

Escanear Vulnerabilidades

Informe de Seguridad Web

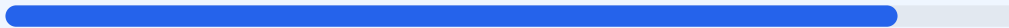
URL https://www.cleliaclevel.cl/
Dominio www.cleliaclevel.cl
Fecha 28 de abril de 2026 a las 16:12

Checks 9 pruebas
Hallazgos 43 totales
Problemas 4 detectados

B

88/100

puntos de seguridad



RESUMEN EJECUTIVO

El análisis de seguridad realizado sobre el sitio web ha arrojado una puntuación de 88/100, lo que equivale a una nota B. Se ejecutaron un total de 9 comprobaciones pasivas, resultando en 6 verificaciones exitosas, 3 advertencias y ningún fallo crítico detectado. Aunque los pilares fundamentales de cifrado están presentes y configurados, se identificaron carencias en las políticas de transporte estricto y la exposición de servicios en puertos no estándar. En conclusión, el sitio se considera mayoritariamente seguro, pero presenta vulnerabilidades de configuración que deben ser subsanadas para mitigar riesgos de interceptación de datos.

Resumen de Riesgos



Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 34 dias
Cabeceras de Seguridad	80	AVISO	5/6 presentes. Faltan: Strict-Transport-Security
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	100	OK	robots.txt y sitemap.xml presentes
Puertos Abiertos	60	AVISO	1 puerto(s) potencialmente riesgoso(s): 8080 (HT...

SSL/TLS — 100/100

Estado: OK

Certificado valido, expira en 34 dias

- INFO **Certificado valido**
El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
34 dias restantes (expira: 2026-06-01T14:36:43.000Z)
- INFO **Fecha de emision**
Emitido desde: 2026-03-03T13:38:06.000Z
- INFO **Puerto 443**
Conexion HTTPS establecida correctamente en puerto 443

Cabeceras de Seguridad — 80/100

Estado: AVISO

5/6 presentes. Faltan: Strict-Transport-Security

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

- INFO **Content-Security-Policy**
Presente: default-src 'none'; script-src 'nonce-GGFDHN6Sp9mZ21l6y3w6FG' 'unsafe-eval' http...
- 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: accelerometer=(),browsing-topics=(),camera=(),clipboard-read=(),clipboard-write=...

Redireccion HTTPS — 70/100

Estado: AVISO

HTTP redirige a HTTPS pero falta HSTS

- INFO **HTTP !' HTTPS redireccion**
HTTP 301 redirige a https://www.cleliaclavel.cl/
- ALTO **HSTS (Strict-Transport-Security)**
HSTS no configurado — El navegador no fuerza HTTPS
- INFO **Respuesta HTTPS**
HTTPS responde con status 403

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 — 100/100

Estado: OK

robots.txt y sitemap.xml presentes

- INFO **robots.txt**
Presente (177 bytes)
- INFO **Reglas robots.txt**
1 Disallow, 0 Allow
- INFO **Sitemap en robots.txt**
https://www.cleliaclavel.cl/sitemap_index.xml
- 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 autentificacion 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] Strict-Transport-Security (HSTS) faltante: No se envía la cabecera que fuerza al navegador a usar HTTPS, permitiendo ataques de degradación de protocolo.

[MEDIUM] Puerto 8080 (HTTP-Alt) abierto: La exposición de un puerto alternativo aumenta la superficie de ataque y puede revelar servicios administrativos o proxies vulnerables.

[LOW] Server header expuesto (cloudflare): El servidor revela información sobre la tecnología de infraestructura utilizada, lo que facilita el perfilado por parte de atacantes.

[INFO] Respuesta HTTPS 403: El servidor responde con un código de acceso denegado, lo cual puede indicar una configuración de seguridad excesivamente restrictiva o mal ajustada en el servidor web.