# EscanearVulnerabilidades

Informe de Seguridad Web

| | | | |
|---|---|---|---|
| URL | https://signup.factoringsecurity.cl | Checks | 9 pruebas |
| Dominio | signup.factoringsecurity.cl | Hallazgos | 43 totales |
| Fecha | 24 de julio de 2026 a las 16:43 | Problemas | 9 detectados |

**B**

77/100

puntos de seguridad

## RESUMEN EJECUTIVO

El análisis de seguridad realizado al sitio signup.factoringsecurity.cl arroja una puntuación de 77/100, lo que representa una calificación de nota B. Durante el proceso se ejecutaron 9 checks pasivos, de los cuales 6 resultaron satisfactorios, 1 presentó advertencias y 2 finalizaron con fallos críticos. Aunque la infraestructura base cuenta con un certificado SSL válido, existen deficiencias importantes en las cabeceras de protección y en la exposición de rutas administrativas. En su estado actual, el sitio se considera vulnerable a ataques de intermediario y de inyección debido a configuraciones de servidor incompletas.

## Resumen de Riesgos

| 0 | 3 | 3 | 3 | 34 |
|---|---|---|---|---|
| CRITICO | ALTO | MEDIO | BAJO | INFO |

## Resumen de Checks

| | | | |
|---|---|---|---|
| SSL/TLS | 100 | OK | Certificado valido, expira en 45 dias |
| Cabeceras de Seguridad | 25 | FALLO | Solo 2/6 presentes. Faltan: Content-Security-Pol... |
| 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 | 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 45 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
  45 dias restantes (expira: 2026-09-07T22:16:01.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2025-08-06T22:16:02.000Z
- INFO **Puerto 443**
  Conexion HTTPS establecida correctamente en puerto 443

## Cabeceras de Seguridad — 25/100

Estado: FALLO

Solo 2/6 presentes. Faltan: Content-Security-Policy, Strict-Transport-Security, X-Content-Type-Options, Permissions-Policy

- BAJO **Server header expuesto**
  Server: cloudflare — 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)
- MEDIO **X-Content-Type-Options**
  Falta — Evita MIME-type sniffing
- INFO **Referrer-Policy**
  Presente: same-origin
- 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://signup.factoringsecurity.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)
- MEDIO **Ruta /wp-login.php**
  Panel de login accesible publicamente
- 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 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 — 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 Inteligencia Artificial

---RESUMEN EJECUTIVO---
El análisis de seguridad realizado al sitio signup.factoringsecurity.cl arroja una puntuación de 77/100, lo que representa una calificación de nota B. Durante el proceso se ejecutaron 9 checks pasivos, de los cuales 6 resultaron satisfactorios, 1 presentó advertencias y 2 finalizaron con fallos críticos. Aunque la infraestructura base cuenta con un certificado SSL válido, existen deficiencias importantes en las cabeceras de protección y en la exposición de rutas administrativas. En su estado actual, el sitio se considera vulnerable a ataques de intermediario y de inyección debido a configuraciones de servidor incompletas.

---VULNERABILITIES---
[HIGH] Content-Security-Policy: Falta esta cabecera esencial para prevenir ataques XSS y la inyección de contenido malicioso.
[HIGH] Strict-Transport-Security: La ausencia de HSTS permite que los atacantes intenten degradar la conexión a protocolos no cifrados.
[HIGH] HSTS no configurado: El navegador no está forzado a utilizar siempre conexiones HTTPS, debilitando la privacidad.
[MEDIUM] X-Content-Type-Options: La falta de esta cabecera permite el MIME-type sniffing, lo que puede llevar a la ejecución de scripts no deseados.
[MEDIUM] Permissions-Policy: No existen restricciones sobre el uso de APIs del navegador como la cámara o el micrófono.

[MEDIUM] Ruta /wp-login.php: El panel de acceso administrativo se encuentra disponible públicamente, facilitando intentos de fuerza bruta.
[LOW] Server header expuesto: El servidor revela el uso de Cloudflare, proporcionando información técnica a posibles atacantes.
[LOW] robots.txt: El archivo no fue encontrado, lo que dificulta el control sobre el rastreo de motores de búsqueda.
[LOW] sitemap.xml: La ausencia de este archivo afecta la indexación y visibilidad controlada del contenido del sitio.