

Escanear Vulnerabilidades

Informe de Seguridad Web

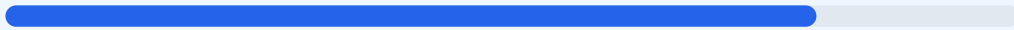
URL https://www.asociacionmarroqui.com/certificado-de-vulnerabilidad/Solituus/?fbclid=PAZXh0bgNhZWQCMTEAc3J0YwZhcHBfaWQMmJjU2Mjg0MDQwNTU4AAAGN3GEMtdm-V-47uG2rrf0xCSoSfAa2t4uu7NJq9K4paviYV2_dDo9RBA03hc_aem_k6CTEVuRfKTKJdsDSm3D9g
Dominio www.asociacionmarroqui.com
Fecha 28 de abril de 2026 a las 22:45

9 pruebas
45 totales
7 detectados
Problemas

B

80/100

puntos de seguridad



RESUMEN EJECUTIVO

El análisis de ciberseguridad realizado arroja una puntuación de 80/100, lo que otorga al sitio una nota B. Se ejecutaron 9 comprobaciones pasivas que resultaron en 4 verificaciones correctas, 4 advertencias técnicas y 1 fallo en la configuración de archivos de control. Aunque el cifrado de datos es sólido, se han detectado carencias en las políticas de transporte seguro y visibilidad de puertos. En conclusión, el sitio se considera mayoritariamente seguro, pero presenta vulnerabilidades moderadas que podrían ser explotadas para interceptar comunicaciones o realizar ataques de falsificación.

Resumen de Riesgos



Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 89 dias
Cabeceras de Seguridad	80	AVISO	5/6 presentes. Faltan: Strict-Transport-Security
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	67	AVISO	__cf_bm: falta SameSite
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 89 dias

- INFO **Certificado valido**
El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
89 dias restantes (expira: 2026-07-26T23:46:12.000Z)
- INFO **Fecha de emision**
Emitido desde: 2026-04-27T22:46:26.000Z
- INFO **Puerto 443**
Conexion HTTPS establecida correctamente en puerto 443

Cabeceras de Seguridad — 80/100

Estado: AVISO

5/6 presentes. Faltan: Strict-Transport-Security

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

- INFO **Content-Security-Policy**
Presente: default-src 'none'; script-src 'nonce-unarV7C1BsTFvJhCM810hu' 'unsafe-eval' http...
- INFO **X-Frame-Options**
Presente: SAMEORIGIN
- ALTO **Strict-Transport-Security**
Falta — Fuerza conexiones HTTPS (HSTS)
- INFO **X-Content-Type-Options**
Presente: nosniiff
- INFO **Referrer-Policy**
Presente: same-origin
- INFO **Permissions-Policy**
Presente: accelerometer=(),browsing-topics=(),camera=(),clipboard-read=(),clipboard-write=...

Redireccion HTTPS — 70/100

Estado: AVISO

HTTP redirige a HTTPS pero falta HSTS

- INFO **HTTP !' HTTPS redireccion**
HTTP 301 redirige a https://www.asociacionmarroqui.com/
- 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 — 67/100

Estado: AVISO

__cf_bm: falta SameSite

- INFO **Cookies detectadas**
1 cookie(s) encontrada(s)
- INFO **Cookie: __cf_bm — HttpOnly**
HttpOnly activo — No accesible via JavaScript
- INFO **Cookie: __cf_bm — Secure**
Flag Secure activo — Solo se envia por HTTPS
- MEDIO **Cookie: __cf_bm — 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 **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] Strict-Transport-Security: Falta la cabecera HSTS, lo que permite que un atacante intente degradar la conexión de HTTPS a HTTP.

[MEDIUM] Cookie __cf_bm: Carece del atributo SameSite, lo que vuelve al sitio vulnerable a ataques de falsificación de peticiones en sitios cruzados (CSRF).

[MEDIUM] Puerto 8080 (HTTP-Alt): Se detectó un puerto alternativo abierto que podría exponer servicios administrativos o proxies no protegidos.

[LOW] Server header expuesto: La cabecera revela el uso de Cloudflare, facilitando a posibles atacantes el reconocimiento de la infraestructura tecnológica.

[LOW] Ausencia de robots.txt y sitemap.xml: El servidor responde con un error 403 al intentar acceder a estos archivos, dificultando la gestión de indexación y rastreo.