Manual de prevención de fraudes

Comisión Fraude y Ciberseguridad - CUF
Diciembre 2025

CÁMARA URUGUAY FINTECH

1. Introducción

Este manual es una iniciativa de la **Cámara Uruguaya de Fintech** (CUF) para promover un ecosistema financiero más seguro y confiable. El mismo ha sido desarrollado por **Forsvar**, plataforma tecnológica especializada en prevención de fraude y prevención de lavado de activos (AML) para medios de pago digitales. Establece el marco de **prevención, detección y respuesta ante fraudes** aplicable a las operaciones de las **fintech en Uruguay**. Su propósito es proveer una estructura, basada en estándares internacionales, datos regionales y prácticas de la industria financiera, para colaborar con la seguridad de los usuarios y la integridad operativa de las compañías tecnológicas financieras de Uruguay.

Este manual no se limita exclusivamente a empresas fintech en sentido estricto, sino que está diseñado para ser aplicable a un espectro amplio de organizaciones que operan o interactúan con servicios financieros digitales y que, por la naturaleza de sus actividades, presentan exposición a riesgos de fraude y delitos financieros.

En particular, los lineamientos aquí descritos resultan relevantes para:

- **Bancos digitales y entidades financieras con canales remotos**, que ofrecen productos y servicios a través de aplicaciones móviles, plataformas web y procesos 100% digitales.
- **Billeteras digitales y proveedores de medios de pago electrónicos**, incluyendo emisores de dinero electrónico, plataformas de pago, transferencias inmediatas y pagos cuenta a cuenta.
- **Aseguradoras**, especialmente en procesos de alta de clientes, gestión de siniestros digitales, pagos de indemnizaciones y prevención de fraude en reclamos.
- **Otras empresas con exposición a fraude**, tales como marketplaces, plataformas de crédito digital, proveedores de servicios financieros embebidos, empresas de remesas, plataformas de inversión online y organizaciones que procesan pagos o gestionan identidades digitales.

El crecimiento acelerado del ecosistema fintech en Uruguay y Latinoamérica ha generado un incremento en los incidentes de fraude digital, incluyendo ataques sofisticados que combinan ingeniería social, malware, abuso de dispositivos móviles, suplantación de identidad, inteligencia artificial y estructuras de lavado de activos.

Estas amenazas requieren un enfoque integral, preventivo y basado en riesgo, con controles técnicos, operativos y organizacionales robustos.

Este manual de prevención de fraudes digitales no sustituye la definición específica de la estrategia de cada empresa ni reemplaza la determinación del apetito de riesgo propio de cada organización. Su propósito es servir como marco de referencia, guía metodológica y herramienta de apoyo para el diseño, implementación y maduración del modelo de gestión de fraude de cada fintech, que deberá considerar las particularidades del negocio, su etapa de vida, la naturaleza de sus productos, su perfil de clientes y su capacidad operativa y tecnológica.

Se recomienda que cada empresa adapte, complemente y ajuste las políticas, controles y procedimientos aquí descriptos de acuerdo con su propia estrategia de gestión de riesgos, su tolerancia y apetito de riesgo explícitamente definidos, las capas de control ya existentes, su estructura organizacional, el volumen y la complejidad de sus operaciones, los servicios que ofrece y el contexto regulatorio, operativo y de mercado en el que desarrolla su actividad. En este sentido, el presente documento no pretende ser prescriptivo ni sustituir el criterio de la organización, sino servir como una guía de referencia que debe ser interpretada y aplicada de manera proporcional y coherente con la realidad de cada negocio.

Este manual puede ser utilizado como insumo para auditorías, evaluaciones regulatorias y procesos de due diligence.

Asimismo, este manual debe entenderse como un documento vivo, sujeto a procesos de revisión periódica y mejora continua, en la medida en que evolucionan las amenazas de fraude digital, se fortalecen o transforman las capacidades internas de la organización, se actualizan las regulaciones locales e internacionales, y surgen nuevas prácticas y estándares recomendados por la industria. La actualización constante de estos lineamientos resulta clave para asegurar la efectividad de los controles, la resiliencia del modelo de prevención y el alineamiento con las mejores prácticas vigentes.

Este documento constituye un **pilar de apoyo esencial** para la introducción a la gestión de riesgos de fraude, lo cual requiere de una **adecuación específica y contextualizada** para convertirse en la estrategia antifraude definitiva para cada empresa.

2. Contexto regional y local de fraude

2.1. Panorama internacional

Diversos organismos internacionales coinciden en que el fraude digital y los delitos financieros asociados a medios de pago electrónicos presentan una tendencia creciente a nivel global y regional. De acuerdo con el Bank for International Settlements (BIS), la digitalización acelerada de los servicios financieros ha incrementado significativamente la superficie de ataque, especialmente en canales remotos, pagos instantáneos y onboarding digital, lo que exige enfoques de gestión de riesgo más sofisticados y dinámicos.

Informes del United Nations Office on Drugs and Crime (UNODC) señalan que las organizaciones criminales utilizan cada vez más plataformas digitales y sistemas de pago electrónicos para cometer fraudes, mover fondos ilícitos y ocultar su origen, aprovechando la velocidad de las transacciones y la fragmentación regulatoria entre jurisdicciones. En este contexto, el fraude de identidad, las cuentas mule y las estafas de ingeniería social se consolidan como facilitadores clave de esquemas de lavado de activos.

A nivel de cibercrimen, el Federal Bureau of Investigation, Internet Crime Complaint Center (FBI IC3) reporta un crecimiento sostenido en los incidentes de fraude financiero digital, con pérdidas que superan los miles de millones de dólares anuales a nivel global, destacándose el aumento de ataques de phishing, account takeover y fraudes habilitados por malware en dispositivos móviles. Estos patrones son consistentes con los hallazgos de INTERPOL, que advierte sobre la profesionalización del fraude digital y el uso creciente de automatización e inteligencia artificial por parte de los atacantes.

El World Bank Group y el International Monetary Fund (IMF) también destacan que la inclusión financiera digital, si bien genera beneficios económicos y sociales relevantes, introduce riesgos operativos y de fraude que deben ser gestionados mediante controles preventivos proporcionales, monitoreo continuo y una gobernanza de riesgo sólida.

