EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://www.sanpedro-valle.gov.co/	Checks	9 pruebas
Dominio	www.sanpedro-valle.gov.co	Hallazgos	44 totales
Fecha	30 de agosto de 2026 a las 06:15	Problemas	9 detectados

C

71/100

puntos de seguridad

RESUMEN EJECUTIVO

La evaluacion de seguridad del sitio web arroja una puntuacion exacta de 71/100, lo que corresponde a una nota C. Durante el proceso se ejecutaron 9 checks pasivos, obteniendo 6 resultados satisfactorios y 3 fallos significativos en areas criticas de configuracion. Se detectaron deficiencias importantes en la implementacion de protocolos de cifrado obligatorio y en la proteccion contra ataques de inyeccion de contenido. Debido a la ausencia de cabeceras de seguridad fundamentales y la falta de redireccion automatica a conexiones seguras, el sitio se considera vulnerable. Es necesaria una intervencion tecnica inmediata para mitigar riesgos de suplantacion y fuga de metadatos tecnicos.

Resumen de Riesgos

0	2	7	0	35
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 70 dias
Cabeceras de Seguridad	50	FALLO	Solo 3/6 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	2 puerto(s) abierto(s), todos esperados

SSL/TLS — 100/100

Estado: OK

Certificado valido, expira en 70 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
  70 dias restantes (expira: 2026-11-07T23:59:59.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2026-08-09T00:00:00.000Z
- INFO **Puerto 443**
  Conexion HTTPS establecida correctamente en puerto 443

Cabeceras de Seguridad — 50/100

Estado: FALLO

Solo 3/6 presentes. Faltan: Content-Security-Policy, Referrer-Policy, Permissions-Policy

- ALTO **Content-Security-Policy**
  Falta — Previene XSS y ataques de inyeccion de contenido

- INFO **X-Frame-Options**
  Presente: SAMEORIGIN
- INFO **Strict-Transport-Security**
  Presente: max-age=31536000
- INFO **X-Content-Type-Options**
  Presente: nosniff
- 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 200 — No redirige a HTTPS
- INFO **HSTS (Strict-Transport-Security)**
  HSTS activo: max-age=31536000
- BAJO **HSTS includeSubDomains**
  HSTS no cubre subdominios
- INFO **HSTS max-age**
  max-age=31536000 (365 dias)
- 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 — 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

[ALTA] Redireccion HTTP a HTTPS: El sitio responde a traves de HTTP sin redirigir automaticamente a la version segura, permitiendo la intercepcion de datos en transito.
[ALTA] Content-Security-Policy (CSP): La ausencia de esta cabecera facilita la ejecucion de ataques Cross-Site Scripting (XSS) y la inyeccion de contenido malicioso.

[MEDIA] Referrer-Policy: No se ha configurado una politica de referencia, lo que podria exponer informacion sensible de la URL en las peticiones salientes.
[MEDIA] Permissions-Policy: La falta de esta cabecera permite que el navegador acceda innecesariamente a APIs como la camara, el microfono o la ubicacion si no se restringen.
[MEDIA] Archivos de informacion expuestos: Los archivos /readme.html y /README.txt son accesibles publicamente, lo que facilita el reconocimiento de la infraestructura por parte de atacantes.
[MEDIA] Paneles de login expuestos: Rutas criticas como /wp-login.php, /administrator/ y /user/login estan accesibles, aumentando el riesgo de ataques de fuerza bruta.
[BAJA] Ausencia de Robots.txt y Sitemap: La falta de estos archivos dificulta la indexacion correcta y el control sobre que partes del sitio deben ser rastreadas por motores de busqueda.