

EscanearVulnerabilidades

Informe de Seguridad Web

URL https://bancoaurora.lat/r17/
Dominio bancoaurora.lat
Fecha 2 de octubre de 2026 a las 19:39

Checks 9 pruebas
Hallazgos 43 totales
Problemas 9 detectados

C

74/100

puntos de seguridad



RESUMEN EJECUTIVO

La auditoría de seguridad realizada al sitio web arrojó una puntuación de 74/100, lo que representa una calificación de grado C. El análisis se basó en 9 checks pasivos, de los cuales 6 resultaron satisfactorios, 2 presentaron advertencias y 1 fue identificado como fallo crítico. Aunque el cifrado de datos es robusto, la ausencia total de cabeceras de seguridad esenciales debilita significativamente la protección del usuario final. En su estado actual, el sitio se considera vulnerable a ataques de interceptación y manipulación de contenido en el lado del cliente.

Resumen de Riesgos



Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 164 dias
Cabeceras de Seguridad	0	FALLO	Solo 0/6 presentes. Faltan: Content-Security-Pol...
Redireccion HTTPS	70	AVISO	HTTP redirige a HTTPS pero falta HSTS
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	100	OK	No se encontraron cookies
Contenido Mixto	100	OK	No se detecto contenido mixto
Robots.txt y Sitemap	60	AVISO	Falta sitemap.xml
Puertos Abiertos	100	OK	2 puerto(s) abierto(s), todos esperados

SSL/TLS — 100/100

Estado: OK

Certificado valido, expira en 164 dias

- INFO Certificado valido
El certificado SSL es valido y de confianza
- INFO Dias hasta expiracion
164 dias restantes (expira: 2027-03-15T23:59:00Z)
- INFO Fecha de emision
Emitido desde: 2026-08-30T00:00:00.000Z
- INFO Puerto 443
Conexion HTTPS establecida correctamente en puerto 443

Cabeceras de Seguridad — 0/100

Estado: FALLO

Solo 0/6 presentes. Faltan: Content-Security-Policy, X-Frame-Options, Strict-Transport-Security, X-Content-Type-Options, Referrer-Policy, Permissions-Policy

- BAJO Server header expuesto
Server: gunicorn — Revela tecnologia del servidor

- ALTO

Content-Security-Policy
Falta — Previene XSS y ataques de inyeccion de contenido
- ALTO

X-Frame-Options
Falta — Protege contra clickjacking
- ALTO

Strict-Transport-Security
Falta — Fuerza conexiones HTTPS (HSTS)
- 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 — 70/100

Estado: AVISO

HTTP redirige a HTTPS pero falta HSTS

- INFO

HTTP !' HTTPS redireccion
HTTP 301 redirige a https://bancoaurora.lat/
- ALTO

HSTS (Strict-Transport-Security)
HSTS no configurado — El navegador no fuerza HTTPS
- 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 — 100/100

Estado: OK

No se encontraron cookies

INFO

Cookies detectadas
El sitio no establece cookies en la respuesta inicial

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 (39 bytes)

INFO

Reglas robots.txt
1 Disallow, 0 Allow

BAJO

sitemap.xml
No encontrado (HTTP 403)

BAJO

security.txt
No encontrado — Recomendado para politica de divulgacion

Puertos Abiertos — 100/100

Estado: OK
2 puerto(s) abierto(s), todos esperados

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)
Abierto (esperado) — Servidor web

INFO

Puerto 443 (HTTPS)
Abierto (esperado) — 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; es crítico para prevenir ataques de Cross-Site Scripting (XSS) e inyecciones de código malicioso.

[HIGH] X-Frame-Options: Falta; deja el sitio expuesto a ataques de clickjacking donde un atacante puede secuestrar clics del usuario.

[HIGH] Strict-Transport-Security: Falta; no se fuerza el mecanismo HSTS, permitiendo posibles degradaciones de conexión de HTTPS a HTTP.

[MEDIUM] X-Content-Type-Options: Falta; permite que el navegador realice MIME-type sniffing, lo que puede llevar a la ejecución de archivos no seguros.

[MEDIUM] Referrer-Policy: Falta; no se controla la información de navegación que se envía a otros dominios externos.

[MEDIUM] Permissions-Policy: Falta; el servidor no restringe el acceso del navegador a funciones sensibles como cámara, micrófono o geolocalización.

[LOW] Server header expuesto: El servidor revela el uso de gunicorn, facilitando a atacantes la identificación de tecnologías para buscar exploits específicos.

[LOW] Sitemap.xml: No encontrado o acceso denegado (403), lo que dificulta la indexación y auditoría de la estructura del sitio.