

Escanear Vulnerabilidades

Informe de Seguridad Web

URL https://petco.com.mx
Dominio petco.com.mx
Fecha 14 de abril de 2026 a las 05:28

Checks 9 pruebas
Hallazgos 47 totales
Problemas 9 detectados

C

70/100

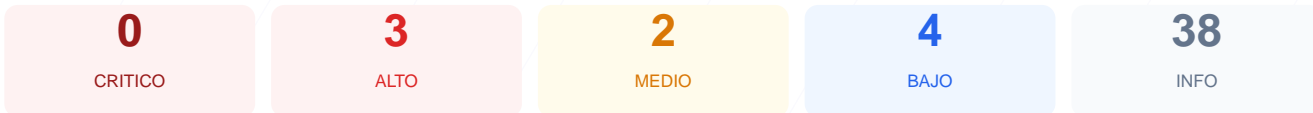
puntos de seguridad



RESUMEN EJECUTIVO

El análisis de seguridad del sitio web ha resultado en una puntuación de 70/100, lo que equivale a una calificación de grado C. Se realizaron 9 verificaciones pasivas que arrojaron 4 resultados satisfactorios, 3 advertencias por configuraciones mejorables y 2 fallos críticos en la infraestructura de transporte. Aunque el cifrado de datos es funcional, la carencia de políticas estrictas de transporte y errores en la redirección de tráfico suponen un riesgo. Por lo tanto, el sitio se clasifica como vulnerable ante ataques de intermediario y de reconocimiento de infraestructura.

Resumen de Riesgos



Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 39 dias
Cabeceras de Seguridad	80	AVISO	5/6 presentes. Faltan: Strict-Transport-Security
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	67	AVISO	__cf_bm: falta SameSite
Contenido Mixto	100	OK	No se detecto contenido mixto
Robots.txt y Sitemap	20	FALLO	Faltan robots.txt y sitemap.xml
Puertos Abiertos	60	AVISO	1 puerto(s) potencialmente riesgoso(s): 8080 (HT...

SSL/TLS — 100/100

Estado: OK

Certificado valido, expira en 39 dias

- INFO **Certificado valido**
El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
39 dias restantes (expira: 2026-05-23T16:00:19.000Z)
- INFO **Fecha de emision**
Emitido desde: 2026-02-22T15:00:22.000Z
- INFO **Puerto 443**
Conexion HTTPS establecida correctamente en puerto 443

Cabeceras de Seguridad — 80/100

Estado: AVISO

5/6 presentes. Faltan: Strict-Transport-Security

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

- **BAJO** **X-Powered-By expuesto**
X-Powered-By: Petco Mexico — Revela framework/lenguaje
- **INFO** **Content-Security-Policy**
Presente: frame-ancestors 'self' https://petco.com.mx https://www.petco.com.mx *.petco.com...
- **INFO** **X-Frame-Options**
Presente: SAMEORIGIN
- **ALTO** **Strict-Transport-Security**
Falta — Fuerza conexiones HTTPS (HSTS)
- **INFO** **X-Content-Type-Options**
Presente: nosniff
- **INFO** **Referrer-Policy**
Presente: strict-origin-when-cross-origin
- **INFO** **Permissions-Policy**
Presente: geolocation=(self), camera=(), microphone=(), accelerometer=(), autoplay=(), ...

Redireccion HTTPS — 0/100

Estado: **FALLO**

No hay redireccion HTTP a HTTPS

- **ALTO** **HTTP !' HTTPS redireccion**
HTTP 499 — No dirige a HTTPS
- **ALTO** **HSTS (Strict-Transport-Security)**
HSTS no configurado — El navegador no fuerza HTTPS
- **INFO** **Respuesta HTTPS**
HTTPS responde con status 499

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**
Petco Mexico

Version CMS Expuesta — 100/100

Estado: **OK**

No se detecto version de CMS expuesta

- **INFO** **Archivo /readme.html**
No accesible (correcto)
- **INFO** **Archivo /README.txt**
No accesible (correcto)
- **INFO** **Version CMS**
No se detecta ninguna version expuesta

Seguridad de Cookies — 67/100

Estado: AVISO

__cf_bm: falta SameSite

- INFO **Cookies detectadas**
1 cookie(s) encontrada(s)
- INFO **Cookie: __cf_bm — HttpOnly**
HttpOnly activo — No accesible via JavaScript
- INFO **Cookie: __cf_bm — Secure**
Flag Secure activo — Solo se envía por HTTPS
- MEDIO **Cookie: __cf_bm — SameSite**
Falta SameSite — Vulnerable a CSRF

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

- BAJO **robots.txt**
No encontrado (HTTP 499)
- BAJO **sitemap.xml**
No encontrado (HTTP 499)
- BAJO **security.txt**
No encontrado — Recomendado para politica de divulgacion

Puertos Abiertos — 60/100

Estado: AVISO

1 puerto(s) potencialmente riesgoso(s): 8080 (HTTP-Alt)

- 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)**
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
- MEDIO **Puerto 8080 (HTTP-Alt)**
ABIERTO — Servidor web alternativo / proxy
- INFO **Puerto 27017 (MongoDB)**
Cerrado — Base de datos MongoDB expuesta

Analisis de Seguridad

VULNERABILIDADES DETECTADAS

[HIGH] Strict-Transport-Security: La ausencia de la cabecera HSTS impide que el sitio obligue a los navegadores a usar conexiones cifradas exclusivamente.

[HIGH] Redirección HTTP a HTTPS: El servidor no redirige el tráfico inseguro al protocolo seguro, devolviendo un error de estado 499 y dejando la comunicación expuesta.

[MEDIUM] Puerto 8080 (HTTP-Alt): Se detectó un puerto de servidor web alternativo abierto, lo cual aumenta la superficie de ataque y posibles accesos no autorizados.

[MEDIUM] Cookie __cf_bm sin atributo SameSite: La falta de esta directiva en las cookies de Cloudflare facilita la ejecución de ataques de falsificación de petición en sitios cruzados (CSRF).

[LOW] Cabecera Server expuesta: El servidor revela el uso de Cloudflare, proporcionando información técnica valiosa para un atacante durante la fase de reconocimiento.

[LOW] Cabecera X-Powered-By expuesta: Se muestra información sobre el framework de Petco Mexico, permitiendo identificar la tecnología interna del sitio.

[LOW] Robots.txt no encontrado: La ausencia de este archivo genera errores de respuesta en el servidor y dificulta el control de la indexación.

[LOW] Sitemap.xml no encontrado: No se localizó el mapa del sitio, lo que resulta en una gestión deficiente de la estructura pública del dominio.