CONFIDENCIAL

FINTRIXS PAY

Riesgo operacional y prevención del fraude

05.4 — MATRIZ DE RIESGOS Y CONTROLES (RESUMEN EJECUTIVO)

CÓDIGO	ROF-004
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

1. Escala de impacto y probabilidad

Probabilidad (P) e Impacto (I) en escala 1–5; Riesgo Inherente = P × I. - Bajo: 1–6 - Medio: 7–12 - Alto: 13–20 - Extremo: 21–25

2. Matriz consolidada

ID	Categoría	Riesgo	P	I	Inherente	Controles clave	Residual
R-001	Ciberseguridad	Compromiso de CDE (PAN)	3	5	15 Alto	Tokenización, vault PCI, mTLS, RBAC, SIEM, pentest	4 Bajo
R-002	Ciberseguridad	Exfiltración de datos personales	3	5	15 Alto	RLS, cifrado, DLP, auditoría, acceso MFA	4 Bajo
R-003	Ciberseguridad	Ransomware en infraestructura corporativa	2	5	10 Medio	Backups 3-2-1, EDR, hardening, segmentación, capacitación anti-phishing	4 Bajo
R-004	Ciberseguridad	DDoS a APIs públicas	3	3	9 Medio	AWS Shield, CloudFront, rate limiting Kong, autoscaling	3 Bajo
R-005	Operacional	Indisponibilidad de servicio crítico	2	4	8 Medio	HA multi-AZ, autoscaling, monitoreo, BCP/DRP	3 Bajo
R-006	Operacional	Error humano en cambio de producción	3	3	9 Medio	CI/CD con gates, peer review, staging, rollback automatizado	3 Bajo
R-007	Fraude externo	Transacciones con tarjetas robadas	4	3	12 Medio	3DS 2.2, scoring transaccional, reglas de velocidad, colaboración con red	4 Bajo
R-008	Fraude externo	Transaction laundering	2	4	8 Medio	KYB estricto, monitoreo de MCC vs. patrón, límites, alertas comportamentales	3 Bajo
R-009	Fraude interno	Abuso de privilegios	2	4	8 Medio	Segregación de funciones, MFA, mínimo privilegio, auditoría inmutable	2 Bajo
R-010	Tercero	Dependencia crítica de proveedor cloud	3	4	12 Medio	Multi-AZ, multi-región DR, plan de reversibilidad, SLA contractual	5 Bajo

ID	Categoría	Riesgo	P	I	Inherente	Controles clave	Residual
R-011	Tercero	Falla de Credibanco / red adquirente	2	4	8 Medio	Monitoreo de salud, canales de contingencia documentados, comunicación 24/7	4 Bajo
R-012	Legal	Sanción SIC por incidente de datos	2	4	8 Medio	Política PDP v2.1, DPO, procedimientos, capacitación, auditoría	3 Bajo
R-013	Legal	Sanción SFC por incumplimiento Circular 007	2	4	8 Medio	Cumplimiento documentado, CSIRT, reportes regulatorios oportunos	3 Bajo
R-014	LAFT	Uso de la plataforma para lavado de activos	2	5	10 Medio	SARLAFT, listas sancionatorias, monitoreo, ROS a UIAF	3 Bajo
R-015	Operacional	Pérdida de talento clave	3	3	9 Medio	Documentación, redundancia de roles, plan de sucesión, retención	5 Bajo
R-016	Regulatorio	Cambios normativos impactando arquitectura	3	3	9 Medio	Monitoreo regulatorio, arquitectura flexible, hoja de ruta de cumplimiento	5 Bajo
R-017	Ciberseguridad	Supply chain attack (dependencias)	3	4	12 Medio	SCA en CI, SBOM, firmas de imagen, dependabot, revisión de CVEs	4 Bajo
R-018	Operacional	Error de procesamiento que genere doble cargo	2	3	6 Bajo	Outbox + Inbox, idempotencia, reconciliación	2 Bajo

3. Frecuencia de revisión

- **Trimestral** por el Comité de Riesgos.
- **Ad hoc** tras incidentes o cambios materiales.

4. Responsables

- **Dueño del riesgo:** área operativa correspondiente.
- **Dueño del control:** líder técnico o funcional.
- **Revisor independiente:** Comité de Riesgos.