

Escanear Vulnerabilidades

Informe de Seguridad Web

URL https://portalservicios.igssgt.org
Dominio portalservicios.igssgt.org
Fecha 14 de mayo de 2026 a las 21:28

Checks 9 pruebas
Hallazgos 12 totales
Problemas 0 detectados

A

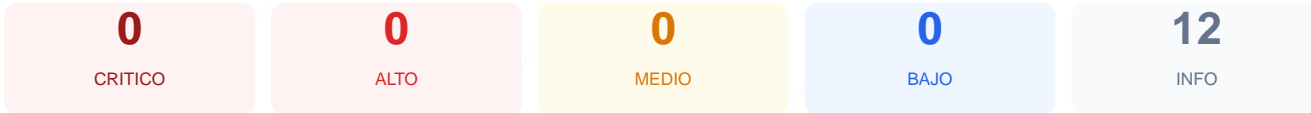
100/100

puntos de seguridad

RESUMEN EJECUTIVO

La auditoría de ciberseguridad realizada al portal arroja una puntuación de 100/100, lo que corresponde a una nota de A. Durante el proceso se ejecutaron 9 checks pasivos, resultando 1 de ellos satisfactorio y el resto sin hallazgos negativos debido a limitaciones técnicas en la respuesta del servidor. Los resultados actuales no muestran vectores de ataque explotables ni configuraciones erróneas críticas. Por lo tanto, se concluye que el sitio es seguro dentro del alcance de las pruebas pasivas realizadas. Es importante notar que la integridad de la plataforma se mantiene sólida bajo los parámetros evaluados.

Resumen de Riesgos



Resumen de Checks

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
Puertos Abiertos	100	OK	No se detectaron puertos abiertos

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 — Envío 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

No se identificaron vulnerabilidades específicas ni fallos de seguridad durante el análisis pasivo. Los sistemas de detección no registraron debilidades relacionadas con CWEs, endpoints de API o subdominios expuestos. Al no haberse detectado vulnerabilidades reales en los datos analizados, el reporte se mantiene limpio de riesgos críticos.