

Escanear Vulnerabilidades

Informe de Seguridad Web

URL https://astracamp.cl
Dominio astracamp.cl
Fecha 28 de mayo de 2026 a las 04:30

Checks 9 pruebas
Hallazgos 42 totales
Problemas 10 detectados

C

72/100

puntos de seguridad



RESUMEN EJECUTIVO

El análisis de ciberseguridad realizado al sitio astracamp.cl arroja una puntuación de 72/100, lo que corresponde a una nota C. Durante la evaluación, se ejecutaron 9 checks pasivos, resultando en 6 verificaciones exitosas, 1 advertencia y 2 fallos críticos en la configuración del servidor. El sitio web presenta una base sólida en cuanto al cifrado de datos, pero carece por completo de cabeceras de seguridad modernas. Esta omisión facilita ataques de inyección de código y suplantación de identidad. En su estado actual, el sitio se considera vulnerable ante ataques dirigidos a la capa de aplicación y navegación del usuario.

Resumen de Riesgos



Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 90 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	100	OK	No se encontraron cookies
Contenido Mixto	100	OK	No se detecto contenido mixto
Robots.txt y Sitemap	20	FALLO	Faltan robots.txt y sitemap.xml
Puertos Abiertos	100	OK	No se detectaron puertos abiertos

SSL/TLS — 100/100

Estado: OK

Certificado valido, expira en 90 dias

- INFO **Certificado valido**
El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
90 dias restantes (expira: 2026-08-26T01:05:37.000Z)
- INFO **Fecha de emision**
Emitido desde: 2026-05-28T01:05:38.000Z
- 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 — 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://astracamp.cl/
- **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 — 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 — 20/100

Estado: FALLO

Faltan robots.txt y sitemap.xml

- BAJO **robots.txt**
No encontrado (HTTP 404)
- BAJO **sitemap.xml**
No encontrado (HTTP 404)
- BAJO **security.txt**
No encontrado — Recomendado para politica 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 — Envio 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 autentificacion 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: La ausencia de esta cabecera permite ataques de Cross-Site Scripting (XSS) y la inyección de contenido malicioso.
- [HIGH] X-Frame-Options: Al no estar presente, el sitio es susceptible a ataques de clickjacking, donde un atacante puede engañar al usuario para que realice acciones no deseadas.
- [HIGH] Strict-Transport-Security: La falta de configuración HSTS impide que el navegador fuerce automáticamente la conexión HTTPS, permitiendo posibles degradaciones de seguridad.
- [MEDIUM] X-Content-Type-Options: El servidor no previene el MIME-type sniffing, lo que podría llevar a la ejecución inadvertida de scripts ocultos en archivos de datos.
- [MEDIUM] Referrer-Policy: No se controla la información de referencia enviada a otros sitios, lo que puede exponer datos sensibles en las URLs de navegación.
- [MEDIUM] Permissions-Policy: El sitio no restringe el acceso a APIs sensibles del navegador como la ubicación, cámara o micrófono.

[LOW] Server header expuesto: El servidor responde con la firma Server: Apache, revelando la tecnología utilizada y facilitando la búsqueda de exploits específicos.

[LOW] robots.txt: No se encontró el archivo en el servidor, dificultando la gestión del rastreo por parte de motores de búsqueda.

[LOW] sitemap.xml: El archivo de mapa de sitio no está disponible, lo que afecta la transparencia de la estructura del sitio para herramientas de indexación.