WireVet – Informe de Seguridad SSL/TLS

Calificación: A+ (máxima posible)

Fecha: 13 noviembre 2025

Resumen Ejecutivo

WireVet.cl obtuvo la calificación **A+** en SSL Labs, demostrando un nivel de seguridad excepcional en su implementación de HTTPS/TLS. El servidor presenta una configuración robusta, con TLS 1.3 habilitado, cifrados modernos, mitigación completa de vulnerabilidades y una correcta implementación de HSTS. Esta infraestructura sitúa a WireVet por encima del estándar común en plataformas SaaS nacionales e internacionales, asegurando comunicaciones cifradas, integridad de datos y protección avanzada contra ataques.

Característica	Estado
TLS 1.3	ACTIVO
TLS 1.2	ACTIVO
Protocolos antiguos (1.0/1.1)	DESHABILITADOS
Vulnerabilidades críticas	MITIGADAS
HSTS Preload	CONFIGURADO
Cipher Suites	MODERNAS
Forward Secrecy	ROBUSTA

1. Certificado & Configuración

• Certificado Let’s Encrypt R13, con SANs completos.
• Cadena correcta sin errores.
• RSA 2048 bits, SHA256.
• Recomendación: agregar DNS CAA para control de emisión.

2. Protocolos TLS

• TLS 1.3 habilitado.
• TLS 1.2 habilitado.
• TLS 1.1 / 1.0 / SSLv3 totalmente deshabilitados.

3. Cifrados

• AES-256-GCM, AES-128-GCM, CHACHA20-POLY1305.
• Perfect Forward Secrecy con X25519 / ECDHE.

4. HSTS

• Strict-Transport-Security configurado con max-age=31536000; includeSubDomains; preload.
• Permite nota A+ y protege contra ataques SSL downgrade.

5. Vulnerabilidades

El servidor no presenta vulnerabilidades conocidas:
• Heartbleed, ROBOT, POODLE, DROWN, LOGJAM, SWEET32 mitigadas.

6. Mejoras Recomendadas

• Activar OCSP Stapling para mayor rendimiento.
• Recursos DNS CAA.
• Mantener auditoría periódica de headers de seguridad.