GRUPO FARINA · MUESTRA DE ENTREGABLE ETAPA 1

Diagnóstico de Preparación en Pagos y Seguridad de APIs

Sistema evaluado de referencia: SecurePay (Java 25 · Spring Boot 4 · PostgreSQL 18) | Corte inicial: 21/10/2026 → Verificación remediada: 26/10/2026 (120 pruebas automatizadas). Nota: Este diagnóstico identifica brechas técnicas y verifica controles; la certificación formal PCI DSS / ISO 27001 la emite un QSA o ente acreditado.

1. Resumen Ejecutivo y Alcance

La Etapa 1 evalúa APIs de pagos y servicios backend en cuatro ejes: (1) Idempotencia y concurrencia en PostgreSQL, (2) Autenticación, titularidad/BOLA y rate limiting (OWASP API Top 10 / PCI DSS Req. 6 y 8), (3) Endurecimiento de contenedores y runtime, y (4) Controles DevSecOps en CI (Gitleaks, SpotBugs/FindSecBugs, Trivy, CycloneDX SBOM).

2. Hallazgos Priorizados y Trazabilidad de Remediación (Etapa 1 → Etapa 2)

ID / Severidad	Hallazgo y Mapeo Normativo	Riesgo Inicial (21/10)	Remediación y Evidencia (26/10)
SP-01 Alta	Doble configuración de autenticación (DemoUsersConfig Basic vs. JWT) OWASP API2 / PCI DSS 8.2	Beans UserDetailsService en conflicto y credenciales demo inline en documentación.	**CERRADO (PR #30–#32):** Unificado en BCrypt + Bearer JWT firmado (HS256); secretos inline eliminados; Gitleaks activo.
SP-02 Alta	Ausencia de rate limiting en /auth/login y /api/payments OWASP API4:2023	Expuesto a fuerza bruta en login y ráfagas de creación de pagos.	**CERRADO (PR #34 y #36):** Filtro token-bucket (429 + Retry-After) por IP y cliente; tests anti-spoofing X-Forwarded-For.
SP-03 Media	Cobertura BOLA / Pertenencia y alteración de payload JWT OWASP API1:2023	Faltaba matriz HTTP completa para lecturas cruzadas y customerId forjado.	**CERRADO (Días 23–25):** Verificada paridad 401/403/404, rechazo de customerId ajeno y pruebas contra inyección SQL.
SP-04 Media	Vulnerabilidades en paquetes de imagen base (musl / brotli) PCI DSS Req. 6.3	Capa runtime Alpine marcada por Trivy por CVE-2026-107891 y CVE-2026-111497.	**CERRADO (PR #35 y #39):** Imagen Temurin 25 JRE fijada por digest, UID 10001, rootfs solo lectura, 0 CVEs Altos/Críticos.
SP-05 Baja	Swagger / OpenAPI con permitAll en SecurityConfig bajo perfil prod OWASP API8:2023	Springdoc estaba deshabilitado en YAML prod, pero SecurityConfig mantenía permitAll.	**CERRADO:** SecurityConfig condiciona Swagger según propiedades springdoc; verificado con ProdSwaggerSecurityTest (401/404).

3. Controles Verificados de Ingeniería y Observabilidad (Días 36–41)

• **Idempotencia y Concurrencia:** Idempotency-Key por cliente + huella SHA-256 del payload verificada bajo carreras concurrentes en PostgreSQL 18.6.
• **Observabilidad y Trazabilidad:** Logs JSON estructurados con X-Correlation-Id validado, métricas Micrometer acotadas (restringidas a ADMIN) y spans OpenTelemetry con propagación W3C Trace Context.
• **Sondas de Resiliencia:** Prueba aislada en Compose confirma que /actuator/health/readiness pasa a 503 ante caída de PostgreSQL mientras /liveness permanece 200 UP, recuperándose automáticamente.
• **Riesgo Residual / Próxima Etapa:** Migración de filtro HS256 manual a Spring OAuth2 Resource Server / IdP OIDC externo, rate limiting distribuido para múltiples réplicas y conciliación de webhooks del proveedor.

Grupo Farina · Rosario, Argentina — nicolasfarina@outlook.com — https://www.nicolasfarina.com/es/