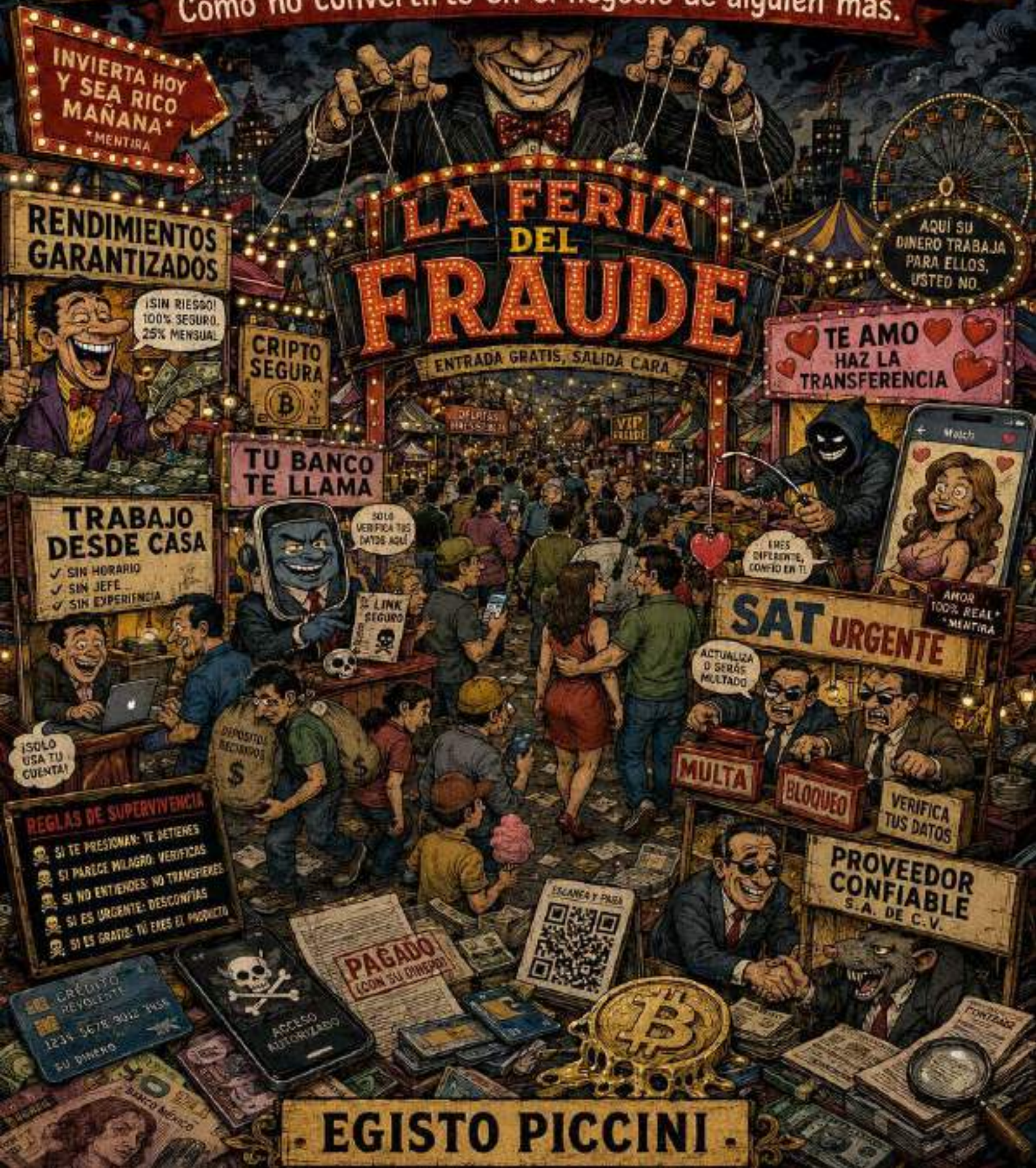
# MANUAL COMUNITARIO DE DEFENSA CONTRA ESTAFAS Y LAVADO DE DINERO

Cómo no convertirte en el negocio de alguien más.




EGISTO PICCINI

**Manual comunitario de defensa contra estafas y lavado de dinero.**


**Primera edición, 2026.**
**Hecho en México.**



**Esta publicación tiene fines informativos, educativos y de prevención comunitaria. El contenido no sustituye asesoría legal, fiscal, contable, financiera, médica, psicológica o de seguridad profesional. El autor no garantiza resultados específicos derivados del uso de la información contenida en esta obra y no asume responsabilidad por decisiones tomadas exclusivamente con base en su lectura.**

**Las referencias a instituciones, leyes, tipologías, delitos, riesgos, plataformas, herramientas, sectores o ejemplos prácticos tienen fines explicativos y de divulgación. Algunos nombres comerciales, marcas, logotipos, denominaciones o referencias mencionadas en esta obra pertenecen a sus respectivos titulares y se utilizan únicamente con fines descriptivos, educativos o de análisis.**

**El fenómeno del fraude, la ciberdelincuencia y el lavado de dinero evoluciona constantemente. En consecuencia, parte de la información, ejemplos, plataformas, métodos o marcos regulatorios aquí descritos puede cambiar con el tiempo. Se recomienda al lector verificar siempre la legislación vigente, los criterios regulatorios actualizados y las fuentes oficiales correspondientes.**

**Este libro busca fortalecer la cultura de prevención, el pensamiento crítico y la defensa comunitaria frente a estafas, fraudes financieros, delitos digitales y esquemas de lavado de dinero.**

**Autor: Egisto Piccini.**
**Año de edición: 2026.**

# Prólogo

Cuando Egisto me pidió escribir estas páginas, dudé un momento. No por falta de palabras —vivo de ellas tanto como él—, sino porque quien comparte la vida con un autor sabe que un prólogo escrito desde el cariño corre el riesgo de sobrar en afecto y faltar en justicia. Así que decidí escribir lo que de verdad pienso, que es algo más simple y más serio: este libro merecía existir, y su autor merecía escribirlo.

Yo vivo del otro lado del mostrador. Mi trabajo transcurre entre circulares de la CNBV, guías de GAFI y criterios de la UIF; entre auditorías, expedientes y manuales que casi nadie fuera del gremio llega a leer. Es un mundo necesario, pero blindado: habla en siglas, se atrinchera en tecnicismos y, demasiadas veces, deja afuera justo a quien más lo necesita —la familia que recibe la llamada "del banco", el estudiante que cae en la oferta de trabajo milagrosa, la PyME que paga la factura falsa del "CEO".

Lo que Egisto hizo en este manual es lo más difícil que conozco en esta profesión: tomar ese conocimiento amurallado y devolvérselo a la gente en su propio idioma. Aquí no hay diploma que ganar ni siglas que memorizar; hay patrones que reconocer y decisiones que tomar cinco minutos antes de hacer clic. Las mismas tipologías que yo persigo en una matriz de riesgo —del lavado clásico al pig butchering, del fraude en SPEI a la suplantación con deepfake— aquí están contadas para la mesa de la cocina y para la junta de los lunes. Eso no es divulgar a la baja: es traducir con respeto.

Y aquí está lo que de verdad me da orgullo. Llevo años viendo cómo esta materia —tan acusada de fría— enamora a quienes la trabajamos. Lo que este libro demuestra es que ese amor no tiene por qué quedarse entre especialistas: puede contagiarse a cualquiera. Empezó, lo confieso, en mi propia casa hace ya algún tiempo. Porque cuidarse y cuidar a los suyos también es una forma de cumplimiento, y cuidar, hecho con constancia, se parece más al amor de lo que esta profesión suele admitir.

Si algo puedo atestiguar —como compañera de vida y, él lo sabe, como colega exigente—, es que Egisto escribe como trabaja: con disciplina, con honestidad técnica y sin atajos. Reviso lo que escribe con el mismo rigor con que reviso un dictamen; por eso puedo decirlo sin adornos: aquí no hay frases que disimulen lo que no se entiende, hay un especialista que entiende lo que dice y decidió compartirlo con generosidad.

Si usted abre este libro por miedo —porque ya le pasó, o porque teme que le pase—, lo entiendo perfectamente. Pero le advierto, con conocimiento de causa, que es muy probable que lo cierre con algo más parecido al poder: la certeza tranquila de que el próximo intento de estafa, esta vez, no le va a ver la cara. Bienvenido a la defensa comunitaria. Y cuídese: esto de protegerse, cuando se hace bien, también enamora.

***Maribel Vázquez Menchaca***
*Querétaro, 2026*

# Introducción

Este libro nació de dos sentimientos que rara vez conviven bien: **indignación** y cariño.

Indignación, porque llevo años viendo cómo gente inteligente, trabajadora y honesta pierde ahorros, empresas, paz mental y hasta relaciones por culpa de estafas que, vistas con calma, tienen la misma estructura de siempre. Cambian las apps, cambian las redes, cambian los logos, pero el truco es el mismo: prisa, miedo, vergüenza, esperanza mal colocada.

Cariño, porque muchas de esas personas tienen nombre y cara para mí: familia, amigos, colegas, clientes, gente que me escribe después de una conferencia o un post para contarme "lo que me pasó" en voz baja, como si la culpa fuera suya. No lo es.

Trabajo en el cruce entre **compliance, prevención de lavado, regulación y comunicación**. Eso significa que vivo leyendo leyes, guías de GAFI, circulares de CNBV, criterios de la UIF, reportes de ciberseguridad y notas sobre escándalos financieros. Y luego, a la hora de explicar eso al mundo real, todo se reduce a la misma pregunta: "Ok, pero… ¿qué hago yo el lunes para que no me vean la cara?".

Este manual intenta responder esa pregunta, pero a lo grande:

- No está escrito para especialistas, está escrito para **comunidad**: familias, estudiantes, PYMEs, personas curiosas que no quieren un diploma, quieren herramientas.
- No glorifica al delincuente ni se obsesiona con el morbo de los casos; se enfoca en **patrones** y decisiones.
- No pretende que todos se vuelvan expertos en lavado, sino que sepan identificar cuando algo "huele" a colocación, estratificación, integración o simplemente a engaño clásico con envoltura moderna.

Vas a encontrar:

- Historias resumidas de estafas y escándalos que han hecho mucho daño, pero contadas en un lenguaje que podrías usar en la mesa con tu familia o en una junta con tu equipo.
- Tipologías clásicas (call center, romance scam, Ponzi) y emergentes (pig butchering, DeFi layering, NFT wash trading, RaaS), siempre aterrizadas a decisiones del día a día.
- Capítulos pensados para que cualquier PyME pueda hacer algo hoy: ajustar un proceso, cambiar un flujo de aprobación, capacitar a su gente, revisar a sus proveedores.
- Y, sobre todo, **reglas simples**, checklists y casos prácticos para que no tengas que memorizar siglas, solo principios.

No esperes aquí neutralidad fría. Creo firmemente que la ignorancia nos sale carísima y que la prevención es un acto político en el mejor sentido: una comunidad informada es una comunidad más difícil de controlar, de robar, de silenciar.

Te invito a leer este libro a tu ritmo, sin obsesionarte con entender cada detalle técnico. Lo importante no es recordar cada sigla, sino que, cuando te llegue la próxima llamada rara, el próximo WhatsApp "urgente", la próxima inversión milagrosa o el próximo correo extraño en tu PyME, algo en tu cabeza haga clic y digas:

"Esto ya lo vi. Aquí hay un patrón.
Voy a frenar, voy a verificar, no voy a decidir en automático."

Si este manual logra que unas cuantas personas tomen una mejor decisión en el momento incómodo donde se define todo —cinco minutos antes de hacer clic en "Aceptar", de dictar un código o de firmar un contrato—, habrá cumplido su función.

Gracias por leerlo, por compartirlo y, sobre todo, por usarlo en tus conversaciones y en tus procesos. La defensa comunitaria empieza exactamente ahí: en lo que hablamos, en lo que dejamos pasar y en lo que decidimos no normalizar.

Egisto Piccini
México, 2026

# Índice general

# Capítulo 1 — Estafas clásicas de calle

La calle siempre ha sido la universidad del fraude: no necesitas internet, solo prisa, confianza mal puesta y un poquito de vergüenza para no quedar como desconfiado. Aquí viven los trucos de siempre con nombres de siempre: cambiazo, estampita, tocomocho, secuestro “virtual” que se siente muy real. Si crees que ya nadie cae en eso, este capítulo es para recordarnos que, con el envoltorio correcto, todos traemos un “yo” capaz de perder dinero en la esquina de la casa.


Bienvenidos al único lugar donde todos saben que es estafa... menos el que paga
CALLE DEL MAÑANA (QUIÉN SABE)
TODO BARATO *MENOS TU TRANQUILIDAD
¡HOY PUEDE SER SU DÍA!
¿QUÉ MÁS DA... TOTAL YA ESTOY CANSADO
EMPANADAS CON SORPRESA ¿DE QUÉ?
ES LA LEY (DE NUESTRA BOLSA)
LOTERÍA MILAGROSA
PREMIO GARANTIZADO (SEGÚN YO)
INSPECTOR DE TODO
MULTA INMEDIATA
PAGUE YA O LLORE DESPUÉS
RECIBO OFICIAL CORRUPCIÓN EXPRESS
YO TAMBIÉN CAÍ UNA VEZ... POR PENDEJO
¡TRUCO MAESTRO! SU DINERO DESAPARECE COMO POR ARTE DE MAGIA
SECUESTROS VIRTUALES AQUÍ, PASE SIN MIEDO
SE HACEN TRÁMITES MÁGICOS
• RÁPIDO
• FÁCIL
• DUDOSO
100% INCIERTO
ADIVINO SU FUTURO (MAÑANA VEMOS)

## 1.1 Cambiazo

### Qué es

El cambiazo es la estafa de billetes por excelencia: el estafador te pide cambiar un billete grande o pagar con uno, y en la maniobra de "te lo devuelvo porque está mal" hace un truco de manos para sustituir el billete bueno por uno falso o de menor denominación. Aprovecha tres cosas: prisa, confianza y la vergüenza de contar el dinero delante de los demás.

### Señales de alerta

- Personas desconocidas que te piden cambiar billetes en la calle o estacionamientos.
- Clientes que "se arrepienten" varias veces y piden que les vuelvas a entregar o revisar el cambio.
- Billetes que "aparecen" en la mano del estafador diciendo que se los diste mal, sin que tú lo hayas visto claro.

### Cómo defenderte

- No cambies billetes a desconocidos en la calle o estacionamientos.
- Si eres comercio, cuenta el efectivo siempre a la vista y deja los billetes grandes encima de la caja hasta cerrar la operación.
- Usa detector de billetes falsos y rechaza cualquier presión por "hacerlo rápido".
- Si la situación te incomoda, cancela la operación y pide al supuesto cliente que vaya al banco.

---

## 1.2 Estampita

### Qué es

La estampita es la versión callejera del "dinero encontrado". Un cómplice finge ser ingenuo y dice haber encontrado un paquete con dinero o valores. Te ofrece repartirlo contigo si aportas un "depósito de confianza" para no quedar mal si aparece el dueño. Cuando quieres abrir el paquete, dentro solo hay papeles recortados, periódicos o billetes falsos. El truco: activar tu codicia y tu sentido de "ganancia rápida".

### Señales de alerta

- Alguien que "se encuentra" dinero o valores en la calle y te lo ofrece a cambio de que pongas efectivo propio.

- Historias de “no quiero problemas, pero podemos ganar los dos”.
- Te apuran a decidir y alejarte rápido del lugar antes de verificar el contenido.

**Cómo defenderte**

- Parte de la base: si alguien te ofrece dinero encontrado, el premio eres tú.
- No aceptes participar en repartos de dinero hallado; es potencialmente delito y casi siempre estafa.
- Si ves algo sospechoso, retírate de la escena y, si es muy evidente, llama al 911.
- Evita manipular paquetes de desconocidos en vía pública.

---

# 1.3 Tocomocho

**Qué es**

El tocomocho es el primo fino de la estampita. Aquí el gancho es un supuesto billete de lotería premiado que “no pueden cobrar” por algún motivo: no tienen identificación, están de paso, son extranjeros, etc. Te lo venden barato para que “tú lo cobres”, pero el billete es falso, ya caducó o nunca estuvo premiado. El estafador juega a la ignorancia combinada con tu sueño de dar el campanazo.

**Señales de alerta**

- Personas que ofrecen un boleto de lotería “seguro ganador” a precio de remate.
- Historias dramáticas sobre por qué no pueden ir a cobrarlo ellos mismos.
- Insistencia en que decidas de inmediato sin verificar en un punto oficial.

**Cómo defenderte**

- Nunca compres boletos “ganadores” en la calle; un premio legítimo se cobra en canales oficiales.
- Verifica siempre en la página o agencia oficial de Lotería Nacional/Pronósticos.
- Si no puedes verificar en ese momento, la respuesta correcta es “no”.
- Desconfía de cualquiera que te ofrezca moneda mágica a cambio de efectivo real.

---

# 1.4 Falsos inspectores

**Qué es**

Los falsos inspectores se disfrazan de autoridad: CFE, agua, Protección Civil, Profeco, SAT, municipio. Llegan con chaleco, gafete y carpeta en mano, diciendo que vienen a revisar medidores, extinguidores o permisos. Una vez dentro de tu casa o negocio, pueden robar directamente o presionarte para pagar una "multa en efectivo" en el acto para evitar "clausura" o "corte del servicio". Lo central es la apariencia de burocracia mezclada con miedo.

**Señales de alerta**

- "Inspectores" que llegan sin visita programada y sin notificación previa por escrito.
- Amenazas de clausura o corte inmediato si no pagas en ese momento.
- Solicitudes de pago en efectivo o a cuentas personales, no institucionales.

**Cómo defenderte**

- Pide siempre credencial oficial y número de oficio o visita; anótalo o toma foto.
- Llama tú al conmutador oficial de la dependencia (no al número que ellos te den) y verifica la visita.
- No permitas el acceso a áreas privadas hasta confirmar la legitimidad.
- Nunca pagues en efectivo "ahí mismo"; exige línea de captura o recibo oficial.

---

## 1.5 Falso accidente familiar

**Qué es**

Es una estafa telefónica basada en el pánico. Recibes una llamada donde alguien dice ser policía, médico o "amigo de tu familiar" y afirma que esa persona tuvo un accidente grave. Te piden depositar o transferir dinero urgente para una cirugía, ambulancia o "fianza" para evitar que lo retengan. El estafador busca que no verifiques nada, solo reacciones al miedo y la culpa.

**Señales de alerta**

- Llamadas de números desconocidos con tono dramático: "soy del hospital", "soy licenciado", todo es "urgente".
- No te permiten colgar ni hablar con tu familiar directamente.
- Exigen que hagas depósitos a cuentas de personas físicas o por OXXO/SPEI:

**Cómo defenderte**

- Cuelga, respira y llama de inmediato al celular de tu familiar o a otros miembros de la familia.

- Establece con tu familia una palabra clave para emergencias que el estafador no pueda conocer.
- No hagas ningún depósito mientras estés al teléfono con el supuesto "abogado" o "doctor".
- Si la llamada es muy agresiva, registra el número y repórtalo a la autoridad local.

---

## 1.6 Secuestro virtual

**Qué es**

El secuestro virtual lleva el falso accidente al siguiente nivel. Escuchas gritos, llanto y una voz que se hace pasar por tu familiar "secuestrado". El grupo exige dinero inmediato y te ordena que no cuelgues ni intentes comunicarte con nadie. En realidad, tu familiar está libre y el montaje se hace con audios grabados o cómplices. El objetivo es mantenerte aislado, en shock y obediente.

**Señales de alerta**

- Gritos y llanto que suenan repetitivos o poco convincentes, muchas veces en altavoz.
- No te dan datos precisos (nombre completo, detalles reales de tu familiar), solo información que tú mismo vas soltando.
- Exigen depósitos urgentes en tiendas de conveniencia o transferencias a cuentas desconocidas.

**Cómo defenderte**

- Cuelga o al menos pon la llamada en altavoz y escribe a tu familiar por WhatsApp, Telegram u otro canal.
- Pregunta cosas que solo tu familiar sabría (apodo, detalle íntimo), y si no responden bien, corta.
- No proporciones nombres ni datos de tu familia durante la llamada; cuanto menos sepan, mejor.
- Contacta a la policía local o a la Policía Cibernética para reportar el número y recibir acompañamiento.

Si algo dejan claro estas estafas es que la calle no perdona la prisa ni el "me dio pena decir que no". La próxima vez que alguien te pida confianza inmediata en un

estacionamiento, en la banqueta o por teléfono, recuerda que no estás siendo grosero: estás cortando el truco a la mitad. En este terreno, el verdadero “tonto” no es el que sospecha, sino el que decide quedar bien con un desconocido

# Capítulo 2 — Fraudes de comercio y consumo digital

A la estafa de toda la vida le pusimos wifi, carrito de compras y botón de "pagar ahora". Las tiendas clonadas, las ofertas imposibles y los productos fantasma son la versión 2.0 del vendedor que te juraba que era "original de fábrica". En este capítulo vamos a ver cómo el marketing, el FOMO y los descuentos ridículos se combinan para que tú pongas los datos, el dinero y, de paso, la excusa de "es que se veía muy real".


# E-COMMERCE:
# TÚ PONES LOS DATOS, ELLOS PONEN LA ESTAFA

## 2.1 Tiendas clonadas y e-commerce falso

### Qué es

Las tiendas clonadas son páginas web que copian logo, colores y estilo de marcas conocidas (Liverpool, Amazon, Mercado Libre, Zara), pero el dominio es ligeramente distinto y no pertenecen a la marca real. Ofrecen ofertas imposibles, cobran por adelantado y nunca entregan nada, o envían basura para simular que "hubo envío". Muchas operan desde redes sociales, con links a dominios recién creados, servidores en el extranjero y métodos de pago difíciles de rastrear (transferencias, depósitos, wallets).

### Señales de alerta

- Dominios raros: terminaciones extrañas, guiones de más, nombres mal escritos (liverpoI.com, amaz0n-ofertas.net).
- Descuentos absurdos (70–90%) en productos que normalmente casi no bajan de precio.
- Sitios sin aviso de privacidad, sin razón social, sin RFC y sin domicilio en México.
- Solo aceptan pago por transferencia, depósito o wallets; no hay opción de tarjeta con protección al comprador.
- Reseñas perfectas pero poco creíbles, todas recientes y sin detalle real.

### Cómo defenderte

- Escribe tú mismo la URL oficial de la tienda en el navegador o entra desde la app, nunca desde un link de anuncio sospechoso.
- Revisa el dominio en el WHOIS: si se registró hace unas semanas y ya "es una gran marca", algo huele mal.
- Prefiere siempre métodos con protección al comprador (tarjeta de crédito, plataformas consolidadas, Mercado Pago).
- Busca reseñas fuera del sitio, en Google, foros o redes; si no aparece nada o todo es negativo, no compres.
- Si ya fuiste víctima, guarda capturas de pantalla, comprobantes y levanta queja en Profeco y tu banco.

---

## 2.2 Productos fantasma en redes sociales

### Qué es

Los productos fantasma son ofertas que ves en Facebook, Instagram, TikTok o WhatsApp: pantallas, consolas, celulares, viajes, a precios demasiado buenos. Te piden pagar por adelantado, muchas veces con el argumento de "precio de mayoreo",

“liquidación de bodega” o “solo hoy”. Una vez que transfieres, bloquean tu número, borran el perfil o cambian de nombre. A veces envían un producto distinto y de baja calidad solo para decir “sí envié algo” ante la plataforma.

**Señales de alerta**

- Perfiles nuevos con pocos seguidores, casi sin publicaciones anteriores y todo lleno de “mega oferta”.
- Mensajes privados que te presionan para pagar “antes de que se acabe la promo” o “porque ya hay otros interesados”.
- Piden transferencia directa a cuentas personales (no a una razón social) y no aceptan pago contra entrega.
- Fotos robadas de otras páginas; si haces búsqueda inversa en Google Images aparecen en mil lados.

**Cómo defenderte**

- Desconfía de cualquier oferta con precio 40–50% por debajo del mercado, salvo que se trate de un outlet oficial.
- Usa siempre plataformas que tengan mediación y protección al comprador (Marketplace con envío protegido, Mercado Libre, Amazon).
- Nunca pagues por adelantado a cuentas personales sin reputación ni referencias.
- Haz búsqueda inversa de las fotos y del texto de la publicación para ver si es contenido robado.
- Si ya fuiste estafado, guarda capturas y denuncia en la propia plataforma y ante Profeco.

---

## 2.3 Estafas de paquetería y envíos

**Qué es**

Las estafas de paquetería suelen llegar por SMS, correo o WhatsApp: “Tu paquete está detenido, paga $35 de aduana”, “No se pudo entregar tu paquete, actualiza tu dirección aquí”. El enlace lleva a una página que imita a DHL, FedEx, Estafeta o Correos, donde te piden datos de tarjeta o instalar una supuesta app de seguimiento. Ahí roban tus datos de pago o infectan tu dispositivo. En otros casos llaman fingiendo ser la paquetería para cobrar un “recargo” por teléfono.

**Señales de alerta**

- Mensajes genéricos que no especifican de qué tienda viene el supuesto paquete.
- Enlaces acortados o dominios que no son los oficiales de la paquetería.

- Peticiones de pago de “impuestos” de pocos pesos por tarjeta bancaria, sin factura ni referencia aduanal real.
- Llamadas que exigen que pagues en ese momento para evitar que el paquete “regrese al extranjero”.

**Cómo defenderte**

- Si esperas un paquete, consulta siempre desde la app oficial o la web oficial de la paquetería escribiendo tú mismo la dirección.
- No uses enlaces que lleguen por SMS, correo o WhatsApp para entrar a supuestas páginas de envío.
- Nunca pongas datos de tu tarjeta para pagar “cargos aduanales” sin un documento formal de la empresa o de la autoridad.
- Ante la duda, llama al número oficial de la paquetería y pregunta por tu guía, no uses el teléfono del mensaje sospechoso.
- Si ya pusiste datos de tarjeta, repórtala de inmediato al banco y pide reposición.

---

## 2.4 QR adulterado y quishing

**Qué es**

El quishing es el phishing con código QR. Un estafador pega una calcomanía con su propio QR encima del QR legítimo de un restaurante, parquímetro, estacionamiento o negocio. Cuando escaneas, en lugar de llevarte a la página del banco/municipio, te manda a una web falsa o una app maliciosa que roba datos de tarjeta, credenciales bancarias o instala malware. Todo se apoya en la confianza ciega de “si es un QR impreso, debe ser seguro”.

**Señales de alerta**

- QR con etiqueta pegada encima de otro QR, o con diseño claramente distinto al resto del material gráfico.
- Te manda a un sitio con dominio raro, sin candadito HTTPS o en idioma distinto.
- La página te pide datos de tarjeta, NIP o CVV cuando se supone que solo ibas a pagar una multa, estacionamiento o cuenta de restaurante.
- QR pegados en postes, paredes o mesas sin ninguna marca ni contexto claro.

**Cómo defenderte**

- Antes de escanear, fíjate si el QR no está encima de otro o no parece una etiqueta improvisada.

- Revisa la URL completa a la que te manda: dominio, HTTPS y nombre de la institución.
- Para pagos a gobierno o bancos, usa mejor la app oficial o la web que ya conoces, no códigos pegados al azar.
- Si eres comercio, protege tus QRs con plástico o impresos grandes, y revisa periódicamente que nadie pegue stickers encima.
- Si escaneaste un QR sospechoso, cierra la página, no instales nada y borra la pestaña del navegador.

---

## 2.5 Empleos falsos y "trabaja desde casa"

### Qué es

Los empleos falsos de comercio y consumo explotan la necesidad económica. Te llegan mensajes por WhatsApp o anuncios en redes ofreciendo "trabajo desde casa, 2 horas al día, gana $3,000 diarios", generalmente dando likes, valorando productos, rellenando encuestas o "probando apps". Al principio pueden pagarte cantidades pequeñas para generar confianza, pero pronto te piden que "inviertas" en paquetes, membresías o desbloqueos. Pagas… y desaparecen. En la versión más burda, te cobran por adelantado por "gestión de vacante" o "curso obligatorio".

### Señales de alerta

- Ofertas con ingresos muy altos por tareas ridículamente simples ("solo dar likes", "solo compartir links").
- Te contactan directamente por WhatsApp sin que hayas aplicado a nada, muchas veces desde números extranjeros.
- Te piden pagar inscripción, curso, membresía, software o "kit de trabajo" antes de darte trabajo real.
- No hay contrato formal, razón social ni RFC claros; todo se maneja en chats y grupos de Telegram.

### Cómo defenderte

- Recuerda la regla de oro: ningún empleo legítimo te pide dinero para darte trabajo. Si tienes que pagar para entrar, no es empleo, es negocio para ellos.
- Verifica siempre la empresa: página web, redes, RFC, opiniones en Google, LinkedIn y OCC / Computrabajo.
- Desconfía de ganancias muy altas sin perfil profesional claro ni proceso de selección real.
- No compartas tus datos personales completos (INE, CURP, cuenta bancaria) solo por "registrarte" en un chat.
- Si ya transferiste, guarda chats y comprobantes y presenta denuncia ante la Policía Cibernética y Profeco.

El comercio digital no es malo ni bueno: solo hace más rápido lo que ya estaba ahí, incluida la estafa. Si una oferta necesita que decidas en segundos, pagues por adelantado y no verifiques nada fuera de la propia página, no estás ante un descuento, estás ante un casting para víctima. Comprar con criterio no mata la emoción de la oferta; mata la probabilidad de terminar comprando un pantallazo.

# Capítulo 3 — Fraudes financieros básicos

Tu banco tiene app, pero la estafa también. Entre correos que parecen oficiales, SMS dramáticos y llamadas “de seguridad”, el juego es siempre el mismo: lograr que tú mismo entregues lo que nadie podría robarte por fuerza. Aquí vamos a desmenuzar phishing, vishing, smishing, SIM swap y compañía, sin tecnicismos de manual, pero con suficiente mala leche para que la próxima vez que veas un enlace “por tu seguridad” te dé más risa que confianza.


NO ES TU BANCO.
SOLO SE VISTE MEJOR QUE ÉL
100%
BANQUERO DIGITAL VIP PREMIUM
OFICIALMENTE SEGURO (SEGÚN NADIE)
SMS
ACTUALIZA TU SEGURIDAD (Y REGÁLAME TODO)
VERIFICA AQUÍ ANTES DE PENSAR
ALERTA DE SU BANCO: INGRESE YA O BLOQUEAREMOS SU CUENTA (PARA SIEMPRE)
ACEPTO
ACEPTO
ACEPTO SIN
SIN LEER
ACEPTO
ACEPTO
ACEPTO SIN
ACEPTO LEER
SU DATOS.
SU DINERO.
SU LIBERTAD.
UN SOLO CLIC.
SONRÍA, LO ESTAMOS AYUDANDO.

# 3.1 Phishing

### Qué es

El phishing es el clásico correo o mensaje que se hace pasar por tu banco, por el SAT, por Mercado Pago o por una institución conocida para robar tu usuario y contraseña. Te dicen que hay un cargo raro, que tu cuenta será bloqueada o que debes "actualizar datos" y te dejan un enlace. La página a la que llegas es una copia visual del sitio real, pero todo lo que escribes va directo al estafador. No atacan al banco; te atacan a ti y a tus decisiones.

### Señales de alerta

- Correos que saludan con "Estimado cliente" sin tu nombre completo.
- Faltas de ortografía o redacción rara, mezcla de tuteo y ustedeo.
- Enlaces que, al pasar el mouse encima, muestran un dominio distinto al de tu banco o SAT.
- Advertencias de "último aviso", "bloqueo inminente", "debes actuar en 24 horas".

### Cómo defenderte

- Nunca entres a tu banca en línea desde un link; escribe tú mismo la dirección en el navegador o usa la app oficial.
- Revisa siempre la barra de direcciones: dominio exacto, HTTPS y candado.
- Si te preocupa un aviso, llama tú al número oficial del banco o entra por tu app, no respondas el correo.
- Activa notificaciones de movimientos en tu app para detectar cargos raros de inmediato.
- Si caíste, cambia tu contraseña de inmediato y reporta al banco para bloquear accesos.

---

# 3.2 Vishing (phishing por voz)

### Qué es

El vishing es el phishing por llamada telefónica. Alguien se hace pasar por ejecutivo del banco, por personal del "área antifraude" o incluso por el call center del SAT. Te dicen que hay cargos sospechosos o que tu cuenta está comprometida, y que para ayudarte necesitan que les des datos de tu tarjeta, NIP, token o el código que te acaba de llegar por SMS. Con esa información, los que hacen el fraude son ellos.

### Señales de alerta

- Llamadas “del banco” pidiéndote NIP, token completo o CVV “para cancelar un cargo”.
- Te generan miedo: “si cuelga se ejecutará el cargo”, “si no actúa ya, le vacían la cuenta”.
- No permiten que cuelgues para “verificar por tu cuenta”.
- A veces usan números que en el identificador parecen del banco (caller ID spoofing).

**Cómo defenderte**

- Ten claro este principio: ningún banco legítimo te pedirá tu NIP, tu token completo ni el CVV por teléfono.
- Cuelga la llamada, toma tu tarjeta y marca tú al número que viene impreso atrás.
- No dictes códigos que te lleguen por SMS mientras estés en una llamada que no iniciaste tú.
- Si ya diste datos, avisa de inmediato al banco para bloqueo de tarjetas, cuentas y banca digital.
- Registra el número y repórtalo a Condusef y a la Policía Cibernética.

---

## 3.3 Smishing (phishing por SMS)

**Qué es**

El smishing es el phishing por mensaje de texto. Te llega un SMS diciendo “Tu cuenta ha sido bloqueada”, “Se ha detectado un acceso desconocido”, “Actualiza tus datos aquí”. Incluye un enlace corto o raro. Al hacer clic, te lleva a una página que imita el sitio de tu banco o servicio, donde te piden usuario, contraseña, token o datos de tarjeta. El SMS explota la sensación de inmediatez y la confianza de que “si llegó al celular, debe ser real”.

**Señales de alerta**

- Mensajes de números celulares normales o remitentes genéricos, no del corto oficial del banco.
- Links acortados (bit.ly, tinyurl) o dominios raros.
- Ortografía floja, emojis fuera de lugar, mayúsculas y minúsculas mezcladas.
- Mensajes que insisten en que “si no das clic perderás acceso a tu cuenta”.

**Cómo defenderte**

- No hagas clic en links que vengan por SMS, aunque parezcan del banco.
- Si te asusta el mensaje, abre tú la app oficial del banco o entra a la web escribiendo la dirección.

- Borra el SMS y bloquea el número remitente.
- Guarda una captura si quieres denunciar; puedes hacerlo ante Condusef y la Policía Cibernética.
- Activa en tu teléfono filtros de spam y mensajería no solicitada.

---

## 3.4 SIM swap (robo de línea telefónica)

**Qué es**

El SIM swap es cuando alguien logra que tu compañía telefónica pase tu número a un chip distinto, diciendo que "perdió su celular" o que "cambió de equipo". En cuanto tu línea se transfiere, tu propio teléfono se queda sin señal. El delincuente recibe todos tus SMS, incluidos los códigos de verificación de tu banco, correo, redes sociales, wallets de cripto, etc. Con eso puede resetear contraseñas y tomar control de tus cuentas.

**Señales de alerta**

- De pronto tu celular se queda sin señal ni datos mientras otros equipos de la casa siguen con servicio.
- Te llegan correos de "cambio de contraseña" que tú no solicitaste.
- Notas intentos de inicio de sesión desde otros dispositivos.
- La compañía telefónica te contacta diciendo que procesó una solicitud que tú no hiciste.

**Cómo defenderte**

- Pide a tu operador que active un PIN de portabilidad o contraseña adicional para cualquier cambio de chip.
- Usa aplicaciones de autenticación (Google Authenticator, Authy, 1Password) en lugar de SMS para 2FA.
- Si de pronto pierdes señal sin explicación, llama desde otra línea a tu operador y a tu banco de inmediato.
- No publiques tu número celular principal en todas tus redes; considera uno exclusivo para banca y servicios críticos.
- Revisa con regularidad qué dispositivos tienen sesión activa en tu correo y redes.

---

## 3.5 Skimming y clonación de tarjetas

**Qué es**

El skimming es el uso de dispositivos físicos para copiar la información de la banda magnética de tu tarjeta cuando la pasas por un cajero automático o terminal punto de venta. Suele complementarse con una microcámara o alguien observando (shoulder surfing) para capturar tu NIP. Con esos datos, crean una tarjeta clonada y realizan retiros o compras como si fueras tú. Es un fraude silencioso: tú sigues con tu tarjeta en la cartera, pero ya existe un clon en algún lado.

**Señales de alerta**

- Cajeros automáticos con ranura extraña, floja, manchada o con piezas añadidas.
- TPVs que el empleado se lleva fuera de tu vista o pasa varias veces "porque no pasa".
- Te piden que dicites el NIP en lugares poco discretos, sin cuidado por la privacidad.
- Aparecen cargos en tu estado de cuenta en lugares donde no estuviste.

