EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://www.registrosocial.gob.cl/	Checks	9 pruebas
Dominio	www.registrosocial.gob.cl	Hallazgos	46 totales
Fecha	16 de abril de 2026 a las 22:31	Problemas	11 detectados

C

71/100

puntos de seguridad

RESUMEN EJECUTIVO

El análisis de seguridad realizado sobre el dominio registrosocial.gob.cl ha resultado en una puntuación de 71/100, lo que equivale a una calificación de grado C. Durante la auditoría se ejecutaron un total de 9 checks pasivos, de los cuales 6 resultaron satisfactorios, se emitió 1 advertencia y se detectaron 2 fallos críticos. Aunque la infraestructura base muestra configuraciones sólidas en cuanto a cifrado y gestión del CMS, la ausencia de políticas de seguridad modernas y la presencia de contenido mixto comprometen la integridad técnica. En su estado actual, el sitio se considera vulnerable a ataques de inyección y degradación de protocolos, requiriendo intervenciones correctivas inmediatas.

Resumen de Riesgos

0	3	7	1	35
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 80 dias
Cabeceras de Seguridad	15	FALLO	Solo 1/6 presentes. Faltan: Content-Security-Pol...
Redireccion HTTPS	70	AVISO	HTTP redirige a HTTPS pero falta HSTS
Deteccion CMS	100	OK	CMS detectado: WordPress
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	4 recursos HTTP en pagina HTTPS
Robots.txt y Sitemap	100	OK	robots.txt y sitemap.xml presentes
Puertos Abiertos	100	OK	No se detectaron puertos abiertos

SSL/TLS — 100/100

Estado: OK

Certificado valido, expira en 80 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
  80 dias restantes (expira: 2026-07-05T23:59:59.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2025-08-06T00:00:00.000Z
- 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: Apache — Revela tecnologia del servidor

- ALTO **Content-Security-Policy**
  Falta — Previene XSS y ataques de inyeccion de contenido
- INFO **X-Frame-Options**
  Presente: SAMEORIGIN, 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 — 70/100

Estado: AVISO

HTTP redirige a HTTPS pero falta HSTS

- INFO **HTTP !' HTTPS redireccion**
  HTTP 302 redirige a https://www.registrosocial.gob.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

CMS detectado: WordPress

- INFO **WordPress**
  Detectado via HTML body
- 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 — 20/100

Estado: FALLO

4 recursos HTTP en pagina HTTPS

- MEDIO **Recurso HTTP (href (link/stylesheet))**
  http://www.desarrollosocialyfamilia.gob.cl/
- MEDIO **Recurso HTTP (href (link/stylesheet))**
  http://www.chileatiende.cl/
- MEDIO **Recurso HTTP (href (link/stylesheet))**
  http://rshmunicipal.ministeriodesarrollosocial.gob.cl/
- MEDIO **href (link/stylesheet)**
  ...y 1 mas del mismo tipo

Robots.txt y Sitemap — 100/100

Estado: OK

robots.txt y sitemap.xml presentes

- INFO **robots.txt**
  Presente (125 bytes)
- INFO **Reglas robots.txt**
  1 Disallow, 1 Allow
- INFO **Sitemap en robots.txt**
  https://www.registrosocial.gob.cl/sitemap.xml
- 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 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

[HIGH] Content-Security-Policy: La ausencia de esta cabecera facilita ataques de Cross-Site Scripting (XSS) y la inyección de contenido malicioso por parte de terceros.
[HIGH] Strict-Transport-Security: No se ha configurado la cabecera HSTS, lo que permite que un atacante pueda forzar la degradación de la conexión de HTTPS a HTTP.
[MEDIUM] Contenido Mixto: Se identificaron 4 recursos (stylesheets y links) cargados a través de HTTP, lo que rompe la cadena de confianza y seguridad del cifrado SSL.
[MEDIUM] X-Content-Type-Options: La falta de esta cabecera permite el MIME-type sniffing, aumentando el riesgo de que archivos cargados sean interpretados como scripts ejecutables.
[MEDIUM] Referrer-Policy: No existe una política definida, lo que puede provocar la fuga involuntaria de información de navegación hacia otros dominios.
[MEDIUM] Permissions-Policy: No se restringe el acceso a APIs sensibles del navegador como la cámara o el micrófono, dejando la seguridad del cliente en manos de la configuración local.
[LOW] Server header expuesto: El servidor responde con la firma Server: Apache, revelando la tecnología subyacente y facilitando la búsqueda de vulnerabilidades específicas de versión.