# EscanearVulnerabilidades

Informe de Seguridad Web

| | | | |
|---|---|---|---|
| URL | https://portal.azure.com/?ocid=AIDcmmxy57gu5y_SEM__k_CjwKCAjw1vXTBhB-EiwAFKr_k5Oq9WgmVu_4kFkZyXHMM1C6gILNS1jZCcwqSW4JtZWWnumlzrynLBoC_gYQAvD_BwE_k_#allservices/category/All | Checks | 9 pruebas |
| Dominio | portal.azure.com | Hallazgos | 41 totales |
| Fecha | 13 de agosto de 2026 a las 15:22 | Problemas | 10 detectados |

C

61/100

puntos de seguridad

## RESUMEN EJECUTIVO

El analisis de seguridad realizado sobre el portal arroja una puntuacion de 61/100, lo que equivale a una nota C. Durante la evaluacion se ejecutaron 9 checks pasivos, de los cuales 6 resultaron satisfactorios y 3 presentaron fallos criticos de configuracion. La ausencia de cabeceras de seguridad esenciales y problemas en la redireccion HTTPS afectan negativamente el resultado. Aunque el cifrado de datos es correcto, la carencia de politicas de proteccion en el navegador compromete la integridad del sitio. En su estado actual, la plataforma se considera vulnerable ante ataques de intermediacion e inyeccion.

## Resumen de Riesgos

| 0 | 5 | 3 | 2 | 31 |
|---|---|---|---|---|
| CRITICO | ALTO | MEDIO | BAJO | INFO |

## Resumen de Checks

| | | | |
|---|---|---|---|
| SSL/TLS | 100 | OK | Certificado valido, expira en 145 dias |
| Cabeceras de Seguridad | 0 | FALLO | Solo 0/6 presentes. Faltan: Content-Security-Pol... |
| Redireccion HTTPS | 0 | FALLO | No hay redireccion HTTP a HTTPS |
| 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 145 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
  145 dias restantes (expira: 2027-01-05T19:53:18.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2026-07-09T19:53:18.000Z
- 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

- 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 — 0/100

Estado: FALLO

No hay redireccion HTTP a HTTPS

- ALTO **HTTP !' HTTPS redireccion**
  HTTP 403 — No redirige a HTTPS
- ALTO **HSTS (Strict-Transport-Security)**
  HSTS no configurado — El navegador no fuerza HTTPS
- INFO **Respuesta HTTPS**
  HTTPS responde con status 403

## 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

- 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 403)
- BAJO **sitemap.xml**
  No encontrado (HTTP 403)
- BAJO **security.txt**
  No encontrado — Recomendado para politica de divulgacion

## 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**

[HIGH] Content-Security-Policy: Falta esta cabecera, lo que permite la ejecucion de ataques XSS y la inyeccion de contenido malicioso en el navegador.
[HIGH] X-Frame-Options: La ausencia de esta directiva deja el sitio expuesto a ataques de clickjacking, permitiendo que sea embebido en marcos externos.
[HIGH] Strict-Transport-Security: No se ha configurado HSTS, por lo que el navegador no fuerza conexiones seguras de manera automatica.
[HIGH] Redireccion HTTPS: El servidor devuelve un error 403 en peticiones HTTP y no redirige el trafico hacia la version cifrada HTTPS.
[MEDIUM] X-Content-Type-Options: La falta de esta cabecera permite el MIME-type sniffing, aumentando el riesgo de ejecucion de scripts no autorizados.
[MEDIUM] Referrer-Policy: No existe una politica que controle la informacion de procedencia enviada a otros dominios, lo que afecta la privacidad.
[MEDIUM] Permissions-Policy: No se restringen las APIs del navegador, permitiendo potencialmente el acceso a funciones sensibles como camara o microfono.
[LOW] robots.txt: El archivo de reglas para buscadores no fue encontrado o devuelve un error de acceso 403.
[LOW] sitemap.xml: No se localizo el mapa del sitio, lo que dificulta la indexacion y el analisis de la estructura web.