**Cómo defenderte**

- Usa preferentemente cajeros dentro de sucursales o lugares bien iluminados, no en la calle o gasolineras solitarias.
- Antes de usar un cajero, mueve ligeramente la ranura: si algo se siente flojo, no lo uses.
- Siempre tapa el teclado con tu mano al teclear el NIP, aunque estés en un lugar "seguro".
- Pide que la terminal te la traigan a la mesa y nunca pierdas de vista tu tarjeta.
- Activa alertas de movimientos por SMS o app y revisa con frecuencia tus estados de cuenta para detectar cargos raros rápido.

En casi todos estos casos, el banco real siempre te da algo que el estafador jamás: tiempo para pensar. Si una llamada, un SMS o un correo te exigen actuar ya, dictar códigos o compartir datos "por tu seguridad", lo más seguro es que el único riesgo seas tú obedeciendo. La regla es simple: con tu dinero y tus claves, primero dudas, luego verificas, y si acaso después haces clic.

# Capítulo 4 — Estafas románticas y emocionales

Hay fraudes que no empiezan con números, empiezan con “hola, ¿cómo amaneciste?”. Romance scams, grooming financiero, sextorsión y demás encantos digitales no te atacan por el saldo, sino por la soledad, el deseo, el ego y las ganas de sentirte especial. En este capítulo vamos a hablar de amor, pero del tipo que llega por chat, pide fotos, pide confianza y termina pidiendo un SPEI.


PRIMERO TE DICEN 'MI AMOR', LUEGO 'HAZ LA TRANSFERENCIA'
100
ESTA VEZ SÍ ES DIFERENTE
Soulmate_01
DoctorHonesto22
InversionistaGuapo
SOLO NECESITO CONFIAR EN ALGUIEN
100
200

# 4.1 Romance scam

### Qué es

El romance scam es la estafa que se disfraza de amor. Un perfil (en Tinder, Bumble, Facebook, Instagram o incluso LinkedIn) construye un vínculo afectivo contigo durante semanas o meses. Se muestra atento, disponible, romántico, dice todo lo correcto. Luego viene la "emergencia": un tratamiento médico, un problema legal, un vuelo urgente para ir a verte, una cuenta hospitalaria, una aduana complicada. Siempre hay una razón para que tú envíes dinero "solo por esta vez" mientras él o ella promete devolvértelo y seguir el plan de vida juntos. El vínculo emocional es el vector del fraude.

### Señales de alerta

- Perfíl demasiado perfecto: guapo/a, exitoso/a, pero "extrañamente solitario/a" con interés exclusivo en ti.
- Se enamora muy rápido y habla de matrimonio, negocios en común o mudarse contigo sin haberte visto en persona.
- Siempre tiene pretextos para no hacer videollamadas claras (mala señal, mala cámara, "estoy en base militar", etc.).
- Historias de emergencia que requieren transferencias o envío de dinero, a veces en cripto o tarjetas de prepago.
- Se molesta o te culpa si dudas o retrasas el envío: "si no confías en mí, no me mereces".

### Cómo defenderte

- Regla dura: nunca envíes dinero a alguien a quien no has conocido en persona y con quien no tengas vínculos reales comprobables.
- Exige videollamadas sin filtros, con cámara estable y acciones específicas (que escriba tu nombre en papel, que muestre su entorno).
- Haz búsqueda inversa de sus fotos en Google o Yandex; si salen en otros perfiles con nombres distintos, es catfish.
- Habla de la relación con alguien de confianza fuera de la burbuja; escucharla en voz alta ayuda a detectar banderas rojas.
- Si ya enviaste dinero, corta contacto, guarda evidencias y denuncia ante Policía Cibernética y tu banco.

---

# 4.2 Catfishing

### Qué es

El catfishing es la construcción de una identidad falsa compleja: fotos robadas, biografía inventada, trabajo ficticio, amigos falsos. No siempre busca dinero inmediatamente; a veces el objetivo es manipular emocionalmente, obtener material íntimo o simplemente jugar con tu percepción. En su versión financiera, el catfish se convierte en la base para pedir préstamos, inversiones o favores económicos. Puede darse en apps de citas, redes sociales, foros, comunidades de gaming o grupos de interés.

### Señales de alerta

- Perfil con pocas fotos, todas "de catálogo", estilo influencer, pero sin tags reales de amigos ni fotos casuales.
- Inconsistencias en su historia: ciudad donde vive, huso horario, datos laborales que no cuadran.
- Se resiste a conocerte en persona aunque vivan en la misma ciudad; siempre hay excusas.
- Evita videollamadas o en las pocas que hay, la calidad es muy mala o se ve raro (puede ser deepfake).
- Sus "amigos" en redes son en su mayoría cuentas vacías o también dudosas.

### Cómo defenderte

- Pide videollamadas desde el inicio; si siempre hay excusas, trata el perfil como falso hasta prueba en contrario.
- Haz búsqueda inversa de imágenes; si la misma cara aparece en perfiles con otros nombres o en bancos de imágenes, alerta.
- Verifica su historia en LinkedIn, Twitter, Google; un director de empresa inexistente probablemente no es director de nada.
- No compartas información demasiado íntima ni documentos personales con alguien cuya identidad no esté verificada.
- Si detectas un catfish, bloquea y reporta el perfil en la plataforma; así ayudas a que otros no caigan.

---

## 4.3 Sextorsión

**Qué es**

La sextorsión ocurre cuando, tras intercambiar fotos o videos íntimos (o incluso solo mensajes subidos de tono), la otra parte te amenaza con publicar ese contenido si no pagas. Puede ser un contacto que conociste en app de citas, una cuenta que finge ser "modelo", o incluso una cuenta hackeada de alguien real. Piden dinero por transferencia, depósitos en tiendas, cripto o tarjetas prepagadas. Su poder no está en la tecnología, sino en la vergüenza: cuentan con que te paralices por miedo a que familia, pareja o trabajo se enteren.

**Señales de alerta**

- Perfiles recién creados que rápidamente llevan la conversación a lo sexual y piden material íntimo.
- Insisten en que prendas la cámara o envíes fotos "para confiar en ti" muy pronto en la conversación.
- En cuanto reciben material, cambian el tono y empiezan las amenazas: "si no pagas, se lo mando a todos tus contactos".
- Envían capturas de pantalla de tu lista de amigos o familiares para presionarte.

**Cómo defenderte**

- La regla más segura: no compartas fotos o videos íntimos con personas que no conoces ni de las que no confías plenamente.
- Si ya ocurrió, no pagues: pagar rara vez detiene la extorsión, solo demuestra que funciona y seguirán pidiendo más.
- Guarda todas las evidencias (capturas, números, perfiles) y denuncia ante la Policía Cibernética.
- Bloquea de inmediato a la persona en todas las redes y cambia configuraciones de privacidad para limitar quién puede ver tus contactos.
- Habla con alguien de confianza; el aislamiento es el mejor aliado del extorsionador.

---

## 4.4 Falso militar, médico o profesional "intachable"

**Qué es**

En esta variante emocional, el estafador se presenta como figura de prestigio y confianza: militar destacado en misión internacional, médico en zona de guerra, ingeniero petrolero en plataforma, piloto de aerolínea, etc. La narrativa: trabaja en un lugar aislado, cobra bien, pero tiene problemas de logística, permisos o aduanas para viajar o mover dinero. Pide que le "hagas el favor" de recibir paquetes, pagar supuestas tarifas o enviar dinero temporalmente. Combina romance scam con estafa logística y, a veces, con lavado.

**Señales de alerta**

- Historias muy dramáticas y peliculeras: misiones secretas, base militar donde "no hay bancos", hospitales de guerra, plataformas en altamar.
- Se justifica constantemente por no poder llamarte o verte: "seguridad nacional", "no tengo señal", "no puedo usar video".
- Pide que recibas paquetes, tarjetas o transferencias "a tu nombre" y luego se las envíes a un tercero.
- Te dice que no puede usar sus propias cuentas por razones "secretas" o restricciones de la misión.

**Cómo defenderte**

- Desconfía de narrativas demasiado cinematográficas; un profesional real puede verificar su identidad sin drama.
- Exige pruebas verificables: credenciales oficiales borrosas en foto no bastan, ni selfies con uniforme genérico.
- Nunca recibas paquetes, tarjetas o dinero de terceros para reenviarlos; eso te convierte en posible mula.
- Si se enfoca en pedir ayuda económica más que en construir relación real, es estafa.
- Corta el contacto, bloquea y reporta el perfil en la plataforma.

---

## 4.5 Carta nigeriana / Estafa 419 (versión emocional)

**Qué es**

La clásica "carta nigeriana" (estafa 419) empezó como correos donde un "príncipe" o funcionario extranjero ofrecía una fortuna a cambio de ayuda para liberar fondos; hoy se ha adaptado a redes y apps. Apela tanto a la codicia como a la empatía: herencias bloqueadas, viudas de guerra, refugiados con oro en el banco, premios de lotería internacionales. Te piden pagar "tasas legales", "impuestos" o "gastos de trámite" para recibir una suma gigantesca que nunca llega.

**Señales de alerta**

- Promesas de recibir millones de dólares por ser “la única persona confiable” que encontraron en internet.
- Historias rebuscadas con conflictos en países lejanos y nombres de instituciones internacionales metidos a fuerza.
- Documentos supuestamente oficiales con logos mal hechos, sellos raros o firmas escaneadas varias veces.
- Te piden aportaciones pequeñas primero, luego montos crecientes para “no perder lo ya invertido”.

**Cómo defenderte**

- Ten claro: no existen herencias, premios ni fondos millonarios que necesiten a un desconocido para ser liberados.
- No contestes correos ni mensajes que ofrezcan sumas gigantes a cambio de adelantos; bórralos y márcalos como spam.
- Si dudas, copia un párrafo del mensaje y pégalo en Google; muchas veces encontrarás la estafa reportada tal cual.
- No envíes documentos personales ni datos bancarios bajo ningún concepto.
- Si ya enviaste dinero, guarda evidencias y denuncia ante autoridades; sirve para inteligencia, aunque sea difícil recuperar fondos.

Cuando el fraude entra por el corazón, la lógica financiera llega tarde y en taxi. No se trata de dejar de confiar o de dejar de ligar, sino de entender que nadie que te quiere de verdad necesita tus claves, tus fotos íntimas ni tus datos de tarjeta “solo por esta vez”. Si una historia de amor te da más ansiedad financiera que paz emocional, no estás en una relación: estás en un funnel

# Capítulo 5 — Esquemas de inversión

Si hay algo que nunca pasa de moda es la promesa de “ganar más sin hacer casi nada”. Pirámides, Ponzis, “clubes de inversión”, trading mágico y proyectos cripto con nombre en inglés funcionan con la misma receta: adornar la codicia para que parezca visión financiera. Aquí vamos a ver cómo huele un rendimiento imposible, qué frases deberían prender todas tus alarmas y por qué el “es que todos mis amigos ya entraron” es la versión adulta de “todos en el salón lo hacen”


RENDIMIENTOS GARANTIZADOS & CÍA.
NO ES PIRÁMIDE, ES MODELO DE NEGOCIO DISRUPTIVO
18% MENSUALES
25% MENSUALES
40% MENSUALES
SALIDA TRASERA
FONDO DE RETIRO DE OTROS
SI SUENA DEMASIADO BUENO PARA SER VERDAD, PASE POR AQUÍ

# 5.1 Esquema Ponzi

### Qué es

El esquema Ponzi promete rendimientos altos y constantes, supuestamente gracias a una estrategia de inversión mágica: trading infalible, real estate VIP, arbitraje secreto, etc. En realidad no hay negocio sólido; los "rendimientos" que ves al inicio se pagan con el dinero de los nuevos inversionistas. Mientras sigue entrando gente, todos parecen ganar. Cuando se agota el flujo de víctimas, el esquema colapsa y el operador desaparece o admite "problemas de liquidez". El fraude vende esperanza, no resultados reales.

### Señales de alerta

- Rendimientos fijos y altos sin volatilidad ("3% mensual garantizado", "30% anual pase lo que pase").
- Explicaciones vagas del modelo ("arbitraje", "bots", "trading cuantitativo") sin estados financieros serios.
- Presión fuerte para "invitar amigos" y crecer la red; te pagan comisión por referidos.
- Dificultad creciente para retirar: primero pagan rápido, luego empiezan pretextos y retrasos.

### Cómo defenderte

- Desconfía de cualquier inversión que prometa rendimientos altos y estables sin mostrar riesgo ni volatilidad.
- Verifica si la empresa está regulada por CNBV, SEC u otro supervisor, y si tiene auditorías externas reales.
- Haz siempre un retiro de prueba pequeño antes de meter más dinero, y no reinviertas todo "para ganar más rápido".
- No pongas en un solo esquema más de lo que podrías permitirte perder sin quebrarte.
- Si detectas que algo es Ponzi, no "aguantes a ver si paga": sal lo antes posible y advierte a tu círculo.

---

# 5.2 Pirámides y multinivel fraudulento

### Qué es

Una pirámide se disfraza muchas veces de multinivel. La diferencia clave: en un multinivel legítimo, el ingreso principal viene de vender productos a clientes finales; en la pirámide, el dinero viene de reclutar gente nueva. Te cobran una inscripción, te entregan un "kit" de productos de valor dudoso y te prometen que ganarás

reclutando. Al saturarse la red, la base se queda con pérdidas. La estructura vive de la entrada de nuevos participantes, no de un negocio real.

**Señales de alerta**

- En las reuniones se habla más de cuánto ganarás reclutando que de las características del producto.
- Los "productos" son genéricos, caros y difíciles de colocar fuera de la propia red.
- Te presionan para inscribir a tu familia y amigos de inmediato para "no perder tu lugar en la estructura".
- No hay claridad sobre márgenes, costos y perfil del cliente final fuera del esquema.

**Cómo defenderte**

- Pregunta con frialdad: "¿De dónde viene el dinero?"; si la respuesta es "de la gente que entra", eso es pirámide.
- Analiza si el producto se vendería solo en el mercado abierto, sin el plan de compensación.
- Evita comprometer ahorros importantes en "paquetes de inventario" difíciles de revender.
- No arrastres a familia y amigos a un esquema que tú mismo no entiendes completamente.
- Si ves que la estructura está más preocupada por reclutar que por vender, aléjate.

---

# 5.3 Rug pull (cripto y tokens)

**Qué es**

El rug pull es el "quita la alfombra" del mundo cripto. Un equipo lanza un token o proyecto DeFi, arma ruido en redes, influencers lo promocionan y el precio sube. Cuando hay suficiente liquidez en el pool, los desarrolladores venden sus tokens, retiran la liquidez y desaparecen. El token se desploma casi a cero y los últimos en entrar se quedan con monedas sin valor. Muchas veces todo el "proyecto" eran solo imágenes bonitas y promesas vagas de metaversos y juegos.

**Señales de alerta**

- Equipo anónimo sin identidades verificadas, sin LinkedIn ni historial en otros proyectos.
- Contrato sin auditoría, sin código abierto revisable, o alojado en sitios dudosos.

- Liquidez desbloqueada: los dueños del contrato pueden retirar todo el pool cuando quieran.
- Mucho hype en redes, grupos de Telegram y YouTube, pero sin documentación técnica seria (whitepaper decente, roadmap creíble).

**Cómo defenderte**

- Verifica si la liquidez está bloqueada (locked liquidity) y por cuánto tiempo.
- Prefiere proyectos con equipos doxxed (identidad pública, historial verificable).
- Lee reseñas y análisis independientes, no solo el marketing del propio token.
- Nunca inviertas en un proyecto solo porque "sube mucho" o "lo mencionó X influencer".
- Limita tu exposición a microcap y memecoins; trátalos como apuestas, no como inversiones serias.

---

# 5.4 Trading falso y bots con "IA mágica"

**Qué es**

Aquí la promesa es que un "bot de trading con IA" operará por ti en Forex, cripto, índices o commodities, generando ganancias constantes. Las plataformas muestran dashboards muy bonitos con gráficas de supuestas ganancias diarias. Te dejan retirar pequeñas cantidades al principio, pero cuando aumentas tu inversión, empiezan los problemas: bloqueos de cuenta, verificaciones eternas, nuevos "impuestos" que debes pagar antes de poder retirar, hasta que finalmente cierran o desaparecen. Lo que hay detrás es un Ponzi con gorrito tecnológico.

**Señales de alerta**

- Rendimientos diarios o semanales muy altos y constantes, sin drawdowns, incluso en mercados muy volátiles.
- El bot es una caja negra: no puedes auditar la estrategia, ver órdenes reales ni el bróker regulado detrás.
- La plataforma no está registrada ni supervisada por ningún regulador financiero serio.
- Para retirar, de pronto te piden pagar impuestos por adelantado, comisiones raras o "upgrades de cuenta".

**Cómo defenderte**

- Verifica siempre si el bróker o la plataforma figuran en registros oficiales (CNBV, FCA, SEC, ESMA).

- Desconfía de cualquier cosa que ofrezca “0 pérdidas” o “ganancias diarias garantizadas”.
- Haz pruebas de retiro desde el inicio y mantén el monto que dejas dentro al mínimo posible.
- No confundas una interfaz bonita con regulación ni con solidez financiera.
- Si ya sospechas, prioriza retirar lo que puedas y no metas más dinero.

---

## 5.5 HYIP (High Yield Investment Programs) y “rendimientos garantizados”

**Qué es**

Los HYIP son programas de “alta rentabilidad” que prometen multiplicar tu dinero en poco tiempo: 20% mensual, 100% en 6 meses, 2% diario, etc. Muchos operan desde páginas web genéricas, con textos copiados y domicilios en paraísos fiscales. Exigen cripto o transferencias internacionales y se apoyan en sistemas de referidos. Algunos pagan al principio, pero los rendimientos son insostenibles y tarde o temprano dejan de pagar y desaparecen. Lo único garantizado es el riesgo.

**Señales de alerta**

- Promesas explícitas de rendimientos fijos muy elevados (“2% diario garantizado”, “triplica tu dinero en 90 días”).
- Empresas registradas en jurisdicciones opacas con capital ridículo y sin presencia física real.
- Todo el tráfico de captación viene de redes sociales y referidos, no de clientes institucionales.
- No existe un producto o servicio claro: solo “planes de inversión” con nombres bonitos (Silver, Gold, VIP).

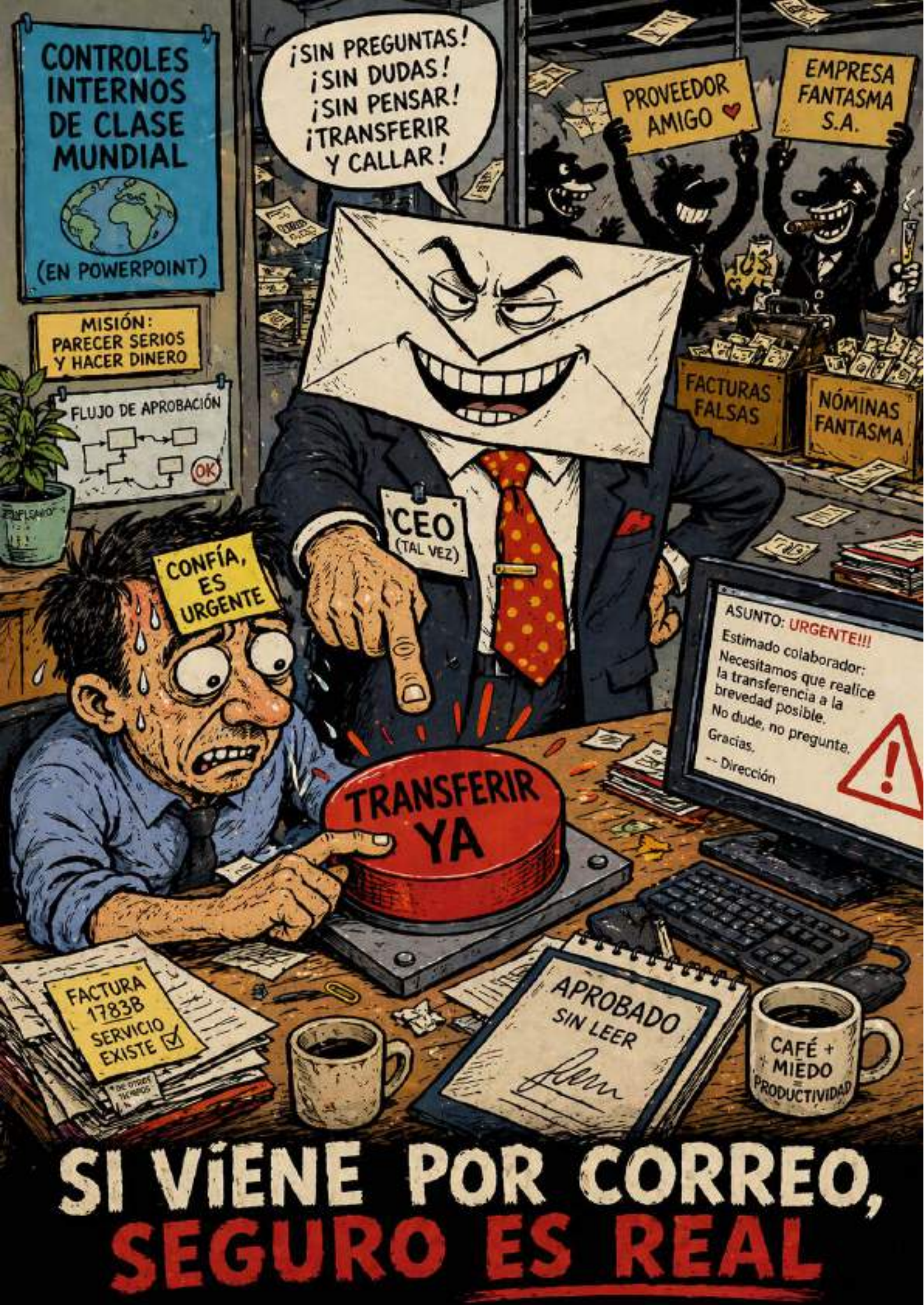
**Cómo defenderte**

- Ten como regla personal que cualquier rendimiento garantizado por encima de lo que paga un instrumento regulado debe tratarse con sospecha.
- Investiga el dominio, la empresa, los dueños y su historial; si no hay huella real, no inviertas.
- Si ya participas, evita reinvertir todo; recupera tu capital inicial lo antes posible.
- No recomiendes a otros algo que tú mismo no entiendes ni puedes explicar con claridad.
- Ante la duda, el “no invierto” siempre es más barato que el “ya me chingaron”.

Los números bonitos no son prueba de nada si nadie te explica de dónde salen sin usar la palabra “confía”. Cualquier inversión que dependa de que no hagas preguntas, de que metas a más gente o de que cierres “antes de que se acabe la oportunidad” es más religión que proyecto. Si no entiendes en qué se gana el dinero, asume que el modelo eres tú y tu rendimiento es lo que se lleva otro.

# Capítulo 6 — Fraudes corporativos

En teoría, la empresa es ese lugar donde todo está controlado, auditado y firmado por tres personas. En la práctica, también es el lugar donde un correo del “CEO”, una nómina inflada o un proveedor demasiado querido pueden sangrar más que cualquier ladrón externo. Aquí vamos a ver cómo se roba desde adentro con cara de proceso normal y por qué “confiar en la gente” no sustituye a revisar lo que hacen con el dinero.


CONTROLES INTERNOS DE CLASE MUNDIAL
(EN POWERPOINT)
MISIÓN: PARECER SERIOS Y HACER DINERO
FLUJO DE APROBACIÓN
OK
¡SIN PREGUNTAS! ¡SIN DUDAS! ¡SIN PENSAR! ¡TRANSFERIR Y CALLAR!
PROVEEDOR AMIGO
EMPRESA FANTASMA S.A.
FACTURAS FALSAS
NÓMINAS FANTASMA
CEO (TAL VEZ)
CONFÍA, ES URGENTE
ASUNTO: URGENTE!!!
Estimado colaborador:
Necesitamos que realice la transferencia a la brevedad posible.
No dude, no pregunte.
Gracias,
-- Dirección
TRANSFERIR YA
FACTURA 1783B SERVICIO EXISTE
APROBADO SIN LEER
CAFÉ + MIEDO = PRODUCTIVIDAD
SI VIENE POR CORREO, SEGURO ES REAL

# 6.1 BEC (Business Email Compromise)

### Qué es

El BEC es el fraude donde el delincuente se mete en el correo corporativo (o lo suplanta) y envía instrucciones falsas de pago haciéndose pasar por un directivo o proveedor. Puede leer correos reales por semanas para entender cómo se habla la empresa, qué montos maneja, quién autoriza qué. Un día manda un correo muy bien redactado: "Hola, por favor paga esta factura urgente al nuevo número de cuenta, el cliente está presionando". El área de finanzas obedece… y el dinero se va a la cuenta del estafador.

### Señales de alerta

- Correos "urgentes" de directivos pidiendo pagos fuera de proceso o a cuentas bancarias nuevas.
- Cambio de CLABE del proveedor sin aviso previo por canales formales (oficio, contrato, anexo).
- Correos con dominios muy parecidos al real (empresa-mx.com vs empresa.com.mx).
- Solicitud de mantener el pago "confidencial" o de no involucrar a otras áreas.

### Cómo defenderte

- Implementa la **regla del segundo canal** para pagos sensibles: si la instrucción llega por correo, se confirma por teléfono interno o Teams.
- Mantén una **lista blanca de cuentas bancarias** por proveedor; cualquier cambio requiere validación documental y aprobación de controles internos.
- Activa DMARC, DKIM y SPF en tu dominio para dificultar la suplantación de correos.
- Capacita a finanzas y tesorería en fraudes BEC, con ejemplos reales y simulacros.
- Ante un pago dudoso, bloquea y notifica de inmediato a tu banco para intentar recuperar vía SPEI.

---

# 6.2 EFOS y EDOS (facturación falsa)

### Qué es

En México, las EFOS son "Empresas que Facturan Operaciones Simuladas" y las EDOS son "Empresas que Deducen Operaciones Simuladas". En términos simples: unas venden facturas por servicios que no dieron, otras las compran para disminuir impuestos o justificar dinero de origen dudoso. Es un ecosistema de papel que sirve a evasión fiscal, corrupción y lavado. Cuando el SAT detecta un EFOS, publica la lista

de presuntos y definitivos (artículo 69-B) y quien se relacionó con ellos hereda el problema.

**Señales de alerta**

- Proveedores sin oficinas reales, sin personal ni equipo, pero con facturación muy alta.
- Servicios difíciles de probar ("asesorías", "consultoría integral", "servicios diversos") sin entregables claros.
- RFC del proveedor aparece en la lista 69-B del SAT como presunto o definitivo.
- Facturas con conceptos genéricos y montos perfectamente redondos.

**Cómo defenderte**

- Consulta periódicamente la lista 69-B del SAT para verificar a tus proveedores.
- Exige **materialidad**: contratos, entregables, reportes, evidencia de que el servicio sí se prestó.
- Implementa un proceso de alta de proveedores que incluya visita física o validación documental robusta.
- Si detectas relación con un EFOS, asesórate de inmediato con fiscalistas y corrige tu situación antes de que escale.
- No entres al "negocio" de las facturas: el ahorro fiscal fácil sale carísimo en multas, penal y reputación.

---

# 6.3 Nómina fantasma

**Qué es**

La nómina fantasma consiste en inflar la nómina con empleados que no existen o que ya no trabajan en la empresa, para desviar sus "sueldos" a cuentas de cómplices. También puede darse como horas extra inventadas, bonos duplicados, prestaciones que nadie recibe pero que sí se pagan. Muchas veces hay colusión entre Recursos Humanos, Nómina y alguien de Finanzas. El daño no solo es financiero, también fiscal y reputacional.

**Señales de alerta**

- Diferencias recurrentes entre el número de empleados que aparecen en sistema y los que realmente ves en piso.
- Transferencias de nómina a cuentas sin relación clara con los supuestos empleados.

- Empleados dados de alta en IMSS y SAT, pero sin registro en controles internos de acceso (relojes, credenciales).
- Quejas internas de personal por pagos raros, mientras la nómina global se mantiene "inflada".

**Cómo defenderte**

- Implementa control biométrico de asistencia y cruza datos con nómina e IMSS.
- Realiza auditorías periódicas de RH y nómina, incluyendo entrevistas y verificaciones en sitio.
- Separa funciones: quien captura nómina no autoriza pagos, y quien autoriza no captura.
- Usa reportes de excepción: nuevas altas, cambios de cuenta, bonos fuera de lo normal.
- Establece un canal de denuncia anónima donde la gente pueda reportar irregularidades sin miedo.

---

## 6.4 Deepfake del CEO y órdenes falsas

**Qué es**

Esta es la versión 2025 del BEC. El estafador ya no manda solo correos: usa **deepfake de voz o video** para hacerse pasar por el director general o un alto ejecutivo. Agenda una videollamada rápida o manda un audio por WhatsApp/Teams dando una instrucción urgente de pago o transferencia. La voz y la cara parecen reales; incluso pueden usar información interna para sonar creíbles. El objetivo es presionar a tesorería o a un CFO intermedio para que autorice un pago millonario "sin preguntar".

**Señales de alerta**

- Llamadas o mensajes en horarios raros (muy tarde, fin de semana) con instrucciones de pagos urgentes.
- El "CEO" insiste en que no se involucre a nadie más, "por sensibilidad del tema".
- Hay pequeñas rarezas en el lenguaje, expresiones que esa persona nunca usa o un ritmo de voz extraño.
- El pago va a un proveedor o cuenta que no te suena de nada, en el extranjero o a nombre de persona física.

**Cómo defenderte**

- No existe urgencia que justifique saltarse los controles de pago establecidos; esto debe ser cultura de la empresa.
- Define una **palabra o protocolo clave** para validar órdenes extraordinarias de directivos (no se escribe en ningún correo).
- Cualquier pago fuera de proceso requiere dos firmas y verificación por segundo canal (llamada a un número ya registrado, no al que venga en el mensaje).
- Capacita a directivos y tesorería en riesgos de deepfake, con ejemplos de casos reales.
- Si sospechas, detén el pago, documenta lo ocurrido y avisa al área de seguridad y cumplimiento.

---

## 6.5 Fraude de seguros y siniestros inflados

### Qué es

En el entorno corporativo, el fraude de seguros se da cuando se inventan siniestros, se exageran daños o se colude la empresa con proveedores (talleres, médicos, abogados) para cobrar más de lo debido. Por ejemplo, facturar rehabilitaciones que nunca se hicieron, piezas de autos que no se cambiaron o pérdidas de inventario infladas. También hay empleados que simulan accidentes laborales para activar pólizas.

### Señales de alerta

- Siniestros frecuentes o muy costosos respecto al tamaño y riesgo real de la empresa.
- Proveedores de servicios (talleres, clínicas) siempre son los mismos y tienen relación cercana con alguien interno.
- Inconsistencias entre el daño reportado y la evidencia fotográfica o pericial.
- Siniestros que siempre ocurren cerca de los cierres de trimestre o año.

### Cómo defenderte

- Establece relación con aseguradoras y ajustadores serios, con rotación de proveedores para evitar colusión.
- Pide evidencia sólida: fotos, reportes médicos, bitácoras, peritajes externos.
- Implementa auditorías aleatorias a siniestros pagados, con revisiones independientes.
- Cruza información con la aseguradora para detectar patrones anormales o repetitivos.
- Sanciona de manera ejemplar cuando se descubran fraudes internos; el mensaje disuasivo es clave.

## 6.6 Quiebra fraudulenta y maquillaje de estados financieros

### Qué es

La quiebra fraudulenta ocurre cuando los dueños o directivos vacían activos de la empresa a través de contratos simulados, ventas a empresas relacionadas o reestructuras sospechosas, para luego declarar que "no pueden pagar" a acreedores, proveedores o trabajadores. El maquillaje de estados financieros complementa esto: se inflan ingresos, se ocultan pasivos, se capitalizan gastos, se manipulan inventarios, todo para engañar a bancos, inversionistas y autoridades.

### Señales de alerta

- Ventas de activos clave a precios muy por debajo de mercado, sobre todo a partes relacionadas.
- Aparición repentina de deudas nuevas con empresas poco conocidas vinculadas a dueños o directivos.
- Cambios constantes de auditor externo, o auditorías "light" sin profundidad.
- Estados financieros demasiado "perfectos" y alejados de la realidad operativa que el personal percibe.

### Cómo defenderte

- Si eres proveedor o acreedor, revisa la salud financiera de tus clientes clave y no te expongas en exceso a uno solo.
- Para inversionistas, exige estados financieros auditados por firmas con reputación sólida y rotación periódica de socio auditor.
- Internamente, implementa un comité de auditoría y riesgos independiente del management operativo.
- Vigila operaciones con partes relacionadas y exige transparencia total en esas transacciones.
- Promueve canales de denuncia para que empleados puedan alertar sobre conductas sospechosas sin represalias.

El fraude interno no empieza el día que alguien roba, empieza el día que alguien descubre que puede hacerlo y no pasa nada. Procesos flojos, autorizaciones de

confianza y cultura de “aquí siempre se ha hecho así” son la mejor incubadora de creativos del desvío. Si tu empresa confía más en las personas que en los controles, quizá no tengas empleados deshonestos… todavía.

# Capítulo 7 — Colocación

El dinero sucio no llega al banco gritando “vengo del narco, ¿me abres una cuenta?”. Entra de puntitas: depósitos chiquitos, terceros “de confianza”, casinos, remesas y efectivo que se disfraza de venta legítima. Este capítulo es la entrada a la lavadora: cómo se rompe el dinero en pedacitos para que parezca normal y en qué momentos cualquier persona o negocio puede convertirse, sin querer, en parte de la tubería.

La colocación es la primera fase del lavado: el momento en que el dinero sucio toca por primera vez el sistema financiero formal. Aquí el objetivo del criminal es meter efectivo o valor ilícito en bancos, comercios, juegos, tarjetas, sin levantar demasiadas sospechas.

# NO SE PREOCUPE, AQUÍ TODO SE LAVA... MENOS LAS MANOS

# 7.1 Pitufeo (smurfing)

### Qué es

El pitufeo consiste en fragmentar grandes cantidades de efectivo en muchos depósitos pequeños, usando varias personas ("pitufos"), sucursales y cuentas. En lugar de llevar 1 millón en efectivo a una sola ventanilla, se reparte en decenas de depósitos de 10,000 o 20,000 pesos, a veces en bancos distintos, ciudades distintas o a nombre de terceros. La idea es permanecer por debajo de umbrales de reporte y camuflar el dinero entre operaciones normales del sistema.

### Señales de alerta (para sujetos obligados)

- Múltiples depósitos en efectivo, por montos similares, realizados el mismo día o en pocos días en distintas sucursales, a la misma cuenta o RFC.
- Personas que parecen recibir instrucciones por teléfono mientras depositan, o que no conocen bien al titular de la cuenta.
- Depósitos que no corresponden con el perfil económico declarado del cliente (ej. estudiante recibiendo cientos de miles en efectivo).
- Uso intensivo de ventanilla, pero poca o nula actividad comercial real detrás.

### Cómo defenderte

- Implementa monitoreo que consolide depósitos por cliente, CURP, RFC y cuentas relacionadas, no solo por operación individual.
- Define umbrales internos de análisis (más bajos que los legales) para detectar patrones repetitivos de depósito en efectivo.
- Capacita al personal de sucursales para identificar casos de pitufeo y generar Reportes de Operaciones Inusuales (ROIs) a la UIF.
- Para personas físicas y negocios, evita prestar tu cuenta para que "amigos" o "conocidos" depositen; puedes terminar como mula financiera.
- Documenta siempre origen de fondos cuando recibas cantidades significativas en efectivo.

---

# 7.2 Testaferros y prestanombres

### Qué es

El testaferro es la persona que presta su nombre para figurar como dueño de cuentas bancarias, autos, casas, empresas o inversiones, cuando en realidad el beneficiario real es otro. Se usan familiares, empleados de confianza, choferes, secretarias, incluso personas vulnerables que firman documentos sin entenderlos. El objetivo: desconectar jurídicamente al verdadero lavador de los bienes o flujos de dinero.

**Señales de alerta**

- Titulares con perfil económico modesto (salario bajo, sin historial) que aparecen como dueños de empresas grandes o propiedades de alto valor.
- Cuentas a nombre de terceros por donde pasan montos muy superiores a sus ingresos declarados.
- Personas que al ser entrevistadas no pueden explicar el origen de fondos ni la estructura de la empresa donde son "socios".
- Uso recurrente de familiares cercanos como socios o representantes legales de empresas sin sustancia real.

**Cómo defenderte**

- Como institución, aplica debida diligencia intensificada a clientes con estructuras donde el titular y el perfil económico no cuadran.
- Identifica siempre al **beneficiario final (UBO)**, no te quedes con el primer nombre que aparece en el contrato.
- Como persona, no prestes tu nombre ni tu firma para abrir cuentas, empresas o comprar bienes para otros, aunque sean familiares; puedes terminar vinculado a lavado.
- Documenta contratos reales, flujos y responsabilidades si participas en sociedad para evitar ser el "pato" sin saberlo.
- Ante presiones de jefes o terceros para figurar solo "de nombre", busca asesoría legal independiente.

