

Escanear Vulnerabilidades

Informe de Seguridad Web

URL https://alejandria-governance-dev.mnc.sancibpl.com
Dominio alejandria-governance-dev.mnc.sancibpl.com
Fecha 14 de mayo de 2026 a las 08:55

Checks 9 pruebas
Hallazgos 46 totales
Problemas 11 detectados

C

74/100

puntos de seguridad



RESUMEN EJECUTIVO

La auditoria de seguridad realizada al sitio web muestra una puntuacion de 74/100, lo que equivale a una nota de C. Se ejecutaron 9 checks pasivos, de los cuales 6 resultaron satisfactorios, 2 generaron advertencias y 1 resultado en fallo critico. A pesar de contar con un certificado SSL robusto, el servidor carece por completo de cabeceras de seguridad esenciales para proteger a los usuarios. El analisis concluye que el sitio es vulnerable debido a la falta de politicas contra ataques de inyeccion y suplantacion. Se recomienda una intervencion inmediata para elevar los estandares de proteccion de la plataforma.

Resumen de Riesgos



Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 305 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	60	AVISO	Falta sitemap.xml
Puertos Abiertos	100	OK	2 puerto(s) abierto(s), todos esperados

SSL/TLS — 100/100

Estado: OK

Certificado valido, expira en 305 dias

- INFO **Certificado valido**
El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
305 dias restantes (expira: 2027-03-14T23:59:59.000Z)
- INFO **Fecha de emision**
Emitido desde: 2026-02-13T00:00:00.000Z
- 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: AmazonS3 — 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://alejandria-governance-dev.mnc.sancibpl.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
- **INFO** **Tecnologias detectadas**
React

Version CMS Expuesta — 100/100

Estado: OK

No se detecto version de CMS expuesta

- **INFO** **Archivo /readme.html**
No accesible (correcto)
- **INFO** **Archivo /README.txt**
No accesible (correcto)
- **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 — 60/100

Estado: AVISO

Falta sitemap.xml

- INFO **robots.txt**
Presente (67 bytes)
- INFO **Reglas robots.txt**
1 Disallow, 0 Allow
- BAJO **sitemap.xml**
No encontrado (HTTP 403)
- 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 que previene ataques de Cross-Site Scripting (XSS) e inyeccion de datos.
- [HIGH] X-Frame-Options: La ausencia de esta politica permite que el sitio sea cargado en frames, facilitando ataques de clickjacking.
- [HIGH] Strict-Transport-Security: No se fuerza el uso de HTTPS mediante HSTS, permitiendo posibles degradaciones de conexion.
- [HIGH] HSTS no configurado: El navegador no tiene instrucciones para comunicarse exclusivamente por canales cifrados.
- [MEDIUM] X-Content-Type-Options: La falta de esta cabecera permite que el navegador intente adivinar el tipo de contenido, facilitando la ejecucion de scripts maliciosos.
- [MEDIUM] Referrer-Policy: No se controla que informacion de procedencia se envia a otros sitios, lo que puede filtrar URLs privadas.
- [MEDIUM] Permissions-Policy: No se restringe el acceso de la aplicacion a funciones del hardware como camara o microfono.
- [MEDIUM] Ruta /administrator/ expuesta: El panel de gestion es accesible publicamente, aumentando el riesgo de ataques de fuerza bruta.
- [MEDIUM] Ruta /user/login expuesta: El formulario de acceso de usuarios no cuenta con restricciones de visibilidad a nivel de red.
- [LOW] Server header expuesto: El servidor responde con la cadena AmazonS3, revelando detalles tecnologicos a posibles atacantes.
- [LOW] sitemap.xml no encontrado: El archivo devuelve un error 403, dificultando la indexacion correcta y sugiriendo permisos mal configurados.