CONFIDENCIAL

FINTRIXS PAY

Anexos técnicos

09.2 — FLUJO DE DATOS PCI (DATA FLOW DIAGRAM)

CÓDIGO	ANX-002
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

09.2 — FLUJO DE DATOS PCI (DATA FLOW DIAGRAM) · Código: ANX-002 · Versión: 1.0 — 16 de abril de 2026 · FINTRIXS S.A.S.

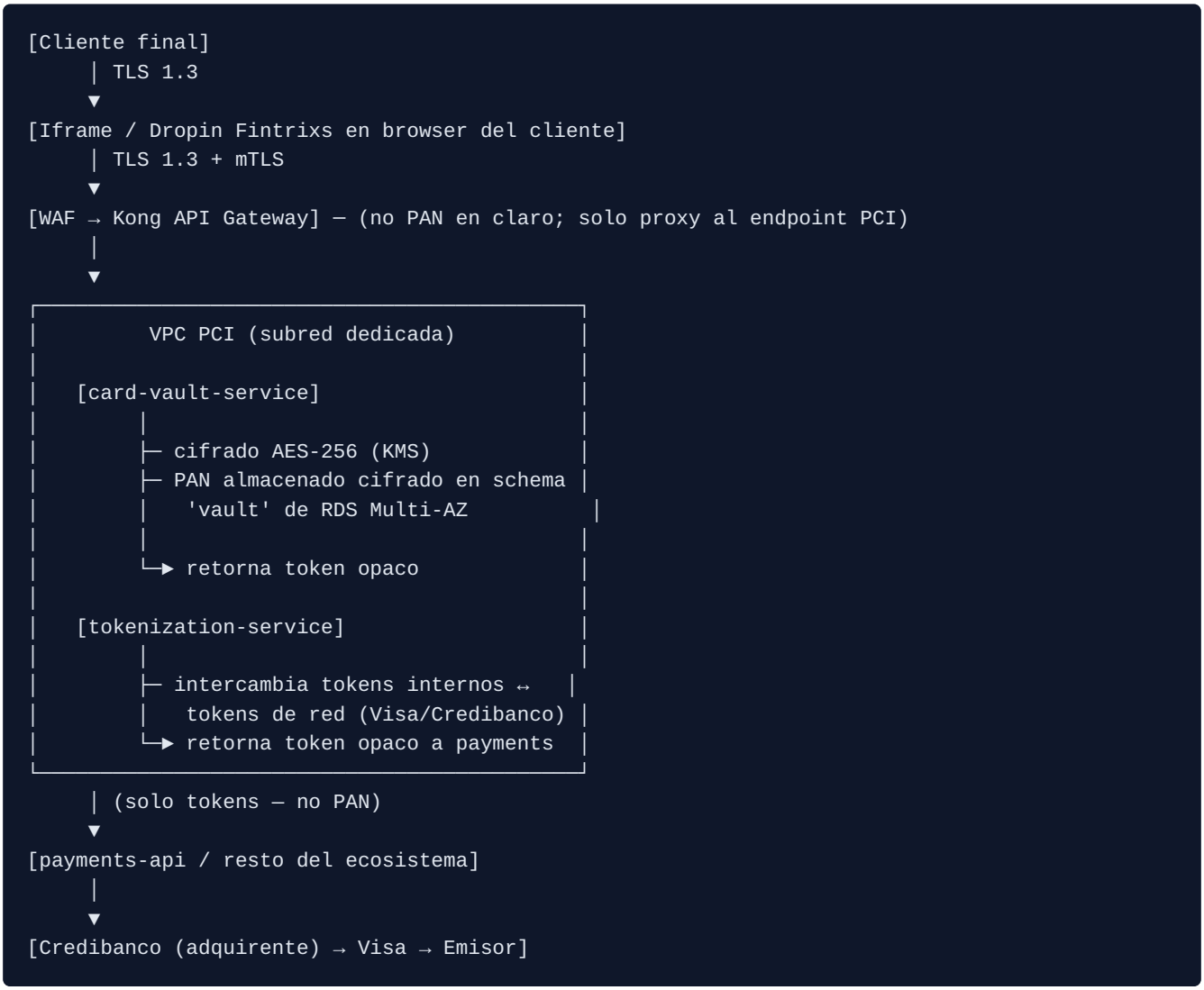
1. Cardholder Data Environment (CDE)

El CDE está **limitado exclusivamente** a dos servicios y a su infraestructura de soporte:

- `card-vault-service` (puerto 3003)
- `tokenization-service` (puerto 3002)

Ningún otro microservicio ni componente de infraestructura procesa, almacena o transmite PAN en claro.