---

## 7.3 Cuentas abiertas con documentos falsos o identidades sintéticas

**Qué es**

En esta tipología se usan documentos falsificados (INE alterada, comprobantes de domicilio apócrifos) o identidades sintéticas (combinar datos reales de varias personas para crear un "cliente" que no existe). Con esas identidades se abren cuentas bancarias, wallets, tarjetas y créditos que luego sirven para mover o colocar dinero ilícito. Como el titular "no existe" realmente, se complica vincular la operación con una persona física real.

**Señales de alerta**

- Documentos de identidad con microdetalles raros: impresión borrosa, laminado mal hecho, tipografía ligeramente distinta, errores mínimos.
- Datos que no cuadran entre sí (CURP incompatible con fecha de nacimiento, domicilio inexistente en mapas).

- Clientes que evitan activamente interacciones presenciales o biométricas, o se resisten a controles de prueba de vida.
- Múltiples cuentas abiertas con datos muy parecidos (mismo domicilio, teléfono, correo) pero nombres distintos.

**Cómo defenderte**

- Valida INE directamente contra bases oficiales cuando sea posible; usa lectores 2D y herramientas antifraude.
- Implementa biometría facial y dactilar con prueba de vida (movimientos, gestos) para evitar suplantaciones.
- Rechaza aperturas donde no se pueda verificar razonablemente la existencia real del cliente y su domicilio.
- Usa motores de vinculación que detecten cluster de datos (misma IP, mismo teléfono, mismo dispositivo) para encontrar identidades sintéticas.
- Como ciudadano, reporta robo o extravío de identificación inmediatamente y congela tu buró de crédito.

---

## 7.4 Negocios intensivos en efectivo

**Qué es**

Son negocios que, por su naturaleza, manejan mucho efectivo: bares, restaurantes, centros nocturnos, estacionamientos, car washes, tienditas, estéticas, etc. El lavador puede comprar o montar uno de estos negocios y mezclar el dinero sucio con las ventas legítimas. En papel, todo es "ingreso por servicios"; en la caja, parte del efectivo proviene de actividades ilícitas. Se inflan ventas sin que el volumen real de clientes lo justifique.

**Señales de alerta**

- Declaraciones de ingresos muy altas en negocios con poca afluencia real de clientes.
- Reportes de ventas que no se corresponden con consumos de insumos (agua, luz, materia prima).
- Alta rotación de socios, administradores o razón social, pero mismo local y operación.
- Pagos recurrentes en efectivo a proveedores y empleados por montos grandes.

**Cómo defenderte**

- Como institución, compara ingresos reportados con indicadores externos: consumo de servicios, ubicación, competencia en la zona.
- Realiza visitas in situ para ver el flujo real de clientes y la operación diaria.

- Usa análisis de riesgo sectorial para identificar giros con más probabilidad de ser usados para lavado.
- Como comerciante honesto, lleva contabilidad clara y bancos limpios; no aceptes “asociarte” solo para “dejar pasar efectivo” de terceros.
- Denuncia de forma anónima si detectas negocios notoriamente vacíos con flujos financieros desproporcionados.

---

## 7.5 Casinos y juegos de azar

**Qué es**

Los casinos, casas de apuestas, bingos y centros de juego son espacios clásicos de colocación. El lavador compra fichas o créditos con efectivo, juega lo mínimo necesario para justificar su presencia y luego pide retirar el dinero como “ganancias” mediante cheque, transferencia o efectivo registrado. En el papel, el flujo se ve como suerte en el juego; en la práctica, es lavado de efectivo. También se usan tickets de apuestas “ganadoras” negociados entre jugadores.

**Señales de alerta**

- Clientes que compran fichas con grandes cantidades de efectivo y casi no juegan.
- Solicitudes recurrentes de cheques o transferencias por “ganancias” sin historial consistente de juego.
- Compra-venta de tickets o fichas entre jugadores dentro o fuera del casino.
- Clientes que rehúsan identificarse o que intentan fragmentar compras para evitar controles.

**Cómo defenderte**

- Como casino, aplica estrictamente los controles de LFPIORPI: identificación de clientes a partir de ciertos montos y avisos a UIF.
- Monitorea la relación entre monto apostado y monto retirado; ganancias sin juego suficiente son banderas rojas.
- Realiza KYC de jugadores frecuentes y aplica debida diligencia reforzada a perfiles de alto riesgo.
- Como jugador, no prestes tu nombre ni tu membresía para que otros depositen o retiren por ti.
- Reporta internamente patrones sospechosos; la omisión también puede generar responsabilidad para el establecimiento.

---

## 7.6 Instrumentos monetarios y tarjetas prepagadas

### Qué es

Además del efectivo directo, los lavadores usan giros, órdenes de pago, tarjetas prepagadas, monederos electrónicos y cheques de viajero como escalón intermedio. Compran muchos instrumentos por montos relativamente bajos, en distintos puntos y con distintas personas, y luego los consolidan en cuentas bancarias o compras de bienes. A simple vista, parecen pequeños movimientos aislados; en conjunto, son colocación sistemática.

### Señales de alerta

- Compra masiva de tarjetas de regalo, monederos o prepagadas en efectivo, especialmente en cadenas de autoservicio.
- Giros y órdenes de pago repetidos por montos similares, enviados/recibidos por las mismas personas.
- Uso intensivo de monederos electrónicos sin relación clara con gasto o ingreso comercial real.
- Múltiples cargas y descargas en instrumentos prepagados que no corresponden a uso típico de consumidor.

### Cómo defenderte

- Como emisor o comercio, establece límites razonables a la compra de tarjetas y monederos en efectivo, y registra operaciones inusuales.
- Integra información de tus distintos puntos de venta para identificar patrones de compras repetitivas.
- Aplica KYC proporcional cuando el cliente use instrumentos por encima de cierto monto acumulado.
- Como persona, evita prestar tu nombre para recibir giros o recargar monederos “para un amigo que no tiene identificación”.
- Documenta siempre el origen de fondos si manejas montos relevantes a través de estos instrumentos.

La colocación no es magia negra, es rutina disfrazada de normalidad: depósitos pequeños, terceros útiles, efectivo que se “formaliza”. El truco está en que nadie haga demasiadas preguntas sobre el origen mientras el dinero se vista de ventas, premios o servicios vagos. Cada vez que aceptas efectivo raro “porque necesito la venta”, una parte de tu negocio se está alquilando como lavadora.

# Capítulo 8 — Estratificación

Aquí el juego se vuelve de magos contables: empresas fantasma, facturación creativa, comercio internacional demasiado complicado para preguntar mucho. El objetivo ya no es solo meter el dinero al sistema, sino marear a cualquiera que intente seguirlo. En este capítulo vamos a recorrer el laberinto de sociedades, contratos y operaciones raras que sirven para que, cuando alguien pregunte “¿de dónde salió esto?”, la respuesta más honesta sea: “ya se nos perdió en la vuelta tres”

La estratificación es la segunda fase del lavado: cuando el dinero ya entró al sistema y ahora hay que perderlo en la estructura. Aquí el lavador mueve fondos entre empresas, países, productos financieros y cripto para que el rastro se vuelva un laberinto.


MIENTRAS MÁS VUELTAS DA EL DINERO,
MÁS MAREADO QUEDA EL REGULADOR
EMPRESA X
100% LEGAL (CREEMOS)
CONSULTORA Y
EXPERIENCIA INEXPLICABLE
COMERCIALIZADORA Z
¡TODO EN ORDEN!
HOLDING GLOBAL
PROPÓSITO: ¿?
FIDEICOMISO
MUY PARTICULAR
FUNDACIÓN ALGO
SIN FINES (DE LUCRO)
SERVICIOS INTEGRALES A.C.
ACTIVIDADES: VARIAS
LOGÍSTICA INFINITA
DOMICILIO: EN TODAS PARTES Y EN NINGUNA
PATRIMONIO AUTÓNOMO
ADMINISTRADOR: ¿QUIÉN?
GRUPO INNOMBRABLE S.A.
PROPIETARIO: CONFIDENCIAL
IMPORTADORA EXPORTADORA DEL SUR
ORIGEN: DUDOSO
DESTINO: MISTERIOSO
DESARROLLOS DEL MAÑANA S. DE R.L.
HOY NO, MAÑANA SÍ
UF...
UFF...
DEBIDA DILIGENCIA
MAQUILADORA DEL TAL VEZ
HECHO EN: ¿QUIÉN SABE? ¿A QUIÉN LE IMPORTA?
OFICINA VIRTUAL 24/7
AQUÍ NO HAY NADA QUE VER

# 8.1 Empresas fantasma y sociedades de papel

### Qué es

Las empresas fantasma son sociedades que existen en el papel (RFC, acta constitutiva, cuenta bancaria), pero no tienen operación real: no tienen oficinas, empleados ni actividad económica legítima. Sirven para emitir facturas simuladas, recibir transferencias, triangular pagos y justificar flujos de dinero ilícito como si fueran ventas o servicios. Pueden ser "fachada" para EFOS, para corrupción, para sobornos o para mover recursos de delincuencia organizada.

### Señales de alerta

- Domicilio fiscal que resulta ser una casa abandonada, una oficina virtual o un local donde nadie conoce a la empresa.
- Sin personal, sin maquinaria, sin evidencia de actividad real; pero con facturación millonaria.
- Giro extremadamente genérico: "servicios integrales", "consultoría empresarial", "soluciones globales".
- Alta rotación de socios y representantes legales, o uso de personas de escasos recursos como accionistas.

### Cómo defenderte

- Como empresa, haz **due diligence** de proveedores: visita física, fotos, entrevista, referencias con otros clientes.
- Cruza información con el SAT, Registro Público de Comercio y listas negras (69-B, OFAC, listas internas).
- No contrates proveedores que no puedan demostrar sustancia: contratos, entregables, personal, activos.
- Como institución financiera, aplica debida diligencia reforzada a empresas jóvenes con facturación desproporcionada.
- Si detectas que un proveedor es fantasma, corta relación, regulariza tu situación fiscal y reporta a la autoridad.

---

# 8.2 TBML (Trade-Based Money Laundering)

### Qué es

El TBML es el lavado basado en comercio exterior. En lugar de mover bolsas de efectivo, se mueven contenedores, facturas y aduanas. El mecanismo clásico: sobrefacturar (declarar precio mucho mayor al real) para sacar valor de un país, o subfacturar (declarar menos valor) para meterlo. También hay sobre/infra

declaración de cantidades, calidad o tipo de mercancía. El contenedor se vuelve excusa para justificar flujos enormes entre empresas vinculadas en distintos países.

**Señales de alerta**

- Precios declarados muy por encima o por debajo del valor de mercado internacional para esa mercancía.
- Empresas recién creadas que de pronto manejan volúmenes grandes de importación/exportación.
- Operaciones trianguladas por países de riesgo o paraísos fiscales que no tienen lógica comercial.
- Discrepancias entre el volumen físico y lo declarado (contenedores medio vacíos, pesos que no cuadran).

**Cómo defenderte**

- Usa bases de datos de precios de referencia (aduanas, organismos internacionales) para validar operaciones.
- Revisa la cadena: quién es el proveedor real, quién es el distribuidor, quién paga, quién recibe.
- Implementa análisis de riesgo específico para comercio exterior en bancos, agentes aduanales y empresas.
- Capacita a áreas de logística, compras y finanzas para identificar patrones inusuales en operaciones de comercio.
- Documenta exhaustivamente contratos, órdenes de compra, embarques, pólizas y pagos correspondientes.

---

## 8.3 Offshore, trusts y jurisdicciones opacas

**Qué es**

La estructura "offshore" consiste en usar sociedades, trusts o fundaciones en jurisdicciones de baja tributación y alta opacidad (BVI, Panamá, Belice, ciertas islas) para mover y esconder capital. En sí, tener una empresa offshore no es delito; el problema es cuando se usan estas estructuras para ocultar beneficiarios finales, pagar menos impuestos de forma ilegal o lavar sobornos y dinero criminal. La estratificación se logra conectando múltiples capas legales en diferentes países.

**Señales de alerta**

- Clientes o contrapartes que insisten en usar sociedades en jurisdicciones con fuerte secreto financiero sin justificación de negocio.
- Cadenas de propietarios donde siempre que preguntas "¿y detrás de esa empresa quién está?" aparece otra empresa, nunca una persona.

- Flujos importantes hacia o desde países en listas de riesgo GAFI sin sustancia económica visible.
- Trusts o fundaciones "de familia" creados a la medida, con cláusulas confusas sobre los beneficiarios.

**Cómo defenderte**

- Identifica siempre al **beneficiario final persona física (UBO)**, aunque haya diez capas intermedias.
- Aplica debida diligencia reforzada a clientes y operaciones con jurisdicciones de alto riesgo o baja transparencia.
- Exige documentación clara sobre actividad real, origen de fondos y razones de negocio para la estructura.
- Como profesional (abogado, notario, contador), no prestes tus servicios para estructuras que solo sirven para ocultar.
- Si no puedes identificar a los beneficiarios o el propósito económico, considera no iniciar la relación.

---

## 8.4 Crypto mixers, tumblers y servicios de mezcla

**Qué es**

Los mixers o tumblers de cripto son servicios que reciben criptomonedas de muchos usuarios y las "revuelven" en un gran pool, enviando de vuelta fondos mezclados. El objetivo es romper la trazabilidad en la cadena de bloques, de modo que no se pueda seguir fácilmente el rastro desde la wallet de origen hasta la de destino. Se han usado para lavar fondos de hacks, ransomware, estafas y mercados de dark web. Algunos han sido sancionados por autoridades internacionales.

**Señales de alerta**

- Fondos que llegan a un exchange habiendo pasado por direcciones vinculadas a mixers conocidos o sancionados.
- Clientes que insisten en usar servicios de mezcla en lugar de rutas directas, sin explicación razonable de privacidad.
- Patrones de muchas transacciones pequeñas hacia servicios de mezcla, seguidas de salidas a wallets nuevas.
- Operaciones en cripto vinculadas a mercados ilegales según herramientas de análisis on-chain.

**Cómo defenderte**

- Como exchange o institución, usa herramientas de análisis de blockchain para evaluar el "riesgo de procedencia" de los fondos.

- Bloquea o somete a revisión reforzada los depósitos provenientes de mixers sancionados o de alto riesgo.
- Implementa políticas claras sobre uso de monedas enfocadas en privacidad (Monero, Zcash) y servicios de mezcla.
- Como usuario, evita interactuar con mixers si no puedes justificar ante un regulador por qué lo hiciste.
- Reporta operaciones inusuales a la UIF cuando la trazabilidad on-chain apunte a delitos claros.

---

# 8.5 Chain-hopping y DeFi hopping

**Qué es**

El chain-hopping es el salto entre diferentes blockchains para complicar el seguimiento: el lavador pasa de Bitcoin a Ethereum, luego a una sidechain, luego a Monero, luego a otra red, usando puentes, swaps y protocolos DeFi. Cada salto agrega ruido al análisis; si además combina mixers, DEX sin KYC y monedas de privacidad, la estratificación se vuelve un laberinto técnico.

**Señales de alerta**

- Clientes que convierten fondos varias veces seguidas entre distintas criptos y redes sin una lógica de inversión clara.
- Uso intensivo de puentes (bridges) y DEX poco conocidos, especialmente en jurisdicciones de alto riesgo.
- Fondos que acaban en monedas centradas en privacidad antes de intentar volver a fiat.
- Patrones de transacciones fragmentadas (muchos montos pequeños) en cadenas diferentes, con tiempos coordinados.

**Cómo defenderte**

- Implementa monitoreo on-chain que abarque múltiples redes (no solo Bitcoin y Ethereum).
- Considera de alto riesgo la conversión repetitiva sin propósito claro de inversión o gestión de tesorería.
- Aplica EDD (debida diligencia reforzada) a clientes que operan intensamente con puentes y DEX sin KYC.
- Coordina la información entre tu rampa fiat (banco/exchange) y tus sistemas de análisis cripto para ver la película completa.
- Documenta claramente las justificaciones de clientes institucionales que hagan gestión activa multichain.

---

# 8.6 Hawala, hundi, fei-chien y sistemas informales de transferencia

### Qué es

La hawala (y sus equivalentes hundi, fei-chien, etc.) es un sistema informal de transferencia de valor basado en confianza comunitaria. No mueve físicamente el dinero entre países; lo hace a través de una red de "hawaladars" que compensan saldos entre sí. Un migrante entrega efectivo a un corredor en un país y un familiar recibe el equivalente en otro, sin que pase por bancos ni sistemas formales. Aunque se usa también para remesas legítimas, su opacidad la vuelve atractiva para lavado.

### Señales de alerta

- Clientes con flujos transfronterizos significativos que declaran usar "amigos" o "contactos" para mover dinero sin bancos.
- Negocios pequeños (tiendas, locutorios) que manejan grandes montos de efectivo vinculados a comunidades migrantes.
- Operaciones frecuentes en efectivo, sin documentación, con múltiples países involucrados.
- Patrón de entradas y salidas en cuentas de personas vinculadas a redes étnicas específicas, sin lógica comercial.

### Cómo defenderte

- Como país e institución, entiende que la hawala existe; reprimirla sin alternativas formales solo empuja más opacidad.
- Aplica enfoque basado en riesgo: analiza giros, montos y jurisdicciones de los negocios que pudieran operar como corredores informales.
- Fomenta remesadoras reguladas y canales formales accesibles en costo para competir con sistemas informales.
- Como individuo, evita encargar grandes montos a redes informales; si algo sale mal, no hay protección.
- Si identificas actividad claramente vinculada a delitos, reporta a UIF y, en su caso, a autoridades penales.

La estratificación vive de dos cosas: estructuras complejas y gente que se rinde antes de entenderlas. Sociedades, facturas, contratos y operaciones circulares se diseñan para que te dé pena admitir "no entiendo nada" y firmes de todos modos. Si un esquema requiere más empresas de las que puedes dibujar en una servilleta, tal vez no estás ante un negocio sofisticado, sino ante un truco viejo con traje caro

# Capítulo 9 — Integración

Después de tantas vueltas, el dinero quiere jubilarse como ciudadano respetable: en forma de casa, rancho, restaurante, obras de arte o negocio de toda la vida. Esta es la fase donde el efectivo sospechoso se convierte en patrimonio que nadie se atreve a cuestionar porque “ha trabajado mucho”. Aquí vamos a ver cómo luce esa transformación mágica y qué señales te dicen que detrás de cierto lujo hay más lavadora que mérito.

La integración es la tercera fase del lavado: cuando el dinero que ya fue colocado y estratificado regresa a la economía formal con apariencia de origen legítimo. Aquí el criminal quiere que el dinero sucio se vea como renta, ganancias, herencias, premios, préstamos pagados o plusvalía de activos.

# DEL EFECTIVO SOSPECHOSO AL PATRIMONIO RESPETABLE EN POCOS PASOS

## 9.1 Inmuebles y desarrollos inmobiliarios

**Qué es**

El inmobiliario es el clásico lavadero elegante: casas, departamentos, terrenos, locales comerciales, bodegas. El lavador compra inmuebles con dinero ilícito (directo o vía empresas y testaferros), a veces a precio inflado o subvaluado según convenga. Luego los renta, los vende o los usa como colateral para créditos bancarios. Lo que entra al sistema como "renta" o "precio de venta" parece un ingreso normal, aunque la compra original se hizo con recursos de procedencia ilícita.

**Señales de alerta**

- Compradores que pagan de contado montos altos, sin crédito hipotecario, y con perfil económico que no justifica el flujo.
- Operaciones frecuentes entre las mismas partes, con precios poco alineados al mercado.
- Uso de múltiples sociedades para comprar y vender inmueble entre sí, elevando el precio cada vez.
- Pagos significativos en efectivo en operaciones donde la ley ya limita el uso de efectivo.

**Cómo defenderte**

- Como notario, agente o desarrollador, aplica controles de PLD: identifica UBO, origen de fondos y perfil del cliente.
- Documenta tasaciones reales y compara precios de venta con valor de mercado.
- Respeta los límites legales de uso de efectivo en operaciones de inmuebles que marca LFPIORPI.
- Rechaza operaciones donde el cliente no pueda demostrar razonablemente origen lícito de recursos.
- Reporta operaciones inusuales a la UIF cuando la estructura o los montos no cuadren con el perfil del cliente.

---

## 9.2 Bienes de lujo: autos, yates, joyería, relojes, arte

**Qué es**

Los bienes de lujo son otra forma clásica de integración. El lavador compra autos de alta gama, motos, yates, relojes finos, joyas, arte, vino, etc., muchas veces a nombre de empresas o terceros. Posteriormente los vende, los hipoteca o los usa como

herramienta de status. El mensaje contable: “es patrimonio legítimo”. En algunos casos, se sobre/factura el bien para inflar patrimonio, o se simulan alquileres y eventos.

**Señales de alerta**

- Clientes que compran bienes de alto valor de contado o con estructuras de pago inusuales.
- Compra de múltiples vehículos de lujo a nombre de una misma persona o empresa sin actividad aparente.
- Pagos fragmentados en efectivo y transferencias, con poca claridad del origen.
- Clientes renuentes a entregar datos KYC o a que se registre su identidad en operaciones de alto precio.

**Cómo defenderte**

- Comercios de autos, joyería, relojes, arte y demás deben cumplir LFPIORPI como actividades vulnerables (avisos, identificación, umbrales).
- No aceptes operaciones grandes en efectivo; su preferencia por efectivo ya es una bandera.
- Documenta identificaciones, datos de contacto y origen de fondos según los umbrales aplicables.
- Revisa a clientes de riesgo (PEP, sectores sensibles) con debida diligencia reforzada.
- Si eres comprador honesto, exige facturas claras y no prestes tu nombre para comprar bienes para terceros.

---

## 9.3 Préstamos saldados en efectivo y back-to-back

**Qué es**

El lavador puede simular préstamos para blanquear dinero. Un ejemplo: crea una empresa en el extranjero que “le presta” dinero a su empresa local. Luego “paga” ese préstamo con recursos ilícitos; en los libros contables, todo se ve como devolución de un crédito legítimo. Otro esquema es el back-to-back: deja dinero en un banco (a veces offshore) como colateral y el banco le presta a una empresa relacionada en otro país. El origen se diluye entre tratados y papeles.

**Señales de alerta**

- Préstamos entre partes relacionadas sin lógica de negocio clara, con tasas y plazos fuera de mercado.
- Empresas sin historial de actividad que de pronto otorgan créditos grandes a otras entidades del mismo grupo.

- Pagos de préstamos en efectivo o con flujos que no corresponden con capacidad real del deudor.
- Contratos de préstamo muy genéricos, sin garantías claras ni calendario serio de pagos.

**Cómo defenderte**

- Como banco, analiza operaciones de crédito intragrupo como posibles vehículos de lavado, no solo como riesgo crediticio.
- Exige documentación sólida del origen de los fondos prestados y del propósito económico.
- Como empresario, no aceptes "préstamos" de entidades dudosas sin transparencia total; puedes salir embarrado.
- Documenta correctamente préstamos entre socios, con tasas y plazos razonables, y registra los flujos bancarios que los soportan.
- Ante estructuras raras, aplica debida diligencia reforzada y considera reportar operación inusual.

---

## 9.4 Franquicias y negocios "legítimos"

**Qué es**

La compra de franquicias y negocios con marca conocida es una forma muy efectiva de integración. El lavador adquiere un restaurante, farmacia, gasolinera, franquicia de comida rápida o minimarket. Inyecta efectivo ilícito como "ventas" que luego salen como utilidades, nómina, proveedores o dividendos. Como el negocio tiene marca y manuales, la apariencia de legitimidad es fuerte. A veces incluso operan con ventas reales, solo que mezcladas con dinero sucio.

**Señales de alerta**

- Nuevos franquiciatarios con poca experiencia en el giro pero alta capacidad de inyección de efectivo.
- Ingresos declarados por encima del promedio de la red, sin explicación por ubicación o estrategia.
- Estructuras societarias complejas detrás de un franquiciado aparentemente pequeño.
- Uso intensivo de efectivo para pagos internos cuando el sector ya opera mayoritariamente con medios electrónicos.

**Cómo defenderte**

- Como franquiciante, realiza due diligence de tus franquiciatarios: UBO, origen de fondos, historial empresarial.

- Compara sus ventas y márgenes con el resto de la red; investiga desviaciones extremas.
- Establece políticas claras de manejo de efectivo y conciliación diaria con sistemas POS.
- Como institución financiera, revisa patrones de depósitos e ingresos de negocios franquiciados contra benchmarks del sector.
- Si eres empresario honesto, evita aceptar "socios capitalistas" que solo quieren "meter efectivo" sin involucrarse en la operación.

---

## 9.5 Deportes, arte, subastas y entretenimiento

### Qué es

Sectores con valores subjetivos son perfectos para integrar dinero: fútbol, box, conciertos, producción audiovisual, arte, subastas. Se puede inflar el valor de un cuadro, de un jugador, de un contrato de artista, de una gira, y justificar pagos exagerados que en realidad son sobornos, retornos de inversión criminal o capital lavado. En deportes, los derechos de imagen, fichajes y traspasos dan margen amplio a estos juegos de valor.

### Señales de alerta

- Precios de transferencia de jugadores, obras de arte u objetos muy alejados del histórico o de la lógica de mercado.
- Pagos a empresas intermediarias "de marketing" o "gestión de derechos" en jurisdicciones opacas.
- Subastas donde los pujadores se conocen entre sí o pertenecen al mismo grupo económico.
- Contratos de entretenimiento inflados para justificar pagos a terceros sin sustancia.

### Cómo defenderte

- En casas de subasta y galerías, identifica UBO de clientes y registra procedencia de obras y trazabilidad.
- En clubes deportivos, documenta claramente contratos, representantes, derechos de imagen y montos, y somételos a revisión externa.
- Aplica controles PLD en pagos a empresas de marketing, derechos y representación, especialmente en paraísos fiscales.
- Como artista o deportista, cuida quién estructura tus contratos; puedes ser usado como pantalla sin saberlo.
- Reporta operaciones que no se expliquen por criterios deportivos o artísticos, sino solo por montos.

## 9.6 Ganancias de casino, lotería y premios ficticios

### Qué es

Otra forma de integración es simular "suerte". El lavador puede comprar boletos de lotería premiados a terceros, pagarles un extra y luego cobrar él el premio "legal", o puede coludirse con personal interno corrupto en casinos y sorteos para generar constancias de premios que no ocurrieron. Así, el dinero ilícito se viste de "ganancia de juego" o "premio de sorteo", difícil de cuestionar fiscalmente si el papel parece en regla.

### Señales de alerta

- Personas que declaran ingresos importantes supuestamente por "ganar seguido" en lotería, quinielas, apuestas.
- Ganadores frecuentes que siempre aparecen en la misma casa de apuestas, sorteo o casino.
- Operaciones de compra-venta de boletos premiados entre particulares.
- Personal o empresas que gestionan sorteos internos sin controles, auditoría ni transparencia.

### Cómo defenderte

- Como operador de lotería o casino, implementa controles de PLD, auditorías y sistemas que registren realmente quién gana qué.
- Limita pagos grandes en efectivo por premios; fomenta pagos bancarizados con KYC completo.
- Audita periódicamente el sistema de sorteos, premios y la integridad del software.
- Como ciudadano, no te prestes a vender o comprar boletos premiados de terceros; eso te vincula con tramos de lavado.
- Recuerda que declarar "ganancias de juego" para justificar flujos puede llamar la atención si el patrón es reiterado.

En la integración, el lavado deja de verse como crimen y empieza a parecer éxito. Casas, negocios, autos y coleccionables se convierten en monumentos a la frase "ha trabajado mucho", aunque nadie sepa exactamente en qué. No se trata de sospechar de todo el que prospera, pero sí de recordar que no todo patrimonio respetable tiene una historia respetable detrás.

# Capítulo 10 — Tipologías sectoriales avanzadas GAFI/GAFILAT

Ningún gran esquema de lavado o fraude camina solo; siempre hay alguien que firma, sella, constituye, certifica o "no vio nada". Abogados, notarios, contadores, fintechs, funcionarios, ONGs y empresas "respetables" pueden ser pared o pueden ser túnel, según qué tan barato vendan sus principios. En este capítulo vamos a hablar de esos jugadores incómodos que prefieren llamarse "asesores" o "facilitadores", pero que, sin ellos, muchas historias jamás habrían salido del PowerPoint

Aquí entran los gatekeepers: abogados, notarios, contadores, fintech, ONGs, e-commerce, greenwashing y tokenización que, bien o mal usados, pueden volver el lavado algo sistémico.

# EL JUEGO NO ES LEGAL, PERO SÍ ESTRATÉGICO


# CUANDO TODOS SON PIEZA CLAVE, NADIE SE SIENTE RESPONSABLE

## 10.1 Gatekeepers legales: abogados, notarios y contadores

### Qué es

Los gatekeepers son los profesionales que, con su firma, su fe pública o su estructura, abren la puerta del sistema: crean empresas, redactan fideicomisos, diseñan estructuras fiscales, autorizan escrituras. Cuando actúan de buena fe, son defensa. Cuando se venden, se vuelven cómplices perfectos: montan sociedades pantalla, blindan testaferratos, diseñan caminos para que el dinero sucio llegue "limpio" a un banco o a un edificio corporativo. A veces participan conscientemente; otras, miran hacia otro lado.

### Señales de alerta

- Estructuras corporativas muy complejas donde el abogado o notario repite una y otra vez como representante de muchas empresas sin relación obvia.
- Despachos que ofrecen abiertamente "optimización fiscal agresiva" basada en offshores sin sustancia.
- Notarías con volumen inusual de operaciones de alto riesgo (inmuebles de lujo, fideicomisos opacos, PEPs) sin reportes de PLD visibles.
- Contadores que insisten en usar proveedores o esquemas "de confianza" para bajar impuestos, sin transparencia.

### Cómo defenderte

- Como cliente, pide explicaciones claras y por escrito de cualquier estructura; si no la entiendes, sospecha.
- Como profesional, establece filtros para aceptar clientes: KYC, UBO, origen de fondos, enfoque basado en riesgo.
- Incorpora programas de cumplimiento PLD internos: manuales, oficial responsable, capacitación anual.
- Rechaza encargos donde la única finalidad sea ocultar al verdadero dueño o mover dinero sin transparencia.
- Coopera con UIF, SAT y colegios profesionales cuando detectes esquemas claramente ilícitos.

---

## 10.2 Fintech, monederos electrónicos y neobancos

### Qué es

Las fintech y monederos electrónicos democratizan el acceso financiero… y también la velocidad del lavado si no tienen buenos controles. Cuentas que se abren en

minutos desde el celular, tarjetas virtuales, wallets con IBAN extranjero, remesas instantáneas. Los lavadores buscan plataformas con KYC laxo, cuentas por niveles fáciles de multiplicar y monitoreo transaccional débil. La estratificación se logra moviendo dinero entre decenas de cuentas fintech antes de tocar la banca tradicional.

**Señales de alerta**

- Mismo dispositivo (misma huella digital) abriendo muchas cuentas con identidades distintas.
- Clientes con múltiples cuentas "nivel básico" que todas reciben y envían montos cercanos al límite.
- Flujos muy altos para el tipo de producto (cuenta "de uso personal" que parece tesorería de empresa).
- Depósitos frecuentes desde comercios físicos de recarga, dispersados en múltiples wallets.

**Cómo defenderte**

- Implementa KYC proporcional pero real desde el nivel 1: no bases todo en selfies y correo electrónico.
- Usa detección de dispositivos, IPs y patrones para identificar multicuentas y redes de mulas.
- Aplica límites razonables, pero sobre todo un **monitoreo inteligente** (no solo topes duros).
- Integra señales externas: listas de sanciones, PEP, reportes de fraude, comportamiento inusual.
- Como usuario, no prestes tu cuenta fintech "porque es más fácil que el banco"; te conviertes en vehículo de lavado.

---

## 10.3 Corrupción y PEPs (Personas Expuestas Políticamente)

**Qué es**

La corrupción es la gasolina premium del lavado en muchos países. Un funcionario (PEP) o su círculo cercano recibe sobornos, comisiones ilegales, contratos inflados. Esos recursos deben ser lavados: contratos simulados, empresas fachada, triangulaciones vía despachos o consultorías, fundaciones, offshores. El sistema se vuelve **sistémico** cuando bancos, notarios, despachos, partidos y empresas privadas se acostumbran a tratar esos flujos como "parte del juego".

**Señales de alerta**

- PEPs (o familiares) con incremento patrimonial desproporcionado a su salario público.
- Contratos gubernamentales repetidos a empresas con poca experiencia y vínculos con funcionarios.
- Pagos de consultoría, asesoría o "intermediación" a empresas sin personal ni sustancia real.
- Uso intensivo de efectivo, bienes de lujo y offshores por parte de círculos cercanos al poder.

**Cómo defenderte**

- Como institución financiera, aplica debida diligencia reforzada a PEPs, sus familiares y estrechos colaboradores.
- Monitorea incrementos patrimoniales, flujos con contratistas de gobierno y operaciones con sectores de riesgo.
- No "normalices" prácticas de corrupción; documenta, eleva a cumplimiento y, si corresponde, reporta a UIF.
- Como empresa, establece políticas anticorrupción claras (ISO 37001, códigos de ética, canales de denuncia).
- Como ciudadano, apoya transparencia: declara, documenta, vota informado y respalda medios que investigan.

---

# 10.4 ONGs, fundaciones y asociaciones fachada

**Qué es**

Las organizaciones sin fines de lucro son esenciales… y también un vehículo cómodo para lavar cuando se pervierten. Una ONG fachada puede recibir donativos nacionales o extranjeros, públicos o privados, y simular proyectos sociales, culturales o religiosos que nunca se ejecutan. El dinero se redistribuye a empresas y personas vinculadas. También se usan para canalizar fondos de corrupción o financiamiento político ilegal disfrazado de filantropía.

**Señales de alerta**

- ONGs con pocos proyectos visibles pero grandes montos de donativos en papel.
- Plantillas mínimas, sin personal técnico, pero con gastos administrativos muy altos.
- Donantes recurrentes vinculados a empresas contratistas de gobierno o a PEPs.
- Proyectos en zonas remotas difíciles de verificar, sin reportes ni evidencias públicas.

**Cómo defenderte**

- Como donante, verifica el registro de la ONG ante el SAT (donataria autorizada) y revisa sus informes anuales.
- Pide transparencia: reportes financieros, proyectos ejecutados, fotos, testimonios.
- Como banco, clasifica a ONGs como clientes de riesgo especial y aplica EDD donde corresponda.
- No uses ONGs para mover recursos entre empresas del mismo grupo; eso ya huele a abuso.
- Si trabajas en una ONG real, documenta exhaustivamente para poder demostrar que no eres fachada.

---

## 10.5 E-commerce ficticio y plataformas de marketplace

**Qué es**

Más allá de las tiendas clonadas al consumidor, existe el **e-commerce ficticio** corporativo. Empresas crean tiendas online B2B o B2C donde simulan ventas masivas de productos que nunca entregan o sobrevaloran. En contabilidad, todo entra como "ingresos por ventas en línea"; en realidad, son flujos de efectivo mezclado que se deposita vía SPEI, agregadores de pago, PSPs o plataformas de marketplace. El lavado se disfraza de economía digital.

**Señales de alerta**

- Tiendas con tráfico web muy bajo pero con volúmenes de cobro altos en la pasarela de pagos.
- Patrones de compra extraños: muchos tickets de alto valor desde pocos usuarios o IPs.
- Ratio de devoluciones y reclamos inusualmente bajo para el volumen reportado (puede indicar que no hay clientes reales).

- Empresas que usan marketplaces B2B para facturar entre sí servicios o productos genéricos.

**Cómo defenderte**

- Como PSP, pasarela o banco adquirente, monitorea comportamiento transaccional vs. tráfico y reseñas del comercio.
- Solicita evidencias de entregas, logística, inventario y clientes cuando veas volúmenes sospechosos.
- Clasifica comercios de alto riesgo (giros, países, patrones) y aplica controles extra.
- Como empresa, no aceptes usar tu e-commerce como "puente" para cobrar a terceros; te vuelves parte del esquema.
- Reporta operaciones inusuales a UIF cuando el patrón digital no tenga lógica comercial.

---

## 10.6 Lavado verde, créditos de carbono y tokenización ESG

**Qué es**

El lavado verde es el uso de discursos y productos "sustentables" para lavar reputación… y dinero. Bonos verdes, créditos de carbono, proyectos de reforestación, energía limpia, tokens ESG: todos pueden ser legítimos o puro humo. Un esquema clásico: inflar el valor de créditos de carbono de proyectos que no existen o están inflados, venderlos a empresas que quieren "compensar" emisiones, y ahí esconder flujos ilícitos disfrazados de inversión ambiental.

**Señales de alerta**

- Proyectos verdes en países lejanos o zonas remotas, difíciles de verificar físicamente.
- Certificaciones dudosas, emitidas por entidades sin reconocimiento internacional.
- Valores de créditos de carbono o tokens verdes muy por encima del mercado, sin explicación técnica.
- Empaques financieros complejos donde nadie sabe exactamente qué proyecto se está financiando.

**Cómo defenderte**

- Verifica estándares y certificadoras (Verra, Gold Standard u otras reconocidas según el mercado).

