

Escanear Vulnerabilidades

Informe de Seguridad Web

URL https://lirioinvitaciones.com/liliana-xv
Dominio lirioinvitaciones.com
Fecha 28 de abril de 2026 a las 19:46

Checks 9 pruebas
Hallazgos 47 totales
Problemas 5 detectados

A

90/100

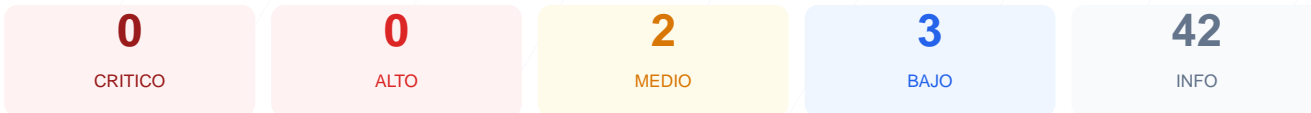
puntos de seguridad



RESUMEN EJECUTIVO

El análisis de seguridad del sitio web arroja una puntuación de 90/100, otorgando una nota final de A. Se ejecutaron 9 checks pasivos, de los cuales 6 resultaron satisfactorios, 2 presentaron advertencias y 1 se marcó como fallo técnico. La infraestructura muestra una base sólida con cifrado SSL óptimo y redirecciones correctas, aunque presenta carencias en cabeceras avanzadas y archivos de configuración. Se concluye que el sitio es seguro para la navegación, pero requiere ajustes menores para mitigar riesgos de privacidad y exposición de información técnica.

Resumen de Riesgos



Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 61 dias
Cabeceras de Seguridad	85	AVISO	5/6 presentes. Faltan: Permissions-Policy
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	67	AVISO	__cf_bm: falta SameSite
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 61 dias

- INFO **Certificado valido**
El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
61 dias restantes (expira: 2026-06-29T03:03:10.000Z)
- INFO **Fecha de emision**
Emitido desde: 2026-03-31T02:04:45.000Z
- INFO **Puerto 443**
Conexion HTTPS establecida correctamente en puerto 443

Cabeceras de Seguridad — 85/100

Estado: AVISO

5/6 presentes. Faltan: Permissions-Policy

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

- INFO **Content-Security-Policy**
Presente: frame-ancestors 'self' *.canva.com canva.com; report-uri https://csp.canva.com/_...
- INFO **X-Frame-Options**
Presente: SAMEORIGIN
- INFO **Strict-Transport-Security**
Presente: max-age=31536000
- INFO **X-Content-Type-Options**
Presente: nosniiff
- INFO **Referrer-Policy**
Presente: strict-origin-when-cross-origin
- 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 301 redirige a https://lirioinvitaciones.com/
- INFO **HSTS (Strict-Transport-Security)**
HSTS activo: max-age=31536000
- BAJO **HSTS includeSubDomains**
HSTS no 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

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 — 67/100

Estado: AVISO

__cf_bm: falta SameSite

- INFO **Cookies detectadas**
1 cookie(s) encontrada(s)
- INFO **Cookie: __cf_bm — HttpOnly**
HttpOnly activo — No accesible via JavaScript
- INFO **Cookie: __cf_bm — Secure**
Flag Secure activo — Solo se envía por HTTPS
- MEDIO **Cookie: __cf_bm — SameSite**
Falta SameSite — Vulnerable a CSRF

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

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 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

[MEDIUM] Permissions-Policy: La ausencia de esta cabecera impide restringir el uso de APIs del navegador como la cámara o el micrófono, lo que aumenta la superficie de ataque.

[MEDIUM] Cookie __cf_bm: Este elemento carece del atributo SameSite, lo que lo hace técnicamente vulnerable a ataques de falsificación de petición en sitios cruzados (CSRF).

[LOW] Server header expuesto: El servidor revela el uso de tecnología Cloudflare, proporcionando información técnica que facilita el reconocimiento por parte de atacantes.

[LOW] Ausencia de robots.txt: No se encontró el archivo en el servidor, lo que impide el control normativo sobre el rastreo de los motores de búsqueda.

[LOW] Ausencia de sitemap.xml: La falta de este recurso dificulta la indexación estructurada y el control de la arquitectura del sitio.