EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://onlinebanking.bancogalicia.com.ar/login	Checks	9 pruebas
Dominio	onlinebanking.bancogalicia.com.ar	Hallazgos	69 totales
Fecha	19 de mayo de 2026 a las 12:59	Problemas	22 detectados

C

73/100

puntos de seguridad

RESUMEN EJECUTIVO

El análisis de seguridad realizado sobre el portal de banca en línea arrojó una puntuación exacta de 73/100, lo que resulta en una calificación de nota C. Se ejecutaron 9 checks pasivos, de los cuales 5 fueron satisfactorios, se identificó 1 advertencia y se registraron 3 fallos en configuraciones críticas. Los principales riesgos se concentran en la gestión de cabeceras de seguridad y la configuración de cookies de sesión. Debido a estas deficiencias técnicas, el sitio se considera vulnerable frente a ataques de inyección de código y secuestro de sesiones. Se requiere atención inmediata para alcanzar estándares de seguridad bancaria aceptables.

Resumen de Riesgos

0	9	11	2	47
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 97 dias
Cabeceras de Seguridad	35	FALLO	Solo 2/6 presentes. Faltan: Content-Security-Pol...
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	42	FALLO	Luke: falta HttpOnly; Luke: falta SameSite; R2D2...
Contenido Mixto	60	AVISO	1 recurso(s) HTTP en pagina HTTPS
Robots.txt y Sitemap	20	FALLO	Faltan robots.txt y sitemap.xml
Puertos Abiertos	100	OK	No se detectaron puertos abiertos

SSL/TLS — 100/100

Estado: OK

Certificado valido, expira en 97 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
  97 dias restantes (expira: 2026-08-24T23:59:59.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2025-08-25T00:00:00.000Z
- INFO **Puerto 443**
  Conexion HTTPS establecida correctamente en puerto 443

Cabeceras de Seguridad — 35/100

Estado: FALLO

Solo 2/6 presentes. Faltan: Content-Security-Policy, X-Content-Type-Options, Referrer-Policy, Permissions-Policy

- 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; preload
- MEDIO **X-Content-Type-Options**
  Falta — Evita MIME-type sniffing
- 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://onlinebanking.bancogalicia.com.ar/
- INFO **HSTS (Strict-Transport-Security)**
  HSTS activo: max-age=31536000; includeSubDomains; preload
- 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
- 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)
- INFO **Archivo /README.txt**
  No accesible (correcto)
- MEDIO **Ruta /administrator/**
  Panel de login accesible publicamente

- INFO **Version CMS**
  No se detecta ninguna version expuesta

Seguridad de Cookies — 42/100

Estado: FALLO

Luke: falta HttpOnly; Luke: falta SameSite; R2D2: falta HttpOnly; R2D2: falta SameSite; __RequestVerificationToken: falta SameSite; f5_cspm: falta HttpOnly; f5_cspm: falta Secure; f5_cspm: falta SameSite; TS010dd3b2: falta HttpOnly; TS010dd3b2: falta Secure; TS010dd3b2: falta SameSite; TS017bfb32: falta HttpOnly; TS017bfb32: falta Secure; TS017bfb32: falta SameSite

