BIBLIOTECA
ACCCF

11
VOLUMEN

ACCCF / CONOCIMIENTO APLICADO

Manual de respuesta ciudadana al fraude digital: phishing, extorsión y cuentas comprometidas

WhatsApp, banca, páginas falsas, préstamos, inversiones, extorsión y apoyo a otras personas

Ayudar a actuar pronto sin entregar más información al fraude y sin destruir las pruebas necesarias para reportar, recuperar cuentas y prevenir nuevas víctimas.

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: la prisa es parte del engaño . . . 4

Capítulo 1. Primeros minutos . . . 4

1.1 Detener la siguiente acción . . . 4

1.2 Preservar lo esencial sin seguir expuesto . . . 5

1.3 Avisar a las personas adecuadas . . . 5

Capítulo 2. WhatsApp y cuentas comprometidas . . . 6

2.1 Recuperación desde un entorno confiable . . . 6

2.2 Revisión de aplicaciones y acceso remoto . . . 6

2.3 Autenticación y recuperación como sistema . . . 7

Capítulo 3. Señales de engaño . . . 7

3.1 Conducta antes que apariencia . . . 7

3.2 Escenarios frecuentes . . . 8

3.3 Cuando el mensaje viene de una cuenta real . . . 8

Capítulo 4. Extorsión y contenido íntimo . . . 9

4.1 No negociar ni difundir . . . 9

4.2 Reducir la exposición posterior . . . 9

4.3 Acompañar sin revictimizar . . . 9

Capítulo 5. Recuperación de cuentas . . . 9

5.1 Orden de recuperación . . . 10

5.2 Banca y operaciones . . . 10

5.3 Reporte y seguimiento . . . 10

Capítulo 6. Preservación y apoyo a otras personas . . . 11

6.1 Paquete mínimo de evidencia . . . 11

6.2 Cómo ayudar a alguien mayor o con poca experiencia . . . 11

6.3 Directorio local que sí puedes usar . . . 12

Anexo A. Tarjetas de emergencia . . . 12

A.1 Cuenta de WhatsApp comprometida 12

A.2 Pago o transferencia realizada 12

A.3 Extorsión o contenido íntimo 13

A.4 Mensaje sospechoso de familiar o banco 13

Anexo B. Cronología, directorio y control final 13

B.1 Cronología mínima 13

B.2 Directorio personal para completar antes de una crisis 13

B.3 Marco jurídico y revisión 14

Presentación: la prisa es parte del engaño

El fraude suele pedir una acción pequeña e irreversible antes de que puedas pensar: compartir un código, instalar una aplicación, pagar una comisión, abrir un enlace o confirmar datos. La apariencia puede ser convincente y el mensaje puede venir de una cuenta conocida comprometida. La primera defensa es una pausa concreta: no pagar, no compartir códigos, no instalar acceso remoto y verificar por un canal que tú ya conocías.

Este manual no te pide investigar al estafador ni seguirle el juego. Te propone detener la pérdida, avisar por canales oficiales, conservar lo necesario y recuperar el entorno. No necesitas demostrar todo antes de llamar al banco o reportar una cuenta. Esperar a tener un expediente perfecto puede aumentar el daño. La preservación se hace sin poner a más personas en riesgo.

Si hay amenaza física, peligro para menores o una emergencia, prioriza la seguridad y los servicios de emergencia de tu localidad. Si el contenido es íntimo, no lo reenvíes para pedir ayuda ni lo subas a servicios de análisis. Puedes conservar el mensaje, la cuenta, la URL y la fecha sin difundir el archivo. Apoyar a una persona no incluye revisar su intimidad sin necesidad.

> **Regla de emergencia**
>
> No uses el número, enlace o QR que llegó con la oferta o amenaza. Abre la aplicación oficial, llama al número de tu tarjeta o contrato, o escribe tú mismo la dirección conocida de la institución.

Capítulo 1. Primeros minutos

1.1 Detener la siguiente acción

Si todavía no pagaste ni entregaste datos, no continúes para comprobar si era verdad. Cierra el enlace, detén la llamada y no respondas. Si ya compartiste un código, una contraseña o acceso remoto, cambia el rumbo: usa otro dispositivo seguro para entrar a tus cuentas, contacta a la institución y revisa sesiones. No ejecutes una segunda instrucción del supuesto soporte para “deshacer” la primera.

