CONFIDENCIAL

FINTRIXS PAY

Ciberseguridad y seguridad de la información

04.4 — RESUMEN EJECUTIVO DE PRUEBAS DE SEGURIDAD / ETHICAL HACKING

CÓDIGO	CIB-004
VERSIÓN	1.0 — 16 de abril de 2026
APROBADO POR	CISO / CTO
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

04.4 — RESUMEN EJECUTIVO DE PRUEBAS DE SEGURIDAD / ETHICAL HACKING · Código: CIB-004 · Versión: 1.0 — 16 de abril de 2026 · FINTRIXS S.A.S.

1. Alcance

Pasarela de pagos Fintrixs Pay integrada con Credibanco y con el banco sponsor. Incluye:

- APIs públicas (`payments-api`, `fintrix-api-gateway`, `postgraphile-gateway`).
- APIs internas expuestas al adquirente (`webhooks-service`, `orchestration-service`).
- Frontend (Vue 3) — panel de administración para comercios.
- Servicios de tokenización y vault (`tokenization-service`, `card-vault-service`) en su perímetro lógico.
- Infraestructura Kong 3.5 (API gateway), Kubernetes / EKS, PostgreSQL 16, Kafka 7.5.
- Aplicaciones móviles (si aplica).

2. Tipos de pruebas ejecutadas

Prueba	Periodicidad	Estado
Análisis de vulnerabilidades externo (ASV)	Trimestral	Ejecutado — Q1 2026
Escaneo autenticado interno	Mensual	Vigente
SAST / SCA en CI	Continuo	Vigente
DAST	Mensual + pre-release	Vigente
Pentest Web/API manual	Anual	**En ejecución Q2 2026 — firma externa**
Pentest infraestructura y cloud	Anual	Programado Q2 2026
Revisión de configuración Kubernetes / Kong	Semestral	Ejecutado
Ejercicio de phishing	Trimestral	Vigente
Red Team	Anual	Planificado Q4 2026

3. Metodología

- OWASP Web Security Testing Guide (WSTG) v4.2.

- OWASP ASVS v4 (niveles 2–3 según componente).
- OWASP API Security Top 10 (2023).
- PTES — Penetration Testing Execution Standard.
- NIST SP 800-115.
- MITRE ATT&CK como marco de TTPs.

4. Clasificación de hallazgos (CVSS v3.1)

- **Críticos:** 0 abiertos
- **Altos:** 0 abiertos (2 remediados en el último ciclo)
- **Medios:** 3 abiertos — en remediación dentro del SLA (30 días)
- **Bajos / informativos:** hallazgos de hardening menor, en seguimiento

5. Resumen de remediaciones recientes

ID	Severidad	Descripción breve	Estado
VULN-2026-001	Alta	Cabeceras de seguridad HTTP ausentes en respuesta del gateway	Cerrado
VULN-2026-002	Alta	Token JWT con TTL superior al recomendado	Cerrado
VULN-2026-003	Media	Rate-limit insuficiente en endpoint de recuperación de clave	En remediación — SLA 30 d
VULN-2026-004	Media	Revisión de CORS en endpoints no críticos	En remediación — SLA 30 d
VULN-2026-005	Media	Dependencia `x` con CVE medio	En plan de patch

(El informe técnico detallado se entrega bajo NDA específico y con hash SHA-256 verificable.)

6. Controles continuos

- Integración con CI: fallo del build ante hallazgos críticos o altos.
- `dependency-check` y `trivy` sobre imágenes Docker.
- Escaneo de secretos con `gitleaks`.
- Revisión de código obligatoria (4 ojos) previo al merge.

7. Certificaciones y proveedores

- ASV certificado por PCI SSC.
- Firma independiente contratada para pentest anual — identificación se entrega al banco bajo NDA.

8. Entregables disponibles bajo NDA

- Informe ejecutivo y técnico del último pentest.
- Reportes de escaneo ASV.
- Certificados de cumplimiento ASV.
- Resultados consolidados de SAST/DAST.
- Evidencias de remediación.

9. Compromiso

Fintrixs se compromete a remitir al banco sponsor el resumen ejecutivo del próximo pentest anual dentro de los 30 días posteriores a su ejecución, así como la notificación de cualquier hallazgo crítico o alto que afecte la integración con los servicios del banco.