

# Escanear Vulnerabilidades

Informe de Seguridad Web

URL https://reymayorista.com.ar/  
Dominio reymayorista.com.ar  
Fecha 19 de abril de 2026 a las 03:17

Checks 9 pruebas  
Hallazgos 15 totales  
Problemas 3 detectados

# C

## 73/100

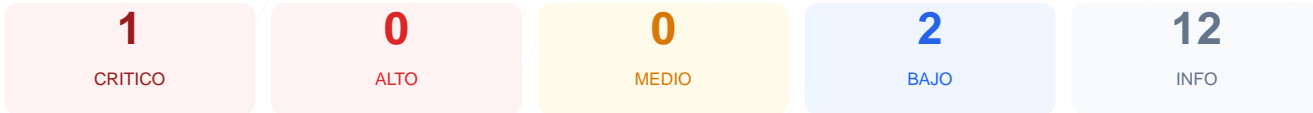
puntos de seguridad



### RESUMEN EJECUTIVO

El análisis de seguridad del sitio web ha arrojado una puntuación de 73/100, obteniendo una calificación de nota C. Durante la evaluación se ejecutaron 9 checks pasivos, resultando en 1 validación correcta, 0 advertencias y 1 fallo crítico identificado. A pesar de la puntuación numérica, la imposibilidad de verificar parámetros esenciales como el cifrado y las cabeceras de protección indica una configuración técnica inestable. Debido a la ausencia de protocolos de seguridad básicos validados, el sitio se considera actualmente vulnerable y no apto para el manejo de datos sensibles.

### 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

- [CRITICO] Error de conexión SSL/TLS: No se pudo establecer una conexión segura, lo que impide el cifrado de la información entre el usuario y el servidor.
- [CRITICO] Cabeceras de Seguridad no verificadas: La ausencia de respuesta en las cabeceras HTTP expone el sitio a ataques de inyección de código y robo de sesiones.
- [CRITICO] Fallo en Redirección HTTPS: No se detectó un forzado automático de tráfico seguro, permitiendo que la navegación ocurra por canales vulnerables.
- [ALTO] Seguridad de Cookies: La falta de validación en los atributos de las cookies facilita ataques de secuestro de sesión.
- [BAJO] Ausencia de archivos de indexación: No se encontraron los archivos robots.txt ni sitemap.xml, lo que dificulta la correcta gestión del rastreo web y puede exponer rutas innecesarias.