- Exige información detallada del proyecto: ubicación, mediciones, reportes, terceros verificadores.
- Evita comprar productos “verdes” solo por marketing; revisa documentación técnica y financiera.
- Como institución, trata estos instrumentos como productos de alto riesgo PLD hasta que se demuestre lo contrario.
- No uses proyectos verdes solo como fachada para mover dinero entre jurisdicciones; el greenwashing ya es riesgo regulatorio serio.

Sin quien constituya, asesore, certifique o “no vea”, muchos esquemas nunca pasarían de idea en servilleta. Los llamados gatekeepers pueden ser la primera línea de defensa o la puerta giratoria por donde entra y sale todo. Cada vez que un profesional decide mirar hacia otro lado “porque no es mi responsabilidad”, un delincuente agrega un eslabón más a su cadena de lavado.

# Capítulo 11 — Fraudes con IA

La inteligencia artificial no inventó el fraude, solo le dio esteroides. Donde antes tenías correos mal escritos y fotos borrosas, ahora tienes voces clonadas, videos “en vivo” que nunca existieron y documentos que parecen más reales que los originales. En este capítulo vamos a ver cómo la IA se volvió el mejor becario de la estafa y qué puedes hacer cuando ya no basta con decir “yo confío porque lo vi y lo escuché”

La IA no inventó el fraude, solo lo hizo más convincente: voces clonadas, caras que no existen, correos perfectos, identidades sintéticas y chatbots que parecen soporte oficial.


# SI LA IA SUENA MÁS REAL QUE TU BANCO, SOSPECHA

## 11.1 Deepfake de voz

**Qué es**

Con unos cuantos segundos de audio robados de redes sociales, entrevistas o notas de voz, hoy se puede clonar la voz de casi cualquiera. El deepfake de voz se usa para llamar a familiares, empleados o ejecutivos y pedir transferencias, códigos o información sensible. El timbre, las muletillas, incluso el acento suenan iguales. La víctima escucha la "voz" de su hijo, de su jefe, de su socio, y baja la guardia. Es el viejo fraude telefónico con esteroides digitales.

**Señales de alerta**

- Llamadas "de emergencia" donde la persona habla poco, rápido, y se enfoca en pedir dinero o códigos.
- Frases repetitivas o respuestas poco naturales cuando le haces preguntas abiertas.
- La llamada llega desde números desconocidos o internacionales, no desde el número habitual de la persona.
- Insisten en que no cortes la llamada y que no valides por otro canal.

**Cómo defenderte**

- Establece **palabras clave** familiares o corporativas que deban usarse en emergencias y que no estén escritas en ningún lado.
- Si algo suena raro, cuelga y vuelve a marcar tú al número oficial o conocido de la persona.
- No compartas códigos de verificación, token o datos bancarios por teléfono, aunque la voz suene familiar.
- En empresas, capacita a finanzas y tesorería sobre este riesgo y refuerza la regla del segundo canal.
- Si sospechas, graba la llamada (si la ley local lo permite) y repórtala a la Policía Cibernética.

---

## 11.2 Deepfake en videollamada (Zoom/Teams)

**Qué es**

El deepfake en video ya no es ciencia ficción. Hay casos documentados donde un CFO asistió a una videollamada con varios "directivos", todos deepfakes, y terminó autorizando transferencias millonarias. El fraude usa una cara sintética o clonada superpuesta en tiempo real sobre un cuerpo, con movimientos apenas suficientes para parecer natural. En llamadas de baja calidad, el engaño se vuelve aún más creíble. La autoridad visual de ver a tu "CEO" en pantalla pesa mucho.

**Señales de alerta**

- Video borroso o con baja resolución "porque la conexión está mala" cuando se trata de una llamada crítica.
- El interlocutor evita movimientos amplios: la cabeza casi no gira, los gestos son mínimos y repetitivos.
- No acepta que haya más personas en la llamada o que se comparta pantalla desde su lado.
- La conversación se dirige rápido a "firma", "código", "autorización de pago" sin contexto habitual.

**Cómo defenderte**

- En decisiones críticas (pagos grandes, cambios de cuenta), la videollamada **no sustituye** la verificación por segundo canal.
- Pide microacciones difíciles de simular: que gire la cabeza 90°, que acerque un objeto, que escriba en tiempo real algo específico en cámara.
- Verifica después por teléfono o mensaje directo en un canal ya establecido con esa persona.
- En procesos de alto monto, exige autorizaciones digitales firmadas (firma electrónica, sistemas internos) además de la llamada.
- Capacita a equipos en ejemplos de deepfake y establece protocolos escritos para no improvisar bajo presión.

---

# 11.3 Phishing potenciado por LLM (IA generativa)

**Qué es**

Antes, el phishing se reconocía por la ortografía espantosa y el "hola querido cliente". Ahora, con modelos de lenguaje, los estafadores generan correos y mensajes impecables, personalizados con información que sacan de LinkedIn, redes sociales y filtraciones de datos. Pueden escribirte como si fueran tu banco, tu área de TI, tu jefe o un proveedor, con tono, vocabulario y contexto creíbles. No solo imitan logos, también imitan cómo escribes y cómo te hablan.

**Señales de alerta**

- Correos extremadamente bien redactados que sin embargo piden acciones inusuales (instalar software, desactivar antivirus, compartir credenciales).
- Mensajes que incluyen detalles personales o laborales (tu puesto, tu jefe, proyectos) para parecer legítimos.
- Formularios o portales que lucen idénticos a los reales, pero alojados en dominios distintos.

- Chatbots en webs sospechosas que “te ayudan” a recuperar cuentas pidiéndote datos sensibles.

**Cómo defenderte**

- Mantén la regla de siempre: jamás introducir credenciales en sitios a los que llegaste por un enlace de correo o mensaje.
- Usa gestores de contraseñas: si el gestor no completa automáticamente el usuario/contraseña, probablemente no es el sitio real.
- Desconfía de instrucciones “de TI” que vengan por correo sin previo aviso y validación interna.
- Usa soluciones de seguridad que analicen links y adjuntos antes de abrirlos.
- Capacita a equipos con simulacros de phishing moderno, no solo los viejos correos mal escritos.

---

## 11.4 Identidades sintéticas generadas con IA

**Qué es**

La identidad sintética es la creación de una “persona” que no existe, combinando datos reales (CURP, fecha de nacimiento, dirección) con datos inventados, fotos generadas por IA y perfiles sociales falsos. Esta identidad puede abrir cuentas, pedir créditos, rentar servicios y dejar deudas que “nadie” paga. A diferencia del robo de identidad clásico, aquí no hay una víctima clara; el deudor nunca existió, pero el fraude sí.

**Señales de alerta**

- Clientes nuevos con historiales de crédito muy breves pero perfectos, que crecen rápido para luego caer en bust-out.
- Documentos que, al verificarse, tienen componentes válidos pero otros que no cuadran (CURP válido pero dirección inexistente).
- Fotos de identificación que parecen “demasiado perfectas” o con rasgos genéricos de cara IA (orejas raras, fondo excesivamente limpio).
- Perfiles en redes con pocas interacciones reales y posts genéricos, pero con foto “profesional” de IA.

**Cómo defenderte**

- Usa validación documental cruzada con fuentes oficiales y biometría con prueba de vida (no solo selfie estática).
- Implementa modelos de riesgo de identidad sintética que analicen velocidad de apertura, comportamiento de crédito y patrones de uso.

- Verifica direcciones físicas y teléfonos de manera aleatoria en onboarding de mayor riesgo.
- Como ciudadano, protege tus datos: evita publicar en abierto CURP, RFC, domicilios detallados, credenciales, etc.
- Activa alertas de crédito y revisa tu buró periódicamente para detectar aperturas que no reconozcas.

---

## 11.5 Chatbots maliciosos y soporte "IA" falso

**Qué es**

Los estafadores montan páginas o apps con chatbots que simulan ser soporte de bancos, wallets, exchanges, tiendas, gobierno. El chatbot conversa contigo en lenguaje natural, parece muy servicial, pero su objetivo es guiarte a entregar datos sensibles ("para ayudarte debo validar tu usuario", "escribe tu NIP para verificar"). A veces se integran en sitios clonados; otras, en apps que se hacen pasar por oficiales en tiendas no oficiales.

**Señales de alerta**

- Chatbots que de inmediato piden datos de acceso completo, NIP, CVV o códigos de verificación.
- Sitios donde el único canal de contacto es el chat, sin teléfono oficial ni correo corporativo verificable.
- Diferencias sutiles de diseño entre la página "oficial" y la que estás usando (colores, tipografía, logotipos).
- Apps de "soporte bancario" fuera de las tiendas oficiales o con desarrollador desconocido.

**Cómo defenderte**

- Nunca ingreses NIP, CVV, seed phrase o códigos de token en un chat, aunque parezca de tu banco.
- Usa únicamente apps oficiales descargadas desde las tiendas oficiales y validadas por el propio banco en su web.
- Verifica la URL del sitio antes de interactuar con cualquier chatbot "oficial".
- Ante dudas, corta chat y comunícate por los canales que ya tenías: teléfono de la tarjeta, app oficial, sucursal.
- Reporta páginas y apps falsas para que sean dadas de baja; ayudas a reducir el ataque para otros.

---

## 11.6 Generación masiva de documentos y pruebas falsas

### Qué es

La IA generativa permite crear facturas, estados de cuenta, contratos, comprobantes de depósito, capturas de pantalla y hasta fotos de "oficinas" y "equipos de trabajo" en segundos. Los defraudadores usan esto para "probar" que tienen ingresos, proyectos, inversiones, garantías, cuando todo es un decorado digital. Bancos, inversionistas ángel, plataformas de lending y hasta potenciales socios pueden caer si no verifican por canales independientes.

### Señales de alerta

- Documentos perfectos visualmente pero con pequeños detalles raros: fuentes ligeramente distintas, logos desproporcionados, datos de contacto que no existen.
- Estados de cuenta o contratos que no coinciden con la información obtenida directamente de la institución supuestamente emisora.
- Fotos de "oficinas" y "equipos" que parecen sacadas de banco de imágenes (gente demasiado diversa y feliz, sin rasgos locales).
- Inversores o empresas que se resisten a que hables directamente con sus "clientes" o "socios" para referencias.

### Cómo defenderte

- Verifica documentos directamente con la fuente: bancos, SAT, notarías, proveedores, no solo con quien te los entrega.
- Implementa controles de lectura automática de documentos (OCR) con reglas de validación cruzada de datos.
- Pide evidencias independientes: referencias de clientes, visitas físicas, llamadas a instituciones mencionadas.
- Para inversiones o créditos grandes, realiza due diligence con terceros especializados.
- Mantén una sana paranoia: un PDF bonito no equivale a realidad contable ni legal.

La IA no volvió tontos a los usuarios, volvió más creíbles a los mentirosos. Ya no basta con "yo lo vi" o "yo lo escuché" para dar algo por cierto; toca volver a lo básico: contexto, verificación y duda razonable. Si una voz, un video o un documento parecen perfectos, la pregunta ya no es "¿por qué confiar?", sino "¿por qué no verificar dos veces?"

# Capítulo 12 — Amenazas técnicas avanzadas

Mientras tú aprendías a usar la app del banco, el fraude se volvió industria multinacional con indicadores, metas y soporte 24/7. Call centers, mafias digitales, grupos mixtos de hackers y delincuencia tradicional trabajan en red mejor que muchas empresas legales. Aquí vamos a hacer un recorrido rápido por lo que pasó en estos diez años: cómo se profesionalizó el engaño, qué cambió con los pagos instantáneos y por qué América Latina está lejos de ser solo "víctima"

Aquí no te roban con pasamontañas, sino con código, Wi-Fi y descuidos digitales. El objetivo sigue siendo el mismo: tomar control de tus cuentas, tus dispositivos y tus decisiones.


EL FRAUDE YA ES GLOBALIZADO;
LA PROTECCIÓN SIGUE EN TRÁMITE
NO ES MI PROBLEMA
NO ES MI PROBLEMA
NO ES MI PROBLEMA
RANSOMWARE DE CONFIANZA
DATOS ROBADOS
PHISHING PREMIUM
CREDENCIALES VIP
CALLER ID FALSOTE
TUS DATOS
MALWARE DELUXE
ARCHIVOS TOP SECRET
INGENIERÍA SOCIAL EXPRESS
TU DINERO
FUGA DE DATOS S.A.
INFORMACIÓN SENSIBLE
NO ES MI PROBLEMA
NO ES MI PROBLEMA
NO ES MI PROBLEMA
COMITÉ DE CIBERSEGURIDAD (REUNIÓN EN 2026)
NORMATIVA EN CONSULTA

## 12.1 Secuestro de WhatsApp

### Qué es

El secuestro de WhatsApp ocurre cuando alguien toma control de tu cuenta en la app usando el código de verificación que te llega por SMS. El guion típico: te llaman diciendo que se equivocaron de número, que te llegará un código por mensaje y que "se lo reenvíes por favor". Ese código, en realidad, es el que WhatsApp usa para activar tu cuenta en otro teléfono. Una vez que lo entregas, te sacan, entran ellos, y desde tu identidad escriben a tus contactos para pedir dinero o datos.

### Señales de alerta

- Te llega un SMS con un código de WhatsApp que tú no pediste, seguido de una llamada o mensaje pidiéndote ese código.
- WhatsApp se cierra de repente en tu teléfono y aparece mensaje de "tu cuenta se está usando en otro dispositivo".
- Amigos o familia te dicen que les estás pidiendo dinero o códigos… y tú no has mandado nada.

### Cómo defenderte

- Nunca compartas códigos de verificación que te lleguen por SMS, ni aunque te los pida "un amigo" o "soporte técnico".
- Activa la **verificación en dos pasos** de WhatsApp: un PIN adicional que bloquea la activación en otro equipo.
- Si te sacan, intenta recuperar de inmediato tu cuenta con tu número y PIN; cuanto más tardes, más daño harán a tus contactos.
- Avísale a tu círculo por otros canales (llamada, SMS) si crees que alguien está usando tu cuenta para estafar.
- Reporta la suplantación en la propia app y, si hay fraude, a la Policía Cibernética.

---

## 12.2 Caller ID spoofing

### Qué es

El caller ID spoofing es la manipulación del número que ves en tu pantalla cuando te llaman. El estafador hace que tu celular muestre el número del banco, de la policía, del SAT o de cualquier institución, aunque la llamada venga de otro lado. Esto se combina con vishing: la voz suena profesional, el número se ve "real" y tú bajas la guardia. No es magia: son servicios de telefonía IP mal usados.

### Señales de alerta

- Llamadas supuestamente del banco que, aun mostrando el número correcto, te piden NIP, token o CVV.
- Llamadas de “autoridades” que amenazan con detenerte o embargarte si no haces pagos inmediatos.
- Te presionan a decidir en la llamada y no te permiten colgar para validar tú por tu cuenta.

**Cómo defenderte**

- No confíes ciegamente en el número que ves en pantalla: los números también se falsifican.
- Cuelga y marca tú al número oficial del banco o institución desde tu app, tarjeta o página web.
- Jamás des datos sensibles por teléfono aunque la llamada “parezca” del número oficial.
- Guarda el número desde el que te llamaron y repórtalo a Condusef y a la Policía Cibernética.
- Capacita a tu familia para que no se dejen intimidar por amenazas telefónicas.

---

## 12.3 MITM en Wi-Fi público (Man in the Middle)

**Qué es**

El ataque Man in the Middle en Wi-Fi público ocurre cuando un atacante se coloca entre tu dispositivo y el router de la red abierta (cafés, aeropuertos, hoteles). Puede crear una red falsa con nombre similar (“CafeGratis”, “Aeropuerto Free”) o comprometer la real. Todo lo que pasa sin cifrado adecuado puede ser interceptado: sesiones web, cookies, credenciales, tráfico de apps mal diseñadas. Tú crees que estás navegando normal; alguien está mirando por encima de tu hombro digital.

**Señales de alerta**

- Muchas redes abiertas con nombres casi iguales (Starbucks-Free, StarbucksFree, Free-WiFi-Starbucks).
- Avisos de certificado inseguro o errores raros de HTTPS al entrar a sitios que normalmente funcionan bien.
- Red muy lenta o inestable cuando haces cosas sensibles (banca, correo, compras).

**Cómo defenderte**

- Evita hacer operaciones sensibles (banca, compras, acceso a sistemas corporativos) en Wi-Fi público.
- Usa siempre una **VPN** confiable cuando te conectes a redes abiertas.

- Verifica el nombre exacto de la red con el personal del lugar antes de conectarte.
- Prioriza usar tu plan de datos móvil para temas bancarios o de trabajo.
- Presta atención a alertas de seguridad del navegador; no ignores advertencias de certificado.

---

## 12.4 Ransomware de doble extorsión

**Qué es**

El ransomware ya no solo cifra tus archivos y pide rescate para devolverte el acceso. En la variante de doble extorsión, los atacantes además exfiltran tus datos antes de cifrarlos y amenazan con publicarlos si no pagas. Así, aunque tengas respaldos, te chantajean por la filtración: datos de clientes, contratos, información personal, propiedad intelectual. Afecta a PYMEs, grandes empresas, hospitales, gobiernos, despachos, cualquiera con datos valiosos.

**Señales de alerta**

- Equipos que de pronto se vuelven lentos, archivos que no abren, extensiones raras agregadas a los nombres.
- Pantalla de rescate con instrucciones de pago en cripto, muchas veces con reloj de cuenta regresiva.
- Correos o notas donde los atacantes demuestran que descargaron una muestra de tus datos sensibles.

**Cómo defenderte**

- Ten respaldos **3-2-1**: tres copias, en dos medios distintos, una offline y desconectada.
- Mantén sistemas, aplicaciones y antivirus actualizados; muchos ataques aprovechan vulnerabilidades conocidas.
- Limita privilegios de usuarios: que nadie tenga más permisos de los necesarios.
- Ten un plan de respuesta a incidentes probado; saber qué hacer reduce el caos cuando pase.
- No asumas que pagar te salvará: muchas bandas no respetan su “palabra”. Consulta siempre con expertos y autoridades.

---

## 12.5 Supply chain attacks (ataques a la cadena de suministro digital)

### Qué es

En los ataques a la cadena de suministro, los delincuentes no te atacan directamente a ti, sino a un proveedor de software o servicio que tú usas. Comprometen una actualización, un plugin, una biblioteca de código, un proveedor de TI gestionada. Cuando ese proveedor te envía una "actualización" legítima, viene envenenada. Es lo que pasó con casos como SolarWinds: una puerta trasera distribuida a miles de clientes.

### Señales de alerta

- Compromisos simultáneos en varias empresas que usan el mismo proveedor de software o servicios.
- Componentes de software en tus sistemas que se actualizan desde servidores o canales no verificados.
- Eventos de seguridad que empiezan poco después de una actualización masiva.

### Cómo defenderte

- Lleva un inventario (SBOM, Software Bill of Materials) de los componentes de software que usas.
- Solo permite actualizaciones desde canales verificados y con firma digital válida.
- Segmenta tu red: que el compromiso de un proveedor no implique acceso inmediato a todo.
- Evalúa el riesgo de tus proveedores críticos: seguridad, procesos, antecedentes de incidentes.
- Prepara cláusulas de seguridad en tus contratos con proveedores de TI y software.

---

## 12.6 Cookies maliciosas y robo de sesión

### Qué es

No siempre te roban la contraseña; a veces te roban la **sesión**. El robo de cookies o tokens de sesión permite que el atacante se haga pasar por ti sin necesidad de conocer tu clave. Puede ocurrir vía malware, exploits del navegador, sitios maliciosos o ataques en redes Wi-Fi. Una vez que tienen la cookie, pueden acceder a tu correo, redes sociales, herramientas de trabajo o banca web hasta que cierres sesión o expire el token.

### Señales de alerta

- Accesos desde dispositivos o ubicaciones desconocidas sin que te hayan "adivinado" la contraseña.
- Notificaciones de inicio de sesión en sitios donde tú ya estabas logueado.
- Actividad rara en tus cuentas a pesar de que tu contraseña no cambió.

**Cómo defenderte**

- Cierra sesión en servicios sensibles cuando termines, sobre todo en equipos compartidos o públicos.
- Usa navegadores y sistemas actualizados, con extensiones mínimas y confiables.
- No instales software pirata ni extensiones dudosas; son canales clásicos de malware.
- Activa alertas de inicio de sesión y revisa regularmente qué dispositivos tienen sesión activa.
- Para cuentas críticas, usa llaves de seguridad físicas FIDO2 cuando sea posible.

---

## 12.7 Phishing laboral (HR phishing y payroll phishing)

**Qué es**

El phishing laboral apunta a empleados usando temas de Recursos Humanos: nómina, prestaciones, evaluaciones, beneficios, vacaciones. Un correo parece venir de RH o de la dirección y te pide que "actualices tus datos bancarios", que firmes un nuevo contrato o que bajes un archivo con "políticas actualizadas". En realidad, te llevan a sitios falsos para robar credenciales o a documentos con malware. También hay payroll phishing, donde se convence a RH de cambiar tu CLABE para que la quincena vaya a otro lado.

**Señales de alerta**

- Correos de "Recursos Humanos" que llegan desde dominios ajenos a la empresa o variantes sospechosas.
- Formularios externos (Google Forms, sitios raros) pidiendo datos sensibles de nómina o credenciales corporativas.
- Solicitudes de cambio de cuenta bancaria que llegan por correo simple, sin el procedimiento usual.

**Cómo defenderte**

- Establece canales claros y únicos para trámites de RH (portal interno, app) y comunícalo a todo el personal.

- Capacita a empleados para que desconfíen de correos sobre nómina que pidan acciones fuera de lo normal.
- Implementa procedimientos de verificación para cambios de cuenta de pago (segundo canal, documentación física).
- Filtra y bloquea correos externos que usen nombres internos de áreas (HR, Payroll, etc.).
- Documenta incidentes y haz retroalimentación interna cada vez que se detecta un intento.

El fraude dejó de ser un cuate con teléfono y se convirtió en una industria con procesos. Mientras sigamos pensando en el estafador como “el tipo de la llamada rara” y no como parte de un ecosistema global, vamos a seguir peleando con resortera contra drones. Entender el panorama no es para asustarse más, es para dejar de subestimar al rival.

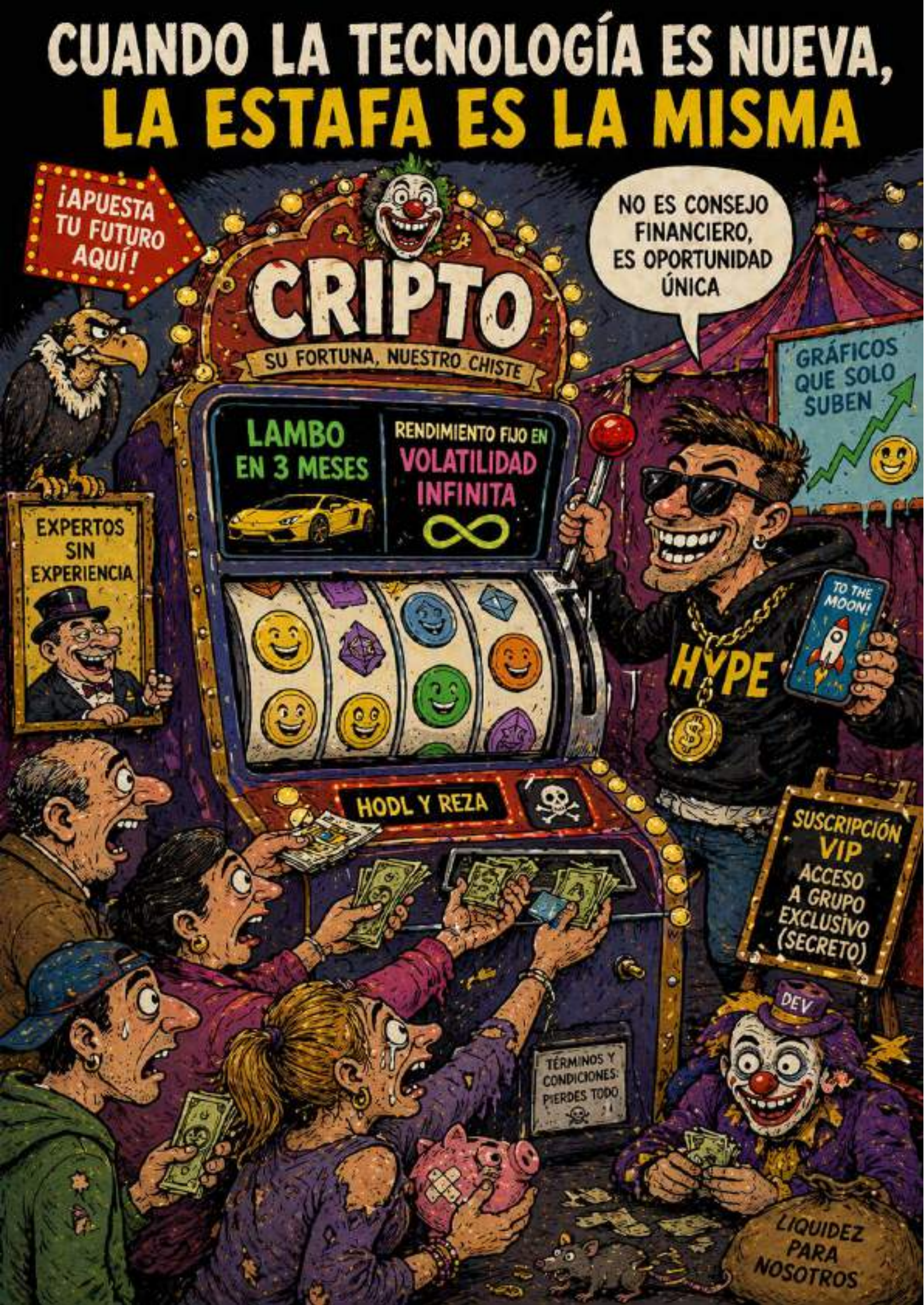
---

# Capítulo 13 — Fraudes emergentes cripto / Web3

Cripto no es sinónimo de fraude, pero el fraude sí se enamoró rápido de cripto. Tokens basura, exchanges fantasma, proyectos "revolucionarios" sin más sustancia que un whitepaper inflado y un influencer con lentes oscuros forman parte del paisaje. En este capítulo vamos a separar tecnología de cuento chino y revisar qué señales te dicen que no estás invirtiendo en el futuro de las finanzas, sino en la jubilación anticipada de alguien más.

Aquí el fraude mezcla romance, trading y FOMO: tokens, DEX, airdrops, wallets conectadas "solo para probar". La frase más cara de Web3 es "solo firmé una vez".

# CUANDO LA TECNOLOGÍA ES NUEVA, LA ESTAFA ES LA MISMA



# 13.1 Pig butchering (engorda del cerdo)

### Qué es

El pig butchering combina romance scam con estafa de inversión cripto. El esquema suele empezar con un mensaje "equivocado" en WhatsApp, Telegram o redes ("Hola, ¿Juan?"). Aunque le digas que no eres Juan, te sigue la conversación, se vuelve amable, comparte su "rutina de inversiones", te muestra pantallazos de supuestas ganancias y, poco a poco, te lleva a una plataforma de trading o cripto que en realidad controlan ellos. Primero te dejan ganar y retirar poco; luego te animan a meter más, y cuando el "cerdo" está bien engordado, bloquean retiros y desaparecen.

### Señales de alerta

- Mensajes de desconocidos que insisten en seguir la conversación aunque ya aclaraste que no eres la persona buscada.
- Personas que muy pronto te hablan de sus "inversiones exitosas" y de lo fácil que es ganar con su método.
- Plataformas de trading a las que solo se accede con link privado, sin regulación ni presencia pública real.
- Puedes retirar cantidades pequeñas al inicio, pero cuando intentas retirar montos grandes empiezan trabas y "impuestos".

### Cómo defenderte

- No mantengas conversaciones largas con contactos desconocidos que insisten en "hacerse amigos" y hablar de dinero.
- Desconfía de cualquier "mentor" que conociste por error en WhatsApp y quiere llevarte a una plataforma fuera de exchanges conocidos.
- Verifica siempre si la plataforma está registrada o supervisada por algún regulador y si otros usuarios la reconocen.
- Nunca metas más dinero del que estarías dispuesto a perder en un casino, y desconfía si te dicen que "no saques nada todavía".
- Si detectas que es un esquema pig butchering, corta contacto y reporta perfiles, números y sitio a autoridades y plataformas.

---

# 13.2 Airdrops envenenados y tokens basura

### Qué es

En Web3, un airdrop es el envío "gratis" de tokens a tu wallet. El fraude: te aparece un token extraño con un valor aparente alto en tu cartera. Cuando intentas venderlo o interactuar con él en la DEX sugerida, firmas una transacción que da permisos amplios al contrato del estafador. Esa firma permite que después drene todos tus

activos. Otras veces, los airdrops son solo para llevarte a sitios maliciosos o estafas de soporte falso.

**Señales de alerta**

- Tokens desconocidos que aparecen en tu wallet sin que tú hayas hecho nada para obtenerlos.
- Sitios o DEX que te dicen que solo ahí puedes vender ese token "raro" y que debes conectar tu wallet.
- Transacciones que, al revisarlas, muestran permisos amplios para mover todos tus tokens, no solo el que quieres vender.

**Cómo defenderte**

- Ignora y oculta tokens no solicitados en tu interfaz; no intentes venderlos ni moverlos.
- Antes de firmar cualquier transacción, revisa qué permisos estás otorgando; si la app no lo muestra claro, no firmes.
- Usa herramientas como Revoke.cash o similares para revisar y revocar permisos otorgados a contratos que no reconoces.
- Mantén una wallet "fría" o hardware wallet para ahorros y otra "caliente" de prueba para interactuar con cosas nuevas.
- No sigas links a DEX desconocidas solo porque alguien en redes te dijo que ahí se vende tal token misterioso.

---

# 13.3 Wallet drainers (drainers scripts)

**Qué es**

Los drainers son scripts o contratos diseñados para **vaciar tu wallet** cuando firmas una transacción tóxica. Se camuflan detrás de supuestos mints de NFT, claims de recompensas, acceso a whitelist, staking, etc. El sitio se ve profesional, parece parte de un proyecto de moda. Te pide conectar la wallet y aprobar una transacción "para autorizar el mint" o "para reclamar el beneficio". En realidad, estás dando permiso para mover o gastar todos tus tokens en nombre del atacante.

**Señales de alerta**

- Páginas que insisten en que conectes tu wallet antes de mostrar información relevante.
- Transacciones con textos genéricos como "SetApprovalForAll" o similares, sin explicación clara de qué moverán.

- Proyectos que solo existen en Twitter/Telegram y en esa web, sin código abierto ni comunidad sólida.
- Falsos sitios de proyectos populares; la URL casi igual pero no idéntica a la oficial.

**Cómo defenderte**

- No conectes tu wallet a cualquier sitio que veas en Twitter o grupos sin antes verificar que es la página oficial del proyecto.
- Usa extensiones o herramientas que avisans de contratos conocidos como drainers o de transacciones sospechosas.
- Lee cuidadosamente el contenido de las transacciones en tu wallet antes de firmar; si no entiendes, cancela.
- Mantén la mayor parte de tus fondos en una hardware wallet y solo cantidades pequeñas en la hot wallet para experimentar.
- Si ya firmaste algo sospechoso, revoca permisos inmediatamente y mueve tus fondos a una nueva wallet segura.

---

## 13.4 Exchanges falsos y retiros bloqueados

**Qué es**

Algunos sitios se hacen pasar por exchanges o plataformas de inversión cripto, pero son solo paneles de control falsos. Ves gráficas, balances, operaciones que "ganan", ganancias diarias. Puedes depositar sin problemas y hasta te permiten retirar montos pequeños al principio. Cuando tu saldo es grande y quieres retirar una parte significativa, comienzan los bloqueos: te piden pagar "impuestos", "tarifas de verificación KYC" o "desbloqueo de cuenta premium". Pagas… y sigues sin poder retirar, hasta que desaparecen.

**Señales de alerta**

- Exchange muy poco conocido, sin app en tiendas oficiales, con dominio reciente y sin menciones reales en la comunidad cripto.
- No hay información clara de quién opera la plataforma, dónde está registrada o qué regulador la supervisa.
- Piden pagos adicionales para poder retirar, con conceptos absurdos ("impuesto de retiro", "cuota de activación").
- Soporte solo por WhatsApp o Telegram, con respuestas genéricas y evasivas.

**Cómo defenderte**

- Usa únicamente exchanges y plataformas con reputación consolidada, listados en sitios serios y, de preferencia, regulados.

- Antes de meter dinero serio, haz un retiro de prueba pequeño; si no dejan, es mala señal.
- Desconfía de cualquier plataforma que te pida pagar extra para "liberar" tu propio saldo.
- Revisa el dominio, antigüedad, reseñas externas y advertencias de reguladores.
- Si ya estás atrapado, no envíes más dinero: guarda evidencias, denuncia y asume que es mejor cortar pérdidas que seguir alimentando el fraude.

---

## 13.5 Rug pulls en DeFi y NFT 2.0

### Qué es

El rug pull no solo ocurre con tokens; también con proyectos DeFi y colecciones NFT. Se lanza un protocolo de yield farming, un juego play-to-earn, o una colección con promesas de roadmap ambicioso: metaverso, series, videojuegos, todo. Se acumula liquidez, se venden NFTs, la comunidad crece. De repente, el equipo desaparece, cierra redes, retira la liquidez, abandona el desarrollo. Los holders se quedan con tokens o NFTs sin utilidad ni mercado.

### Señales de alerta

- Roadmap grandioso pero sin equipo técnico reconocido ni código abierto verificable.
- Fondos del proyecto (treasury, fondos de desarrollo) bajo control de pocas llaves sin mecanismos de gobernanza claros.
- Contratos sin auditoría independiente o con auditorías dudosas de "firmas" desconocidas.
- Comunicación hiperoptimista en redes, pero sin entregables reales ni avances técnicos visibles.

### Cómo defenderte

- Investiga al equipo: identidades reales, experiencia anterior, presencia en la comunidad.
- Revisa si el contrato y la tesorería del proyecto tienen mecanismos de gobernanza y multi-firma.
- No te dejes llevar solo por el hype; busca análisis independientes, no solo el discurso del propio proyecto.
- Distribuye riesgo: no pongas una parte significativa de tu patrimonio en un solo protocolo experimental.
- Si ves señales de abandono (sin updates, sin soporte, redes muertas), considera salir antes de que sea tarde.

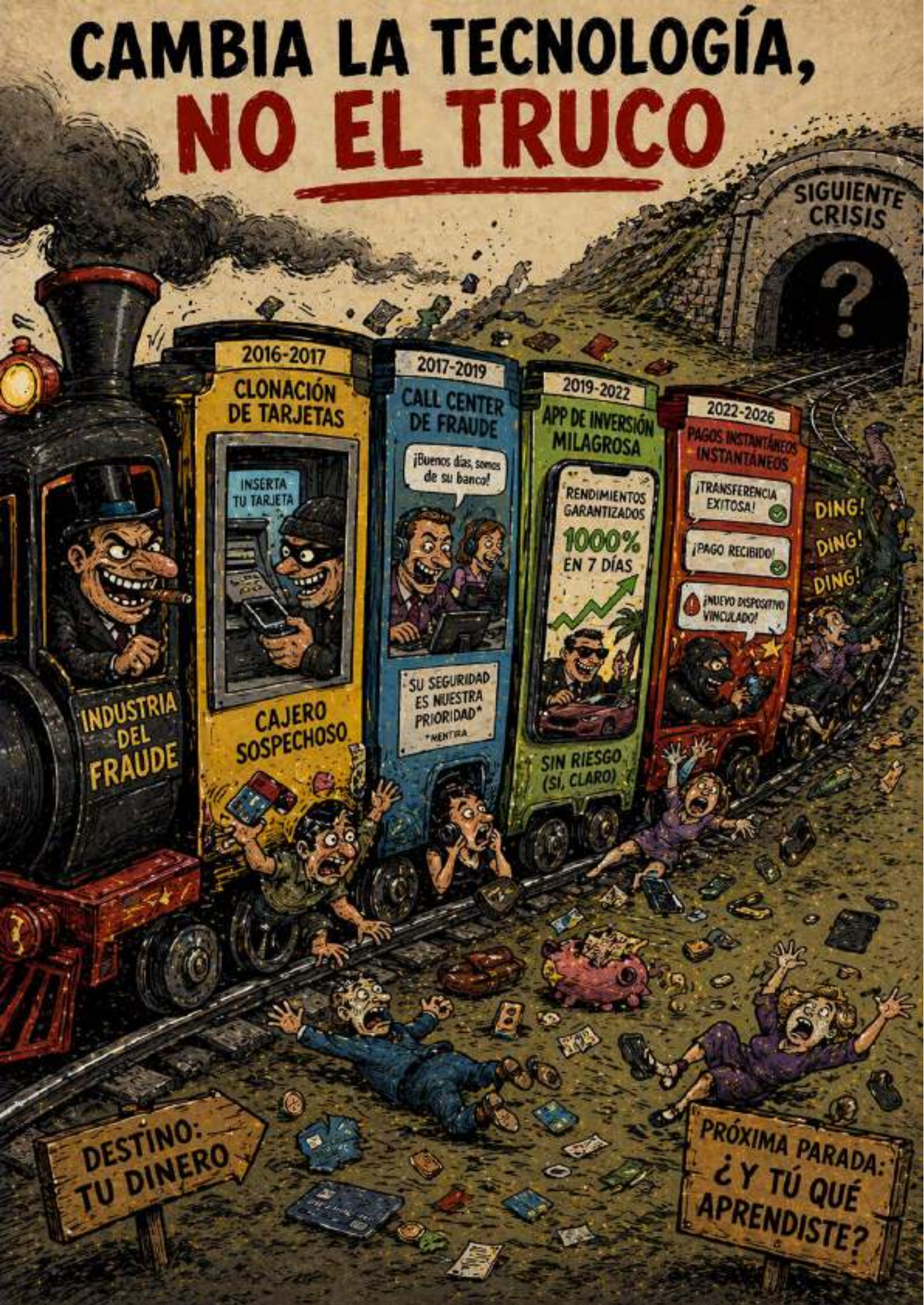
Cripto y Web3 pueden cambiar muchas cosas, pero no cambian el apetito por el dinero fácil. Cuando alguien use la palabra “revolucionario” más veces que la palabra “riesgo”, ya tienes tu primera bandera roja. Si el proyecto depende más de hype y de fe que de entender cómo se genera valor, no estás invirtiendo: estás apostando en un casino donde la casa ni siquiera existe.

