EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://www.Bancolombia.com	Checks	9 pruebas
Dominio	www.bancolombia.com	Hallazgos	52 totales
Fecha	12 de junio de 2026 a las 17:57	Problemas	10 detectados

B

87/100

puntos de seguridad

RESUMEN EJECUTIVO

La auditoría de seguridad realizada al dominio bancolombia.com ha resultado en una puntuación de 87/100 con una calificación de grado B. El análisis constó de 9 checks pasivos, de los cuales 6 resultaron satisfactorios, 2 generaron advertencias y 1 fue identificado como fallo crítico. Aunque el sitio presenta una configuración de cifrado y transporte de datos excelente, se han detectado exposiciones graves en la infraestructura de red. Debido a la apertura de puertos de bases de datos y servicios de administración remota, el sitio se considera actualmente vulnerable ante ataques dirigidos.

Resumen de Riesgos

3	2	5	0	42
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 297 dias
Cabeceras de Seguridad	85	AVISO	5/6 presentes. Faltan: Permissions-Policy
Redireccion HTTPS	100	OK	HTTP redirige a HTTPS y HSTS esta habilitado
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	incap_ses_690_3189513: falta HttpOnly
Contenido Mixto	100	OK	No se detecto contenido mixto
Robots.txt y Sitemap	100	OK	robots.txt y sitemap.xml presentes
Puertos Abiertos	20	FALLO	5 puertos riesgosos abiertos

SSL/TLS — 100/100

Estado: OK

Certificado valido, expira en 297 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
  297 dias restantes (expira: 2027-04-05T14:01:16.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2026-03-04T14:01:17.000Z
- INFO **Puerto 443**
  Conexion HTTPS establecida correctamente en puerto 443

Cabeceras de Seguridad — 85/100

Estado: AVISO

5/6 presentes. Faltan: Permissions-Policy

- INFO **Content-Security-Policy**
  Presente: default-src 'self' https://play.vidyard.com *.vidyard.com *.onesignal.com *.segm...

- INFO **X-Frame-Options**
  Presente: SAMEORIGIN
- INFO **Strict-Transport-Security**
  Presente: max-age=31536000;
- INFO **X-Content-Type-Options**
  Presente: nosniff
- INFO **Referrer-Policy**
  Presente: strict-origin
- 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 301 redirige a https://www.bancolombia.com/
- INFO **HSTS (Strict-Transport-Security)**
  HSTS activo: max-age=31536000;
- BAJO **HSTS includeSubDomains**
  HSTS no 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
- INFO **Tecnologias detectadas**
  Next.js

Version CMS Expuesta — 100/100

Estado: OK

No se detecto version de CMS expuesta

- MEDIO **Archivo /readme.html**
  Archivo accesible publicamente — Puede revelar version e informacion del CMS
- MEDIO **Archivo /README.txt**
  Archivo accesible publicamente — Puede revelar version e informacion del CMS
- INFO **Version CMS**
  No se detecta ninguna version expuesta

Seguridad de Cookies — 83/100

Estado: AVISO

incap_ses_690_3189513: falta HttpOnly

- INFO **Cookies detectadas**
  2 cookie(s) encontrada(s)
- INFO **Cookie: visid_incap_3189513 — HttpOnly**
  HttpOnly activo — No accesible via JavaScript
- INFO **Cookie: visid_incap_3189513 — Secure**
  Flag Secure activo — Solo se envia por HTTPS
- INFO **Cookie: visid_incap_3189513 — SameSite**
  SameSite=none
- ALTO **Cookie: incap_ses_690_3189513 — HttpOnly**
  Falta HttpOnly — Cookie accesible via document.cookie (riesgo XSS)
- INFO **Cookie: incap_ses_690_3189513 — Secure**
  Flag Secure activo — Solo se envia por HTTPS
- INFO **Cookie: incap_ses_690_3189513 — SameSite**
  SameSite=none

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 — 100/100

Estado: OK

robots.txt y sitemap.xml presentes

- INFO **robots.txt**
  Presente (6062 bytes)
- INFO **Reglas robots.txt**
  77 Disallow, 23 Allow
- MEDIO **Bloqueo total**
  robots.txt bloquea todo el sitio con Disallow: /
- INFO **Sitemap en robots.txt**
  https://www.bancolombia.com/sitemap-index.xml
- INFO **security.txt**
  Presente en /.well-known/security.txt — Buena practica

Puertos Abiertos — 20/100

Estado: FALLO

5 puertos riesgosos abiertos

- 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

- CRITICO **Puerto 3389 (RDP)**
  ABIERTO — Escritorio remoto Windows
- INFO **Puerto 5432 (PostgreSQL)**
  Cerrado — Base de datos PostgreSQL expuesta
- CRITICO **Puerto 6379 (Redis)**
  ABIERTO — Cache Redis sin autenticacion por defecto
- MEDIO **Puerto 8080 (HTTP-Alt)**
  ABIERTO — 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 se encuentra expuesta a internet, permitiendo intentos de conexión externa y ataques de fuerza bruta contra los datos.
[CRITICAL] Puerto 3389 (RDP): El servicio de Escritorio Remoto de Windows es visible públicamente, lo que facilita vectores de intrusión directa al servidor.
[CRITICAL] Puerto 6379 (Redis): Instancia de caché expuesta que suele carecer de autenticación por defecto, permitiendo la extracción de datos sensibles en memoria.
[HIGH] Puerto 21 (FTP): El uso de un protocolo de transferencia de archivos sin cifrar permite la interceptación de credenciales y datos en tránsito.
[HIGH] Cookie incap_ses_690_3189513: Falta el atributo HttpOnly, permitiendo que la cookie sea accesible mediante scripts y aumentando el riesgo de secuestro de sesión (XSS).
[MEDIUM] Permissions-Policy: Ausencia de esta cabecera de seguridad que debería restringir el acceso del navegador a APIs sensibles como la cámara o el micrófono.
[MEDIUM] Archivo /readme.html y /README.txt: Estos archivos son accesibles públicamente y pueden revelar detalles técnicos sobre la configuración o versiones del sistema.
[MEDIUM] Puerto 8080 (HTTP-Alt): Servidor web secundario abierto que puede ser utilizado como un vector de entrada no monitorizado o proxy.
[MEDIUM] Bloqueo total en robots.txt: El archivo bloquea el rastreo de todo el sitio, lo cual puede ser una medida de seguridad reactiva pero insuficiente si no hay controles de acceso reales.