

# Escanear Vulnerabilidades

Informe de Seguridad Web

URL https://vipweb.vv.com.br  
Dominio vipweb.vv.com.br  
Fecha 15 de junio de 2026 a las 00:30

Checks 9 pruebas  
Hallazgos 15 totales  
Problemas 3 detectados

# C

## 73/100

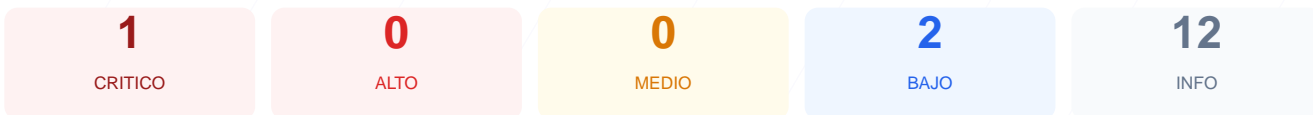
puntos de seguridad



### RESUMEN EJECUTIVO

El análisis de seguridad realizado al sitio web ha resultado en una puntuación de 73/100, lo que equivale a una nota de grado C. Durante la evaluación se ejecutaron 9 checks pasivos, identificando 1 resultado satisfactorio y 1 fallo crítico relacionado con la infraestructura de indexación y el cifrado. La imposibilidad de establecer una conexión SSL/TLS y verificar las cabeceras de seguridad sugiere una configuración de servidor deficiente. Debido a estos hallazgos, se concluye que el sitio es actualmente vulnerable y presenta riesgos significativos para la integridad de los datos de los usuarios. Se requiere una intervención técnica inmediata para elevar los estándares de protección del dominio.

### Resumen de Riesgos



### Resumen de Checks

SSL/TLS	0	ERROR	No se pudo verificar SSL/TLS
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: ERROR

No se pudo verificar SSL/TLS

- **CRITICO** **Conexion SSL**  
No se pudo establecer conexion SSL/TLS

### 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

## Analisis de Seguridad

---

### VULNERABILIDADES DETECTADAS

[CRITICAL] Conexión SSL/TLS: No se pudo establecer una conexión cifrada, lo que permite la interceptación de datos en tránsito por terceros.

[HIGH] Cabeceras de Seguridad: La falta de verificación de cabeceras indica que el sitio carece de protecciones contra ataques de inyección y clickjacking.

[HIGH] Redirección HTTPS: La ausencia de una redirección forzada expone a los usuarios a navegar por canales no seguros.

[LOW] Ausencia de robots.txt: No se pudo acceder al archivo de directrices para rastreadores, lo que puede resultar en la exposición de directorios sensibles.

[LOW] Ausencia de sitemap.xml: El error al acceder a este archivo dificulta la auditoría de la estructura del sitio y afecta el SEO técnico.

[MEDIUM] Seguridad de Cookies: No se pudo verificar la presencia de atributos Secure o HttpOnly, aumentando el riesgo de secuestro de sesiones.