

EscanearVulnerabilidades

Informe de Seguridad Web

URL https://idicom.mx/home-two
Dominio idicom.mx
Fecha 1 de octubre de 2026 a las 17:33

Checks 9 pruebas
Hallazgos 46 totales
Problemas 13 detectados

B

76/100

puntos de seguridad

RESUMEN EJECUTIVO

El análisis de seguridad realizado sobre el sitio idicom.mx arroja una puntuación de 76/100 con una calificación de grado B. De los 9 checks pasivos ejecutados, 7 resultaron satisfactorios, uno presentó advertencias y uno falló debido a configuraciones ausentes. Aunque la comunicación está cifrada correctamente, la falta total de cabeceras de seguridad y la exposición de rutas administrativas representan un riesgo latente. En su estado actual, el sitio se considera moderadamente vulnerable debido a la carencia de políticas de endurecimiento en el servidor.

Resumen de Riesgos



Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 105 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	100	OK	robots.txt y sitemap.xml presentes
Puertos Abiertos	100	OK	2 puerto(s) abierto(s), todos esperados

SSL/TLS — 100/100

Estado: OK

Certificado valido, expira en 105 dias

- INFO Certificado valido
El certificado SSL es valido y de confianza
- INFO Dias hasta expiracion
105 dias restantes (expira: 2027-01-14T23:59:59.000Z)
- INFO Fecha de emision
Emitido desde: 2026-07-01T00:00:00.000Z
- 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: AmazonS3 — 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://idicom.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

- MEDIO

Archivo /readme.html
Archivo accesible publicamente — Puede revelar version e informacion del CMS
- MEDIO

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

Ruta /wp-login.php
Panel de login accesible publicamente
- MEDIO

Ruta /administrator/
Panel de login accesible publicamente
- MEDIO

Ruta /user/login
Panel de login accesible publicamente

●	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 — 100/100

Estado: OK

robots.txt y sitemap.xml presentes

●	INFO	robots.txt
Presente (393 bytes)		
●	INFO	Reglas robots.txt
14 Disallow, 1 Allow		
●	INFO	Sitemap en robots.txt
https://idicom.mx/sitemap.xml		
●	INFO	security.txt
Presente en /.well-known/security.txt — Buena practica		

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 autenticacion 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 permite ataques de Cross-Site Scripting (XSS) e inyección de contenido no autorizado.

[HIGH] X-Frame-Options: La falta de configuración hace que el sitio sea susceptible a ataques de Clickjacking.

[HIGH] Strict-Transport-Security: No se implementa HSTS, lo que permite ataques de degradación de protocolo de HTTPS a HTTP.

[MEDIUM] X-Content-Type-Options: Al no estar presente, el navegador puede realizar MIME-type sniffing, ejecutando potencialmente archivos maliciosos.

[MEDIUM] Rutas administrativas expuestas: Las rutas /wp-login.php, /administrator/ y /user/login son accesibles, facilitando ataques de fuerza bruta.

[MEDIUM] Archivos de información accesibles: Los archivos /readme.html y /README.txt están expuestos y pueden revelar detalles técnicos de la plataforma.

[MEDIUM] Referrer-Policy: La falta de esta política puede causar la fuga de información sensible en los encabezados de referencia hacia sitios externos.

[MEDIUM] Permissions-Policy: No se restringen las APIs del navegador, permitiendo potencialmente el uso no autorizado de hardware como cámara o micrófono.

[LOW] Server header expuesto: El servidor revela el uso de AmazonS3, proporcionando información útil para el perfilamiento por parte de atacantes.