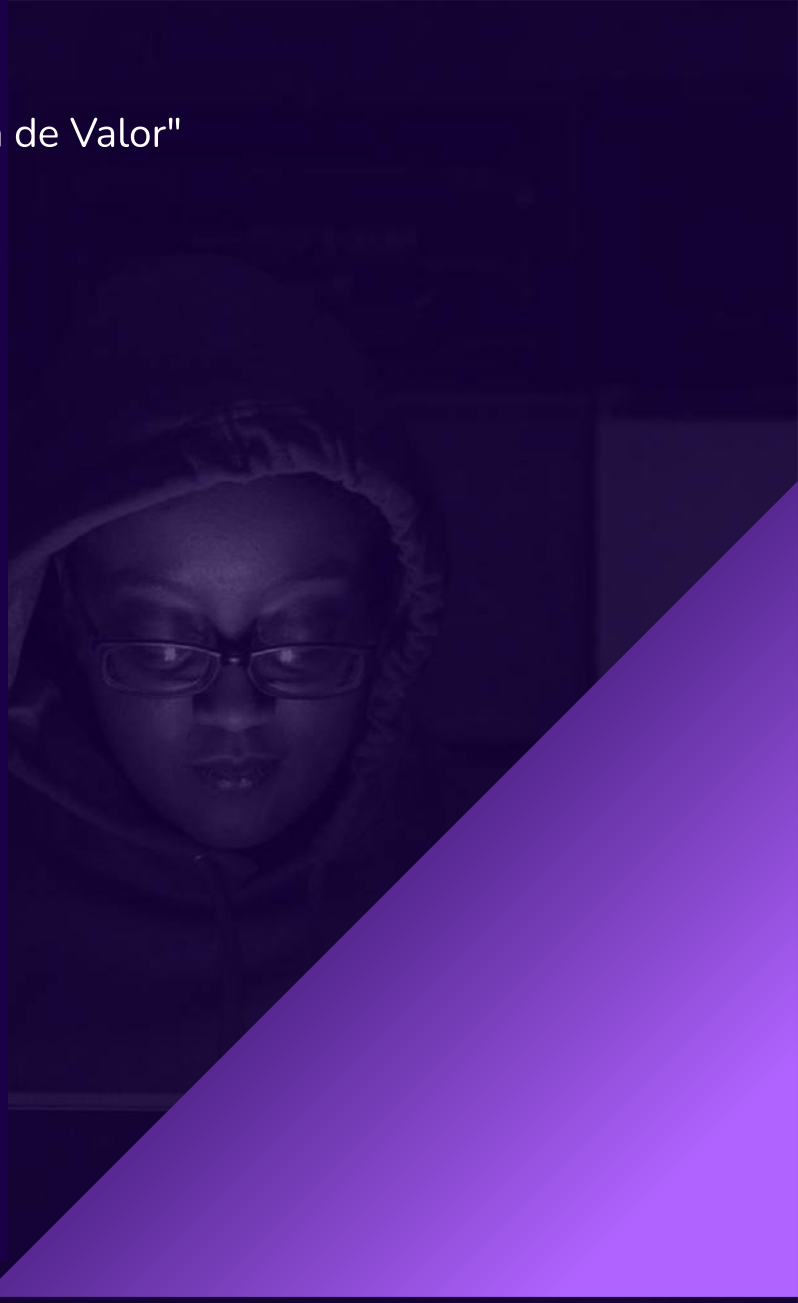
ZCD & Asociados
"Innovación, Evolución y Generación de Valor"

Fraude Digital, Deepfakes y Suplantación de Identidad



Elaborado por:

Lic. Raúl Joel Díaz Zárate

Tabla de **CONTENIDO**

GLOSARIO

- **Account Takeover — ATO**: Apropiación de una cuenta legítima mediante credenciales robadas, SIM swapping, malware, ingeniería social o fallas en los procesos de recuperación de contraseña. El defraudador no crea una cuenta nueva: toma control de una cuenta real.

- **Anti-injection**: Control técnico diseñado para detectar si la imagen, video o señal biométrica que recibe una plataforma proviene de una fuente falsa, pregrabada, manipulada o inyectada artificialmente al sistema.

