

Escanear Vulnerabilidades

Informe de Seguridad Web

URL <https://resultadoelectoral.onpe.gob.pe/>
Dominio resultadoelectoral.onpe.gob.pe
Fecha 21 de abril de 2026 a las 18:54

Checks 9 pruebas
Hallazgos 45 totales
Problemas 6 detectados

A

96/100

puntos de seguridad



RESUMEN EJECUTIVO

La auditoría de seguridad realizada al sitio web ha arrojado una puntuación de 96/100 con una calificación de nota A. Se ejecutaron 9 controles pasivos, obteniendo 8 resultados satisfactorios y 1 fallo relacionado con la gestión de archivos de indexación. Aunque el cifrado y las cabeceras de respuesta son excelentes, se identificaron múltiples rutas de administración y archivos técnicos accesibles de forma pública. En conclusión, el sitio es seguro en sus capas de transporte y políticas de cabeceras, pero presenta vulnerabilidades de exposición de información que deben ser corregidas.

Resumen de Riesgos



Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 298 dias
Cabeceras de Seguridad	100	OK	Todas las cabeceras de seguridad presentes
Redireccion HTTPS	100	OK	HTTP redirige a HTTPS y HSTS esta habilitado
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	100	OK	No se encontraron cookies
Contenido Mixto	100	OK	No se detecto contenido mixto
Robots.txt y Sitemap	20	FALLO	Faltan robots.txt y sitemap.xml
Puertos Abiertos	100	OK	2 puerto(s) abierto(s), todos esperados

SSL/TLS — 100/100

Estado: OK

Certificado valido, expira en 298 dias

- INFO **Certificado valido**
El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
298 dias restantes (expira: 2027-02-14T05:39:36.000Z)
- INFO **Fecha de emision**
Emitido desde: 2026-02-14T05:39:36.000Z
- INFO **Puerto 443**
Conexion HTTPS establecida correctamente en puerto 443

Cabeceras de Seguridad — 100/100

Estado: OK

Todas las cabeceras de seguridad presentes

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

- INFO **Content-Security-Policy**
Presente: default-src 'self' blob:; frame-src 'self' blob: https://www.google.com https://...
- INFO **X-Frame-Options**
Presente: SAMEORIGIN
- INFO **Strict-Transport-Security**
Presente: max-age=31536000
- INFO **X-Content-Type-Options**
Presente: nosniiff
- INFO **Referrer-Policy**
Presente: strict-origin-when-cross-origin
- INFO **Permissions-Policy**
Presente: camera=(), microphone=(), geolocation=(), payment=(), usb=()

Redireccion HTTPS — 100/100

Estado: OK

HTTP redirige a HTTPS y HSTS esta habilitado

- INFO **HTTP !' HTTPS redireccion**
HTTP 301 redirige a https://resultadoelectoral.onpe.gob.pe/
- INFO **HSTS (Strict-Transport-Security)**
HSTS activo: max-age=31536000
- **BAJO** **HSTS includeSubDomains**
HSTS no cubre subdominios
- INFO **HSTS max-age**
max-age=31536000 (365 dias)
- 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

- **MEDIO** **Archivo /readme.html**
Archivo accesible publicamente — Puede revelar version e informacion del CMS
- **MEDIO** **Archivo /README.txt**
Archivo accesible publicamente — Puede revelar version e informacion del CMS
- **MEDIO** **Ruta /wp-login.php**
Panel de login accesible publicamente

- MEDIO** Ruta /administrator/
Panel de login accesible publicamente
- MEDIO** Ruta /user/login
Panel de login accesible publicamente
- INFO** Version CMS
No se detecta ninguna version expuesta

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 — 20/100

Estado: FALLO

Faltan robots.txt y sitemap.xml

- INFO** security.txt
Presente en /.well-known/security.txt — Buena practica

Puertos Abiertos — 100/100

Estado: OK

2 puerto(s) abierto(s), todos esperados

- 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
- 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

[LOW] Server header expuesto: La cabecera revela el uso de CloudFront, lo cual facilita el reconocimiento de la infraestructura tecnologica por parte de terceros.

[MEDIUM] Archivo /readme.html expuesto: Este archivo es accesible públicamente y puede revelar detalles técnicos o versiones del sistema subyacente.

[MEDIUM] Archivo /README.txt expuesto: La disponibilidad de este archivo permite a un atacante obtener información sobre la configuración o el desarrollo del sitio.

[MEDIUM] Ruta /wp-login.php accesible: El panel de acceso está expuesto a Internet, lo que aumenta el riesgo de ataques automatizados de fuerza bruta.

[MEDIUM] Ruta /administrator/ accesible: La exposición de este directorio administrativo representa un vector de ataque para intentos de acceso no autorizado.

[MEDIUM] Ruta /user/login accesible: La visibilidad pública del formulario de ingreso de usuarios facilita el compromiso potencial de credenciales.

[FAIL] Ausencia de robots.txt y sitemap.xml: La falta de estos archivos impide un control adecuado sobre el rastreo de motores de búsqueda y la estructura del sitio.