# Capítulo 14 — Panorama general del fraude 2016-2026

Si ves la última década en cámara rápida, parece un montaje de tarjeta clonada, llamada sospechosa, app rara y notificación de transferencia que nunca hiciste. La esencia del fraude no cambió: sigue siendo engañar para que tú hagas clic donde no debes; lo que cambió fue la velocidad y el volumen. Aquí vamos a usar la línea de tiempo 2016-2026 como tren de la bruja: vagón por vagón, fraude por fraude, hasta entender cómo llegamos a un mundo donde el dinero viaja en segundos y el criterio a veces se queda en casa.

De 2016 a 2026 el fraude pasó de “me clonaron la tarjeta” a “autoricé yo mismo la transferencia porque un bot, un deepfake o un WhatsApp me convenció”. El fraude ya no solo roba dinero: roba identidad, reputación, tiempo y paz mental.

# CAMBIA LA TECNOLOGÍA, NO EL TRUCO



## 14.1 De la clonación al APP fraud (Authorized Push Payment)

### Qué es

El gran cambio de la década es que muchas estafas ya no se basan en que te roben credenciales, sino en que **tú mismo autorices** la operación. El APP fraud (fraude por pago autorizado) ocurre cuando, bajo engaño, haces una transferencia, un SPEI, un CoDi, un PIX, un Zelle, creyendo que pagas algo legítimo: proveedor, familiar, inversión, rescate, premio, Hacienda. El banco te dirá: "usted digitó la CLABE, usted confirmó". La estafa se mudó del cajero al cerebro.

### Señales de alerta

- Operaciones "urgentes" que no estaban en tu plan del día y que alguien más te presiona a hacer.
- Solicitudes de pago que llegan por canales informales (WhatsApp, redes sociales, llamadas desconocidas).
- Cambios de cuenta de proveedores o "oportunidades" que solo puedes aprovechar si transfieres de inmediato.

### Cómo defenderte

- Aplica la **regla del segundo canal** para cualquier transferencia que no sea rutinaria: si te piden por WhatsApp, confirma por llamada a un número ya guardado, no al que llegó en el mensaje.
- Antes de pagar, pregúntate "¿quién lo inició realmente, yo o alguien que me empuja?".
- Usa confirmación de beneficiario cuando tu banco la tenga (ver nombre asociado a la CLABE).
- Si dudas, retrasa el pago 10 minutos; la prisa es del estafador, no tuya.

---

## 14.2 El fraude como industria global

### Qué es

El fraude dejó de ser cosa de "dos listos en la esquina" y se convirtió en **industria internacional**: call centers criminales, cadenas de mulas, proveedores de malware, desarrolladores de paneles de estafa, diseñadores de campañas. Hay manuales, franquicias, Ransomware-as-a-Service, kits de phishing, "soporte al cliente" para estafas. Se estima que las pérdidas globales por fraude y cibercrimen superan fácilmente el billón de dólares anuales cuando sumas bancos, comercio, empresas, gobiernos y ciudadanos.

**Señales de alerta**

- Campañas idénticas de fraude replicadas en muchos países con ligeras variaciones de idioma.
- Plataformas que parecen “profesionales” pero solo sirven para robar: webs, apps, paneles de inversión.
- Incremento constante en la sofisticación de correos, llamadas y sitios fraudulentos.

**Cómo defenderte**

- Cambia el chip: no pienses en “un ratero aislado”, sino en una industria que prueba técnicas a escala.
- No subestimes ningún canal: correo, SMS, WhatsApp, redes, apps, llamadas, QR, todos son vectores.
- Mantente al día: sigue fuentes confiables de ciberseguridad, reguladores y bancos que publican alertas de nuevas campañas.
- Asume que, si hay dinero en juego, alguien ya está pensando cómo explotarlo.

---

## 14.3 Tendencia: más datos, más personalización, más daño

**Qué es**

Entre 2016 y 2026 se dispararon las filtraciones de datos: bases de correos, teléfonos, direcciones, historiales de compras, ubicaciones. Esos datos se venden en foros y dark web y alimentan fraudes cada vez más personalizados. El correo ya no dice “querido cliente”, dice tu nombre, menciona tu banco, sabe en qué ciudad vives y a qué hora te conectas. El ataque emocional y la ingeniería social se adaptan a tu perfil.

**Señales de alerta**

- Mensajes que usan información personal que tú nunca diste a esa persona o canal.
- Llamadas donde el estafador sabe datos sobre tu trabajo, tu banco, tu familia, que podrían haber salido de redes o filtraciones.
- Ofertas y estafas que encajan demasiado bien con tu situación financiera actual.

**Cómo defenderte**

- Da solo los datos necesarios a cada servicio; mientras menos información circule, menos hay para explotar.

- Usa correos diferentes para distintos tipos de servicios (banca, redes, compras, newsletters).
- Revisa noticias de brechas de seguridad y cambia contraseñas si estuviste en una.
- No sobreexpongas tu vida en redes: menos es más seguridad.

---

## 14.4 Del efectivo a los pagos instantáneos

**Qué es**

En estos años migramos de “me robaron efectivo” a “me robaron vía app”. Los pagos instantáneos (SPEI, CoDi, PIX, Zelle, etc.) son maravillosos… y casi irreversibles. El fraude se adapta: extorsiones, engaños, invoice redirection, mulas. Una vez que tú autorizas, el dinero salta entre cuentas y bancos en segundos. Muchas legislaciones y bancos están apenas ajustando procesos para tratar el APP fraud como un problema compartido, no solo “culpa del cliente”.

**Señales de alerta**

- Transferencias que salen de tu cuenta a altas horas, bajo presión, a cuentas jamás usadas.
- “Proveedores” que cambian de CLABE sobre la marcha y piden que olvides la anterior.
- Pedidos de devolución instantánea de transferencias que supuestamente se equivocaron contigo.

**Cómo defenderte**

- Configura límites diarios y por transacción que reflejen tu realidad; no necesitas tener el límite en el techo.
- Activa notificaciones push/SMS para cada operación; mientras más rápido veas algo raro, más posibilidad de reaccionar.
- Para empresas, establece flujos claros de autorización y verificación de pagos: nadie debería poder cambiar cuentas de proveedores sin triple check.
- Recuerda que “no hay trato” mientras no hayas enviado dinero; el poder de decir “no” está antes de apretar “Aceptar”.

---

## 14.5 México y Latinoamérica: caldo perfecto, pero también laboratorio de defensa

**Qué es**

México y Latam combinan alta digitalización (banca móvil, e-commerce, fintech), desigualdad, informalidad y confianza en canales como WhatsApp. Eso es oro para el fraude. Pero también se han vuelto laboratorio de soluciones: modelos antifraude en tiempo real, regulación fintech, unidades de inteligencia financiera activas, campañas de educación financiera. Lo que funcione aquí para frenar el fraude, probablemente servirá en otros mercados.

**Señales de alerta**

- Oleadas de la misma estafa en varios países: falsas ayudas gubernamentales, bonos COVID, apoyos sociales, becas, supuestas devoluciones de impuestos.
- Reutilización de esquemas: lo que fue "boletos de avión baratos" en 2018 ahora es "paquetes de streaming", lo que fue "tarjeta alimentaria" ahora es "Crédito Jóvenes Construyendo el Futuro".

**Cómo defenderte**

- Aprovecha los recursos locales: Condusef, Profeco, Policía Cibernética, UIF, bancos, fintech y medios que publican alertas periódicas.
- Participa en la defensa comunitaria: avisa en tus grupos (familia, colegas, vecinos) cuando identifiques una nueva estafa.
- Como empresario o sujeto obligado, no esperes a que la regulación te obligue; implementar controles hoy siempre será más barato que un escándalo mañana.
- Como ciudadano, asume tu papel de primera línea: el sistema se fortalece cuando tú dudas, verificas y denuncias.

Visto en retrospectiva, la historia reciente del fraude es una secuencia de "lo nuevo" haciendo viejo al truco anterior. Del plástico a la llamada, de la llamada a la app, de la app al pago instantáneo, el objetivo siempre fue el mismo: llegar a tu cerebro antes que tu criterio. Saber cómo llegamos aquí no arregla el pasado, pero te da una ventaja incómoda: ya no puedes decir que no veías venir el siguiente vagón.

# Capítulo 15 — Fraude de identidad

Tu nombre, tu cara y tu historial financiero valen más de lo que crees, sobre todo cuando alguien más los usa mejor que tú. Robo de identidad, cuentas que se abren a tu nombre, tarjetas que nunca pediste y créditos que solo conoces cuando llegan los cobros son parte del menú. En este capítulo vamos a ver cómo se fabrica una identidad sintética, qué es un "bust-out" y por qué proteger tus datos no es paranoia: es higiene básica, como lavarse las manos, pero versión 2026.

Aquí el negocio no es robarte la cartera, sino convertirse en ti ante bancos, tiendas, plataformas y autoridades. A veces clonan tu identidad; otras, la inventan desde cero.

# TU CARA PUEDE TRABAJAR PARA ALGUIEN MÁS SIN AVISARTE

# 15.1 Robo de identidad y Account Takeover (ATO)

### Qué es

En el robo de identidad clásico, alguien usa tus datos reales (nombre, CURP, RFC, INE, domicilio) para contratar servicios, pedir créditos, comprar a plazos o abrir cuentas a tu nombre. El Account Takeover (ATO) es la toma de control de tus cuentas ya existentes: correo, banca, redes sociales, e-commerce. Generalmente empieza con una filtración de datos, phishing, malware o ingeniería social. Cuando te das cuenta, ya hay cargos, créditos y mensajes enviados como si fueras tú.

### Señales de alerta

- Te llegan estados de cuenta, cartas o correos de créditos y tarjetas que nunca solicitaste.
- Recibes notificaciones de inicio de sesión desde dispositivos o ubicaciones desconocidas.
- Te aparecen consultas o aperturas recientes en tu buró de crédito que no reconoces.
- Tus contactos reciben mensajes raros tuyos pidiendo dinero o datos.

### Cómo defenderte

- Activa 2FA en todas tus cuentas críticas (correo, redes, banca, wallets); sin correo seguro, nada es seguro.
- Revisa tu buró de crédito al menos una vez al año y activa alertas o bloqueos de consulta si hay intentos raros.
- Usa contraseñas únicas y largas, gestionadas con un gestor de contraseñas, no con tu memoria ni el bloc de notas.
- Si detectas robo de identidad, levanta reportes con el banco, buró de crédito, Condusef y autoridades; documenta todo.
- Considera congelar temporalmente tu historial de crédito mientras se aclara el caso.

---

# 15.2 Identidad sintética

### Qué es

La identidad sintética no es tanto robo como Frankenstein: combinan datos reales (CURP válido, fecha de nacimiento, RFC) con nombre, dirección y otros datos inventados. Esa "persona" no existe, pero los sistemas la tratan como real. Se abre una cuenta, se pide un crédito pequeño, se paga puntualmente un tiempo para construir historial… y luego viene el bust-out: se maximizan todas las líneas de

crédito y se desaparece. No hay víctima directa evidente, solo instituciones que se quedan con cartera incobrable.

**Señales de alerta (para instituciones)**

- Clientes nuevos con historial "limpio" pero extremadamente corto que escalan límites muy rápido.
- Información personal que pasa validaciones básicas, pero falla en verificaciones más profundas (direcciones inexistentes, teléfonos no atribuibles).
- Múltiples identidades que comparten atributos técnicos (misma IP, mismo dispositivo, mismo patrón de navegación).

**Cómo defenderte**

- Implementa verificaciones de identidad con múltiples capas: documentos, biometría, verificación de domicilio, validación cruzada de datos.
- Usa modelos específicos de detección de identidad sintética basados en comportamiento y patrones de uso, no solo en scoring tradicional.
- Limita el crecimiento de líneas de crédito nuevas hasta ver comportamiento sostenido en el tiempo.
- Como regulador o industria, comparte información de patrones de fraude para detectar clusters entre entidades.
- Como ciudadano, protege tus datos básicos; mientras menos se filtren, más difícil será construir identidades sintéticas con tus elementos.

---

## 15.3 Bust-out

**Qué es**

El bust-out es la "estafa final" de un historial construido. Un defraudador (con identidad real o sintética) se porta bien durante meses: paga puntual, mantiene buen uso del crédito, gana confianza. Una vez que tiene varias tarjetas, líneas, préstamos y límites altos, de pronto maximiza todo a la vez: saca efectivo, compra caro, mueve dinero… y deja de pagar. Las instituciones creen que enfrentan un problema de morosidad, pero muchas veces fue planeado desde el inicio.

**Señales de alerta (para instituciones)**

- Clientes que aumentan simultáneamente el uso de todas sus líneas de crédito en poco tiempo.
- Cambios de dirección, correo o teléfono poco antes del pico de endeudamiento.

- Transferencias y disposiciones de efectivo atípicas respecto al comportamiento histórico de ese cliente.
- Solicitudes de aumento de límite en varias tarjetas casi al mismo tiempo.

**Cómo defenderte**

- Usa modelos de riesgo que detecten cambios bruscos de comportamiento, no solo impagos.
- Limita aumentos de límite frecuentes y cruzados, especialmente en clientes de historial corto.
- Verifica cambios de datos sensibles (domicilio, teléfono, correo) por segundo canal.
- Como persona, no prestes tu identidad o tu crédito a terceros para que "ellos usen el dinero y te paguen"; el bust-out puede acabar con tu historial.
- Documenta e investiga bust-outs sospechosos como fraude, no solo como cartera vencida.

---

## 15.4 KYC vulnerado y onboarding débil

**Qué es**

El proceso KYC (Know Your Customer) es la puerta de entrada de clientes a bancos, fintech, casas de bolsa, cripto, etc. Cuando esa puerta es débil, el sistema entero se vuelve vulnerable. Onboardings que sólo piden selfie + INE y no validan nada, validaciones automáticas mal configuradas, ausencia de prueba de vida… Todo eso permite que identidades robadas, sintéticas o suplantadas abran cuentas y productos a tu nombre o a nombre de fantasmas.

**Señales de alerta (para instituciones)**

- Tasas muy altas de fraude en cuentas abiertas por canales 100% digitales, frente a sucursales o procesos presenciales.
- Documentos repetidos en varios clientes (misma INE usada para identidades distintas).
- Volúmenes de alta de cuentas muy superiores a la media del mercado, sin controles proporcionales.

**Cómo defenderte**

- Refuerza el KYC usando múltiples fuentes: validación con autoridades, biometría, listas de riesgo, pruebas de vida dinámicas.
- No sacrifiques seguridad por "menos fricción" en onboarding; el costo del fraude suele ser mayor que el abandono inicial.

- Realiza revisiones periódicas de tu base de clientes para depurar identidades dudosas o inconsistentes.
- Documenta claramente los niveles de KYC por tipo de producto y riesgo.
- Educa a tu equipo de negocio: crecimiento sano no es abrir cuentas a cualquier cosa que respira (o ni respira).

---

## 15.5 Data breaches y mercados de datos

**Qué es**

Entre 2016 y 2026 explotaron las filtraciones de datos: bancos, aseguradoras, e-commerce, aerolíneas, redes sociales, gobiernos. Bases con millones de correos, contraseñas, teléfonos, direcciones, historiales de compra y hasta datos financieros circulan en foros y dark web. Esos datos alimentan campañas de phishing, ATO, robo de identidad y estafas dirigidas. El problema ya no es si te filtraron, sino cuántas veces y qué uso le dan a esa información.

**Señales de alerta**

- Recibes correos y llamadas que contienen datos tuyos que solo deberías haber dado a ciertas empresas.
- Apareces en buscadores que indexan filtraciones ("tu correo aparece en X breaches").
- Te llegan intentos de recuperación de contraseña de servicios que tú no pediste.

**Cómo defenderte**

- Usa correos distintos para distintos tipos de servicios y no reutilices contraseñas entre sitios.
- Activa 2FA siempre; una contraseña filtrada duele menos si sola no basta para entrar.
- Monitorea si tu correo o teléfono aparecen en bases filtradas y, si es así, cambia contraseñas y refuerza seguridad.
- Reduce tu huella de datos: cancela servicios que no uses, pide eliminación de cuentas antiguas, limita la información que das por default.
- Si eres empresa, asume que eres un objetivo y trabaja en serio en seguridad de la información, no solo en compliance de papel.

Tu identidad no es solo algo que "está en el buró", es un activo que se puede rentar, robar o copiar. Cada dato que regalas sin pensar es una pieza más para que alguien arme un "tú alternativo" que pide créditos y abre cuentas. Si te da flojera cuidar tus datos, piensa que quizá estás trabajando horas extra para pagar las deudas de un desconocido con tu cara.

# Capítulo 16 — Los 10 fraudes corporativos más comunes en México

En México, muchas empresas no quiebran por la competencia, quiebran por la confianza mal puesta en casa. Proveedores "de toda la vida", nóminas que pagan a gente que nadie ha visto, inventarios mágicos que nunca cuadran y gastos "de representación" que parecen agencia de viajes son parte del paisaje. En este capítulo vamos a ponerle nombre y apellidos (genéricos) a los fraudes más comunes dentro de las organizaciones, para que cuando alguien diga "aquí jamás pasaría eso", tengas al menos motivos para levantar una ceja.

En la empresa mexicana promedio, el riesgo no solo viene "de afuera". Mucho daño lo causan los de adentro con acceso, confianza y creatividad.


# LA EMPRESA PIERDE DINERO, PERO GANA HISTORIAS

## 16.1 Fraude de proveedores (sobornos y comisiones por debajo del agua)

**Qué es**

Ocurre cuando un comprador, gerente o directivo recibe pagos, regalos o favores de un proveedor a cambio de darle contratos, inflar precios, aceptar calidad mediocre o simular servicios. La empresa paga de más, recibe menos y el diferencial se reparte en lo oscurito. Puede ser en efectivo, viajes, autos, comisiones "por fuera" o facturas por servicios inventados.

**Señales de alerta**

- Siempre ganan los mismos proveedores, aunque sus cotizaciones sean más caras o con peor servicio.
- Cambios de último minuto en las órdenes para favorecer a un proveedor concreto.
- Proveedores nuevos que entran sin cumplir requisitos que a otros sí se exigen.
- Relación demasiado cercana entre personal de compras y ciertos proveedores (viajes, comidas constantes, favores).

**Cómo defenderte**

- Implementa procesos de licitación transparentes con mínimo tres cotizaciones y criterios claros de evaluación.
- Separa funciones: quien pide, quien cotiza y quien autoriza no deben ser la misma persona.
- Lleva registro de obsequios y atenciones permitidos y prohíbe regalos de alto valor.
- Realiza auditorías periódicas de compras, comparando precios contra mercado.
- Habilita un canal de denuncia anónima para que el personal pueda reportar favoritismos y sobornos.

---

## 16.2 Desvío y fraude en nómina

**Qué es**

Incluye empleados fantasma, horas extra inventadas, bonos duplicados, ajustes de nómina a favor de personas específicas y uso personal de prestaciones. RH y Nómina

pueden coludirse con jefes para inflar pagos o registrar personas que no trabajan ahí. La empresa paga sueldos que nadie cobra honestamente.

**Señales de alerta**

- Nombres en nómina que nadie reconoce en las áreas operativas.
- Diferencias entre el número de empleados registrados ante IMSS y los que cobran en la nómina interna.
- Horas extra, bonos o comisiones inusuales concentradas en ciertas personas o áreas.
- Cuentas bancarias repetidas o vinculadas a familiares de alguien de nómina.

**Cómo defenderte**

- Usa control biométrico o sistemas de asistencia confiables y crúzalos con pagos de nómina.
- Haz auditorías sorpresa de personal (headcount) por área.
- Separa la función de alta/baja de empleados de la función de autorización de pagos.
- Revisa periódicamente nómina contra registros de IMSS, SAT y organigramas.
- Investiga cualquier discrepancia significativa y sanciona de forma ejemplar.

---

## 16.3 Robo hormiga e inventarios inflados

**Qué es**

El robo hormiga es la sustracción constante de inventario por parte de empleados, proveedores o transportistas: cajas que "se pierden", mermas exageradas, productos que salen sin registrarse. También puede haber inventarios inflados en sistemas para maquillar faltantes físicos. En retail, logística, manufactura y farmacias esto pega directo a la utilidad.

**Señales de alerta**

- Diferencias recurrentes entre inventario físico y contable, siempre a la baja.
- Productos de alto valor que "caducan" o "se dañan" con frecuencia.
- Empleados que acumulan rechazos en revisiones de bultos, lockers o vehículos.
- Quejas de clientes por faltantes en entregas cuando en sistema todo aparece "entregado".

**Cómo defenderte**

- Implementa conteos cíclicos de inventario, no solo inventario anual.

- Usa cámaras, controles de acceso y, si aplica, RFID o códigos de barras bien gestionados.
- Separa funciones: quien recibe, quien almacena y quien embarca deben ser distintos.
- Analiza patrones por turno, sucursal y supervisor para detectar focos rojos.
- Crea una cultura donde reportar robos no sea "ser sapo", sino proteger la chamba de todos.

---

## 16.4 Uso personal de recursos y tarjetas corporativas

### Qué es

Aquí la empresa se vuelve cajero automático o tarjeta de puntos del empleado o directivo "vivo". Gastos personales disfrazados de representación, viáticos inflados, gasolina para el coche de la familia, compras en línea cargadas a la tarjeta corporativa y facturadas como "insumos". El recurso se va en Uber, restaurantes, gadgets y viajes que nada tienen que ver con el negocio.

### Señales de alerta

- Gastos recurrentes en restaurantes, tiendas, hoteles y servicios que no corresponden al rol del usuario.
- Tickets sin detalles, sin nombres de clientes, sin anotaciones de motivo de la reunión.
- Comprobaciones tardías, anticipo de viáticos que nunca se regularizan, saldos siempre altos.
- Mismas categorías de gasto inusualmente elevadas en uno o dos empleados respecto al promedio.

### Cómo defenderte

- Define políticas claras de gastos: qué sí, qué no, montos máximos, documentación requerida.
- Usa tarjetas corporativas con límites por perfil y restricciones por categoría de comercio.
- Revisa y aprueba gastos por niveles; nadie debe aprobar sus propios gastos.
- Haz auditorías aleatorias de notas y comprobantes, llamando a los supuestos "clientes" si hace falta.
- Retira de inmediato privilegios de gasto y sanciona cuando se detecten abusos.

---

## 16.5 Lapping y jineteo de cobranza

### Qué es

El lapping es cuando alguien en cobranza o caja se queda con los pagos de un cliente y luego usa el pago de otro para tapar el hueco. Es una especie de Ponzi interno: el dinero entra, pero se retrasa su registro, se "jinetear" y el desorden contable lo oculta hasta que estalla. Muchas veces se apoya en ajustes manuales de cuentas por cobrar y notas de crédito dudosas.

### Señales de alerta

- Clientes que aseguran haber pagado, pero en sistema aparecen como morosos.
- Aplicaciones de pago manuales, fuera de las reglas normales.
- Notas de crédito frecuentes sin documentación clara, siempre gestionadas por la misma persona.
- Conciliaciones bancarias complicadas, con muchos "en tránsito" o partidas sin identificar.

### Cómo defenderte

- Realiza conciliaciones bancarias diarias y cruza con registros de cobranza.
- Separa funciones: quien recibe pagos no debe registrar en el sistema ni aplicar notas de crédito.
- Implementa políticas claras para ajustes manuales y requiere autorización de un superior no involucrado.
- Ofrece a los clientes comprobantes digitales inmediatos y fomenta que reporten discrepancias.
- Rota al personal de caja/cobranza y revisa especialmente cuando alguien deje el puesto.

---

## 16.6 Facturación falsa interna (EDOS doméstico)

### Qué es

Más allá de EFOS externos, muchas empresas dentro de México compran facturas para deducir gastos inexistentes. Se simulan servicios, se cargan gastos inventados a proyectos, se justifican retiros de efectivo con CFDI de empresas "amigas". Parte de ese dinero se reparte en sobres, parte se usa para cajas negras, parte para sobornos.

### Señales de alerta

- Facturas por servicios genéricos ("asesoría", "gestión", "servicios varios") sin entregables reales.

- Proveedores con poco personal o infraestructura que facturan montos desproporcionados.
- Pagos a empresas que aparecen en lista 69-B del SAT o en listas internas de riesgo.
- Conexión evidente entre dueños de proveedores y directivos de la empresa.

**Cómo defenderte**

- Revisa la **materialidad** de todos los gastos significativos: contratos, entregables, correos, evidencia.
- Consulta de forma periódica la lista 69-B del SAT y actualiza tu padrón de proveedores.
- Haz revisiones cruzadas entre compras, contabilidad e impuestos para detectar patrones atípicos.
- Establece una política de cero tolerancia a la compra de facturas; lo fiscal y lo penal van de la mano.
- Protege y empodera a quien señale estas prácticas; si lo despiden por "incómodo", el mensaje es devastador.

---

## 16.7 Colusión en licitaciones y compras públicas

**Qué es**

En empresas que venden al gobierno (y en el propio gobierno), proveedores se ponen de acuerdo para repartirse contratos: fijan precios, simulan competencia, alternan quién "gana". A cambio, funcionarios y directivos reciben comisiones. El resultado: la institución paga más por menos y el dinero público se escurre.

**Señales de alerta**

- Las mismas empresas participan en todas las licitaciones y se reparten los ganadores de forma sospechosamente ordenada.
- Propuestas económicas muy similares o con errores idénticos, señal de que vienen del mismo origen.
- Cambios en requisitos del concurso diseñados a medida para excluir a ciertos participantes.

**Cómo defenderte**

- Publica y documenta procesos de licitación de forma abierta, con criterios y resultados claros.
- Analiza patrones de participación y adjudicación a lo largo del tiempo.
- Fomenta denuncias internas y externas de colusión; ofrece protección a denunciantes.

- Consulta a COFECE y otras autoridades cuando haya indicios de prácticas monopólicas.
- Dentro de la empresa, establece barreras para que compras no sea “club de cuates”.

---

## 16.8 Fraude en seguros corporativos

**Qué es**

Incluye siniestros inventados o inflados: robos simulados, accidentes exagerados, daños fabricados, normalmente en colusión con talleres, médicos, abogados o agentes. La empresa paga primas más altas a largo plazo, la aseguradora absorbe pérdidas y el costo se socializa.

**Señales de alerta**

- Aumento repentino en la frecuencia de siniestros en ciertas áreas o líneas de negocio.
- Costos de reparación o tratamiento persistentemente más altos con ciertos proveedores.
- Reclamaciones que ocurren justo antes de cambios de póliza, cierres de año o revisiones de primas.

**Cómo defenderte**

- Trabaja con aseguradoras y ajustadores de confianza, con rotación de proveedores para evitar colusión.
- Exige evidencia documental y fotográfica sólida de cada siniestro.
- Implementa controles internos sobre quién reporta, quién valida y quién gestiona siniestros.
- Compara tus tasas de siniestralidad con benchmarks de tu sector.
- Investiga y sanciona la colusión interna; no la tapes para “no afectar la imagen”.

---

## 16.9 Quiebra fraudulenta y vaciamiento de activos

**Qué es**

Antes de declararse en crisis o concurso mercantil, algunos dueños vacían la empresa: venden activos a precio de regalo a empresas relacionadas, sacan efectivo vía contratos simulados, transfieren marcas y patentes a otras sociedades. Luego

dejan a proveedores, empleados, bancos y fisco con una carcasa vacía. Legalmente se declaran insolventes, moralmente se declaran inexistentes.

**Señales de alerta**

- Venta rápida de activos clave sin razones estratégicas claras.
- Aparición de "deudas" con empresas poco conocidas, cercanas al dueño, poco antes de la crisis.
- Transferencia de marca, cartera de clientes o know-how a nuevas sociedades del mismo grupo.

**Cómo defenderte**

- Como proveedor o acreedor, monitorea la salud financiera de tus clientes grandes y diversifica riesgos.
- Incluye cláusulas de garantías, retenciones y pagos anticipados en contratos relevantes.
- Como regulador y auditor, revisa operaciones con partes relacionadas en empresas en apuros.
- Documenta y, de ser necesario, persigue acciones legales para recuperar activos o responsabilidades.
- Internamente, exige transparencia en reestructuras y venta de activos; cuestiona operaciones opacas.

---

## 16.10 Manipulación de estados financieros

**Qué es**

Es el arte oscuro de maquillar números: inflar ingresos, ocultar pasivos, capitalizar gastos, subestimar provisiones, inventariar humo. Se hace para conseguir crédito, atraer inversión, mejorar bonos, cumplir convenios con bancos o simplemente sostener la farsa un trimestre más. Casos como Enron, Wirecard o empresas locales muestran que un Excel creativo puede valer miles de millones… hasta que ya no.

**Señales de alerta**

- Crecimiento de ingresos y utilidades muy por encima del mercado sin explicación razonable.
- Cambios frecuentes de política contable que mágicamente mejoran resultados.
- Rotación sospechosa de auditores externos o presiones para que "no sean tan estrictos".
- Falta de transparencia en notas a los estados financieros y negativa a entregar detalle cuando se solicita.

**Cómo defenderte**

- Asegura independencia real del auditor externo y rota periódicamente al socio encargado.
- Crea un comité de auditoría fuerte, con miembros independientes que entiendan de números.
- Premia a la dirección por gestión de riesgos y sostenibilidad, no solo por resultados a corto plazo.
- Como inversionista o banco, no creas solo en el PDF bonito; pide detalle, haz preguntas incómodas y compara con pares.
- Como colaborador, si ves manipulación de cifras, documenta y usa canales de denuncia; los casos grandes casi siempre tuvieron alertas internas ignoradas.

En el mundo corporativo, el fraude rara vez es un rayo caído del cielo; casi siempre es goteo acumulado. Lo que hoy parece “detalle” en proveedores, nómina o inventario es muchas veces el piloto de algo más grande. Una empresa que solo se escandaliza cuando llega el escándalo ya empezó tarde.

# Capítulo 17 — Grandes escándalos de lavado y fraude

Los grandes casos internacionales son como series de moda: todo mundo los comenta, casi nadie aprende la lección. Bancos gigantes, fondos brillantes, empresas "innovadoras" y políticos de tiempo completo han protagonizado historias que parecen ficción, pero la factura la pagó gente muy real. Aquí no vamos a hacer culto al escándalo, sino disección: qué patrones se repiten, qué señales ignoraron todos y por qué, si eso pasó a ese nivel, tu PyME y tu familia no son excepción a la regla, solo jugadores más pequeños.

Estos casos son el Olimpo del desmadre financiero: miles de millones, políticos, bancos globales, auditors dormidos y una lección clara: si les funcionó a ellos, alguien lo está intentando en chiquito cerca de ti.


# CUANDO EL ESCÁNDALO ES SHOW, LA LECCIÓN SE PIERDE

## 17.1 1MDB (Malasia) — Fondo soberano convertido en cochinito personal

**Qué es**

1MDB era un fondo soberano de desarrollo de Malasia; entre 2009 y 2015 se robaron más de 4,5 mil millones de dólares a través de empresas fachada, bonos inflados y estructuras offshore. El dinero financió propiedades de lujo, arte, joyas, casinos y hasta la película "The Wolf of Wall Street". El escándalo tumbó políticamente al entonces primer ministro Najib Razak y obligó a bancos globales a pagar multas millonarias.

**Lecciones para México y Latam**

- Los fondos públicos y fideicomisos opacos son perfectos para mezclar política con lavado.
- La banca corresponsal sin debida diligencia real se vuelve autopista para miles de millones.
- Periodistas y sociedad civil pueden destapar lo que los controles internos dejaron pasar años.

---

## 17.2 Panama Papers y Pandora Papers — Offshore a plena luz

**Qué es**

Los Panama Papers (2016) y Pandora Papers (2021) expusieron millones de documentos de despachos offshore que creaban sociedades y trusts en paraísos fiscales para políticos, empresarios, celebridades y criminales. Muchas estructuras eran legales, pero otras mostraban esquemas de evasión fiscal, ocultamiento patrimonial y posible lavado a gran escala. Más que un caso, fue un radiografía del uso sistémico de opacidad.

**Lecciones**

- Tener empresa offshore no es delito; usarla para ocultar sobornos, sí.

- Abogados y proveedores de estructuras son gatekeepers críticos, no simples "tramitadores".
- La presión internacional por transparencia de beneficiarios finales va a seguir creciendo.

---

## 17.3 Danske Bank (Estonia) — 200 mil millones de euros sospechosos

**Qué es**

La sucursal de Danske Bank en Estonia lavó, entre 2007 y 2015, alrededor de 200 mil millones de euros en transacciones sospechosas de clientes no residentes, principalmente de Rusia y otros países del Este. La filial era pequeña, pero procesaba volúmenes absurdos sin controles efectivos ni supervisión adecuada, hasta que el escándalo explotó y la matriz tuvo que reconocer el desastre.

**Lecciones**

- Una sucursal "chiquita" puede ser el hoyo negro de todo el grupo si nadie la mira.
- El negocio de "cliente no residente" es de altísimo riesgo si se maneja solo con papeles.
- Supervisores locales y extranjeros van a revisar con lupa banca corresponsal y filiales en jurisdicciones débiles.

---

## 17.4 Wirecard — Fintech europea que era puro PowerPoint

**Qué es**

Wirecard era la joya fintech alemana hasta que en 2020 se descubrió que 1,9 mil millones de euros en efectivo supuestamente resguardados en cuentas de Asia simplemente **no existían**. El auditor no verificó a tiempo la existencia real de esos fondos; habían inflado ingresos, balances y operaciones de acquiring durante años.

La empresa colapsó, directivos fueron detenidos y la reputación de la supervisión alemana quedó tocada.

**Lecciones**

- "Somos fintech" no es excusa para relajar controles básicos: ¿existe el dinero que dices tener?
- Auditores que no confirman saldos de efectivo con bancos independientes hacen más relaciones públicas que auditoría.
- Los inversores y bancos deben exigir pruebas duras, no solo narrativa de innovación.

---

# 17.5 FTX y Alameda Research — Cripto exchange disfrazando agujeros

**Qué es**

FTX era una de las casas de cambio cripto más grandes del mundo hasta que colapsó en noviembre de 2022. La ex CEO de Alameda Research confesó que Alameda tomó miles de millones de dólares de depósitos de clientes de FTX para cubrir pérdidas y financiar apuestas riesgosas, maquillando la situación con estados financieros falsos. Cuando los clientes quisieron retirar en masa, el castillo de naipes se vino abajo.

**Lecciones**

- "Not your keys, not your coins": dejar fondos en exchanges no regulados es confiar a ciegas.
- Segregar fondos de clientes y fondos propios no es opcional; es línea roja.
- La falta de gobernanza y de consejo independiente en empresas cripto es receta para el desastre.

---

# 17.6 Archegos — Family office que reventó bancos

**Qué es**

Archegos Capital Management era un family office que usó derivados (total return swaps) para tomar posiciones gigantes en pocas acciones, financiadas por varios bancos prime brokers. Como usaban derivados, las posiciones no aparecían claramente en reportes tradicionales, multiplicando el apalancamiento oculto. Cuando el mercado se movió en contra, Archegos colapsó y dejó pérdidas por más de 10 mil millones de dólares en bancos como Credit Suisse y Nomura.

**Lecciones**

- La opacidad de ciertos instrumentos permite acumular riesgos sistémicos invisibles hasta que es tarde.
- Los bancos deben mirar el **riesgo agregado** de clientes compartidos, no solo lo que cada uno ve por separado.
- "Cliente sofisticado" no significa "cliente que no hay que supervisar".

---

## 17.7 Odebrecht / Lava Jato — Corrupción en serie en Latinoamérica

**Qué es**

La constructora brasileña Odebrecht montó durante décadas un sistema de sobornos a funcionarios y políticos en al menos 12 países, pagando más de 780 millones de dólares en coimas para ganar contratos por más de 3,300 millones. Tenía un "Departamento de Operaciones Estructuradas", básicamente una oficina dedicada a la corrupción: offshores, bancos, mensajeros y códigos para mover el dinero.