- **Behavioral Analytics**: Análisis del comportamiento digital de un usuario para identificar patrones normales o anómalos. Puede considerar velocidad de navegación, frecuencia de operaciones, horarios, dispositivo, ubicación, beneficiarios y forma de interacción.

- **Bust-out fraud**: Modalidad en la que una identidad fraudulenta se comporta de forma aparentemente legítima durante un tiempo para generar confianza y después ejecutar un fraude relevante, normalmente mediante créditos, compras o retiros.

- **Cash-out**: Fase final del fraude en la que el defraudador convierte la operación ilícita en beneficio económico. Puede realizarse mediante retiros, transferencias, compras, dispersión de fondos, cuentas mula o activos de fácil reventa.

- **Cuenta mula**: Cuenta bancaria, wallet o perfil digital utilizado para recibir, mover, dividir u ocultar recursos obtenidos mediante fraude u otra actividad ilícita.

- **Deepfake**: Contenido de audio, imagen o video manipulado mediante inteligencia artificial para aparentar que una persona dijo, autorizó o hizo algo que en realidad no ocurrió. Puede utilizarse para suplantar directivos, clientes o usuarios.

- **Device fingerprinting**: Técnica que identifica un dispositivo a partir de sus características digitales, como navegador, sistema operativo, IP, configuración, ubicación, historial de conexión y patrones de uso.

- **Enfoque Basado en Riesgo — EBR**: Metodología que permite aplicar controles proporcionales al nivel de riesgo del cliente, operación, producto, canal, jurisdicción o comportamiento observado.

- **Falso positivo**: Caso en el que una operación legítima es marcada erróneamente como fraudulenta. Puede generar fricción, pérdida de clientes y costos operativos innecesarios.

- **Graph analytics**: Análisis de redes que permite identificar conexiones entre usuarios, cuentas, teléfonos, dispositivos, beneficiarios, IP, domicilios o patrones transaccionales. Es útil para detectar redes de fraude y cuentas mula.

- **Identidad sintética**: Perfil construido mediante la combinación de datos reales y falsos para aparentar legitimidad. Por ejemplo: nombre ficticio, CURP real, domicilio inventado, teléfono válido y documentos editados.

- **Ingeniería social**: Técnica de manipulación utilizada para engañar a una persona y lograr que entregue información, credenciales, códigos de acceso, autorizaciones o datos sensibles.

- **KYC — Know Your Customer**: Proceso de identificación y conocimiento del cliente. Incluye validación documental, perfil transaccional, actividad económica, nivel de riesgo y consistencia de la información proporcionada.

- **KYB — Know Your Business**: Proceso de identificación y conocimiento de una empresa o persona moral. Incluye revisión de estructura corporativa, representantes legales, beneficiarios controladores, actividad económica y riesgos asociados.

- **Logs / bitácoras**: Registros técnicos generados por sistemas digitales. Permiten reconstruir accesos, horarios, IP, dispositivos, intentos fallidos, modificaciones, operaciones y decisiones dentro de una plataforma.

- **Mora temprana fraudulenta**: Incumplimiento de pago que ocurre poco después de otorgarse un crédito y que puede indicar que la solicitud nació con intención de fraude, no con una imposibilidad real de pago.

- **MTU — Monto Transaccional del Usuario**: Límite o parámetro operativo asociado al comportamiento transaccional de un usuario. Cuando se supera, pueden activarse controles adicionales de autenticación, revisión o monitoreo.

- **Onboarding digital**: Proceso de alta, registro o contratación de un cliente mediante canales digitales. Es una etapa crítica porque ahí pueden presentarse documentos falsos, identidades sintéticas o suplantación de identidad.

- **Out-of-band validation**: Validación realizada por un canal distinto al canal principal de operación. Por ejemplo, confirmar una operación desde una aplicación, correo, llamada o dispositivo previamente registrado.

- **Phishing**: Engaño realizado mediante correos electrónicos falsos que simulan provenir de instituciones legítimas para obtener contraseñas, datos bancarios o información personal.

- **Playbook antifraude**: Guía operativa que indica qué hacer ante una tipología específica de fraude: responsables, tiempos, evidencia requerida, criterios de bloqueo, escalamiento y cierre del caso.

- **Red de mulas**: Conjunto de cuentas o personas utilizadas para recibir y dispersar recursos de origen fraudulento, dificultando la trazabilidad del dinero.

