

Escanear Vulnerabilidades

Informe de Seguridad Web

URL https://sst.carabineros.cl
Dominio sst.carabineros.cl
Fecha 8 de mayo de 2026 a las 13:20

Checks 9 pruebas
Hallazgos 15 totales
Problemas 3 detectados

C

73/100

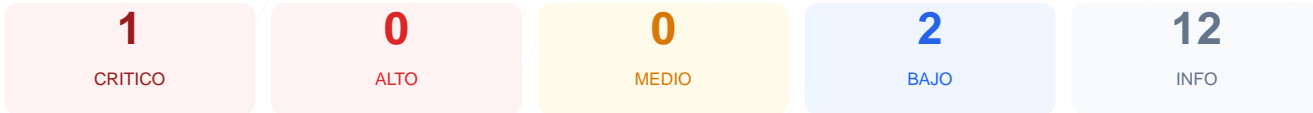
puntos de seguridad



RESUMEN EJECUTIVO

Tras realizar el análisis de seguridad en el dominio sst.carabineros.cl, se ha obtenido una puntuación de 73/100 con una nota final de C. Los resultados de los checks pasivos indican que se ejecutaron 9 pruebas, de las cuales 1 resultó satisfactoria, no hubo advertencias y se registró 1 fallo crítico de configuración. El sistema no permitió validar componentes esenciales como el cifrado y las cabeceras de seguridad debido a errores de conexión. Por tanto, el sitio se considera vulnerable y presenta un riesgo operativo alto debido a la falta de visibilidad sobre sus protocolos de protección básicos.

Resumen de Riesgos



Resumen de Checks

| | | | |
|------------------------|-----|-------|---|
| SSL/TLS | 0 | ERROR | No se pudo verificar SSL/TLS |
| Cabeceras de Seguridad | 0 | ERROR | No se pudieron verificar las cabeceras |
| Redireccion HTTPS | 0 | ERROR | No se pudo verificar la redireccion HTTPS |
| Deteccion CMS | 0 | ERROR | No se pudo analizar el CMS |
| Version CMS Expuesta | 0 | ERROR | No se pudo verificar la version del CMS |
| Seguridad de Cookies | 0 | ERROR | No se pudieron verificar las cookies |
| Contenido Mixto | 0 | ERROR | No se pudo verificar contenido mixto |
| Robots.txt y Sitemap | 20 | FALLO | Faltan robots.txt y sitemap.xml |
| Puertos Abiertos | 100 | OK | No se detectaron puertos abiertos |

SSL/TLS — 0/100

Estado: ERROR

No se pudo verificar SSL/TLS

- CRITICO** Conexion SSL
No se pudo establecer conexion SSL/TLS

Robots.txt y Sitemap — 20/100

Estado: FALLO

Faltan robots.txt y sitemap.xml

- BAJO** robots.txt
Error al acceder
- BAJO** sitemap.xml
Error al acceder

Puertos Abiertos — 100/100

Estado: OK

No se detectaron puertos abiertos

- **INFO Puerto 21 (FTP)**
Cerrado — Transferencia de archivos sin cifrar
- **INFO Puerto 22 (SSH)**
Cerrado — Acceso remoto seguro
- **INFO Puerto 23 (Telnet)**
Cerrado — Acceso remoto sin cifrar
- **INFO Puerto 25 (SMTP)**
Cerrado — Envío de correo
- **INFO Puerto 80 (HTTP)**
Cerrado — Servidor web
- **INFO Puerto 443 (HTTPS)**
Cerrado — Servidor web seguro
- **INFO Puerto 3306 (MySQL)**
Cerrado — Base de datos MySQL expuesta
- **INFO Puerto 3389 (RDP)**
Cerrado — Escritorio remoto Windows
- **INFO Puerto 5432 (PostgreSQL)**
Cerrado — Base de datos PostgreSQL expuesta
- **INFO Puerto 6379 (Redis)**
Cerrado — Cache Redis sin autenticación por defecto
- **INFO Puerto 8080 (HTTP-Alt)**
Cerrado — Servidor web alternativo / proxy
- **INFO Puerto 27017 (MongoDB)**
Cerrado — Base de datos MongoDB expuesta

Analisis de Seguridad

VULNERABILIDADES DETECTADAS

[CRITICAL] Conexión SSL: No se pudo establecer una conexión SSL/TLS válida, lo que impide garantizar la integridad y confidencialidad de la información transmitida.

[LOW] Ausencia de archivos de indexación: El sistema no dispone de robots.txt ni sitemap.xml, lo cual dificulta la gestión del rastreo y puede exponer rutas innecesarias.

[MEDIUM] Indeterminación de cabeceras de seguridad: La imposibilidad de verificar las cabeceras HTTP sugiere una configuración de servidor restrictiva o incorrecta que podría ocultar la falta de protecciones contra ataques XSS o Clickjacking.

[MEDIUM] Seguridad de Cookies no verificada: No se ha podido confirmar el uso de atributos Secure o HttpOnly, lo que representa un riesgo potencial para el secuestro de sesiones de usuario.