# EscanearVulnerabilidades

Informe de Seguridad Web

| | | | |
|---|---|---|---|
| URL | https://istpoxapampa.edu.pe/ | Checks | 9 pruebas |
| Dominio | istpoxapampa.edu.pe | Hallazgos | 45 totales |
| Fecha | 6 de mayo de 2026 a las 02:43 | Problemas | 11 detectados |

C

68/100

puntos de seguridad

## RESUMEN EJECUTIVO

El análisis de ciberseguridad realizado al sitio web ha arrojado una puntuación de 68/100, lo que equivale a una calificación de grado C. Se ejecutaron un total de 9 comprobaciones pasivas, de las cuales 6 resultaron satisfactorias, se registró una advertencia y se identificaron dos fallos críticos en la configuración. Aunque el cifrado de datos es correcto, la ausencia total de cabeceras de seguridad y el uso de software desactualizado representan un riesgo latente. En consecuencia, el sitio se considera actualmente vulnerable ante ataques dirigidos que podrían comprometer la integridad de la plataforma.

## Resumen de Riesgos

| 0 | 5 | 4 | 2 | 34 |
|---|---|---|---|---|
| CRITICO | ALTO | MEDIO | BAJO | INFO |

## Resumen de Checks

| | | | |
|---|---|---|---|
| SSL/TLS | 100 | OK | Certificado valido, expira en 48 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 | 100 | OK | No se detecto contenido mixto |
| 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 48 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
  48 dias restantes (expira: 2026-06-22T15:41:15.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2026-03-24T15:41:16.000Z
- 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

- 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://istpoxapampa.edu.pe/
- 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, Astro

## 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)

## 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 — 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 (269 bytes)
- INFO **Reglas robots.txt**
  4 Disallow, 1 Allow
- BAJO **Ruta sensible en robots.txt**
  Referencia a "admin" — Puede revelar rutas sensibles a atacantes
- INFO **Sitemap en robots.txt**
  https://istpoxapampa.edu.pe/wp-sitemap.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] Ausencia de Content-Security-Policy: La falta de esta política permite la ejecución de scripts maliciosos y ataques de inyección de contenido XSS.
[HIGH] Ausencia de X-Frame-Options: El sitio es susceptible a ataques de clickjacking al no restringir su visualización dentro de marcos o frames externos.

[HIGH] Ausencia de Strict-Transport-Security: No se obliga al navegador a utilizar conexiones seguras, lo que facilita ataques de degradación de protocolo.
[HIGH] Versión de WordPress expuesta: La versión 6.9.4 es visible públicamente, permitiendo a atacantes identificar y explotar vulnerabilidades conocidas en dicha versión.
[MEDIUM] Ausencia de X-Content-Type-Options: El servidor no previene que el navegador intente interpretar el tipo de contenido, aumentando el riesgo de ejecución de archivos peligrosos.
[MEDIUM] Ausencia de Referrer-Policy: No existe control sobre la información de procedencia enviada a otros dominios, lo que podría filtrar datos de navegación.
[MEDIUM] Ausencia de Permissions-Policy: No se restringe el acceso de las APIs del navegador a funciones sensibles como la cámara o el micrófono.
[MEDIUM] Archivo /readme.html accesible: Este archivo revela información técnica y detalles de la instalación del gestor de contenidos a cualquier usuario.
[LOW] Exposición de meta generator: El código fuente revela explícitamente el uso de WordPress 6.9.4, facilitando el reconocimiento para posibles intrusiones.
[LOW] Ruta sensible en robots.txt: Se hace referencia directa a directorios de administración, ayudando a los atacantes a mapear áreas restringidas del servidor.