- **SIM swapping**: Técnica mediante la cual un defraudador toma control del número telefónico de la víctima para recibir códigos, recuperar contraseñas o acceder a cuentas digitales.

- **Smishing**: Variante del phishing realizada mediante mensajes SMS o aplicaciones de mensajería.

- **Spoofing**: Suplantación técnica de identidad, número telefónico, correo, ubicación, dispositivo, rostro, voz o señal digital.

- **Velocity rules:** Reglas que detectan velocidad anormal en registros, operaciones, accesos, cambios de datos, transferencias o retiros. Sirven para identificar automatización, bots o ataques masivos.

- **Vishing**: Fraude realizado mediante llamadas telefónicas en las que el defraudador simula ser una institución, ejecutivo, proveedor, autoridad o persona de confianza.....

- **Wallet / billetera digital**: Aplicación, cuenta o plataforma digital que permite almacenar, recibir, enviar o administrar dinero electrónico, saldos, tarjetas, medios de pago o activos digitales.

Resumen **EJECUTIVO**

El fraude digital se ha convertido en uno de los riesgos empresariales más relevantes para las organizaciones que operan en entornos digitales, financieros, comerciales y de servicios. Ya no se trata únicamente de operaciones aisladas realizadas mediante engaño, sino de esquemas cada vez más sofisticados que combinan robo de identidad, ingeniería social, uso indebido de datos personales, automatización, inteligencia artificial, deepfakes, identidades sintéticas, phishing, smishing, malware, apropiación de cuentas y manipulación de procesos de onboarding digital. Este fenómeno afecta directamente la seguridad patrimonial de las empresas, la confianza de los usuarios, la continuidad operativa, la reputación corporativa y el cumplimiento regulatorio. En sectores como banca, fintech, casinos online, agregadores de pago, marketplaces, crédito digital, aseguradoras y plataformas tecnológicas, el fraude digital ya no puede verse como un problema meramente tecnológico: debe entenderse como un riesgo legal, operativo, financiero, reputacional y de cumplimiento que exige una respuesta institucional coordinada.

El objetivo de este estudio es proporcionar a la Alta Dirección, áreas de TI y comités de riesgos una visión clara del fraude digital sus principales amenazas, impacto sectorial y las *medidas* preventivas que deben adoptarse para reducir su exposición.

Este fenómeno afecta directamente la seguridad patrimonial de las empresas, la confianza de los usuarios, la continuidad operativa, la reputación corporativa y el cumplimiento regulatorio.

contexto del fraude
DIGITAL EN MÉXICO

El fraude digital se ha convertido en una de las amenazas más relevantes para empresas, instituciones financieras, plataformas tecnológicas y usuarios finales. La digitalización acelerada de los servicios financieros, el comercio electrónico, los pagos electrónicos, el crédito digital y los procesos de contratación remota abrió nuevas oportunidades de negocio, pero también amplió la superficie de ataque para organizaciones criminales.

En México, este fenómeno tiene especial relevancia por el crecimiento de fintech, wallets, agregadores de pago, crédito digital, casinos online, marketplaces, aplicaciones de delivery, plataformas de inversión y servicios financieros no presenciales. La operación digital permite rapidez, inclusión y eficiencia, pero también genera riesgos cuando los controles de identificación, autenticación, monitoreo y trazabilidad no evolucionan al mismo ritmo que las amenazas. El problema central no es la digitalización en sí misma, sino la falta de controles proporcionales al riesgo.

Desde una perspectiva empresarial, el fraude digital debe analizarse como un riesgo integral; afecta ingresos, cartera vencida, experiencia del cliente, reputación, cumplimiento regulatorio, protección de datos personales, prevención de lavado de dinero y continuidad operativa. En otras palabras, ya no basta con que el área tecnológica implemente medidas de seguridad; se requiere una respuesta coordinada entre dirección general, jurídico, cumplimiento, riesgos, auditoría, operaciones, tecnología, atención al cliente y seguridad de la información.

71%

de todos los fraudes financieros en México ya son cibernéticos

CONDUSEF 2023

$20B

MXN reclamados en fraudes cibernéticos en un solo año

CONDUSEF 2023

208

instituciones financieras con suplantación reportada en 2023

CONDUSEF 2023

Digitalización sin controles

Fintech, wallets, crédito digital, casinos online y marketplaces crecieron exponencialmente ampliando la superficie de ataque. La rapidez de adopción superó la madurez de los controles.

