

# Escanear Vulnerabilidades

Informe de Seguridad Web

URL https://hub.pagatokens.com  
Dominio hub.pagatokens.com  
Fecha 30 de junio de 2026 a las 20:14

Checks 9 pruebas  
Hallazgos 43 totales  
Problemas 12 detectados

# B

## 75/100

puntos de seguridad

### RESUMEN EJECUTIVO

El análisis de ciberseguridad realizado al sitio hub.pagatokens.com ha determinado una puntuación de 75/100, lo que equivale a una nota B. Durante la evaluación se ejecutaron 9 checks pasivos, de los cuales 6 resultaron satisfactorios, 1 presentó advertencias y 2 finalizaron con fallos críticos por falta de configuraciones esenciales. Aunque el cifrado de datos es robusto, la ausencia de políticas de seguridad en las cabeceras del servidor expone a los usuarios a riesgos de interceptación y manipulación. En conclusión, el sitio se considera vulnerable a ataques de inyección de contenido y suplantación debido a una configuración de servidor incompleta.

### Resumen de Riesgos



### Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 68 dias
Cabeceras de Seguridad	15	FALLO	Solo 1/6 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 68 dias

- INFO **Certificado valido**  
El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**  
68 dias restantes (expira: 2026-09-06T15:49:59.000Z)
- INFO **Fecha de emision**  
Emitido desde: 2026-06-08T15:50:00.000Z
- INFO **Puerto 443**  
Conexion HTTPS establecida correctamente en puerto 443

### Cabeceras de Seguridad — 15/100

Estado: FALLO

Solo 1/6 presentes. Faltan: Content-Security-Policy, X-Frame-Options, Strict-Transport-Security, Referrer-Policy, Permissions-Policy

- BAJO **Server header expuesto**  
Server: railway-hikari — 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)
- **INFO** **X-Content-Type-Options**  
Presente: nosniiff
- **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://hub.pagatokens.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

● INFO **security.txt**  
Presente en /.well-known/security.txt — Buena practica

## 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, lo que facilita ataques de Cross-Site Scripting (XSS) e inyección de código malicioso.  
[HIGH] X-Frame-Options: La ausencia de esta protección permite ataques de clickjacking, donde un atacante puede engañar al usuario para que realice acciones no deseadas.  
[HIGH] Strict-Transport-Security: HSTS no está configurado, por lo que el sitio no obliga al navegador a usar siempre conexiones seguras, permitiendo ataques de degradación de SSL.  
[MEDIUM] Rutas de administración expuestas: Se detectó acceso público a /wp-login.php, /administrator/ y /user/login, facilitando intentos de acceso no autorizado.

[MEDIUM] Archivos informativos accesibles: Los archivos /readme.html y /README.txt están disponibles públicamente y pueden revelar detalles técnicos del sistema.

[MEDIUM] Referrer-Policy: No hay una política definida, lo que puede provocar la fuga de información sensible en las URL hacia sitios externos.

[MEDIUM] Permissions-Policy: La falta de esta cabecera impide restringir el uso de funciones del navegador como la cámara, el micrófono o la geolocalización.

[LOW] Cabecera Server expuesta: Se detectó el valor "railway-hikari", lo que revela información sobre la infraestructura tecnológica utilizada.

[LOW] Ausencia de robots.txt y sitemap.xml: El sitio carece de archivos de control para buscadores, afectando la visibilidad y el rastreo controlado de la web.