# EscanearVulnerabilidades

Informe de Seguridad Web

| | | | |
|---|---|---|---|
| URL | https://neumaticosatlantico.com | Checks | 9 pruebas |
| Dominio | neumaticosatlantico.com | Hallazgos | 54 totales |
| Fecha | 5 de mayo de 2026 a las 14:53 | Problemas | 13 detectados |

C

66/100

puntos de seguridad

## RESUMEN EJECUTIVO

El análisis de seguridad realizado sobre el sitio web neumaticosatlantico.com ha dado como resultado una puntuación de 66/100, lo que corresponde a una calificación de nota C. Durante la evaluación se ejecutaron un total de 9 checks pasivos, identificando 5 verificaciones exitosas, 2 advertencias y 2 fallos críticos de seguridad. Los principales riesgos se concentran en la exposición de servicios de infraestructura y la ausencia total de cabeceras de protección en el servidor. Aunque el cifrado de transporte es correcto, la configuración global presenta debilidades estructurales importantes. En su estado actual, se concluye que el sitio es vulnerable ante ataques de red y de manipulación de contenido.

## Resumen de Riesgos

| 1 | 5 | 5 | 2 | 41 |
|---|---|---|---|---|
| CRITICO | ALTO | MEDIO | BAJO | INFO |

## Resumen de Checks

| | | | |
|---|---|---|---|
| SSL/TLS | 100 | OK | Certificado valido, expira en 61 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: PrestaShop |
| Version CMS Expuesta | 100 | OK | No se detecto version de CMS expuesta |
| Seguridad de Cookies | 100 | OK | 3 cookies, todas con flags correctos |
| Contenido Mixto | 100 | OK | No se detecto contenido mixto |
| Robots.txt y Sitemap | 60 | AVISO | Falta sitemap.xml |
| Puertos Abiertos | 20 | FALLO | 3 puertos riesgosos abiertos |

## SSL/TLS — 100/100

Estado: OK

Certificado valido, expira en 61 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
  61 dias restantes (expira: 2026-07-05T13:15:46.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2026-04-06T13:15:47.000Z
- 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: Apache — 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://neumaticosatlantico.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

CMS detectado: PrestaShop

- INFO **WordPress**
  No detectado
- 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
- INFO **Tecnologias detectadas**
  Next.js

## 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

3 cookies, todas con flags correctos

- INFO **Cookies detectadas**
  3 cookie(s) encontrada(s)
- INFO **Cookie: PHPSESSID — HttpOnly**
  HttpOnly activo — No accesible via JavaScript
- INFO **Cookie: PHPSESSID — Secure**
  Flag Secure activo — Solo se envia por HTTPS
- INFO **Cookie: PHPSESSID — SameSite**
  SameSite=lax
- INFO **Cookie: PrestaShop-ca1a339d81e40bd205f728f1dd49fa59 — HttpOnly**
  HttpOnly activo — No accesible via JavaScript
- INFO **Cookie: PrestaShop-ca1a339d81e40bd205f728f1dd49fa59 — Secure**
  Flag Secure activo — Solo se envia por HTTPS
- INFO **Cookie: PrestaShop-ca1a339d81e40bd205f728f1dd49fa59 — SameSite**
  SameSite=lax
- INFO **Cookie: PrestaShop-ca1a339d81e40bd205f728f1dd49fa59 — HttpOnly**
  HttpOnly activo — No accesible via JavaScript
- INFO **Cookie: PrestaShop-ca1a339d81e40bd205f728f1dd49fa59 — Secure**
  Flag Secure activo — Solo se envia por HTTPS
- INFO **Cookie: PrestaShop-ca1a339d81e40bd205f728f1dd49fa59 — SameSite**
  SameSite=lax

## 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 (525 bytes)
- INFO **Reglas robots.txt**
  1 Disallow, 0 Allow
- MEDIO **Bloqueo total**
  robots.txt bloquea todo el sitio con Disallow: /
- BAJO **sitemap.xml**
  No encontrado (HTTP 404)
- BAJO **security.txt**
  No encontrado — Recomendado para politica de divulgacion

## Puertos Abiertos — 20/100

Estado: FALLO

3 puertos riesgosos abiertos

- ALTO **Puerto 21 (FTP)**
  ABIERTO — Transferencia de archivos sin cifrar
- MEDIO **Puerto 22 (SSH)**
  ABIERTO — 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

- CRITICO **Puerto 3306 (MySQL)**
  ABIERTO — 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**

[CRITICAL] Puerto 3306 (MySQL): Servicio de base de datos expuesto a internet, lo que permite intentos de conexión externa y ataques de fuerza bruta.
[HIGH] Puerto 21 (FTP): El servicio de transferencia de archivos está abierto y transmite información de forma no cifrada, facilitando la interceptación de credenciales.
[HIGH] Content-Security-Policy: La ausencia de esta cabecera permite la ejecución de scripts maliciosos y ataques de inyección de contenido (XSS).
[HIGH] X-Frame-Options: El sitio no protege contra clickjacking, permitiendo que la web sea cargada en marcos externos para engañar al usuario.
[HIGH] Strict-Transport-Security: No se utiliza la política HSTS, lo que deja a los usuarios vulnerables ante ataques de degradación de HTTPS a HTTP.
[HIGH] HSTS (Strict-Transport-Security): El servidor no fuerza de manera estricta el uso de conexiones seguras en el navegador del cliente.
[MEDIUM] Puerto 22 (SSH): El puerto de administración remota está abierto al público, aumentando la superficie de ataque del servidor.
[MEDIUM] X-Content-Type-Options: Falta de protección contra el rastreo de tipos MIME, lo que podría llevar a la ejecución de archivos con contenido inesperado.
[MEDIUM] Referrer-Policy: No se controla la información de navegación que se envía a otros sitios mediante los enlaces de referencia.
[MEDIUM] Permissions-Policy: No existen restricciones sobre el acceso a funciones del navegador como la cámara o la geolocalización.
[MEDIUM] Robots.txt: El archivo bloquea el rastreo de todo el sitio mediante la directiva Disallow, afectando negativamente la indexación.
[LOW] Server header expuesto: La cabecera revela que el servidor utiliza Apache, proporcionando información útil para atacantes sobre posibles exploits.
[LOW] sitemap.xml: No se encuentra el archivo de mapa del sitio, lo cual es una deficiencia en la estructura de navegación y visibilidad.