Si ya pagaste, contacta al banco o al proveedor de pago por el canal oficial inmediatamente y pregunta por las opciones de reporte, bloqueo o revisión de la operación. No prometas que recuperarán el dinero: el resultado depende del canal, el tiempo, la norma y el caso. Conserva referencia, fecha, importe, cuenta receptora, comprobante y comunicaciones, sin ocultar información por vergüenza.

1.2 Preservar lo esencial sin seguir expuesto

Objeto	Qué conservar	Qué evitar
Mensaje	Texto completo, remitente, fecha, zona y contexto.	Editarlo o responder para obtener más pruebas.
Enlace	URL completa y página sin interacción adicional.	Abrirlo en tu dispositivo principal.
Cuenta	Usuario, perfil, identificador y plataforma.	Confiar solo en nombre o fotografía.
Pago	Comprobante, referencia, importe, receptor y canal.	Enviarlo a un supuesto agente de recuperación.
Correo	EML con encabezados y adjuntos.	Guardar solo una captura del cuerpo.
Acciones	Qué instalaste, códigos dados, cambios y horas.	Ocultar pasos que pueden explicar el acceso.

La captura debe incluir remitente, fecha y contenido suficiente, no solo la frase alarmante. Si el mensaje llegó por correo, se exporta EML con encabezados y adjuntos. Si hay enlace, se registra sin visitarlo de nuevo. Si hay aplicación instalada, se anota nombre, origen, permisos y fecha antes de desinstalarla cuando la seguridad lo requiera; no se conserva una muestra en el teléfono personal para analizarla.

1.3 Avisar a las personas adecuadas

Si tu cuenta fue comprometida, avisa a tus contactos por otro canal: llamada, correo de recuperación o mensaje desde una cuenta confirmada. Pide que no envíen dinero ni códigos al número afectado. Un aviso breve puede detener nuevas víctimas. No reenvíes el enlace fraudulento para advertir: describe el mensaje y comparte solo los datos necesarios.

> **Mensaje útil para contactos**
>
> “Perdí el control de esta cuenta. No envíes dinero, códigos ni documentos a este número ni abras sus enlaces. Estoy verificando la recuperación por canales oficiales. Si recibiste una solicitud, llámame al número que ya conocías.”



Figura 1. La urgencia no debe crear otra pérdida. Secuencia breve para contener el daño y conservar evidencia Reconstrucción editorial; no constituye evidencia real.

Capítulo 2. WhatsApp y cuentas comprometidas

2.1 Recuperación desde un entorno confiable

Usa un dispositivo que no haya sido alterado, actualiza el sistema y entra por los mecanismos oficiales de recuperación. Cambia primero el correo que permite recuperar otras cuentas y revisa sus reglas de reenvío, filtros, delegados y métodos de recuperación. Después cambia contraseñas con un gestor seguro y cierra sesiones y dispositivos vinculados. Una contraseña nueva no elimina una sesión persistente ni un filtro creado por el atacante.

Revisa número registrado, correo, PIN, dispositivos vinculados, sesiones, copias de seguridad y contactos de recuperación. Si el operador cambió tu SIM o el servicio dejó de funcionar, contacta al operador por sus canales oficiales y pregunta por el procedimiento de protección. No compartas con un desconocido el código que la plataforma acaba de enviarte para recuperar tu propia cuenta.

2.2 Revisión de aplicaciones y acceso remoto

Si instalaste una aplicación de soporte desconocida, registra su nombre y permisos y desconecta el equipo de redes según la necesidad de seguridad. Solicita ayuda técnica confiable para revisar persistencia, perfiles y aplicaciones con privilegios. No basta cerrar la ventana del programa de acceso remoto. Desinstalar puede ser necesario, pero conserva primero la información del paquete y los cambios observados si no aumenta el riesgo.

Si el atacante vio pantalla, archivos o códigos, considera comprometidas las credenciales relacionadas y cambia desde otro dispositivo. No le pidas al mismo “soporte” que desinstale su herramienta ni que revise tus cuentas. No ejecutes limpiadores recomendados por el contacto fraudulento: pueden ser una

segunda etapa del engaño.

