EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://sai-ine-archivo.ine.mx/	Checks	9 pruebas
Dominio	sai-ine-archivo.ine.mx	Hallazgos	47 totales
Fecha	2 de mayo de 2026 a las 07:25	Problemas	8 detectados

C

72/100

puntos de seguridad

RESUMEN EJECUTIVO

El análisis técnico de seguridad realizado al portal ha resultado en una puntuación de 72/100, lo que otorga una calificación de nota C. Durante la evaluación se ejecutaron 9 checks pasivos, de los cuales 4 resultaron satisfactorios, 4 generaron advertencias y 1 fue identificado como fallo crítico. La infraestructura presenta una base sólida en cuanto a la validez de su certificado SSL, pero carece de configuraciones esenciales en la gestión de tráfico cifrado y cabeceras de seguridad. Debido a la falta de redirección automática a HTTPS y la ausencia de políticas de transporte estricto, el sitio se considera vulnerable a ataques de interceptación de datos. Es imperativo corregir las deficiencias en la configuración del servidor para alcanzar un nivel de seguridad óptimo.

Resumen de Riesgos

0	3	3	2	39
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 197 dias
Cabeceras de Seguridad	80	AVISO	5/6 presentes. Faltan: Strict-Transport-Security
Redireccion HTTPS	0	FALLO	No hay redireccion HTTP a HTTPS
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	__cf_bm: falta SameSite
Contenido Mixto	100	OK	No se detecto contenido mixto
Robots.txt y Sitemap	60	AVISO	Falta sitemap.xml
Puertos Abiertos	60	AVISO	1 puerto(s) potencialmente riesgoso(s): 8080 (HT...

SSL/TLS — 100/100

Estado: OK

Certificado valido, expira en 197 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
  197 dias restantes (expira: 2026-11-14T23:59:59.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2025-12-23T00:00:00.000Z
- INFO **Puerto 443**
  Conexion HTTPS establecida correctamente en puerto 443

Cabeceras de Seguridad — 80/100

Estado: AVISO

5/6 presentes. Faltan: Strict-Transport-Security

- BAJO **Server header expuesto**
  Server: cloudflare — Revela tecnologia del servidor

- INFO **Content-Security-Policy**
  Presente: default-src 'none'; script-src 'nonce-nMeqnog0l5xzrK08p69bGj' 'unsafe-eval' http...
- INFO **X-Frame-Options**
  Presente: SAMEORIGIN
- ALTO **Strict-Transport-Security**
  Falta — Fuerza conexiones HTTPS (HSTS)
- INFO **X-Content-Type-Options**
  Presente: nosniff
- INFO **Referrer-Policy**
  Presente: same-origin
- INFO **Permissions-Policy**
  Presente: accelerometer=(),browsing-topics=(),camera=(),clipboard-read=(),clipboard-write=...

Redireccion HTTPS — 0/100

Estado: FALLO

No hay redireccion HTTP a HTTPS

- ALTO **HTTP !' HTTPS redireccion**
  HTTP 403 — No redirige a HTTPS
- 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)
- INFO **Version CMS**
  No se detecta ninguna version expuesta

Seguridad de Cookies — 67/100

Estado: AVISO

__cf_bm: falta SameSite

- INFO **Cookies detectadas**
  1 cookie(s) encontrada(s)
- INFO **Cookie: __cf_bm — HttpOnly**
  HttpOnly activo — No accesible via JavaScript
- INFO **Cookie: __cf_bm — Secure**
  Flag Secure activo — Solo se envia por HTTPS
- MEDIO **Cookie: __cf_bm — 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 — 60/100

Estado: AVISO

Falta sitemap.xml

- INFO **robots.txt**
  Presente (1738 bytes)
- INFO **Reglas robots.txt**
  9 Disallow, 1 Allow
- MEDIO **Bloqueo total**
  robots.txt bloquea todo el sitio con Disallow: /
- BAJO **sitemap.xml**
  No encontrado (HTTP 403)
- BAJO **security.txt**
  No encontrado — Recomendado para politica de divulgacion

Puertos Abiertos — 60/100

Estado: AVISO

1 puerto(s) potencialmente riesgoso(s): 8080 (HTTP-Alt)

- 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)**
  Abierto (esperado) — Servidor web
- INFO **Puerto 443 (HTTPS)**
  Abierto (esperado) — 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
- MEDIO **Puerto 8080 (HTTP-Alt)**
  ABIERTO — Servidor web alternativo / proxy
- INFO **Puerto 27017 (MongoDB)**
  Cerrado — Base de datos MongoDB expuesta

Analisis de Seguridad

VULNERABILIDADES DETECTADAS

[HIGH] Falta de redirección HTTP a HTTPS: El sitio no redirige automáticamente el tráfico inseguro al protocolo cifrado, respondiendo con un error 403, lo que expone a los usuarios a conexiones no protegidas.
[HIGH] Strict-Transport-Security (HSTS) ausente: Al no existir esta cabecera, el navegador no fuerza la conexión segura, permitiendo ataques de degradación de SSL (SSL Stripping).
[MEDIUM] Cookie __cf_bm sin atributo SameSite: La cookie de Cloudflare carece de la directiva SameSite, lo que podría facilitar ataques de falsificación de petición en sitios cruzados (CSRF).
[MEDIUM] Puerto 8080 (HTTP-Alt) abierto: La exposición de este puerto alternativo aumenta la superficie de ataque al dejar disponible un servicio web o proxy potencialmente vulnerable.
[MEDIUM] Bloqueo total en robots.txt: El archivo de configuración bloquea el acceso a todo el sitio (Disallow: /), lo que puede ser un error de configuración o una medida de ocultamiento ineficiente.
[LOW] Cabecera Server expuesta: Se revela el uso de Cloudflare como tecnología de servidor, facilitando a un atacante el reconocimiento de la infraestructura empleada.
[LOW] sitemap.xml no encontrado: El servidor devuelve un error 403 al intentar acceder al mapa del sitio, dificultando la visibilidad controlada del contenido indexado.