

Escanear Vulnerabilidades

Informe de Seguridad Web

URL https://www.100x100banco.com/
Dominio www.100x100banco.com
Fecha 11 de junio de 2026 a las 01:42

Checks 9 pruebas
Hallazgos 19 totales
Problemas 3 detectados

F

37/100

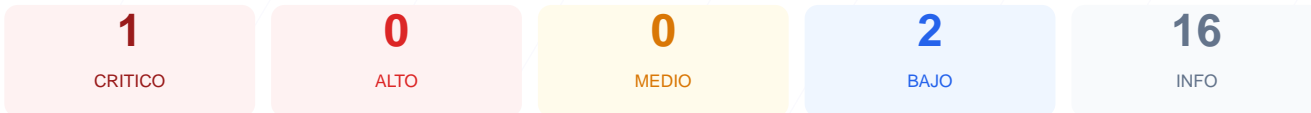
puntos de seguridad



RESUMEN EJECUTIVO

El análisis de ciberseguridad realizado al dominio arroja una puntuación de 37/100, lo que equivale a una nota de F. Durante la evaluación se ejecutaron 9 checks pasivos, de los cuales solo uno resultó exitoso, detectándose fallos críticos en el cifrado y la configuración básica del servidor. La ausencia de un certificado SSL válido y la imposibilidad de verificar cabeceras de seguridad fundamentales indican una postura defensiva inexistente. Debido a estos resultados, se concluye que el sitio es altamente vulnerable y no ofrece garantías mínimas de confidencialidad para sus usuarios.

Resumen de Riesgos



Resumen de Checks

SSL/TLS	0	FALLO	Certificado SSL no valido
Cabeceras de Seguridad	0	ERROR	No se pudieron verificar las cabeceras
Redireccion HTTPS	0	ERROR	No se pudo verificar la redireccion HTTPS
Deteccion CMS	0	ERROR	No se pudo analizar el CMS
Version CMS Expuesta	0	ERROR	No se pudo verificar la version del CMS
Seguridad de Cookies	0	ERROR	No se pudieron verificar las cookies
Contenido Mixto	0	ERROR	No se pudo verificar contenido mixto
Robots.txt y Sitemap	20	FALLO	Faltan robots.txt y sitemap.xml
Puertos Abiertos	100	OK	No se detectaron puertos abiertos

SSL/TLS — 0/100

Estado: FALLO

Certificado SSL no valido

- CRITICO** Certificado valido
El certificado SSL NO es valido
- INFO** Dias hasta expiracion
66 dias restantes (expira: 2026-08-15T19:44:55.000Z)
- INFO** Fecha de emision
Emitido desde: 2025-08-07T20:55:22.000Z
- INFO** Puerto 443
Conexion HTTPS establecida correctamente en puerto 443

Redireccion HTTPS — 0/100

Estado: ERROR

No se pudo verificar la redireccion HTTPS

- INFO** HTTP !' HTTPS redireccion
HTTP 301 redirige a https://www.100x100banco.com/

Robots.txt y Sitemap — 20/100

Estado: FALLO

Faltan robots.txt y sitemap.xml

- BAJO **robots.txt**
Error al acceder
- BAJO **sitemap.xml**
Error al acceder

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 — Envío 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 autenticación por defecto
- INFO **Puerto 8080 (HTTP-Alt)**
Cerrado — Servidor web alternativo / proxy
- INFO **Puerto 27017 (MongoDB)**
Cerrado — Base de datos MongoDB expuesta

Análisis de Seguridad

VULNERABILIDADES DETECTADAS

[CRITICAL] Certificado SSL no válido: El certificado SSL es inválido o no existe, lo que impide el cifrado de datos y permite la interceptación de información sensible por parte de terceros.

[MEDIUM] Error en Cabeceras de Seguridad: No se pudieron verificar las cabeceras de protección, lo que deja al servidor expuesto a ataques de inyección, clickjacking y otros vectores comunes de explotación web.

[MEDIUM] Fallo en Redirección HTTPS: No se ha podido confirmar el salto automático de HTTP a HTTPS, permitiendo potencialmente conexiones inseguras que exponen el tráfico del usuario.

[LOW] Ausencia de robots.txt: No se pudo acceder al archivo de directrices de rastreo, lo que dificulta la gestión técnica de la indexación en motores de búsqueda.

[LOW] Ausencia de sitemap.xml: El archivo de estructura del sitio no está presente o no es accesible, afectando la visibilidad y organización técnica de la plataforma.

[LOW] Error de verificación de cookies: La imposibilidad de analizar las cookies impide confirmar si cuentan con los atributos de seguridad Secure y HttpOnly necesarios para evitar el robo de sesiones.