

# Escanear Vulnerabilidades

Informe de Seguridad Web

URL https://Guiamu.com.ar  
Dominio guiamu.com.ar  
Fecha 7 de mayo de 2026 a las 11:15

Checks 9 pruebas  
Hallazgos 48 totales  
Problemas 13 detectados

# C

## 65/100

puntos de seguridad



### RESUMEN EJECUTIVO

Tras realizar la auditoría técnica sobre el sitio web, se ha obtenido una puntuación de 65/100, lo que resulta en una nota C. El análisis se basó en 9 comprobaciones pasivas, resultando en 5 verificaciones correctas, 2 advertencias y 2 fallos críticos de configuración. Si bien la base del cifrado de datos es sólida, la ausencia total de cabeceras de seguridad y la gestión deficiente de cookies representan riesgos significativos. Concluimos que el sitio es actualmente vulnerable a ataques de inyección de contenido y secuestro de sesiones. Es imperativo aplicar medidas correctivas para elevar el estándar de protección.

### Resumen de Riesgos



### Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 59 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	No se detecto un CMS conocido
Version CMS Expuesta	100	OK	No se detecto version de CMS expuesta
Seguridad de Cookies	33	FALLO	PHPSESSID: falta Secure; PHPSESSID: falta SameSi...
Contenido Mixto	100	OK	No se detecto contenido mixto
Robots.txt y Sitemap	100	OK	robots.txt y sitemap.xml presentes
Puertos Abiertos	60	AVISO	1 puerto(s) potencialmente riesgoso(s): 8080 (HT...

### SSL/TLS — 100/100

Estado: OK

Certificado valido, expira en 59 dias

- INFO **Certificado valido**  
El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**  
59 dias restantes (expira: 2026-07-04T23:52:30.000Z)
- INFO **Fecha de emision**  
Emitido desde: 2026-04-05T23:52:31.000Z
- 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: cloudflare — 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://guiamu.com.ar/
- **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

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 — 33/100

---

Estado: FALLO

PHPSESSID: falta Secure; PHPSESSID: falta SameSite

- INFO **Cookies detectadas**  
1 cookie(s) encontrada(s)
- INFO **Cookie: PHPSESSID — HttpOnly**  
HttpOnly activo — No accesible via JavaScript
- ALTO **Cookie: PHPSESSID — Secure**  
Falta flag Secure — Cookie se envia en conexiones HTTP
- MEDIO **Cookie: PHPSESSID — 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 — 100/100

Estado: OK

robots.txt y sitemap.xml presentes

- INFO **robots.txt**  
Presente (1836 bytes)
- INFO **Reglas robots.txt**  
9 Disallow, 3 Allow
- MEDIO **Bloqueo total**  
robots.txt bloquea todo el sitio con Disallow: /
- BAJO **Ruta sensible en robots.txt**  
Referencia a "admin" — Puede revelar rutas sensibles a atacantes
- INFO **Sitemap en robots.txt**  
https://guiamu.com.ar/sitemap.xml
- BAJO **security.txt**  
No encontrado — Recomendado para politica de divulgacion

## Puertos Abiertos — 60/100

Estado: AVISO

1 puerto(s) potencialmente riesgoso(s): 8080 (HTTP-Alt)

- 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)**  
Abierto (esperado) — Servidor web
- INFO **Puerto 443 (HTTPS)**  
Abierto (esperado) — 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
- MEDIO **Puerto 8080 (HTTP-Alt)**  
ABIERTO — Servidor web alternativo / proxy



## Analisis de Seguridad

---

### VULNERABILIDADES DETECTADAS

- [HIGH] Content-Security-Policy: Falta — Previene XSS y ataques de inyección de contenido malicioso.
- [HIGH] X-Frame-Options: Falta — Protege a los usuarios contra ataques de clickjacking.
- [HIGH] Strict-Transport-Security: Falta — Impide que el navegador realice conexiones no cifradas mediante HSTS.
- [HIGH] Cookie PHPSESSID (Flag Secure): Falta — Permite que la cookie de sesión se envíe por canales HTTP inseguros.
- [MEDIUM] X-Content-Type-Options: Falta — Evita que el navegador interprete archivos de forma errónea mediante sniffing.
- [MEDIUM] Referrer-Policy: Falta — Controla la cantidad de información que el sitio comparte al navegar hacia otros enlaces.
- [MEDIUM] Permissions-Policy: Falta — No restringe el acceso del navegador a funciones sensibles como cámara o micrófono.
- [MEDIUM] Cookie PHPSESSID (Flag SameSite): Falta — Aumenta el riesgo de ataques de falsificación de petición en sitios cruzados (CSRF).
- [MEDIUM] Puerto 8080 abierto: El servicio HTTP-Alt está accesible, lo que supone un vector de ataque adicional.
- [MEDIUM] Bloqueo en robots.txt: La directiva Disallow impide la indexación general del contenido por motores de búsqueda.
- [LOW] Server header expuesto: Se revela el uso de Cloudflare, facilitando la fase de reconocimiento de un atacante.
- [LOW] Ruta sensible en robots.txt: La mención directa a la ruta de administración puede orientar ataques de fuerza bruta.