

EscanearVulnerabilidades

Informe de Seguridad Web

URL https://www.ciec.com.ar
Dominio www.ciec.com.ar
Fecha 7 de octubre de 2026 a las 14:18

Checks 9 pruebas
Hallazgos 49 totales
Problemas 10 detectados

C

72/100

puntos de seguridad



RESUMEN EJECUTIVO

La auditoría de seguridad realizada al sitio www.ciec.com.ar arroja una puntuación de 72/100, lo que equivale a una nota de C. El análisis se basó en 9 checks pasivos, de los cuales 5 resultaron satisfactorios, 3 generaron advertencias y 1 falló completamente. Aunque el sitio posee un cifrado de conexión válido, la ausencia crítica de cabeceras de seguridad modernas compromete la protección del usuario final. En su estado actual, el sitio se considera vulnerable a ataques de inyección y suplantación de identidad debido a configuraciones incompletas en el servidor.

Resumen de Riesgos



Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 47 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	No se detecto un CMS conocido
Version CMS Expuesta	100	OK	No se detecto version de CMS expuesta
Seguridad de Cookies	83	AVISO	XSRF-TOKEN: falta HttpOnly
Contenido Mixto	100	OK	No se detecto contenido mixto
Robots.txt y Sitemap	60	AVISO	Falta sitemap.xml
Puertos Abiertos	100	OK	No se detectaron puertos abiertos

SSL/TLS — 100/100

Estado: OK

Certificado valido, expira en 47 dias

- INFO Certificado valido
El certificado SSL es valido y de confianza
- INFO Dias hasta expiracion
47 dias restantes (expira: 2026-11-23T13:08:18.000Z)
- INFO Fecha de emision
Emitido desde: 2026-08-25T13:08:19.000Z
- 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/2 — 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://www.ciec.com.ar/
- 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

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 — 83/100

Estado: AVISO

XSRF-TOKEN: falta HttpOnly

- INFO

Cookies detectadas
2 cookie(s) encontrada(s)
- ALTO

Cookie: XSRF-TOKEN — HttpOnly
Falta HttpOnly — Cookie accesible via document.cookie (riesgo XSS)
- INFO

Cookie: XSRF-TOKEN — Secure
Flag Secure activo — Solo se envía por HTTPS
- INFO

Cookie: XSRF-TOKEN — SameSite
SameSite=lax
- INFO

Cookie: laravel-session — HttpOnly
HttpOnly activo — No accesible via JavaScript
- INFO

Cookie: laravel-session — Secure
Flag Secure activo — Solo se envía por HTTPS
- INFO

Cookie: laravel-session — 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 (24 bytes)
- INFO

Reglas robots.txt
1 Disallow, 0 Allow
- BAJO

sitemap.xml
No encontrado (HTTP 404)
- BAJO

security.txt
No encontrado — Recomendado para política de divulgacion

Puertos Abiertos — 100/100

Estado: OK

No se detectaron puertos abiertos

- 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 — Envío de correo
- INFO

Puerto 80 (HTTP)
Cerrado — Servidor web
- INFO

Puerto 443 (HTTPS)
Cerrado — 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



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

[HIGH] Content-Security-Policy: Falta esta cabecera, lo que permite la ejecución de scripts maliciosos y ataques de inyección de contenido (XSS).

[HIGH] X-Frame-Options: La ausencia de esta directiva hace que el sitio sea susceptible a ataques de clickjacking, permitiendo que un atacante lo cargue en marcos invisibles.

[HIGH] Strict-Transport-Security: No está configurado, por lo que el navegador no fuerza la conexión HTTPS, facilitando ataques de degradación de SSL.

[HIGH] Cookie XSRF-TOKEN: Falta el atributo HttpOnly, lo que permite que la cookie sea accesible mediante scripts de cliente, aumentando el riesgo de robo de sesión.

[MEDIUM] X-Content-Type-Options: La falta de esta cabecera permite que el navegador realice "MIME-type sniffing", lo que podría derivar en la ejecución de archivos maliciosos disfrazados.

[MEDIUM] Referrer-Policy: No existe una política definida, lo que puede exponer información sensible de la URL en las peticiones salientes a otros sitios.

[MEDIUM] Permissions-Policy: El servidor no restringe el acceso a APIs del navegador, dejando abierta la posibilidad de que se utilicen funciones como la cámara o el micrófono sin control estricto.

[LOW] Server header expuesto: El servidor revela "Apache/2", proporcionando información técnica valiosa que un atacante puede usar para buscar exploits específicos de esa versión.

[LOW] sitemap.xml: El archivo no fue encontrado, lo que dificulta la indexación correcta y el análisis de la estructura del sitio por herramientas legítimas.