Latinoamérica se ha consolidado en los últimos años como una de las regiones más expuestas al fraude en servicios financieros digitales. El crecimiento acelerado de pagos electrónicos, billeteras digitales, transferencias inmediatas, créditos online y modelos de negocio 100% remotos ha ampliado de forma significativa la superficie de ataque para organizaciones criminales, muchas de ellas operando de manera coordinada y transfronteriza.

Estudios del World Bank Group indican que, en mercados de latinoamérica y en verticales digitales de riesgo, las pérdidas por fraude y abuso pueden alcanzar rangos de dos dígitos sobre el volumen transaccionado, llegando en algunos segmentos específicos a niveles cercanos al 20%, particularmente cuando existen procesos de onboarding simplificados o controles preventivos insuficientes. A esto se suma un crecimiento sostenido de esquemas como mule accounts, account takeover (ATO), phishing avanzado, estafas de ingeniería social y fraudes cross-border, donde los fondos se mueven rápidamente entre países para dificultar su trazabilidad y recuperación.

El dinamismo del ecosistema fintech latinoamericano, si bien ha sido clave para la inclusión financiera, también ha generado un entorno altamente atractivo para el fraude organizado. Wallets interoperables, transferencias inmediatas, créditos de aprobación rápida, remesas digitales y criptoactivos permiten operar con gran velocidad y bajo costo, reduciendo el margen de reacción de las empresas que no cuentan con controles preventivos robustos. La incorporación de inteligencia artificial por parte de los atacantes, ya sea para automatizar ataques, crear identidades sintéticas o generar deepfakes, refuerza la expectativa de que el fraude continúe creciendo tanto en volumen como en complejidad.

2.2. Tendencias en Uruguay

En Uruguay, el crecimiento de los servicios financieros digitales ha venido acompañado de un aumento sostenido de las estafas y fraudes cometidos a través de canales electrónicos. Datos oficiales del Ministerio del Interior y reportes públicos del Banco Central del Uruguay (BCU) evidencian un incremento significativo en las denuncias asociadas a estafas digitales, phishing y accesos indebidos a cuentas, en línea con la tendencia regional e internacional.

Las denuncias por estafa en el país han crecido más de un 2.000% en la última década, pasando de aproximadamente 8 a más de 870 denuncias cada 100.000 habitantes en 2024, reflejando no solo una mayor incidencia del delito sino también una mayor exposición de la población a esquemas fraudulentos. Este crecimiento se da en paralelo con una adopción acelerada de pagos digitales, billeteras electrónicas, transferencias inmediatas y servicios fintech, tanto en consumidores como en comercios.

El BCU, en sus comunicaciones y marcos regulatorios sobre sistemas de pago y gestión de riesgos, reconoce explícitamente la necesidad de que las entidades financieras y no financieras adopten controles robustos para mitigar riesgos de fraude, ciberseguridad y lavado de activos en entornos digitales.

Este contexto refuerza la idea de que el fraude digital no constituye un evento excepcional, sino un riesgo estructural inherente a los modelos de negocio basados en canales remotos, pagos electrónicos y procesos automatizados. Uruguay, si bien presenta un menor volumen absoluto de transacciones respecto a otras economías de la región, no es ajeno a estas tendencias y muestra señales claras de maduración del riesgo. En este contexto, el fraude ya no puede ser considerado un evento excepcional o marginal, sino un riesgo estructural del negocio digital.

Todo esto vuelve indispensable la adopción de un marco de prevención de fraude alineado tanto con los riesgos regionales como con las mejores prácticas internacionales. Uruguay se encuentra en un punto de inflexión donde esperar a "tener problemas" ya no es aceptable, ni desde una perspectiva técnica, ni desde una óptica regulatoria, ni desde la responsabilidad fiduciaria hacia usuarios y clientes. La prevención temprana, la detección en tiempo real y la capacidad de respuesta organizada pasan a ser elementos centrales de la sostenibilidad del ecosistema financiero digital local.

2.3. Marco regulatorio aplicable en Uruguay

El marco normativo vigente en Uruguay, liderado por el Banco Central del Uruguay (BCU), establece principios y obligaciones que resultan directamente relevantes para la prevención de fraude y delitos financieros en entornos digitales, aun cuando no siempre se refieran de forma explícita al término “fraude” como categoría autónoma. La Recopilación de Normas de Regulación y Control del Sistema Financiero (RNRCSF) exige a las entidades supervisadas contar con sistemas adecuados de gestión de riesgos operativos, tecnológicos y de seguridad de la información, incluyendo mecanismos de control interno, trazabilidad de operaciones, auditoría y responsabilidad ante reclamos de los usuarios. En línea con ello, recientes actualizaciones regulatorias refuerzan la obligación de implementar sistemas de monitoreo capaces de detectar transacciones inusuales, desvíos de comportamiento, uso de dispositivos no reconocidos y patrones sospechosos, así como de aplicar mecanismos de autenticación reforzada en accesos, transferencias, pagos y modificaciones de datos sensibles, junto con notificaciones proactivas al usuario ante eventos o intentos de cambio relevantes.

Estos lineamientos son plenamente aplicables a riesgos de fraude digital, accesos indebidos, manipulación transaccional y abuso de canales electrónicos. Asimismo, la normativa en materia de prevención de lavado de activos y financiamiento del terrorismo (AML/CFT) impone obligaciones de debida diligencia, monitoreo transaccional continuo, identificación de operaciones inusuales y reporte de operaciones sospechosas, siendo el fraude digital en muchos casos un delito precedente o facilitador del lavado de activos. En este contexto, un sistema de prevención de fraude basado en riesgo, con monitoreo en tiempo real, autenticación robusta, gestión estructurada de casos y evidencias auditables, no solo responde a buenas prácticas internacionales, sino que se alinea directamente con las expectativas regulatorias vigentes en Uruguay.

3. Tipos de fraude

Esta sección detalla los tipos de fraudes más comunes y su relación con los eventos críticos en el ciclo del usuario. No todos los controles son obligatorios para todas las fintech, su aplicación debe ser proporcional al producto, volumen y apetito de riesgo.

3.1. Onboarding

El onboarding es el momento en que interactuamos por primera vez con el usuario, momento en el cual es importante realizar el proceso de KYC más robusto posible. Los riesgos identificados y fraudes más comunes en esta etapa son:

3.1.1 Suplantación de identidad (robo de documento)

A partir de una práctica fraudulenta se accede al documento de identidad de un tercero y se utiliza para la apertura de una cuenta o la realización de operaciones a su nombre, sin su consentimiento.