- INFO **Cookies detectadas**
  8 cookie(s) encontrada(s)
- INFO **Cookie: ASP.NET_SessionId — HttpOnly**
  HttpOnly activo — No accesible via JavaScript
- INFO **Cookie: ASP.NET_SessionId — Secure**
  Flag Secure activo — Solo se envia por HTTPS
- INFO **Cookie: ASP.NET_SessionId — SameSite**
  SameSite=lax
- INFO **Cookie: ASP.NET_SessionId — HttpOnly**
  HttpOnly activo — No accesible via JavaScript
- INFO **Cookie: ASP.NET_SessionId — Secure**
  Flag Secure activo — Solo se envia por HTTPS
- INFO **Cookie: ASP.NET_SessionId — SameSite**
  SameSite=lax
- ALTO **Cookie: Luke — HttpOnly**
  Falta HttpOnly — Cookie accesible via document.cookie (riesgo XSS)
- INFO **Cookie: Luke — Secure**
  Flag Secure activo — Solo se envia por HTTPS
- MEDIO **Cookie: Luke — SameSite**
  Falta SameSite — Vulnerable a CSRF
- ALTO **Cookie: R2D2 — HttpOnly**
  Falta HttpOnly — Cookie accesible via document.cookie (riesgo XSS)
- INFO **Cookie: R2D2 — Secure**
  Flag Secure activo — Solo se envia por HTTPS
- MEDIO **Cookie: R2D2 — SameSite**
  Falta SameSite — Vulnerable a CSRF
- INFO **Cookie: __RequestVerificationToken — HttpOnly**
  HttpOnly activo — No accesible via JavaScript
- INFO **Cookie: __RequestVerificationToken — Secure**
  Flag Secure activo — Solo se envia por HTTPS
- MEDIO **Cookie: __RequestVerificationToken — SameSite**
  Falta SameSite — Vulnerable a CSRF
- ALTO **Cookie: f5_cspm — HttpOnly**
  Falta HttpOnly — Cookie accesible via document.cookie (riesgo XSS)
- ALTO **Cookie: f5_cspm — Secure**
  Falta flag Secure — Cookie se envia en conexiones HTTP
- MEDIO **Cookie: f5_cspm — SameSite**
  Falta SameSite — Vulnerable a CSRF
- ALTO **Cookie: TS010dd3b2 — HttpOnly**
  Falta HttpOnly — Cookie accesible via document.cookie (riesgo XSS)
- ALTO **Cookie: TS010dd3b2 — Secure**
  Falta flag Secure — Cookie se envia en conexiones HTTP
- MEDIO **Cookie: TS010dd3b2 — SameSite**
  Falta SameSite — Vulnerable a CSRF
- ALTO **Cookie: TS017bfb32 — HttpOnly**
  Falta HttpOnly — Cookie accesible via document.cookie (riesgo XSS)
- ALTO **Cookie: TS017bfb32 — Secure**
  Falta flag Secure — Cookie se envia en conexiones HTTP
- MEDIO **Cookie: TS017bfb32 — SameSite**
  Falta SameSite — Vulnerable a CSRF

Contenido Mixto — 60/100

Estado: AVISO

1 recurso(s) HTTP en pagina HTTPS

- MEDIO **Recurso HTTP (href (link/stylesheet))**
  http://www.bancogalicia.com/banca/online/web/Personas

Robots.txt y Sitemap — 20/100

Estado: FALLO

Faltan robots.txt y sitemap.xml

- BAJO **robots.txt**
  No encontrado (HTTP 404)
- 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] Content-Security-Policy: Falta esta cabecera que previene ataques de Cross-Site Scripting (XSS) e inyección de contenido malicioso.
[HIGH] Cookies sin flag HttpOnly (Luke, R2D2, f5_cspm, TS010dd3b2, TS017bfb32): Permite que scripts maliciosos accedan a las cookies, facilitando el robo de sesiones.
[HIGH] Cookies sin flag Secure (f5_cspm, TS010dd3b2, TS017bfb32): La información sensible se envía por conexiones no cifradas, exponiéndola a interceptación.
[MEDIUM] X-Content-Type-Options: La ausencia de esta cabecera permite el MIME-type sniffing, lo que puede derivar en la ejecución de archivos no autorizados.
[MEDIUM] Referrer-Policy: Falta de control sobre la información de procedencia enviada a otros dominios.
[MEDIUM] Permissions-Policy: No se restringen APIs del navegador como la cámara o el micrófono, aumentando la superficie de ataque.
[MEDIUM] Cookies sin flag SameSite (Luke, R2D2, __RequestVerificationToken, f5_cspm, TS010dd3b2, TS017bfb32): El sitio es vulnerable a ataques de Cross-Site Request Forgery (CSRF).
[MEDIUM] Ruta /administrator/ accesible: Panel de login expuesto públicamente, lo que facilita intentos de acceso no autorizado.
[MEDIUM] Contenido Mixto: Presencia de un recurso HTTP en una página HTTPS, comprometiendo la integridad de la conexión cifrada.

[LOW] robots.txt y sitemap.xml: No encontrados, lo que dificulta la gestión de indexación y visibilidad de la estructura del sitio.