EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://picoyplacasolidario.movilidadbogota.gov.co/	Checks	9 pruebas
Dominio	picoyplacasolidario.movilidadbogota.gov.co	Hallazgos	41 totales
Fecha	19 de marzo de 2026 a las 19:53	Problemas	10 detectados

C

61/100

puntos de seguridad

RESUMEN EJECUTIVO

La evaluacion de seguridad realizada arroja una puntuacion de 61/100 con una calificacion de nota C. Se ejecutaron un total de 9 checks pasivos, identificando 6 componentes correctos y 3 fallos de seguridad significativos en la infraestructura de red y aplicacion. La ausencia total de cabeceras de proteccion y la gestion deficiente del trafico cifrado representan riesgos criticos de exposicion. Por lo tanto, el sitio se clasifica actualmente como vulnerable, requiriendo acciones correctivas inmediatas para mitigar posibles vectores de ataque.

Resumen de Riesgos

0	5	3	2	31
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 199 dias
Cabeceras de Seguridad	0	FALLO	Solo 0/6 presentes. Faltan: Content-Security-Pol...
Redireccion HTTPS	0	FALLO	No hay redireccion HTTP a HTTPS
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	No se detectaron puertos abiertos

SSL/TLS — 100/100

Estado: OK

Certificado valido, expira en 199 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
  199 dias restantes (expira: 2026-10-04T23:59:59.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2025-09-03T00:00:00.000Z
- 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

- 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 — 0/100

Estado: FALLO

No hay redireccion HTTP a HTTPS

- ALTO **HTTP !' HTTPS redireccion**
  HTTP 403 — No redirige a HTTPS
- ALTO **HSTS (Strict-Transport-Security)**
  HSTS no configurado — El navegador no fuerza HTTPS
- INFO **Respuesta HTTPS**
  HTTPS responde con status 403

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

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

- BAJO **robots.txt**
  No encontrado (HTTP 403)
- BAJO **sitemap.xml**
  No encontrado (HTTP 403)
- BAJO **security.txt**
  No encontrado — Recomendado para politica de divulgacion

Puertos Abiertos — 100/100

Estado: OK

No se detectaron puertos abiertos

- 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)**
  Cerrado — Servidor web
- INFO **Puerto 443 (HTTPS)**
  Cerrado — 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 facilita ataques de Cross-Site Scripting (XSS) e inyeccion de contenido malicioso al no restringir el origen de los recursos.
[HIGH] X-Frame-Options: La falta de esta directiva permite que el portal sea cargado en iframes externos, exponiendo a los usuarios a ataques de clickjacking.
[HIGH] Strict-Transport-Security: La carencia de HSTS impide forzar conexiones cifradas, permitiendo potenciales ataques de degradacion de protocolo y ataques Man-in-the-Middle.
[HIGH] Redireccion HTTP a HTTPS: El servidor no redirige automaticamente las peticiones inseguras a la version cifrada, devolviendo errores de acceso en lugar de asegurar la conexion.
[MEDIUM] X-Content-Type-Options: Al no estar configurada, el navegador puede intentar interpretar el contenido de forma distinta al tipo MIME declarado, facilitando la ejecucion de scripts.
[MEDIUM] Referrer-Policy: No existe control sobre la informacion de referencia enviada a otros sitios, lo que puede derivar en la fuga de datos de navegacion privados.
[MEDIUM] Permissions-Policy: La falta de restriccion en las APIs del navegador permite que funciones sensibles como camara o microfono queden expuestas sin una politica clara de control.

[LOW] Ausencia de robots.txt: No se detecto el archivo de control de rastreo, lo que impide gestionar adecuadamente la indexacion por parte de motores de busqueda.
[LOW] Ausencia de sitemap.xml: La falta de un mapa del sitio dificulta el analisis estructurado y la auditoria de los recursos publicos disponibles en el servidor.