3.1.2 Identidades sintéticas

Se crean identidades falsas combinando datos reales (por ejemplo, un número de documento válido) con información inventada, generando perfiles que aparentan ser legítimos y logran superar controles básicos de verificación.

3.1.3 Documentos falsificados

Uso de documentos de identidad falsos o modificados (alteración de datos, fotos o formatos) para evadir controles KYC y obtener acceso a productos o servicios financieros.

3.1.4 Deepfakes

Creación de imágenes y videos generados con inteligencia artificial para simular la presencia de una persona real durante procesos de verificación biométrica o prueba de vida.

3.1.5 Cuentas mule creadas masivamente

Creación sistemática de múltiples cuentas con fines fraudulentos, utilizadas como intermediarias para mover, dispersar o retirar fondos provenientes de actividades ilícitas, dificultando su rastreo. Suelen ser cuentas validadas por personas en contexto crítico a cambio de un beneficio económico, para luego ser utilizadas con su nombre e identidad.

3.1.6 Bots para registro automático

Uso de scripts o software automatizado para realizar registros masivos en plataformas digitales, generando cuentas falsas a gran escala y explotando promociones, bonificaciones o debilidades en el onboarding.

Ejemplos:

- Persona A usa documento robado o foto obtenida por redes sociales para abrir cuenta.
- Individuo crea 20 cuentas desde el mismo dispositivo para operar como mule.
- Se utiliza un documento extranjero falso para eludir KYC.

Los controles recomendados para el proceso de onboarding deben cubrir de forma integral la validación de identidad, el análisis de riesgo y la prevención de abusos automatizados. Esto implica combinar la verificación documental con una selfie del usuario, asegurando que la identidad presentada corresponda a una persona real y vigente. A su vez, resulta clave incorporar validación biométrica en tiempo real, que permita contrastar el rostro del usuario con el documento presentado y detectar intentos de suplantación. Estos controles deben complementarse con la verificación de datos contra fuentes oficiales y proveedores confiables, lo que ayuda a confirmar la existencia de la persona, la validez del documento y la consistencia de la información declarada.

Adicionalmente, es fundamental aplicar controles técnicos como device fingerprinting, análisis de reputación de IP y mecanismos de detección de bots, con el objetivo de identificar registros masivos, automatizados o coordinados desde un mismo entorno tecnológico.

Durante el onboarding también se deben ejecutar validaciones contra listas AML, PEP y sanciones internacionales, reduciendo el riesgo regulatorio desde el primer contacto con el usuario. Todo este conjunto de señales debe consolidarse en un score de riesgo de onboarding, alimentado por matrices de riesgo personalizadas según el tipo de empresa, su apetito de riesgo, los productos ofrecidos y el contexto geográfico en el que opera.

En cuanto a reglas explícitas, el sistema debe permitir decisiones claras y auditables. Por ejemplo, el onboarding debe rechazarse automáticamente si el documento presentado pertenece a una persona reportada como fallecida en fuentes oficiales o bases confiables. Asimismo, se recomienda marcar para revisión manual aquellos casos en los que tres o más identidades diferentes intentan registrarse desde un mismo dispositivo dentro de una ventana de 24 horas, ya que este patrón suele estar asociado a la creación masiva de cuentas fraudulentas. También resulta crítico rechazar el alta cuando la selfie no coincide con el documento o cuando se detectan señales de deepfake, especialmente si existen múltiples intentos fallidos de validación biométrica previos a una supuesta aprobación, lo que requiere una calibración específica de los controles antifraude.

Finalmente, durante el proceso de onboarding, se deben bloquear automáticamente los intentos cuyo origen de IP corresponda a países catalogados como de alto riesgo, salvo que exista una justificación de negocio explícita y controles compensatorios adecuados.

Es importante realizar un onboarding, siempre que el producto lo permita, que brinde toda la información posible del usuario cuidando en simultáneo la experiencia del cliente. Para ello, todo dato que pueda ser recopilado debe ser analizado (Email, Teléfono, Número de documento, etc.), y en simultáneo debemos evitar solicitar datos que no aporten valor. Existen diferentes modelos y listas para analizar estos datos, asignarles un nivel de riesgo y complementar así, junto con la validación biométrica y de dispositivo, un score de riesgo al usuario desde su primera interacción con el producto.

3.2. Log in

Cada inicio de sesión, en caso de que el producto así lo requiera, es una interacción clave a analizar en términos de riesgo. En este punto se encuentra diversas modalidades de fraude que pueden ser detectadas en situaciones tempranas del accionar fraudulento:

3.2.1 Credential stuffing

Uso automatizado de combinaciones de usuario y contraseña filtradas de otros servicios para intentar acceder masivamente a cuentas, aprovechando la reutilización de credenciales por parte de los usuarios.

3.2.2 Accesos desde dispositivos comprometidos

Ingresos a cuentas desde dispositivos infectados o previamente utilizados en fraudes, donde el atacante ya tiene control parcial o total del entorno del usuario.

3.2.3 Malware en mobile

Software malicioso instalado en dispositivos móviles que permite interceptar credenciales, OTPs o sesiones activas, facilitando el acceso no autorizado a la cuenta.

3.2.4 Intentos masivos de login (botnets)

Ataques distribuidos desde múltiples IPs y dispositivos controlados por bots que realizan grandes volúmenes de intentos de inicio de sesión para evadir controles básicos de seguridad.

Ejemplos:

- Usuario recibe phishing (solicitud de información a través de mensaje falso que se hace pasar por la empresa), entrega sus datos y su contraseña, el atacante hace login en la cuenta desde otro país.
- Malware móvil enviado a través de Email o SMS que se instala en el dispositivo y captura los datos de la persona.
- Robo de credenciales de un ecommerce usado luego para entrar a la wallet de sus clientes.

En los flujos de autenticación y acceso a cuentas se recomienda aplicar un conjunto de controles orientados a reducir el riesgo de Account Takeover y accesos no autorizados sin degradar innecesariamente la experiencia del usuario. Entre estos controles se incluye el uso de autenticación multifactor (MFA) como capa adicional de seguridad ante señales de riesgo, la detección de patrones de "impossible travel" para identificar accesos desde ubicaciones geográficas incompatibles en lapsos de tiempo reducidos, y la validación continua del device fingerprint para reconocer dispositivos previamente asociados al usuario. Complementariamente, es clave notificar proactivamente al usuario ante accesos sospechosos, establecer límites estrictos a los intentos fallidos de autenticación y calcular un score de sesión que evalúe el riesgo del comportamiento observado durante el login y la navegación inicial.

