

EscanearVulnerabilidades

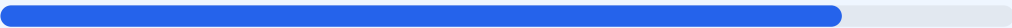
Informe de Seguridad Web

URL	https://clientes.transportesdyh.cl	Checks	9 pruebas
Dominio	clientes.transportesdyh.cl	Hallazgos	45 totales
Fecha	1 de octubre de 2026 a las 22:49	Problemas	6 detectados

B

83/100

puntos de seguridad



RESUMEN EJECUTIVO

La auditoría de seguridad realizada al sitio clientes.transportesdyh.cl ha arrojado una puntuación de 83/100, lo que corresponde a una calificación de grado B. Durante el proceso se ejecutaron 9 checks pasivos, resultando en 6 verificaciones exitosas, 2 advertencias y 1 fallo crítico en la configuración de archivos de acceso. Aunque el cifrado de datos y la gestión de cookies son correctos, la ausencia de cabeceras de seguridad fundamentales eleva el riesgo de ataques de inyección. En su estado actual, el sitio se considera mayoritariamente seguro pero vulnerable a vectores de ataque específicos que podrían mitigarse con ajustes en la configuración del servidor.

Resumen de Riesgos

0	3	0	3	39
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 52 dias
Cabeceras de Seguridad	55	AVISO	4/6 presentes. Faltan: Content-Security-Policy, ...
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	1 cookies, todas con flags correctos
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 52 dias

- INFO Certificado valido
El certificado SSL es valido y de confianza
- INFO Dias hasta expiracion
52 dias restantes (expira: 2026-11-23T01:23:25.000Z)
- INFO Fecha de emision
Emitido desde: 2026-08-25T01:23:26.000Z
- INFO Puerto 443
Conexion HTTPS establecida correctamente en puerto 443

Cabeceras de Seguridad — 55/100

Estado: AVISO

4/6 presentes. Faltan: Content-Security-Policy, Strict-Transport-Security

- BAJO Server header expuesto
Server: LiteSpeed — Revela tecnologia del servidor

- 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)
- INFO

X-Content-Type-Options
Presente: nosniiff
- INFO

Referrer-Policy
Presente: same-origin
- INFO

Permissions-Policy
Presente: camera=(), microphone=(), geolocation=(self)

Redireccion HTTPS — 70/100

Estado: AVISO

HTTP redirige a HTTPS pero falta HSTS

- INFO

HTTP !' HTTPS redireccion
HTTP 301 redirige a https://clientes.transportesdyh.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

1 cookies, todas con flags correctos

- INFO **Cookies detectadas**
1 cookie(s) encontrada(s)
- INFO **Cookie: PHPSESSID — HttpOnly**
HttpOnly activo — No accesible via JavaScript
- INFO **Cookie: PHPSESSID — Secure**
Flag Secure activo — Solo se envía por HTTPS
- INFO **Cookie: PHPSESSID — 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 — 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 — 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

[ALTA] Content-Security-Policy (CSP) faltante: La carencia de esta política permite la ejecución de scripts no autorizados, facilitando ataques de Cross-Site Scripting (XSS) y el secuestro de sesiones.

[ALTA] Strict-Transport-Security (HSTS) no configurado: Al no forzar conexiones HTTPS mediante esta cabecera, el sitio es susceptible a ataques de degradación de protocolo y robo de cookies de sesión.

[BAJA] Server header expuesto: El servidor revela el uso de la tecnología LiteSpeed, lo que proporciona a potenciales atacantes información valiosa para buscar exploits específicos de dicha plataforma.

[BAJA] robots.txt no encontrado: La inexistencia de este archivo impide regular el comportamiento de bots y rastreadores, pudiendo exponer directorios que no deberían ser indexados.

[BAJA] sitemap.xml no encontrado: La falta de un mapa del sitio dificulta la visibilidad de la estructura de rutas y la auditoría de activos web disponibles.