EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://glpi.copecemoac.tech	Checks	9 pruebas
Dominio	glpi.copecemoac.tech	Hallazgos	42 totales
Fecha	30 de abril de 2026 a las 17:30	Problemas	9 detectados

C

73/100

puntos de seguridad

RESUMEN EJECUTIVO

El análisis de seguridad técnica realizado al dominio glpi.copecemoac.tech arroja una puntuación de 73/100, lo que corresponde a una nota C. Durante la evaluación se ejecutaron un total de 9 checks pasivos, de los cuales 5 resultaron satisfactorios, 2 generaron advertencias y 2 finalizaron con fallos críticos. Aunque la implementación del cifrado de transporte es sólida, la ausencia de cabeceras de seguridad fundamentales representa un riesgo significativo. En su estado actual, el sitio se considera vulnerable a ataques de inyección y de intermediario debido a configuraciones incompletas en el servidor web.

Resumen de Riesgos

0	3	3	3	33
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 54 dias
Cabeceras de Seguridad	25	FALLO	Solo 2/6 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	60	AVISO	1 puerto(s) potencialmente riesgoso(s): 8080 (HT...

SSL/TLS — 100/100

Estado: OK

Certificado valido, expira en 54 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
  54 dias restantes (expira: 2026-06-23T08:20:05.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2026-03-25T07:21:27.000Z
- INFO **Puerto 443**
  Conexion HTTPS establecida correctamente en puerto 443

Cabeceras de Seguridad — 25/100

Estado: FALLO

Solo 2/6 presentes. Faltan: Content-Security-Policy, Strict-Transport-Security, X-Content-Type-Options, 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
- 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
- INFO **Referrer-Policy**
  Presente: same-origin
- 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://glpi.copecemoac.tech/
- ALTO **HSTS (Strict-Transport-Security)**
  HSTS no configurado — El navegador no fuerza HTTPS
- 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 — 20/100

Estado: FALLO

Faltan robots.txt y sitemap.xml

- BAJO **robots.txt**
  No encontrado (HTTP 403)
- 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

[HIGH] Content-Security-Policy: La ausencia de esta cabecera facilita la ejecución de ataques de Cross-Site Scripting (XSS) e inyección de contenido malicioso.
[HIGH] Strict-Transport-Security: Al no contar con HSTS, el navegador no fuerza conexiones cifradas, permitiendo posibles degradaciones de seguridad en la comunicación.
[MEDIUM] Puerto 8080 (HTTP-Alt) ABIERTO: La exposición de un puerto alternativo aumenta la superficie de ataque y puede revelar servicios internos no protegidos.
[MEDIUM] X-Content-Type-Options: La falta de esta directiva permite que los navegadores realicen sniffing de tipos MIME, lo que puede derivar en la ejecución de archivos no autorizados.
[MEDIUM] Permissions-Policy: No se restringe el acceso a APIs sensibles del navegador como la cámara o el micrófono, incrementando el riesgo de privacidad para el usuario.

[LOW] Server header expuesto: La cabecera revela el uso de Cloudflare, proporcionando información técnica que asiste a un atacante en el reconocimiento del entorno.
[LOW] robots.txt y sitemap.xml ausentes: El servidor devuelve un error 403 para estos archivos, impidiendo una indexación controlada y una auditoría de recursos públicos.