CONFIDENCIAL

FINTRIXS PAY

Ciberseguridad y seguridad de la información

04.3 — PROCESO DE GESTIÓN DE VULNERABILIDADES E INCIDENTES DE CIBERSEGURIDAD

CÓDIGO	CIB-003
VERSIÓN	1.0 — 16 de abril de 2026
APROBADO POR	CISO / CTO
VIGENCIA	12 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

04.3 — PROCESO DE GESTIÓN DE VULNERABILIDADES E INCIDENTES DE CIBERSEGURIDAD · Código: CIB-003 · Versión: 1.0 — 16 de abril de 2026 · FINTRIXS S.A.S.

A. GESTIÓN DE VULNERABILIDADES

1. Objetivo

Identificar, priorizar, remediar y validar las vulnerabilidades de los sistemas de Fintrixs Pay de manera continua.

2. Fuentes de identificación

Fuente	Frecuencia	Herramienta / Servicio
Escaneo de infraestructura (IP públicas)	Semanal	ASV (Approved Scanning Vendor) externo — PCI DSS Req. 11.3
Escaneo interno	Mensual	Scanner interno (Nessus / Qualys / OpenVAS)
Análisis de composición de software (SCA)	En cada commit	Snyk / GitHub Dependabot / Trivy
SAST	En CI	SonarQube / Semgrep / CodeQL
DAST	Mensual y pre-releases	OWASP ZAP / Burp Enterprise
Pentest externo	Anual + cambios críticos	Firma independiente certificada
Intelligence feeds	Diario	Boletines CVE, CISA KEV, proveedores

3. Priorización

Severidad (CVSS v3.1)	SLA de remediación
Crítica (9.0–10.0)	72 horas
Alta (7.0–8.9)	15 días calendario
Media (4.0–6.9)	30 días calendario
Baja (0.1–3.9)	90 días calendario o próxima liberación

Criterios adicionales de escalamiento: explotabilidad pública, presencia en CISA KEV, exposición a internet, impacto sobre CDE (PCI).

4. Ciclo

1. Identificación y registro en el tracker interno.
2. Análisis de contexto y priorización.
3. Remediación (parche, configuración, mitigación compensatoria).
4. Validación (re-escaneo y verificación).
5. Cierre y reporte al comité de seguridad.

5. Gestión de parches

- Ventana preferencial: martes/jueves por la noche.
- Cambios de emergencia autorizados por el CISO.
- Prueba previa en staging en 100% de los casos no críticos.
- Validación post-despliegue automatizada.

6. Métricas

- Tiempo promedio de remediación (MTTR) por severidad.
- % de vulnerabilidades cerradas dentro del SLA.
- Densidad de vulnerabilidades por 100 LOC / activo.
- Cobertura de escaneo.

B. GESTIÓN DE INCIDENTES DE CIBERSEGURIDAD

7. Objetivo

Detectar, contener, erradicar, recuperar y aprender de incidentes de ciberseguridad, siguiendo NIST SP 800-61r2 y PCI DSS Req. 12.10.

8. Definición de incidente

Cualquier evento que comprometa (real o potencialmente) la confidencialidad, integridad o disponibilidad de los sistemas o datos.

9. Clasificación

Severidad	Ejemplos
S1 — Crítica	Compromiso del CDE, exposición de PAN, ransomware, exfiltración masiva
S2 — Alta	Accesos no autorizados, malware contenido, DDoS con afectación
S3 — Media	Intentos de intrusión bloqueados, fuga parcial no sensible
S4 — Baja	Eventos sospechosos, falsos positivos, acciones formativas

10. Roles del CSIRT

- Líder (CISO).
- Ingeniero de respuesta (plataforma).
- Forense digital.
- Coordinador de comunicaciones.
- Legal y cumplimiento.
- Enlaces externos (banco sponsor, Credibanco, SFC, SIC).

11. Flujo operativo

1. **Detección** (SIEM, logs, alertas, reportes).
2. **Triage inicial** en ≤ 15 min para S1.
3. **Contención** (cortar, aislar, revocar).
4. **Análisis forense** (snapshots, memoria, logs).
5. **Erradicación** (remover causa raíz).
6. **Recuperación** (restaurar desde backup validado, reinstaurar servicios).
7. **Notificación** (ver matriz abajo).
8. **Post-mortem** en 15 días.

12. Matriz de notificación

Destinatario	Umbral	Plazo
Banco sponsor	Cualquier incidente que afecte el ecosistema	≤ 24 h
Credibanco / Visa	Compromiso de datos de tarjeta	Inmediato por canal de la red
SFC (Circular 007/2018)	Incidentes con impacto regulatorio	Según plazos SFC
SIC	Incidentes con datos personales	≤ 72 h titular / 15 días hábiles RNBD
Titulares	Brechas con riesgo para sus derechos	≤ 72 h
UIAF	Si implica LAFT	Según ROS
FISCALÍA / POLICIA	Si hay conducta delictiva	Según gravedad

13. Simulacros

- Table-top exercise: trimestral.
- Ejercicio técnico (ej. phishing simulado, breach attack simulation): al menos anual.
- Red Team: anual a partir de 2026.

14. Evidencias y registros

- Todos los incidentes quedan documentados con: ID, fecha, categoría, severidad, descripción, activos afectados, acciones, responsables, lecciones aprendidas.
- Conservación mínima 5 años.

15. Herramientas

- SIEM: stack basado en logs estructurados de `@fintrixs/logging`.
- Tracker de incidentes interno.
- Runbooks vivos en repositorio documentado.