Riesgo integral

El fraude afecta ingresos, cartera, reputación, cumplimiento, protección de datos, PLD y continuidad operativa. Ya no puede tratarse como un problema exclusivo del área tecnológica.

Respuesta urgente

En sectores regulados (banca, fintech, AV), el incumplimiento en controles antifraude puede derivar en sanciones CNBV, SAT/UIF, INAI y CONDUSEF de forma simultánea.

Conceptos Clave

Fraude Digital

Cualquier conducta engañosa realizada mediante medios tecnológicos, plataformas digitales, sistemas informáticos o canales electrónicos con el propósito de obtener un beneficio indebido, causar un perjuicio patrimonial o manipular procesos de identificación, autorización, contratación, pago o retiro de recursos.

A diferencia del fraude tradicional, el fraude digital se ejecuta de forma remota, rápida, automatizada y con alto nivel de anonimato, lo que dificulta su detección temprana y persecución posterior.

Identidad Sintética

Combinación de datos reales y falsos para construir un perfil aparentemente legítimo: nombre ficticio + CURP real + domicilio inventado + documentos editados + comportamiento simulado.

Especialmente peligrosa en crédito digital, onboarding remoto, wallets y fintech. El perfil 'crece' en el sistema financiero durante 6-18 meses antes de defraudar (bust-out fraud).

Es la tipología más difícil de detectar con controles documentales básicos.

Suplantación de Identidad

Utilizar datos, documentos, imágenes, credenciales, cuentas o información personal de un tercero para hacerse pasar por él ante una institución o plataforma. Puede presentarse en apertura de cuenta, solicitudes de crédito, recuperación de contraseñas, contratación de servicios, dispersión de recursos u operaciones financieras.

Afecta tanto a la empresa defraudada como al titular legítimo de los datos. El afectado real puede no enterarse hasta semanas o meses después.

Deepfakes

Contenidos audiovisuales manipulados mediante IA (GAN, modelos de difusión) para aparentar que una persona dijo o hizo algo que no ocurrió. Incluye falsificación de rostros, voz, video y documentos visuales.

En el ámbito empresarial: engañar empleados, autorizar transferencias, superar biometría, simular instrucciones de directivos, clonar voz para call center o fraude del CEO.

Principales Tipologías De Fradue Digital

Cada tipología tiene su vector de entrada, señales de alerta y control dominante — el análisis debe ser específico, no genérico

Tipología	¿Como funciona?	Impacto Sectorial	Señales de alerta
01. Phishing·Smishing Vishing	Correos, SMS o llamadas falsas que simulan instituciones legítimas para robar credenciales, datos bancarios o información personal del usuario.	Banca, fintech, aseguradoras, usuarios de servicios digitales	Links sospechosos, urgencia artificial, remitente inconsistente, pantallas de login falsas
02. Account Takeover (ATO)	Acceso a cuenta legítima mediante credenciales robadas, SIM swapping, malware, ingeniería social o debilidades en procesos de recuperación.	Banca digital, wallets, fintech, e-commerce, plataformas de inversión	Cambio súbito de dispositivo/IP, intentos fallidos, geolocalización imposible, reconfiguración de alertas
03. Fraude en Onboarding	Manipulación del proceso de alta con documentos falsos, identidades sintéticas, biometría manipulada o datos robados para crear un perfil fraudulento.	Fintech, SOFOMES, bancos digitales, casinos online, marketplaces, crédito digital	Datos inconsistentes, device sin historial, geolocalización distinta al domicilio, metadatos de documentos recientes
04. Fraude de Crédito Digital	Solicitar financiamiento con intención de no pago desde el origen, usando identidades falsas, historial manipulado o patrones atípicos de solicitud.	SOFOMES, fintech de crédito, modalidad BNPL, plataformas de crédito al consumo	Mora temprana sistemática, solicitudes masivas, historial reciente inconsistente, domicilios repetidos
05. Fraude en Pagos y Cash-out	Contracargos abusivos, tarjetas robadas, cuentas mula, dispersión de recursos a múltiples beneficiarios para monetizar el fraude antes de la detección.	Pagos digitales, SPEI, wallets, e-commerce, gaming, remesas	Velocity alta, importes justo bajo umbral, cuentas nuevas activas, dispersión inmediata

Cadena Operativa Del Fraude

01

Obtención de Datos

Filtraciones de bases de datos, ingeniería social, malware, scraping de redes sociales, robo de documentos, compra en mercados ilícitos o engaños directos al usuario.

