

# Escanear Vulnerabilidades

Informe de Seguridad Web

URL https://invix.munimolina.gob.pe  
Dominio invix.munimolina.gob.pe  
Fecha 9 de mayo de 2026 a las 01:14

Checks 9 pruebas  
Hallazgos 18 totales  
Problemas 3 detectados

# F

## 37/100

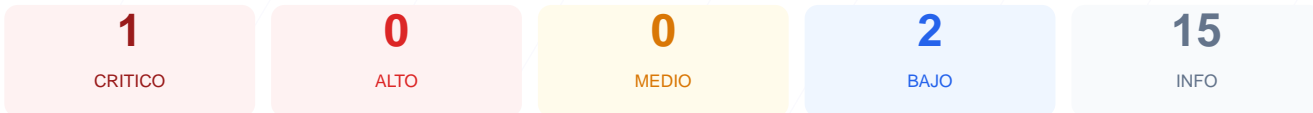
puntos de seguridad



## RESUMEN EJECUTIVO

El análisis de ciberseguridad realizado al dominio invix.munimolina.gob.pe ha resultado en una puntuación crítica de 37/100, obteniendo una calificación de nota F. Durante la evaluación se ejecutaron 9 checks pasivos, de los cuales solo 1 resultó exitoso, detectándose 2 fallos directos y múltiples errores que impidieron verificar controles esenciales de seguridad. La ausencia de un certificado SSL válido y la falta de configuraciones básicas de indexación representan riesgos significativos. Debido a estos hallazgos, se concluye que el sitio es actualmente vulnerable y no cumple con los estándares mínimos de seguridad web.

## Resumen de Riesgos



## Resumen de Checks

SSL/TLS	0	FALLO	Certificado SSL no valido
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: FALLO

Certificado SSL no valido

- CRITICO** Certificado valido  
El certificado SSL NO es valido
- INFO** Dias hasta expiracion  
169 dias restantes (expira: 2026-10-24T23:59:59.000Z)
- INFO** Fecha de emision  
Emitido desde: 2025-09-23T00:00:00.000Z
- INFO** Puerto 443  
Conexion HTTPS establecida correctamente en puerto 443

## Robots.txt y Sitemap — 20/100

Estado: FALLO

Faltan robots.txt y sitemap.xml

- BAJO** robots.txt  
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] Certificado SSL no válido: El sitio no cuenta con un certificado de seguridad vigente o correctamente configurado, lo que impide el cifrado de datos y expone la información de los usuarios a ataques de interceptación.

[LOW] Ausencia de archivo robots.txt: No se pudo acceder a las directivas de rastreo para buscadores, lo que dificulta el control sobre qué partes del sitio deben ser indexadas.

[LOW] Ausencia de archivo sitemap.xml: El mapa del sitio no está disponible o es inaccesible, lo que afecta la visibilidad y organización de la estructura web ante agentes externos.