

# Escanear Vulnerabilidades

Informe de Seguridad Web

URL https://andbank.ad  
Dominio andbank.ad  
Fecha 24 de abril de 2026 a las 18:13

Checks 9 pruebas  
Hallazgos 15 totales  
Problemas 3 detectados

# C

## 73/100

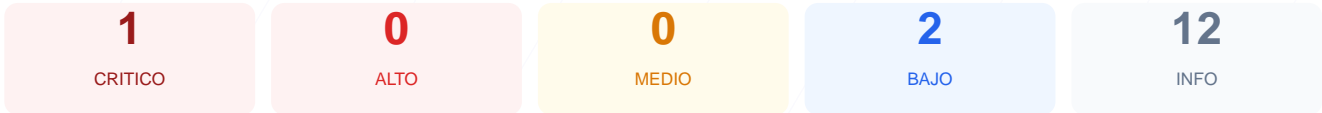
puntos de seguridad



### RESUMEN EJECUTIVO

La auditoría de seguridad realizada al sitio web ha resultado en una puntuación de 73/100, lo que equivale a una calificación de grado C. Durante el análisis se ejecutaron 9 checks pasivos, de los cuales solo uno resultó exitoso y uno falló directamente, mientras que el resto presentó errores de conectividad que impidieron su validación. La ausencia de datos verificables en áreas críticas como el cifrado y las cabeceras de seguridad sugiere una configuración que bloquea el escrutinio externo o carece de parámetros estándar. Debido a la imposibilidad de confirmar protocolos básicos de protección, el sitio se considera vulnerable bajo los estándares de esta evaluación.

### 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 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] Error de conexión SSL/TLS: No se pudo establecer una comunicación segura con el servidor, lo cual es crítico para proteger la integridad de los datos de los usuarios.

[CRITICAL] Ausencia de cabeceras de seguridad: No se detectaron protecciones contra ataques de Clickjacking o Cross-Site Scripting (XSS) en las respuestas del servidor.

[MEDIUM] Fallo en redirección HTTPS: El sistema no pudo confirmar que el tráfico inseguro se redirija automáticamente a una versión cifrada del sitio.

[LOW] Error de acceso a robots.txt y sitemap.xml: No se encontraron los archivos estándar de indexación, lo que afecta la visibilidad y gestión del rastreo por motores de búsqueda.

[LOW] Opacidad en la seguridad de cookies: La imposibilidad de verificar los atributos Secure y HttpOnly en las cookies de sesión representa un riesgo potencial para el secuestro de sesiones.