**Lecciones**

- La corrupción corporativa a gran escala requiere departamentos completos, no solo "un gerente desviado".
- Empresas que dependen del contrato público sin controles anticorrupción son bombas de tiempo.
- Del lado de los países receptores, los sistemas de compras públicas y los bancos locales son parte del problema o de la solución.

---

## 17.8 Madoff — El Ponzi que todos quisieron creer

### Qué es

Bernard Madoff dirigió el mayor esquema Ponzi conocido: prometía rendimientos constantes y altos a inversionistas institucionales y particulares, y pagaba a los antiguos con el dinero de los nuevos. Durante años, reguladores y bancos recibieron alertas de analistas que no creían las cifras, pero el prestigio de Madoff y el miedo a perderse "la oportunidad" mantuvieron el esquema vivo hasta que colapsó tras la crisis de 2008, con pérdidas estimadas en 65 mil millones de dólares.

### Lecciones

- Rendimientos demasiado estables en mercados volátiles son una bandera roja gigantesca, no un sueño dorado.
- La reputación no sustituye al análisis técnico; que todos entren no significa que sea seguro.
- Los reguladores pueden fallar; la primera línea de defensa es la duda saludable de inversionistas y contrapartes.

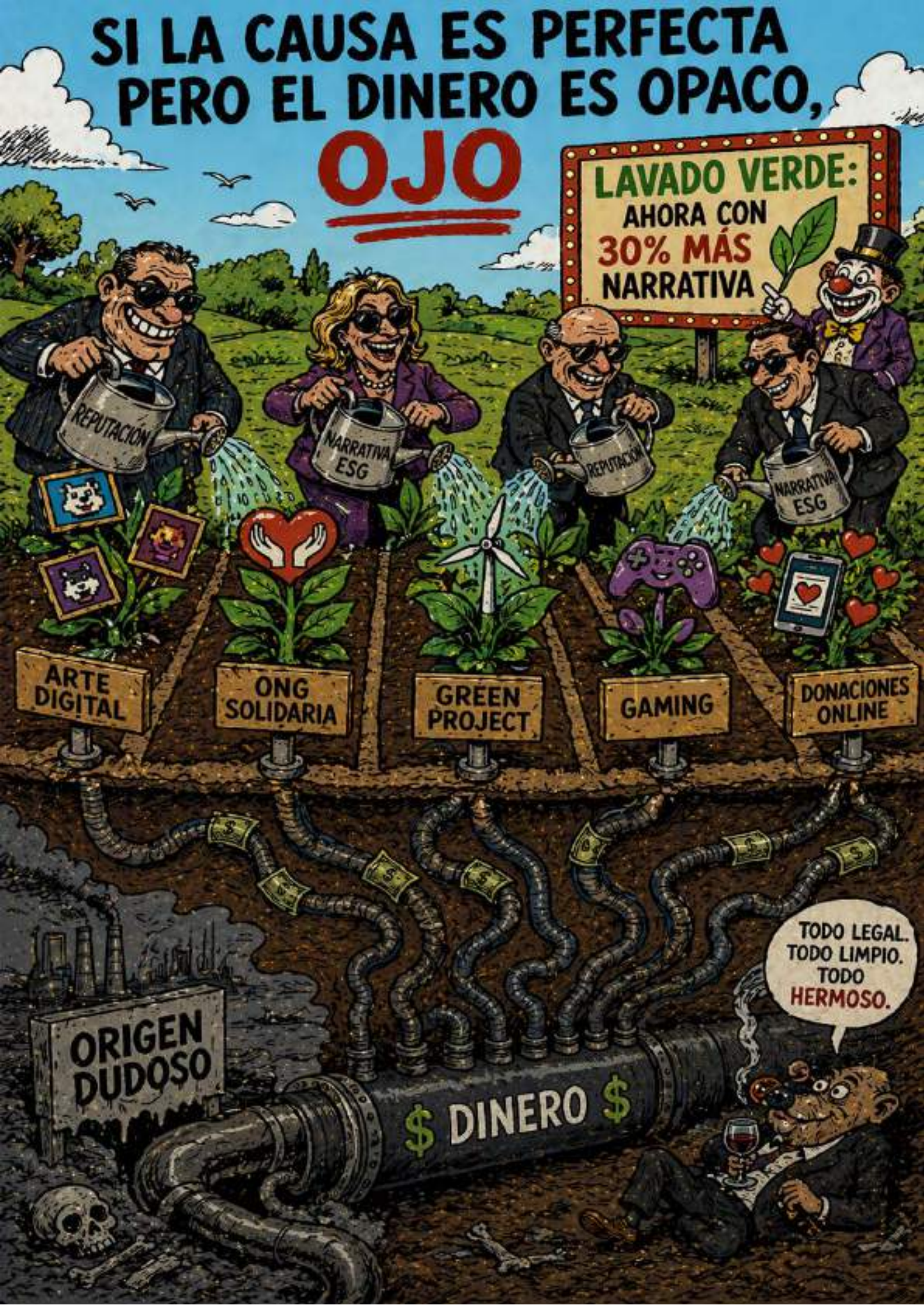
Los grandes casos sirven de poco si solo nos dejan memes y documentales. Cada escándalo que consumimos como entretenimiento sin preguntarnos "¿qué se repite aquí en chiquito cerca de mí?" es una oportunidad perdida. La idea no es vivir cazando conspiraciones, sino reconocer patrones antes de que tu propia historia acabe en un reportaje.

---

# Capítulo 18 — Lavado emergente 2016-2026

Cada vez que el mundo inventa una causa noble o una moda financiera, alguien pregunta en voz baja: “¿y esto cómo se lava?”. Proyectos verdes, arte digital, gaming, donaciones online, ONGs hiperactivas y esquemas “solidarios” se pueden usar para bien… o para convertir dinero raro en reputación impecable. En este capítulo vamos a revisar esas nuevas macetas donde florece el lavado y qué preguntas hay que hacer para distinguir un proyecto serio de un jardín de plástico muy caro.

Aquí el lavado se disfraza de start-up, e-commerce, influencer, gaming y salvación verde. Misma película de siempre, nuevos escenarios.


SI LA CAUSA ES PERFECTA PERO EL DINERO ES OPACO,
OJO
LAVADO VERDE:
AHORA CON
30% MÁS
NARRATIVA
REPUTACIÓN
NARRATIVA ESG
REPUTACIÓN
NARRATIVA ESG
ARTE DIGITAL
ONG SOLIDARIA
GREEN PROJECT
GAMING
DONACIONES ONLINE
ORIGEN DUDOSO
$ DINERO $
TODO LEGAL.
TODO LIMPIO.
TODO
HERMOSO.

## 18.1 TBML en e-commerce y dropshipping

**Qué es**

El viejo comercio exterior con sobrefacturación/subfacturación ahora viaja en cajas de Amazon y paquetes de "dropshipping". Se crean tiendas en línea que "venden" productos a precios inflados o subvaluados entre empresas relacionadas; los paquetes contienen artículos baratos o nada, pero en papeles parecen operaciones internacionales normales. También se usa la excusa del dropshipping para mover mercancía de origen dudoso y mezclar pagos legítimos con flujos ilícitos.

**Señales de alerta**

- Tiendas que declaran ventas internacionales muy altas, pero con logística laxa y sin marca reconocible.
- Envíos entre las mismas contrapartes en varios países, con valores fuera de mercado.
- Mucho movimiento transfronterizo para productos genéricos que podrían conseguirse localmente.

**Cómo defenderte**

- Como banco o PSP, analiza valores declarados vs. tipo de producto y mercado objetivo.
- Como empresa, documenta contratos, proveedores, precios y rutas de envío; si no se puede explicar sencillo, está mal.
- Revisa patrones de devoluciones, reembolsos y quejas: el e-commerce fantasma suele fallar ahí.
- Para ciudadanos, desconfía de "tiendas" que solo existen como pasarela de cobro sin reputación real.

---

## 18.2 Real estate con cripto y tokenización

**Qué es**

Una evolución de la integración inmobiliaria: ahora se compran casas y terrenos directamente con cripto, o se "tokenizan" inmuebles en plataformas Web3. El riesgo aparece cuando las plataformas no tienen KYC serio, cuando la procedencia de las criptos es dudosa o cuando los tokens solo sirven para mover valor entre wallets sin transparencia. Un edificio puede estar "fraccionado" en miles de tokens que cambian de manos sin que nadie sepa quién es el verdadero dueño final.

**Señales de alerta**

- Operaciones inmobiliarias pagadas total o mayoritariamente en cripto sin trazabilidad suficiente.
- Proyectos de tokenización sin regulación, sin auditoría independiente y sin claridad jurídica sobre los derechos que el token da.
- Uso de exchanges y wallets en jurisdicciones opacas como rampa principal de entrada de fondos.

**Cómo defenderte**

- Como notario, desarrollador o bróker, exige identificación completa del comprador y origen de fondos, aunque pague en cripto.
- Como plataforma de tokenización, integra KYC, KYB y monitoreo on-chain serio; si no, eres un imán de basura.
- Como inversor, investiga si el token representa un derecho real o solo es una promesa bonita sin valor legal.
- No aceptes compras "rápidas" sin documentación solo porque "el cliente trae Bitcoin".

---

## 18.3 DeFi layering

**Qué es**

En DeFi, el lavador no necesita bancos: usa DEX, pools de liquidez, lending y staking para hacer **layering** de fondos ilícitos. Convierte cripto robada o de delitos en otros tokens, los presta, los vuelve a cambiar, los pasa por varias redes y protocolos, los mezcla con servicios tipo mixer y privacy coins, y termina en una rampa fiat "limpia". Cada swap es una nueva capa.

**Señales de alerta**

- Wallets que interactúan con muchos protocolos DeFi en poco tiempo, con volúmenes altos y sin lógica de inversión.
- Flujos que pasan por DEX sin KYC, mixers y privacidad (Monero, Zcash) antes de llegar a exchanges regulados.
- Actividad de alta frecuencia que prioriza mover fondos, no generar rendimiento sostenible.

**Cómo defenderte**

- Exchanges y bancos deben integrar análisis de DeFi en sus herramientas on-chain, no solo transacciones directas.
- Tratar como alto riesgo los fondos que vienen de protocolos sin controles, mixers y privacy coins.

- Implementar políticas que requieran información reforzada cuando se detecta patrón típico de layering DeFi.
- Como usuario, desconfía de "servicios" que prometen anonimato total y rendimiento alto; suelen ser capas de humo criminal.

---

## 18.4 NFT wash trading y NFT como lavadero

**Qué es**

En el NFT wash trading, el mismo actor compra y vende el NFT entre wallets que controla para inflar artificialmente su precio y volumen. Luego lo vende a un tercero al precio inflado y justifica un ingreso grande como "venta de arte digital". El NFT también se usa para lavar comprando con dinero sucio, moviéndolo entre wallets y revendiéndolo, igual que en el arte físico.

**Señales de alerta**

- Misma obra vendida muchas veces en poco tiempo entre wallets recién creadas o claramente vinculadas.
- NFT sin trayectoria artística ni comunidad que de pronto se vende por montos exagerados.
- Compradores y vendedores que solo interactúan entre sí en múltiples operaciones.

**Cómo defenderte**

- Marketplaces deben aplicar análisis de patrones de wash trading y marcar o bloquear cuentas sospechosas.
- Implementar KYC mínimo para creadores y grandes compradores reduce el anonimato criminal.
- Como comprador, investiga: artista, comunidad, historial de ventas, no solo el "floor price".
- Si eres regulador o institución, trata el mercado NFT de alto valor como tratarías arte físico en PLD.

---

## 18.5 Gaming, metaverso y activos in-game

**Qué es**

Juegos play-to-earn, skins, ítems, terrenos virtuales y monedas in-game permiten mover valor entre cuentas de forma relativamente opaca. Se compran ítems con fondos ilícitos, se transfieren entre cuentas propias o de terceros y se venden

“legítimamente” en mercados secundarios. También hay torneos y premios ficticios que justifican pagos altos a “jugadores” o “equipos” fachada.

**Señales de alerta**

- Cuentas nuevas que hacen compras y ventas de ítems de alto valor sin jugar realmente.
- Transferencias frecuentes de activos entre pocas cuentas conectadas por IP o dispositivos.
- Premios grandes en torneos poco transparentes, sin comunidad real ni visibilidad.

**Cómo defenderte**

- Plataformas de gaming deben aplicar KYC a jugadores de alto valor y a quienes comercian con activos de forma regular.
- Implementar monitoreo de patrones atípicos: cuentas que solo compran y venden, pero no juegan.
- Como usuario, evita prestar tu cuenta o actuar como “intermediario” de terceros; puedes ser mula en un juego.
- Para instituciones, considerar gaming y metaverso como sectores emergentes de riesgo PLD, no solo entretenimiento.

---

## 18.6 Streaming fraud y contenidos digitales

**Qué es**

En el streaming fraud, bots y granjas de dispositivos reproducen canciones, podcasts o videos para inflar reproducciones y generar regalías que luego se reparten. Si ese contenido lo crearon empresas vinculadas, las regalías sirven para lavar dinero como “ingresos por derechos”. También se usan plataformas de video y suscripciones para justificar pagos regulares a creadores fachada.

**Señales de alerta**

- Contenidos con millones de reproducciones pero casi sin interacciones reales (comentarios, likes, comunidad).
- Reproducciones concentradas en pocas cuentas o ubicaciones, horarios artificiales.
- Ingresos elevados para creadores sin presencia orgánica ni promoción evidente.

**Cómo defenderte**

- Plataformas deben usar análisis antifraude para detectar patrones de bots y listening farms.
- Aplicar KYC y KYB a creadores que reciben pagos significativos.
- Como empresa, no uses streaming para mover dinero entre entidades relacionadas; deja huellas rastreables.
- Como usuario, sospecha de "oportunidades" para ganar dinero fácil con apps de reproducción en segundo plano.

---

## 18.7 Gift cards, puntos y millas como vehículo de lavado

**Qué es**

Las tarjetas de regalo y programas de puntos/millas permiten convertir efectivo o fondos ilícitos en saldos digitales relativamente anónimos. Se compran gift cards en grandes cantidades con dinero sucio, se revenden online o se usan para comprar productos que luego se revenden por efectivo. Es una forma de ir de efectivo a bienes/efectivo "limpio" saltándose parte de la banca formal.

**Señales de alerta**

- Compras frecuentes de gift cards de alto valor en efectivo en supermercados, tiendas departamentales o en línea.
- Personas o negocios que se dedican casi exclusivamente a comprar y revender tarjetas y códigos.
- Uso intensivo de gift cards para compras de electrónica, lujo u otros bienes fácilmente revendibles.

**Cómo defenderte**

- Comercios y emisores deben poner límites a compra de gift cards en efectivo y monitorear patrones atípicos.
- Requerir identificación para volúmenes altos y conservar registros de operaciones.
- Como ciudadano, desconfía si te piden pagar servicios o supuestas deudas con gift cards; es firma de fraude.
- Plataformas de reventa de tarjetas deben aplicar KYC y monitoreo para evitar ser mercado gris del lavado.

---

## 18.8 Crowdfunding y donaciones falsas

**Qué es**

Campañas de crowdfunding (salud, causas sociales, proyectos creativos) pueden ser auténticas… o fachadas para estafar y lavar. Se montan historias emotivas, fotos robadas, videos llorones, se captan donativos y luego los organizadores desaparecen. O se usa la campaña para justificar ingresos como "apoyos de la comunidad" cuando en realidad parte son fondos criminales que se cuelan.

**Señales de alerta**

- Campañas con historias muy dramáticas pero sin detalles verificables (nombres, hospitales, documentos).
- Organizadores que no quieren transparencia sobre uso de fondos ni permiten auditoría o actualización real.
- Mismas fotos o textos usados en varias campañas distintas al hacer búsqueda inversa.

**Cómo defenderte**

- Dona preferentemente a través de plataformas conocidas y a organizaciones con historial verificable.
- Verifica identidad de los organizadores y, si es un caso individual, busca confirmación por otros canales.
- Desconfía de campañas que solo aceptan medios opacos o no bancarizados cuando la plataforma ofrece más opciones.
- Como plataforma, integra KYC, monitoreo y mecanismos de devolución si se prueba fraude.

---

## 18.9 Influencer laundering y marketing inflado

**Qué es**

El influencer laundering consiste en usar contratos de "influencer marketing" para mover dinero entre empresas y personas, justificando pagos inflados como "campañas, menciones, posts y lives". Parte es evasión fiscal; parte, lavado de fondos de corrupción, crimen o esquemas Ponzi. Nadie sabe cuántos views reales tuvo la campaña, pero la factura y el contrato dicen que valía millones.

**Señales de alerta**

- Pagos muy altos a influencers con métricas poco verificables o audiencia inflada (bots, compra de followers).
- Contratos genéricos sin objetivos medibles ni KPIs claros.

- Empresas de marketing sin equipo, sin portafolio real, pero con facturación robusta hacia o desde sectores de alto riesgo.

**Cómo defenderte**

- Como marca, exige métricas reales: alcance, clics, conversiones, fuentes de datos y reportes auditables.
- No pagues montos altos sin entregables concretos (piezas, fechas, medición) y sin cláusulas de transparencia.
- Como influencer, evita prestarte para facturar servicios inexistentes; tu marca personal también se lava.
- Como banco, mira con lupa empresas de marketing digital que mueven volúmenes grandes sin sustancia visible.

---

## 18.10 Lavado verde y tokenización 2.0

**Qué es**

Además de lo visto en el Capítulo 10, la versión 2.0 del lavado verde integra **tokens ESG**, bonos verdes estructurados y proyectos ambientales tokenizados. Se colocan productos complejos que financian supuestos proyectos de reforestación, energías limpias o impacto social, pero en realidad una parte substancial se pierde en comisiones, estructuras y empresas vinculadas. La opacidad técnica y el aura "verde" reducen el escrutinio.

**Señales de alerta**

- Proyectos verdes o sociales con descripciones bonitas pero sin KPIs medibles ni reportes de impacto verificables.
- Estructuras financieras con muchas capas de empresas, fondos y SPVs en jurisdicciones opacas.
- Tokens ESG sin claridad jurídica sobre qué representan ni quién responde si sale mal.

**Cómo defenderte**

- Como inversor, trata los productos verdes y tokenizados con el mismo escepticismo que cualquier otro instrumento complejo.
- Exige métricas de impacto, auditorías externas y documentación transparente del flujo de fondos.
- Como emisor, no uses el greenwashing para maquillar estructuras opacas; ahora también es riesgo reputacional y regulatorio.
- Reguladores y UIF deben incorporar el riesgo ESG/tokenizado en sus matrices, no solo verlo como "tema de clima".

Las causas nobles no son antibalas; a veces son el mejor chaleco para el dinero sucio. Cuando un proyecto se vende con más narrativa que datos, más fotos que estados financieros y más emoción que transparencia, merece preguntas incómodas. Apoyar algo bueno no implica apagar el criterio, implica usarlo mejor.

# Capítulo 19 — Fraudes de pagos instantáneos

Los pagos instantáneos llegaron para hacerte la vida más fácil y la reacción más difícil. Cuando el dinero se mueve en segundos, la estafa también: APP fraud, mulas financieras, redirección de facturas y devoluciones fantasmas viven de esa combinación exacta de velocidad y descuido. Aquí vamos a ver cómo se arma un engaño en tiempo real, por qué "yo nunca doy mis datos" ya no alcanza y qué controles mínimos necesitas antes de acostumbrarte a que todo se pague "ahorita".

Los pagos instantáneos son magníficos… hasta que el fraude los usa como cohete. Cuando el dinero vuela en segundos, el margen para arrepentirse se vuelve microscópico.

# LA VELOCIDAD DEL DINERO, LA LENTITUD DE LA REACCIÓN

# 19.1 APP fraud (Authorized Push Payment)

### Qué es

El APP fraud ocurre cuando la víctima **autoriza** por sí misma una transferencia, pero lo hace engañada. No es que el banco "falle" técnicamente, sino que el estafador manipula a la persona para que ella misma envíe el dinero a una cuenta criminal. Puede disfrazarse de proveedor, familiar, inversión, multa, soporte técnico, premio o urgencia médica. En pagos instantáneos, esa autorización equivocada es casi una bala disparada: sale rápido, rebota entre cuentas y se esfuma.

### Señales de alerta

- La operación la inicia "otro" y tú solo obedeces la urgencia.
- El pago es a una cuenta nueva, nunca usada, y con presión emocional o de tiempo.
- Te dicen que no cortes la llamada o que no confirmes por otro canal.
- El concepto del pago es ambiguo: "apoyo", "rescate", "regularización", "inversión segura".

### Cómo defenderte

- Nunca hagas una transferencia importante bajo presión de tiempo, miedo o secreto.
- Aplica la **regla del segundo canal**: si te lo pidieron por WhatsApp, confirma por llamada a un número ya conocido; si fue por correo, valida por llamada o videollamada interna.
- Guarda listas blancas de cuentas frecuentes y trata cualquier cuenta nueva como operación de alto riesgo.
- Si eres empresa, exige doble autorización para cambios de beneficiario y pagos extraordinarios.

---

# 19.2 Fraude en SPEI

### Qué es

En México, el SPEI es rápido, útil y casi irrevertible. Esa velocidad lo convierte en objetivo ideal para extorsiones, pagos por proveedores falsos, BEC, secuestro virtual y engaños comerciales. Muchas víctimas creen que "el banco puede detenerlo", pero si el dinero ya salió y pasó a otra cuenta que también se vacía rápido, la recuperación se complica muchísimo.

### Señales de alerta

- Te piden enviar un SPEI “ahorita mismo” para evitar un problema mayor.
- La CLABE cambia a última hora y te dicen que “la otra ya no sirve”.
- El nombre del beneficiario no coincide del todo con la persona o empresa que te dice cobrar.
- Te piden fraccionar el pago en varias transferencias a distintas cuentas.

**Cómo defenderte**

- Verifica el nombre del beneficiario cuando tu banco muestre la coincidencia.
- No transfieras a cuentas nuevas sin validación documental y telefónica.
- Usa montos de prueba pequeños cuando se trate de un proveedor nuevo.
- Si sospechas fraude, reporta de inmediato al banco con folio, hora, CLABE y monto; los minutos importan.

---

## 19.3 CoDi y cobros por QR

**Qué es**

CoDi permite cobros inmediatos con QR y mensajes de cobro, lo que facilita pagos sin efectivo. El riesgo aparece cuando el QR está adulterado, cuando el mensaje de cobro no lo genera el comercio real o cuando un tercero suplanta el proceso y dirige el pago a otra cuenta. La comodidad del QR puede anestesiar la verificación.

**Señales de alerta**

- QRs pegados encima de otros o impresos de forma improvisada.
- Mensajes de cobro recibidos fuera de la app oficial del banco.
- Cobros con conceptos genéricos o sin el nombre claro del comercio.
- Personal que te “ayuda demasiado” a escanear y te apura a confirmar.

**Cómo defenderte**

- Antes de pagar, revisa en la app el nombre del beneficiario y el monto exacto.
- Evita escanear QRs de procedencia dudosa o pegados sobre otros.
- Si eres comercio, protege y revisa constantemente tus QRs físicos.
- Si hay cualquier duda, paga por otro método o solicita una confirmación directa del comercio.

---

## 19.4 Pix, Zelle y sistemas equivalentes

**Qué es**

Aunque este libro se centra en México, el fraude en pagos instantáneos comparte lógica con Pix en Brasil, Zelle en Estados Unidos y otros sistemas similares en Latam y fuera de ella. El patrón es el mismo: engañar a la víctima para que ella misma mande el dinero. Las diferencias son regulatorias y de interfaz, no de fondo. El estafador viaja más rápido que la ley.

**Señales de alerta**

- Mensajes o llamadas que apelan a sistemas "modernos y seguros" para convencerte de transferir de inmediato.
- Operaciones entre personas que nunca antes han hecho negocios juntas.
- Falsos comprobantes de transferencia para generar confianza o apurar una entrega.

**Cómo defenderte**

- Nunca entregues un producto o servicio basándote solo en un screenshot; verifica saldo real recibido.
- Aprende cómo funciona el sistema local de pagos que uses; la ignorancia operativa es aliada del fraude.
- Usa confirmación de recepción real, no promesas ni capturas editables.
- Desconfía de "expertos" improvisados que te dicen cómo mover dinero rápido y "sin riesgo".

---

## 19.5 Invoice redirection

**Qué es**

El invoice redirection es una variante muy común de APP fraud en empresas. Un delincuente compromete el correo de un proveedor o suplanta su identidad y manda la factura correcta… pero con una cuenta bancaria modificada. La empresa pagadora cree que todo está normal porque el PDF, el monto y el concepto son reales. Solo cambia la cuenta. Y ese "pequeño detalle" manda el dinero a la boca del lobo.

**Señales de alerta**

- Proveedor habitual que cambia CLABE o banco de forma repentina.
- Correo con tono normal, pero desde un dominio apenas distinto o reenviado desde un hilo comprometido.
- Presión por pagar ese mismo día "porque el sistema del proveedor cambió".
- Carta de cambio de cuenta con errores menores o firmas escaneadas raras.

**Cómo defenderte**

- Todo cambio de cuenta debe validarse por teléfono con un contacto ya registrado del proveedor, no con el del correo recibido.
- Mantén lista blanca de cuentas bancarias autorizadas por proveedor.
- Revisa encabezados y dominios de correos sospechosos en operaciones sensibles.
- Capacita a finanzas: la factura correcta con la cuenta incorrecta sigue siendo fraude.

---

## 19.6 Mulas financieras en pagos instantáneos

**Qué es**

Una mula financiera es la persona que presta su cuenta para recibir y reenviar dinero. En pagos instantáneos son piezas centrales porque permiten sacar rápidamente los fondos de la cuenta original y dispersarlos en minutos. Algunas mulas saben perfectamente lo que hacen; otras caen por ofertas de "trabajo desde casa", "cobranza digital" o "gestión de pagos".

**Señales de alerta**

- Ofertas laborales donde te piden usar tu cuenta personal para recibir y reenviar pagos.
- Ingresos de muchas personas desconocidas seguidos de salidas casi inmediatas.
- Cuentas de personas sin actividad empresarial que mueven montos altos en lapsos cortos.

**Cómo defenderte**

- Nunca uses tu cuenta personal como "puente" para terceros; eso puede ser lavado o fraude.
- Como banco o fintech, monitorea cuentas que reciben y dispersan en segundos múltiples transferencias.
- Como empresa, evita contratar a personas o "gestores" que cobren usando cuentas personales.
- Si sospechas que alguien cercano está siendo usado como mula, adviértele antes de que acabe con una carpeta de investigación.

---

## 19.7 Refund fraud y falsa devolución

**Qué es**

En esta modalidad, el estafador dice que por error te transfirió de más o te pagó dos veces y exige que le devuelvas la diferencia de inmediato. A veces usa comprobantes falsos; otras, el dinero sí entra, pero proviene de otra víctima o de una cuenta comprometida. Si tú lo "devuelves", ya no estás corrigiendo un error: estás ayudando a lavar o a consolidar el fraude.

**Señales de alerta**

- Te piden que devuelvas de inmediato sin esperar confirmación del banco.
- La devolución debe ir a una cuenta distinta a la que supuestamente te depositó.
- El remitente se pone agresivo o te amenaza si pides tiempo para revisar.

**Cómo defenderte**

- Nunca devuelvas dinero recibido por sorpresa sin hablar antes con tu banco.
- Verifica si la transferencia es firme y cuál es su origen.
- Si la situación es dudosa, no hagas movimiento alguno hasta tener claridad bancaria.
- Como negocio, establece protocolo para "pagos de más": nadie devuelve nada sin conciliación interna y bancaria.

---

## 19.8 Triangulation fraud

**Qué es**

En el triangulation fraud intervienen tres puntas: un comprador real, un vendedor fraudulento y un comercio legítimo. El estafador publica un producto barato en una plataforma. El comprador le paga. Luego el estafador usa una tarjeta robada para comprar ese producto en un comercio real y manda el envío al comprador. Todos creen que la operación salió bien… hasta que el titular real de la tarjeta desconoce el cargo y el comercio pierde.

**Señales de alerta**

- Productos muy baratos ofrecidos por vendedores sin reputación sólida.
- Cliente que paga rápido, pero el vendedor tarda y da explicaciones raras sobre "su sistema de envío".
- Comercios legítimos con aumento de contracargos en ciertas categorías o productos muy revendibles.

**Cómo defenderte**

- Como comprador, sospecha de precios demasiado bajos y vendedores improvisados.

- Como comercio, usa herramientas antifraude en checkout y revisa direcciones de envío inusuales.
- No te confíes solo por tener una venta; el contracargo puede llegar después.
- Como plataforma, monitorea vendedores nuevos con alto volumen y precios anómalos.

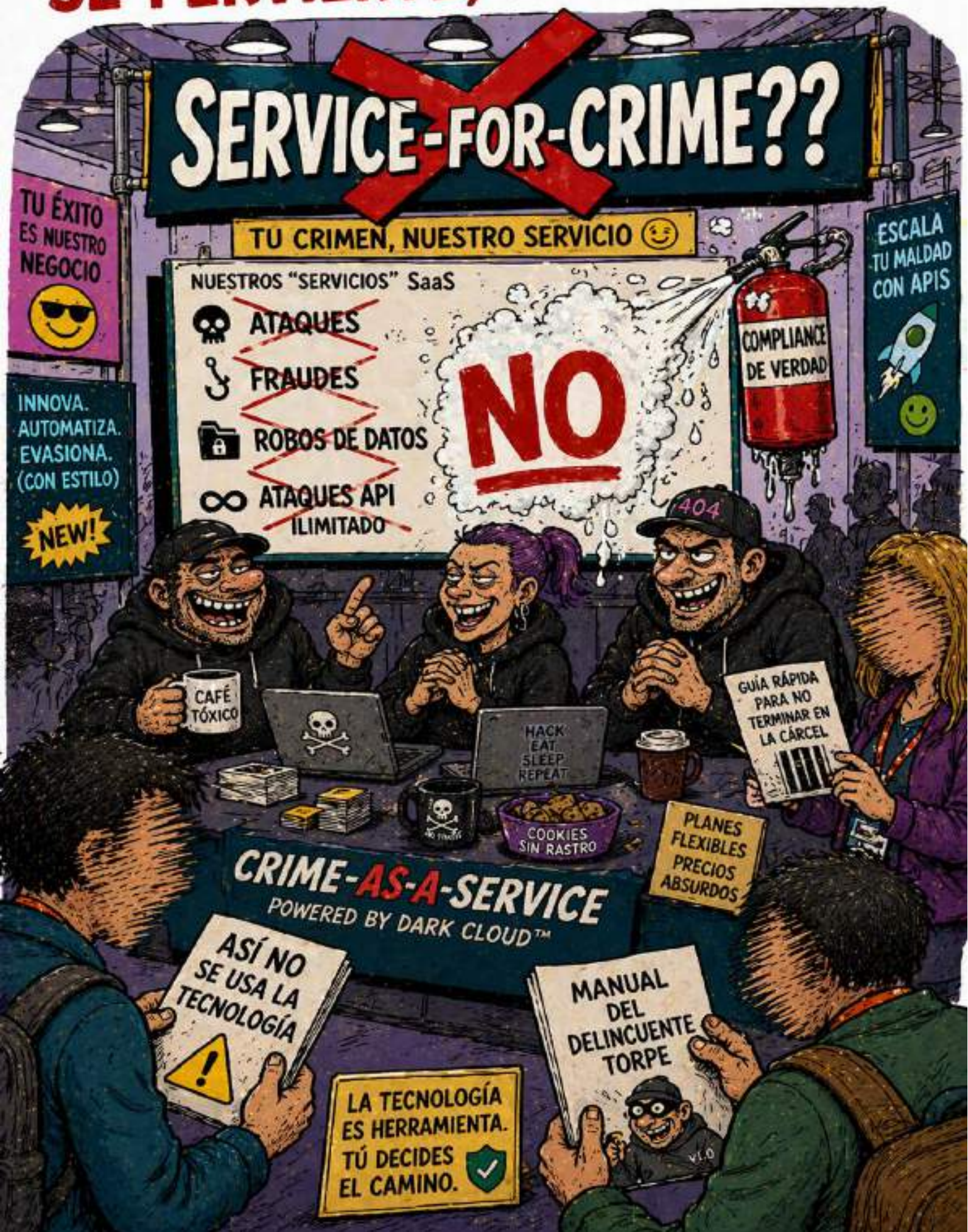
La velocidad de los pagos instantáneos no es enemiga, pero sí es una pésima consejera. Si te acostumbras a autorizar todo en automático “porque así es más ágil”, no te sorprenda que un día autorices también tu propio desastre financiero. La única parte del proceso que puede y debe ser lenta eres tú diciendo “déjame revisar”.

# Capítulo 20 — Ciberfraude avanzado

Mientras tú peleas con la contraseña del correo, hay gente comprando y vendiendo accesos, datos y ataques como si fueran servicios de streaming. Ransomware "llave en mano", kits de phishing listos para usar, robo de sesiones y abuso de APIs son el menú de una economía paralela que funciona mejor que muchos departamentos de TI. En este capítulo no vas a salir convertido en hacker ético, pero sí con un mapa decente de por qué "un clic" ya no es solo un clic, sino la puerta a un ecosistema entero de crimen empacado bonito.

Aquí el fraude ya no solo manda correos feos: usa RaaS, skimmers en tu e-commerce, minado oculto y acceso comprado al por mayor.

# CUANDO LA TECNOLOGÍA SE PERVIERTE, TODOS PERDEMOS



# 20.1 Ransomware-as-a-Service (RaaS)

**Qué es**

El RaaS convierte el ransomware en franquicia criminal: desarrolladores crean el malware y la infraestructura, y "afiliados" lo alquilan para lanzar ataques a cambio de una parte del rescate. Así, cualquiera con poca capacidad técnica puede montar campañas de cifrado y extorsión usando paneles listos, kits y soporte, igual que si comprara un SaaS legítimo, pero para secuestrar sistemas.

**Señales de alerta**

- Campañas de ransomware similares afectando a muchas organizaciones de diferentes países y sectores.
- Notas de rescate estandarizadas, con portales "de soporte" para víctimas en la dark web.
- Ataques que combinan cifrado de datos con robo y amenaza de publicación (doble o triple extorsión).

**Cómo defenderte**

- Refuerza higiene básica: parches, backups 3-2-1, segmentación, mínimos privilegios.
- Trata el acceso inicial (phishing, RDP expuesto, VPN sin MFA) como fuego: es lo que compran los afiliados.
- Ten un plan de respuesta a incidentes que incluya decisión sobre pago (o no) y contacto con autoridad.
- Usa EDR/XDR y monitoreo continuo para detectar movimiento lateral antes del cifrado.

---

# 20.2 Magecart y formjacking

**Qué es**

Magecart y el formjacking son skimmers digitales: inyectan JavaScript malicioso en formularios de pago de sitios e-commerce para copiar datos de tarjetas y credenciales en el momento del checkout. El sitio aparentemente funciona normal, el cliente

compra, pero una copia silenciosa de los datos se envía a los atacantes, que luego los venden o usan para fraude de tarjetas.

**Señales de alerta**

- Cambios no autorizados en scripts de terceros, plugins o tags en el front del sitio.
- Picos de fraude con tarjetas vinculados a compras recientes en tu tienda.
- Carga de recursos JavaScript desde dominios raros o no documentados.

**Cómo defenderte**

- Minimiza y controla scripts de terceros en el checkout; usa Content Security Policy y subresource integrity.
- Monitorea integridad de código en producción (file integrity monitoring, escaneos regulares).
- Separa front de pago en dominios y flujos controlados (por ejemplo, checkout en pasarela certificada).
- Como cliente, prefiere sitios conocidos y revisa movimientos de tu tarjeta periódicamente.

---

# 20.3 Cryptojacking

**Qué es**

El cryptojacking usa tu CPU y electricidad para minar cripto sin que lo sepas. Puede llegar vía scripts en el navegador (código incrustado en webs o anuncios) o como malware instalado en tu equipo, servidor o incluso infraestructura en la nube. No siempre roban datos, pero degradan rendimiento, elevan costos y pueden encubrir otras actividades criminales.

**Señales de alerta**

- Equipos o servidores muy lentos, ventiladores a tope, uso de CPU/GPU alto incluso en reposo.
- Aumento inusual en la factura de electricidad o de cómputo en la nube.
- Procesos desconocidos consumiendo recursos, o scripts raros cargados en webs propias.

**Cómo defenderte**

- Mantén sistemas y navegadores actualizados, con bloqueadores de scripts maliciosos.
- Usa monitoreo de recursos y alertas ante consumo anómalo en endpoints y nube.
- Revisa el código de tu web, plugins y anuncios integrados para detectar scripts de minería.
- En empresas, segmenta workloads críticos y aplica controles de ejecución de código.