2. Diagrama de flujo (descripción textual)



3. Datos manejados por elemento

Componente	Dato	Estado	Protección
Browser cliente	PAN	En tránsito	TLS 1.3
Iframe Fintrixs	PAN	En tránsito	TLS 1.3 + CSP estricto
Kong	—	Proxy	TLS passthrough hacia vault
card-vault-service	PAN	En reposo + tránsito	AES-256, KMS, mTLS, RBAC, logs con masking
Schema `vault` RDS	PAN cifrado	En reposo	AES-256, KMS, acceso restringido
tokenization-service	Token interno	Volátil	mTLS, RBAC
payments-api	Token	En reposo	Token en DB, PAN nunca llega aquí
Kafka	Token	Mensajes	TLS + SASL, ACLs por topic
admin-audit-service	Tokens y eventos (sin PAN)	Append-only	Auditoría inmutable
Logs (toda la plataforma)	Tokens y hashes (sin PAN)	—	`@fintrix/logging` con masking automático

4. Reglas clave del flujo

- **Una sola puerta de entrada del PAN:** el iframe/dropin envía el PAN directamente al `card-vault-service`.
- **Separación física:** `card-vault-service` vive en su propia subred VPC con network policies restrictivas.
- **Sin paso intermedio:** el backend no-PCI nunca toca el PAN; opera con tokens.
- **Detokenización controlada:** ocurre solo en el vault, bajo contexto autorizado (pago, disputa, reembolso), con correlación de auditoría.
- **Cifrado en reposo y tránsito:** TLS 1.3 externa; mTLS interno; AES-256 para datos en reposo; llaves en AWS KMS con rotación automatizada.
- **Masking de logs:** el logger rechaza payloads que coincidan con patrones PAN; violaciones fallan el CI.
- **Retención mínima:** el PAN se conserva solo el tiempo requerido por reglas de negocio y normativa; tras expiración se elimina criptográficamente (destrucción de la clave de objeto).

5. Controles PCI DSS asociados (mapeo rápido)

Req. PCI DSS v4.0	Control en Fintrixs
1.2.4 (DFD)	Este documento + `docs/pci-dss/data_flow_diagram.md`
2.2 (Configuración segura)	Hardening CIS + IaC
3.5 (Protección de PAN)	AES-256, KMS, masking
3.6 (Llaves criptográficas)	KMS, rotación automatizada
4.1 (Cifrado en tránsito)	TLS 1.3 + mTLS
6.2 (Desarrollo seguro)	OWASP ASVS, SAST/DAST/SCA, peer review
7.1 (Control de acceso)	RBAC + JWT + MFA
8.3 (MFA)	MFA obligatorio para accesos privilegiados y acceso al vault
10 (Monitoreo)	Logs + SIEM + `admin-audit-service`
11 (Testing)	Pentest anual + escaneo continuo
12 (Política)	POL-001 a POL-015 en `docs/security/policies/`

6. Evidencia de soporte

- `docs/security/TOKENIZATION_FLOW.md` — flujo técnico detallado de tokenización.
- `docs/pci-dss/data_flow_diagram.md` — DFD maestro.
- `docs/pci-dss/EVD-CRYPTO-DATA-evidence.md` — evidencia de cifrado.
- `docs/pci-dss/EVD-ACCESS-CONTROL-evidence.md` — evidencia de control de acceso.
- `docs/pci-dss/EVD-LOGGING-evidence.md` — evidencia de logging y monitoreo.

(Los documentos completos se entregan bajo NDA por contener detalles sensibles.)