CONFIDENCIAL

FINTRIXS PAY

Riesgo operacional y prevención del fraude

05.1 — METODOLOGÍA DE GESTIÓN DE RIESGOS OPERACIONALES Y CIBERNÉTICOS

CÓDIGO	ROF-001
VERSIÓN	1.0 — 16 de abril de 2026
APROBADO POR	Representante Legal / CTO
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

05.1 — METODOLOGÍA DE GESTIÓN DE RIESGOS OPERACIONALES Y CIBERNÉTICOS · Código: ROF-001 · Versión: 1.0 — 16 de abril de 2026 · FINTRIXS S.A.S.

1. Objetivo

Definir la metodología y el ciclo que Fintrixs S.A.S. aplica para identificar, medir, controlar, monitorear y comunicar los riesgos operacionales, tecnológicos y de ciberseguridad que afectan su modelo de pasarela de pagos.

2. Marcos de referencia

- ISO 31000:2018.
- COSO ERM.
- NIST SP 800-30 (Risk Assessment) y NIST CSF 2.0.
- Circular Externa 007 de 2018 SFC.
- PCI DSS v4.0 Req. 12.3 (TRA — Targeted Risk Analysis).

3. Taxonomía de riesgos

Categoría	Ejemplos
Operacional	Errores de procesos, fallos humanos, interrupciones operativas
Tecnológico	Indisponibilidad de sistemas, fallos de integración, obsolescencia
Ciberseguridad	Malware, DDoS, exfiltración, ransomware, ingeniería social
Fraude interno	Infidelidad de empleados, abuso de privilegios
Fraude externo	Transacciones fraudulentas, phishing, chargebacks abusivos
Legal/regulatorio	Sanciones, cambios normativos, incumplimientos
Terceros	Dependencia de proveedores críticos
LA/FT	Cubierto por el SARLAFT (ver 02.1)

4. Ciclo de gestión del riesgo

4.1. Identificación

Fuentes: talleres de riesgo, revisión de procesos, inteligencia de amenazas, auditorías, incidentes previos, aportes de empleados.

4.2. Evaluación

Escalas 1–5 para **probabilidad** e **impacto**. El **riesgo inherente** = probabilidad × impacto.

Nivel	Probabilidad	Impacto
1	Muy baja	Insignificante
2	Baja	Menor
3	Media	Moderado
4	Alta	Mayor
5	Muy alta	Catastrófico

4.3. Apetito y tolerancia

- **Apetito general:** bajo a moderado.
- **Tolerancia cero** en: compromiso de CDE, violación material de datos personales, incumplimiento regulatorio, fraude interno, LAFT materializado.

4.4. Tratamiento

Opciones: evitar, transferir (seguros / contratos), mitigar (controles), asumir (dentro del apetito).

4.5. Control

Los controles se registran con: tipo (preventivo/detectivo/correctivo), frecuencia, responsable, evidencia, efectividad (alta/media/baja).

4.6. Monitoreo

- KRIs (Key Risk Indicators) con umbrales de alerta.
- Tableros de control actualizados.
- Revisión trimestral por el Comité de Riesgos.

4.7. Comunicación

- Reporte mensual al Representante Legal.
- Reporte trimestral al máximo órgano de administración.
- Reportes regulatorios obligatorios.

5. Integración con otros procesos

- **Secure SDLC:** el riesgo técnico se considera en el diseño.
- **Gestión de incidentes:** alimenta la reevaluación de riesgos.
- **BCP/DRP:** los riesgos altos/muy altos alimentan los escenarios de continuidad.
- **SARLAFT:** gestiona los riesgos LAFT bajo marco específico.
- **Proveedores:** cada alta de proveedor incluye evaluación de riesgo.

6. Nivel de madurez actual

Fintrixs evalúa su madurez contra CMMI-like:

- **Identificación:** Nivel 3 (Definido) — procesos documentados.
- **Evaluación:** Nivel 3.
- **Control:** Nivel 2–3 (parcial) — controles en operación, algunos aún en fortalecimiento.
- **Monitoreo:** Nivel 2 — tableros en construcción.

Objetivo 2026: Nivel 3 en todos los dominios; Nivel 4 en ciberseguridad para 2027.

7. Entregables asociados

- Matriz de riesgos y controles (documento 05.4).
- TRA PCI DSS (`docs/security/procedures/TRA-001-TARGETED_RISK_ANALYSIS.md`).
- Informe anual de riesgos.