

Escanear Vulnerabilidades

Informe de Seguridad Web

URL https://sistemaset.tamaulipas.gob.mx
Dominio sistemaset.tamaulipas.gob.mx
Fecha 8 de mayo de 2026 a las 22:19

Checks 9 pruebas
Hallazgos 42 totales
Problemas 10 detectados

C

72/100

puntos de seguridad



RESUMEN EJECUTIVO

El análisis de seguridad realizado al sitio sistemaset.tamaulipas.gob.mx arroja una puntuación de 72/100, lo que representa una calificación final de C. Durante la evaluación se ejecutaron 9 checks pasivos, de los cuales 6 resultaron exitosos, uno presentó advertencias y dos fueron calificados como fallos críticos. Los resultados demuestran que, aunque la infraestructura básica es estable, existe una ausencia total de cabeceras de seguridad modernas que protejan al usuario. Por lo tanto, se concluye que el sitio es vulnerable ante ataques de intermediarios e inyecciones de código debido a una configuración de servidor incompleta.

Resumen de Riesgos



Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 146 dias
Cabeceras de Seguridad	0	FALLO	Solo 0/6 presentes. Faltan: Content-Security-Pol...
Redireccion HTTPS	70	AVISO	HTTP redirige a HTTPS pero falta HSTS
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 146 dias

- INFO **Certificado valido**
El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
146 dias restantes (expira: 2026-10-01T23:59:59.000Z)
- INFO **Fecha de emision**
Emitido desde: 2026-03-24T00:00:00.000Z
- 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/1.18.0 (Ubuntu) — 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 — 70/100

Estado: AVISO

HTTP redirige a HTTPS pero falta HSTS

- **INFO** **HTTP !' HTTPS redireccion**
HTTP 301 redirige a https://sistemaset.tamaulipas.gob.mx/
- **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

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 — 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

- BAJO **robots.txt**
No encontrado (HTTP 404)
- BAJO **sitemap.xml**
No encontrado (HTTP 404)
- BAJO **security.txt**
No encontrado — Recomendado para politica de divulgacion

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 autentificacion 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] Content-Security-Policy: La ausencia de esta cabecera facilita la ejecución de ataques de Cross-Site Scripting (XSS) y la inyección de contenido malicioso.

[HIGH] X-Frame-Options: Al no estar configurada, el sitio es susceptible a ataques de clickjacking, permitiendo que un tercero cargue la web en un marco invisible para engañar al usuario.

[HIGH] Strict-Transport-Security: La falta de HSTS impide que el navegador fuerce conexiones HTTPS de manera obligatoria, permitiendo posibles ataques de degradación de protocolo.

[MEDIUM] X-Content-Type-Options: La falta de esta directiva permite el MIME-type sniffing, lo que podría derivar en la ejecución de scripts disfrazados de otros tipos de archivos.

[MEDIUM] Referrer-Policy: No existe un control sobre la información de navegación que se envía a sitios externos cuando un usuario hace clic en un enlace.

[MEDIUM] Permissions-Policy: El servidor no restringe el acceso de las APIs del navegador a funciones sensibles como la cámara o el micrófono, aumentando la superficie de ataque.

[LOW] Server header expuesto: El encabezado revela el uso de nginx/1.18.0 (Ubuntu), proporcionando información técnica valiosa que un atacante puede usar para buscar exploits específicos.

[LOW] robots.txt: No se encontró el archivo en el servidor, lo que dificulta el control de los rastreadores sobre qué directorios deben ser públicos o privados.

[LOW] sitemap.xml: La ausencia de este archivo afecta la correcta indexación y visibilidad de la estructura del sitio web por parte de los motores de búsqueda.