2.3 Autenticación y recuperación como sistema

NIST SP 800-63B-4 trata autenticación, niveles de garantía y autenticación resistente al phishing. En la práctica, una clave o segundo factor puede seguir siendo vulnerable si el usuario lo entrega o si el atacante controla la recuperación. Revisa que los códigos lleguen al canal esperado y prefiere métodos resistentes al phishing cuando el servicio los ofrezca. No desactives protecciones para facilitar el acceso del supuesto técnico.[1]

Revisión	Acción segura	Error evitado
Correo principal	Contraseña nueva, sesiones cerradas, filtros y reenvíos revisados.	Recuperar otras cuentas con el correo comprometido.
Dispositivos	Cerrar vinculados y eliminar accesos no reconocidos.	Cambiar solo contraseña.
Recuperación	Verificar teléfono, correo, preguntas y contactos.	Dejar un canal controlado por el atacante.
Aplicaciones	Revisar origen, permisos y perfiles.	Confiar en el nombre de una app de soporte.
Contactos	Avisar por otro canal y compartir advertencia.	Permitir que el fraude continúe con otras personas.

Caso ficticio

Una persona comparte el código de WhatsApp con un supuesto agente. Desde otro teléfono recupera la cuenta, revisa dispositivos vinculados y cambia el correo de recuperación. Luego descubre una regla que reenviaba mensajes a otra dirección. Si solo hubiera cambiado la contraseña, la regla habría seguido exponiendo información.

Capítulo 3. Señales de engaño

3.1 Conducta antes que apariencia

El logotipo, la fotografía, el dominio parecido y la buena redacción no acreditan identidad. Revisa qué pide el mensaje: secreto, urgencia, instalación, transferencia, cambio de canal o amenaza. Un familiar real puede tener una emergencia, pero también puedes llamarlo al número conocido. Un banco puede pedir una acción, pero no debes validarla por el número que aparece en el texto.

Un enlace puede mostrar una dirección y abrir otra. No uses el texto visible para decidir; evita abrirlo y entra desde la aplicación o escribe el dominio oficial conocido. Un dominio con HTTPS solo indica una conexión cifrada, no que el sitio pertenezca a la institución ni que sea honesto. El certificado no evalúa la intención de la página.

3.2 Escenarios frecuentes

Escenario	Señal de riesgo	Respuesta inmediata
Familiar con número nuevo	Pide dinero o datos con urgencia y evita llamada.	Llamar al número anterior o a otro familiar.
Banco o soporte	Solicita código, contraseña o acceso remoto.	Colgar y contactar por canal oficial.
Premio o herencia	Exige comisión o documentos para liberar.	No pagar ni enviar identificación.
Inversión	Garantiza retorno y presiona para aumentar depósito.	No aportar más; conservar y reportar.
Préstamo	Pide contactos, permisos y pagos anticipados.	No instalar ni autorizar acceso a la agenda.
Paquetería	Cobro pequeño por enlace para liberar envío.	Consultar número de guía en canal oficial.
Empleo	Pide depósito, equipo o tareas con pago anticipado.	Verificar empresa por contacto independiente.
Recuperación de dinero	Promete recuperar por otra comisión.	No pagar segunda vez; reportar al canal oficial.

3.3 Cuando el mensaje viene de una cuenta real

Una cuenta conocida puede estar comprometida. La confianza no se basa en reconocer la foto, sino en comprobar la solicitud por otra vía. Pregunta algo que la persona pueda responder en llamada y, sobre todo, no realices la transferencia hasta hablar con ella. Una nota de voz o un video también puede reutilizarse o sintetizarse; la verificación del canal sigue siendo necesaria.

Regla doméstica útil

Acordar en familia una frase de verificación para solicitudes de dinero puede ayudar, pero no sustituye la llamada a un número conocido. Si la petición evita toda comprobación, la respuesta segura es detenerse.

El mensaje se evalúa por conducta, no por apariencia

ACCCF · RECONSTRUCCIÓN EDITORIAL · DATOS FICTICIOS

Logotipos y buena redacción no verifican una identidad

Señal	Pregunta útil	Respuesta segura
Urgencia	¿Impide verificar antes de actuar?	Pausa y canal oficial.
Código o enlace	¿Pide secreto o instalar acceso remoto?	No compartir ni instalar.
Pago irreversible	¿Exige tarjeta, cripto o cuenta nueva?	No enviar; conservar referencia.
Contacto familiar	¿Cambia número y pide ayuda inmediata?	Llamar al número ya conocido.
Garantía de ganancia	¿Promete retorno sin riesgo?	No aportar fondos ni documentos.