A nivel de reglas explícitas, pueden definirse criterios automáticos que activen fricción o bloqueos temporales cuando el contexto lo amerita. Por ejemplo, si un inicio de sesión ocurre desde un dispositivo no visto previamente y además proviene de una geolocalización distinta a las habituales, el sistema puede requerir MFA adicional o bloquear el acceso de forma preventiva hasta una validación exitosa. Asimismo, se recomienda bloquear automáticamente cuando se detectan más de diez intentos fallidos de autenticación en un período de cinco minutos desde la misma dirección IP, como medida contra ataques de fuerza bruta o credential stuffing. Finalmente, se debe generar una alerta cuando un usuario cambia de geolocalización en menos de diez minutos entre dos accesos consecutivos, ya que este patrón suele ser indicativo de compromiso de credenciales o uso de infraestructuras anómalas.

Cada inicio de sesión debe ser analizado en tiempo real, permitiendo la detección de sesiones anómalas previo a la realización de actividades fraudulentas. Los remedies como MFA o selfie ID son un gran mecanismo de resolución rápida que permiten escalar la gestión de estas sesiones de riesgo sin acumular trabajo operativo manual ni generar malas experiencias en posibles falsos positivos a los usuarios.

3.3. Transacciones

Las transacciones de dinero suelen ser el momento en que los fraudulentos consuman su cometido, por lo que es clave contar con un monitoreo en tiempo real que nos permita detectar el siguiente tipo de riesgos:

3.3.1 Transferencias fraudulentas

Movimientos de dinero realizados sin el consentimiento del usuario legítimo, generalmente tras un account takeover, ingeniería social o abuso de credenciales comprometidas. La cuenta destino está asociada al fraudulento, a través de la cual se hace del dinero.

3.3.2 Fraude en pagos con tarjeta de crédito/débito

Uso fraudulento de tarjetas en entornos card not present (e-commerce), incluyendo ataques de fuerza bruta para validar BINs, enumerar PAN/fecha/CVV o probar tarjetas robadas en pequeños montos.

3.3.3 Triangulación

Esquema en el que el dinero se mueve a través de múltiples cuentas intermedias para ocultar su origen, dificultar la trazabilidad y facilitar lavado de activos o retiro final de fondos.

3.3.4 Mule accounts (envíos P2P)

Cuentas utilizadas como intermediarias para recibir y enviar fondos fraudulentos, muchas veces controladas por terceros o creadas específicamente para dispersar dinero ilícito vía transferencias P2P.

3.3.5 Préstamos fraudulentos

Obtención de créditos mediante identidades robadas, sintéticas o información falsa, con el objetivo de retirar el dinero sin intención de repago.

3.3.6 Abuso de límites

Explotación de límites transaccionales, diarios o mensuales (por ejemplo, fraccionando montos o usando múltiples cuentas) para maximizar el beneficio fraudulento sin disparar controles básicos.

3.3.7 Fraude de remesas

Uso fraudulento de transferencias internacionales para mover fondos ilícitos entre países, aprovechando diferencias regulatorias, tiempos de liquidación o menor visibilidad transaccional.

3.3.8 Pagos a cuentas fraudulentas

Pagos cuenta a cuenta dirigidos a cuentas receptoras controladas por estafadores, comúnmente originados por phishing, ingeniería social o manipulación del beneficiario. El usuario envía el dinero de forma voluntaria pero siendo engañado.

3.3.9 Abuso de vulnerabilidades y bugs de la plataforma

Explotación intencional de errores lógicos, fallas de validación o condiciones de carrera dentro de la plataforma para obtener beneficios económicos indebidos. Incluye duplicación de transacciones, acreditaciones múltiples, desincronización entre balances disponibles y contables, bypass de validaciones de límites o ejecución de flujos no previstos por el diseño funcional.

3.3.10 Abuso de cancelaciones, reversas y refunds

Uso sistemático y malicioso de mecanismos legítimos de cancelación, reversión o devolución para generar créditos indebidos, extraer fondos antes de la reversa efectiva o forzar inconsistencias contables. Suele combinarse con ventanas de tiempo, latencias operativas o debilidades en los procesos de conciliación.

3.3.11 Auto fraude

Fraude cometido por el propio usuario titular de la cuenta, quien niega transacciones legítimas, simula compromisos de cuenta o utiliza mecanismos como chargebacks, reclamos o denuncias falsas para obtener un beneficio económico o evitar obligaciones de pago. Este tipo de fraude representa un desafío particular por su similitud con casos legítimos.

3.3.12 Fraude interno

Actividades fraudulentas realizadas por empleados, contratistas o terceros con acceso legítimo a sistemas internos. Puede incluir manipulación de estados transaccionales, bypass de controles, creación o aprobación indebida de operaciones, filtración de información sensible o colusión con redes externas de fraude.

3.3.13 Manipulación o simulación de historial bancario y financiero

Creación, alteración o presentación de historiales transaccionales falsos o artificiales con el objetivo de aparentar actividad legítima, justificar el origen de fondos o facilitar procesos de lavado de activos. Puede combinarse con cuentas mule, circularidad de fondos y operaciones de bajo monto repetidas.

3.3.14 Abuso de promociones

Modalidad en la que los usuarios explotan incentivos comerciales (bonificaciones, cashback, cupones, referidos o promociones de bienvenida) de forma indebida o fraudulenta, mediante la creación de múltiples cuentas y transacciones por montos mínimos sin otro fin más que el premio económico.

Ejemplos:

- Después de phishing, el atacante transfiere dinero a mule accounts.
- Se hacen pagos con tarjeta virtual robada o generada por ataques BIN.
- Usuario realiza depósitos de múltiples cuentas terceros (structuring para lavado).
- Se realizan 30 pagos pequeños en 10 minutos, patrón típico de bots.

El esquema de controles transaccionales se apoya en un conjunto de mecanismos dinámicos y complementarios diseñados para adaptarse en tiempo real al comportamiento de los usuarios y a la evolución del riesgo. La plataforma debe permitir la definición de límites dinámicos sobre montos, frecuencia y ventanas horarias, ajustados según variables como la antigüedad de la cuenta, el perfil de riesgo, el historial transaccional y el contexto operativo. Estos límites no son estáticos, sino que se recalibran de forma continua para equilibrar seguridad y experiencia de usuario.

