CONFIDENCIAL

FINTRIXS PAY

Ciberseguridad y seguridad de la información

04.7 — CONTROLES DE CIBERSEGURIDAD EN APLICACIONES WEB Y MÓVILES

CÓDIGO	CIB-007
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

04.7 — CONTROLES DE CIBERSEGURIDAD EN APLICACIONES WEB Y MÓVILES · Código: CIB-007 · Versión: 1.0 — 16 de abril de 2026 · FINTRIXS S.A.S.

1. Aplicación web (Dashboard Fintrixs)

Frontend Vue 3 con `<script setup>` (Composition API), Pinia 2.1, Tailwind 3.4, Vite 5.0, Axios.

1.1. Controles implementados

Control	Implementación
Prevención de inyección (SQLi, XSS)	Vue auto-escapa por defecto; CSP estricta; validación en backend con `class-validator`; uso de ORM parametrizado (TypeORM).
CSRF	Tokens anti-CSRF en cookies `SameSite=Strict` + verificación en endpoints que cambian estado.
DoS/DDoS	AWS CloudFront + Shield + rate limiting en Kong + alertas.
Clickjacking	Headers `X-Frame-Options: DENY` + CSP `frame-ancestors 'none'`.
Fuerza bruta y enumeración	Respuestas uniformes, delays progresivos, captcha adaptativo, MFA.
Legitimidad front-back	JWT firmado + mTLS en capa interna + validación de Origin/Referer.
Sesiones y tokens	JWT RS256 con TTL corto + refresh token rotativo.
Validaciones de entrada	En front y en back (defense in depth).
Control de acceso (RBAC)	Guard `@fintrix/authz` en cada ruta y operación.
Cifrado en tránsito	HTTPS obligatorio (HSTS, TLS 1.2+).
Cifrado de datos sensibles en reposo	AES-256 gestionado por KMS.
Logging y monitoreo	`@fintrix/logging` con correlación + SIEM + alertas.

1.2. Buenas prácticas de OWASP ASVS aplicadas

- Nivel 2 mínimo en todas las pantallas; nivel 3 en pantallas que tocan datos PCI.
- Content Security Policy con nonces.
- Subresource Integrity (SRI) para scripts externos (cuando aplican).
- Cabeceras: `X-Content-Type-Options: nosniff`, `Referrer-Policy`, `Permissions-Policy`.

2. Aplicación móvil (si la integración del banco requiere un cliente móvil propio)

2.1. Controles implementados

Control	Implementación
Prevención de ingeniería inversa	Ofuscación (R8 / ProGuard en Android, SwiftShield en iOS), detección de hooks (Frida/Substrate), detección de debugging.
Detección Jailbreak/Root	Limitación de funcionalidades sensibles; bloqueo de operaciones críticas; reporte telemétrico.
Validación SSL/TLS + pinning	Certificate pinning para endpoints críticos; validación de cadena.
Legitimidad de comunicaciones	Firma de requests + JWT + mTLS cuando aplica.
Sesiones y tokens	TTL corto, logout por inactividad, revocación por pérdida del dispositivo.
Validaciones de entrada	En cliente y servidor.
Control de acceso / RBAC	Endpoints protegidos, mínimo privilegio.
Cifrado en tránsito	TLS 1.3 + pinning.
Cifrado en reposo	Almacenes seguros (Keychain iOS / Keystore Android) para credenciales y tokens.
Logging y monitoreo	Telemetría de seguridad (sin PII).

2.2. Estándares

- OWASP Mobile Application Security Verification Standard (MASVS) v2.
- OWASP MSTG.
- Apple Platform Security / Android Security Best Practices.

3. Pruebas aplicadas

- SAST + dependency scanning sobre el frontend y la app móvil.
- DAST sobre el frontend.
- Pentest anual específico al canal móvil (cuando aplique).
- Pruebas de integración con el gateway Kong y mTLS.

4. Gestión de actualizaciones

- Versionamiento semántico.
- Actualizaciones forzadas ante vulnerabilidades críticas.
- Deprecación controlada de versiones no soportadas.