EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://www.codejalisco.gob.mx/pista/registro	Checks	9 pruebas
Dominio	www.codejalisco.gob.mx	Hallazgos	46 totales
Fecha	6 de mayo de 2026 a las 17:30	Problemas	13 detectados

D

53/100

puntos de seguridad

RESUMEN EJECUTIVO

Tras realizar una auditoría de seguridad en el sitio web, se ha obtenido una puntuación de 53/100 con una nota de grado D. Los resultados de los nueve checks pasivos ejecutados revelan deficiencias estructurales importantes, habiendo superado satisfactoriamente cuatro de ellos, con una advertencia y cuatro fallos críticos. A pesar de contar con un certificado SSL válido, la carencia de cabeceras de seguridad y la falta de redirección forzada a protocolos seguros comprometen la integridad de la navegación. Se detectó una gestión de cookies deficiente y la exposición de información técnica sensible sobre el servidor. Por lo tanto, se concluye que el sitio es vulnerable y requiere medidas correctivas inmediatas para proteger la información de los usuarios.

Resumen de Riesgos

0	5	5	3	33
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 73 dias
Cabeceras de Seguridad	15	FALLO	Solo 1/6 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	33	FALLO	__RequestVerificationToken: falta Secure; __Requ...
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 73 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
  73 dias restantes (expira: 2026-07-18T10:08:46.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2026-04-19T09:08:49.000Z
- INFO **Puerto 443**
  Conexion HTTPS establecida correctamente en puerto 443

Cabeceras de Seguridad — 15/100

Estado: FALLO

Solo 1/6 presentes. Faltan: Content-Security-Policy, Strict-Transport-Security, X-Content-Type-Options, Referrer-Policy, Permissions-Policy

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

- BAJO **X-Powered-By expuesto**
  X-Powered-By: ASP.NET — Revela framework/lenguaje
- ALTO **Content-Security-Policy**
  Falta — Previene XSS y ataques de inyeccion de contenido
- INFO **X-Frame-Options**
  Presente: SAMEORIGIN
- 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**
  ASP.NET

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 — 33/100

Estado: FALLO

__RequestVerificationToken: falta Secure; __RequestVerificationToken: falta SameSite

- INFO **Cookies detectadas**
  1 cookie(s) encontrada(s)
- INFO **Cookie: __RequestVerificationToken — HttpOnly**
  HttpOnly activo — No accesible via JavaScript
- ALTO **Cookie: __RequestVerificationToken — Secure**
  Falta flag Secure — Cookie se envia en conexiones HTTP
- MEDIO **Cookie: __RequestVerificationToken — 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 **sitemap.xml**
  No encontrado (HTTP 404)
- 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

[HIGH] Falta de redirección HTTP a HTTPS: El servidor no fuerza la conexión cifrada, permitiendo que la comunicación sea interceptada mediante ataques de hombre en el medio.
[HIGH] Ausencia de Strict-Transport-Security (HSTS): El navegador no recibe instrucciones para conectarse exclusivamente por HTTPS, dejando la sesión expuesta a degradaciones de seguridad.
[HIGH] Falta de Content-Security-Policy (CSP): El sitio no posee una política de seguridad de contenido, lo que facilita ataques de Cross-Site Scripting (XSS) e inyecciones de código.
[HIGH] Cookie __RequestVerificationToken sin atributo Secure: Esta cookie de seguridad puede ser enviada a través de conexiones no cifradas, permitiendo su robo en redes inseguras.
[MEDIUM] Cookie __RequestVerificationToken sin atributo SameSite: La ausencia de este atributo hace que el sitio sea susceptible a ataques de falsificación de solicitudes en sitios cruzados (CSRF).
[MEDIUM] Puerto 8080 abierto: La exposición del puerto HTTP-Alt representa una superficie de ataque adicional que podría albergar servicios no supervisados o vulnerables.
[MEDIUM] Falta de X-Content-Type-Options: La ausencia de esta cabecera permite el sniffing de tipos MIME, lo que podría llevar a la ejecución involuntaria de scripts maliciosos.
[MEDIUM] Falta de Referrer-Policy: No se controla la información de referencia que el sitio envía a otros dominios, lo que puede filtrar URLs privadas.
[MEDIUM] Falta de Permissions-Policy: No se restringen las APIs del navegador, permitiendo potencialmente el acceso no deseado a funciones como la cámara o el micrófono.
[LOW] Cabecera de servidor expuesta: Se revela el uso de Cloudflare como infraestructura de red, lo cual ayuda a un atacante en la fase de reconocimiento.
[LOW] Cabecera X-Powered-By expuesta: El sitio revela que utiliza el framework ASP.NET, permitiendo que potenciales atacantes busquen vulnerabilidades específicas de esa tecnología.
[LOW] Ausencia de robots.txt y sitemap.xml: El servidor devuelve un error 404 para estos archivos, lo que dificulta la gestión de indexación y el control de rastreo.