Sobre esta base se incorporan controles de velocidad (velocity checks) aplicados de manera transversal a múltiples dimensiones, incluyendo usuario, tarjeta, dirección IP y dispositivo. Este enfoque permite detectar patrones anómalos como ráfagas de intentos, automatización maliciosa, enumeración de tarjetas o abuso de infraestructura comprometida, incluso cuando cada evento individual parece legítimo.

El análisis relacional entre cuentas es un componente clave para la detección de fraudes organizados. Mediante técnicas de grafos y linkage analysis, el sistema identifica relaciones directas e indirectas entre usuarios, dispositivos, medios de pago y destinos de fondos. Este análisis permite descubrir clusters sospechosos, redes de cuentas mule, esquemas de triangulación y reutilización de activos digitales que no son evidentes desde una evaluación aislada de eventos.

Adicionalmente, se incorporan mecanismos de detección de uso de proxies, VPNs y otras técnicas de ocultamiento de origen, los cuales son evaluados en conjunto con señales de geolocalización, reputación de red y consistencia histórica del usuario. Estas señales permiten identificar el nivel de riesgo en escenarios donde se intenta evadir controles geográficos o simular comportamientos legítimos.

Todos estos controles determinísticos se complementan con un score de riesgo basado en modelos de machine learning ejecutados en tiempo real. Este score sintetiza cientos de variables de comportamiento, contexto y relación histórica, permitiendo tomar decisiones más precisas, reducir falsos positivos y adaptarse a nuevos patrones de fraude sin depender exclusivamente de reglas manuales.

En términos operativos, el motor de decisiones permite implementar reglas explícitas que materializan estos controles. Por ejemplo, una cuenta puede ser marcada como potencial mule cuando recibe fondos de más de cinco emisores no relacionados dentro de una ventana de una hora, ya que este patrón suele asociarse a esquemas de dispersión y lavado de dinero. De forma similar, una transacción puede ser rechazada automáticamente si el BIN de la tarjeta corresponde a un país prohibido o catalogado como de riesgo extremo según la política de la organización.

El sistema también habilita restricciones contextuales más finas, como el bloqueo de pagos nocturnos por montos elevados para cuentas recientemente creadas, donde la combinación de baja antigüedad y horarios atípicos incrementa significativamente el riesgo. En el plano de medios de pago, se generan alertas cuando un usuario intenta realizar múltiples transacciones consecutivas con tarjetas fallidas, lo que puede indicar pruebas de tarjetas robadas o errores sistemáticos asociados a fraude.

Desde una perspectiva relacional, se pueden detonar alertas cuando dos o más usuarios comparten múltiples dispositivos en un período acotado, señal típica de operación coordinada o control centralizado de cuentas.

Finalmente, para mitigar ataques de enumeración, el sistema puede bloquear automáticamente una tarjeta cuando se detectan múltiples intentos fallidos en un intervalo muy corto, previniendo la validación masiva de datos sensibles.

Este enfoque integral permite combinar reglas claras y auditables con inteligencia adaptativa, logrando una cobertura robusta frente a fraudes simples y avanzados, sin sacrificar escalabilidad ni capacidad de evolución del sistema.

Toda transacción que el usuario realice, así sea un pago, una transferencia, un retiro de dinero, un préstamo o una inversión, debe tener un análisis por detrás que permita aprobar, rechazar, enviar a revisión o alertar a la empresa sobre eventuales riesgos. Se debe contar con reglas específicas para cada negocio y modelos de IA entrenados y adaptados a cada realidad.

4. Herramientas clave para la prevención

La prevención de fraude moderna no depende de un único control, sino de un ecosistema de herramientas integradas que permiten detectar, analizar, decidir y actuar sobre eventos de riesgo en tiempo real y de forma escalable. Estas herramientas combinan automatización, análisis avanzado y revisión humana, equilibrando eficiencia operativa, reducción de pérdidas y experiencia de usuario.

4.1 Motor de decisión

El motor de decisión es el núcleo de la estrategia antifraude. Centraliza la evaluación de riesgo de cada evento (onboarding, login, transacción, transferencia) y ejecuta decisiones automáticas basadas en reglas, scores y políticas definidas por la organización. Permite combinar reglas determinísticas, modelos de machine learning, listas de referencia y umbrales dinámicos, generando decisiones explicables y auditables.

Los modelos de inteligencia artificial de machine learning son un input fundamental para nutrir el árbol, utilizando el historial de fraudes de la empresa y el procesamiento avanzado de datos para sumar indicativos de riesgo adicionales que permitan una mejor decisión, pero no se

sugiere dejar el 100% de la decisión a los modelos sin combinarlos con reglas específicas que el negocio requiera.

Un motor de decisión robusto permite versionar reglas, priorizarlas, ejecutar pruebas controladas y mantener trazabilidad completa de por qué una operación fue aprobada, rechazada o enviada a revisión. Esto es clave tanto para la mejora continua como para auditorías regulatorias y defensa ante reclamos.

4.2 Herramientas de visualización y análisis

Las herramientas de visualización permiten transformar grandes volúmenes de datos y alertas en información accionable. Incluyen dashboards operativos, tableros ejecutivos y visualizaciones avanzadas como grafos de relación entre cuentas, dispositivos y transacciones.

Los dashboards permiten monitorear KPIs críticos (tasa de fraude, falsos positivos, tiempos de resolución, alertas por tipo), mientras que los grafos facilitan la detección de esquemas complejos como mule accounts, triangulación o redes de fraude coordinado, imposibles de identificar con análisis lineales.

Estas herramientas no solo mejoran la capacidad de detección, sino que reducen tiempos de investigación y aumentan la calidad de las decisiones humanas.

4.3 Gestión de casos y equipo

La gestión de casos es el puente entre la detección automática y la intervención humana. Permite agrupar alertas relacionadas, asignarlas a analistas, documentar evidencias, registrar decisiones y mantener trazabilidad completa del ciclo de vida de cada investigación.

Un sistema de case management eficiente estandariza procesos, reduce errores humanos y permite escalar el equipo antifraude sin perder control. Además, es fundamental para cumplir con requerimientos regulatorios, ya que centraliza evidencias, decisiones y reportes.

