EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://frigosrono.cl	Checks	9 pruebas
Dominio	frigosrono.cl	Hallazgos	15 totales
Fecha	24 de marzo de 2026 a las 15:26	Problemas	3 detectados

C

73/100

puntos de seguridad

RESUMEN EJECUTIVO

La auditoría de ciberseguridad realizada al sitio web ha resultado en una puntuación de 73/100, lo que equivale a una nota C. Durante el proceso se ejecutaron 9 checks pasivos, de los cuales 1 resultó satisfactorio y 1 fue clasificado como fallo crítico de conectividad. La imposibilidad de validar el certificado de seguridad y las cabeceras de protección representa un riesgo elevado para la integridad de la plataforma. El análisis técnico revela deficiencias estructurales en la configuración del servidor que exponen la comunicación del usuario. Se concluye que el sitio es vulnerable y requiere intervención inmediata para garantizar un entorno de navegación seguro.

Resumen de Riesgos

1	0	0	2	12
CRITICO	ALTO	MEDIO	BAJO	INFO

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 — Envio 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 autenticacion 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] Conexion SSL: No se pudo establecer una conexión SSL/TLS válida, lo que impide el cifrado de la información y permite la interceptación de datos por terceros.
[ERROR] Cabeceras de Seguridad: Ausencia total de cabeceras HTTP de protección (HSTS, CSP, X-Content-Type-Options), lo que facilita ataques de intermediario y ejecución de scripts maliciosos.
[LOW] Archivos de Rastreo: El servidor deniega el acceso a robots.txt y sitemap.xml, lo que afecta negativamente la indexación y oculta la estructura de directorios permitidos.
[ERROR] Seguridad de Cookies: No se pudo verificar el atributo Secure o HttpOnly, lo que podría permitir el robo de sesiones si existen cookies activas.