EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://salud.municipalidadrengo.cl/	Checks	9 pruebas
Dominio	salud.municipalidadrengo.cl	Hallazgos	50 totales
Fecha	20 de agosto de 2026 a las 19:06	Problemas	17 detectados

C

60/100

puntos de seguridad

RESUMEN EJECUTIVO

El análisis de seguridad realizado a salud.municipalidadrengo.cl arroja una puntuación exacta de 60/100, lo que equivale a una nota C. Durante la evaluación se ejecutaron 9 checks pasivos, de los cuales 5 resultaron correctos, se emitió 1 advertencia y se identificaron 3 fallos críticos. Se han detectado debilidades importantes en la configuración de cabeceras de seguridad y exposición de versiones desactualizadas del gestor de contenidos. En su estado actual, se concluye que el sitio es vulnerable ante ataques de inyección y suplantación. Resulta prioritario aplicar las correcciones técnicas detalladas para elevar el nivel de protección de la plataforma.

Resumen de Riesgos

0	5	9	3	33
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 33 dias
Cabeceras de Seguridad	0	FALLO	Solo 0/6 presentes. Faltan: Content-Security-Pol...
Redireccion HTTPS	70	AVISO	HTTP redirige a HTTPS pero falta HSTS
Deteccion CMS	100	OK	CMS detectado: WordPress, PrestaShop
Version CMS Expuesta	20	FALLO	WordPress 6.0.14 expuesta, WordPress 2 expuesta
Seguridad de Cookies	100	OK	No se encontraron cookies
Contenido Mixto	20	FALLO	30 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 33 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
  33 dias restantes (expira: 2026-09-22T21:32:57.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2026-06-24T21:32:58.000Z
- INFO **Puerto 443**
  Conexion HTTPS establecida correctamente en puerto 443

Cabeceras de Seguridad — 0/100

Estado: FALLO

Solo 0/6 presentes. Faltan: Content-Security-Policy, X-Frame-Options, 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
- ALTO **X-Frame-Options**
  Falta — Protege contra clickjacking
- 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 301 redirige a https://salud.municipalidadrengo.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, PrestaShop

- INFO **WordPress**
  Detectado via HTML body
- INFO **Joomla**
  No detectado
- INFO **Drupal**
  No detectado
- INFO **Magento**
  No detectado
- INFO **Shopify**
  No detectado
- INFO **PrestaShop**
  Detectado via HTML body
- INFO **Wix**
  No detectado
- INFO **Squarespace**
  No detectado
- BAJO **Meta generator**
  Expone: WordPress 6.0.14
- INFO **Tecnologias detectadas**
  Next.js

Version CMS Expuesta — 20/100

Estado: FALLO

WordPress 6.0.14 expuesta, WordPress 2 expuesta

- ALTO **WordPress version**
  Version 6.0.14 expuesta publicamente — Permite a atacantes buscar CVEs conocidos
- MEDIO **Archivo /readme.html**
  Archivo accesible publicamente — Puede revelar version e informacion del CMS
- INFO **Archivo /README.txt**
  No accesible (correcto)

- MEDIO **Ruta /wp-login.php**
  Panel de login accesible publicamente

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

30 recursos HTTP en pagina HTTPS

- MEDIO **Recurso HTTP (href (link/stylesheet))**
  http://gmpg.org/xfn/11
- MEDIO **Recurso HTTP (href (link/stylesheet))**
  http://salud.municipalidadrengo.cl/wp/
- MEDIO **Recurso HTTP (href (link/stylesheet))**
  http://browsehappy.com/
- MEDIO **href (link/stylesheet)**
  ...y 27 mas del mismo tipo

Robots.txt y Sitemap — 100/100

Estado: OK

robots.txt y sitemap.xml presentes

- INFO **robots.txt**
  Presente (128 bytes)
- INFO **Reglas robots.txt**
  1 Disallow, 1 Allow
- BAJO **Ruta sensible en robots.txt**
  Referencia a "admin" — Puede revelar rutas sensibles a atacantes
- INFO **Sitemap en robots.txt**
  https://salud.municipalidadrengo.cl/wp-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: Falta esta cabecera, lo que permite ataques de Cross-Site Scripting (XSS) e inyección de contenido malicioso.
[HIGH] X-Frame-Options: La ausencia de esta cabecera deja el sitio desprotegido frente a ataques de clickjacking que pueden engañar al usuario.
[HIGH] Strict-Transport-Security: No se fuerza el uso de conexiones seguras mediante HSTS, permitiendo posibles degradaciones de protocolo.
[HIGH] WordPress version: Se expone públicamente el uso de WordPress 6.0.14, lo que facilita a atacantes la búsqueda de exploits específicos para esta versión.
[MEDIUM] Contenido Mixto: Se detectaron 30 recursos cargados mediante HTTP en una página HTTPS, comprometiendo la integridad de la cifrado.
[MEDIUM] X-Content-Type-Options: La falta de esta cabecera permite el sniffing de tipos MIME por parte del navegador, aumentando el riesgo de ejecución de archivos maliciosos.
[MEDIUM] Referrer-Policy: No existe control sobre la información de referencia enviada a otros sitios, lo que podría filtrar rutas internas.
[MEDIUM] Permissions-Policy: No se restringen las APIs del navegador, permitiendo potencialmente el acceso no autorizado a funciones como cámara o micrófono.
[MEDIUM] Archivo /readme.html: Este archivo es accesible públicamente y revela información técnica sensible sobre el CMS instalado.
[MEDIUM] Ruta /wp-login.php: El panel de acceso administrativo es visible para cualquier usuario de internet, facilitando ataques de fuerza bruta.
[LOW] Server header expuesto: El servidor revela el uso de Apache, entregando información útil para perfilar el entorno tecnológico.
[LOW] Meta generator: La etiqueta meta expone explícitamente la versión WordPress 6.0.14 en el código fuente.
[LOW] Ruta sensible en robots.txt: Se hace referencia directa a directorios de administración, guiando a posibles atacantes hacia zonas sensibles.