# EscanearVulnerabilidades

Informe de Seguridad Web

| | | | |
|---|---|---|---|
| URL | https://linea.coopdgii.com | Checks | 9 pruebas |
| Dominio | linea.coopdgii.com | Hallazgos | 51 totales |
| Fecha | 25 de septiembre de 2026 a las 17:46 | Problemas | 9 detectados |

C

64/100

puntos de seguridad

## RESUMEN EJECUTIVO

La auditoría de ciberseguridad realizada al sitio web presenta una puntuación de 64/100, lo que otorga una calificación de nota C. Durante el análisis, se ejecutaron 9 checks pasivos que resultaron en 3 verificaciones correctas, 4 advertencias y 2 fallos críticos de configuración. Se han detectado riesgos significativos relacionados con la exposición de bases de datos y la falta de protocolos de cifrado forzado en la navegación. Debido a la gravedad de los puertos abiertos y la gestión de cookies, el sitio se concluye como vulnerable y requiere intervención técnica inmediata.

## Resumen de Riesgos

| 2 | 4 | 1 | 2 | 42 |
|---|---|---|---|---|
| CRITICO | ALTO | MEDIO | BAJO | INFO |

## Resumen de Checks

| | | | |
|---|---|---|---|
| SSL/TLS | 70 | AVISO | Certificado expira en 26 dias |
| Cabeceras de Seguridad | 75 | AVISO | 5/6 presentes. Faltan: Content-Security-Policy |
| 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 | 20 | FALLO | 4 puertos riesgosos abiertos |

## SSL/TLS — 70/100

Estado: AVISO

Certificado expira en 26 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- MEDIO **Dias hasta expiracion**
  26 dias restantes (expira: 2026-10-21T23:59:59.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2026-04-06T00:00:00.000Z
- INFO **Puerto 443**
  Conexion HTTPS establecida correctamente en puerto 443

## Cabeceras de Seguridad — 75/100

Estado: AVISO

5/6 presentes. Faltan: Content-Security-Policy

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

- ALTO **Content-Security-Policy**
  Falta — Previene XSS y ataques de inyeccion de contenido
- INFO **X-Frame-Options**
  Presente: SAMEORIGIN
- INFO **Strict-Transport-Security**
  Presente: max-age=31536000; includeSubDomains
- INFO **X-Content-Type-Options**
  Presente: nosniff
- INFO **Referrer-Policy**
  Presente: strict-origin-when-cross-origin
- INFO **Permissions-Policy**
  Presente: camera=(), microphone=(), geolocation=(self)

## Redireccion HTTPS — 0/100

Estado: FALLO

No hay redireccion HTTP a HTTPS

- ALTO **HTTP !' HTTPS redireccion**
  HTTP 301 — No redirige a HTTPS
- INFO **HSTS (Strict-Transport-Security)**
  HSTS activo: max-age=31536000; includeSubDomains
- BAJO **HSTS includeSubDomains**
  HSTS cubre subdominios
- INFO **HSTS max-age**
  max-age=31536000 (365 dias)
- 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: coopdgii_session — HttpOnly**
  HttpOnly activo — No accesible via JavaScript
- INFO **Cookie: coopdgii_session — Secure**
  Flag Secure activo — Solo se envia por HTTPS
- INFO **Cookie: coopdgii_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 — 20/100

Estado: FALLO

4 puertos riesgosos abiertos

- ALTO **Puerto 21 (FTP)**
  ABIERTO — Transferencia de archivos sin cifrar
- MEDIO **Puerto 22 (SSH)**
  ABIERTO — 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

- CRITICO **Puerto 5432 (PostgreSQL)**
  ABIERTO — 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 5432 (PostgreSQL) ABIERTO: El servicio de base de datos es visible desde internet, lo que permite intentos de acceso no autorizado y ataques dirigidos.
[CRITICAL] Puerto 3306 (MySQL) ABIERTO: La exposición de este puerto facilita la explotación de vulnerabilidades en el motor de base de datos y riesgos de exfiltración de datos.
[HIGH] HTTP a HTTPS redireccion FAIL: El sitio no redirige automáticamente a los usuarios a la versión segura, permitiendo la interceptación de datos en tránsito.
[HIGH] Content-Security-Policy (CSP) FALTA: La ausencia de esta cabecera aumenta drásticamente el riesgo de ataques Cross-Site Scripting (XSS) e inyección de código.
[HIGH] Cookie XSRF-TOKEN falta HttpOnly: Esta vulnerabilidad permite que scripts maliciosos accedan a la cookie de sesión, facilitando el secuestro de la misma.
[HIGH] Puerto 21 (FTP) ABIERTO: El uso de este protocolo implica la transferencia de archivos y credenciales sin cifrado, siendo vulnerable a escucha activa.
[MEDIUM] Puerto 22 (SSH) ABIERTO: Mantener el acceso remoto visible al público facilita ataques de fuerza bruta para intentar tomar control del servidor.
[LOW] SSL/TLS advertencia de expiración: El certificado actual caduca en 26 días, lo que podría generar pérdida de confianza y errores de acceso próximamente.
[LOW] Server header expuesto (Apache): Revelar la tecnología exacta del servidor ayuda a atacantes a identificar vulnerabilidades específicas del software.
[LOW] sitemap.xml no encontrado: La falta de este archivo dificulta la auditoría de rutas del sitio y puede ocultar problemas de arquitectura web.