

Escanear Vulnerabilidades

Informe de Seguridad Web

URL https://sub-legadoavicola.pages.dev/
Dominio sub-legadoavicola.pages.dev
Fecha 24 de mayo de 2026 a las 22:05

Checks 9 pruebas
Hallazgos 46 totales
Problemas 11 detectados

B

80/100

puntos de seguridad

RESUMEN EJECUTIVO

El análisis de seguridad del sitio web ha resultado en una puntuación de 80/100 con una calificación de grado B. Se ejecutaron un total de 9 controles pasivos, de los cuales 6 resultaron satisfactorios, 2 generaron advertencias y 1 fue calificado como fallo crítico. Aunque la infraestructura base es sólida, la ausencia de cabeceras de seguridad esenciales representa un riesgo para la integridad de los datos. Se concluye que el sitio es generalmente seguro pero vulnerable a ataques de inyección y degradación de protocolo.

Resumen de Riesgos



Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 69 dias
Cabeceras de Seguridad	40	FALLO	Solo 3/6 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	60	AVISO	1 puerto(s) potencialmente riesgoso(s): 8080 (HT...

SSL/TLS — 100/100

Estado: OK

Certificado valido, expira en 69 dias

- INFO Certificado valido**
El certificado SSL es valido y de confianza
- INFO Dias hasta expiracion**
69 dias restantes (expira: 2026-08-02T02:28:08.000Z)
- INFO Fecha de emision**
Emitido desde: 2026-05-04T02:28:09.000Z
- INFO Puerto 443**
Conexion HTTPS establecida correctamente en puerto 443

Cabeceras de Seguridad — 40/100

Estado: FALLO

Solo 3/6 presentes. Faltan: Content-Security-Policy, Strict-Transport-Security, Permissions-Policy

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

- **ALTO** **Content-Security-Policy**
Falta — Previene XSS y ataques de inyección de contenido
- **INFO** **X-Frame-Options**
Presente: DENY
- **ALTO** **Strict-Transport-Security**
Falta — Fuerza conexiones HTTPS (HSTS)
- **INFO** **X-Content-Type-Options**
Presente: nosniif
- **INFO** **Referrer-Policy**
Presente: strict-origin-when-cross-origin
- **MEDIO** **Permissions-Policy**
Falta — Restringe APIs del navegador (camara, micro, etc.)

Redirección HTTPS — 70/100

Estado: AVISO

HTTP redirige a HTTPS pero falta HSTS

- **INFO** **HTTP !' HTTPS redirección**
HTTP 301 redirige a <https://sub-legadoavicola.pages.dev/>
- **ALTO** **HSTS (Strict-Transport-Security)**
HSTS no configurado — El navegador no fuerza HTTPS
- **INFO** **Respuesta HTTPS**
HTTPS responde con status 200

Detección CMS — 100/100

Estado: OK

No se detectó 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 detectó versión de CMS expuesta

- **MEDIO** **Archivo /readme.html**
Archivo accesible públicamente — Puede revelar versión e información del CMS
- **MEDIO** **Archivo /README.txt**
Archivo accesible públicamente — Puede revelar versión e información del CMS
- **MEDIO** **Ruta /wp-login.php**
Panel de login accesible públicamente
- **MEDIO** **Ruta /administrator/**
Panel de login accesible públicamente
- **MEDIO** **Ruta /user/login**
Panel de login accesible públicamente

- 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 (80 bytes)
- INFO **Reglas robots.txt**
0 Disallow, 1 Allow
- INFO **Sitemap en robots.txt**
<https://sub-legadoavicola.pages.dev/sitemap.xml>
- INFO **security.txt**
Presente en /.well-known/security.txt — Buena practica

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 permite la ejecución de scripts no autorizados, aumentando el riesgo de ataques XSS.

[HIGH] Strict-Transport-Security: No se detectó configuración HSTS, lo que permite que un atacante intente degradar la conexión del usuario a HTTP inseguro.

[MEDIUM] Permissions-Policy: Falta restringir el acceso a APIs del navegador, permitiendo potencialmente el uso no deseado de hardware como cámara o micrófono.

[MEDIUM] Puerto 8080 (HTTP-Alt): Este puerto se encuentra abierto y expuesto, lo que suele ser un vector para servicios de administración desprotegidos.

[MEDIUM] Rutas de administración expuestas: Se detectó acceso público a paneles en /wp-login.php, /administrator/ y /user/login, facilitando intentos de fuerza bruta.

[MEDIUM] Archivos informativos accesibles: Los archivos /readme.html y /README.txt están expuestos y pueden revelar detalles técnicos sobre el entorno.

[LOW] Server header expuesto: El servidor revela el uso de Cloudflare, lo cual entrega información técnica que ayuda a un atacante en la fase de reconocimiento.