LFPDPPP · Monitoreo de filtraciones · Gestión de incidentes · Educación al usuario

02

Preparación de Identidad

Correos, teléfonos, dispositivos, IPs, documentos editados, fotos, videos y perfiles de comportamiento. También: automatización, VPN, emuladores, proxies y deepfakes.

Device fingerprint · Anti-emulación · Reputación email/tel · Detección VPN/proxy · Liveness anti-injection

03

Interacción con Empresa

Abrir cuenta, solicitar crédito, recuperar contraseña, cambiar dispositivo, modificar datos. Primero operaciones pequeñas para evaluar los controles antes del fraude principal.

KYC robusto · Validación documental · Biometría + liveness · Step-up auth · Límites iniciales

04

Monetización del Fraude

Retiro de fondos, dispersión a cuentas mula, compra de activos digitales, bienes de fácil reventa, contracargos, conversión en instrumentos menos trazables.

Monitoreo transaccional · Graph analytics · MTU + factor adicional · Congelamiento automático · UIF/CNBV

05

Ocultamiento y Dispersión

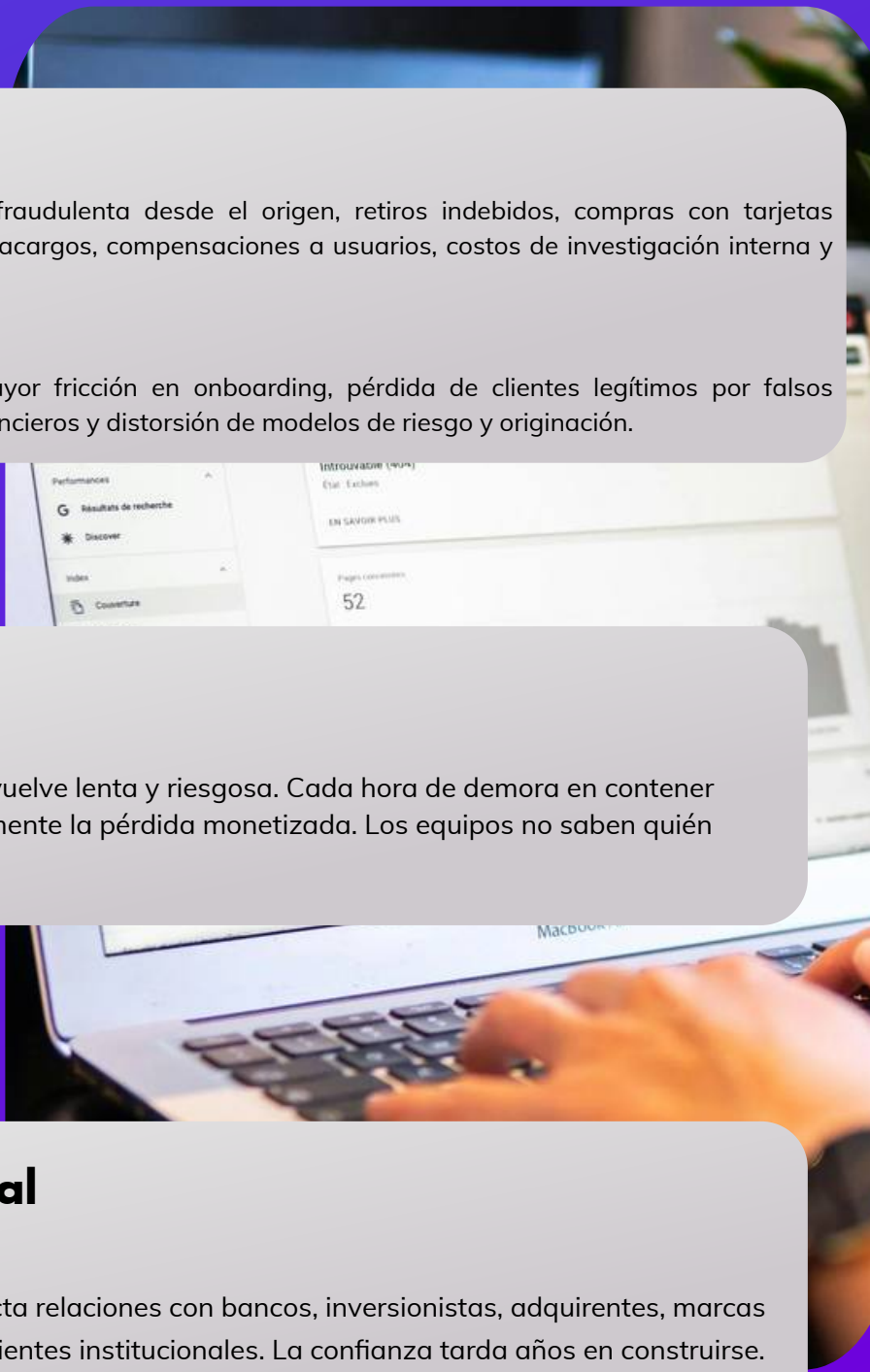
Eliminar rastros, abandonar cuentas, cambiar dispositivos, usar nuevas identidades, fragmentar operaciones. La empresa debe conservar toda la evidencia digital.

