CONFIDENCIAL

FINTRIXS PAY

Protección de datos personales

03.1 — PROCEDIMIENTO DE CICLO DE VIDA DE DATOS PERSONALES

CÓDIGO	PDP-001
VERSIÓN	1.0 — 16 de abril de 2026
APROBADO POR	Oficial de Protección de Datos (DPO) / Representante Legal
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

03.1 — PROCEDIMIENTO DE CICLO DE VIDA DE DATOS PERSONALES · Código: PDP-001 · Versión: 1.0 — 16 de abril de 2026 · FINTRIXS S.A.S.

1. Objetivo

Definir la forma en que Fintrixs S.A.S. recolecta, almacena, usa, circula y suprime datos personales en cumplimiento de la Ley 1581 de 2012, el Decreto 1377 de 2013, la Ley 2300 de 2023 y la Circular Externa 002 de 2024 de la SIC, garantizando la trazabilidad y protección durante todo el ciclo de vida.

2. Alcance

Aplica a todos los datos personales tratados por Fintrixs en sus plataformas, incluyendo:

- **Datos de titulares / pagadores** (nombre, identificación, correo, teléfono, dirección de facturación).
- **Datos transaccionales** asociados a personas naturales.
- **Datos de representantes legales y colaboradores de subcomercios**.
- **Datos de empleados y contratistas internos**.

Datos excluidos (manejo especial): PAN (Primary Account Number) y CVV — únicamente procesados por `card-vault-service` y `tokenization-service` en zonas PCI DSS segmentadas; ver flujo específico en `16 Tokenización de Datos de Pago` de la Política v2.1.

3. Etapas del ciclo de vida

3.1. Recolección

Aspecto	Control
Principio de minimización	Solo se recolectan datos necesarios para la finalidad.
Fuente	Directamente del titular o de fuentes autorizadas (Registraduría, Cámara de Comercio) bajo autorización expresa.
Canales	Formularios web, APIs, onboarding en app, integración con redes adquirentes.
Autorización	Cada recolección requiere aviso de privacidad + casilla de autorización informada.
Registro	`onboarding-service` (puerto 3007) registra timestamp, IP, versión de la política aceptada, hash de evidencia.

3.2. Almacenamiento

Aspecto	Control
Infraestructura	AWS (us-east-1 / us-west-2) con cifrado en reposo (AES-256).
Motor	PostgreSQL 16 con RLS (Row-Level Security) — aislamiento por `merchant_id`.
Backups	Cifrados con AES-256, política 3-2-1 con snapshots automáticos.
Segmentación	Datos PCI aislados en schema y red CDE (Cardholder Data Environment).
Logs	`@fintrixs/logging` realiza masking automático de PII y PAN antes de escribir.

3.3. Uso

Finalidad	Base de legitimación	Control técnico
Procesamiento de transacciones	Ejecución contractual	Tokenización + RLS
KYC / KYB	Obligación legal (SARLAFT)	Consulta auditada vía `admin-audit-service`
Prevención de fraude	Interés legítimo	Análisis comportamental en modelos explicables
Soporte al cliente	Ejecución contractual	Acceso granular RBAC
Comunicaciones de servicio	Consentimiento / ejecución contractual	Opt-out disponible
Marketing	Consentimiento expreso	Opt-in obligatorio

3.4. Circulación / transferencia

- **Dentro de Fintrixs:** comunicación vía Kafka (patrón Outbox + Inbox) con cifrado TLS 1.3 y autenticación mTLS.
- **Hacia encargados del tratamiento:** contrato de encargo firmado + cláusulas de confidencialidad + evaluación de seguridad.
- **Transferencias internacionales:** evaluadas bajo los artículos 26 y 27 de la Ley 1581 de 2012. Fintrixs opera con proveedores de infraestructura en Estados Unidos que cumplen con estándares equivalentes (SOC 2, PCI DSS, ISO 27001).
- **Hacia redes adquirentes (Credibanco):** a través de conexiones certificadas y tokenización de PAN.

3.5. Supresión / eliminación

Tipo de dato	Retención	Motivación
Datos transaccionales	10 años	Estatuto Tributario + normativa financiera
Datos KYC/KYB	5 años posteriores al fin de la relación	Ley 526/1999
Datos de marketing	Hasta revocatoria o 2 años sin interacción	Consentimiento
Logs de auditoría	5 años (inmutables)	Buenas prácticas y PCI DSS Req. 10
Cookies técnicas / analíticas	12 meses	Best practice

Procedimiento de supresión:

1. Verificación de obligaciones legales vigentes.
2. Ejecución vía endpoint interno del `auth-service` / `onboarding-service` (`DELETE /titulares/{id}`) con control dual (dos aprobadores).
3. Emisión de evento `fintrixs.privacy.right_to_erasure` consumido por todos los servicios poseedores.
4. Los servicios confirman supresión o seudonimización irreversible en los casos en que se conserven por obligaciones legales.
5. Registro de evidencia en `admin-audit-service` con hash SHA-256 de la constancia.

4. Controles transversales

- **Cifrado en reposo:** AES-256 (KMS gestionado).
- **Cifrado en tránsito:** TLS 1.2+ (preferente TLS 1.3) con mTLS en integraciones críticas.
- **Control de acceso:** RBAC + ABAC + MFA para roles privilegiados.
- **Logging PCI-safe:** `@fintrixs/logging` con masking de PAN, CVV, contraseñas y datos personales sensibles.
- **Multi-tenancy:** Row-Level Security en PostgreSQL con contexto `app.current_merchant_id` inyectado desde el JWT.
- **DLP:** monitoreo de exfiltración de datos en los perímetros.

5. Indicadores (KPI)

KPI	Objetivo
Tiempo de atención de derechos ARCO	≤ 10 días hábiles (SIC: 15)
% de accesos con MFA a datos personales	100%
Incidentes de seguridad de datos por trimestre	0 incidentes materiales
Cobertura de cifrado en reposo	100%
Cumplimiento de retención (auditoría de supresión)	100%

6. Evidencia técnica

Los controles de este procedimiento están implementados en los microservicios y paquetes:

- `auth-service` (3001) — gestión de sesiones y JWT RS256.
- `tokenization-service` (3002) — tokenización de PANs.
- `card-vault-service` (3003) — vault PCI de datos de tarjeta.
- `onboarding-service` (3007) — KYC/KYB, subida de documentos (S3/MinIO).
- `admin-audit-service` (3009) — auditoría inmutable.
- `@fintrixs/tenant-context` — aislamiento multi-tenant.
- `@fintrixs/logging` — logger estructurado con masking automático.