CONFIDENCIAL

FINTRIXS PAY

Ciberseguridad y seguridad de la información

04.2 — MARCO DE REFERENCIA Y ESTÁNDARES ADOPTADOS

CÓDIGO	CIB-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

04.2 — MARCO DE REFERENCIA Y ESTÁNDARES ADOPTADOS · Código: CIB-002 · Versión: 1.0 — 16 de abril de 2026 · FINTRIXS S.A.S.

1. Estándares internacionales adoptados

Estándar / Marco	Nivel de adopción	Evidencia
PCI DSS v4.0	En implementación — avance ~95%	Pre-auditoría completada; evidencias en `docs/pci-dss/` (Data Flow, Firewall, Logging, Crypto, Access, Incident, Anti-Malware, Secure Dev, Governance)
NIST Cybersecurity Framework (CSF 2.0)	Adoptado como marco guía	Mapa de controles en documento 04.6
ISO/IEC 27001:2022	En proceso de alineación	Controles anexo A implementados; certificación en roadmap 2027
OWASP ASVS v4 / Top 10	Adoptado	Requisitos en el Secure SDLC, validaciones en pipeline CI
CSA CCM v4 (Cloud Security Alliance)	Adoptado en controles cloud	Hardening AWS + política Circular 005/2019
ITIL v4	Adoptado en operación	Gestión de cambios, incidentes, problemas
NIST SP 800-61r2	Adoptado	Runbooks de respuesta a incidentes
NIST SP 800-53 / 800-171	Referencia complementaria	Controles de protección de información
CIS Benchmarks	Adoptado en hardening	Imágenes base y hardening scripts
ISO 22301 — BCMS	Adopción parcial	BCP/DRP documentados (carpeta `07_Continuidad_Negocio/`)

2. Regulación nacional cumplida

Norma	Aplicabilidad	Evidencia
Ley 1581 de 2012 y Decreto 1377 de 2013	Protección de datos personales	Política v2.1 + procedimientos PDP-001 a PDP-006
Ley 2300 de 2023 (habeas data financiero)	Derechos de titulares de datos crediticios	Política v2.1, sección 10
Circular Externa 005 de 2019 SFC	Servicios de computación en la nube	Documento 04.6 sección 6 (controles cloud)
Circular Externa 007 de 2018 SFC	Requerimientos mínimos de ciberseguridad	Política CIB-001, gestión de incidentes, SOC-like
Circular Externa 008 de 2018 SFC	Protección del consumidor financiero en pasarelas	Tokenización + 3DS + monitoreo transaccional
Circular Externa 002 de 2024 SIC	Tratamiento de datos personales en IA	Documento PDP-006
Ley 1266 de 2008 (habeas data financiero)	Información crediticia	Procedimientos específicos cuando aplique
Ley 527 de 1999	Mensajes de datos y firma electrónica	Firma electrónica en autorizaciones
Decreto 338 de 2022	Ciberseguridad en entidades obligadas	Buenas prácticas adoptadas como referencia

3. Regulación de redes de pago

Marco	Aplicabilidad	Evidencia
PCI DSS v4.0	Pasarela de pagos (adquirencia)	Evidencia documental en `docs/pci-dss/`
EMV 3-D Secure (3DS 2.2)	Venta no presente	Integración vía Credibanco
EMV Co Chip	Si aplica en POS	Terminales certificadas de la red adquirente
Visa Core Rules	Obligaciones como participante	Cumplimiento a través del banco sponsor y Credibanco
Visa TIP/VIP (Transaction Integrity / Velocity)	Controles de fraude	Integrados vía red adquirente

4. Documentación PCI DSS disponible

El repositorio `docs/pci-dss/` contiene:

- `pci_dss_contexto_fintrixs.md` — alcance y definición del CDE.
- `scope_definition.md` — alcance formal.
- `asset_inventory.md` — inventario de activos PCI.
- `data_flow_diagram.md` — flujo de datos de tarjeta.
- `network_diagram.md` — diagrama de red segmentado.
- `firewall_rules.md` — reglas de firewall.
- `EVD-*-evidence.md` — paquete de evidencias por requisito (12 documentos).
- `compliance_checklist_preaudit.md` — check-list pre-auditoría.

5. Hojas de ruta (evidencia del estándar adoptado)

Iniciativa	Plazo
Certificación PCI DSS v4.0 — nivel aplicable	2026 Q3 (auditor externo QSA)
ISO/IEC 27001:2022 — etapa de certificación	2027 Q1
SOC 2 Type II	2027 Q2
Informe externo de ethical hacking anual	Cada 12 meses + cambios críticos
Ejercicio RED TEAM	Anual

6. Anexos del expediente

- Carta de compromiso de adopción de estándares (este documento).
- Evidencias PCI DSS pre-auditoría (carpeta `docs/pci-dss/`).
- Certificaciones de proveedores cloud (AWS SOC 2 / ISO 27001 / PCI DSS) disponibles bajo solicitud.