

EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://www.soledad-atlantico.gov.co/	Checks	9 pruebas
Dominio	www.soledad-atlantico.gov.co	Hallazgos	46 totales
Fecha	19 de marzo de 2026 a las 19:55	Problemas	5 detectados

A

90/100

puntos de seguridad



RESUMEN EJECUTIVO

El analisis de seguridad realizado arroja una puntuacion de 90/100 con una calificacion final de nota A. Se ejecutaron un total de 9 checks pasivos, obteniendo 8 resultados exitosos y unicamente 1 fallo relacionado con la configuracion de cabeceras de seguridad. Aunque la infraestructura base muestra una configuracion solida en cifrado y redireccion, se detectaron omisiones importantes en politicas de seguridad del navegador y exposicion de rutas administrativas. En conclusion, el sitio presenta un nivel de seguridad alto, pero se considera vulnerable a ataques de inyeccion y fuerza bruta debido a las carencias tecnicas mencionadas.

Resumen de Riesgos

0 CRITICO	1 ALTO	4 MEDIO	0 BAJO	41 INFO
--------------	-----------	------------	-----------	------------

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 77 dias
Cabeceras de Seguridad	50	FALLO	Solo 3/6 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	100	OK	robots.txt y sitemap.xml presentes
Puertos Abiertos	100	OK	2 puerto(s) abierto(s), todos esperados

SSL/TLS — 100/100

Estado: OK

Certificado valido, expira en 77 dias

- INFO Certificado valido
El certificado SSL es valido y de confianza
- INFO Dias hasta expiracion
77 dias restantes (expira: 2026-06-04T23:59:59.000Z)
- INFO Fecha de emision
Emitido desde: 2026-03-06T00:00:00.000Z
- 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 — 100/100

Estado: OK

HTTP redirige a HTTPS y HSTS esta habilitado

- INFO

HTTP !' HTTPS redireccion
HTTP 302 redirige a https://www.soledad-atlantico.gov.co/
- 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 días)
- 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

- 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 — 100/100

Estado: OK

robots.txt y sitemap.xml presentes

●	INFO	robots.txt
Presente (165 bytes)		
●	INFO	Reglas robots.txt
3 Disallow, 1 Allow		
●	INFO	Sitemap en robots.txt
https://www.soledad-atlantico.gov.co/sitemap.xml		
●	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 autentificacion 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 ejecucion de scripts maliciosos de terceros, facilitando ataques de Cross-Site Scripting (XSS) e inyeccion de contenido.

[MEDIUM] Referrer-Policy: La falta de esta politica impide controlar la cantidad de informacion de navegacion que el sitio web comparte al seguir enlaces externos.

[MEDIUM] Permissions-Policy: Al no estar presente, no se restringe el acceso de las APIs del navegador a funciones sensibles como la camara, el microfono o la geolocalizacion del usuario.

[MEDIUM] Ruta /administrator/: El panel de administracion es accesible de manera publica, lo que permite a atacantes realizar intentos de fuerza bruta o explotacion de vulnerabilidades de login.

[MEDIUM] Ruta /user/login: El endpoint de inicio de sesion de usuarios se encuentra expuesto, aumentando la superficie de ataque para comprometer cuentas de usuario.