EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://larioja.gob.ar	Checks	9 pruebas
Dominio	larioja.gob.ar	Hallazgos	43 totales
Fecha	27 de abril de 2026 a las 17:47	Problemas	11 detectados

C

64/100

puntos de seguridad

RESUMEN EJECUTIVO

El análisis de seguridad realizado al dominio arroja una puntuación de 64/100 con una calificación de C. Se ejecutaron un total de 9 checks pasivos, resultando en 5 verificaciones satisfactorias, 2 advertencias y 2 fallos críticos en la configuración. El estado actual revela una carencia total de cabeceras de seguridad esenciales y un riesgo inminente por la expiración del certificado SSL. Debido a estas deficiencias técnicas en la protección del canal de comunicación, el sitio se considera vulnerable ante ataques de interceptación y suplantación de identidad.

Resumen de Riesgos

0	5	3	3	32
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	50	AVISO	Certificado expira en 6 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	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	No se detectaron puertos abiertos

SSL/TLS — 50/100

Estado: AVISO

Certificado expira en 6 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- ALTO **Dias hasta expiracion**
  6 dias restantes (expira: 2026-05-03T23:59:59.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2025-05-07T00:00:00.000Z
- 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

- 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://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

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, Astro

Version CMS Expuesta — 100/100

Estado: OK

No se detecto version de CMS expuesta

- INFO **Archivo /readme.html**
  No accesible (correcto)
- INFO **Archivo /README.txt**
  No accesible (correcto)
- 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

- BAJO **robots.txt**
  No encontrado (HTTP 404)
- BAJO **sitemap.xml**
  No encontrado (HTTP 404)
- 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] Expiración de Certificado SSL: El certificado expira en 6 días, lo que provocará alertas de seguridad a los usuarios y posible inaccesibilidad.
[HIGH] Ausencia de Content-Security-Policy (CSP): No existe protección contra ataques de inyección de contenido o Cross-Site Scripting (XSS).
[HIGH] Ausencia de X-Frame-Options: El sitio es vulnerable a ataques de clickjacking al permitir que el contenido sea embebido en otros marcos.
[HIGH] Ausencia de Strict-Transport-Security (HSTS): El servidor no instruye al navegador para usar exclusivamente conexiones HTTPS, permitiendo ataques de degradación.
[MEDIUM] Ausencia de X-Content-Type-Options: El navegador podría intentar interpretar el tipo de contenido de forma incorrecta, facilitando la ejecución de scripts maliciosos.
[MEDIUM] Ausencia de Referrer-Policy: No se controla la cantidad de información que el navegador envía al navegar hacia otros enlaces.
[MEDIUM] Ausencia de Permissions-Policy: No se restringen las funcionalidades del navegador como la cámara, micrófono o geolocalización.
[LOW] Exposición de cabecera Server: Se revela el uso de Apache, lo que facilita a un atacante identificar vulnerabilidades específicas de esa tecnología.

[LOW] Ausencia de archivos de control: No se encontraron los archivos robots.txt ni sitemap.xml, necesarios para la gestión adecuada de rastreo.