EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://bancocoopnacional.com	Checks	9 pruebas
Dominio	bancocoopnacional.com	Hallazgos	52 totales
Fecha	13 de mayo de 2026 a las 16:30	Problemas	10 detectados

B

86/100

puntos de seguridad

RESUMEN EJECUTIVO

El análisis de seguridad técnica realizado sobre el dominio bancocoopnacional.com arroja una puntuación de 86/100, lo que otorga una calificación de grado B. Durante la evaluación se ejecutaron 9 checks pasivos, resultando en 6 verificaciones satisfactorias, 2 advertencias y 1 fallo crítico identificado en la gestión de sesiones. El sitio web demuestra una implementación robusta en su cifrado de transporte y redirecciones HTTPS, pero presenta debilidades en la configuración de cabeceras y seguridad de cookies. Se concluye que, si bien el sitio cuenta con una base de seguridad aceptable, se considera vulnerable a ataques de secuestro de sesión y divulgación de información técnica. Es imperativo aplicar las correcciones recomendadas para mitigar los riesgos de nivel medio y alto detectados.

Resumen de Riesgos

0	1	5	4	42
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 167 dias
Cabeceras de Seguridad	75	AVISO	4/6 presentes. Faltan: Referrer-Policy, Permissi...
Redireccion HTTPS	100	OK	HTTP redirige a HTTPS y HSTS esta habilitado
Deteccion CMS	100	OK	CMS detectado: Drupal, PrestaShop
Version CMS Expuesta	100	OK	No se detecto version de CMS expuesta
Seguridad de Cookies	33	FALLO	cookiesession1: falta Secure; cookiesession1: fa...
Contenido Mixto	100	OK	No se detecto contenido mixto
Robots.txt y Sitemap	60	AVISO	Falta sitemap.xml
Puertos Abiertos	100	OK	No se detectaron puertos abiertos

SSL/TLS — 100/100

Estado: OK

Certificado valido, expira en 167 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
  167 dias restantes (expira: 2026-10-27T20:56:18.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2025-09-25T20:56:19.000Z
- INFO **Puerto 443**
  Conexion HTTPS establecida correctamente en puerto 443

Cabeceras de Seguridad — 75/100

Estado: AVISO

4/6 presentes. Faltan: Referrer-Policy, Permissions-Policy

- INFO **Content-Security-Policy**
  Presente: report-uri /report-csp-violation; upgrade-insecure-requests

- INFO **X-Frame-Options**
  Presente: SAMEORIGIN
- INFO **Strict-Transport-Security**
  Presente: max-age=15552000; includeSubDomains
- INFO **X-Content-Type-Options**
  Presente: nosniff, nosniff
- MEDIO **Referrer-Policy**
  Falta — Controla la informacion de referer enviada
- MEDIO **Permissions-Policy**
  Falta — Restringe APIs del navegador (camara, micro, etc.)

Redireccion HTTPS — 100/100

Estado: OK

HTTP redirige a HTTPS y HSTS esta habilitado

- INFO **HTTP !' HTTPS redireccion**
  HTTP 302 redirige a https://bancocoopnacional.com
- INFO **HSTS (Strict-Transport-Security)**
  HSTS activo: max-age=15552000; includeSubDomains
- BAJO **HSTS includeSubDomains**
  HSTS cubre subdominios
- INFO **HSTS max-age**
  max-age=15552000 (180 dias)
- INFO **Respuesta HTTPS**
  HTTPS responde con status 200

Deteccion CMS — 100/100

Estado: OK

CMS detectado: Drupal, PrestaShop

- INFO **WordPress**
  No detectado
- INFO **Joomla**
  No detectado
- INFO **Drupal**
  Detectado via HTML body
- INFO **Magento**
  No detectado
- INFO **Shopify**
  No detectado
- INFO **PrestaShop**
  Detectado via HTML body
- INFO **Wix**
  No detectado
- INFO **Squarespace**
  No detectado
- BAJO **Meta generator**
  Expone: Drupal 9 (https://www.drupal.org)
- INFO **Tecnologias detectadas**
  Next.js

Version CMS Expuesta — 100/100

Estado: OK

No se detecto version de CMS expuesta

- INFO **Archivo /readme.html**
  No accesible (correcto)
- MEDIO **Archivo /README.txt**
  Archivo accesible publicamente — Puede revelar version e informacion del CMS

- MEDIO **Ruta /user/login**
  Panel de login accesible publicamente
- INFO **Version CMS**
  No se detecta ninguna version expuesta

Seguridad de Cookies — 33/100

Estado: FALLO

cookiesession1: falta Secure; cookiesession1: falta SameSite

- INFO **Cookies detectadas**
  1 cookie(s) encontrada(s)
- INFO **Cookie: cookiesession1 — HttpOnly**
  HttpOnly activo — No accesible via JavaScript
- ALTO **Cookie: cookiesession1 — Secure**
  Falta flag Secure — Cookie se envia en conexiones HTTP
- MEDIO **Cookie: cookiesession1 — SameSite**
  Falta SameSite — Vulnerable a CSRF

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 (1706 bytes)
- INFO **Reglas robots.txt**
  26 Disallow, 18 Allow
- BAJO **Ruta sensible en robots.txt**
  Referencia a "admin" — Puede revelar rutas sensibles a atacantes
- BAJO **Ruta sensible en robots.txt**
  Referencia a "config" — Puede revelar rutas sensibles a atacantes
- BAJO **sitemap.xml**
  No encontrado (HTTP 404)
- BAJO **security.txt**
  No encontrado — Recomendado para politica de divulgacion

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 — Envio 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 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

[HIGH] Cookie cookiesession1 sin flag Secure: La ausencia de este atributo permite que la cookie de sesión sea enviada a través de conexiones HTTP no cifradas, facilitando su interceptación por atacantes.
[MEDIUM] Cookie cookiesession1 sin atributo SameSite: La falta de esta configuración hace que el sitio sea susceptible a ataques de falsificación de petición en sitios cruzados (CSRF).
[MEDIUM] Falta de cabecera Referrer-Policy: El servidor no controla qué información de procedencia se envía a otros dominios, lo que podría filtrar rutas internas o datos sensibles.
[MEDIUM] Falta de cabecera Permissions-Policy: No se restringe el acceso a APIs del navegador como la cámara o el micrófono, incrementando la superficie de ataque potencial.
[MEDIUM] Archivo README.txt accesible públicamente: Este archivo puede revelar detalles internos de la instalación del CMS, facilitando la fase de reconocimiento a un atacante.
[MEDIUM] Ruta /user/login expuesta: El panel de acceso administrativo es visible para cualquier usuario, lo que permite intentos de acceso no autorizado mediante fuerza bruta.
[LOW] Meta generator expuesto: El código fuente revela el uso de Drupal 9, permitiendo que atacantes identifiquen vulnerabilidades específicas para esa versión.
[LOW] Rutas sensibles en robots.txt: Se referencian directorios como admin y config, guiando a posibles atacantes hacia secciones críticas de la estructura web.
[LOW] Ausencia de sitemap.xml: El archivo de mapa del sitio no fue encontrado, lo que dificulta la auditoría de contenidos y la indexación controlada.