EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://intecssa.com/	Checks	9 pruebas
Dominio	intecssa.com	Hallazgos	12 totales
Fecha	5 de mayo de 2026 a las 20:33	Problemas	0 detectados

A

100/100

puntos de seguridad

RESUMEN EJECUTIVO

La auditoría de seguridad realizada al sitio web muestra un desempeño excepcional, alcanzando una puntuación de 100/100 y una nota A. Durante el proceso se ejecutaron 9 checks pasivos, de los cuales uno fue validado satisfactoriamente mientras que los restantes no reportaron fallos ni advertencias de seguridad. Al no encontrarse brechas ni configuraciones de riesgo en los puntos analizados, se concluye que el sitio es seguro bajo los parámetros actuales de evaluación. No obstante, la ausencia de hallazgos críticos en esta fase debe complementarse con revisiones periódicas para mantener este estándar de protección.

Resumen de Riesgos

0	0	0	0	12
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

Puertos Abiertos	100	OK	2 puerto(s) abierto(s), todos esperados

Puertos Abiertos — 100/100

Estado: OK

2 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 — Envio de correo
- INFO **Puerto 80 (HTTP)**
  Abierto (esperado) — 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 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 detectaron vulnerabilidades durante los checks pasivos realizados. El análisis de infraestructura reveló que no existen puertos expuestos de forma indebida ni fallos de configuración visibles externamente. Debido a que el PentestAgent no fue ejecutado en esta sesión, no se han identificado CWEs, endpoints de API adicionales o subdominios expuestos. Los puertos detectados como abiertos se consideran necesarios y seguros para la operación estándar del servicio.