

Escanear Vulnerabilidades

Informe de Seguridad Web

URL https://negocios.bravo.com.do/
Dominio negocios.bravo.com.do
Fecha 8 de mayo de 2026 a las 13:40

Checks 9 pruebas
Hallazgos 45 totales
Problemas 5 detectados

A

96/100

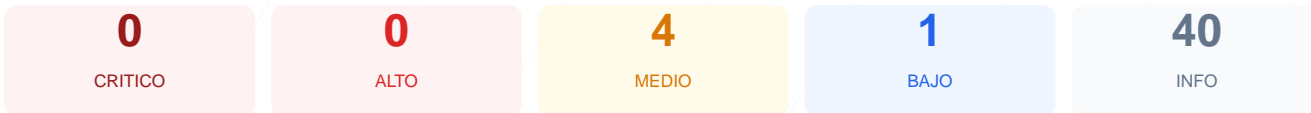
puntos de seguridad



RESUMEN EJECUTIVO

La auditoría de seguridad realizada al sitio negocios.bravo.com.do arroja una puntuación de 96/100, obteniendo una calificación de grado A. Durante el proceso se ejecutaron 9 checks pasivos, de los cuales 8 resultaron satisfactorios y únicamente uno presentó fallos técnicos. Aunque la infraestructura base es sólida, se han identificado hallazgos de severidad media relacionados con la exposición de rutas administrativas y archivos de información. En conclusión, el sitio se considera seguro en su configuración actual, pero presenta vectores de reconocimiento que deben ser mitigados para evitar ataques dirigidos.

Resumen de Riesgos



Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 65 dias
Cabeceras de Seguridad	100	OK	Todas las cabeceras de seguridad presentes
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	No se detectaron puertos abiertos

SSL/TLS — 100/100

Estado: OK

Certificado valido, expira en 65 dias

- INFO **Certificado valido**
El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
65 dias restantes (expira: 2026-07-12T18:32:53.000Z)
- INFO **Fecha de emision**
Emitido desde: 2026-04-13T17:38:40.000Z
- INFO **Puerto 443**
Conexion HTTPS establecida correctamente en puerto 443

Cabeceras de Seguridad — 100/100

Estado: OK

Todas las cabeceras de seguridad presentes

- BAJO **Server header expuesto**
Server: Google Frontend — Revela tecnologia del servidor

- INFO **Content-Security-Policy**
Presente: default-src 'self'; script-src 'self'; style-src 'self' 'unsafe-inline' https://...
- INFO **X-Frame-Options**
Presente: DENY
- INFO **Strict-Transport-Security**
Presente: max-age=31536000; includeSubDomains
- INFO **X-Content-Type-Options**
Presente: nosniiff
- INFO **Referrer-Policy**
Presente: strict-origin-when-cross-origin
- INFO **Permissions-Policy**
Presente: camera=(), microphone=(), geolocation=()

Redireccion HTTPS — 100/100

Estado: OK

HTTP redirige a HTTPS y HSTS esta habilitado

- INFO **HTTP !' HTTPS redireccion**
HTTP 301 redirige a https://negocios.bravo.com.do:443/
- INFO **HSTS (Strict-Transport-Security)**
HSTS activo: max-age=31536000; includeSubDomains
- 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**
React

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

- MEDIO** Ruta /administrator/
Panel de login accesible publicamente
- MEDIO** Ruta /user/login
Panel de login accesible publicamente
- 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

- INFO** security.txt
Presente en /.well-known/security.txt — Buena practica

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

[LOW] Server header expuesto: El encabezado Server revela el uso de Google Frontend, lo que facilita a un atacante identificar la tecnologia de infraestructura subyacente.

[MEDIUM] Archivo /readme.html: Este archivo es accesible públicamente y puede contener detalles sobre la versión y configuración interna del sistema.

[MEDIUM] Archivo /README.txt: El acceso público a este archivo de documentación puede filtrar información técnica innecesaria a terceros.

[MEDIUM] Ruta /administrator/ expuesta: El panel de acceso administrativo es visible desde internet, lo que permite intentos de acceso no autorizado o ataques de fuerza bruta.

[MEDIUM] Ruta /user/login expuesta: La interfaz de inicio de sesión de usuarios está abierta al público, aumentando la superficie de ataque para comprometer cuentas.

[FAIL] Ausencia de archivos de control: No se detectaron robots.txt ni sitemap.xml, lo que impide una gestión adecuada del rastreo por parte de motores de búsqueda.