Bitácoras Banxico · Conservación 10 años · Expediente completo · Playbooks de respuesta

IMPACTO ECONÓMICO, OPERATIVO Y REPUTACIONAL

En instituciones financieras y plataformas de crédito, el fraude puede contaminar la cartera desde su originación. Esto significa que ciertos créditos o usuarios nacen con una intención fraudulenta, por lo que el incumplimiento posterior no deriva de incapacidad de pago, sino de engaño estructurado.

Si la empresa no distingue entre mora ordinaria y fraude, puede tomar malas decisiones de negocio, ajustar indebidamente sus modelos de riesgo o asumir que el problema está en cobranza cuando realmente está en originación.



Impacto Económico

Pérdidas directas

Créditos no pagados con intención fraudulenta desde el origen, retiros indebidos, compras con tarjetas robadas, devoluciones abusivas, contracargos, compensaciones a usuarios, costos de investigación interna y gastos legales.

Daño indirecto

Incremento de costos operativos, mayor fricción en onboarding, pérdida de clientes legítimos por falsos positivos, deterioro de indicadores financieros y distorsión de modelos de riesgo y originación.

Impacto Operativo

Respuesta improvisada

Sin protocolos claros, la respuesta se vuelve lenta y riesgosa. Cada hora de demora en contener un ATO puede aumentar significativamente la pérdida monetizada. Los equipos no saben quién hace qué.

Impacto Reputacional

Relaciones de negocio

En sectores regulados, la reputación afecta relaciones con bancos, inversionistas, adquirentes, marcas de tarjetas, proveedores tecnológicos y clientes institucionales. La confianza tarda años en construirse.

Alertas Y Señales De Riesgo

En Onboarding

· Inconsistencias nombre/CURP/RFC/domicilio/geoloc/documento/rostro

· Datos válidos sin coherencia entre sí = identidad sintética

· Múltiples registros desde mismo device o IP

· Documentos con metadatos de creación recientes

· Comportamiento robótico: velocidad uniforme, sin errores

En Transacciones

· Fondeo inmediato seguido de retiro o dispersión

· Uso de múltiples tarjetas o cuentas en corto tiempo

· Operaciones de prueba previas al fraude principal

· Dispersión a beneficiarios recurrentes entre usuarios no relacionados

· Contracargos posteriores a compras de alto monto

Deepfake / Biometría

· Movimientos faciales poco naturales o sin parpadeo espontáneo

· Audio desfasado o voz con cadencia artificial

· Iluminación inconsistente entre cara y fondo

· Negativa a realizar movimientos dinámicos del challenge

· Bordes pixelados, latencia inusual, respuesta incorrecta

Velocidad y Conducta

· Solicitudes repetidas con cambios mínimos en datos

· Correos recién creados (menos de 24 horas de antigüedad)

· Intentos fallidos de verificación biométrica o documental

· Cambios frecuentes de contraseña o datos de contacto

· Tiempos de sesión idénticos: señal de automatización

CONTROLES PREVENTIVOS

KYC ROBUSTO — MÁS ALLÁ DEL DOCUMENTO

Consite en validar la consistencia, autenticidad, trazabilidad y comportamiento. Verificar que los datos coincidan entre sí, que el documento no presente alteraciones (OCR forense), que la biometría corresponda con la persona evaluada, que el dispositivo no esté vinculado a eventos previos y que la operación sea congruente con el perfil declarado.

