EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://sgoe.ine.gob.cl/	Checks	9 pruebas
Dominio	sgoe.ine.gob.cl	Hallazgos	47 totales
Fecha	15 de mayo de 2026 a las 13:41	Problemas	10 detectados

C

71/100

puntos de seguridad

RESUMEN EJECUTIVO

El análisis de ciberseguridad realizado al sitio sgoe.ine.gob.cl presenta una puntuación de 71/100, lo que otorga una nota de calificación C. Durante la evaluación se ejecutaron 9 checks pasivos, resultando en 5 verificaciones correctas, 2 advertencias por configuraciones incompletas y 2 fallos críticos en políticas de seguridad. Si bien el cifrado de datos mediante SSL es óptimo, la ausencia de cabeceras de protección esenciales deja la plataforma expuesta a diversas técnicas de ataque. Se concluye que el sitio es vulnerable a nivel de configuración de servidor y gestión de sesiones, requiriendo intervenciones técnicas para alcanzar un estándar de seguridad robusto.

Resumen de Riesgos

0	4	4	2	37
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 152 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	No se detecto un CMS conocido
Version CMS Expuesta	100	OK	No se detecto version de CMS expuesta
Seguridad de Cookies	67	AVISO	ASP.NET_SessionId: falta Secure; BIGipServerpool...
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 152 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
  152 dias restantes (expira: 2026-10-14T23:59:59.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2026-03-30T00:00:00.000Z
- 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

- 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
- 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://sgoe.ine.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

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 — 67/100

Estado: AVISO

ASP.NET_SessionId: falta Secure; BIGipServerpool_sgoe: falta SameSite

- INFO **Cookies detectadas**
  2 cookie(s) encontrada(s)

- INFO **Cookie: ASP.NET_SessionId — HttpOnly**
  HttpOnly activo — No accesible via JavaScript
- ALTO **Cookie: ASP.NET_SessionId — Secure**
  Falta flag Secure — Cookie se envia en conexiones HTTP
- INFO **Cookie: ASP.NET_SessionId — SameSite**
  SameSite=lax
- INFO **Cookie: BIGipServerpool_sgoe — HttpOnly**
  HttpOnly activo — No accesible via JavaScript
- INFO **Cookie: BIGipServerpool_sgoe — Secure**
  Flag Secure activo — Solo se envia por HTTPS
- MEDIO **Cookie: BIGipServerpool_sgoe — SameSite**
  Falta SameSite — Vulnerable a CSRF

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 Seguridad

VULNERABILIDADES DETECTADAS

[HIGH] Content-Security-Policy: La ausencia de esta cabecera permite la ejecución de scripts no autorizados, facilitando ataques de XSS e inyección de contenido malicioso.
[HIGH] Strict-Transport-Security: No se fuerza el uso de HTTPS mediante HSTS, permitiendo que un atacante intercepte la comunicación degradándola a una conexión no cifrada.
[HIGH] Cookie ASP.NET_SessionId sin flag Secure: El identificador de sesión puede ser enviado a través de canales HTTP inseguros, lo que facilita el robo de la sesión del usuario.
[MEDIUM] X-Content-Type-Options: Al no estar configurada, el navegador queda vulnerable a ataques de "MIME-type sniffing", pudiendo ejecutar archivos maliciosos disfrazados de otros tipos.
[MEDIUM] Referrer-Policy: No se controla qué información de origen se envía a otros sitios, lo que podría filtrar rutas internas o datos sensibles en la URL.
[MEDIUM] Permissions-Policy: El sitio no restringe el acceso a APIs del navegador como la cámara o el micrófono, aumentando el riesgo de abuso de funcionalidades del cliente.
[MEDIUM] Cookie BIGipServerpool_sgoe sin SameSite: La falta de este atributo hace que la cookie sea susceptible a ataques de falsificación de petición en sitios cruzados (CSRF).
[LOW] robots.txt no encontrado: La falta de este archivo impide dar instrucciones a los buscadores sobre qué áreas del servidor deben permanecer privadas.
[LOW] sitemap.xml no encontrado: La ausencia de un mapa del sitio dificulta la auditoría de rutas legítimas y la correcta indexación de la arquitectura web.