CONFIDENCIAL

FINTRIXS PAY

Riesgo operacional y prevención del fraude

05.2 — POLÍTICA DE PREVENCIÓN Y DETECCIÓN DE FRAUDE

CÓDIGO	ROF-002
VERSIÓN	1.0 — 16 de abril de 2026
APROBADO POR	Representante Legal / CTO / CISO
VIGENCIA	24 meses

FINTRIXS S.A.S. · NIT 901.994.194-3
Paquete de Due Diligence — Banco Sponsor Agregador
Emitido el 16 de abril de 2026 — Versión 1.0 del paquete

05.2 — POLÍTICA DE PREVENCIÓN Y DETECCIÓN DE FRAUDE · Código: ROF-002 · Versión: 1.0 — 16 de abril de 2026 · FINTRIXS S.A.S.

1. Objetivo

Establecer el marco de prevención, detección, investigación y respuesta al fraude interno y externo en la operación de Fintrixs Pay.

2. Clases de fraude consideradas

2.1. Fraude externo (tarjetahabientes y comercios)

- Uso de tarjetas robadas o sintéticas.
- Account takeover (ATO) de cuentas de comercios.
- Compras fraudulentas en venta no presente.
- Chargebacks abusivos.
- Transaction laundering (uso de un comercio legítimo para lavar transacciones de otro negocio).
- Phishing dirigido a tarjetahabientes o comercios.

2.2. Fraude interno

- Infidelidad de empleados (acceso indebido a datos, manipulación de transacciones).
- Colusión con terceros.
- Abuso de privilegios administrativos.

3. Principios

1. Prevención sobre detección; detección sobre reacción.
2. Segregación de funciones.
3. Mínimo privilegio y MFA.
4. Trazabilidad total (auditoría inmutable en `admin-audit-service`).
5. Cooperación con redes adquirentes y banco sponsor.

4. Controles preventivos

Control	Detalle
KYC/KYB robusto	Ver procedimiento SAR-002.
MFA obligatoria	Para operadores y para operaciones de alto riesgo en comercios.
Tokenización	PAN nunca visible en la plataforma.
3DS 2.2	Activo en venta no presente, vía red adquirente Credibanco.
Control de acceso a datos	RBAC + RLS + auditoría.
Onboarding con validación de identidad	Fuentes oficiales (Registraduría, DIAN, RUES).
Límites transaccionales iniciales	Ramp-up gradual por subcomercio.
Segregación de ambientes	Dev / staging / prod aislados.

5. Controles detectivos

Control	Detalle
Monitoreo transaccional	Reglas y modelos de scoring sobre eventos Kafka.
Monitoreo comportamental	Detección de anomalías (volumen, ticket promedio, geografía, horarios).
Reglas de velocidad	Límites por BIN, dispositivo, IP, geolocalización.
Análisis de grafos	Relaciones entre comercios, dispositivos, IPs y tarjetas.
Detección de transaction laundering	MCC vs. patrón real de pagos.
Alertas tempranas	KRIs (chargeback rate, fraud rate, approval rate).
SIEM	Correlación de eventos técnicos y transaccionales.
Sandbox de pruebas	Análisis previo antes de activar nuevos BINs o canales.

6. Controles correctivos

- Bloqueo inmediato del subcomercio sospechoso.
- Retención de fondos conforme a contrato y regulación.
- Notificación al banco sponsor, Credibanco y titular cuando aplica.

- Reporte a UIAF (si se presume LAFT).
- Disputa de contracargos según reglas Visa.

7. Gestión de contracargos

- Recepción y clasificación automática.
- Plazos Visa: atención en 7 días hábiles.
- Evidencia consolidada (logs, 3DS, autenticación del comercio, tracking de entrega).
- Registro en `admin-audit-service`.

8. Notificación a clientes

- Notificaciones transaccionales por email y/o push.
- Alertas ante operaciones inusuales.
- Canal de contacto para reporte de transacción no reconocida.

9. KRIs

Indicador	Umbral de alerta	Fuente
Fraud rate (%)	> 0.1% en 24h	Motor transaccional
Chargeback rate (%)	> 0.9%	Red adquirente
Approval rate anómalo	Desviación > 10%	Estadística histórica
Intentos fallidos de autenticación	> umbral por minuto	`auth-service`
Anomalías de comportamiento	Score > X	Motor analítico

10. Inteligencia de amenazas

- Feeds de tarjetas comprometidas (CPP — Common Purchase Point).
- Listas de dispositivos fraudulentos (device fingerprinting).
- Colaboración con redes y banco sponsor en alertas de fraude.

11. Cultura y capacitación

- Capacitación anual a operaciones y soporte.
- Playbooks específicos para casos comunes (chargeback, ATO, phishing).

- Canal interno para reporte anónimo.

12. Responsables

Rol	Responsabilidad
CTO / CISO	Controles técnicos, modelos, SIEM
Operaciones / Riesgos	Monitoreo operativo, disputas
Representante Legal	Toma de decisiones críticas, notificaciones regulatorias
Comité antifraude	Revisión quincenal de KRIs e incidentes