

# Escanear Vulnerabilidades

Informe de Seguridad Web

URL https://seproban.maserp.mx/  
Dominio seproban.maserp.mx  
Fecha 29 de abril de 2026 a las 23:14

Checks 9 pruebas  
Hallazgos 46 totales  
Problemas 4 detectados

# A

## 94/100

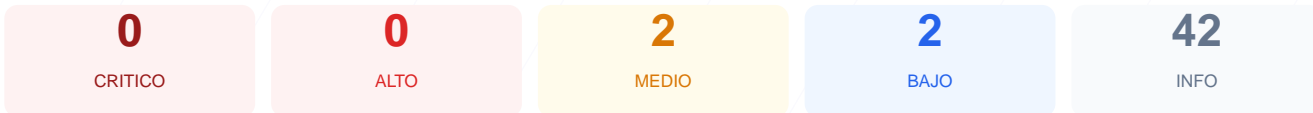
puntos de seguridad



### RESUMEN EJECUTIVO

La auditoría de ciberseguridad realizada al sitio web ha arrojado una puntuación de 94/100, lo que equivale a una calificación de grado A. Se ejecutaron 9 controles pasivos de seguridad, de los cuales 7 resultaron satisfactorios y 2 generaron advertencias técnicas que no comprometen la integridad inmediata del sistema. No se detectaron fallos críticos ni vulnerabilidades de alta prioridad durante esta fase de análisis. En conclusión, el sitio se presenta como una plataforma altamente segura y bien configurada bajo los estándares actuales. Se recomienda atender las observaciones menores para consolidar un entorno totalmente robusto.

### Resumen de Riesgos



### Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 66 dias
Cabeceras de Seguridad	100	OK	Todas las cabeceras de seguridad presentes
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	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 66 dias

- INFO **Certificado valido**  
El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**  
66 dias restantes (expira: 2026-07-05T05:24:07.000Z)
- INFO **Fecha de emision**  
Emitido desde: 2026-04-06T04:24:21.000Z
- INFO **Puerto 443**  
Conexion HTTPS establecida correctamente en puerto 443

### Cabeceras de Seguridad — 100/100

Estado: OK

Todas las cabeceras de seguridad presentes

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

- INFO **Content-Security-Policy**  
Presente: Content-Security-Policy: default-src 'self'; base-uri 'self'; object-src '...
- INFO **X-Frame-Options**  
Presente: SAMEORIGIN
- INFO **Strict-Transport-Security**  
Presente: max-age=15552000; includeSubDomains; preload
- INFO **X-Content-Type-Options**  
Presente: nosniff
- INFO **Referrer-Policy**  
Presente: strict-origin-when-cross-origin
- INFO **Permissions-Policy**  
Presente: accelerometer=(),browsing-topics=(),camera=(),clipboard-read=(),clipboard-write=...

## Redireccion HTTPS — 100/100

---

Estado: OK

HTTP redirige a HTTPS y HSTS esta habilitado

- INFO **HTTP !' HTTPS redireccion**  
HTTP 301 redirige a https://seproban.maserp.mx/
- INFO **HSTS (Strict-Transport-Security)**  
HSTS activo: max-age=15552000; includeSubDomains; preload
- **BAJO** **HSTS includeSubDomains**  
HSTS cubre subdominios
- INFO **HSTS max-age**  
max-age=15552000 (180 dias)
- 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)
- 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 — 60/100

---

Estado: AVISO

Falta sitemap.xml

- INFO **robots.txt**  
Presente (1738 bytes)
- INFO **Reglas robots.txt**  
9 Disallow, 1 Allow
- MEDIO **Bloqueo total**  
robots.txt bloquea todo el sitio con Disallow: /
- BAJO **sitemap.xml**  
No encontrado (HTTP 403)
- 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 — 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

## Analisis de Seguridad

---

## VULNERABILIDADES DETECTADAS

[MEDIUM] Puerto 8080 (HTTP-Alt) abierto: Se detectó un puerto de servicio alternativo activo que podría ser utilizado para acceder a interfaces de gestión o proxies no protegidos.

[MEDIUM] Configuración restrictiva en robots.txt: El archivo bloquea el rastreo de todo el sitio mediante la directiva Disallow, lo cual puede ocultar rutas sensibles pero también indica una configuración de visibilidad inusual.

[LOW] Server header expuesto: La cabecera de respuesta revela el uso de la tecnología Cloudflare, lo cual facilita a un atacante potencial el reconocimiento de la infraestructura de red.

[LOW] Ausencia de sitemap.xml: No se encontró el mapa del sitio o el acceso fue denegado, lo que dificulta la auditoría de rutas legítimas y la indexación controlada.