

# Escanear Vulnerabilidades

Informe de Seguridad Web

URL https://cmsirrh.igssgt.org  
Dominio cmsirrh.igssgt.org  
Fecha 8 de mayo de 2026 a las 20:09

Checks 9 pruebas  
Hallazgos 31 totales  
Problemas 3 detectados

# C

## 65/100

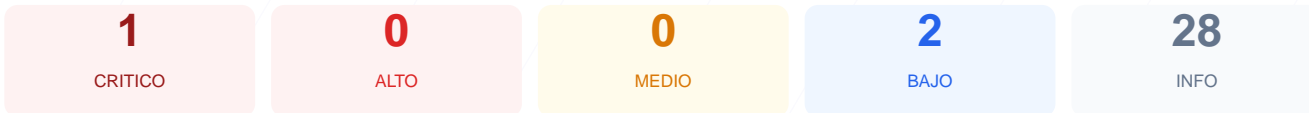
puntos de seguridad



### RESUMEN EJECUTIVO

El análisis de seguridad realizado al dominio arroja una puntuación de 65/100, lo que corresponde a una nota de C. Se ejecutaron 9 checks pasivos, de los cuales 4 resultaron exitosos, 0 generaron advertencias y 2 presentaron fallos críticos directos, sumado a varios errores de verificación. La ausencia de un certificado SSL válido es el hallazgo más preocupante, ya que impide establecer conexiones cifradas seguras. Debido a estas deficiencias técnicas en la infraestructura de transporte y seguridad, se concluye que el sitio es actualmente vulnerable y no es apto para el manejo de información sensible.

### Resumen de Riesgos



### Resumen de Checks

SSL/TLS	0	FALLO	Certificado SSL no valido
Cabeceras de Seguridad	0	ERROR	No se pudieron verificar las cabeceras
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	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: FALLO

Certificado SSL no valido

- CRITICO** Certificado valido  
El certificado SSL NO es valido
- INFO** Dias hasta expiracion  
189 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

### 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

## 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
- 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 autentificación 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] Certificado SSL no válido: El certificado SSL del sitio no es válido, lo que impide el cifrado de la comunicación y permite que terceros intercepten los datos transmitidos.
- [HIGH] Cabeceras de Seguridad ausentes o no verificables: No se detectaron cabeceras de protección, lo que deja al servidor expuesto a ataques de inyección, suplantación de identidad y clickjacking.
- [HIGH] Fallo en Redirección HTTPS: El sistema no pudo confirmar que el sitio fuerce automáticamente el uso de conexiones seguras, permitiendo accesos potenciales por canales no cifrados.
- [MEDIUM] Incapacidad de verificación de Contenido Mixto: No fue posible validar si existen elementos inseguros cargándose dentro de páginas seguras, lo que podría comprometer la integridad del sitio.
- [LOW] Ausencia de archivos robots.txt y sitemap.xml: No se encontraron estos archivos de control, lo que dificulta la indexación correcta y el control sobre qué partes del sitio deben ser rastreadas por buscadores.