CONFIDENCIAL

FINTRIXS PAY

Ciberseguridad y seguridad de la información

04.1 — POLÍTICA DE CIBERSEGURIDAD Y SEGURIDAD DE LA INFORMACIÓN

CÓDIGO	CIB-001
VERSIÓN	1.0 — 16 de abril de 2026
APROBADO POR	Representante Legal y máximo órgano de administración de Fintrixs S.A.S.
VIGENCIA	24 meses (revisión anual obligatoria)

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

04.1 — POLÍTICA DE CIBERSEGURIDAD Y SEGURIDAD DE LA INFORMACIÓN · Código: CIB-001 · Versión: 1.0 — 16 de abril de 2026 · FINTRIXS S.A.S.

1. Declaración de compromiso

Fintrixs S.A.S. reconoce la información, los sistemas que la soportan y los procesos transaccionales de su pasarela de pagos como activos estratégicos. La Administración se compromete a:

- Proteger la confidencialidad, integridad y disponibilidad de la información.
- Cumplir con la regulación aplicable (Ley 1581/2012, Circulares SFC 005/2019, 007/2018, 008/2018, Ley 2300/2023) y con estándares internacionales (PCI DSS v4.0, NIST CSF, ISO/IEC 27001, OWASP, CSA).
- Asignar los recursos humanos, tecnológicos y financieros necesarios.
- Promover una cultura de ciberseguridad en toda la organización.
- Mejorar continuamente el Sistema de Gestión de Seguridad de la Información (SGSI).

2. Alcance

Aplica a todos los activos de información, infraestructura tecnológica, empleados, contratistas, aliados y proveedores que interactúen con la plataforma Fintrixs Pay y sus microservicios (aproximadamente 15 servicios NestJS, frontend Vue 3, bases de datos PostgreSQL, Kafka, Kong, S3/MinIO).

3. Objetivos de seguridad

1. **Confidencialidad:** solo las personas autorizadas acceden a la información.
2. **Integridad:** la información se mantiene exacta y completa.
3. **Disponibilidad:** la información y los servicios están accesibles cuando se requieran (RTO ≤ 4 h, RPO ≤ 15 min para servicios críticos).
4. **Trazabilidad:** toda acción sobre información sensible queda registrada.
5. **Cumplimiento:** se observan las normas aplicables al sector.

4. Estructura de gobierno

Rol	Responsabilidad
Representante Legal	Aprueba la política y provee recursos
CISO / CTO	Lidera el SGSI, gestiona el presupuesto de seguridad
DPO	Protección de datos personales
Líder de Plataforma	Operación segura y hardening
Líder de Desarrollo	Secure SDLC, OWASP
Comité de Seguridad	Revisa riesgos, incidentes, mejoras (mensual)
Todos los colaboradores	Cumplen la política y reportan eventos

5. Dominios de control (SGSI)

5.1. Gobierno y gestión del riesgo

- Inventario de activos de información clasificado (ver `09_Anexos_Tecnicos/inventario_activos.md`).
- Análisis de riesgo basado en NIST 800-30 y TRA (Targeted Risk Analysis por PCI DSS v4.0 Req. 12.3).
- Revisión anual del SGSI.

5.2. Recursos humanos

- Verificación de antecedentes en el proceso de vinculación.
- Acuerdos de confidencialidad y código de ética.
- Formación obligatoria (onboarding + refresco anual) en ciberseguridad, PCI DSS y protección de datos.
- Desvinculación segura (revocación inmediata de accesos).

5.3. Gestión de activos

- Clasificación: Pública / Interna / Confidencial / Restringida (PCI/PII).
- Ciclo de vida documentado.

5.4. Control de acceso

- Principio de mínimo privilegio y segregación de funciones.

- RBAC + ABAC.
- MFA obligatoria para roles privilegiados y VPN corporativa.
- Revisión trimestral de accesos.
- SSO corporativo con IDP federado.
- JWT RS256 para autenticación API.

5.5. Criptografía

- TLS 1.2+ (preferente 1.3) en todas las comunicaciones.
- AES-256 para datos en reposo.
- KMS centralizado con rotación periódica de llaves.
- Prohibido SHA-1 y MD5 en nuevas implementaciones.
- Gestión de certificados digitales centralizada.

5.6. Seguridad física y del entorno

- Nube AWS (certificada ISO 27001, SOC 2, PCI DSS).
- Oficinas con control de acceso físico, videovigilancia y políticas de escritorio limpio.

5.7. Operaciones

- Gestión de cambios (SDLC con revisión, QA, aprobación, CI/CD).
- Separación de ambientes (dev / staging / prod).
- Hardening basado en CIS Benchmarks.
- Antimalware y EDR en endpoints.
- Monitoreo 24/7 con alertas automatizadas.

5.8. Comunicaciones

- Segmentación de red (CDE segregado del resto).
- WAF, IDS/IPS, DDoS protection (CloudFront / AWS Shield / Kong rate-limiting).
- Zero Trust (cada microservicio autentica al otro con mTLS).

5.9. Desarrollo seguro

- Secure SDLC basado en OWASP SAMM y ASVS.
- Revisión de código obligatoria antes de merge a `main`.
- SAST, SCA, DAST automatizados en CI.
- Pentesting anual externo + internos trimestrales.
- Gestión de secretos con KMS / vault (nunca en repos ni en variables planas).

5.10. Proveedores y terceros

- Evaluación de seguridad antes de contratar.
- DPA + NDA.
- Monitoreo periódico.

5.11. Gestión de incidentes

- Runbooks documentados (ver documento 04.3).
- CSIRT interno.
- Reporte regulatorio conforme Circular 007/2018 SFC.
- Simulacros al menos anuales.

5.12. Continuidad del negocio

- BCP y DRP (ver carpeta `07_Continuidad_Negocio`).

5.13. Cumplimiento

- Auditoría interna anual del SGSI.
- Pre-auditoría PCI DSS v4.0 y remediación.
- Cumplimiento regulatorio trazable en `admin-audit-service`.

6. Sanciones

El incumplimiento es falta grave. Aplica régimen disciplinario interno, terminación justa de contratos laborales o comerciales y las acciones legales pertinentes.

7. Vigencia y mejora continua

- Vigencia 24 meses.
- Revisión anual por el Comité de Seguridad.
- Revisión extraordinaria ante cambios materiales (nueva regulación, incidente mayor, evolución arquitectural).

8. Aprobación

Juan Carlos Traslaviña Abaunza — Representante Legal Suplente / COO **Gabriel Ureña Chacón** — CEO / CTO / CISO

Firmado en Bogotá D.C., el 16 de abril de 2026.