EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://expedientes.igssgt.org	Checks	9 pruebas
Dominio	expedientes.igssgt.org	Hallazgos	40 totales
Fecha	4 de junio de 2026 a las 20:52	Problemas	12 detectados

C

72/100

puntos de seguridad

RESUMEN EJECUTIVO

La auditoría de seguridad realizada sobre la plataforma arroja una puntuación de 72/100, lo que otorga una nota de C según los estándares de evaluación. Se ejecutaron un total de 9 checks pasivos, de los cuales 6 resultaron satisfactorios y 2 presentaron fallos críticos relacionados con la configuración del servidor y la protección de datos. Aunque la base del cifrado es sólida, la ausencia total de políticas de seguridad modernas en las cabeceras HTTP compromete la integridad del sitio. En su estado actual, el sitio se considera vulnerable a ataques de suplantación de identidad y ejecución de código malicioso.

Resumen de Riesgos

0	3	8	1	28
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 162 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 162 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
  162 dias restantes (expira: 2026-11-13T23:59:59.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2025-11-17T00:00:00.000Z
- 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: nginx/1.27.1 — 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

- MEDIO **Archivo /readme.html**
  Archivo accesible publicamente — Puede revelar version e informacion del CMS
- MEDIO **Archivo /README.txt**
  Archivo accesible publicamente — Puede revelar version e informacion del CMS
- MEDIO **Ruta /wp-login.php**
  Panel de login accesible publicamente
- MEDIO **Ruta /administrator/**
  Panel de login accesible publicamente
- MEDIO **Ruta /user/login**
  Panel de login accesible publicamente
- 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

- INFO **security.txt**
  Presente en /.well-known/security.txt — Buena practica

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 cross-site scripting (XSS) e inyección de contenido externo no autorizado.
[HIGH] X-Frame-Options: Al no estar presente, el sitio es susceptible a ataques de clickjacking donde un atacante puede cargar la web en un marco invisible para engañar al usuario.
[HIGH] Strict-Transport-Security: No se fuerza el uso de conexiones seguras, lo que facilita ataques de degradación de protocolo y la interceptación de datos en tránsito.
[MEDIUM] X-Content-Type-Options: La falta de esta instrucción permite que el navegador intente adivinar el tipo de contenido, abriendo la puerta a ataques de MIME-sniffing.
[MEDIUM] Referrer-Policy: No existe un control sobre la información de procedencia que se envía a otros sitios, lo que podría filtrar rutas internas privadas.
[MEDIUM] Permissions-Policy: No se restringe el acceso a funciones sensibles del navegador como la cámara, el micrófono o la geolocalización.
[MEDIUM] Exposición de archivos informativos y rutas: Los archivos /readme.html y /README.txt son accesibles, junto con rutas de login como /wp-login.php y /administrator/, revelando posibles vectores de ataque.
[LOW] Cabecera Server expuesta: El servidor informa explícitamente que utiliza nginx/1.27.1, facilitando a un atacante la búsqueda de vulnerabilidades específicas para esa versión.
[LOW] Ausencia de robots.txt y sitemap.xml: La falta de estos archivos dificulta la auditoría de indexación y el control de rastreo de los motores de búsqueda.