

Escanear Vulnerabilidades

Informe de Seguridad Web

URL https://sigo.minsal.cl
Dominio sigo.minsal.cl
Fecha 19 de mayo de 2026 a las 23:12

Checks 9 pruebas
Hallazgos 43 totales
Problemas 3 detectados

A

93/100

puntos de seguridad



RESUMEN EJECUTIVO

El análisis de seguridad realizado al sitio sigo.minsal.cl arroja una puntuación de 93/100 con una calificación de nota A. Se ejecutaron un total de 9 checks pasivos, de los cuales 7 resultaron satisfactorios, identificando una advertencia y un fallo técnico relacionado con archivos de configuración. El sitio presenta una infraestructura sólida en términos de cifrado y protección de datos, aunque se detectaron omisiones menores en cabeceras de seguridad y visibilidad para rastreadores. En conclusión, el sitio se considera seguro y cumple con la mayoría de los estándares internacionales de seguridad web, requiriendo únicamente ajustes preventivos.

Resumen de Riesgos



Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 157 dias
Cabeceras de Seguridad	85	AVISO	5/6 presentes. Faltan: Permissions-Policy
Redireccion HTTPS	100	OK	HTTP redirige a HTTPS y HSTS esta habilitado
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 157 dias

- INFO **Certificado valido**
El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
157 dias restantes (expira: 2026-10-23T23:59:59.000Z)
- INFO **Fecha de emision**
Emitido desde: 2026-04-09T00:00:00.000Z
- INFO **Puerto 443**
Conexion HTTPS establecida correctamente en puerto 443

Cabeceras de Seguridad — 85/100

Estado: AVISO

5/6 presentes. Faltan: Permissions-Policy

- INFO **Content-Security-Policy**
Presente: default-src 'self' api-sigo.minsal.cl 'unsafe-inline'; script-src 'self' api-sig...

- INFO **X-Frame-Options**
Presente: DENY
- INFO **Strict-Transport-Security**
Presente: max-age=63072000; includeSubDomains; preload
- INFO **X-Content-Type-Options**
Presente: nosniff
- INFO **Referrer-Policy**
Presente: strict-origin-when-cross-origin
- MEDIO **Permissions-Policy**
Falta — Restringe APIs del navegador (camara, micro, etc.)

Redireccion HTTPS — 100/100

Estado: OK

HTTP redirige a HTTPS y HSTS esta habilitado

- INFO **HTTP !' HTTPS redireccion**
HTTP 301 redirige a https://sigo.minsal.cl/
- INFO **HSTS (Strict-Transport-Security)**
HSTS activo: max-age=63072000; includeSubDomains; preload
- BAJO **HSTS includeSubDomains**
HSTS cubre subdominios
- INFO **HSTS max-age**
max-age=63072000 (730 dias)
- 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 — 20/100

Estado: FALLO

Faltan robots.txt y sitemap.xml

- BAJO **robots.txt**
No encontrado (HTTP 403)
- BAJO **sitemap.xml**
No encontrado (HTTP 403)
- 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

[MEDIUM] Permissions-Policy: Falta esta cabecera de seguridad, lo que impide restringir el acceso del navegador a APIs sensibles como la cámara, el micrófono o la ubicación, aumentando el riesgo en caso de ataques de inyección de scripts.

[LOW] robots.txt: El archivo no fue encontrado o devuelve un error de acceso denegado (403), lo que dificulta la gestión del rastreo por parte de motores de búsqueda.

[LOW] sitemap.xml: El mapa del sitio no está disponible o es inaccesible, impidiendo una indexación estructurada y transparente de los recursos del portal.