

EscanearVulnerabilidades

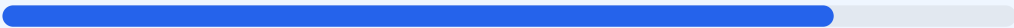
Informe de Seguridad Web

URL	https://ticketscostadelsol.com/	Checks	9 pruebas
Dominio	ticketscostadelsol.com	Hallazgos	37 totales
Fecha	3 de octubre de 2026 a las 11:52	Problemas	5 detectados

B

82/100

puntos de seguridad



RESUMEN EJECUTIVO

El análisis de ciberseguridad del sitio web arroja una puntuación de 82/100, lo que otorga una calificación de nota B. Se ejecutaron un total de 9 checks pasivos, de los cuales 3 resultaron satisfactorios, se generaron 2 advertencias y se identificó 1 fallo de seguridad. La infraestructura presenta una base sólida en el manejo de cabeceras, pero se han detectado debilidades críticas en la gestión de servicios de transferencia de archivos. En su estado actual, el sitio se considera vulnerable debido a la exposición de puertos inseguros y la falta de políticas estrictas de transporte cifrado.

Resumen de Riesgos

0 CRITICO	2 ALTO	0 MEDIO	3 BAJO	32 INFO
--------------	-----------	------------	-----------	------------

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 70 dias
Cabeceras de Seguridad	100	OK	Todas las cabeceras de seguridad presentes
Redireccion HTTPS	70	AVISO	HTTP redirige a HTTPS pero falta HSTS
Deteccion CMS	100	OK	No se detecto un CMS conocido
Robots.txt y Sitemap	20	FALLO	Faltan robots.txt y sitemap.xml
Puertos Abiertos	60	AVISO	1 puerto(s) potencialmente riesgoso(s): 21 (FTP)

SSL/TLS — 100/100

Estado: OK

Certificado valido, expira en 70 dias

- INFO **Certificado valido**
El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
70 dias restantes (expira: 2026-12-12T16:46:53.000Z)
- INFO **Fecha de emision**
Emitido desde: 2026-09-13T16:46:54.000Z
- INFO **Puerto 443**
Conexion HTTPS establecida correctamente en puerto 443

Cabeceras de Seguridad — 100/100

Estado: OK

Todas las cabeceras de seguridad presentes

- BAJO **Server header expuesto**
Server: nginx — Revela tecnologia del servidor
- INFO **Content-Security-Policy**
Presente: default-src 'self'; img-src 'self' data: https;; media-src 'self' https;; frame-...
- INFO **X-Frame-Options**
Presente: SAMEORIGIN

- INFO

Strict-Transport-Security
Presente: max-age=31536000; includeSubDomains
- INFO

X-Content-Type-Options
Presente: nosniff
- INFO

Referrer-Policy
Presente: strict-origin-when-cross-origin
- INFO

Permissions-Policy
Presente: camera=(), microphone=(), geolocation=(self)

Redireccion HTTPS — 70/100

Estado: AVISO

HTTP redirige a HTTPS pero falta HSTS

- INFO

HTTP !' HTTPS redireccion
HTTP 301 redirige a https://ticketscostadelsol.com/
- ALTO

HSTS (Strict-Transport-Security)
HSTS no configurado — El navegador no fuerza HTTPS
- INFO

Respuesta HTTPS
HTTPS responde con status 503

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

Robots.txt y Sitemap — 20/100

Estado: FALLO

Faltan robots.txt y sitemap.xml

- BAJO

robots.txt
No encontrado (HTTP 503)
- BAJO

sitemap.xml
No encontrado (HTTP 503)
- BAJO

security.txt
No encontrado — Recomendado para politica de divulgacion

Puertos Abiertos — 60/100

Estado: AVISO

1 puerto(s) potencialmente riesgoso(s): 21 (FTP)

- ALTO

Puerto 21 (FTP)
ABIERTO — 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 — Envío 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] Puerto 21 (FTP) ABIERTO: El servicio FTP transmite datos y credenciales en texto plano, facilitando el robo de información sensible.

[HIGH] HSTS (Strict-Transport-Security) no configurado: La ausencia de esta cabecera permite ataques de degradación de protocolo de HTTPS a HTTP.

[LOW] Server header expuesto: El servidor revela el uso de nginx, lo que ayuda a posibles atacantes a identificar vulnerabilidades específicas de esa tecnología.

[LOW] Ausencia de robots.txt y sitemap.xml: No se encontraron estos archivos esenciales, lo que puede afectar la indexación y refleja una falta de mantenimiento estructural.

[INFO] Respuesta HTTPS 503: El servidor devolvió un error de servicio no disponible, lo que podría indicar problemas de estabilidad o bloqueos durante el escaneo.