

EscanearVulnerabilidades

Informe de Seguridad Web

URL https://app.antartik.com.ar
Dominio app.antartik.com.ar
Fecha 7 de agosto de 2026 a las 01:29

Checks 9 pruebas
Hallazgos 46 totales
Problemas 4 detectados

A

94/100

puntos de seguridad



RESUMEN EJECUTIVO

El análisis de seguridad del sitio app.antartik.com.ar arroja una puntuación de 94/100 con una calificación final de grado A. Se ejecutaron un total de 9 verificaciones pasivas, obteniendo 7 resultados satisfactorios, 2 advertencias y 0 fallos críticos. Aunque no se detectaron vulnerabilidades que comprometan de forma inmediata la integridad de los datos, existen configuraciones en puertos y archivos de rastreo que deben ser revisadas. Se concluye que el sitio es seguro y sigue las mejores prácticas de la industria en su configuración actual.

Resumen de Riesgos



Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 61 dias
Cabeceras de Seguridad	100	OK	Todas las cabeceras de seguridad presentes
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	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 61 dias

- INFO Certificado valido
El certificado SSL es valido y de confianza
- INFO Dias hasta expiracion
61 dias restantes (expira: 2026-10-06T20:00:01.000Z)
- INFO Fecha de emision
Emitido desde: 2026-07-08T19:00:04.000Z
- INFO Puerto 443
Conexion HTTPS establecida correctamente en puerto 443

Cabeceras de Seguridad — 100/100

Estado: OK

Todas las cabeceras de seguridad presentes

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

- INFO

Content-Security-Policy
Presente: default-src 'none'; script-src 'nonce-TczmSngmUOGRRt8xyZkKQ1' 'unsafe-eval' http...
- INFO

X-Frame-Options
Presente: SAMEORIGIN
- INFO

Strict-Transport-Security
Presente: max-age=15552000; includeSubDomains; preload
- INFO

X-Content-Type-Options
Presente: nosniff
- INFO

Referrer-Policy
Presente: same-origin
- INFO

Permissions-Policy
Presente: accelerometer=(),camera=(),clipboard-read=(),clipboard-write=(),geolocation=(),g...

Redireccion HTTPS — 100/100

Estado: OK

HTTP redirige a HTTPS y HSTS esta habilitado

- INFO

HTTP !' HTTPS redireccion
HTTP 301 redirige a https://app.antartik.com.ar/
- INFO

HSTS (Strict-Transport-Security)
HSTS activo: max-age=15552000; includeSubDomains; preload
- BAJO

HSTS includeSubDomains
HSTS cubre subdominios
- INFO

HSTS max-age
max-age=15552000 (180 dias)
- 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 — 60/100

Estado: AVISO

Falta sitemap.xml

- INFO

robots.txt
Presente (1836 bytes)
- INFO

Reglas robots.txt
9 Disallow, 1 Allow
- MEDIO

Bloqueo total
robots.txt bloquea todo el sitio con Disallow: /
- BAJO

sitemap.xml
No encontrado (HTTP 403)
- BAJO

security.txt
No encontrado — Recomendado para politica de divulgacion

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

[MEDIUM] Puerto 8080 (HTTP-Alt) abierto: La presencia de un servidor web alternativo o proxy abierto incrementa la superficie de ataque y puede exponer servicios administrativos.

[MEDIUM] Bloqueo total en robots.txt: La instrucción Disallow: / bloquea completamente el rastreo, lo cual puede ser una configuración restrictiva que oculte errores de configuración de acceso.

[LOW] Server header expuesto: Se detectó la cabecera Server: cloudflare, lo cual revela información sobre la tecnología de infraestructura utilizada.

[LOW] sitemap.xml no encontrado: El archivo devuelve un código de estado 403, impidiendo una indexación estructurada y correcta del sitio.