La gestión de casos también habilita métricas de performance del equipo (SLA, backlog, tasa de confirmación de fraude) y retroalimenta modelos y reglas.

4.4 Verificación de identidad biométrica

La verificación de identidad biométrica es una capa crítica, especialmente en onboarding, recuperación de cuentas y operaciones de alto riesgo. Incluye validación documental, selfie en tiempo real, biometría facial y detección de intentos de fraude avanzados como deepfakes o reutilización de identidades.

Integrada correctamente, la biometría reduce drásticamente el fraude de identidad sin introducir fricción innecesaria, ya que permite aplicar controles adaptativos según el nivel de riesgo detectado.

Además, la biometría actúa como señal fuerte dentro del motor de decisión y como evidencia sólida ante disputas o revisiones regulatorias.

El verdadero valor surge cuando estas herramientas operan de forma integrada: el motor de decisión consume señales biométricas y comportamentales, las visualizaciones permiten entender patrones complejos, y la gestión de casos cierra el ciclo con análisis humano y mejora continua. Este enfoque multicapa es el estándar esperado por reguladores, partners financieros y mercados maduros.

5. Gestión de casos y procedimientos

La gestión de casos es un punto de suma importancia para el sistema de prevención de fraude y AML. Permite transformar señales automáticas en decisiones trazables, auditables y consistentes.

5.1 Flujo de un caso

Todo evento relevante en el cual se detecte un riesgo que requiera de tratamiento, debe seguir un conjunto de etapas:

5.1.1 Detección

Evento identificado por reglas, modelos de riesgo, listas AML, anomalías de comportamiento o alertas externas. Puede deberse a un aumento de pagos con un determinado BIN, un cambio en el comportamiento general de los usuarios o cualquier situación que requiera una revisión e investigación.

5.1.2 Alerta

Una alerta es una señal generada de forma automática por la plataforma como resultado de la evaluación de un evento. Cada alerta se encuentra asociada a un tipo de riesgo claramente identificado, como fraude, AML, identidad, account takeover o detección de cuentas mule, e incluye un nivel de severidad previamente definido (P1, P2 o P3).

Asimismo, la alerta incorpora un score de riesgo cuantitativo y el motivo activador que explica qué regla, modelo o condición dio origen a su generación, garantizando trazabilidad y explicabilidad desde el primer momento.

5.1.3 Caso

El caso constituye la agrupación lógica y estructurada de una o más alertas que guardan relación entre sí. Esta relación puede estar dada por un mismo usuario, una cuenta específica, un dispositivo, una transacción puntual o incluso una red de cuentas interconectadas. El objetivo del caso es centralizar toda la información relevante en una única unidad de análisis, permitiendo una visión integral del riesgo y evitando evaluaciones aisladas o fragmentadas.

5.1.4 Análisis

El análisis corresponde a la etapa de revisión humana o semiautomática realizada por un analista especializado. Este proceso se ejecuta bajo criterios, políticas y procedimientos previamente establecidos, asegurando consistencia, objetividad y alineación con la estrategia de riesgo de la organización. Durante el análisis se evalúan las evidencias disponibles, el contexto del caso y los antecedentes históricos antes de avanzar hacia una resolución.

5.1.5 Decisión

La decisión es la resolución final del caso y debe quedar debidamente documentada. Esta resolución puede implicar la aprobación del evento, el rechazo definitivo, el escalamiento a un nivel superior o la solicitud de información adicional al usuario u otras áreas internas. La decisión representa el cierre operativo del análisis y es un insumo crítico para auditoría, métricas y reporting.

5.1.6 Marca

La marca consiste en el etiquetado formal del caso una vez resuelto. Estas etiquetas permiten clasificar los resultados para su uso posterior en el entrenamiento y mejora continua de modelos de riesgo, en la generación de métricas operativas y estratégicas, en procesos de auditoría interna o externa y en reportes regulatorios cuando corresponda. La correcta marcación es clave para la retroalimentación del sistema.

5.1.7 Reporte

El reporte implica el registro interno del caso y, cuando resulta aplicable, la notificación o comunicación a autoridades regulatorias o a áreas internas como Compliance, Legal u Operaciones. Este paso asegura el cumplimiento normativo, la transparencia del proceso y la correcta documentación ante eventuales requerimientos regulatorios o auditorías futuras.

Esta secuencia de gestión de casos, permite que las situaciones que requieran una investigación o un análisis con mayor profundidad, sean analizadas con mayor profundidad, generando los logs y reportes necesarios para eventuales auditorías. Es importante destacar que los sistemas de prevención de fraude pueden y deben tomar decisiones automáticas y esta gestión de casos no implica que cada rechazo o bloqueo pase por todas estas etapas, pero sí es importante definir situaciones en las que sí es importante que este procedimiento se realice para mayor conocimiento de lo sucedido, reporte y retroalimentación.

5.2 Evidencias mínimas por caso

Para garantizar la trazabilidad completa de cada decisión y asegurar una adecuada defensa ante auditorías internas, externas o requerimientos regulatorios, todos los casos gestionados deben contar con un conjunto de evidencias estructuradas, coherentes y fácilmente auditables. Estas evidencias constituyen el respaldo objetivo de las evaluaciones realizadas por los sistemas automáticos y por los analistas, y permiten reconstruir de forma precisa el contexto del evento analizado.

En primer lugar, se deben conservar evidencias de carácter técnico que documenten el evento en sí y su evaluación por la plataforma.

Esto incluye los registros de logs asociados al evento, con el detalle de los requests y responses intercambiados, así como las reglas, controles o modelos que hayan sido activados durante el análisis. Asimismo, resulta fundamental preservar la información del device fingerprint utilizado, la dirección IP de origen junto con su geolocalización, y el user agent reportado, ya que estos elementos permiten validar la consistencia técnica del acceso o de la transacción y detectar posibles señales de suplantación, automatización o uso de infraestructura anómala.

Adicionalmente, cada caso debe incorporar evidencias de comportamiento que reflejen la actividad histórica y el patrón de uso del usuario o cuenta involucrada. Esto comprende el historial transaccional relevante, el análisis de patrones de comportamiento habituales y desviaciones significativas, así como métricas de velocity asociadas a intentos, montos y frecuencia de operaciones. Este conjunto de información permite contextualizar el evento dentro del comportamiento normal del cliente y sustentar la identificación de anomalías o abusos.

