

# EscanearVulnerabilidades

Informe de Seguridad Web

URL https://tribulob.tidelta.com  
Dominio tribulob.tidelta.com  
Fecha 7 de octubre de 2026 a las 15:33

Checks 9 pruebas  
Hallazgos 43 totales  
Problemas 13 detectados

C

72/100

puntos de seguridad



## RESUMEN EJECUTIVO

La auditoria de seguridad realizada sobre el sitio web tribulob.tidelta.com arroja una puntuacion exacta de 72/100, lo que equivale a una nota de C. Durante el analisis se ejecutaron 9 checks pasivos, obteniendo como resultado 6 conformes, 1 advertencia y 2 fallos criticos en la configuracion del servidor. Aunque la base de cifrado es correcta, la ausencia total de cabeceras de proteccion expone la plataforma a diversos vectores de ataque comunes. En su estado actual, el sitio se considera vulnerable debido a una configuracion defensiva incompleta que debe ser subsanada.

## Resumen de Riesgos



## Resumen de Checks

|                        |     |       |                                                     |
|------------------------|-----|-------|-----------------------------------------------------|
| SSL/TLS                | 100 | OK    | Certificado valido, expira en 53 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    | 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       | 100 | OK    | 2 puerto(s) abierto(s), todos esperados             |

## SSL/TLS — 100/100

Estado: OK

Certificado valido, expira en 53 dias

- INFO Certificado valido  
El certificado SSL es valido y de confianza
- INFO Dias hasta expiracion  
53 dias restantes (expira: 2026-11-29T19:56:08.000Z)
- INFO Fecha de emision  
Emitido desde: 2026-08-31T19:56:09.000Z
- 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: nginx/1.18.0 — 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://tribulob.tidelta.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

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

- MEDIO

**Archivo /readme.html**  
Archivo accesible publicamente — Puede revelar version e informacion del CMS
- MEDIO

**Archivo /README.txt**  
Archivo accesible publicamente — Puede revelar version e informacion del CMS
- MEDIO

**Ruta /wp-login.php**  
Panel de login accesible publicamente
- MEDIO

**Ruta /administrator/**  
Panel de login accesible publicamente
- MEDIO

**Ruta /user/login**  
Panel de login accesible publicamente

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

security.txt

No encontrado — Recomendado para politica de divulgacion

## Puertos Abiertos — 100/100

Estado: OK  
2 puerto(s) abierto(s), todos esperados

- 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
- 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] Content-Security-Policy: Falta esta cabecera esencial que previene ataques de inyeccion de codigo y XSS.  
[HIGH] X-Frame-Options: La ausencia de esta directiva permite que el sitio sea embebido en marcos externos, facilitando ataques de clickjacking.  
[HIGH] Strict-Transport-Security: No se ha configurado HSTS, lo que impide que el navegador fuerce conexiones seguras y deja la sesion expuesta a ataques de degradacion.  
[MEDIUM] X-Content-Type-Options: La falta de esta cabecera permite el MIME-type sniffing, aumentando el riesgo de ejecucion de archivos maliciosos disfrazados.  
[MEDIUM] Referrer-Policy: No se controla la informacion de referencia enviada a otros sitios, lo que podria comprometer la privacidad de los usuarios.

[MEDIUM] Permissions-Policy: El sitio no restringe el acceso a APIs del navegador como camara o microfono, aumentando la superficie de ataque.  
[MEDIUM] Archivo /readme.html y /README.txt: Estos archivos son accesibles publicamente y pueden revelar detalles tecnicos de la infraestructura.  
[MEDIUM] Paneles de login expuestos: Las rutas /wp-login.php, /administrator/ y /user/login son accesibles, lo cual atrae ataques de fuerza bruta.  
[LOW] Server header expuesto: El servidor revela el uso de nginx/1.18.0, facilitando a un atacante la busqueda de exploits especificos para esa version.  
[LOW] Robots.txt y Sitemap: La ausencia de estos archivos dificulta la correcta gestion de la indexacion y el control de acceso para rastreadores.