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

Figura 2. El mensaje se evalúa por conducta, no por apariencia. Logotipos y buena redacción no verifican una identidad Reconstrucción editorial; no constituye evidencia real.

Capítulo 4. Extorsión y contenido íntimo

4.1 No negociar ni difundir

Si alguien amenaza con difundir contenido íntimo o información privada, no pagues ni sigas enviando material. Pagar no garantiza eliminación ni fin de la extorsión. Conserva usuario, mensajes, URL, fecha, cuenta receptora y cualquier referencia sin descargar ni compartir el contenido íntimo con más personas. Busca apoyo de confianza y canales especializados o autoridades locales.

Si hay menores o peligro inmediato, se prioriza protección y denuncia especializada. No se almacena ni redistribuye material que pueda ser ilegal. Describe el objeto sin copiarlo y pide instrucciones al canal competente. La ayuda no debe condicionarse a que la persona entregue imágenes o cuente detalles que no necesitas para actuar.

4.2 Reducir la exposición posterior

Revisa privacidad, listas de contactos, fotos, enlaces, recuperación y cuentas conectadas. Cambia contraseñas desde un dispositivo seguro y cierra sesiones. Informa a contactos sin describir el material. Si el extorsionador contacta desde otra cuenta, conserva la relación entre perfiles y evita bloquear antes de preservar si eso no aumenta riesgo.

En México, los artículos 199 Octies y 199 Nonies del Código Penal Federal comprenden determinadas conductas de contenido íntimo sexual sin consentimiento, incluso cuando el material no corresponde a la persona identificada. En otros países cambian los tipos y vías; se consulta la norma local sin asumir que toda conducta tiene el mismo nombre o efecto.[2]

4.3 Acompañar sin revictimizar

No preguntes por qué envió el material ni le pidas que lo muestre. Ofrece ayuda concreta: estar presente, registrar lo mínimo, llamar al canal competente, revisar cuentas y evitar nuevos contactos. La culpa puede hacer que la persona acepte más exigencias del agresor. Escuchar sin juzgar puede impedir que la extorsión continúe por aislamiento.

> **Criterio de ayuda**
>
> Protege a la persona antes que al expediente. Si una acción de preservación puede aumentar difusión o peligro, se consulta primero con el canal especializado y se registra solo lo necesario.

Capítulo 5. Recuperación de cuentas

5.1 Orden de recuperación

Primero asegura dispositivo y correo principal, después autenticación y métodos de recuperación, luego sesiones, aplicaciones, banca y contactos. Cambia contraseñas repetidas con valores únicos y un gestor confiable. No anotes nuevas claves en una libreta abierta ni las envíes al mismo correo comprometido. Si un servicio ofrece llaves de acceso o métodos resistentes al phishing, evalúa su uso con una recuperación segura.

Revisa reglas de correo, filtros, delegación, respuestas automáticas, aplicaciones autorizadas, accesos de terceros y perfiles de administración. Un atacante puede conservar acceso mediante un filtro o aplicación aunque cambies contraseña. Conserva capturas de la configuración antes de modificar cuando eso no aumenta el riesgo.

5.2 Banca y operaciones

Contacta al banco con referencias y describe qué ocurrió sin inventar detalles. Pregunta por bloqueo, revisión, alertas y documentos necesarios. Si existe una operación no reconocida, solicita comprobante y registros del canal disponibles. La autenticación aceptada no demuestra por sí sola autorización: cambios de factor, enrolamiento y alertas pueden ser decisivos.

En México, las instituciones de crédito tienen reglas específicas de comprobantes, incidencias, bitácoras y atención de operaciones no reconocidas dentro de su régimen. En otros países cambian condiciones y plazos. El banco no garantiza restitución por el simple hecho de reportar, pero la notificación oportuna puede ser relevante. Guarda folio, fecha, nombre del canal y respuesta.[345]

5.3 Reporte y seguimiento

Registro	Contenido útil	Por qué importa
Banco	Folio, fecha, operación, canal y respuesta.	Seguimiento y comprobación de aviso.
Plataforma	Reporte, URL, cuenta y respuesta.	Relación con contenido y futuras copias.
Autoridad local	Canal, expediente, documentos y fecha.	No reemplazar por una publicación.
Operador	SIM, cambios, protección y folio.	Controlar recuperación por línea.
Contactos	Aviso, canal y fecha.	Prevenir nuevas víctimas.
Revisión	Cambios y alertas posteriores.	Detectar persistencia o segundo intento.

