EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://cipi.fgr.org.mx	Checks	9 pruebas
Dominio	cipi.fgr.org.mx	Hallazgos	15 totales
Fecha	17 de julio de 2026 a las 16:48	Problemas	3 detectados

C

73/100

puntos de seguridad

RESUMEN EJECUTIVO

La auditoría de seguridad realizada al dominio cipi.fgr.org.mx arrojó una puntuación de 73/100, lo que equivale a una nota de calificación C. Durante el proceso se ejecutaron 9 checks pasivos, resultando en 1 validación exitosa, 0 advertencias y 1 fallo crítico relacionado con la visibilidad de archivos de configuración. El análisis técnico se vio severamente limitado por la imposibilidad de establecer una conexión SSL/TLS estable, lo que impidió verificar las cabeceras de seguridad y la protección de cookies. Debido a la ausencia de cifrado funcional y la falta de configuraciones básicas de servidor, se concluye que el sitio es actualmente vulnerable y no garantiza la confidencialidad de los datos.

Resumen de Riesgos

1	0	0	2	12
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	0	ERROR	No se pudo verificar SSL/TLS
Cabeceras de Seguridad	0	ERROR	No se pudieron verificar las cabeceras
Redireccion HTTPS	0	ERROR	No se pudo verificar la redireccion HTTPS
Deteccion CMS	0	ERROR	No se pudo analizar el CMS
Version CMS Expuesta	0	ERROR	No se pudo verificar la version del CMS
Seguridad de Cookies	0	ERROR	No se pudieron verificar las cookies
Contenido Mixto	0	ERROR	No se pudo verificar 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 — 0/100

Estado: ERROR

No se pudo verificar SSL/TLS

- CRITICO **Conexion SSL**
  No se pudo establecer conexion SSL/TLS

Robots.txt y Sitemap — 20/100

Estado: FALLO

Faltan robots.txt y sitemap.xml

- BAJO **robots.txt**
  Error al acceder
- BAJO **sitemap.xml**
  Error al acceder

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

[CRITICAL] Conexión SSL: No se pudo establecer una conexión SSL/TLS, lo cual es peligroso porque toda la información viaja en texto plano y puede ser interceptada por terceros.
[HIGH] Cabeceras de Seguridad: No se detectaron encabezados de protección, lo que expone al sitio a ataques de inyección, XSS y Clickjacking.
[HIGH] Redirección HTTPS: La ausencia de una redirección forzada hacia un protocolo seguro facilita ataques de degradación de conexión.
[MEDIUM] Seguridad de Cookies: No se pudo validar el atributo Secure y HttpOnly, aumentando el riesgo de robo de sesiones mediante scripts maliciosos.
[LOW] Archivo robots.txt: Error al acceder al archivo, lo que impide gestionar correctamente qué áreas del sitio deben ser indexadas por buscadores.
[LOW] Archivo sitemap.xml: Error al acceder al mapa del sitio, lo que dificulta el control sobre la estructura pública de directorios expuestos.