

# Escanear Vulnerabilidades

Informe de Seguridad Web

URL https://sisweb.msal.gov.ar  
Dominio sisweb.msal.gov.ar  
Fecha 30 de mayo de 2026 a las 01:05

Checks 9 pruebas  
Hallazgos 16 totales  
Problemas 4 detectados

# C

## 73/100

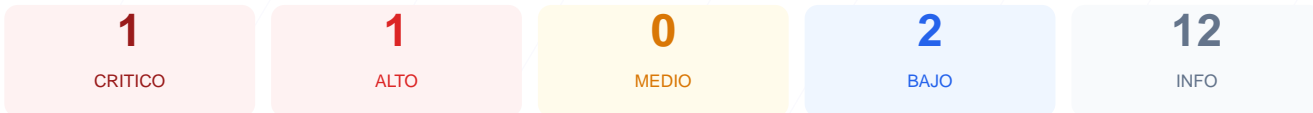
puntos de seguridad



### RESUMEN EJECUTIVO

El análisis de ciberseguridad realizado al sitio web arroja una puntuación de 73/100, lo que corresponde a una nota C. Durante la evaluación se ejecutaron 9 checks pasivos, de los cuales 1 resultado en estado OK, 0 generaron advertencias y 1 fue marcado como fallo según el resumen de ejecución. Los hallazgos principales revelan deficiencias críticas en la implementación de protocolos de cifrado y configuración de acceso seguro. Debido a la incapacidad de establecer una conexión SSL/TLS y la falta de redirección automática a HTTPS, se concluye que el sitio es actualmente vulnerable y no garantiza la confidencialidad de los datos transmitidos.

### Resumen de Riesgos



### Resumen de Checks

SSL/TLS	0	ERROR	No se pudo verificar SSL/TLS
Cabeceras de Seguridad	0	ERROR	No se pudieron verificar las cabeceras
Redirección HTTPS	0	ERROR	No se pudo verificar la redirección HTTPS
Detección CMS	0	ERROR	No se pudo analizar el CMS
Version CMS Expuesta	0	ERROR	No se pudo verificar la versión del CMS
Seguridad de Cookies	0	ERROR	No se pudieron verificar las 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: ERROR

No se pudo verificar SSL/TLS

- CRITICO** Conexión SSL  
No se pudo establecer conexión SSL/TLS

### Redirección HTTPS — 0/100

Estado: ERROR

No se pudo verificar la redirección HTTPS

- ALTO** HTTP !' HTTPS redirección  
HTTP 200 — No redirige a HTTPS

### 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

## 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 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

[CRITICAL] Conexion SSL: No se pudo establecer una conexion cifrada SSL/TLS, lo que permite que la informacion viaje en texto plano y sea interceptada por terceros.

[HIGH] Redireccion HTTPS: El sitio permite el acceso mediante HTTP sin redirigir al protocolo seguro HTTPS, facilitando ataques de hombre en el medio (MitM).

[LOW] Archivo robots.txt: Se detecto un error al intentar acceder a este archivo, lo que impide gestionar adecuadamente que partes del sitio deben ser rastreadas por buscadores.

[LOW] Archivo sitemap.xml: El acceso al mapa del sitio fallo, lo que afecta negativamente la indexacion y la visibilidad de la estructura jerarquica del portal.