

Escanear Vulnerabilidades

Informe de Seguridad Web

URL https://system.unisupergt.com
Dominio system.unisupergt.com
Fecha 19 de mayo de 2026 a las 22:00

Checks 9 pruebas
Hallazgos 39 totales
Problemas 9 detectados

C

72/100

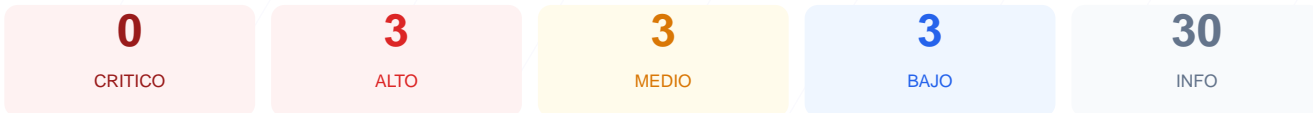
puntos de seguridad



RESUMEN EJECUTIVO

El análisis de seguridad técnica realizado al sitio web ha arrojado una puntuación de 72/100, lo que corresponde a una calificación de grado C. Durante la auditoría se ejecutaron 9 checks pasivos, obteniendo 6 resultados satisfactorios y 2 fallos críticos en la configuración de seguridad. Aunque el cifrado de datos es correcto, la ausencia total de cabeceras de protección en el servidor representa un riesgo significativo. Se concluye que el sitio es actualmente vulnerable a ataques dirigidos al navegador del usuario final y a técnicas de suplantación.

Resumen de Riesgos



Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 117 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	1 puerto(s) abierto(s), todos esperados

SSL/TLS — 100/100

Estado: OK

Certificado valido, expira en 117 dias

- INFO **Certificado valido**
El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
117 dias restantes (expira: 2026-09-13T11:30:50.000Z)
- INFO **Fecha de emision**
Emitido desde: 2025-08-12T11:30:50.000Z
- 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: Microsoft-IIS/10.0 — 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 política de divulgación

Puertos Abiertos — 100/100

Estado: OK

1 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 — Envío de correo
- **INFO Puerto 80 (HTTP)**
Cerrado — 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 autenticación 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 aumenta drásticamente el riesgo de ataques Cross-Site Scripting (XSS).

[HIGH] X-Frame-Options: El sitio carece de protección contra clickjacking, lo que permitiría a un atacante embeber la web en un marco invisible para engañar al usuario.

[HIGH] Strict-Transport-Security: No se fuerza el uso de conexiones seguras mediante HSTS, permitiendo posibles ataques de degradación de SSL/TLS.

[MEDIUM] X-Content-Type-Options: La falta de esta cabecera permite que el navegador intente adivinar el tipo de contenido, facilitando la ejecución de archivos maliciosos camuflados.

[MEDIUM] Referrer-Policy: No existe una política definida para el control de la información de procedencia enviada a otros dominios durante la navegación.

[MEDIUM] Permissions-Policy: El sitio no restringe el acceso de las APIs del navegador, como la cámara o el micrófono, a través de políticas de seguridad explícitas.

[LOW] Server header expuesto: El servidor responde con la cabecera Microsoft-IIS/10.0, revelando información técnica que facilita la búsqueda de exploits específicos para esa versión.

[LOW] Ausencia de robots.txt y sitemap.xml: No se encontraron estos archivos de control, lo que genera errores HTTP 404 y dificulta la indexación controlada por parte de buscadores.