Por otra parte, resulta clave incluir evidencias de tipo relacional que permitan analizar el vínculo del usuario o cuenta con otros actores del ecosistema.

Esto abarca el análisis de relaciones entre cuentas potencialmente involucradas en esquemas de muleo o triangulación, la identificación de dispositivos compartidos entre múltiples usuarios y las coincidencias de datos sensibles o semi-sensibles, como correos electrónicos, números telefónicos o documentos de identidad. Este enfoque relacional es especialmente relevante para la detección de fraude organizado y redes coordinadas.

Finalmente, los casos deben complementarse con evidencias externas que aporten contexto adicional y soporte regulatorio a la decisión. Entre ellas se incluyen los resultados de cruces contra listas AML y sancionatorias, la existencia de reportes previos asociados al usuario o a la cuenta, y la información proveniente de reclamos, disputas o chargebacks históricos. La integración de estas fuentes externas fortalece la robustez del análisis y permite demostrar diligencia debida frente a organismos de control y auditoría.

En conjunto, este esquema de evidencias garantiza un marco sólido de trazabilidad, explicabilidad y defensa, alineado con las mejores prácticas de la industria y con los estándares regulatorios aplicables a la prevención de fraude y al cumplimiento normativo.

Es recomendable contar con una plataforma unificada que permita el registro y recopilación de todos estos datos y eventos, a modo de simplificar el análisis, reporte y auditorías.

6. Políticas formales

Toda empresa debe contar desde un primer momento con políticas de riesgo, abordando estos temas en la estrategia del negocio. Esto Incluye:

6.1 Política de prevención de fraude

Define los principios, responsabilidades y controles destinados a identificar, prevenir, detectar y responder a eventos de fraude en todos los canales y productos de la organización. Establece el uso de reglas, monitoreo transaccional, análisis de comportamiento y gestión de alertas, así como los criterios de decisión (aprobación, revisión o rechazo), asegurando un balance adecuado entre mitigación de riesgo y experiencia de usuario.

6.2 Política AML (Prevención de lavado de activos)

Establece el marco para la identificación, monitoreo y reporte de operaciones sospechosas, alineado con la normativa local y estándares internacionales.

Incluye lineamientos sobre KYC/KYB, evaluación de riesgo del cliente, monitoreo transaccional continuo, detección de patrones de lavado y los procedimientos para la generación y escalamiento de reportes a las autoridades competentes.

6.3 Política de identidad

Define cómo la organización valida, gestiona y protege la identidad de sus usuarios y clientes a lo largo de todo el ciclo de vida. Incluye criterios de verificación documental, biometría (cuando aplique), controles contra identidades sintéticas o robadas y procesos de actualización de datos, garantizando que cada cuenta esté vinculada a una identidad legítima y verificable.

6.4 Política de autenticación

Establece los mecanismos de autenticación permitidos y obligatorios para el acceso a cuentas, sistemas y operaciones sensibles. Define el uso de contraseñas robustas, autenticación multifactor (MFA), controles adaptativos basados en riesgo y gestión de sesiones, con el objetivo de reducir riesgos de account takeover sin fricciones innecesarias para el usuario legítimo.

6.5 Política de monitoreo y límites

Define los criterios para el monitoreo continuo de operaciones y la aplicación de límites transaccionales dinámicos según el perfil de riesgo del cliente.

Incluye límites por monto, frecuencia, canal, geografía y comportamiento, así como mecanismos de alertas automáticas ante desvíos, permitiendo prevenir abusos, fraudes y exposiciones operativas excesivas.

6.6 Política de logs y auditoría

Establece la obligación de registrar de forma íntegra, trazable e inalterable todos los eventos relevantes de negocio, seguridad y riesgo. Define qué eventos deben loguearse, los tiempos de retención, los controles de acceso a la información y los procedimientos de auditoría interna y externa, asegurando evidencia suficiente ante incidentes, investigaciones y requerimientos regulatorios.

6.7 Política de gestión de casos

Define el proceso formal para la creación, análisis, resolución y cierre de casos de fraude, AML y seguridad. Establece estados, tiempos de resolución, roles y responsabilidades, criterios de escalamiento y documentación obligatoria, garantizando decisiones consistentes, trazables y defendibles frente a auditorías o reclamos.

6.8 Política de protección de datos

Establece los principios y medidas para la protección de datos personales y sensibles, alineados con regulaciones de privacidad aplicables.

Incluye criterios de minimización, cifrado, control de accesos, retención y eliminación segura de datos, así como la gestión de incidentes de seguridad, garantizando confidencialidad, integridad y disponibilidad de la información.

Estas políticas deben contar con un responsable designado y aprobación de la alta dirección. Es importante que las políticas se mantengan actualizadas y reflejen la realidad de las operaciones y controles de la empresa. Por más burocráticas que puedan parecer, la definición de las mismas son un elemento clave para una correcta gestión del riesgo.

7. KPIs

7.1 Métricas de fraude y riesgo

Tasa de fraude (%)
Mide el porcentaje de transacciones confirmadas como fraudulentas sobre el total de transacciones procesadas. Es el indicador principal del nivel de exposición al fraude y permite evaluar la efectividad global de los controles implementados.

Falsos positivos (%)
Indica el porcentaje de transacciones legítimas que fueron incorrectamente bloqueadas o rechazadas por los sistemas de prevención. Un nivel elevado impacta directamente en la experiencia del usuario y en los ingresos del negocio.

Tiempo de resolución
Refleja el tiempo promedio desde la generación de una alerta hasta su cierre definitivo. Es clave para medir la eficiencia operativa del equipo de fraude y el cumplimiento de SLAs internos y regulatorios.

Alertas por tipo
Distribuye las alertas generadas según su categoría (fraude transaccional, ATO, AML, onboarding, comportamiento anómalo). Permite identificar patrones dominantes de riesgo y ajustar reglas y modelos.

Operaciones por nivel de riesgo
Clasifica las transacciones u operaciones en niveles de riesgo (alto, medio, bajo) según el scoring antifraude. Ayuda a entender el perfil de riesgo del negocio y a definir umbrales de acción.

Aprobación de transacciones (%)
Mide el porcentaje de transacciones aprobadas sobre el total evaluado. Es un KPI de equilibrio entre control de fraude y continuidad del negocio.

Casos mule detectados
Cantidad de cuentas identificadas como mulas financieras. Es un indicador crítico para fraude P2P, AML y redes organizadas, y suele correlacionar con riesgo sistémico.