Cierre de la recuperación

No cierres cuando la pantalla vuelve a abrir tu cuenta. Cierra cuando recuperación, sesiones, filtros, dispositivos y contactos fueron revisados y tienes registro de los reportes.



Figura 3. Recuperar acceso también es revisar el entorno. La contraseña nueva no elimina sesiones ni reglas del atacante
Reconstrucción editorial; no constituye evidencia real.

Capítulo 6. Preservación y apoyo a otras personas

6.1 Paquete mínimo de evidencia

El paquete contiene cronología, mensajes, EML si existe, URL, cuentas, comprobantes, referencias, reportes y cambios observados. No incluye contraseñas, códigos, claves privadas ni datos personales innecesarios. Los archivos se conservan sin editar y se separan versiones de trabajo. La persona no necesita una colección enorme: necesita objetos que puedan relacionarse con su relato.

La cronología incluye cuándo llegó el mensaje, qué hizo la persona, cuándo pagó, cuándo llamó, qué cambió y qué reportó. Las horas se anotan con zona y se distinguen las declaradas de las comprobadas. Si no recuerda una hora, se indica aproximada, no se inventa precisión.

6.2 Cómo ayudar a alguien mayor o con poca experiencia

Pide permiso antes de revisar su teléfono y explica cada acción. No tomes su tarjeta ni le pidas contraseñas. Si necesita cambiar claves, que las escriba en privado mientras le explicas qué pantalla está viendo. Practica una regla sencilla: no compartir códigos, no instalar soporte remoto y llamar antes de pagar. La paciencia evita que la presión del fraude se sustituya por presión del ayudante.

Si la persona ya envió dinero, no la regañes. Ayuda a contactar al banco y a reunir referencias. El fraude explota confianza, miedo y prisa, no falta de inteligencia. La segunda estafa suele prometer recuperación: advierte que nadie debe cobrar otra comisión por supuestamente liberar fondos sin verificación institucional.

6.3 Directorio local que sí puedes usar

En lugar de copiar números de internet sin verificar, prepara un directorio con los canales que ya conoces: número oficial de tu banco en tarjeta o contrato, operador, plataforma, policía o fiscalía local, protección al consumidor, emergencia local, contacto familiar y persona de apoyo. Revisa los datos antes de una crisis y guárdalos en papel y en un lugar accesible.

Necesidad	Canal que debes verificar	No usar
Operación bancaria	Número en tarjeta, contrato o app oficial.	Teléfono enviado por el supuesto banco.
Cuenta o publicación	Centro de ayuda dentro de la plataforma.	Enlace de un comentario desconocido.
SIM o línea	Operador en app, contrato o sucursal oficial.	Código enviado por un tercero.
Emergencia física	Número de emergencia de tu localidad.	Esperar respuesta de redes.
Denuncia	Fiscalía o canal oficial de tu jurisdicción.	Publicación como única denuncia.
Apoyo emocional	Persona de confianza o servicio local.	Contactos que piden ver el contenido íntimo.

Cierre

La mejor preparación es una pausa acordada y un directorio verificado. No necesitas convertirte en investigador para evitar la siguiente pérdida.

Anexo A. Tarjetas de emergencia

A.1 Cuenta de WhatsApp comprometida

Secuencia breve

```
1. No compartas otro código ni pulses nuevos enlaces.
2. Desde un dispositivo seguro, recupera por el mecanismo oficial.
3. Revisa correo, recuperación, dispositivos vinculados y sesiones.
4. Cambia contraseñas y cierra accesos no reconocidos.
5. Revisa reglas, filtros, respaldo y apps autorizadas.
6. Avisa a contactos por otro canal.
7. Conserva mensajes, cambios y folios de reporte.
8. Vigila nuevos intentos; no contactes al atacante.
```

