

# Escanear Vulnerabilidades

Informe de Seguridad Web

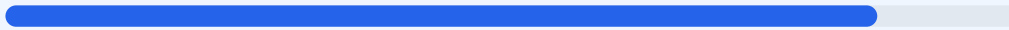
URL https://annetworksoluciones.com.ar  
Dominio annetworksoluciones.com.ar  
Fecha 21 de abril de 2026 a las 15:14

Checks 9 pruebas  
Hallazgos 44 totales  
Problemas 7 detectados

# B

## 86/100

puntos de seguridad



### RESUMEN EJECUTIVO

El análisis de seguridad realizado sobre el dominio analizado arrojó una puntuación de 86/100, lo que equivale a una nota de B. Durante la evaluación, se ejecutaron 9 checks pasivos, de los cuales 5 resultaron satisfactorios y 4 generaron advertencias, sin detectarse fallos críticos inmediatos. Aunque la base de seguridad es sólida, existen configuraciones pendientes en las cabeceras de transporte y exposición de puertos que deben corregirse. En su estado actual, el sitio se considera mayoritariamente seguro, pero vulnerable a ataques de degradación de protocolo y reconocimiento de infraestructura.

### Resumen de Riesgos



### Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 62 dias
Cabeceras de Seguridad	80	AVISO	5/6 presentes. Faltan: Strict-Transport-Security
Redireccion HTTPS	70	AVISO	HTTP redirige a HTTPS pero falta HSTS
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	60	AVISO	Falta sitemap.xml
Puertos Abiertos	60	AVISO	1 puerto(s) potencialmente riesgoso(s): 8080 (HT...

### SSL/TLS — 100/100

Estado: OK

Certificado valido, expira en 62 dias

- INFO **Certificado valido**  
El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**  
62 dias restantes (expira: 2026-06-22T20:10:48.000Z)
- INFO **Fecha de emision**  
Emitido desde: 2026-03-24T19:14:20.000Z
- INFO **Puerto 443**  
Conexion HTTPS establecida correctamente en puerto 443

### Cabeceras de Seguridad — 80/100

Estado: AVISO

5/6 presentes. Faltan: Strict-Transport-Security

- BAJO **Server header expuesto**  
Server: cloudflare — Revela tecnologia del servidor

- INFO **Content-Security-Policy**  
Presente: default-src 'none'; script-src 'nonce-a4qBEDp0DSTyko41GvYp19' 'unsafe-eval' http...
- INFO **X-Frame-Options**  
Presente: SAMEORIGIN
- ALTO **Strict-Transport-Security**  
Falta — Fuerza conexiones HTTPS (HSTS)
- INFO **X-Content-Type-Options**  
Presente: nosniiff
- INFO **Referrer-Policy**  
Presente: same-origin
- INFO **Permissions-Policy**  
Presente: accelerometer=(),browsing-topics=(),camera=(),clipboard-read=(),clipboard-write=...

## Redireccion HTTPS — 70/100

---

Estado: AVISO

HTTP redirige a HTTPS pero falta HSTS

- INFO **HTTP !' HTTPS redireccion**  
HTTP 301 redirige a https://annetworksoluciones.com.ar/
- 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)
- MEDIO **Archivo /README.txt**  
Archivo accesible publicamente — Puede revelar version e informacion del CMS
- 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 — 60/100

Estado: AVISO

Falta sitemap.xml

- INFO **robots.txt**  
Presente (1805 bytes)
- INFO **Reglas robots.txt**  
10 Disallow, 1 Allow
- MEDIO **Bloqueo total**  
robots.txt bloquea todo el sitio con Disallow: /
- BAJO **sitemap.xml**  
No encontrado (HTTP 403)
- INFO **security.txt**  
Presente en /.well-known/security.txt — Buena practica

## 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] Strict-Transport-Security (HSTS): La cabecera no está configurada, lo que permite que un atacante intente degradar la conexión del usuario de HTTPS a HTTP.

[MEDIUM] Puerto 8080 (HTTP-Alt) abierto: La presencia de un servidor web alternativo o proxy abierto puede ser utilizada para acceder a interfaces administrativas no protegidas.

[MEDIUM] Archivo /README.txt accesible: Este archivo se encuentra expuesto públicamente y puede revelar detalles técnicos o versiones de la tecnología subyacente.

[MEDIUM] Configuración de Robots.txt: El archivo bloquea el acceso total al sitio mediante la directiva Disallow: /, lo cual puede indicar una configuración de desarrollo o restricciones de acceso inconsistentes.

[LOW] Server header expuesto: La cabecera revela el uso de Cloudflare, facilitando a posibles atacantes el reconocimiento de las capas de protección empleadas.

[LOW] Falta de sitemap.xml: El archivo no fue encontrado o devuelve un error 403, limitando la visibilidad y auditoría de las rutas legítimas del sitio.