

# Escanear Vulnerabilidades

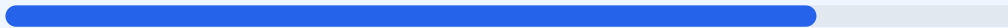
Informe de Seguridad Web

URL	https://www.change.org/p/clauidiashein-salvemos-mahahual-detengamos-el-proyecto-que-estruela-de-royal-caribbean/actions	Checks	9 pasivos
Dominio	www.change.org	Hallazgos	42 totales
Fecha	18 de mayo de 2026 a las 02:27	Problemas	8 detectados

# B

## 80/100

puntos de seguridad



### RESUMEN EJECUTIVO

El análisis de seguridad técnica realizado al sitio web arroja una puntuación de 80/100 con una calificación final de nota B. Se completaron exitosamente 9 checks pasivos, identificando 7 elementos correctamente configurados y 2 fallos de seguridad en las políticas de respuesta del servidor. Aunque la plataforma demuestra una gestión de cifrado impecable, la ausencia de cabeceras de protección críticas la hace vulnerable ante ataques de inyección y manipulación de interfaz. Por tanto, se concluye que el sitio es seguro en su infraestructura de red, pero vulnerable en su configuración de seguridad web orientada al cliente.

### Resumen de Riesgos



### Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 160 dias
Cabeceras de Seguridad	20	FALLO	Solo 1/6 presentes. Faltan: Content-Security-Pol...
Redireccion HTTPS	100	OK	HTTP redirige a HTTPS y HSTS esta habilitado
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 160 dias

- INFO Certificado valido**  
El certificado SSL es valido y de confianza
- INFO Dias hasta expiracion**  
160 dias restantes (expira: 2026-10-24T23:59:00Z)
- INFO Fecha de emision**  
Emitido desde: 2026-04-10T00:00:00Z
- INFO Puerto 443**  
Conexion HTTPS establecida correctamente en puerto 443

### Cabeceras de Seguridad — 20/100

Estado: FALLO

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

- BAJO Server header expuesto**  
Server: CloudFront — 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
- **INFO** **Strict-Transport-Security**  
Presente: max-age=15552000; includeSubDomains
- **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 — 100/100

---

Estado: OK

HTTP redirige a HTTPS y HSTS esta habilitado

- **INFO** **HTTP !' HTTPS redireccion**  
HTTP 301 redirige a https://www.change.org/
- **INFO** **HSTS (Strict-Transport-Security)**  
HSTS activo: max-age=15552000; includeSubDomains
- **BAJO** **HSTS includeSubDomains**  
HSTS cubre subdominios
- **INFO** **HSTS max-age**  
max-age=15552000 (180 dias)
- **INFO** **Respuesta HTTPS**  
HTTPS responde con status 202

## 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
- **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: La ausencia de esta cabecera permite la ejecución de scripts no autorizados y ataques de inyección de contenido XSS.
- [HIGH] X-Frame-Options: Al no estar presente, el sitio es susceptible a ataques de clickjacking donde un atacante puede cargar la web en un marco invisible.
- [MEDIUM] X-Content-Type-Options: La falta de esta configuración permite que los navegadores realicen sniffing de tipos MIME, pudiendo ejecutar archivos maliciosos.
- [MEDIUM] Referrer-Policy: No existe control sobre la información de referencia que el navegador envía a otros dominios al hacer clic en enlaces externos.
- [MEDIUM] Permissions-Policy: No se han restringido las APIs del navegador, permitiendo potencialmente el acceso no deseado a funciones de hardware o geolocalización.

[MEDIUM] Archivos técnicos expuestos: Se detectó acceso público a /readme.html y /README.txt, lo cual puede revelar detalles sobre la tecnología y versiones del sitio.

[LOW] Server header expuesto: El servidor revela el uso de CloudFront, proporcionando información útil para que un atacante planifique vectores específicos de explotación.