BIOMETRÍA Y PRUEBA DE VIDA

La biometría no debe considerarse infalible. Los deepfakes, fotografías manipuladas, videos pregrabados y técnicas de spoofing obligan a utilizar pruebas de vida activas (challenge dinámico no predecible) y pasivas (análisis de textura y micro-movimientos), detección anti-injection para señal de video sintética y validación out-of-band para operaciones críticas.

MONITOREO TRANSACCIONAL 24/7

Opera en tiempo real. No solo revisa montos: analiza frecuencia, horario, dispositivo, canal, beneficiario, geografía, velocidad, historial, contracargos y relación con otros usuarios. Graph analytics para redes de mulas. Reglas de velocity. Alertas en ≤10 segundos (obligatorio Banxico).

AUTENTICACIÓN REFORZADA Y MTU

Factores por nivel de riesgo: contraseña + token + biometría + validación de dispositivo + geolocalización + confirmación por canal alterno. Factor adicional obligatorio al superar el MTU (Monto Transaccional del Usuario) según CNBV. Bloqueo automático tras 5 intentos fallidos (Banxico).

Modelo de Gobierno Interno

- Primera línea de Defensa - Áreas Operativas y Comerciales
- Segunda Línea de Defensa - Compliance, Riesgos y Seguridad de la información
- Tercera Línea de Defensa - Auditoría Interna /Extrerna

Primera Línea	Segunda Línea	Tercera Línea
Identificar señales de alerta en tiempo real. Aplicar controles iniciales. Escalar oportunamente. NO improvisar.	Diseñar políticas. Validar obligaciones regulatorias. Determinar reportes. Documentar decisiones. Evaluar riesgos múltiples.	Evaluar si el modelo funciona. Si los controles se aplican. Si las alertas se atienden. Si los expedientes están completos y son trazables.
Procedimientos claros · Capacitación específica · Criterios de escalamiento · Herramientas de detección automática. Su función no es investigar — es detectar y escalar.	Evaluar si el evento es fraude, incidente de datos, operación inusual, incumplimiento contractual, conducta penal o combinación. Decidir si se presenta aviso a la autoridad en 24 horas.	No limitarse a revisar manuales: probar evidencia real, casos cerrados, tiempos de respuesta, calidad de investigación. Evaluar la calidad de expedientes y trazabilidad de decisiones.
Requisito mínimo: Manual operativo · Capacitación anual · Acceso a listas y herramientas de scoring · Protocolo de escalamiento con tiempos definidos	Requisito mínimo: Manual antifraude aprobado · Matriz de riesgos · Playbooks por tipología · Flujo de escalamiento · Coordinación activa con PLD/FT	Requisito mínimo: Plan de auditoría específico antifraude · Evaluación end-to-end · Prueba de controles técnicos · Revisión de bitácoras y logs

CONCLUSIONES

El incumplimiento regulatorio en materia antifraude ya tiene nombre, artículo y consecuencia. No es un riesgo futuro: es una obligación exigible hoy.

El error más costoso que comete una organización frente al fraude digital no es técnico, es conceptual: tratar las obligaciones regulatorias como si fueran recomendaciones de buenas prácticas, cuando en realidad son texto legal vigente con consecuencias sancionadoras directas. La CNBV exige desde 2024 un Plan de Gestión para la Prevención del Fraude aprobado al nivel del órgano de gobierno, con identificación expresa de conductas observables de suplantación, sistemas de alerta, monitoreo de operaciones y medidas diferenciadas para personas en situación de vulnerabilidad.

