EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://empleadospublicos.larioja.gob.ar	Checks	9 pruebas
Dominio	empleadospublicos.larioja.gob.ar	Hallazgos	46 totales
Fecha	27 de abril de 2026 a las 17:30	Problemas	14 detectados

C

62/100

puntos de seguridad

RESUMEN EJECUTIVO

El análisis de seguridad realizado sobre el portal empleadospublicos.larioja.gob.ar ha arrojado una puntuación de 62/100, lo que equivale a una calificación de grado C. Se han ejecutado 9 comprobaciones pasivas de las cuales 4 resultaron correctas, 3 generaron advertencias y 2 fallaron críticamente debido a la falta de protecciones en el servidor. El sitio web utiliza un certificado SSL válido, pero la exposición de versiones antiguas del software y la ausencia total de cabeceras de seguridad representan riesgos evitables. Concluyo que el sitio es actualmente vulnerable a ataques conocidos de interceptación de datos y explotación de vulnerabilidades de software desactualizado.

Resumen de Riesgos

0	5	7	2	32
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 58 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 6.0.1 expuesta
Seguridad de Cookies	100	OK	No se encontraron cookies
Contenido Mixto	60	AVISO	3 recurso(s) HTTP en pagina HTTPS
Robots.txt y Sitemap	60	AVISO	Falta robots.txt
Puertos Abiertos	100	OK	No se detectaron puertos abiertos

SSL/TLS — 100/100

Estado: OK

Certificado valido, expira en 58 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
  58 dias restantes (expira: 2026-06-24T12:55:06.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2026-03-26T12:55:07.000Z
- 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/2.4.58 (Ubuntu) — 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://empleadospublicos.larioja.gob.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

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
- INFO **Tecnologias detectadas**
  Next.js

Version CMS Expuesta — 20/100

Estado: FALLO

WordPress 6.0.1 expuesta

- ALTO **WordPress version**
  Version 6.0.1 expuesta publicamente — Permite a atacantes buscar CVEs conocidos
- INFO **Archivo /readme.html**
  No accesible (correcto)
- INFO **Archivo /README.txt**
  No accesible (correcto)
- MEDIO **Ruta /administrator/**
  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

3 recurso(s) HTTP en pagina HTTPS

- MEDIO **Recurso HTTP (href (link/stylesheet))**
  http://gmpg.org/xfn/11
- MEDIO **Recurso HTTP (href (link/stylesheet))**
  http://legislaturalarioja.gob.ar/
- MEDIO **Recurso HTTP (href (link/stylesheet))**
  http://www.justicialarioja.gob.ar/

Robots.txt y Sitemap — 60/100

Estado: AVISO

Falta robots.txt

- BAJO **robots.txt**
  No encontrado (HTTP 404)
- INFO **sitemap.xml**
  Presente, ? URLs
- 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] WordPress versión expuesta: Se detectó el uso de la versión 6.0.1, lo cual permite a potenciales atacantes identificar vulnerabilidades públicas conocidas (CVEs) para esta versión específica.
[HIGH] Ausencia de Content-Security-Policy: No existe una política de seguridad de contenido, dejando el sitio expuesto a ataques de Cross-Site Scripting (XSS) e inyecciones maliciosas.
[HIGH] Ausencia de X-Frame-Options: La falta de esta cabecera permite que el sitio sea embebido en marcos externos, facilitando ataques de clickjacking.
[HIGH] HSTS no configurado: La cabecera Strict-Transport-Security está ausente, lo que significa que el servidor no obliga al navegador a usar siempre conexiones seguras HTTPS.
[MEDIUM] Presencia de contenido mixto: Se han detectado 3 recursos cargados mediante HTTP dentro de la página protegida por HTTPS, lo que compromete la integridad de la sesión cifrada.
[MEDIUM] Ruta de administración accesible: El panel de login /administrator/ está disponible públicamente, lo que facilita intentos de acceso no autorizado por fuerza bruta.
[MEDIUM] Ausencia de X-Content-Type-Options: El sitio no previene el sniffing de tipos MIME, lo que podría permitir que el navegador ejecute archivos con formatos incorrectos de forma maliciosa.
[MEDIUM] Cabeceras de privacidad ausentes: No se han configurado Referrer-Policy ni Permissions-Policy para controlar la información enviada a terceros o restringir el uso de APIs del navegador.
[LOW] Cabecera de servidor expuesta: El servidor revela el uso de Apache/2.4.58 (Ubuntu), proporcionando información valiosa a atacantes sobre la infraestructura subyacente.
[LOW] Falta de archivo robots.txt: No se encontró este archivo, lo que impide definir reglas claras para los rastreadores web y puede exponer directorios que no deberían indexarse.