EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://www.bancoatlantida.com.sv/	Checks	9 pruebas
Dominio	www.bancoatlantida.com.sv	Hallazgos	44 totales
Fecha	11 de junio de 2026 a las 04:24	Problemas	7 detectados

B

80/100

puntos de seguridad

RESUMEN EJECUTIVO

El análisis de ciberseguridad realizado al portal web arroja una puntuación de 80/100 con una calificación final de B. Durante la auditoría se ejecutaron 9 checks pasivos, resultando en 7 validaciones exitosas y 2 fallos críticos relacionados con la configuración del servidor. El sitio demuestra un manejo excelente del cifrado de datos y la seguridad en el transporte, pero presenta deficiencias notables en la protección contra ataques de inyección y suplantación. En conclusión, el sitio web es mayoritariamente seguro, pero se considera vulnerable frente a amenazas modernas que aprovechan la falta de cabeceras de seguridad en el navegador.

Resumen de Riesgos

0	2	3	2	37
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 128 dias
Cabeceras de Seguridad	20	FALLO	Solo 1/6 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	100	OK	No se encontraron cookies
Contenido Mixto	100	OK	No se detecto contenido mixto
Robots.txt y Sitemap	20	FALLO	Faltan robots.txt y sitemap.xml
Puertos Abiertos	100	OK	2 puerto(s) abierto(s), todos esperados

SSL/TLS — 100/100

Estado: OK

Certificado valido, expira en 128 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
  128 dias restantes (expira: 2026-10-16T23:59:59.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2025-10-09T00:00:00.000Z
- INFO **Puerto 443**
  Conexion HTTPS establecida correctamente en puerto 443

Cabeceras de Seguridad — 20/100

Estado: FALLO

Solo 1/6 presentes. Faltan: Content-Security-Policy, X-Frame-Options, X-Content-Type-Options, Referrer-Policy, Permissions-Policy

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

- ALTO **X-Frame-Options**
  Falta — Protege contra clickjacking
- 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://www.bancoatlantida.com.sv/
- 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)
- 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 — 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

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 esta cabecera, lo que aumenta significativamente el riesgo de ataques XSS y la ejecución de contenido malicioso no autorizado.
[HIGH] X-Frame-Options: La ausencia de esta directiva hace que el portal sea susceptible a ataques de clickjacking, permitiendo que un atacante cargue el sitio en un marco invisible.

[MEDIUM] X-Content-Type-Options: Al no estar configurada, el navegador podría intentar interpretar el contenido de forma distinta a la declarada, facilitando ataques de MIME-sniffing.
[MEDIUM] Referrer-Policy: No se detectó una política de referencia, lo que puede provocar la filtración involuntaria de datos de navegación hacia sitios externos.
[MEDIUM] Permissions-Policy: La falta de esta cabecera impide restringir el acceso a funciones sensibles del hardware del usuario, como la cámara o el micrófono, desde el navegador.
[LOW] robots.txt: El archivo no fue encontrado (HTTP 404), lo que impide dar instrucciones claras a los rastreadores sobre qué áreas del sitio deben ser indexadas.
[LOW] sitemap.xml: La carencia de este archivo dificulta la comprensión de la estructura del sitio para los motores de búsqueda y auditorías de inventario de activos.