# EscanearVulnerabilidades

Informe de Seguridad Web

| | | | |
|---|---|---|---|
| URL | https://akros.inemjose.net/login | Checks | 9 pruebas |
| Dominio | akros.inemjose.net | Hallazgos | 49 totales |
| Fecha | 15 de julio de 2026 a las 19:13 | Problemas | 8 detectados |

C

73/100

puntos de seguridad

## RESUMEN EJECUTIVO

El análisis de ciberseguridad realizado en el sitio web ha dado como resultado una puntuación exacta de 73/100, lo que otorga una nota de C. Durante la evaluación se ejecutaron 9 checks pasivos, de los cuales 4 resultaron exitosos, 4 generaron advertencias y 1 fue calificado como fallo crítico. Aunque la plataforma cuenta con un cifrado SSL válido, presenta debilidades significativas en la configuración del servidor y la exposición de servicios internos. Se concluye que el sitio es actualmente vulnerable, principalmente debido a la apertura de puertos sensibles y la falta de políticas de transporte seguro. Es necesaria una intervención técnica inmediata para proteger la integridad de los datos de los usuarios.

## Resumen de Riesgos

| 1 | 5 | 0 | 2 | 41 |
|---|---|---|---|---|
| CRITICO | ALTO | MEDIO | BAJO | INFO |

## Resumen de Checks

| | | | |
|---|---|---|---|
| SSL/TLS | 100 | OK | Certificado valido, expira en 62 dias |
| Cabeceras de Seguridad | 80 | AVISO | 5/6 presentes. Faltan: Strict-Transport-Security |
| Redireccion HTTPS | 0 | FALLO | No hay redireccion HTTP a HTTPS |
| Deteccion CMS | 100 | OK | No se detecto un CMS conocido |
| Version CMS Expuesta | 100 | OK | No se detecto version de CMS expuesta |
| Seguridad de Cookies | 83 | AVISO | XSRF-TOKEN: falta HttpOnly |
| Contenido Mixto | 100 | OK | No se detecto contenido mixto |
| Robots.txt y Sitemap | 60 | AVISO | Falta sitemap.xml |
| Puertos Abiertos | 60 | AVISO | 2 puerto(s) potencialmente riesgoso(s): 21 (FTP)... |

## SSL/TLS — 100/100

Estado: OK

Certificado valido, expira en 62 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
  62 dias restantes (expira: 2026-09-15T10:03:18.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2026-06-17T10:03:19.000Z
- INFO **Puerto 443**
  Conexion HTTPS establecida correctamente en puerto 443

## Cabeceras de Seguridad — 80/100

Estado: AVISO

5/6 presentes. Faltan: Strict-Transport-Security

- BAJO **Server header expuesto**
  Server: LiteSpeed — Revela tecnologia del servidor

- INFO **Content-Security-Policy**
  Presente: frame-ancestors 'self' ...
- INFO **X-Frame-Options**
  Presente: SAMEORIGIN
- ALTO **Strict-Transport-Security**
  Falta — Fuerza conexiones HTTPS (HSTS)
- INFO **X-Content-Type-Options**
  Presente: nosniff
- INFO **Referrer-Policy**
  Presente: no-referrer-when-downgrade
- INFO **Permissions-Policy**
  Presente: geolocation=(), microphone=(), camera=(self)

## Redireccion HTTPS — 0/100

Estado: FALLO

No hay redireccion HTTP a HTTPS

- ALTO **HTTP !' HTTPS redireccion**
  HTTP 302 — No redirige a HTTPS
- ALTO **HSTS (Strict-Transport-Security)**
  HSTS no configurado — El navegador no fuerza HTTPS
- INFO **Respuesta HTTPS**
  HTTPS responde con status 200

## Deteccion CMS — 100/100

Estado: OK

No se detecto un CMS conocido

- INFO **WordPress**
  No detectado
- INFO **Joomla**
  No detectado
- INFO **Drupal**
  No detectado
- INFO **Magento**
  No detectado
- INFO **Shopify**
  No detectado
- INFO **PrestaShop**
  No detectado
- INFO **Wix**
  No detectado
- INFO **Squarespace**
  No detectado

## Version CMS Expuesta — 100/100

Estado: OK

No se detecto version de CMS expuesta

- INFO **Archivo /readme.html**
  No accesible (correcto)
- INFO **Archivo /README.txt**
  No accesible (correcto)
- INFO **Version CMS**
  No se detecta ninguna version expuesta

## Seguridad de Cookies — 83/100

Estado: AVISO

XSRF-TOKEN: falta HttpOnly

- INFO **Cookies detectadas**
  2 cookie(s) encontrada(s)
- ALTO **Cookie: XSRF-TOKEN — HttpOnly**
  Falta HttpOnly — Cookie accesible via document.cookie (riesgo XSS)
- INFO **Cookie: XSRF-TOKEN — Secure**
  Flag Secure activo — Solo se envia por HTTPS
- INFO **Cookie: XSRF-TOKEN — SameSite**
  SameSite=lax
- INFO **Cookie: soluciones-akros-session — HttpOnly**
  HttpOnly activo — No accesible via JavaScript
- INFO **Cookie: soluciones-akros-session — Secure**
  Flag Secure activo — Solo se envia por HTTPS
- INFO **Cookie: soluciones-akros-session — SameSite**
  SameSite=lax

## Contenido Mixto — 100/100

Estado: OK

No se detecto contenido mixto

- INFO **Contenido mixto**
  Todos los recursos se cargan por HTTPS

## Robots.txt y Sitemap — 60/100

Estado: AVISO

Falta sitemap.xml

- INFO **robots.txt**
  Presente (24 bytes)
- INFO **Reglas robots.txt**
  1 Disallow, 0 Allow
- BAJO **sitemap.xml**
  No encontrado (HTTP 404)
- BAJO **security.txt**
  No encontrado — Recomendado para politica de divulgacion

## Puertos Abiertos — 60/100

Estado: AVISO

2 puerto(s) potencialmente riesgoso(s): 21 (FTP), 3306 (MySQL)

- ALTO **Puerto 21 (FTP)**
  ABIERTO — 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
- CRITICO **Puerto 3306 (MySQL)**
  ABIERTO — 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**

[CRITICAL] Puerto 3306 (MySQL): La base de datos está expuesta a internet, permitiendo intentos de conexión externa y ataques de fuerza bruta.
[HIGH] Puerto 21 (FTP): Servicio de transferencia de archivos abierto que utiliza protocolos no cifrados, facilitando la interceptación de archivos y credenciales.
[HIGH] Redirección HTTPS: El sitio no redirige automáticamente el tráfico HTTP hacia HTTPS, dejando las sesiones de los usuarios vulnerables a ataques de interceptación.
[HIGH] HSTS (Strict-Transport-Security): La ausencia de esta cabecera impide que los navegadores fuercen siempre una conexión segura.
[HIGH] Cookie XSRF-TOKEN: Falta el atributo HttpOnly, lo que permite que la cookie sea leída por scripts maliciosos y facilita ataques de Cross-Site Scripting (XSS).
[LOW] Server header expuesto: El servidor revela el uso de LiteSpeed, información que ayuda a potenciales atacantes a buscar vulnerabilidades específicas para esa tecnología.
[LOW] sitemap.xml: El archivo no fue encontrado, lo que afecta la visibilidad de la estructura del sitio y la auditoría de rutas disponibles.