

# Escanear Vulnerabilidades

Informe de Seguridad Web

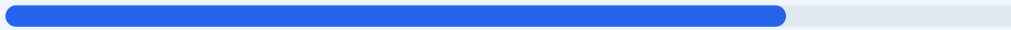
URL https://chronos-juxdeveloper.pages.dev/  
Dominio chronos-juxdeveloper.pages.dev  
Fecha 9 de junio de 2026 a las 16:04

Checks 9 pruebas  
Hallazgos 46 totales  
Problemas 12 detectados

# B

## 77/100

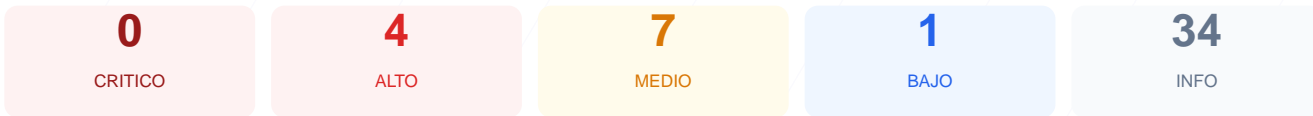
puntos de seguridad



### RESUMEN EJECUTIVO

El análisis de seguridad del sitio web ha arrojado una puntuación de 77/100, lo que equivale a una nota de B. Durante la auditoría se ejecutaron un total de 9 checks pasivos, de los cuales 6 resultaron satisfactorios, 2 generaron advertencias y 1 fue calificado como fallo crítico. No se realizó un pentest activo, por lo que los resultados se limitan a la superficie de exposición externa y configuraciones de red visibles. En su estado actual, el sitio presenta una base de seguridad aceptable pero es vulnerable a ataques de inyección y suplantación debido a la ausencia de cabeceras de seguridad fundamentales. Se concluye que el sitio es parcialmente seguro, requiriendo ajustes inmediatos en la configuración del servidor para mitigar riesgos de nivel alto.

### Resumen de Riesgos



### Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 88 dias
Cabeceras de Seguridad	25	FALLO	Solo 2/6 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 88 dias

- INFO **Certificado valido**  
El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**  
88 dias restantes (expira: 2026-09-05T07:19:33.000Z)
- INFO **Fecha de emision**  
Emitido desde: 2026-06-07T06:21:52.000Z
- INFO **Puerto 443**  
Conexion HTTPS establecida correctamente en puerto 443

### Cabeceras de Seguridad — 25/100

Estado: FALLO

Solo 2/6 presentes. Faltan: Content-Security-Policy, X-Frame-Options, 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 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: nosniif
- **INFO** **Referrer-Policy**  
Presente: strict-origin-when-cross-origin
- **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://chronos-juxdeveloper.pages.dev/>
- **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 — 100/100

---

Estado: OK

robots.txt y sitemap.xml presentes

- INFO **robots.txt**  
Presente (84 bytes)
- INFO **Reglas robots.txt**  
0 Disallow, 1 Allow
- INFO **Sitemap en robots.txt**  
<https://chronos-juxdeveloper.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 Cross-Site Scripting (XSS) e inyección de datos.

[HIGH] X-Frame-Options: Al no estar configurada, el sitio es vulnerable a ataques de Clickjacking, donde un atacante puede cargar la web en un frame invisible para engañar al usuario.

[HIGH] Strict-Transport-Security: La falta de HSTS impide que el navegador fuerce conexiones cifradas, facilitando ataques de degradación de SSL y robo de sesiones en redes inseguras.

[MEDIUM] Puerto 8080 (HTTP-Alt) abierto: La exposición de este puerto sugiere la presencia de un servidor web alternativo o proxy que podría ser explotado si no está debidamente protegido.

[MEDIUM] Rutas de administración accesibles: Se detectaron rutas como /wp-login.php, /administrator/ y /user/login disponibles públicamente, lo que facilita intentos de fuerza bruta.

[MEDIUM] Archivos informativos expuestos: El acceso público a /readme.html y /README.txt puede revelar detalles técnicos internos o versiones de software a posibles atacantes.

[MEDIUM] Permissions-Policy: La falta de esta cabecera permite que el sitio acceda a APIs sensibles del navegador sin restricciones granulares.

[LOW] Server header expuesto: La cabecera revela el uso de Cloudflare, proporcionando información técnica que ayuda a un atacante a perfilar la infraestructura.