

Escanear Vulnerabilidades

Informe de Seguridad Web

URL https://fiks.com.mx
Dominio fiks.com.mx
Fecha 4 de mayo de 2026 a las 16:57

Checks 9 pruebas
Hallazgos 45 totales
Problemas 6 detectados

B

84/100

puntos de seguridad

RESUMEN EJECUTIVO

La auditoría de seguridad realizada al dominio fiks.com.mx arroja una puntuación de 84/100, lo que equivale a una nota B. Se ejecutaron 9 checks pasivos, resultando 8 de ellos satisfactorios y 1 con fallos significativos relacionados con la configuración de red. El sitio presenta una base sólida en cuanto a cifrado SSL y gestión de redirecciones, pero falla en la implementación de medidas de defensa proactivas en el navegador. Debido a la carencia de cabeceras de seguridad fundamentales, se concluye que el sitio es parcialmente vulnerable a ataques de inyección y suplantación.

Resumen de Riesgos



Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 67 dias
Cabeceras de Seguridad	20	FALLO	Solo 1/6 presentes. Faltan: Content-Security-Pol...
Redireccion HTTPS	100	OK	HTTP redirige a HTTPS y HSTS esta habilitado
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	100	OK	robots.txt y sitemap.xml presentes
Puertos Abiertos	100	OK	2 puerto(s) abierto(s), todos esperados

SSL/TLS — 100/100

Estado: OK

Certificado valido, expira en 67 dias

- INFO **Certificado valido**
El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
67 dias restantes (expira: 2026-07-11T01:34:57.000Z)
- INFO **Fecha de emision**
Emitido desde: 2026-04-12T01:34:58.000Z
- INFO **Puerto 443**
Conexion HTTPS establecida correctamente en puerto 443

Cabeceras de Seguridad — 20/100

Estado: FALLO

Solo 1/6 presentes. Faltan: Content-Security-Policy, X-Frame-Options, X-Content-Type-Options, Referrer-Policy, Permissions-Policy

- BAJO **Server header expuesto**
Server: Netlify — 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
- **INFO** **Strict-Transport-Security**
Presente: max-age=31536000
- **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 — 100/100

Estado: OK

HTTP redirige a HTTPS y HSTS esta habilitado

- **INFO** **HTTP !' HTTPS redireccion**
HTTP 301 redirige a https://fiks.com.mx/
- **INFO** **HSTS (Strict-Transport-Security)**
HSTS activo: max-age=31536000
- **BAJO** **HSTS includeSubDomains**
HSTS no cubre subdominios
- **INFO** **HSTS max-age**
max-age=31536000 (365 dias)
- **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 — 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 — 100/100

Estado: OK

robots.txt y sitemap.xml presentes

- INFO **robots.txt**
Presente (72 bytes)
- INFO **Reglas robots.txt**
0 Disallow, 1 Allow
- INFO **Sitemap en robots.txt**
<https://graffikstattoo.com/sitemap.xml>
- BAJO **security.txt**
No encontrado — Recomendado para politica de divulgacion

Puertos Abiertos — 100/100

Estado: OK

2 puerto(s) abierto(s), todos esperados

- 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
- 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 maliciosos y ataques de Cross-Site Scripting (XSS).

[HIGH] X-Frame-Options: Al no estar presente, el sitio es susceptible a ataques de clickjacking donde un tercero puede secuestrar la interfaz de usuario.

[MEDIUM] X-Content-Type-Options: La falta de esta instrucción permite que el navegador realice sniffing de tipos MIME, facilitando la ejecución de archivos con contenido malicioso disfrazado.

[MEDIUM] Referrer-Policy: No se controla qué información de procedencia se envía a otros sitios, lo que puede comprometer la privacidad de la navegación.

[MEDIUM] Permissions-Policy: No existen restricciones sobre el acceso a funciones sensibles del dispositivo del usuario desde el navegador.

[LOW] Server header expuesto: El encabezado Server revela el uso de Netlify, información técnica que ayuda a potenciales atacantes a perfilar la infraestructura.