

Escanear Vulnerabilidades

Informe de Seguridad Web

URL https://www.garciatech.com.mx/
Dominio www.garciatech.com.mx
Fecha 26 de abril de 2026 a las 03:34

Checks 9 pruebas
Hallazgos 45 totales
Problemas 7 detectados

A

93/100

puntos de seguridad



RESUMEN EJECUTIVO

La auditoría de seguridad realizada al sitio garciatech.com.mx ha dado como resultado una puntuación de 93/100, obteniendo una nota de calificación A. Durante el proceso se ejecutaron 9 checks pasivos, de los cuales 7 resultaron satisfactorios, uno presentó advertencias y uno fue calificado como fallo técnico. El sitio demuestra una implementación sólida de protocolos de cifrado y redirección de tráfico, lo que protege eficazmente la integridad de los datos en tránsito. En conclusión, el sitio se considera seguro, aunque requiere ajustes preventivos en la configuración de cabeceras y en la restricción de archivos informativos expuestos.

Resumen de Riesgos



Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 66 dias
Cabeceras de Seguridad	85	AVISO	5/6 presentes. Faltan: Permissions-Policy
Redireccion HTTPS	100	OK	HTTP redirige a HTTPS y HSTS esta habilitado
Deteccion CMS	100	OK	No se detecto un CMS conocido
Version CMS Expuesta	100	OK	No se detecto version de CMS expuesta
Seguridad de Cookies	100	OK	No se encontraron cookies
Contenido Mixto	100	OK	No se detecto contenido mixto
Robots.txt y Sitemap	20	FALLO	Faltan robots.txt y sitemap.xml
Puertos Abiertos	100	OK	2 puerto(s) abierto(s), todos esperados

SSL/TLS — 100/100

Estado: OK

Certificado valido, expira en 66 dias

- INFO **Certificado valido**
El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
66 dias restantes (expira: 2026-07-01T02:22:55.000Z)
- INFO **Fecha de emision**
Emitido desde: 2026-04-02T02:22:56.000Z
- INFO **Puerto 443**
Conexion HTTPS establecida correctamente en puerto 443

Cabeceras de Seguridad — 85/100

Estado: AVISO

5/6 presentes. Faltan: Permissions-Policy

- BAJO **Server header expuesto**
Server: Vercel — Revela tecnologia del servidor

- INFO **Content-Security-Policy**
Presente: default-src 'self'; script-src 'self' 'unsafe-inline' 'unsafe-eval'; style-src '...
- INFO **X-Frame-Options**
Presente: DENY
- INFO **Strict-Transport-Security**
Presente: max-age=63072000
- INFO **X-Content-Type-Options**
Presente: nosniff
- INFO **Referrer-Policy**
Presente: strict-origin-when-cross-origin
- MEDIO **Permissions-Policy**
Falta — Restringe APIs del navegador (camara, micro, etc.)

Redireccion HTTPS — 100/100

Estado: OK

HTTP redirige a HTTPS y HSTS esta habilitado

- INFO **HTTP !' HTTPS redireccion**
HTTP 308 redirige a https://www.garciatech.com.mx/
- INFO **HSTS (Strict-Transport-Security)**
HSTS activo: max-age=63072000
- BAJO **HSTS includeSubDomains**
HSTS no cubre subdominios
- INFO **HSTS max-age**
max-age=63072000 (730 dias)
- INFO **Respuesta HTTPS**
HTTPS responde con status 200

Deteccion CMS — 100/100

Estado: OK

No se detecto un CMS conocido

- INFO **WordPress**
No detectado
- INFO **Joomla**
No detectado
- INFO **Drupal**
No detectado
- INFO **Magento**
No detectado
- INFO **Shopify**
No detectado
- INFO **PrestaShop**
No detectado
- INFO **Wix**
No detectado
- INFO **Squarespace**
No detectado

Version CMS Expuesta — 100/100

Estado: OK

No se detecto version de CMS expuesta

- MEDIO **Archivo /readme.html**
Archivo accesible publicamente — Puede revelar version e informacion del CMS
- MEDIO **Archivo /README.txt**
Archivo accesible publicamente — Puede revelar version e informacion del CMS
- MEDIO **Ruta /wp-login.php**
Panel de login accesible publicamente

- MEDIO** Ruta /administrator/
Panel de login accesible publicamente
- MEDIO** Ruta /user/login
Panel de login accesible publicamente
- INFO** Version CMS
No se detecta ninguna version expuesta

Seguridad de Cookies — 100/100

Estado: OK

No se encontraron cookies

- INFO** Cookies detectadas
El sitio no establece cookies en la respuesta inicial

Contenido Mixto — 100/100

Estado: OK

No se detecto contenido mixto

- INFO** Contenido mixto
Todos los recursos se cargan por HTTPS

Robots.txt y Sitemap — 20/100

Estado: FALLO

Faltan robots.txt y sitemap.xml

- INFO** security.txt
Presente en /.well-known/security.txt — Buena practica

Puertos Abiertos — 100/100

Estado: OK

2 puerto(s) abierto(s), todos esperados

- 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)
Abierto (esperado) — Servidor web
- INFO** Puerto 443 (HTTPS)
Abierto (esperado) — 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

[LOW] Server header expuesto: El servidor revela el uso de Vercel, proporcionando información técnica que podría ser aprovechada por atacantes para dirigir exploits específicos.

[MEDIUM] Permissions-Policy faltante: La ausencia de esta cabecera impide restringir el acceso del navegador a funciones sensibles como la cámara, el micrófono o la geolocalización.

[MEDIUM] Archivos informativos accesibles: Los archivos /readme.html y /README.txt están disponibles públicamente, lo que puede exponer metadatos del sistema o detalles de la arquitectura.

[MEDIUM] Rutas administrativas expuestas: Se detectaron accesos públicos a paneles en /wp-login.php, /administrator/ y /user/login, aumentando el riesgo de ataques de fuerza bruta.

[FAIL] Ausencia de archivos de indexación: No se localizaron los archivos robots.txt ni sitemap.xml, lo que compromete la gestión del rastreo y la visibilidad controlada del contenido.