EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://www.cpuinformatica.com.ar/	Checks	9 pruebas
Dominio	www.cpuinformatica.com.ar	Hallazgos	44 totales
Fecha	15 de mayo de 2026 a las 11:15	Problemas	6 detectados

B

86/100

puntos de seguridad

RESUMEN EJECUTIVO

El análisis de seguridad realizado sobre la plataforma ha dado como resultado una puntuación de 86/100, lo que representa una calificación de grado B. Durante la evaluación se ejecutaron un total de 9 comprobaciones pasivas, de las cuales 5 resultaron satisfactorias y 4 generaron advertencias de seguridad, sin detectarse fallos críticos inmediatos. Cabe destacar que no se realizó un pentest activo, por lo que los resultados se limitan a la configuración externa y de red. En conclusión, el sitio se considera moderadamente seguro, aunque presenta vulnerabilidades de configuración en el transporte de datos y exposición de servicios que deben ser subsanadas.

Resumen de Riesgos

0	2	2	2	38
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 42 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 42 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
  42 dias restantes (expira: 2026-06-26T06:11:56.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2026-03-28T06:11:57.000Z
- 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-uBmmpRfwcL5i48NQxCy7XC' 'unsafe-eval' http...
- INFO **X-Frame-Options**
  Presente: SAMEORIGIN
- ALTO **Strict-Transport-Security**
  Falta — Fuerza conexiones HTTPS (HSTS)
- INFO **X-Content-Type-Options**
  Presente: nosniff
- 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://www.cpuinformatica.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)
- 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 (1738 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

[HIGH] HSTS (Strict-Transport-Security): No configurado. Esto es peligroso porque permite ataques de degradación de protocolo donde un atacante puede interceptar la comunicación pasando de HTTPS a HTTP.
[MEDIUM] Puerto 8080 (HTTP-Alt) ABIERTO: Se detectó un servidor web alternativo o proxy expuesto. Esto aumenta la superficie de ataque al ofrecer un punto de entrada adicional no estándar.

[MEDIUM] Bloqueo total en robots.txt: El archivo contiene la directiva Disallow: / que impide el rastreo total. Es peligroso si se usa para ocultar directorios que deberían estar protegidos por autenticación y no por simple omisión.
[MEDIUM] sitemap.xml no encontrado: El servidor responde con un error 403 al intentar acceder al mapa del sitio. Esto indica una configuración de permisos restrictiva que afecta la indexación y auditoría de contenidos.
[LOW] Server header expuesto: Se detectó la cabecera Server: cloudflare. Revelar la tecnología del servidor facilita a los atacantes la búsqueda de vulnerabilidades específicas para esa infraestructura.