# EscanearVulnerabilidades

Informe de Seguridad Web

| | | | |
|---|---|---|---|
| URL | https://www.blinnova.uy | Checks | 9 pruebas |
| Dominio | www.blinnova.uy | Hallazgos | 46 totales |
| Fecha | 5 de mayo de 2026 a las 13:18 | Problemas | 14 detectados |

**D**

56/100

puntos de seguridad

## RESUMEN EJECUTIVO

El análisis de seguridad realizado sobre blinnova.uy arroja una puntuación de 56/100, lo que equivale a una calificación de grado D. Durante la auditoría se ejecutaron 9 comprobaciones pasivas, resultando en 4 verificaciones correctas, 3 advertencias y 2 fallos críticos. El sitio presenta deficiencias severas en la configuración de cabeceras de seguridad y mantiene software desactualizado expuesto públicamente. Debido a estos hallazgos y a la proximidad del vencimiento del certificado SSL, el sitio se clasifica actualmente como vulnerable.

## Resumen de Riesgos

| 0 | 6 | 6 | 2 | 32 |
|---|---|---|---|---|
| CRITICO | ALTO | MEDIO | BAJO | INFO |

## Resumen de Checks

| | | | |
|---|---|---|---|
| SSL/TLS | 50 | AVISO | Certificado expira en 7 dias |
| Cabeceras de Seguridad | 0 | FALLO | Solo 0/6 presentes. Faltan: Content-Security-Pol... |
| Redireccion HTTPS | 70 | AVISO | HTTP redirige a HTTPS pero falta HSTS |
| Deteccion CMS | 100 | OK | CMS detectado: WordPress, PrestaShop |
| Version CMS Expuesta | 20 | FALLO | WordPress 6.9.4 expuesta, WordPress 2 expuesta |
| Seguridad de Cookies | 100 | OK | No se encontraron cookies |
| Contenido Mixto | 60 | AVISO | 1 recurso(s) HTTP en pagina HTTPS |
| Robots.txt y Sitemap | 100 | OK | robots.txt y sitemap.xml presentes |
| Puertos Abiertos | 100 | OK | No se detectaron puertos abiertos |

## SSL/TLS — 50/100

Estado: AVISO

Certificado expira en 7 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- ALTO **Dias hasta expiracion**
  7 dias restantes (expira: 2026-05-12T23:59:59.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2026-02-11T00:00:00.000Z
- INFO **Puerto 443**
  Conexion HTTPS establecida correctamente en puerto 443

## Cabeceras de Seguridad — 0/100

Estado: FALLO

Solo 0/6 presentes. Faltan: Content-Security-Policy, X-Frame-Options, Strict-Transport-Security, X-Content-Type-Options, Referrer-Policy, Permissions-Policy

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

- ALTO **Content-Security-Policy**
  Falta — Previene XSS y ataques de inyeccion de contenido
- ALTO **X-Frame-Options**
  Falta — Protege contra clickjacking
- ALTO **Strict-Transport-Security**
  Falta — Fuerza conexiones HTTPS (HSTS)
- 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 — 70/100

Estado: AVISO

HTTP redirige a HTTPS pero falta HSTS

- INFO **HTTP !' HTTPS redireccion**
  HTTP 301 redirige a https://blinnova.uy/
- ALTO **HSTS (Strict-Transport-Security)**
  HSTS no configurado — El navegador no fuerza HTTPS
- INFO **Respuesta HTTPS**
  HTTPS responde con status 200

## Deteccion CMS — 100/100

Estado: OK

CMS detectado: WordPress, PrestaShop

- INFO **WordPress**
  Detectado via HTML body
- INFO **Joomla**
  No detectado
- INFO **Drupal**
  No detectado
- INFO **Magento**
  No detectado
- INFO **Shopify**
  No detectado
- INFO **PrestaShop**
  Detectado via HTML body
- INFO **Wix**
  No detectado
- INFO **Squarespace**
  No detectado
- BAJO **Meta generator**
  Expone: WordPress 6.9.4
- INFO **Tecnologias detectadas**
  Next.js

## Version CMS Expuesta — 20/100

Estado: FALLO

WordPress 6.9.4 expuesta, WordPress 2 expuesta

- ALTO **WordPress version**
  Version 6.9.4 expuesta publicamente — Permite a atacantes buscar CVEs conocidos
- MEDIO **Archivo /readme.html**
  Archivo accesible publicamente — Puede revelar version e informacion del CMS
- INFO **Archivo /README.txt**
  No accesible (correcto)

- MEDIO **Ruta /wp-login.php**
  Panel de login accesible publicamente

## 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 — 60/100

Estado: AVISO

1 recurso(s) HTTP en pagina HTTPS

- MEDIO **Recurso HTTP (href (link/stylesheet))**
  http://gmpg.org/xfn/11

## Robots.txt y Sitemap — 100/100

Estado: OK

robots.txt y sitemap.xml presentes

- INFO **robots.txt**
  Presente (169 bytes)
- INFO **Reglas robots.txt**
  1 Disallow, 0 Allow
- INFO **Sitemap en robots.txt**
  https://blinnova.uy/sitemap_index.xml
- 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 — 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

[HIGH] Expiración de Certificado SSL: El certificado TLS expira en solo 7 días, lo que provocará errores de conexión y pérdida de confianza de los usuarios.
[HIGH] Content-Security-Policy: La ausencia de esta cabecera facilita ataques de inyección de contenido y Cross-Site Scripting (XSS).
[HIGH] X-Frame-Options: La falta de esta protección permite ataques de clickjacking, donde un atacante puede superponer interfaces invisibles.
[HIGH] Strict-Transport-Security: No se ha configurado HSTS, lo que permite ataques de degradación de protocolo de HTTPS a HTTP.
[HIGH] Versión de WordPress Expuesta: Se detectó el uso de WordPress 6.9.4, lo que permite a atacantes buscar exploits específicos para esta versión.
[MEDIUM] X-Content-Type-Options: La falta de esta cabecera permite que el navegador intente adivinar el tipo de contenido, facilitando la ejecución de scripts maliciosos.
[MEDIUM] Referrer-Policy: No existe una política definida para controlar cuánta información se envía a otros sitios al navegar desde blinnova.uy.
[MEDIUM] Permissions-Policy: No se restringen las capacidades del navegador como la cámara, el micrófono o la ubicación a través de políticas de seguridad.
[MEDIUM] Archivo /readme.html expuesto: Este archivo es accesible y confirma detalles técnicos sobre la instalación del CMS.
[MEDIUM] Ruta /wp-login.php expuesta: El panel de administración es accesible públicamente, lo que facilita ataques de fuerza bruta.
[MEDIUM] Contenido Mixto: Se detectó un recurso (gmpg.org) cargando mediante HTTP inseguro dentro de la página protegida por HTTPS.
[LOW] Cabecera Server expuesta: El servidor revela el uso de Apache, ayudando a los atacantes en la fase de reconocimiento técnico.
[LOW] Meta generator: La etiqueta meta revela directamente la versión de WordPress empleada.