# EscanearVulnerabilidades

Informe de Seguridad Web

| | | | |
|---|---|---|---|
| URL | https://www.policia.bo | Checks | 9 pruebas |
| Dominio | www.policia.bo | Hallazgos | 46 totales |
| Fecha | 7 de mayo de 2026 a las 04:26 | Problemas | 13 detectados |

C

64/100

puntos de seguridad

## RESUMEN EJECUTIVO

La auditoría de seguridad realizada al sitio web policia.bo ha arrojado una puntuación de 64/100, lo que equivale a una nota de C. El análisis pasivo ejecutó un total de 9 comprobaciones, de las cuales 5 resultaron satisfactorias, 2 generaron advertencias y 2 fueron calificadas como fallos críticos. Aunque el sitio posee un certificado SSL válido, la exposición de una versión de WordPress obsoleta y la ausencia total de cabeceras de seguridad representan riesgos significativos. No se realizó un pentest activo en esta sesión, limitando los resultados a la superficie de ataque expuesta públicamente. Debido a las deficiencias encontradas en la configuración del servidor y la gestión de parches, se concluye que el sitio es actualmente vulnerable.

## Resumen de Riesgos

| 0 | 5 | 5 | 3 | 33 |
|---|---|---|---|---|
| CRITICO | ALTO | MEDIO | BAJO | INFO |

## Resumen de Checks

| | | | |
|---|---|---|---|
| SSL/TLS | 100 | OK | Certificado valido, expira en 45 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 | CMS detectado: WordPress, PrestaShop |
| Version CMS Expuesta | 20 | FALLO | WordPress 2.0.2 expuesta, WordPress 2 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 45 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
  45 dias restantes (expira: 2026-06-20T18:20:49.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2026-03-22T17:22:08.000Z
- 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: 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)
- 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://www.policia.bo/
- 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

CMS detectado: WordPress, PrestaShop

- INFO **WordPress**
  Detectado via HTML body
- INFO **Joomla**
  No detectado
- INFO **Drupal**
  No detectado
- INFO **Magento**
  No detectado
- INFO **Shopify**
  No detectado
- INFO **PrestaShop**
  Detectado via HTML body
- INFO **Wix**
  No detectado
- INFO **Squarespace**
  No detectado
- BAJO **Meta generator**
  Expone: Elementor 3.25.5; features: additional_custom_breakpoints, e_optimized_control_loading; settings: css_print_method-external, google_font-enabled, font_display-swap
- INFO **Tecnologias detectadas**
  React, Next.js, Astro

## Version CMS Expuesta — 20/100

Estado: FALLO

WordPress 2.0.2 expuesta, WordPress 2 expuesta

- ALTO **WordPress version**
  Version 2.0.2 expuesta publicamente — Permite a atacantes buscar CVEs conocidos
- MEDIO **Archivo /readme.html**
  Archivo accesible publicamente — Puede revelar version e informacion del CMS
- INFO **Archivo /README.txt**
  No accesible (correcto)

## 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 (115 bytes)
- INFO **Reglas robots.txt**
  1 Disallow, 1 Allow
- BAJO **Ruta sensible en robots.txt**
  Referencia a "admin" — Puede revelar rutas sensibles a atacantes
- INFO **Sitemap en robots.txt**
  https://www.policia.bo/wp-sitemap.xml
- BAJO **security.txt**
  No encontrado — Recomendado para politica de divulgacion

## 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] WordPress version: Versión 2.0.2 expuesta públicamente — Permite a atacantes buscar y explotar CVEs conocidos para comprometer el servidor.
[HIGH] Content-Security-Policy: Falta — Facilita ataques de Cross-Site Scripting (XSS) e inyección de contenido malicioso al no restringir el origen de los recursos.
[HIGH] X-Frame-Options: Falta — El sitio es vulnerable a ataques de clickjacking, permitiendo que un atacante cargue el portal en un marco invisible para engañar al usuario.
[HIGH] Strict-Transport-Security: Falta — No se obliga al navegador a utilizar conexiones HTTPS, facilitando ataques de degradación de protocolo y robo de cookies.
[MEDIUM] Puerto 8080 (HTTP-Alt): ABIERTO — La presencia de un servidor alternativo o proxy abierto puede ser una vía de entrada para servicios no protegidos.
[MEDIUM] X-Content-Type-Options: Falta — Permite que el navegador intente adivinar el tipo de contenido (MIME-sniffing), lo que puede derivar en la ejecución de scripts maliciosos.
[MEDIUM] Referrer-Policy: Falta — No se controla qué información de procedencia se envía a otros sitios, lo que podría filtrar rutas internas o datos de navegación.
[MEDIUM] Permissions-Policy: Falta — El navegador no restringe el acceso a funciones sensibles como cámara o micrófono, aumentando el riesgo en caso de compromiso.
[MEDIUM] Archivo /readme.html: Archivo accesible públicamente — Confirma detalles técnicos y versiones del sistema de gestión de contenidos a potenciales atacantes.
[LOW] Server header expuesto: Server: cloudflare — Proporciona información técnica sobre la infraestructura, facilitando la fase de reconocimiento de un ataque.
[LOW] Meta generator: Expone Elementor 3.25.5 y configuraciones — Revela detalles específicos de plugins y métodos de impresión de CSS.
[LOW] Ruta sensible en robots.txt: Referencia a "admin" — Indica a los rastreadores, incluidos los maliciosos, la ubicación de paneles de administración o rutas privadas.