

# Escanear Vulnerabilidades

Informe de Seguridad Web

URL https://www.ids.alinet.cu  
Dominio www.ids.alinet.cu  
Fecha 20 de abril de 2026 a las 20:02

Checks 9 pruebas  
Hallazgos 15 totales  
Problemas 3 detectados

# C

## 73/100

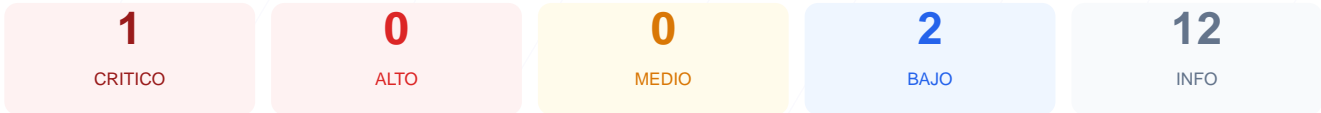
puntos de seguridad



### RESUMEN EJECUTIVO

La auditoria de seguridad realizada al sitio web arrojó una puntuación de 73/100, lo que equivale a una nota de C. Durante el análisis se ejecutaron 9 checks pasivos, de los cuales 1 resultado exitoso y 1 presentó un fallo crítico directo, mientras que el resto no pudo ser verificado por errores de conexión. La imposibilidad de validar protocolos básicos de cifrado y cabeceras de protección sugiere una configuración de servidor inestable o restrictiva. Debido a estas deficiencias técnicas en la infraestructura de seguridad, se concluye que el sitio es actualmente vulnerable.

### 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
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
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** Conexion SSL  
No se pudo establecer conexion SSL/TLS

### 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 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] Conexion SSL: No se pudo establecer una conexion cifrada SSL/TLS, lo que impide proteger la integridad y confidencialidad de los datos transmitidos.

[CRITICAL] Cabeceras de Seguridad: El sistema no pudo verificar la presencia de cabeceras de proteccion, dejando el sitio expuesto a ataques de tipo Cross-Site Scripting y Clickjacking.

[CRITICAL] Redireccion HTTPS: No existe una transicion forzada de trafico inseguro a seguro, lo que permite que los usuarios naveguen por canales vulnerables.

[LOW] Ausencia de robots.txt y sitemap.xml: El servidor denego el acceso o no cuenta con estos archivos, dificultando la indexacion correcta y el control de rastreo.

[MEDIUM] Seguridad de Cookies: No se pudo confirmar el uso de atributos Secure o HttpOnly, lo que podria facilitar el robo de sesiones de usuario.