CONFIDENCIAL

FINTRIXS PAY

Riesgo operacional y prevención del fraude

05.3 — AUTENTICACIÓN 3D SECURE Y TOKENIZACIÓN

CÓDIGO	ROF-003
VERSIÓN	1.0 — 16 de abril de 2026
APROBADO POR	Representante Legal
VIGENCIA	—

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

05.3 — AUTENTICACIÓN 3D SECURE Y TOKENIZACIÓN · Código: ROF-003 · Versión: 1.0 — 16 de abril de 2026 · FINTRIXS S.A.S.

1. 3D Secure 2.2

1.1. Esquema

Fintrixs Pay soporta **3D Secure 2.2** (EMV 3DS 2.2) como protocolo de autenticación para venta no presente.

- **Proveedor del servicio 3DS:** Credibanco como red adquirente, que a su vez se integra con el **Directory Server de Visa** (Visa Secure).
- **Intermediación:** Fintrixs actúa como 3DS Requestor Initiator dentro del ecosistema.
- **Mensajes:** AReq/ARes, CReq/CRes, RReq/RRes intercambiados sobre canales certificados.

1.2. Flujo transaccional (resumen)

1. El comercio envía a Fintrixs Pay los datos de la transacción.
2. `tokenization-service` tokeniza la tarjeta (si no estaba tokenizada).
3. Fintrixs enruta al adquirente (Credibanco) junto con la data 3DS.
4. Credibanco inicia el flujo 3DS con el emisor.
5. Respuesta: **frictionless** (autenticada sin interacción), **challenge** (interacción del titular), o **no autenticada**.
6. Resultado se comunica al comercio; transacción continúa o se rechaza.
7. Toda la traza queda en `admin-audit-service` y en `payments-api` con outbox.

1.3. Cobertura

- 100% de las transacciones con tarjeta en venta no presente cuando el emisor soporta 3DS 2.2.
- Fallback a 3DS 1.0 solo si la red/emisor no soporta 2.x.
- Reglas de exención bien definidas (p. ej., recurring, MIT) según normativa de la red.

1.4. Evidencia

- CAVV/EECI recibidos y almacenados para cada transacción autenticada.
- ECI (Electronic Commerce Indicator) clasifica el resultado de la autenticación.
- En contracargos de fraude, esta evidencia se presenta al emisor.

2. Tokenización

2.1. Modelo híbrido

Fintrixs opera un modelo de tokenización en dos capas:

1. **Tokenización de red (Visa/Credibanco)** — se usa cuando el emisor soporta network tokenization, maximizando tasa de aprobación y permitiendo actualización automática en caso de reemisión de tarjeta.
2. **Tokenización interna (Fintrixs)** — implementada por `tokenization-service` + `card-vault-service` (PCI DSS). Los demás microservicios solo manejan tokens Fintrixs.

2.2. Ciclo del token

1. El PAN ingresa **una sola vez** al `card-vault-service` vía canal TLS + mTLS desde el frontend (iframe o dropin) que nunca expone el PAN al backend no-PCI.
2. El vault cifra con AES-256 (llave gestionada por KMS) y almacena en un schema aislado.
3. `tokenization-service` emite un token opaco no-reversible fuera del vault.
4. El resto del ecosistema opera con tokens.
5. La detokenización se hace exclusivamente en el vault, a petición autorizada (pago, disputa, reembolso).

2.3. Implementación

- El vault vive en un VPC / subnet PCI dedicada.
- Network policies restrictivas.
- Acceso por JWT con scope PCI + MFA.
- Registro exhaustivo de cada operación con IDs de correlación.
- Retención por política: token perdura; dato subyacente se elimina según PCI DSS cuando ya no se requiere.

2.4. Documentación asociada

- `docs/security/TOKENIZATION_FLOW.md` — flujo detallado.
- `docs/pci-dss/data_flow_diagram.md` — DFD PCI.
- `docs/pci-dss/EVD-CRYPTO-DATA-evidence.md` — evidencia de cifrado y protección.

3. Estado actual

Ítem	Estado
3DS 2.2 operativo	SÍ (vía Credibanco)
Tokenización de red	SÍ
Tokenización interna	SÍ (implementada)
Certificación PCI DSS v4.0	En proceso — ~95% de avance
Auditor externo QSA	Contratación en curso