# EscanearVulnerabilidades

Informe de Seguridad Web

| | | | |
|---|---|---|---|
| URL | https://www.sagperu.com | Checks | 9 pruebas |
| Dominio | www.sagperu.com | Hallazgos | 45 totales |
| Fecha | 9 de septiembre de 2026 a las 17:57 | Problemas | 13 detectados |

C

68/100

puntos de seguridad

## RESUMEN EJECUTIVO

El análisis de seguridad realizado sobre el dominio arroja una puntuación de 68/100, lo que se traduce en una calificación de grado C. Durante la auditoría se ejecutaron 9 checks pasivos, de los cuales 5 resultaron satisfactorios, 2 generaron advertencias, 1 fue catalogado como fallo crítico y 1 sufrió un error de tiempo de espera. A pesar de contar con un certificado de cifrado válido, la configuración del servidor carece de las medidas de protección modernas necesarias para repeler ataques comunes. Por lo tanto, se concluye que el sitio es vulnerable ante ataques de inyección, suplantación de identidad y degradación de protocolos de seguridad.

## Resumen de Riesgos

| 0 | 4 | 5 | 4 | 32 |
|---|---|---|---|---|
| CRITICO | ALTO | MEDIO | BAJO | INFO |

## Resumen de Checks

| | | | |
|---|---|---|---|
| SSL/TLS | 100 | OK | Certificado valido, expira en 55 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 |
| Seguridad de Cookies | 100 | OK | No se encontraron cookies |
| Contenido Mixto | 60 | AVISO | 2 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 — 100/100

Estado: OK

Certificado valido, expira en 55 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
  55 dias restantes (expira: 2026-11-03T07:17:33.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2026-08-05T07:17:34.000Z
- 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
- BAJO **X-Powered-By expuesto**
  X-Powered-By: PHP/8.1.34 — Revela framework/lenguaje

- 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://www.sagperu.com/
- 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 7.1
- INFO **Tecnologias detectadas**
  Next.js, Astro, PHP/8.1.34

## 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

2 recurso(s) HTTP en pagina HTTPS

- MEDIO **Recurso HTTP (href (link/stylesheet))**
  http://recepcion@sagperu.com
- MEDIO **Recurso HTTP (href (link/stylesheet))**
  http://churchsupport@gmail.com

## Robots.txt y Sitemap — 100/100

Estado: OK

robots.txt y sitemap.xml presentes

- INFO **robots.txt**
  Presente (119 bytes)
- INFO **Reglas robots.txt**
  1 Disallow, 1 Allow
- BAJO **Ruta sensible en robots.txt**
  Referencia a "admin" — Puede revelar rutas sensibles a atacantes
- INFO **Sitemap en robots.txt**
  https://www.sagperu.com/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] Content-Security-Policy: La ausencia de esta cabecera permite la ejecución de scripts no autorizados y ataques de inyección de contenido (XSS).
[HIGH] X-Frame-Options: Falta de protección contra ataques de clickjacking, permitiendo que el sitio sea cargado dentro de marcos externos maliciosos.
[HIGH] Strict-Transport-Security: No se ha configurado HSTS, lo que deja a los usuarios expuestos a ataques de degradación de HTTPS a HTTP.
[MEDIUM] Contenido Mixto: Se detectaron 2 recursos cargados a través de conexiones no seguras (HTTP), lo que compromete la integridad de la navegación cifrada.
[MEDIUM] X-Content-Type-Options: La falta de esta cabecera permite que el navegador realice sniffing de tipos MIME, facilitando la ejecución de archivos maliciosos disfrazados.
[MEDIUM] Referrer-Policy: No existe una política definida para el control de la información de navegación que se envía a sitios externos mediante el referer.

[MEDIUM] Permissions-Policy: Ausencia de restricciones sobre el uso de APIs del navegador como la cámara, el micrófono o la geolocalización.
[LOW] Server header expuesto: El servidor revela el uso de tecnología Apache, proporcionando información útil para atacantes que busquen vulnerabilidades específicas de software.
[LOW] X-Powered-By expuesto: La cabecera revela el uso de PHP/8.1.34, lo que facilita la identificación de la infraestructura interna del sitio.
[LOW] Meta generator: El código fuente expone el uso de WordPress 7.1, permitiendo a los atacantes dirigir exploits conocidos para esa versión específica.
[LOW] Ruta sensible en robots.txt: El archivo menciona rutas de administración que pueden ser utilizadas para ataques de enumeración o fuerza bruta.