# EscanearVulnerabilidades

Informe de Seguridad Web

| | | | |
|---|---|---|---|
| URL | https://tienda.fade-ti.com.mx/ | Checks | 9 pruebas |
| Dominio | tienda.fade-ti.com.mx | Hallazgos | 48 totales |
| Fecha | 29 de mayo de 2026 a las 00:05 | Problemas | 14 detectados |

C

65/100

puntos de seguridad

**RESUMEN EJECUTIVO**

El análisis de seguridad del sitio web arroja una puntuación de 65/100, lo que equivale a una nota C. Se ejecutaron 9 checks pasivos, resultando en 7 aprobados y 2 fallos críticos relacionados con la configuración del servidor y la protección de datos. La infraestructura actual permite conexiones no cifradas y carece de todas las cabeceras de seguridad fundamentales para proteger a los usuarios. Aunque el certificado SSL es válido, la ausencia de una política de transporte estricto eleva el riesgo de interceptación de datos. En su estado actual, el sitio se considera vulnerable a ataques de intermediario y de inyección de contenido.

## Resumen de Riesgos

| 0 | 5 | 7 | 2 | 34 |
|---|---|---|---|---|
| CRITICO | ALTO | MEDIO | BAJO | INFO |

## Resumen de Checks

| | | | |
|---|---|---|---|
| SSL/TLS | 100 | OK | Certificado valido, expira en 52 dias |
| Cabeceras de Seguridad | 0 | FALLO | Solo 0/6 presentes. Faltan: Content-Security-Pol... |
| Redireccion HTTPS | 0 | FALLO | No hay redireccion HTTP a HTTPS |
| 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 | 100 | OK | robots.txt y sitemap.xml presentes |
| Puertos Abiertos | 100 | OK | No se detectaron puertos abiertos |

## SSL/TLS — 100/100

Estado: OK

Certificado valido, expira en 52 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
  52 dias restantes (expira: 2026-07-19T21:59:40.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2026-04-20T21:59:41.000Z
- INFO **Puerto 443**
  Conexion HTTPS establecida correctamente en puerto 443

## Cabeceras de Seguridad — 0/100

Estado: FALLO

Solo 0/6 presentes. Faltan: Content-Security-Policy, X-Frame-Options, Strict-Transport-Security, X-Content-Type-Options, Referrer-Policy, Permissions-Policy

- BAJO **Server header expuesto**
  Server: nginx/1.27.4 — Revela tecnologia del servidor

- ALTO **Content-Security-Policy**
  Falta — Previene XSS y ataques de inyeccion de contenido
- ALTO **X-Frame-Options**
  Falta — Protege contra clickjacking
- ALTO **Strict-Transport-Security**
  Falta — Fuerza conexiones HTTPS (HSTS)
- MEDIO **X-Content-Type-Options**
  Falta — Evita MIME-type sniffing
- MEDIO **Referrer-Policy**
  Falta — Controla la informacion de referer enviada
- MEDIO **Permissions-Policy**
  Falta — Restringe APIs del navegador (camara, micro, etc.)

## Redireccion HTTPS — 0/100

Estado: FALLO

No hay redireccion HTTP a HTTPS

- ALTO **HTTP !' HTTPS redireccion**
  HTTP 200 — No redirige a HTTPS
- ALTO **HSTS (Strict-Transport-Security)**
  HSTS no configurado — El navegador no fuerza HTTPS
- 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
- INFO **Tecnologias detectadas**
  React

## Version CMS Expuesta — 100/100

Estado: OK

No se detecto version de CMS expuesta

- INFO **Archivo /readme.html**
  No accesible (correcto)
- 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 — 100/100

Estado: OK

robots.txt y sitemap.xml presentes

- INFO **robots.txt**
  Presente (161 bytes)
- INFO **Reglas robots.txt**
  4 Disallow, 1 Allow
- BAJO **Ruta sensible en robots.txt**
  Referencia a "admin" — Puede revelar rutas sensibles a atacantes
- INFO **Sitemap en robots.txt**
  https://tienda.fade-ti.com.mx/sitemap.xml
- INFO **security.txt**
  Presente en /.well-known/security.txt — Buena practica

## 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**

[HIGH] Falta de redirección HTTP a HTTPS: El servidor responde con éxito en el puerto 80 sin forzar el cifrado, exponiendo cualquier intercambio de datos.
[HIGH] Ausencia de Strict-Transport-Security (HSTS): No se instruye al navegador para usar exclusivamente conexiones seguras, facilitando ataques de degradación.
[HIGH] Ausencia de Content-Security-Policy (CSP): El sitio no restringe el origen de scripts o recursos, permitiendo posibles ataques de Cross-Site Scripting (XSS).
[HIGH] Ausencia de X-Frame-Options: La falta de esta directiva permite que la web sea cargada en marcos externos, habilitando ataques de clickjacking.
[MEDIUM] Ausencia de X-Content-Type-Options: No se previene el MIME-type sniffing, lo que podría permitir la ejecución de archivos maliciosos disfrazados de texto.
[MEDIUM] Ausencia de Referrer-Policy: La configuración actual no controla la información de procedencia enviada en los enlaces, pudiendo filtrar rutas internas.
[MEDIUM] Ausencia de Permissions-Policy: No existen restricciones sobre el uso de APIs del navegador como la cámara, el micrófono o la ubicación.
[MEDIUM] Archivo README.txt expuesto: El acceso público a este archivo puede revelar detalles técnicos sobre el software o la estructura interna del sitio.
[MEDIUM] Paneles de login expuestos: Las rutas /wp-login.php, /administrator/ y /user/login son accesibles, lo que facilita intentos de acceso no autorizado.
[LOW] Cabecera Server expuesta: Se revela el uso de nginx/1.27.4, lo que ayuda a posibles atacantes a buscar vulnerabilidades específicas de esa versión.
[LOW] Ruta sensible en robots.txt: Se hace referencia directa a directorios de administración, guiando a atacantes hacia puntos críticos del sistema.