EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://ingenieriauribespa.cl	Checks	9 pruebas
Dominio	ingenieriauribespa.cl	Hallazgos	44 totales
Fecha	26 de mayo de 2026 a las 17:36	Problemas	12 detectados

D

59/100

puntos de seguridad

RESUMEN EJECUTIVO

El análisis de seguridad realizado al sitio web arroja una puntuación de 59/100 con una calificación de nota D. Se ejecutaron 9 comprobaciones pasivas, de las cuales 5 resultaron satisfactorias, 2 generaron advertencias y 2 finalizaron en fallo crítico debido a configuraciones de servidor deficientes. Aunque el certificado SSL es válido, la ausencia de cabeceras de seguridad y la falta de redirección forzosa a HTTPS comprometen la integridad del sitio. En su estado actual, ingenieriauribespa.cl se considera un sitio vulnerable ante ataques de interceptación y manipulación de contenido.

Resumen de Riesgos

0	5	5	2	32
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 70 dias
Cabeceras de Seguridad	0	FALLO	Solo 0/6 presentes. Faltan: Content-Security-Pol...
Redireccion HTTPS	0	FALLO	No hay redireccion HTTP a HTTPS
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 70 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
  70 dias restantes (expira: 2026-08-05T01:01:51.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2026-05-07T00:01:55.000Z
- 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: cloudflare — 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 — 0/100

Estado: FALLO

No hay redireccion HTTP a HTTPS

- ALTO **HTTP !' HTTPS redireccion**
  HTTP 200 — No redirige a HTTPS
- 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 — 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 404)
- 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] Content-Security-Policy (CSP): Falta la cabecera CSP, lo que facilita la ejecución de ataques de inyección de código y Cross-Site Scripting (XSS).
[HIGH] X-Frame-Options: La ausencia de esta cabecera hace que el sitio sea vulnerable a ataques de clickjacking.
[HIGH] Strict-Transport-Security (HSTS): No se aplica HSTS, por lo que el navegador no obliga a realizar conexiones seguras permanentemente.

[HIGH] Redirección HTTPS fallida: El sitio responde a través de HTTP sin redirigir automáticamente a los usuarios a la versión cifrada HTTPS.
[MEDIUM] Puerto 8080 (HTTP-Alt) abierto: La exposición de este puerto alternativo aumenta la superficie de ataque y puede revelar servicios internos.
[MEDIUM] X-Content-Type-Options: Al faltar esta cabecera, los navegadores podrían intentar adivinar el tipo de contenido, permitiendo la ejecución de scripts maliciosos.
[MEDIUM] Referrer-Policy: No existe una política definida para controlar la cantidad de información enviada en las peticiones salientes.
[MEDIUM] Permissions-Policy: No se restringen las capacidades del navegador (cámara, micrófono, geolocalización) mediante políticas de cabecera.
[MEDIUM] Bloqueo total en robots.txt: El archivo de rastreo está configurado para bloquear el acceso a todo el sitio, lo que afecta la visibilidad en buscadores.
[LOW] Cabecera Server expuesta: Se revela el uso de Cloudflare, proporcionando a posibles atacantes información sobre la infraestructura de red.
[LOW] Sitemap no encontrado: La ausencia de un mapa del sitio dificulta la auditoría de activos y la indexación correcta de contenidos.