

Escanear Vulnerabilidades

Informe de Seguridad Web

URL https://teologiasana.com/
Dominio teologiasana.com
Fecha 1 de mayo de 2026 a las 17:20

Checks 9 pruebas
Hallazgos 46 totales
Problemas 12 detectados

C

64/100

puntos de seguridad



RESUMEN EJECUTIVO

La auditoría de seguridad realizada a teologiasana.com ha resultado en una puntuación de 64/100, lo que otorga al sitio una calificación de C. Durante el proceso se ejecutaron 9 checks pasivos, obteniendo 5 resultados satisfactorios, 2 advertencias y 2 fallos críticos. Aunque la comunicación cifrada es correcta, se han detectado debilidades importantes en la configuración del servidor y la exposición de metadatos del sistema. Debido a la ausencia total de cabeceras de seguridad y la visibilidad de la versión del CMS, el sitio se considera vulnerable a diversos vectores de ataque comunes.

Resumen de Riesgos



Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 49 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	CMS detectado: WordPress
Version CMS Expuesta	20	FALLO	WordPress 1776980270 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	60	AVISO	1 puerto(s) potencialmente riesgoso(s): 8080 (HT...

SSL/TLS — 100/100

Estado: OK

Certificado valido, expira en 49 dias

- INFO **Certificado valido**
El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
49 dias restantes (expira: 2026-06-19T06:19:46.000Z)
- INFO **Fecha de emision**
Emitido desde: 2026-03-21T05:21:01.000Z
- 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: cloudflare — 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://teologiasana.com/>
- **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

CMS detectado: WordPress

- **INFO** **WordPress**
Detectado via HTML body
- **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
- **BAJO** **Meta generator**
Expone: Site Kit by Google 1.177.0
- **INFO** **Tecnologias detectadas**
Next.js

Version CMS Expuesta — 20/100

Estado: FALLO

WordPress 1776980270 expuesta

- **ALTO** **WordPress version**
Version 1776980270 expuesta publicamente — Permite a atacantes buscar CVEs conocidos
- **INFO** **Archivo /readme.html**
No accesible (correcto)
- **INFO** **Archivo /README.txt**
No accesible (correcto)

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 (1912 bytes)
- INFO **Reglas robots.txt**
10 Disallow, 1 Allow
- MEDIO **Bloqueo total**
robots.txt bloquea todo el sitio con Disallow: /
- INFO **Sitemap en robots.txt**
https://teologiasana.com/sitemap_index.xml
- 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] WordPress version: La versión 1776980270 se encuentra expuesta públicamente, permitiendo a potenciales atacantes identificar vulnerabilidades específicas para esta versión.

[HIGH] Content-Security-Policy: Cabecera ausente, lo que facilita la ejecución de ataques XSS y la inyección de contenido malicioso.

[HIGH] X-Frame-Options: No implementada, dejando el sitio desprotegido contra ataques de secuestro de clics o clickjacking.

[HIGH] Strict-Transport-Security: HSTS no configurado, lo que impide obligar al navegador a mantener conexiones seguras en todo momento.

[MEDIUM] Puerto 8080 (HTTP-Alt): Se detectó un puerto alternativo abierto que puede ser utilizado para acceder a servicios internos o proxies no protegidos.

[MEDIUM] robots.txt: El archivo bloquea la indexación de todo el sitio mediante la directiva Disallow: /, lo cual es una configuración inusual para un sitio público.

[MEDIUM] X-Content-Type-Options: Cabecera faltante que permite el sniffing de tipos MIME, aumentando el riesgo de ejecución de scripts disfrazados de otros archivos.

[MEDIUM] Referrer-Policy: No configurada, lo que provoca que no se controle la información de referencia enviada a otros dominios.

[MEDIUM] Permissions-Policy: Ausencia de restricciones sobre el uso de APIs del navegador como cámara, micrófono o geolocalización.

[LOW] Server header: La cabecera expone el uso de Cloudflare, proporcionando información sobre la infraestructura de red.

[LOW] Meta generator: Se expone la presencia de Site Kit by Google en su versión 1.177.0, revelando detalles técnicos innecesarios.