# EscanearVulnerabilidades

Informe de Seguridad Web

| | | | |
|---|---|---|---|
| URL | https://www.itson.mx | Checks | 9 pruebas |
| Dominio | www.itson.mx | Hallazgos | 39 totales |
| Fecha | 5 de mayo de 2026 a las 16:31 | Problemas | 9 detectados |

C

72/100

puntos de seguridad

**RESUMEN EJECUTIVO**

La evaluación de seguridad realizada al sitio web arroja una puntuación de 72/100, lo que corresponde a una calificación de grado C. El análisis se basó en 9 checks pasivos, de los cuales 6 resultaron satisfactorios y 2 presentaron fallos críticos relacionados con la configuración de seguridad del servidor. Aunque el cifrado de datos mediante SSL es correcto, se detectó una ausencia total de cabeceras de protección y fallos en la redirección segura. Debido a la falta de políticas de seguridad activas, el sitio se clasifica actualmente como vulnerable ante ataques de inyección y suplantación. Es fundamental implementar las medidas correctivas para elevar el nivel de protección de la plataforma.

## Resumen de Riesgos

| 0 | 3 | 3 | 3 | 30 |
|---|---|---|---|---|
| CRITICO | ALTO | MEDIO | BAJO | INFO |

## Resumen de Checks

| | | | |
|---|---|---|---|
| SSL/TLS | 100 | OK | Certificado valido, expira en 50 dias |
| Cabeceras de Seguridad | 0 | FALLO | Solo 0/6 presentes. Faltan: Content-Security-Pol... |
| Redireccion HTTPS | 0 | ERROR | No se pudo verificar la redireccion 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 | 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 50 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
  50 dias restantes (expira: 2026-06-24T23:59:59.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2025-06-24T00:00:00.000Z
- 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.)

## 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 — 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 Seguridad

**VULNERABILIDADES DETECTADAS**

[HIGH] Content-Security-Policy: La ausencia de esta cabecera permite ataques de inyección de contenido y Cross-Site Scripting (XSS) al no restringir las fuentes de scripts permitidas.
[HIGH] X-Frame-Options: Al no estar presente, el sitio es vulnerable a ataques de clickjacking, permitiendo que atacantes carguen la página en marcos invisibles para engañar a los usuarios.
[HIGH] Strict-Transport-Security: No se fuerza el uso de conexiones seguras, lo que facilita ataques de intermediario (Man-in-the-Middle) mediante la degradación del cifrado.
[MEDIUM] X-Content-Type-Options: La falta de esta directiva permite el sniffing de tipos MIME, lo que podría llevar a la ejecución de archivos maliciosos disfrazados de contenido legítimo.
[MEDIUM] Referrer-Policy: No se controla la información de procedencia enviada en las peticiones, lo que puede exponer rutas internas o datos sensibles a dominios externos.
[MEDIUM] Permissions-Policy: No se restringen las APIs del navegador como la cámara o el micrófono, incrementando el riesgo de acceso no autorizado a funciones del hardware del cliente.
[LOW] Server header expuesto: La cabecera revela el uso de Apache, proporcionando a potenciales atacantes información específica sobre la tecnología del servidor para buscar exploits conocidos.
[LOW] robots.txt y sitemap.xml: La inexistencia de estos archivos indica una falta de configuración en la estructura pública y dificulta la auditoría técnica de los recursos del sitio.