# EscanearVulnerabilidades

Informe de Seguridad Web

| | | | |
|---|---|---|---|
| URL | https://atd.qroo.gob.mx | Checks | 9 pruebas |
| Dominio | atd.qroo.gob.mx | Hallazgos | 12 totales |
| Fecha | 17 de septiembre de 2026 a las 16:02 | Problemas | 0 detectados |

**A**

100/100

puntos de seguridad

## RESUMEN EJECUTIVO

El sitio web analizado ha obtenido una puntuacion de 100/100 con una nota de A en nuestra evaluacion de seguridad. Se ejecutaron un total de 9 checks pasivos, de los cuales 1 resulto satisfactorio y no se registraron advertencias ni fallos. Debido a la ausencia de vulnerabilidades detectadas y la correcta proteccion de los puertos, el portal se clasifica actualmente como seguro. Es importante destacar que la calificacion maxima refleja la falta de hallazgos negativos, a pesar de las limitaciones tecnicas encontradas durante el escaneo. Se recomienda mantener esta postura de seguridad robusta mediante revisiones periodicas.

## Resumen de Riesgos

| 0 | 0 | 0 | 0 | 12 |
|---|---|---|---|---|
| CRITICO | ALTO | MEDIO | BAJO | INFO |

## Resumen de Checks

| | | | |
|---|---|---|---|
| Cabeceras de Seguridad | 0 | ERROR | No se pudieron verificar las cabeceras |
| Redireccion HTTPS | 0 | ERROR | No se pudo verificar la redireccion HTTPS |
| Deteccion CMS | 0 | ERROR | No se pudo analizar el CMS |
| Version CMS Expuesta | 0 | ERROR | No se pudo verificar la version del CMS |
| Seguridad de Cookies | 0 | ERROR | No se pudieron verificar las cookies |
| Contenido Mixto | 0 | ERROR | No se pudo verificar contenido mixto |
| Puertos Abiertos | 100 | OK | No se detectaron puertos abiertos |

## 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**

No se detectaron vulnerabilidades durante el escaneo pasivo realizado.
Los hallazgos del PentestAgent no muestran CWEs, endpoints de API descubiertos, subdominios expuestos ni cabeceras faltantes debido a que las pruebas no arrojaron vectores de ataque explotables.