A.2 Pago o transferencia realizada

Secuencia breve

```
1. No envíes más dinero ni comisiones de recuperación.
2. Llama al banco por el número de tarjeta, contrato o app oficial.
3. Da referencia, fecha, importe, receptor y lo ocurrido sin inventar.
4. Conserva comprobantes, mensajes, URL y cuentas.
5. Pregunta por bloqueo, revisión y documentos del caso.
6. Guarda folio y respuesta.
7. Reporta a plataforma y autoridad local.
8. No sigas instrucciones del supuesto receptor.
```

A.3 Extorsión o contenido íntimo

Secuencia segura

1. No pagues ni envíes más contenido.
2. No reenvíes ni subas el material para pedir ayuda.
3. Conserva cuenta, mensajes, URL, fechas y referencias mínimas.
4. Busca una persona de confianza y el canal especializado local.
5. Si hay peligro o menores, prioriza emergencia y denuncia especializada.
6. Recupera cuentas y sesiones desde un dispositivo seguro.
7. Reporta publicaciones por canales oficiales.
8. No investigues ni negocies por tu cuenta.

A.4 Mensaje sospechoso de familiar o banco

Verificación antes de actuar

1. Detén la acción aunque parezca urgente.
2. No compartas códigos, contraseñas ni acceso remoto.
3. Llama al número que ya conocías, no al del mensaje.
4. Verifica la solicitud y la identidad por otra vía.
5. No pagues hasta comprobar.
6. Conserva mensaje, URL, cuenta y fecha.
7. Advierte a tus contactos si la cuenta real fue comprometida.

Anexo B. Cronología, directorio y control final

B.1 Cronología mínima

Fecha / zona	Evento y fuente	Acción realizada	Folio / evidencia
[Aproximada o exacta]	Mensaje recibido y objeto conservado.	Sin interacción adicional.	[ID]
[ ]	Código, instalación, pago o cambio.	Qué ocurrió realmente.	[Comprobante]
[ ]	Contacto con banco / plataforma.	Bloqueo, revisión o reporte.	[Folio]
[ ]	Recuperación de cuenta.	Contraseña, sesiones, filtros y apps.	[Registro]
[ ]	Aviso a contactos.	Prevención de nuevas víctimas.	[Canal]
[ ]	Revisión posterior.	Persistencia o nuevo intento.	[Pendiente]

B.2 Directorio personal para completar antes de una crisis

Servicio	Canal oficial verificado	Alternativa
Banco principal	[Número en tarjeta, contrato o app]	[Sucursal o app oficial]
Operador móvil	[App, contrato o sucursal]	[Canal de recuperación]
Plataforma principal	[Centro de ayuda interno]	[Correo oficial conocido]
Autoridad local	[Sitio o teléfono oficial]	[Fiscalía o dependencia]
Emergencia local	[Número oficial de tu ubicación]	[Servicio médico o seguridad]
Persona de apoyo	[Nombre y teléfono conocido]	[Segundo contacto]

B.3 Marco jurídico y revisión

Las operaciones electrónicas se analizan con reglas de mensaje de datos, registros y operaciones no reconocidas del país y sector. En México se revisan CCom 89–94 y 1205 y las disposiciones CNBV aplicables; Perú tiene reglas SBS; Argentina BCRA; España RD-ley 19/2018. Colombia y Ecuador exigen conservación de mensajes con contexto; Chile diferencia efectos de firma. No existe una restitución universal por presentar un comprobante.[6][7][8][9][10][11][12][13]

Control final	Respuesta esperada
¿Se detuvo el daño?	No más pagos, códigos, instalaciones ni difusión.
¿Se avisó?	Banco, plataforma, operador, autoridad y contactos según el caso.
¿Se preservó?	Mensajes, URL, EML, comprobantes, cambios y cronología.
¿Se recuperó?	Dispositivo, correo, contraseñas, sesiones, filtros y apps.
¿Se protegió a la persona?	Sin exposición, culpa ni segunda estafa.
¿Qué sigue?	Folio, pendientes, alertas y revisión posterior.

Cierre

Actuar pronto no exige actuar a ciegas. Una pausa, un canal oficial y una buena cronología pueden evitar que el primer engaño se convierta en varios.

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] 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

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

[3] 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

[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] 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] 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

[8] 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

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

[10] 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

[11] 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

[12] 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

[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

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.