

EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://panama.com.mx/	Checks	9 pruebas
Dominio	panama.com.mx	Hallazgos	43 totales
Fecha	24 de septiembre de 2026 a las 04:15	Problemas	7 detectados

B

75/100

puntos de seguridad

RESUMEN EJECUTIVO

La auditoría de seguridad realizada al sitio web ha arrojado una puntuación de 75/100, lo que equivale a una nota de B. Durante el análisis se ejecutaron 9 checks pasivos, de los cuales 5 resultaron satisfactorios, 3 generaron advertencias y 1 fue clasificado como fallo. A pesar de contar con un cifrado de transporte válido, se detectaron deficiencias críticas en la configuración de las directivas de seguridad y la gestión de puertos del servidor. En su estado actual, el sitio se considera vulnerable debido a la falta de mecanismos automáticos para forzar conexiones seguras y la exposición de información técnica.

Resumen de Riesgos

0	3	2	2	36
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 83 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	100	OK	No se encontraron cookies
Contenido Mixto	100	OK	No se detecto contenido mixto
Robots.txt y Sitemap	60	AVISO	Falta sitemap.xml
Puertos Abiertos	60	AVISO	1 puerto(s) potencialmente riesgoso(s): 8080 (HT...

SSL/TLS — 100/100

Estado: OK

Certificado valido, expira en 83 dias

- INFO Certificado valido
El certificado SSL es valido y de confianza
- INFO Dias hasta expiracion
83 dias restantes (expira: 2026-12-16T03:37:30.000Z)
- INFO Fecha de emision
Emitido desde: 2026-09-17T02:37:43.000Z
- 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

- INFO

Content-Security-Policy
Presente: default-src 'none'; script-src 'nonce-Sn5JNhTxwRxpjyCHBbEHTw' 'unsafe-eval' http...
- INFO

X-Frame-Options
Presente: SAMEORIGIN
- ALTO

Strict-Transport-Security
Falta — Fuerza conexiones HTTPS (HSTS)
- INFO

X-Content-Type-Options
Presente: nosniiff
- INFO

Referrer-Policy
Presente: same-origin
- INFO

Permissions-Policy
Presente: accelerometer=(),camera=(),clipboard-read=(),clipboard-write=(),geolocation=(),g...

Redireccion HTTPS — 0/100

Estado: FALLO

No hay redireccion HTTP a HTTPS

- ALTO

HTTP !' HTTPS redireccion
HTTP 403 — No redirige a HTTPS
- ALTO

HSTS (Strict-Transport-Security)
HSTS no configurado — El navegador no fuerza HTTPS
- INFO

Respuesta HTTPS
HTTPS responde con status 403

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

- INFO

Archivo /readme.html
No accesible (correcto)
- MEDIO

Archivo /README.txt
Archivo accesible publicamente — Puede revelar version e informacion del CMS
- 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 — 60/100

Estado: AVISO
Falta sitemap.xml

- INFO **robots.txt**
Presente (22 bytes)
- INFO **Reglas robots.txt**
0 Disallow, 1 Allow
- BAJO **sitemap.xml**
No encontrado (HTTP 403)
- BAJO **security.txt**
No encontrado — Recomendado para política 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 — 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
- MEDIO **Puerto 8080 (HTTP-Alt)**
ABIERTO — Servidor web alternativo / proxy
- INFO **Puerto 27017 (MongoDB)**
Cerrado — Base de datos MongoDB expuesta

Análisis de Seguridad

VULNERABILIDADES DETECTADAS

[ALTA] Redirección HTTPS ausente: El servidor no redirige el tráfico HTTP hacia HTTPS, devolviendo un código de error 403 en lugar de asegurar la conexión del usuario.
[ALTA] HSTS (Strict-Transport-Security) no configurado: La falta de esta cabecera impide que los navegadores fuercen conexiones cifradas, permitiendo ataques de degradación de protocolo.
[MEDIA] Archivo /README.txt accesible: La exposición pública de este archivo puede revelar información interna sobre la infraestructura o versiones de componentes técnicos.
[MEDIA] Puerto 8080 (HTTP-Alt) abierto: La presencia de este puerto activo aumenta la superficie de ataque al ofrecer un vector de entrada alternativo no estándar.

[BAJA] Cabecera Server expuesta: El servidor revela el uso de tecnología Cloudflare, facilitando a posibles atacantes el reconocimiento de la arquitectura de red.

[BAJA] Falta de sitemap.xml: La ausencia de este archivo dificulta el control sobre la indexación y la auditoría de rutas legítimas de la plataforma.