---

# 20.4 Initial Access Brokers (IAB) y venta de accesos

**Qué es**

Los IAB son “mayoristas” de acceso: grupos o individuos que vulneran empresas (credenciales, RDP, VPN, paneles) y venden ese acceso a otros criminales para ransomware, fraude o espionaje. No siempre lanzan ellos el ataque final; su negocio es abrir la puerta y cobrar por dejarla entreabierta.

**Señales de alerta**

- Credenciales corporativas filtradas en foros, paste sites o dark web.
- Múltiples intentos de acceso desde ubicaciones inusuales a VPN, RDP o paneles administrativos.
- Cambios sospechosos en configuraciones de seguridad o creación de cuentas admin “fantasma”.

**Cómo defenderte**

- Implementa MFA fuerte en todos los accesos remotos y paneles críticos.
- Monitorea y bloquea intentos de fuerza bruta y patrones de acceso anómalos.
- Usa servicios de vigilancia de credenciales filtradas y rota claves comprometidas.
- Trata cada alerta de acceso sospechoso como posible puerta vendible en el mercado negro.

---

## 20.5 Business Email Compromise 2.0 (con IA y deepfake)

**Qué es**

El BEC clásico era el correo del "CEO" pidiendo un pago urgente. La versión 2.0 mezcla cuentas de correo comprometidas, redacción perfecta con IA y, en algunos casos, videollamadas con deepfake de voz o video para cerrar el engaño. Los delincuentes estudian calendarios, tono de escritura, flujo de aprobación y proveedores antes de lanzar el golpe.

**Señales de alerta**

- Correos que vienen de cuentas reales pero piden saltarse procesos normales de aprobación.
- Mensajes que imitan muy bien el estilo del ejecutivo, pero con cambios sutiles en cuentas o montos.
- Peticiones de mantener el tema "confidencial" y no involucrar a otros.

**Cómo defenderte**

- Establece políticas claras: ningún pago importante se autoriza solo por correo o chat.
- Usa firmas digitales, portales internos o sistemas de aprobación, no solo emails sueltos.
- Capacita a ejecutivos y finanzas sobre BEC con IA y deepfake; el ego es un vector de ataque.
- Aplica alertas cuando se cambian datos de proveedores o cuentas de pago.

---

## 20.6 Fraude en APIs y automatización abusiva

**Qué es**

Las APIs permiten integrar servicios, pero también automatizar fraude a escala: bots que prueban credenciales filtradas, que llenan formularios de crédito, que simulan clientes, que extraen datos sensibles. Cuando una API no está bien protegida (rate limits, autenticación, validaciones), se convierte en manguera abierta para ataques de relleno de credenciales, scraping y abuso de lógica de negocio.

**Señales de alerta**

- Tráfico inusual a endpoints específicos de la API (login, reset, alta de cliente) desde pocas IPs o rangos.
- Picos de errores de autenticación y de intentos fallidos de login.
- Crecimiento repentino de cuentas nuevas con patrones similares (nombres, correos, dispositivos).

**Cómo defenderte**

- Protege APIs con autenticación robusta, rate limiting, detección de bots y validaciones de negocio.
- Monitorea patrones de uso y crea reglas de bloqueo para comportamientos anómalos.
- Limita datos sensibles en respuestas de API, incluso en errores.
- Revisa regularmente documentación y exposición de tus APIs públicas y privadas.

---

# 20.7 Fraude omni-canal y kits de ataque "llave en mano"

**Qué es**

Los kits de fraude actuales integran todo: páginas clonadas, scripts de phishing, paneles para gestionar víctimas, bots para enviar SMS y WhatsApp, e incluso manuales para operadores. Una misma campaña golpea por correo, SMS, redes, llamadas y anuncios. El atacante compra o renta el paquete, personaliza logos y empieza a operar.

**Señales de alerta**

- Oleadas de reportes de clientes sobre intentos de phishing muy bien hechos usando tu marca.
- Reutilización de diseños, textos y flujos entre correos, SMS y webs falsas.
- Paneles de fraude encontrados en investigaciones internas o externas que usan tu imagen corporativa.

**Cómo defenderte**

- Monitorea activamente el uso de tu marca en dominios, redes y anuncios para detectar clonaciones.
- Ten un canal visible y simple para que clientes reporten intentos de phishing.
- Coopera con otros bancos/fintech del mercado para compartir indicadores de campaña (URLs, números, textos).
- Lanza comunicaciones proactivas educando a clientes sobre cómo luce tu canal legítimo y qué nunca pedirás.

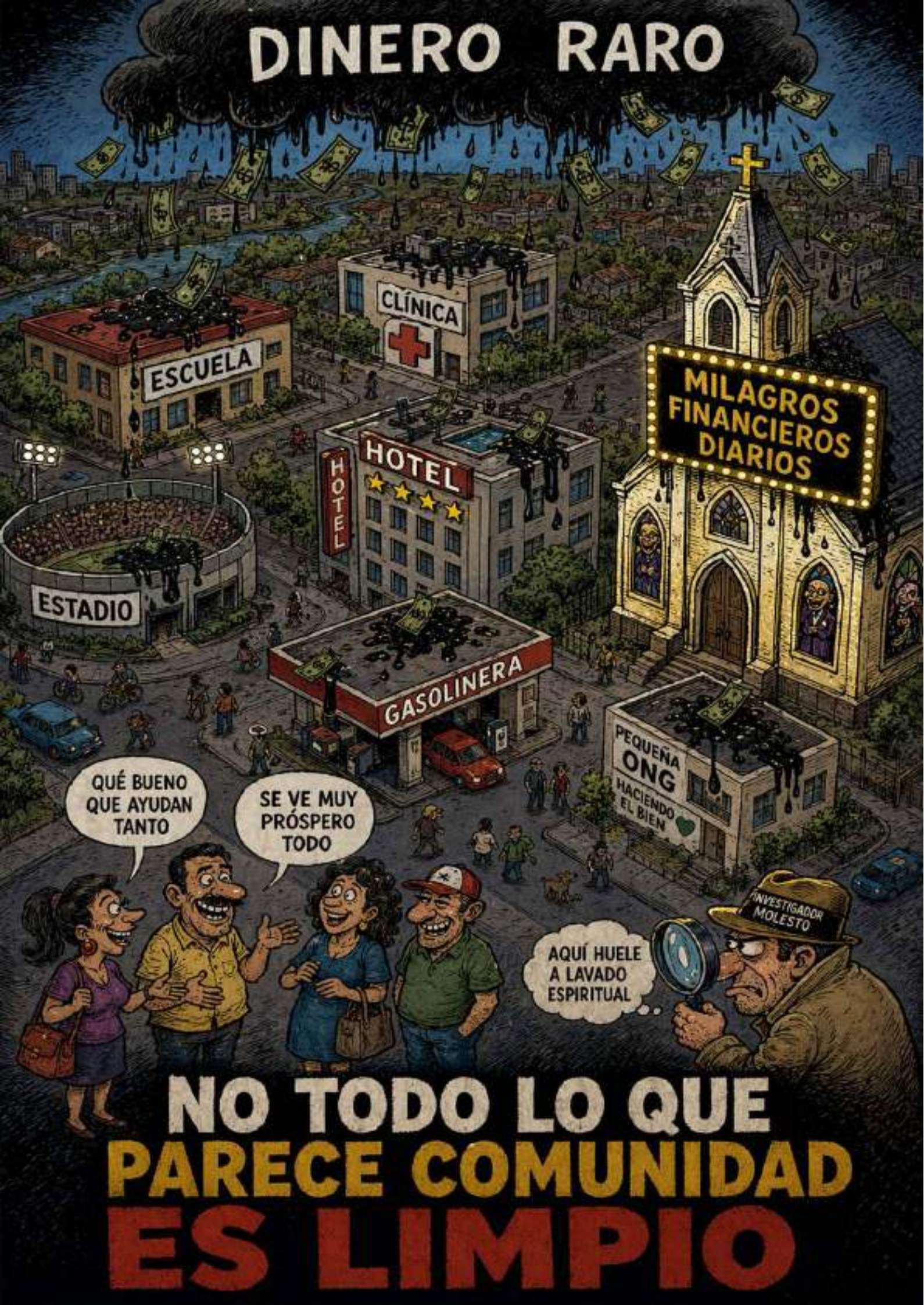
El ciberfraude dejó de ser cosa de genios solitarios y se volvió franquicia. Que existan kits, tutoriales y "servicios" solo significa que cada vez hay más manos capaces de apretar el botón equivocando. No puedes controlar todo el ecosistema, pero sí puedes decidir si tu organización sigue creyendo que "con antivirus basta" o entra, por fin, al siglo XXI.

---

# Capítulo 21 — Tipologías sectoriales poco discutidas

Cuando hablamos de lavado y fraude, todos miran a los bancos… mientras el dinero pasea tranquilamente por escuelas privadas, clínicas, iglesias, equipos locales, productoras culturales y negocios “familiares”. No porque todos sean malos, sino porque algunos aprendieron que nada blanquea mejor que la buena reputación de barrio. En este capítulo vamos a entrar a esos sectores que casi nunca salen en las noticias, pero donde a veces circula más dinero raro del que cabría en un maletín.

No todo es banca y grandes empresas. Hay sectores “chicos” que mueven dinero, efectivo, donativos y patrocinios… con muy poco foco de cumplimiento. Ahí el fraude y el lavado pasan casi a la vista de todos.


DINERO RARO
ESCUELA
CLÍNICA
MILAGROS FINANCIEROS DIARIOS
HOTEL
HOTEL
ESTADIO
GASOLINERA
PEQUEÑA ONG HACIENDO EL BIEN
QUÉ BUENO QUE AYUDAN TANTO
SE VE MUY PRÓSPERO TODO
AQUÍ HUELE A LAVADO ESPIRITUAL
INVESTIGADOR MOLESTO
NO TODO LO QUE PARECE COMUNIDAD ES LIMPIO

## 21.1 Educación privada y “cajas” escolares

**Qué es**

En escuelas privadas, asociaciones de padres y universidades pequeñas se manejan colegiaturas, donativos, cuotas y “cajas” internas. Cuando no hay controles, las cuentas escolares se usan para: desviar recursos, pagar en efectivo a proveedores opacos, justificar donativos de origen dudoso o hasta recibir pagos de terceros ajenos a la comunidad. Todo se viste de “apoyo a la educación”.

**Señales de alerta**

- Cuentas de la escuela que reciben depósitos de personas o empresas sin relación clara con la comunidad.
- Donativos grandes sin contrato ni condiciones definidas, a cambio de “apoyos” o “gestiones”.
- Falta de estados financieros claros para padres, patronatos o consejos.

**Cómo defenderte**

- Como escuela, lleva contabilidad transparente, auditada, con reportes periódicos a la comunidad.
- No recibas donativos significativos sin contratos claros y KYC básico del donante.
- Separa fondos operativos, donativos y cajas especiales; mientras más se mezclan, más fácil es el abuso.
- Como padre/madre, pregunta, pide informes, revisa números; la educación también es un negocio que debe rendir cuentas.

---

## 21.2 Salud, clínicas pequeñas y farmacias

**Qué es**

Clínicas, laboratorios, consultorios y farmacias pequeñas manejan mucho efectivo, seguros, recetas y facturas. Pueden usarse para inflar tratamientos, simular facturación de servicios no prestados, justificar pagos por “estudios” o “material médico” inexistente, o blanquear dinero a través de cadenas de farmacias “de barrio” que reportan ventas artificialmente infladas.

**Señales de alerta**

- Facturación de procedimientos caros a pacientes que casi no recuerdan haber sido atendidos.
- Pacientes fantasmas o muy pocos pacientes reales para los ingresos declarados.
- Compras de medicamentos o insumos incoherentes con la capacidad instalada del lugar.

**Cómo defenderte**

- Como clínica, establece controles de facturación, inventario y reconciliación con aseguradoras.
- No prestes tu razón social ni tu sello médico para facturar a terceros sin atención real.
- Como aseguradora, monitorea patrones por médico, clínica y diagnóstico.
- Como paciente, revisa tus estados de cuenta de seguros y cuestiona cobros que no reconozcas.

---

## 21.3 Deportes locales, ligas y asociaciones pequeñas

**Qué es**

Ligas locales, clubes deportivos, escuelas de futbol, academias de box o gimnasios pueden servir como vehículos para mover efectivo, patrocinios y donativos opacos. A veces son genuinos; otras, se inflan costos de uniformes, viajes, concentraciones o se simulan torneos para justificar flujos de empresas o políticos.

**Señales de alerta**

- Presencia repentina de “patrocinadores” con negocios dudosos o sin presencia real.
- Gastos opacos: nadie sabe exactamente cuánto costó el viaje, el equipo o el torneo.
- Uso constante de efectivo sin recibos ni cuentas claras.

**Cómo defenderte**

- Como club o liga, lleva libros y cuentas bancarias separadas, no cajas personales del entrenador o presidente.
- Transparencia básica: reportes periódicos a padres, socios y patrocinadores.
- No permitas que terceros paguen “todo en efectivo” sin registro formal.
- Como patrocinador, exige contratos sencillos y comprobantes; tu marca también se arriesga.

---

## 21.4 Cultura, festivales y proyectos artísticos

**Qué es**

Proyectos culturales (festivales, exposiciones, colectivos, “casas de cultura”) reciben apoyos públicos y privados, donativos y patrocinios. El riesgo: usar esos proyectos para sobrevaluar servicios (escenografía, sonido, logística), simular eventos o canalizar recursos a empresas amigas a través de contratos “creativos”. El arte se vuelve coartada para rebotar dinero.

**Señales de alerta**

- Presupuestos abultados para eventos con poca asistencia real o casi sin evidencia de ejecución.
- Proveedores recurrentes vinculados a organizadores o funcionarios.
- Falta de rendición de cuentas públicas sobre el uso de apoyos y subsidios.

**Cómo defenderte**

- Como organizador, documenta todo: contratos, proveedores, facturas, memorias fotográficas, reportes.
- Como financiador (público o privado), exige informes de resultados y desglose de gastos.
- Evita triangulaciones: si el apoyo es para el proyecto, que el dinero vaya directo al proyecto, no a capas de intermediarios.
- No uses la cultura como fachada; cuando se descubren abusos, se castiga a todo el sector.

---

## 21.5 Iglesias, congregaciones y asociaciones religiosas pequeñas

**Qué es**

Las comunidades religiosas recaudan diezmos, ofrendas, donativos y aportaciones para obras sociales. La mayoría son legítimas, pero su estructura de confianza y efectivo también puede ser usada para lavar: donativos grandes con origen opaco, compra de propiedades a nombre de la congregación, uso de cuentas de la iglesia para recibir pagos de terceros que nada tienen que ver con la comunidad.

**Señales de alerta**

- Donativos de alto monto de personas o empresas desconocidas para la congregación.
- Uso de cuentas de la iglesia para operaciones comerciales de particulares.

- Falta absoluta de estados financieros internos y externos.

**Cómo defenderte**

- Como liderazgo religioso, adopta buenas prácticas: contabilidad, auditoría básica, transparencia hacia la comunidad.
- No aceptes "favores" financieros que requieran prestar cuentas bancarias o personalidad jurídica a terceros.
- Como donante, verifica a dónde va el dinero y cómo se usa, especialmente en proyectos específicos.
- Recuerda que fe y transparencia no son opuestos; se refuerzan.

---

## 21.6 ONGs micro y colectivos de barrio

**Qué es**

Pequeñas ONGs, colectivos y asociaciones de barrio manejan donativos, apoyos y microproyectos. Pueden ser blanco de captura por grupos criminales o políticos que buscan una fachada "social" para mover o dispersar fondos, o simplemente terreno de pequeños desvíos y simulación de proyectos.

**Señales de alerta**

- Organizaciones nuevas que reciben montos grandes sin experiencia previa.
- Proyectos repetidos en papel pero sin evidencia de ejecución (fotos recicladas, testimonios genéricos).
- Estructuras de decisión opacas, concentradas en una sola persona.

**Cómo defenderte**

- Como colectivo genuino, documenta bien, aunque sea en pequeño: actas, gastos, resultados.
- Diversifica fuentes de financiamiento; depender de un solo "patrocinador" poderoso te hace vulnerable.
- No aceptes dinero bajo condiciones de opacidad o favores políticos.
- Como donante, empieza con montos pequeños y aumenta solo cuando veas resultados claros.

---

## 21.7 Servicios profesionales "de confianza" (despachos pequeños)

**Qué es**

Despachos pequeños de abogados, contadores, notarios locales y consultores independientes muchas veces operan sin programas formales de cumplimiento. Eso los vuelve presa fácil para convertirse en "arquitectos" de esquemas de terceros: sociedades, contratos, fideicomisos, facturación, todo sin preguntar demasiado.

**Señales de alerta**

- Clientes que buscan explícitamente "no dejar rastro" o "hacerlo por fuera".
- Estructuras repetitivas donde el despacho siempre aparece como representante o administrador de muchas empresas sin actividad real.
- Pagos importantes en efectivo o vía intermediarios a los profesionales.

**Cómo defenderte**

- Como profesional, establece tus propias reglas de KYC y riesgo, aunque la ley no te obligue todavía.
- Rechaza encargos que claramente busquen ocultar patrimonio o beneficiarios sin lógica jurídica válida.
- Documenta siempre el propósito económico de las estructuras que diseñas.
- Recuerda que "solo hice el contrato" no te exime de responsabilidad si sabías para qué servía.

---

## 21.8 Microfinancieras, cajas de ahorro y tandas organizadas

**Qué es**

Más allá de bancos y sofipos, existen microfinancieras informales, cajas de ahorro comunitarias y tandas organizadas que mueven dinero de muchas personas. Pueden usarse para captar recursos sin supervisión, financiar actividades ilícitas o servir como capa de estratificación y dispersión.

**Señales de alerta**

- Promesas de rendimientos altos sin supervisión de CNBV o autoridad similar.
- Opacidad sobre quién administra, dónde se guarda el dinero y bajo qué reglas.
- Uso de estas estructuras para mover montos muy superiores a los típicos de ahorro comunitario.

**Cómo defenderte**

- Como participante, entiende bien reglas, responsables y riesgos; no metas dinero que no estés dispuesto a perder.

- Como organizador, formaliza lo más posible: actas, reglas escritas, registros de entradas y salidas.
- No uses cajas o tandas para mover dinero de origen dudoso; la comunidad se vuelve responsable sin saberlo.
- Si escalas montos, evalúa migrar a figuras reguladas.

El banco no es el único lugar donde se mueve dinero; solo es el más obvio. Cuando un sector vive blindado por la narrativa de "somos comunidad, somos familia, somos servicio", es fácil que nadie pregunte de dónde sale y a dónde va tanto flujo. No es desconfiar de todo, es entender que la reputación también se puede usar como estructura.

# Capítulo 22 — Principios de defensa ciudadana

La mala noticia: nadie te va a cuidar el dinero, los datos ni la calma mental con el mismo cariño con que lo harías tú. La buena: no necesitas un diplomado para dejar de ser presa fácil, solo unas cuantas reglas simples repetidas hasta el cansancio. Aquí vas a encontrar esos principios básicos —pausar, verificar, usar un segundo canal, desconfiar de lo perfecto— puestos en lenguaje de casa, para que se puedan platicar en la mesa y en la junta sin que nadie bostece.

La mejor herramienta contra el fraude no es una app ni un antivirus: es tu criterio. Este capítulo destila reglas simples para que cualquier persona, familia o pequeña empresa tenga una línea base de defensa diaria.


# NO NECESITAS SER EXPERTO, SOLO DEJAR DE DECIDIR EN AUTOMÁTICO.

## 22.1 Regla de oro: si te presionan, te detienes

**Idea clave**

La mayoría de fraudes tienen un elemento en común: **prisa + miedo + secreto**. Quieren que actúes antes de pensar. Llamadas de emergencia, ultimátums, "ofertas que se acaban hoy", amenazas de autoridad: todo eso busca apagar tu sistema crítico.

**Cómo aplicarla**

- Si la otra parte grita "es urgente", tú bajas la velocidad.
- Toma al menos 10 minutos para revisar, llamar a alguien de confianza y validar por otro canal.
- Repite mentalmente: "Si me urge decidir ya, probablemente es mala decisión".
- Corta la llamada si alguien no te deja colgar "porque se corta el trámite".

---

## 22.2 Regla del segundo canal

**Idea clave**

Nunca completes una operación importante con **un solo canal** de comunicación. Si un dato crítico (cuenta, clave, monto, documento) llegó por WhatsApp, correo, llamada o redes, debes validarlo por un canal distinto que tú ya tenías con esa persona o institución.

**Cómo aplicarla**

- Proveedores: si te envían nueva CLABE por correo, llama al número oficial que ya tenías, no al del correo.
- Familia: si te piden dinero por WhatsApp, llama al celular conocido o a otro familiar.
- Banco: si te llaman, cuelga y tú marca al número oficial de la tarjeta o app.
- Oficinas: conecta con la extensión interna, no con el número que te dicte el correo.

---

## 22.3 Regla de la desconfianza proporcional al monto

**Idea clave**

Entre más dinero, datos o impacto en tu vida tenga una decisión, más **desconfiado** debes volverte. No puedes dedicar la misma atención a un pago de 100 pesos que a una transferencia de todo tu ahorro o a firmar un crédito.

**Cómo aplicarla**

- Cualquier operación que afecte más de un mes de tu ingreso merece revisión doble.
- Si implica endeudarte, vender patrimonio o usar ahorros, pide segunda opinión (al menos una).
- Si no entiendes el contrato o la inversión, no lo firmes: lo que no entiendes es riesgo.
- No tomes decisiones grandes cuando estés cansado, enojado, triste o eufórico.

---

## 22.4 Regla de la identidad blindada

**Idea clave**

Tu identidad es llave maestra: con ella piden créditos, abren cuentas, contratan servicios y te suplantan. Protegerla vale casi tanto como proteger tu dinero.

**Cómo aplicarla**

- No envíes foto de tu INE, pasaporte, estados de cuenta o comprobantes por WhatsApp a desconocidos o correos genéricos.
- Borra o tacha datos sensibles si debes compartir documentos (por ejemplo, solo últimos 4 dígitos).
- No publiques en redes CURP, RFC, domicilio completo ni fotos de tarjetas o boletos con códigos.
- Revisa tu buró de crédito una vez al año y activa alertas si hay movimientos raros.

---

## 22.5 Regla de las contraseñas y el correo raíz

**Idea clave**

Tu correo principal es la “llave de todas las llaves”: desde ahí se recuperan contraseñas de bancos, redes, tiendas, wallets. Si pierdes ese correo, pierdes el castillo completo.

**Cómo aplicarla**

- Usa contraseñas largas y distintas en cada servicio; apóyate en un gestor de contraseñas.
- Activa **doble factor** (2FA) en correo, banca, redes y wallets; preferible con app o llaves físicas, no solo SMS.
- Nunca uses la misma contraseña para correo y redes sociales o banca.
- Si recibes avisos de inicio de sesión extraño, cambia claves de inmediato y revisa dispositivos.

---

## 22.6 Regla de verifica antes de compartir

**Idea clave**

La mayoría de fraudes necesitan que tú compartas algo: código, token, NIP, foto de tarjeta, dato personal. Ninguna institución seria te pedirá eso por canales inseguros.

**Cómo aplicarla**

- Nunca des códigos de verificación, tokens ni NIPs por teléfono, chat o correo.
- Ningún banco necesita tu CVV completo ni tu NIP para "ayudarte" en una llamada.
- Si un supuesto ejecutivo insiste, cuelga y llama tú al banco.
- Si un enlace te pide credenciales, entra escribiendo tú la dirección del sitio, no desde el link.

---

## 22.7 Regla anti-gancho: si suena demasiado bueno...

**Idea clave**

Fraudes de inversión, apuestas, trading, cripto, bienes raíces o negocios usan promesas exageradas: "garantizado", "sin riesgo", "rendimiento fijo altísimo". El gancho es exactamente eso: sonar mejor que cualquier cosa legítima del mercado.

**Cómo aplicarla**

- Compara siempre con alternativas formales (bancos, CETES, fondos, sofipos) y revisa qué tasas manejan.
- Desconfía de cualquiera que ofrezca rendimiento fijo muy por encima del mercado y sin explicar riesgos.
- Evita mezclar amistad/romance con decisiones de inversión; mezcla explosiva.

- No metas dinero que no puedes permitirte perder en esquemas que no estén regulados y supervisados.

---

## 22.8 Regla de la trazabilidad: prefiere canales formales

**Idea clave**

El efectivo, las gift cards, las remesas informales y los tratos en efectivo "sin papel" son terreno fértil para el fraude y para que no puedas demostrar nada después. Entre más trazado quede, más fácil defenderte.

**Cómo aplicarla**

- Paga y cobra por medios electrónicos cuando sea posible; deja rastro.
- Pide facturas o recibos por servicios importantes; guarda contratos y comprobantes.
- Evita pagar deudas, compras o servicios con gift cards y criptos cuando la otra parte lo exige.
- Si alguien te pide manejar dinero "por fuera" para evitar impuestos, pregúntate qué más quiere evitar.

---

## 22.9 Regla de hablarlo en casa (defensa familiar)

**Idea clave**

Fraudes a adultos mayores, jóvenes y niños funcionan mejor cuando hay **silencio**. Si cada quien vive sus miedos por separado, el estafador juega uno por uno.

**Cómo aplicarla**

- Hablen en familia, al menos una vez al año, de estafas comunes: llamadas falsas, WhatsApp, secuestro virtual, inversiones milagro.
- Tengan acuerdos: si alguien recibe una llamada rara, cuelga y avisa al grupo familiar.
- Establezcan palabra clave o preguntas que solo ustedes conozcan para emergencias.
- Ayuda a los más vulnerables (adultos mayores, adolescentes) a configurar bien sus dispositivos y redes.

---

## 22.10 Regla de denunciar y compartir

**Idea clave**

Al fraude no le conviene el ruido. Cada vez que compartes una experiencia o denuncias, le quitas terreno al estafador y ayudas a que otros no caigan.

**Cómo aplicarla**

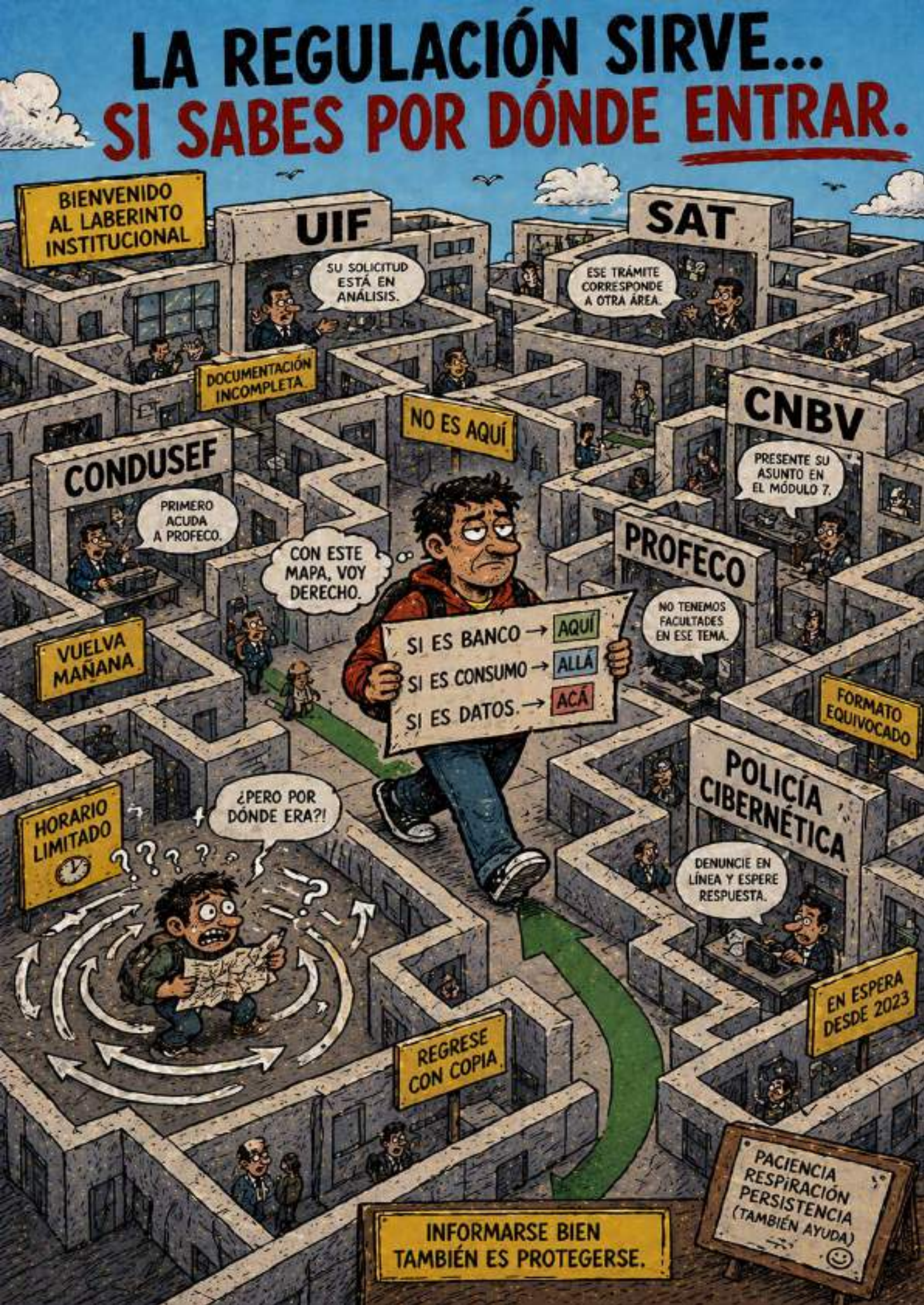
- Reporta intentos de fraude a banco, Condusef, Profeco, Policía Cibernética o autoridades locales.
- Cuenta tu historia (sin datos sensibles) en familia, trabajo o comunidad; convierte tu golpe en vacuna para otros.
- No te avergüences por haber caído: la vergüenza es herramienta del delincuente para que no hables.
- Si eres empresa, documenta y usa cada incidente como caso de aprendizaje interno.

La regulación no es una pared lejana en la CDMX, es un mapa útil si sabes leerlo. No necesitas memorizar leyes ni artículos, solo tener claro quién ve qué y cómo se les toca la puerta. El día que la reacción estándar deje de ser “no sirve de nada denunciar” y pase a ser “sé a quién le toca”, algo habrá cambiado en serio.

# Capítulo 23 — Regulación mexicana básica para ciudadanos y PYMEs

México tiene más leyes, normas y autoridades de las que caben en una tarjeta de presentación; el problema es saber a cuál le toca qué. Entre UIF, SAT, CNBV, Condusef, Profeco, fiscalías y policía cibernética, es fácil terminar diciendo "mejor no hago nada, qué flojera". En este capítulo vamos a hacer lo contrario: un mapa mínimo, en cristiano, de a dónde voltear cuando te estafan, te usan como canal o simplemente huele mal, sin necesidad de volverte experto en acrónimos.

No necesitas ser abogado para usar la ley a tu favor. Este capítulo resume quién es quién en el ecosistema mexicano contra el fraude y el lavado, y qué puede hacer un ciudadano o una PyME con cada uno.


LA REGULACIÓN SIRVE...
SI SABES POR DÓNDE ENTRAR.
BIENVENIDO AL LABERINTO INSTITUCIONAL
UIF
SU SOLICITUD ESTÁ EN ANÁLISIS.
SAT
ESE TRÁMITE CORRESPONDE A OTRA ÁREA.
DOCUMENTACIÓN INCOMPLETA.
NO ES AQUÍ
CNBV
PRESENTE SU ASUNTO EN EL MÓDULO 7.
CONDUSEF
PRIMERO ACUDA A PROFECO.
CON ESTE MAPA, VOY DERECHO.
PROFECO
NO TENEMOS FACULTADES EN ESE TEMA.
SI ES BANCO → AQUÍ
SI ES CONSUMO → ALLÁ
SI ES DATOS → ACÁ
VUELVA MAÑANA
FORMATO EQUIVOCADO
HORARIO LIMITADO
¿PERO POR DÓNDE ERA?!
POLICÍA CIBERNÉTICA
DENUNCIE EN LÍNEA Y ESPERE RESPUESTA.
EN ESPERA DESDE 2023
REGRESE CON COPIA
PACIENCIA
RESPIRACIÓN
PERSISTENCIA
(TAMBIÉN AYUDA)
INFORMARSE BIEN TAMBIÉN ES PROTEGERSE.

## 23.1 UIF y LFPIORPI en una frase

**Qué es**

La **UIF (Unidad de Inteligencia Financiera)** es el cerebro analítico del Estado mexicano contra el lavado: recibe reportes de bancos, SOFIPOs, fintech, notarios, casinos, joyerías y otros sujetos obligados, analiza patrones y presenta casos a la FGR. La **LFPIORPI** (Ley Federal para la Prevención e Identificación de Operaciones con Recursos de Procedencia Ilícita) es la famosa "Ley Antilavado" que obliga a ciertas actividades vulnerables a identificar clientes, integrar expedientes y enviar avisos al SAT/UIF.

**Qué te importa como ciudadano o PyME**

- Si prestas servicios o vendes bienes listados como **actividad vulnerable** (inmuebles, autos, joyería, casinos, tarjetas prepagadas, outsourcing, etc.), tienes obligaciones ante SAT/UIF: avisos, integración de expedientes, límites de efectivo.
- Si eres cliente, debes saber que cuando te piden datos PLD no es "porque sí", sino porque la ley lo exige en ciertos casos.

---

## 23.2 SAT — Portal Antilavado y obligaciones básicas

**Qué es**

El **SAT** administra el Portal de Prevención de Lavado de Dinero (**SPPLD**) donde se registran quienes realizan actividades vulnerables, se envían avisos y se consultan obligaciones. El objetivo de la LFPIORPI es proteger el sistema financiero y la economía nacional, imponiendo medidas para prevenir y detectar operaciones ilícitas.

**Qué deberías tener claro si eres PyME**

- Debes revisar si tu giro entra en la lista del artículo 17 de la LFPIORPI (actividades vulnerables).
- Si sí, te toca:
    - Registrarte en el portal del SAT antilavado.
    - Identificar a tus clientes cuando rebasan ciertos montos.
    - Integrar expedientes con documentación básica (ID, RFC, comprobantes, etc.).
    - Presentar avisos mensuales cuando superas umbrales.

- No cumplir no solo es multa: puede interpretarse como facilitar operaciones con recursos de procedencia ilícita.

---

## 23.3 CNBV y regulación de bancos, fintech, SOFIPOs

**Qué es**

La **CNBV** supervisa entidades financieras: bancos, casas de bolsa, SOFIPOs, SOFOMES reguladas, fintech de la Ley para Regular las Instituciones de Tecnología Financiera, entre otras. Emite disposiciones de carácter general en materia de PLD/FT: manuales, oficial de cumplimiento, matrices de riesgo, modelos, capacitación, reportes de operaciones inusuales y relevantes.

**Qué te importa**

- Si eres cliente: CNBV marca el estándar mínimo de lo que tu banco o fintech debe hacer para protegerte (aunque a veces se queden cortos en la práctica).
- Si eres institución regulada: estás obligado a tener un sistema de PLD robusto; el "manual en PDF y ya" no alcanza.
- Si algo sale mal y hay negligencia grave, la CNBV puede imponer multas fuertes y medidas correctivas.

---

## 23.4 Condusef y Profeco — dónde quejarte cuando te pegan

**Qué es**

La **Condusef** atiende controversias entre usuarios y entidades financieras (bancos, aseguradoras, Afores, sofomes, fintech reguladas). La **Profeco** se encarga de relaciones de consumo en general: comercio electrónico, servicios, compras, publicidad engañosa.

**Qué puedes hacer**

- Si te cargaron algo en tarjeta que no reconoces, si un banco o fintech no responde sobre un posible fraude, puedes ir a Condusef para conciliación y asesoría.
- Si un comercio o plataforma te estafó (productos, servicios, cláusulas abusivas), Profeco es la puerta para quejarte y buscar reparación.

- En ambos casos, llegar con documentación ayuda: estados de cuenta, correos, contratos, capturas.

---

## 23.5 Policía Cibernética, Fiscalía y denuncias

**Qué es**

La **Policía Cibernética** (a nivel federal y en estados como CDMX) recibe reportes de fraudes en línea, phishing, extorsiones, suplantación de identidad y otros delitos digitales. La denuncia penal formal se presenta ante la **Fiscalía local o la FGR**, según el caso.

**Canales clave (ejemplos)**

- 911 para emergencias inmediatas.
- Líneas como 088 o contactos de Policía Cibernética federal para reportar intentos de fraude o ciberdelitos.
- Portales de denuncia electrónica en sitios de CNS/SSC/Fiscalías donde se pueden adjuntar evidencias (capturas, correos, chats).

**Por qué denunciar aunque "no me vayan a regresar el dinero"**

- Tu caso alimenta investigaciones mayores y estadísticas.
- Ayuda a detectar patrones y redes (mismas cuentas, mismos números, mismos correos).
- Aumenta la presión para mejorar regulación y respuesta de autoridades.

