EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://www.municipalidadosorno.cl/new/	Checks	9 pruebas
Dominio	www.municipalidadosorno.cl	Hallazgos	46 totales
Fecha	6 de agosto de 2026 a las 02:37	Problemas	15 detectados

D

52/100

puntos de seguridad

RESUMEN EJECUTIVO

La auditoría de seguridad realizada al sitio web ha arrojado una puntuación de 52/100, lo que equivale a una calificación de nota D. Durante el análisis se ejecutaron 9 checks pasivos, de los cuales 4 resultaron satisfactorios, 1 generó una advertencia y 4 presentaron fallos críticos. Se detectaron deficiencias significativas en la implementación de cabeceras de seguridad y en la gestión de protocolos de conexión cifrada. Debido a la falta de políticas de protección contra inyecciones y la presencia de contenido mixto, el sitio se considera vulnerable y presenta un riesgo considerable para la integridad de los datos de los usuarios. Es imperativo abordar las configuraciones de red y servidor para mejorar la postura de seguridad actual.

Resumen de Riesgos

0	4	8	3	31
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 78 dias
Cabeceras de Seguridad	15	FALLO	Solo 1/6 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	20	FALLO	11 recursos HTTP en pagina HTTPS
Robots.txt y Sitemap	20	FALLO	Faltan robots.txt y sitemap.xml
Puertos Abiertos	60	AVISO	1 puerto(s) potencialmente riesgoso(s): 8080 (HT...

SSL/TLS — 100/100

Estado: OK

Certificado valido, expira en 78 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
  78 dias restantes (expira: 2026-10-23T13:00:36.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2026-07-25T12:02:17.000Z
- INFO **Puerto 443**
  Conexion HTTPS establecida correctamente en puerto 443

Cabeceras de Seguridad — 15/100

Estado: FALLO

Solo 1/6 presentes. Faltan: Content-Security-Policy, Strict-Transport-Security, X-Content-Type-Options, Referrer-Policy, Permissions-Policy

- BAJO **Server header expuesto**
  Server: cloudflare — Revela tecnologia del servidor

- BAJO **X-Powered-By expuesto**
  X-Powered-By: PHP/8.3.0 — Revela framework/lenguaje
- ALTO **Content-Security-Policy**
  Falta — Previene XSS y ataques de inyeccion de contenido
- INFO **X-Frame-Options**
  Presente: SAMEORIGIN
- 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
- INFO **Tecnologias detectadas**
  Next.js, PHP/8.3.0

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 — 20/100

Estado: FALLO

11 recursos HTTP en pagina HTTPS

- MEDIO **Recurso HTTP (href (link/stylesheet))**
  http://www.municipalidadosorno.cl/sitios/cp/webimo2.0/rss/rs...
- MEDIO **Recurso HTTP (href (link/stylesheet))**
  http://www.portaltransparencia.cl/PortalPdT/pdtta?codOrganis...
- MEDIO **Recurso HTTP (href (link/stylesheet))**
  http://www.imo.cl/ter/
- MEDIO **href (link/stylesheet)**
  ...y 8 mas del mismo tipo

Robots.txt y Sitemap — 20/100

Estado: FALLO

Faltan robots.txt y sitemap.xml

- 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: La ausencia de esta cabecera permite ataques de Cross-Site Scripting (XSS) e inyección de contenido malicioso.
[HIGH] Redirección HTTP a HTTPS: El sitio no redirige automáticamente el tráfico no cifrado, permitiendo conexiones inseguras por el puerto 80.
[HIGH] Strict-Transport-Security: La falta de HSTS impide que el navegador fuerce conexiones seguras, exponiendo a los usuarios a ataques de degradación de protocolo.
[MEDIUM] Contenido Mixto: Se detectaron 11 recursos cargados a través de HTTP en una página HTTPS, lo que debilita el cifrado general del sitio.
[MEDIUM] X-Content-Type-Options: La falta de esta cabecera permite el MIME-type sniffing, lo que puede llevar a la ejecución de archivos maliciosos disfrazados.
[MEDIUM] Puerto 8080 (HTTP-Alt): Este puerto se encuentra abierto, lo cual suele ser utilizado para servicios administrativos o proxies que pueden ser vectores de ataque.
[MEDIUM] Referrer-Policy: La ausencia de esta política puede filtrar información sensible sobre la procedencia del tráfico hacia sitios externos.
[MEDIUM] Permissions-Policy: No se restringen las APIs del navegador, permitiendo potencialmente el acceso no autorizado a funciones como cámara o micrófono.
[LOW] Cabecera Server expuesta: Se revela que el servidor utiliza Cloudflare, facilitando la identificación de la infraestructura tecnológica por parte de atacantes.
[LOW] X-Powered-By expuesto: El sitio revela el uso de PHP/8.3.0, proporcionando información específica sobre el lenguaje y su versión para buscar exploits conocidos.
[LOW] Robots.txt y Sitemap: La falta de estos archivos dificulta la auditoría de rutas permitidas y la correcta indexación de contenidos.