La institución que hoy no pueda acreditar ante una auditoría regulatoria o una reclamación que tiene estos controles implementados y funcionando no tiene defensa — ni jurídica, ni operativa, ni reputacional. Y la exposición no se limita al plano administrativo: cuando el fraude digital se conecta con operaciones de dispersión de recursos, uso de identidades falsas o redes de mulas, el análisis penal bajo el Código Penal Federal y el régimen de responsabilidad de personas jurídicas previsto en el Código Nacional de Procedimientos Penales puede alcanzar a los propios directivos de la organización que no acredite diligencia debida. En ese escenario, la pregunta que responderá si la empresa sale bien parada no es si tenía tecnología sofisticada, sino si tenía política aprobada, manual documentado, evidencia de capacitación, bitácoras conservadas y protocolo de respuesta activado. Lo que no está documentado, en un procedimiento legal o regulatorio, simplemente no existió.

La confianza digital es el activo más valioso de la economía digital y el más difícil de reconstruir una vez destruido. La pregunta ya no es si invertir en controles antifraude, sino cuánto costará no haberlo hecho.

El cambio de paradigma que este estudio propone es concreto: los controles antifraude no son un costo de cumplimiento — son una inversión en confianza digital, y la confianza digital es hoy un activo estratégico con precio, con rentabilidad y con costo de oportunidad medible. Los bancos corresponsales, los adquirentes, los fondos de inversión y las aseguradoras ya evalúan la madurez antifraude de sus contrapartes antes de establecer condiciones. Las organizaciones con controles documentados, expedientes trazables y evidencia de diligencia obtienen acceso, términos y condiciones diferenciadas que sus competidores menos maduros no obtienen.

Construir esa reputación de seguridad toma años; destruirla puede tomar horas. En el sector financiero y fintech mexicano, donde la diferenciación entre productos es a menudo marginal y la competencia por la confianza del usuario es intensa, la percepción de seguridad es un factor de decisión real que impacta directamente la captación, la retención y el valor de vida del cliente. La pregunta que toda Alta Dirección debe formularse no es cuánto costará implementar los controles — es cuánto costará, en pérdidas directas, en relaciones de negocio perdidas, en sanciones regulatorias y en oportunidades no aprovechadas, no haberlos implementado a tiempo.

Bibliografía y uso de AI

- GAFI / FATF: recomendaciones internacionales en materia de prevención de lavado de dinero, financiamiento al terrorismo, enfoque basado en riesgo, nuevas tecnologías, activos virtuales y debida diligencia del cliente. https://www.fatf-gafi.org/en/publications/Fatfrecommendations/Guidance-rba-virtual-assets-2021.html?utm_source=chatgpt.com

- UNODC: documentos sobre ciberdelincuencia, crimen organizado, lavado de dinero, cooperación internacional y uso de tecnología por redes criminales.

- INTERPOL: reportes y análisis sobre cibercrimen, fraude financiero, ingeniería social, phishing, ransomware y amenazas digitales transnacionales. Banco Mundial: estudios sobre digitalización, inclusión financiera, transformación digital y riesgos asociados al crecimiento de servicios financieros digitales.

- Banco de México: información sobre sistemas de pago, medios de disposición, seguridad operativa, infraestructura financiera y funcionamiento del ecosistema de pagos.

- CNBV: disposiciones de carácter general aplicables a entidades financieras, criterios de supervisión, PLD/FT, gestión de riesgos, controles internos y reportes regulatorios.

- CONDUSEF: información sobre reclamaciones, fraudes financieros, protección a usuarios de servicios financieros, cargos no reconocidos y alertas al público.

- INAI: criterios y guías en materia de protección de datos personales, deber de seguridad, vulneraciones, avisos de privacidad y gestión responsable de información personal. https://home.inai.org.mx/wp-content/documentos/DocumentosSectorPrivado/Guia_Implementacion_SGSDP.pdf

- Association of Certified Fraud Examiners : estudios sobre fraude ocupacional, presión económica, controles antifraude, cultura organizacional y detección temprana. https://www.acfe.com/fraud-resources

- Círculo de Crédito / Featurespace: análisis sobre fraude financiero, behavioral analytics, machine learning, crédito digital, fraude de originación e impacto financiero de modelos antifraude.

Se utilizó Chat GPT Agent y Claude para la estructura de este estudio

Contacto

Oficina: 5526905362

rdiaz@zcdasesorespld.com

WTC, Montecito 38, Piso 28, Col. Nápoles, CDMX 03810 /
www.zcdasesorespld.com