

# Escanear Vulnerabilidades

Informe de Seguridad Web

URL https://mail.coopnacional.com  
Dominio mail.coopnacional.com  
Fecha 13 de mayo de 2026 a las 16:31

Checks 9 pruebas  
Hallazgos 18 totales  
Problemas 3 detectados

# F

## 37/100

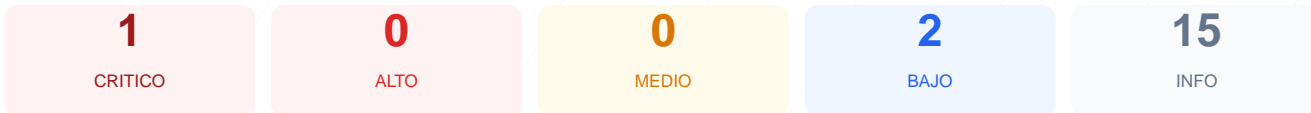
puntos de seguridad



## RESUMEN EJECUTIVO

La auditoría de seguridad realizada sobre el dominio analizado ha resultado en una puntuación crítica de 37/100, obteniendo una calificación final de grado F. Durante la evaluación se ejecutaron 9 checks pasivos que revelaron fallos estructurales graves, especialmente en lo que respecta al cifrado de datos y la configuración del servidor. Se detectó la ausencia de un certificado SSL válido y la carencia de archivos de gestión de indexación fundamentales. Debido a estas deficiencias técnicas, se concluye que el sitio es actualmente vulnerable y representa un riesgo para la integridad de los datos de los usuarios.

## 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
- MEDIO** Dias hasta expiracion  
21 dias restantes (expira: 2026-06-03T23:59:59.000Z)
- INFO** Fecha de emision  
Emitido desde: 2025-06-02T00:00:00.000Z
- 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 servidor no dispone de un certificado legítimo, lo que expone cualquier comunicación a ataques de interceptación de datos.

[LOW] Ausencia de robots.txt: No se pudo acceder a este archivo, lo que impide una gestión controlada del rastreo por parte de motores de búsqueda.

[LOW] Ausencia de sitemap.xml: El sitio carece de un mapa de estructura web, lo que dificulta la auditoría de contenidos y la navegación automatizada.

[ERROR] Fallo en cabeceras de seguridad: No se pudo verificar la presencia de protecciones contra ataques de tipo Cross-Site Scripting (XSS) o Clickjacking.

[ERROR] Redirección HTTPS inexistente: La falta de una redirección forzada hacia el protocolo seguro impide garantizar conexiones cifradas por defecto.

[ERROR] Seguridad de cookies no verificada: Al no detectarse la configuración de cookies, no es posible asegurar que los identificadores de sesión estén protegidos.