Fraude evitado ($)
Monto estimado de pérdidas prevenidas gracias a bloqueos, rechazos o acciones antifraude. Es el KPI que mejor traduce el impacto del sistema de fraude en términos financieros.

7.2 Métricas de chargebacks y rechazos

Tasa de chargeback USD (>60d)
Monto total de contracargos recibidos después de 60 días sobre el total de transacciones aprobadas. Es un indicador financiero clave para esquemas de tarjetas y monitoreo de riesgo histórico.

Tasa de chargeback Q (>60d)
Cantidad de contracargos sobre el total de transacciones aprobadas. Complementa la métrica en USD y permite analizar volumen más allá del monto.

Tasa de chargeback USD proyectado (real time)
Estimación en tiempo real del monto de chargebacks futuros, ajustando por el ratio histórico de reporte. Permite tomar decisiones preventivas antes del impacto financiero real.

Tasa de chargeback Q proyectado (real time)
Proyección del volumen de contracargos futuros sobre las transacciones actuales. Útil para monitoreo temprano de deterioro en la calidad del tráfico.

Tasa de rechazo fraud risk USD
Monto de transacciones rechazadas por riesgo de fraude sobre el total de transacciones evaluadas. Permite medir el costo económico del control antifraude.

Tasa de rechazo fraud risk Q
Cantidad de transacciones rechazadas por riesgo sobre el total procesado. Ayuda a detectar sobre-bloqueo o reglas demasiado agresivas.

Reason de fraude en chargebacks USD
Distribución del monto de contracargos por categoría de fraude. Permite identificar los tipos de fraude con mayor impacto económico.

Reason de fraude en chargebacks Q
Distribución del volumen de contracargos por tipo de fraude. Útil para priorizar acciones operativas y ajustes de reglas.

7.3 Métricas operativos y de usuarios

Tasa de bloqueo antifraude
Porcentaje de usuarios bloqueados por controles antifraude sobre el total de usuarios activos. Refleja la agresividad del sistema y su impacto en la base de clientes.

Ratio de rehabilitación
Proporción de bloqueos que fueron levantados tras revisión manual. Es un indicador directo de calidad de las decisiones automáticas.

Distribución de usuarios en matriz de riesgo de fraude
Clasificación de usuarios en riesgo alto, medio o bajo. Permite segmentar controles y definir estrategias diferenciadas.

Tasa de alertas de fraude
Cantidad de alertas de fraude sobre el total de alertas revisadas. Ayuda a evaluar la precisión del sistema de generación de alertas.

7.4 Métricas de onboarding (KYC)

Aprobación en onboarding
Porcentaje de procesos KYC aprobados sobre el total completado. Refleja la calidad del funnel de alta y los controles de identidad.

Drop-off en onboarding
Relación entre KYC completados y KYC iniciados. Permite medir fricción en el proceso de alta y su impacto comercial.

Rechazo por fraude en onboarding
Porcentaje de altas rechazadas por fraude o identidad falsa. Indicador clave para prevención temprana de cuentas de riesgo.

7.5 Métricas de AML

Distribución de usuarios en matriz de riesgo AML
Clasifica a los usuarios según su riesgo AML (alto, medio, bajo). Es fundamental para priorizar monitoreo y revisiones regulatorias.

Reportes AML generados
Cantidad de reportes de operaciones sospechosas generados por cada 1.000 usuarios activos. Refleja la efectividad del monitoreo AML.

Usuarios con match en listas
Porcentaje de usuarios con coincidencias en listas restrictivas o sancionatorias. Permite medir exposición regulatoria.

Usuarios PEPs
Porcentaje de usuarios identificados como Personas Políticamente Expuestas sobre el total. Es un KPI clave para cumplimiento y supervisión reforzada.

8. Conclusiones

El presente manual establece un **marco integral de referencia para la prevención del fraude y del lavado de activos en fintechs que operan en Uruguay,** alineado con estándares internacionales y adaptado a las particularidades del ecosistema local y regional. Su objetivo es servir como guía estratégica y operativa para abordar de forma estructurada riesgos que hoy forman parte inherente de cualquier operación financiera digital.

La evidencia demuestra que el fraude digital y las estructuras de lavado de activos no constituyen eventos excepcionales, sino amenazas permanentes y previsibles. En la práctica, muchas organizaciones tienden a enfrentar estos riesgos de manera reactiva, actuando únicamente cuando las pérdidas económicas, los reclamos de usuarios o las exigencias regulatorias ya se han materializado.

Este enfoque reactivo incrementa de forma significativa el impacto financiero de los incidentes, eleva el riesgo reputacional, amplifica la exposición regulatoria y genera mayores costos operativos asociados a correcciones tardías y medidas de contingencia.

En contraposición, un modelo preventivo, basado en un enfoque de riesgo y sustentado en múltiples capas de control, permite a las fintechs detectar y mitigar amenazas en etapas tempranas del ciclo operativo. Este enfoque reduce las pérdidas económicas y los falsos positivos, facilita la escalabilidad segura del negocio, preserva una experiencia de usuario competitiva y demuestra un mayor nivel de madurez operativa frente a reguladores, inversores y socios estratégicos.

La implementación de políticas formales, controles técnicos, reglas antifraude, modelos de análisis avanzado, esquemas de monitoreo continuo y una gestión estructurada de casos no debe interpretarse como un freno al crecimiento, sino como un habilitador clave para una escalabilidad sostenible y ordenada. Estos elementos constituyen la base sobre la cual se construye una operación resiliente, capaz de crecer sin comprometer la seguridad ni el cumplimiento normativo.

Resulta fundamental que cada fintech defina de manera explícita su apetito y tolerancia al riesgo, adapte este marco a su etapa de madurez y a su modelo de negocio, establezca responsables claros para la gestión de fraude y AML, revise y actualice periódicamente sus controles y métricas, e incorpore procesos de mejora continua basados en datos y resultados reales.

Este manual no pretende ser una solución cerrada ni universal, sino una base de referencia sobre la cual cada organización pueda construir su propia estrategia de prevención de fraude y lavado de activos, ajustada a su realidad operativa, regulatoria y tecnológica. Abordar estos riesgos desde el inicio, con una visión estratégica y apoyándose en herramientas especializadas y asesoría experta, constituye hoy una ventaja competitiva tangible y un requisito esencial para la sostenibilidad de cualquier fintech moderna.