es el que hace cuadrar todo, sino el que muestra con precisión qué coincide, qué no, por qué podría ser y qué falta para decidir.

Anexo A. Formatos de conciliación y solicitud

A.1 Matriz de conciliación

Campo	Registro requerido	Control
Operación	Identificador, fecha, importe, moneda y partes.	Unidad de análisis única.
Contrato / pedido	Documento, versión y condiciones.	Objeto y alcance.
CFDI / XML	Archivo, UUID, versión y hash.	No solo PDF.
Materialidad	Entrega, ejecución y evidencia independiente.	No inferir del folio.
Remesa / procesador	Lote, canal, filtros y cobertura.	No mezclar períodos.
Banco	Referencia, instrucción, liquidación y canal.	No asignar por importe solo.
Contabilidad	Asiento, período, moneda y explicación.	Relación con documentos.
Estado	Conciliado, parcial, pendiente, duplicado o no determinado.	No forzar correspondencia.

A.2 Solicitud de registros financieros

Modelo ficticio para canal autorizado

```
Asunto: EXP-DEMO-2026-010 · Operaciones y registros asociados

Solicito, por el canal autorizado, los comprobantes y registros relacionados con las referencias incluidas en el expediente, com

Cuando estén disponibles, incluir fecha/hora de instrucción y liquidación, importe, moneda, referencia, ordenante/beneficiario,

Entregar formato nativo, PDF de consulta, diccionario, proceso y fecha de extracción. En el cuerpo de la respuesta indicar algor

Responsable autorizado · EXP-DEMO-2026-010
```

A.3 Matriz de operación no reconocida

Ficha de análisis

```
Operación / referencia: [identificador y fuente]
Alegación del titular: [literal y fecha]
Instrucción y liquidación: [eventos, zona y canal]
Enrolamiento y factores: [altas, cambios, bajas]
Dispositivo y sesión: [registros disponibles]
Alertas y respuesta del sistema: [regla y resultado]
Operaciones comparables: [patrón y diferencias]
Comunicaciones: [avisos y recepción]
Hipótesis A / B / C: [explicaciones]
Fuentes que las distinguen: [comprobaciones]
Resultado técnico: [compatible, incompatible o inconcluso]
Régimen aplicable: [instrumento, artículo, sujeto y fecha]
Límites: [cobertura y datos faltantes]
```

Anexo B. Marco documental comparado y control final

La equivalencia funcional se concentra en documento electrónico, conservación, atribución, valoración y registros sectoriales. En México se combinan CCom 89–94 y 1205, CFPC/CNPCF según transición, NOM-151 y CNBV; Perú distribuye IOFE, proceso y SBS; Chile diferencia firma y seguridad; Argentina usa Ley 25.506, CCyC y BCRA; Colombia integra Ley 527 y CPACA; Ecuador usa Ley 67 y su régimen de pagos; España combina eIDAS, LEC y RD-ley 19/2018.[7891011121314151617181920212223]

La equivalencia no convierte las reglas en una única obligación mundial. Se cita función + instrumento + artículo + sujeto + versión. Si una fuente no permite fijar plazos o numerales, se marca como pendiente en vez de inventarlos. La información financiera y personal se trata con acceso restringido y minimización.[24252627]

Control final	Pregunta de aceptación
Fuente	¿XML, banco, entrega, proceso y diccionario disponibles?
Cobertura	¿Período, canales, cuentas y filtros están escritos?
Conciliación	¿Cada relación tiene identidad y no solo importe?
Materialidad	¿La operación real está separada del documento?
Autenticación	¿Se revisaron enrolamiento, alertas y recuperación?
Cronología	¿Emisión, instrucción, liquidación y registro están separados?
Conclusión	¿No se atribuye consentimiento ni responsabilidad por una sola señal?

Cierre

La contabilidad puede cuadrar y la pregunta seguir abierta. El peritaje aporta valor cuando muestra qué hay detrás del documento y qué no puede demostrarse.

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] SAT. Material de ayuda para facturar: guías de llenado de CFDI versión 4.0 y complementos. El XML debe analizarse con sus nodos, catálogos y versión aplicables; el PDF es una representación visual, no sustituto del comprobante estructurado. Fuente oficial en línea

[2] 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

[3] 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

[4] 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] 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

[6] NIST SP 800-63B-4 (julio de 2025). Directrices de autenticación y gestión de autenticadores, incluidos niveles de garantía y autenticación resistente al phishing. La recuperación de cuentas forma parte del riesgo y no debe reducirse a contraseñas. Fuente oficial en línea

[7] 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

[8] 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

[9] 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

[10] 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

[11] 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

[12] 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

[13] 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

[14] 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

[15] 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

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

[17] 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

[18] 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

[19] 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

[20] 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

[21] 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

[22] 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

[23] 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

[24] 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

[25] 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

[26] Ecuador. Ley Orgánica de Protección de Datos Personales, Registro Oficial Suplemento 459 de 26-05-2021. Artículos 10, 37–44: principios, medidas de seguridad, protección desde el diseño, riesgos y tratamiento ante incidentes. Fuente oficial en línea

[27] 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.