---

## 23.6 LFPDPPP — tus datos personales

**Qué es**

La **Ley Federal de Protección de Datos Personales en Posesión de los Particulares (LFPDPPP)** regula cómo empresas, despachos, apps y comercios manejan tus datos personales. Les obliga a tener avisos de privacidad, seguridad adecuada y a respetar tus derechos ARCO (Acceso, Rectificación, Cancelación, Oposición).

**Qué puedes exigir**

- Saber qué datos tuyos tienen y para qué los usan.
- Pedir rectificación o cancelación cuando proceda.
- Oponerte a ciertos usos (por ejemplo, fines mercadotécnicos).

- Denunciar ante el INAI cuando una empresa no responda o filtre tus datos por negligencia.

---

## 23.7 Para el ciudadano: mapa mínimo de acción

**Qué hacer ante…**

- Cargo no reconocido: reporta al banco de inmediato, exige aclaración, usa Condusef si no te resuelven.
- Estafa de e-commerce: guarda evidencia y acude a Profeco; si hay montos altos, también Fiscalía.
- Extorsión o fraude digital: cuelga, guarda evidencias, reporta a Policía Cibernética y considera denuncia penal.
- Robo de identidad: bloquea productos, levanta reporte con bancos, buró de crédito, Condusef y Fiscalía.

---

## 23.8 Para la PyME: mapa mínimo de acción

**Checklist rápido**

- Verifica si eres **actividad vulnerable** LFPIORPI; si sí, regístrate en SPPLD y cumple.
- Ten políticas internas básicas de PLD y antifraude (al menos flujos de pago, cambios de cuenta, alta de proveedores).
- Capacita personal aunque sea con sesiones cortas mensuales: tipos de fraude, señales de alerta, a quién avisar.
- Usa banca en línea con permisos y límites diferenciados, no una sola token para todo.
- Documenta todo incidente: te servirá para Condusef, Profeco, aseguradora y autoridad.

La regulación no es una pared lejana en la CDMX, es un mapa útil si sabes leerlo. No necesitas memorizar leyes ni artículos, solo tener claro quién ve qué y cómo se les toca la puerta. El día que la reacción estándar deje de ser “no sirve de nada denunciar” y pase a ser “sé a quién le toca”, algo habrá cambiado en serio.

---

# Capítulo 24 — Checklists de defensa rápida (hogar y PyME)

En momentos de crisis, tu cerebro no piensa en manuales de 200 páginas, piensa en listas cortas y claras. Hogar, familia, negocio y reacción ante incidente necesitan exactamente eso: recordatorios simples que puedas seguir incluso con el corazón acelerado. Este capítulo es el lado nerd del libro: checklists que parecen básicos hasta que te das cuenta de que casi nadie los tiene escritos, menos pegados en la pared donde sí se ven.

Aquí no hay teoría, solo listas prácticas para que cualquier persona o negocio revise si está mínimamente protegido.

# LA LISTA QUE ODIAN LOS ESTAFADORES

LA MEJOR DEFENSA: ESTAR ATENTOS JUNTOS

| HOGAR | NEGOCIO | REACCIÓN |
|---|---|---|
| ☑ PALABRA CLAVE FAMILIAR | ☑ DOBLE VERIFICACIÓN DE PAGOS | ☑ SI ALGO NO CUADRA, PAUSAMOS |
| ☑ NO COMPARTIMOS CÓDIGOS | ☑ VALIDAMOS CAMBIOS DE CUENTA | ☑ NÚMERO DE DENUNCIA A LA MANO |
| ☑ VERIFICAMOS ANTES DE PAGAR | ☑ CONTRASEÑAS SEGURAS Y ÚNICAS | ☑ GUARDAMOS EVIDENCIAS |
| ☑ USAMOS DOBLE VERIFICACIÓN | ☑ CAPACITAMOS A NUESTRO EQUIPO | ☑ BLOQUEAMOS Y REPORTAMOS |
| ☑ RESPALDO DE INFORMACIÓN | ☑ RESPALDO DE INFORMACIÓN | ☑ PEDIMOS APOYO SIN VERGÜENZA |
| ☑ HABLAMOS EN FAMILIA SOBRE ESTAFAS | ☑ REVISAMOS PROVEEDORES Y ALIADOS | ☑ APRENDEMOS, MEJORAMOS, PROTEGEMOS |

SE BUSCA: VÍCTIMA ~~DISTRAÍDA~~

PLAN MAESTRO DE FRAUDE

PYME CON ORGULLO

NOS TIENEN BIEN PREPARADOS ESTOS...

PLAN FAMILIAR Y DE NEGOCIO

UNIDOS + ALERTAS = SEGUROS ☺

PREVENIR ES GANAR

## 24.1 Checklist hogar y familia

**Cuentas y accesos**

- El correo principal de cada adulto tiene doble factor de seguridad activado.
- Nadie reutiliza la misma contraseña en correo, banca y redes sociales.
- Se usa al menos un gestor de contraseñas en la familia (aunque sea el básico).

**Teléfonos y mensajería**

- Todos tienen bloqueos de pantalla con PIN, huella o reconocimiento.
- WhatsApp (y similares) tienen activada la verificación en dos pasos.
- Nadie comparte códigos por SMS (WhatsApp, banco, correo, apps).

**Reglas familiares**

- Está hablada y entendida la regla: si hay prisa, colgamos y confirmamos por otro canal.
- Hay una palabra clave o pregunta secreta para validar emergencias.
- Los adultos mayores saben que "Hacienda, bancos y premios" no llaman para pedir códigos.

**Compras y pagos**

- Se revisan estados de cuenta bancarios al menos una vez al mes.
- Se evita pagar con tarjetas en sitios muy desconocidos o sin candado HTTPS.
- Nadie paga servicios o "deudas" con gift cards si se lo piden por teléfono o mensaje.

---

## 24.2 Checklist PyME — personas y cultura

**Conciencia interna**

- Se han dado al menos 2–3 sesiones de capacitación al año sobre fraudes comunes (BEC, invoice fraud, WhatsApp, SPEI).
- Todo empleado sabe a quién reportar un correo, llamada o mensaje raro.
- Se comparten casos reales (propios o públicos) en juntas, sin culpar pero sí aprendiendo.

**Reglas básicas de operación**

- Está escrito que ningún pago importante se autoriza solo por correo o chat.
- Cambios de cuenta de proveedores siempre se validan por segundo canal.

- Nunca se comparte token, NIP o claves por teléfono, ni aunque llame “el banco”.

---

## 24.3 Checklist PyME — tecnología básica

**Correo y dominios**

- El dominio corporativo tiene configuración mínima de seguridad (SPF, DKIM, DMARC básico).
- Se evita usar correos genéricos gratuitos para funciones críticas (cobranza, pagos, facturación).
- Hay filtros de correo para phishing y spam, no solo el del proveedor default.

**Equipos y redes**

- Todos los equipos tienen antivirus/endpoint de empresa, actualizado.
- El Wi-Fi de la oficina tiene contraseña robusta y separado red invitados de red interna.
- Se hacen actualizaciones de sistema operativo y software periódicamente.

**Accesos y permisos**

- No todos los usuarios son administradores; cada quien tiene solo lo que necesita.
- Se revisan accesos cuando alguien entra o sale de la empresa.
- Hay al menos un respaldo periódico de información crítica (contabilidad, clientes, contratos).

---

## 24.4 Checklist PyME — finanzas y procesos

**Pagos y SPEI**

- Existen límites diarios y por operación acordes al tamaño de la empresa.
- Hay doble autorización para pagos mayores a cierto monto.
- Se realizan transferencias de prueba para cuentas nuevas importantes.

**Proveedores y clientes**

- Se verifica existencia básica de proveedores: RFC, domicilio, teléfono, web.
- No se trabaja con proveedores que no dan factura o piden manejar todo en efectivo.
- Se revisan periódicamente listas negras (SAT 69-B) para evitar EFOS.

**Controles contables**

- Conciliaciones bancarias mensuales (idealmente semanales) sin “partidas huérfanas”.
- Nadie puede iniciar y aprobar pagos de forma individual (segregación de funciones).
- Se revisan inventarios físicos vs. contables al menos una vez al año.

---

## 24.5 Checklist de reacción ante incidente

**Si crees que fuiste víctima de fraude o hackeo**

- Cambias inmediatamente contraseñas de correo, banca y servicios afectados.
- Avisas a tu banco y bloqueas productos o accesos comprometidos.
- Documentas: capturas de pantalla, correos, mensajes, folios, nombres.
- Presentas reporte ante Policía Cibernética y consideras denuncia ante Fiscalía.
- Informas internamente (familia o empresa) para que nadie más caiga por el mismo vector.

Un buen checklist es humilde y poderoso: no presume, pero salva. Tener por escrito qué hacer en casa, en el negocio y durante un incidente no te vuelve paranoico, te vuelve predecible en los momentos en que el cerebro quiere huir. Si la lista solo existe en tu cabeza, en realidad no existe.

# Capítulo 25 — Casos prácticos de defensa

La teoría se olvida; la historia bien contada, no. Llamada del “banco”, WhatsApp del “familiar”, inversión garantizada, correo del “CEO” y chamba remota de “gestionar pagos” ya le pasaron a alguien que conoces, aunque no lo haya dicho en voz alta. Aquí vamos a recrear esos momentos incómodos y a poner en cámara lenta qué se pudo haber hecho distinto, para que la próxima vez tu yo del futuro pueda presumir que sí colgó, sí preguntó o sí dijo “no”.

Este capítulo aterriza todo en escenas concretas: qué pasa, qué sientes, qué haría la mayoría… y qué deberías hacer tú para salirte del guion del estafador.


TEATRO DE LA PREVENCIÓN
HOY: 5 ESCENAS QUE LOS ESTAFADORES ODIAN
1 LA LLAMADA DEL "BANCO"
SOMOS DE SU BANCO. HAY UN CARGO SOSPECHOSO. ¿ME DA SUS DATOS?
VOY A LLAMAR YO AL NÚMERO OFICIAL.
CLICK
2 EL WHATSAPP DEL "HIJO"
Hijo
En línea
¡Papá, se me bloqueó el celular! Este es mi número nuevo.
¿Me ayudas con $5,000? Es urgente
11:47
MÁNDAME NOTA DE VOZ CON LA PALABRA CLAVE.
3 LA INVERSIÓN MILAGROSA
CON SOLO $10,000 HOY, MAÑANA SERÁS MILLONARIO. SIN RIESGOS. 100% SEGURO.
RENDIMIENTOS IMPRESIONANTES!!!
GARANTIZADO
1000%
MÁNDAME CONTRATO Y RFC PRIMERO.
4 EL CORREO DEL "CEO"
De: ceo@empresa.com
Para: pagos@empresa.com
Asunto: Urgente
Necesito que hagas la transferencia de inmediato a esta cuenta nueva. Es confidencial.
– CEO
URGENTE
CONFIRMO POR OTRO CANAL.
5 TRABAJO REMOTO "FÁCIL"
TRABAJO REMOTO
ALTAS GANANCIAS
POCO ESFUERZO
SIN EXPERIENCIA
SOLO NECESITAMOS QUE MUEVAS DINERO POR TI
SI EL TRABAJO ES MOVER DINERO, EL PRODUCTO SOY YO.
¡CORTO!
CINCO MINUTOS DE CRITERIO
VALEN MÁS QUE
CINCO AÑOS DE PLEITO.

## 25.1 “Me llamaron del banco por un cargo raro”

**Escena**

Te entra una llamada. En el identificador, aparece el nombre de tu banco. La persona al otro lado conoce tu nombre y los últimos dígitos de tu tarjeta. Te dice que detectaron cargos no reconocidos y que, para “cancelarlos”, necesita que le dictees el número completo de tu tarjeta, fecha de vencimiento y el código que te va a llegar por SMS.

**Lo que suele pasar**

- Te asustas: “me están robando”.
- Piensas: “¿cómo tendría mis datos si no fuera el banco?”.
- Le dictas el código que llegó por SMS “para cancelar”. En realidad autoriza una compra o acceso.
- Minutos después ves retiros o transferencias que tú mismo facilitaste.

**Lo que deberías hacer**

- Recuerda la regla: ningún banco te pedirá NIP, CVV ni códigos por teléfono.
- Cuelga con educación (“gracias, llamaré yo al banco”) y **marca tú** al número oficial que está en tu tarjeta o app.
- Verifica con el banco si hay cargos; si sí, repórtalos desde la app o por la línea oficial.
- Si ya diste datos, bloquea tarjetas y cuentas, cambia claves y levanta reporte inmediato.

**Qué aprender**

- El spoofing de número es real: que el identificador diga “tu banco” no prueba nada.
- Que tengan algunos datos tuyos solo demuestra que hay filtraciones; no que sean legítimos.
- Siempre tienes derecho a cortar una llamada y volver a marcar por tu cuenta.

---

## 25.2 “Mi hijo / mi mamá me pide dinero por WhatsApp”

**Escena**

Te escribe un número nuevo en WhatsApp: “Mamá, cambié de número, guarda este. Oye, necesito un favor urgente, me bloquearon la app del banco y tengo que pagar algo hoy, me ayudas haciendo una transferencia y al rato te lo regreso”. El estilo de escritura se parece, hay emojis que usaría, quizá hasta una foto de perfil robada.

**Lo que suele pasar**

- Entras en modo protector: quieres ayudar ya.
- No quieres quedar como “desconfiado” con tu familiar.
- Pides la cuenta y haces el SPEI, sin validar fuera de WhatsApp.

**Lo que deberías hacer**

- Aplica la **regla del segundo canal**: llamas al antiguo número o haces videollamada.
- Si no contesta, llama a otra persona cercana (pareja, hermano, amigo) para confirmar.
- No transfieres un peso hasta hablarle por un canal que tú ya tenías.
- Si resulta ser fraude, bloqueas el número, reportas a la plataforma y avisas en grupos familiares.

**Qué aprender**

- Los delincuentes estudian redes sociales para imitar estilo, fotos y contexto.
- Es más importante parecer “desconfiado” que “generoso y estafado”.
- Un audio o una videollamada suelen desenmascarar la suplantación.

---

## 25.3 “Me ofrecieron una inversión con 18–20% garantizado”

**Escena**

Un conocido, colega o incluso familiar te habla de una empresa que paga 18–22% anual “garantizado” si les confías tu ahorro. Te enseñan fotos de oficinas bonitas, coches de lujo, reuniones con coffee break y presentaciones. “No somos banco, pero trabajamos con una SOFOM, está todo bien”. Te dicen que muchos ya entraron y están felices.

**Lo que suele pasar**

- Te da FOMO: “todos están aprovechando menos yo”.
- Te tranquiliza ver gente real, oficinas, logos, influencers.

- Pones una cantidad “para probar”; al principio te pagan puntualmente, como reloj.
- Con el tiempo metes más, o recomiendas a otros. Cuando quieres retirar fuerte, se rompe la magia.

**Lo que deberías hacer**

- Pregunta qué licencia tienen: ¿están regulados por CNBV o Condusef? ¿Figuran en el SIPRES?
- Compara la tasa con CETES, bancos y fondos regulados; si está muy arriba, la palabra clave es riesgo, no milagro.
- Desconfía de rendimientos **fijos** altos sin explicación técnica (qué invierten, cómo gestionan riesgo).
- Si ya entraste, recupera capital lo antes posible y nunca metas dinero de otros bajo tu responsabilidad.

**Qué aprender**

- Muchos esquemas tipo Ponzi en México se disfrazan de “sofom aliada” o “empresa de inversión patrimonial”.
- Que paguen puntualmente al inicio no prueba que sea sano; al contrario, es parte del guion Ponzi.
- Una oficina bonita no sustituye licencias, regulación ni estados financieros auditados.

---

## 25.4 “Mi PyME recibió un correo del ‘CEO’ para hacer un pago urgente”

**Escena**

Eres responsable de tesorería en una PyME. En la bandeja de entrada aparece un correo del director general (DG): “Necesito que hagas hoy mismo una transferencia de X monto a este proveedor, es por un tema de confidencialidad con un cliente grande, te paso datos de la cuenta. Por favor no comentes con nadie, yo me encargo de explicarlo después”. El tono se parece, la firma también.

**Lo que suele pasar**

- Te sientes halagado y presionado: el DG te escribió directamente.
- Quieres cumplir y no quedar mal.
- Si la empresa no tiene reglas claras, haces el pago directo desde banca electrónica.

**Lo que deberías hacer**

- Revisar con lupa el correo: dominio, hilos previos, forma de escribir.
- Aplicar política interna: ningún pago extraordinario se hace sin doble autorización y validación por segundo canal.
- Llamar o mandar mensaje interno al DG (Teams, WhatsApp conocido) para confirmar.
- Si algo suena raro, escalar a Compliance o a otro director antes de mover un peso.

**Qué aprender**

- El BEC explota jerarquías y ego; la validación es un acto de responsabilidad, no de rebeldía.
- Un proceso escrito que diga "aunque el DG lo pida, se aplica protocolo" te protege también a ti.
- El correo es fácil de imitar; la voz por un canal conocido y el workflow, no tanto.

---

## 25.5 "Me llegó una oferta de trabajo remoto que suena demasiado fácil"

**Escena**

Ves en redes una oferta: "Gana desde casa ayudando a empresas a procesar pagos. Solo necesitas una cuenta bancaria, WhatsApp y unas horas al día. No se requiere experiencia". Te dicen que recibirás depósitos en tu cuenta y solo tendrás que reenviarlos a otras cuentas, quedándote con una comisión.

**Lo que suele pasar**

- Lo ves como ingreso extra "legal".
- Comienzas a recibir transferencias de personas que no conoces y envías el dinero a otras cuentas, quedándote con un porcentaje.
- Un día te bloquean la cuenta o te busca el banco/autoridad por operaciones vinculadas a fraude o lavado.

**Lo que deberías hacer**

- Reconocer que eso es una **mula financiera**: están usando tu cuenta como lavadero.
- No aceptar trabajos donde tu principal "función" es mover dinero de terceros.
- Si ya empezaste, detente, informa al banco y documenta todo por si hay investigación.
- Nunca uses tu cuenta personal para negocios ajenos sin contratos y facturación formal.

**Qué aprender**

- Si te pagan solo por “prestar tu cuenta”, es casi seguro que hay delito detrás.
- La responsabilidad legal no desaparece porque “tú no sabías”; tu cuenta está a tu nombre.
- Es mejor decir que no a un ingreso dudoso que tirar años de historial limpio.

---

## 25.6 “Compré en una tienda muy barata de redes y nunca llegó”

**Escena**

Ves un anuncio en Instagram/TikTok: productos de marca, muy baratos, con fotos bonitas y comentarios positivos. Pagas por transferencia o por una pasarela poco conocida. El pedido nunca llega o llega algo distinto y luego la página desaparece.

**Lo que suele pasar**

- Al principio piensas que es retraso logístico.
- Escribes a “soporte” y te dan largas o ya ni responden.
- Cuando quieres denunciar, la página, el perfil y el número ya no existen.

**Lo que deberías hacer**

- Antes de comprar, revisa: dominio, reseñas fuera de su propia página, RFC, domicilio, políticas claras.
- Desconfía de tiendas que solo aceptan transferencia, sin tarjeta ni plataformas conocidas.
- Para montos relevantes, prefiere comercios establecidos o marketplaces con protección al comprador.
- Si ya fuiste víctima, guarda evidencia y acude a Profeco; si hay montos altos o patrón, también a Fiscalía.

**Qué aprender**

- El “demasiado barato” también aplica para e-commerce.
- Los comentarios pueden ser falsos; busca reseñas externas y señales de presencia real.
- Tu experiencia negativa puede ayudar a otros si la compartes y denuncias.

---

## 25.7 “En mi empresa alguien está robando o haciendo trampa, ¿y ahora?”

**Escena**

Eres dueño o directivo de PyME. Empiezas a notar que el margen ya no cuadra, que ciertos gastos crecen sin explicación o que algunos proveedores siempre ganan. Sospechas pero no quieres “hacer escándalo” ni confrontar sin pruebas.

**Lo que suele pasar**

- Dejas pasar meses esperando que se “corrija solo”.
- Das mensajes ambiguos de “cuidemos los recursos” sin acciones concretas.
- El fraude continua y se normaliza; la gente honesta se desmotiva.

**Lo que deberías hacer**

- Documentar: inventarios, conciliaciones, gastos, proveedores, patrones.
- Pedir auditoría interna o externa, aunque sea focalizada.
- Revisar y reforzar controles: segregación de funciones, límites de autorización, revisiones sorpresivas.
- Crear canal confidencial de denuncia interna y proteger al que señale irregularidades.

**Qué aprender**

- El silencio favorece al defraudador, no a la reputación de la empresa.
- La mayoría de fraudes corporativos se descubren por alertas internas que nadie atendió.
- Corregir controles hoy es más barato que enfrentar un escándalo mañana.

---

## 25.8 “Mi correo fue hackeado y mandó mensajes pidiendo dinero”

**Escena**

Te avisan amigos o clientes: “Oye, me escribiste que necesitabas dinero y un favor urgente, ¿todo bien?”. Entras a tu correo y ves mensajes que tú no escribiste. Quizá ya no puedes entrar porque la contraseña fue cambiada.

**Lo que suele pasar**

- Te da pena y piensas que solo es “un virus”.
- Cambias la contraseña y sigues como si nada.

- No dimensionas que desde ese correo pueden resetear tus demás cuentas.

**Lo que deberías hacer**

- Recuperar el acceso (si aún puedes) o usar procesos de recuperación con máximo cuidado.
- Activar 2FA en ese correo y en todos los servicios ligados a él.
- Revisar filtros, reenvíos y dispositivos conectados; eliminar lo que no reconozcas.
- Avisar a tus contactos que ignoren y borren mensajes raros que hayan recibido tu "yo hackeado".

**Qué aprender**

- El correo es el eslabón central de tu vida digital; protegerlo es prioridad uno.
- Los atacantes pueden usarlo como base para resets de banca, redes y tiendas.
- Avisar a tu red es parte de la contención del daño.

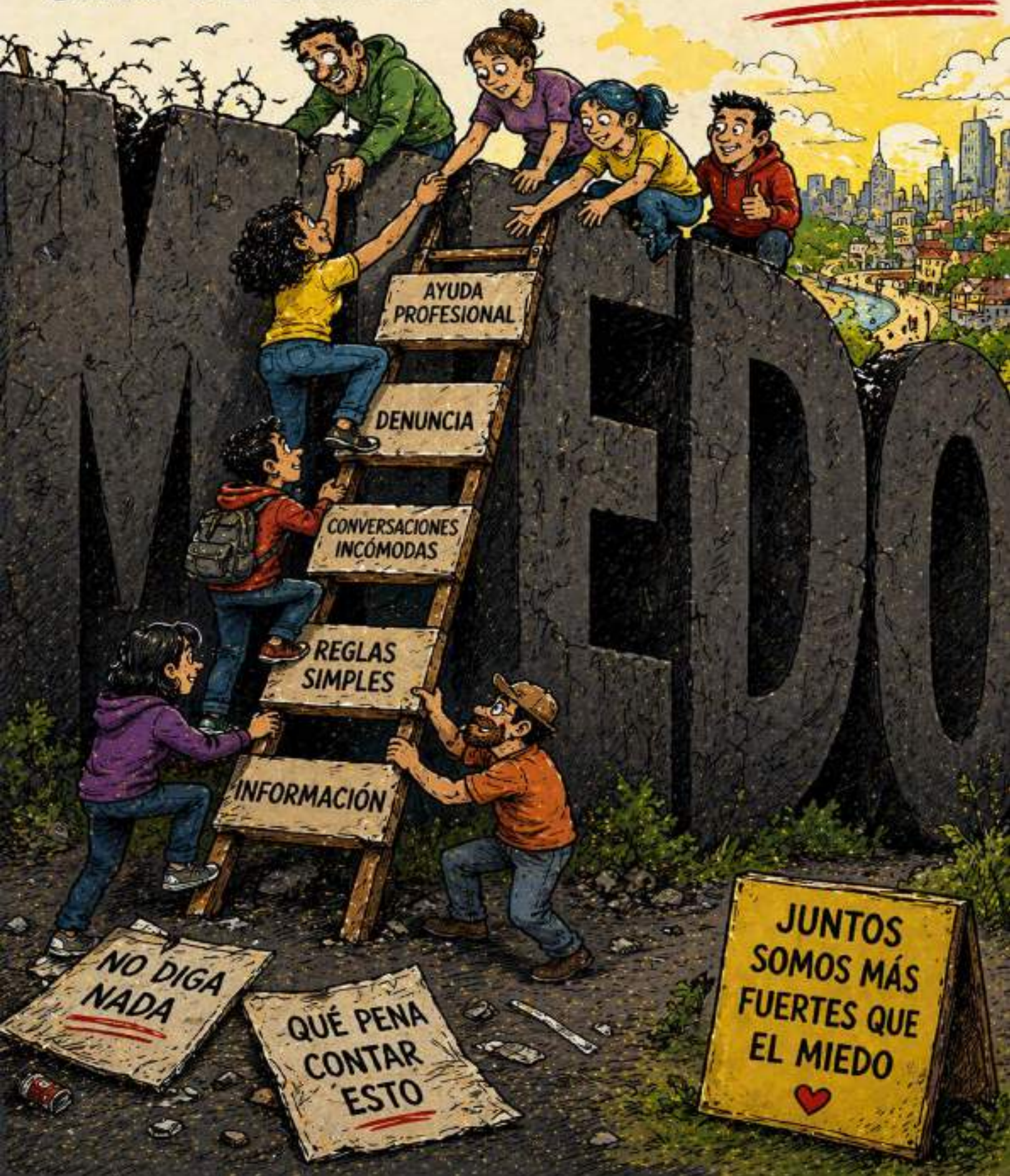
Los casos reales no están ahí para que digas "qué tonto el que cayó", sino "yo pude haber sido esa persona". La diferencia entre una anécdota vergonzosa y una historia que termina bien casi siempre son cinco minutos de incomodidad: hacer la pregunta, colgar, verificar, decir "no". Este capítulo no busca asustarte, busca que cuando te toque la escena, sientas que ya la habías ensayado.

# Capítulo 26 — Cierre: del miedo al criterio

Si después de leer todo esto te queda la sensación de que el mundo es una trampa gigante, algo hicimos mal. La idea no es que vivas paranoico, sino que dejes de vivir en piloto automático: el miedo sirve solo si se convierte en criterio y en conversación. En este capítulo cerramos el mapa, aterrizamos cómo usar el manual sin volverte policía de todo y te propongo algo radicalmente subversivo: hablar de estos temas sin pena, como quien comparte una receta para que a otros no les vuelva a salir crudo.

Este manual no busca que vivas con miedo, sino que conviertas el miedo en criterio práctico. El fraude y el lavado no se van a terminar, pero tú puedes volverte un blanco mucho más difícil.

# NO SE TRATA DE NO TENER MIEDO, SINO DE SABER QUÉ HACER CON ÉL.



## 26.1 Lo que ya sabes (aunque no seas experto)

Después de leer los capítulos anteriores, ya no ves el fraude como "cosas que le pasan a otros". Ahora sabes que se cuela por llamadas, apps, inversiones, empresas, offshores, juegos, ONGs, iglesias, tokens y proyectos verdes. También sabes que la mayoría de ataques no rompen tecnología, sino decisiones: empujan emociones, sesgos y prisas.

---

## 26.2 Cómo usar este manual en la vida real

Piensa este libro como un **MAPA + BOTIQUÍN**. El mapa son las tipologías: cuando veas algo raro, podrás decir "esto se parece a BEC", "esto huele a pig butchering", "esto suena a APP fraud". El botiquín son las reglas de defensa, los checklists y los casos prácticos.

Cómo aplicarlo:

- Antes de tomar decisiones grandes (créditos, inversiones, compras, cambios de procesos en tu PyME), revisa el índice y lee el capítulo que más se parezca a lo que vas a hacer.
- Usa los checklists de los Capítulos 22–24 como listas de verificación anuales en familia y empresa.
- Toma los casos del Capítulo 25 para talleres internos: léelos en voz alta y pregúntale a la gente "¿qué harías tú?".

---

## 26.3 Mantenerlo vivo (fraude 2030)

El fraude evoluciona más rápido que los manuales: nuevas apps, nuevos medios de pago, nuevas regulaciones, nuevas guerras y crisis. Tal vez en 2030 haya cosas que aquí no existían (o que aún eran marginales), pero los **principios** seguirán vigentes:

- Regla del segundo canal.
- Desconfianza proporcional al monto.
- Identidad y correo raíz blindados.
- Duda sistemática ante urgencias y ofertas "únicas".

Actualiza este manual cada cierto tiempo: añade ejemplos, notas, recortes de noticia, experiencias propias.

---

## 26.4 Del “me da pena” al “me da poder”

Mucha gente no habla de fraude porque le da pena “haber caído”. Esa vergüenza es uno de los activos más valiosos del delincuente. Si en cambio conviertes tu experiencia en historia compartida, te pasa algo importante:

- Recuperas parte del control: tú decides qué hacer con lo que te ocurrió.
- Ayudas a que otros no paguen “la misma colegiatura”.
- Presionas a bancos, fintech, autoridades y empresas para mejorar sus defensas.

Hablar del fraude no te hace débil, te hace **referente** para tu comunidad.

---

## 26.5 Tu lugar en la defensa sistémica

Gobiernos, bancos, UIF, CNBV, SAT, Condusef, Profeco, INAI y policías tienen responsabilidades enormes. Pero el primer firewall real está en la cabeza de cada persona que decide no dar un código, no firmar a ciegas, no hacer un pago bajo presión.

Cada vez que:

- dices “no voy a hacer esa transferencia hasta confirmar”,
- acompañas a alguien vulnerable a revisar su correo o su banca,
- denuncias y documentas,

estás empujando el sistema entero un centímetro hacia un lugar más sano.

El miedo sin acción es solo ruido interno; el miedo con reglas y conversación se vuelve herramienta. No vas a eliminar los riesgos, pero sí puedes dejar de caminar con los ojos cerrados. Si algo te llevas de este libro, que sea esto: pensar antes de hacer clic no es exagerar, es el nuevo respirar hondo.

---

# Capítulo 27 — Glosario esencial

Nada aleja más a la gente de un tema importante que un idioma que parece inventado para que solo lo entiendan tres personas en traje. Lavado, fraude, cibercrimen y regulación se han llenado de siglas y tecnicismos que, si nadie traduce, se vuelven una forma elegante de excluir. Este último capítulo es el antídoto: un glosario en lenguaje de mesa familiar para que, la próxima vez que alguien suelte “APP fraud”, “TBML” o “mulas financieras”, no tengas que asentir con cara de “claro” mientras piensas “ni idea”

Glosario rápido para no perderse entre siglas y términos. Definiciones pensadas para comunidad, no para examen de certificación.

# PONERLE NOMBRE A LAS COSAS ES EMPEZAR A DEFENDERSE

## 27.1 Siglas y actores clave

- **AML / PLD**: Anti-Money Laundering / Prevención de Lavado de Dinero. Conjunto de leyes, procesos y controles para evitar que dinero criminal se mezcle con la economía formal.
- **UIF**: Unidad de Inteligencia Financiera. Analiza reportes de operaciones sospechosas y presenta casos a la Fiscalía.
- **LFPIORPI**: Ley Federal para la Prevención e Identificación de Operaciones con Recursos de Procedencia Ilícita ("Ley Antilavado"). Define actividades vulnerables, umbrales, avisos y obligaciones.
- **CNBV**: Comisión Nacional Bancaria y de Valores. Supervisa bancos y entidades financieras reguladas y emite reglas PLD.
- **SAT**: Servicio de Administración Tributaria. Recauda impuestos y opera el portal antilavado (SPPLD) para actividades vulnerables.
- **Condusef**: Comisión Nacional para la Protección y Defensa de los Usuarios de Servicios Financieros. Atiende quejas entre clientes y entidades financieras.
- **Profeco**: Procuraduría Federal del Consumidor. Atiende abusos y fraudes en relaciones de consumo (comercio, servicios, e-commerce).
- **INAI / LFPDPPP**: Instituto Nacional de Transparencia y Ley Federal de Protección de Datos Personales en Posesión de los Particulares. Protegen tus datos personales y tus derechos ARCO.

---

## 27.2 Tipologías de fraude y lavado

- **APP fraud (Authorized Push Payment)**: Fraude donde la víctima autoriza una transferencia o pago engañada, creyendo que paga algo legítimo (proveedor, familiar, autoridad).
- **BEC (Business Email Compromise)**: Compromiso de correo empresarial para instruir pagos falsos, cambiar cuentas de proveedores o robar información.
- **TBML (Trade-Based Money Laundering)**: Lavado basado en comercio exterior; se manipulan facturas, cantidades y precios en importaciones/exportaciones.
- **RaaS (Ransomware-as-a-Service)**: Modelo en el que desarrolladores de ransomware alquilan sus herramientas a afiliados, que lanzan ataques a cambio de una parte del rescate.
- **Pig butchering**: Estafa donde mezclan romance/amistad con falsa inversión cripto; primero "engordan" tu confianza, luego te sacan todo el capital.

- **Rug pull**: Abandono repentino de un proyecto cripto/DeFi/NFT por parte de sus creadores tras captar liquidez o vender tokens, dejando a inversores con activos sin valor.
- **Wash trading**: Comprar y vender el mismo activo (token, NFT, acción) entre cuentas controladas por la misma persona para inflar precio o volumen.
- **Chain-hopping**: Mover cripto entre diferentes blockchains para complicar el seguimiento de fondos.

---

## 27.3 Herramientas, canales y técnicas

- **Deepfake**: Contenido de audio o video sintético generado con IA que imita la voz o la cara de una persona real.
- **Phishing / Vishing / Smishing**: Phishing por correo, vishing por llamada de voz, smishing por SMS o mensajería, para robar datos o credenciales.
- **SIM swap**: Robo de línea telefónica mediante cambio de SIM en la compañía, para recibir códigos SMS y tomar cuentas.
- **Man-in-the-Middle (MITM)**: Ataque donde alguien se interpone entre tu dispositivo y la red (por ejemplo, Wi-Fi público) para interceptar o alterar comunicaciones.
- **Cryptojacking**: Uso no autorizado de tus recursos (CPU/energía) para minar criptomonedas.
- **Formjacking / Magecart**: Inyección de código malicioso en formularios de pago para robar datos de tarjetas en e-commerce.

---

## 27.4 Conceptos de identidad y cuentas

- **Robo de identidad**: Uso no autorizado de tus datos reales para contratar servicios, pedir créditos o cometer delitos a tu nombre.
- **Identidad sintética**: "Persona" creada mezclando datos reales (p. ej. CURP) con datos falsos; se usa para abrir cuentas y pedir créditos que luego no se pagan.
- **Bust-out**: Estrategia en la que un defraudador construye buen historial de pago para luego maximizar créditos en todas sus líneas y dejar de pagar.
- **Account Takeover (ATO)**: Toma de control de tus cuentas existentes (correo, banca, redes) mediante credenciales robadas o ingeniería social.
- **Mula financiera**: Persona que presta su cuenta para recibir y reenviar dinero de terceros, voluntaria o engañada, convirtiéndose en vehículo de lavado.

---

## 27.5 Empresas y estructuras

- **Empresa fantasma / EFOS**: Compañía sin operaciones reales que emite facturas falsas para simular gastos y mover dinero.
- **EDOS**: Empresas que Deducen Operaciones Simuladas, es decir, que compran facturas falsas para deducir impuestos, aunque sí tengan operación real.
- **Offshore**: Empresa o estructura (sociedad, trust, fundación) en jurisdicción distinta al país de residencia, a veces usada para ocultar patrimonios o lavar.
- **Gatekeepers**: Profesionales como abogados, notarios, contadores y consultores que, por su rol, pueden facilitar (o prevenir) estructuras de lavado y fraude.

---

## 27.6 Pagos, tarjetas y comercio

- **SPEI / CoDi**: Sistemas de pagos electrónicos en México; SPEI para transferencias interbancarias, CoDi para cobros por QR y mensajes de cobro.
- **QR adulterado**: Código QR modificado para enviar pagos a una cuenta distinta a la del comercio legítimo.
- **Gift card laundering**: Uso de tarjetas de regalo para convertir efectivo ilícito en saldos digitales y luego en bienes o efectivo más difícil de rastrear.
- **Triangulation fraud**: Estafa donde un vendedor fraudulento usa tarjeta robada en un comercio legítimo para cumplir pedidos de compradores reales, generando pérdidas al comercio cuando llega el contracargo.

---

## 27.7 Ciberseguridad y respuesta

- **Ransomware**: Malware que cifra tus archivos o sistemas y exige pago (normalmente en cripto) para liberarlos.
- **Backups 3-2-1**: Tres copias de tus datos, en dos tipos de medio, una fuera de línea; estrategia básica contra ransomware.
- **IAB (Initial Access Broker)**: Actor que vende acceso inicial a redes o sistemas comprometidos a otros criminales.
- **Zero trust**: Enfoque de seguridad que asume que ningún usuario o dispositivo es confiable por defecto, aunque esté “dentro” de la red.

El glosario no es un apéndice decorativo, es el traductor entre dos mundos: el de los especialistas y el de la gente a la que realmente afectan las decisiones. Cuando todos

entienden de qué se habla, disminuye el espacio para el humo, el abuso y la simulación. Ponerle nombre claro a las cosas es el primer paso para dejar de normalizarlas.