EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://identidad.reniec.gob.pe/	Checks	9 pruebas
Dominio	identidad.reniec.gob.pe	Hallazgos	42 totales
Fecha	16 de abril de 2026 a las 21:16	Problemas	4 detectados

B

88/100

puntos de seguridad

RESUMEN EJECUTIVO

La auditoría de seguridad realizada al sitio web arroja una puntuación de 88/100 con una calificación de grado B. El análisis se basó en 9 checks pasivos ejecutados, de los cuales 5 resultaron satisfactorios, identificando 1 advertencia y 1 fallo en las configuraciones de seguridad. El sitio presenta una base sólida en cuanto a cifrado SSL y gestión de cookies, pero muestra carencias en cabeceras de seguridad y visibilidad de archivos de indexación. Se concluye que el sitio es generalmente seguro para el usuario, aunque presenta vulnerabilidades de configuración técnica que deben ser subsanadas para prevenir ataques dirigidos.

Resumen de Riesgos

0	0	2	2	38
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 84 dias
Cabeceras de Seguridad	75	AVISO	4/6 presentes. Faltan: Referrer-Policy, Permissi...
Redireccion HTTPS	0	ERROR	No se pudo verificar la redireccion HTTPS
Deteccion CMS	100	OK	No se detecto un CMS conocido
Seguridad de Cookies	100	OK	2 cookies, todas con flags correctos
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	No se detectaron puertos abiertos

SSL/TLS — 100/100

Estado: OK

Certificado valido, expira en 84 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
  84 dias restantes (expira: 2026-07-09T23:59:59.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2025-06-27T00:00:00.000Z
- INFO **Puerto 443**
  Conexion HTTPS establecida correctamente en puerto 443

Cabeceras de Seguridad — 75/100

Estado: AVISO

4/6 presentes. Faltan: Referrer-Policy, Permissions-Policy

- INFO **Content-Security-Policy**
  Presente: default-src 'self'; script-src 'self' https: 'unsafe-inline' 'unsafe-eval'; styl...
- INFO **X-Frame-Options**
  Presente: SAMEORIGIN, SAMEORIGIN

- INFO **Strict-Transport-Security**
  Presente: max-age=31536000; includeSubDomains
- INFO **X-Content-Type-Options**
  Presente: nosniff, nosniff
- MEDIO **Referrer-Policy**
  Falta — Controla la informacion de referer enviada
- MEDIO **Permissions-Policy**
  Falta — Restringe APIs del navegador (camara, micro, etc.)

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
- INFO **Tecnologias detectadas**
  React, Next.js

Seguridad de Cookies — 100/100

Estado: OK

2 cookies, todas con flags correctos

- INFO **Cookies detectadas**
  2 cookie(s) encontrada(s)
- INFO **Cookie: JSESSIONID — HttpOnly**
  HttpOnly activo — No accesible via JavaScript
- INFO **Cookie: JSESSIONID — Secure**
  Flag Secure activo — Solo se envia por HTTPS
- INFO **Cookie: JSESSIONID — SameSite**
  SameSite=strict
- INFO **Cookie: SERVER_ID — HttpOnly**
  HttpOnly activo — No accesible via JavaScript
- INFO **Cookie: SERVER_ID — Secure**
  Flag Secure activo — Solo se envia por HTTPS
- INFO **Cookie: SERVER_ID — SameSite**
  SameSite=strict

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

- BAJO **robots.txt**
  No encontrado (HTTP 403)
- BAJO **sitemap.xml**
  No encontrado (HTTP 403)
- 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

[MEDIUM] Referrer-Policy: La ausencia de esta cabecera impide controlar qué información de procedencia se envía a otros sitios, lo que podría exponer datos sensibles en la URL.
[MEDIUM] Permissions-Policy: Falta esta cabecera que restringe el acceso a APIs del navegador como cámara, micrófono y geolocalización, aumentando el riesgo ante posibles inyecciones de código.
[LOW] robots.txt: El archivo no fue encontrado o el acceso fue denegado (HTTP 403), lo que dificulta la gestión de los rastreadores de motores de búsqueda.
[LOW] sitemap.xml: No se detectó un mapa del sitio (HTTP 403), afectando la transparencia de la estructura del sitio para herramientas de auditoría y búsqueda.
[ERROR] Redirección HTTPS: No se pudo verificar la redirección automática de tráfico inseguro a seguro, lo que podría permitir conexiones vulnerables a ataques de intermediario.