EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://cloud.antartik.com.ar	Checks	9 pruebas
Dominio	cloud.antartik.com.ar	Hallazgos	68 totales
Fecha	7 de agosto de 2026 a las 01:31	Problemas	7 detectados

B

87/100

puntos de seguridad

RESUMEN EJECUTIVO

El análisis de seguridad realizado sobre la plataforma ha arrojado una puntuación de 87/100, lo que otorga una calificación de nota B. Se ejecutaron un total de 9 controles pasivos, de los cuales 6 resultaron satisfactorios, 2 generaron advertencias y 1 fue identificado como fallo crítico. Aunque el sitio presenta una configuración web sólida en cuanto a cifrado y gestión de identidad, se han detectado riesgos importantes en la infraestructura del servidor. Se concluye que el sitio es seguro para la navegación del usuario final, pero se considera vulnerable ante ataques dirigidos a nivel de red debido a servicios expuestos.

Resumen de Riesgos

0	1	4	2	61
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 52 dias
Cabeceras de Seguridad	85	AVISO	5/6 presentes. Faltan: Permissions-Policy
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	7 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 52 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
  52 dias restantes (expira: 2026-09-27T20:40:45.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2026-06-29T20:40:46.000Z
- INFO **Puerto 443**
  Conexion HTTPS establecida correctamente en puerto 443

Cabeceras de Seguridad — 85/100

Estado: AVISO

5/6 presentes. Faltan: Permissions-Policy

- BAJO **Server header expuesto**
  Server: Apache/2.4.58 (Ubuntu) — Revela tecnologia del servidor

- INFO **Content-Security-Policy**
  Presente: default-src 'none';base-uri 'none';manifest-src 'self';script-src 'nonce-51MmBIU...
- INFO **X-Frame-Options**
  Presente: SAMEORIGIN
- INFO **Strict-Transport-Security**
  Presente: max-age=63072000; includeSubDomains; preload
- INFO **X-Content-Type-Options**
  Presente: nosniff
- INFO **Referrer-Policy**
  Presente: same-origin
- 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 301 redirige a https://cloud.antartik.com.ar/
- INFO **HSTS (Strict-Transport-Security)**
  HSTS activo: max-age=63072000; includeSubDomains; preload
- BAJO **HSTS includeSubDomains**
  HSTS cubre subdominios
- INFO **HSTS max-age**
  max-age=63072000 (730 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
- 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

7 cookies, todas con flags correctos

- INFO **Cookies detectadas**
  7 cookie(s) encontrada(s)
- INFO **Cookie: ocpxusybls6g — HttpOnly**
  HttpOnly activo — No accesible via JavaScript
- INFO **Cookie: ocpxusybls6g — Secure**
  Flag Secure activo — Solo se envia por HTTPS
- INFO **Cookie: ocpxusybls6g — SameSite**
  SameSite=lax
- INFO **Cookie: oc_sessionPassphrase — HttpOnly**
  HttpOnly activo — No accesible via JavaScript
- INFO **Cookie: oc_sessionPassphrase — Secure**
  Flag Secure activo — Solo se envia por HTTPS
- INFO **Cookie: oc_sessionPassphrase — SameSite**
  SameSite=lax
- INFO **Cookie: ocpxusybls6g — HttpOnly**
  HttpOnly activo — No accesible via JavaScript
- INFO **Cookie: ocpxusybls6g — Secure**
  Flag Secure activo — Solo se envia por HTTPS
- INFO **Cookie: ocpxusybls6g — SameSite**
  SameSite=lax
- INFO **Cookie: __Host-nc_sameSiteCookielax — HttpOnly**
  HttpOnly activo — No accesible via JavaScript
- INFO **Cookie: __Host-nc_sameSiteCookielax — Secure**
  Flag Secure activo — Solo se envia por HTTPS
- INFO **Cookie: __Host-nc_sameSiteCookielax — SameSite**
  SameSite=lax
- INFO **Cookie: __Host-nc_sameSiteCookiestrict — HttpOnly**
  HttpOnly activo — No accesible via JavaScript
- INFO **Cookie: __Host-nc_sameSiteCookiestrict — Secure**
  Flag Secure activo — Solo se envia por HTTPS
- INFO **Cookie: __Host-nc_sameSiteCookiestrict — SameSite**
  SameSite=strict
- INFO **Cookie: ocpxusybls6g — HttpOnly**
  HttpOnly activo — No accesible via JavaScript
- INFO **Cookie: ocpxusybls6g — Secure**
  Flag Secure activo — Solo se envia por HTTPS
- INFO **Cookie: ocpxusybls6g — SameSite**
  SameSite=lax
- INFO **Cookie: ocpxusybls6g — HttpOnly**
  HttpOnly activo — No accesible via JavaScript
- INFO **Cookie: ocpxusybls6g — Secure**
  Flag Secure activo — Solo se envia por HTTPS
- INFO **Cookie: ocpxusybls6g — 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 (26 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)
- INFO **security.txt**
  Presente en /.well-known/security.txt — Buena practica

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
- 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] Puerto 21 (FTP) abierto: El servicio de transferencia de archivos está accesible, lo que permite el envío de datos y credenciales sin cifrado a través de la red.
[MEDIUM] Puerto 8080 (HTTP-Alt) abierto: La exposición de un puerto alternativo suele indicar la presencia de servicios de gestión o proxys que aumentan la superficie de ataque.
[MEDIUM] Puerto 22 (SSH) abierto: El servicio de acceso remoto está expuesto públicamente, quedando vulnerable a intentos de intrusión por fuerza bruta.
[MEDIUM] Permissions-Policy ausente: La falta de esta cabecera impide restringir el acceso del navegador a funciones sensibles como la cámara, el micrófono o la geolocalización.
[MEDIUM] Bloqueo total en robots.txt: El archivo de configuración contiene una instrucción Disallow que prohíbe el rastreo de todo el sitio, afectando la visibilidad legítima.
[LOW] Exposición de cabecera de servidor: Se revela el uso de Apache/2.4.58 sobre Ubuntu, lo que facilita a un atacante la búsqueda de vulnerabilidades específicas para esa versión.
[LOW] Falta de archivo sitemap.xml: No se encontró el mapa del sitio, lo que se considera una deficiencia en la estructura y organización de los recursos web.