# EscanearVulnerabilidades

Informe de Seguridad Web

| | | | |
|---|---|---|---|
| URL | https://www.tigo.com.sv | Checks | 9 pruebas |
| Dominio | www.tigo.com.sv | Hallazgos | 49 totales |
| Fecha | 10 de mayo de 2026 a las 23:37 | Problemas | 9 detectados |

**B**

89/100

puntos de seguridad

## RESUMEN EJECUTIVO

La auditoria de seguridad realizada al sitio tigo.com.sv arrojo una puntuacion de 89/100, lo que corresponde a una nota B. El analisis consistio en la ejecucion de 9 checks pasivos, de los cuales 6 resultaron satisfactorios y 3 generaron advertencias de seguridad. No se detectaron fallos criticos, destacando un excelente desempeño en el cifrado SSL y la redireccion HTTPS. No obstante, la presencia de contenido mixto y configuraciones de cabeceras incompletas impiden una calificacion perfecta. En conclusion, el sitio se considera seguro para el usuario final, aunque presenta vulnerabilidades de severidad media que deben ser mitigadas para prevenir ataques de interceptacion o reconocimiento.

## Resumen de Riesgos

| 0 | 0 | 7 | 2 | 40 |
|---|---|---|---|---|
| CRITICO | ALTO | MEDIO | BAJO | INFO |

## Resumen de Checks

| | | | |
|---|---|---|---|
| SSL/TLS | 100 | OK | Certificado valido, expira en 270 dias |
| Cabeceras de Seguridad | 85 | AVISO | 5/6 presentes. Faltan: Permissions-Policy |
| 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 | 60 | AVISO | 3 recurso(s) HTTP en pagina HTTPS |
| Robots.txt y Sitemap | 100 | OK | robots.txt y sitemap.xml presentes |
| Puertos Abiertos | 60 | AVISO | 1 puerto(s) potencialmente riesgoso(s): 8080 (HT... |

## SSL/TLS — 100/100

Estado: OK

Certificado valido, expira en 270 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
  270 dias restantes (expira: 2027-02-04T23:59:59.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2026-01-13T00:00:00.000Z
- INFO **Puerto 443**
  Conexion HTTPS establecida correctamente en puerto 443

## Cabeceras de Seguridad — 85/100

Estado: AVISO

5/6 presentes. Faltan: Permissions-Policy

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

- INFO **Content-Security-Policy**
  Presente: default-src 'self' wss: wss://*.ooklaserver.net https://*.tigocloud.net https://...
- INFO **X-Frame-Options**
  Presente: SAMEORIGIN
- INFO **Strict-Transport-Security**
  Presente: max-age=0; includeSubDomains
- INFO **X-Content-Type-Options**
  Presente: nosniff
- INFO **Referrer-Policy**
  Presente: same-origin
- MEDIO **Permissions-Policy**
  Falta — Restringe APIs del navegador (camara, micro, etc.)

## Redireccion HTTPS — 100/100

Estado: OK

HTTP redirige a HTTPS y HSTS esta habilitado

- INFO **HTTP !' HTTPS redireccion**
  HTTP 301 redirige a https://www.tigo.com.sv/
- INFO **HSTS (Strict-Transport-Security)**
  HSTS activo: max-age=0; includeSubDomains
- BAJO **HSTS includeSubDomains**
  HSTS cubre subdominios
- MEDIO **HSTS max-age**
  max-age=0 (0 dias) — Recomendado minimo 180 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

- 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 — 60/100

Estado: AVISO

3 recurso(s) HTTP en pagina HTTPS

- MEDIO **Recurso HTTP (href (link/stylesheet))**
  http://b.tigo.com/MTData2
- MEDIO **Recurso HTTP (href (link/stylesheet))**
  http://b.tigo.com/MTData2
- MEDIO **Recurso HTTP (href (link/stylesheet))**
  http://b.tigo.com/MTData2

## Robots.txt y Sitemap — 100/100

Estado: OK

robots.txt y sitemap.xml presentes

- INFO **robots.txt**
  Presente (4470 bytes)
- INFO **Reglas robots.txt**
  62 Disallow, 2 Allow
- MEDIO **Bloqueo total**
  robots.txt bloquea todo el sitio con Disallow: /
- BAJO **Ruta sensible en robots.txt**
  Referencia a "admin" — Puede revelar rutas sensibles a atacantes
- INFO **Sitemap en robots.txt**
  https://www.tigo.com.sv/sitemap.xml
- BAJO **security.txt**
  No encontrado — Recomendado para politica de divulgacion

## Puertos Abiertos — 60/100

Estado: AVISO

1 puerto(s) potencialmente riesgoso(s): 8080 (HTTP-Alt)

- 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

- MEDIO **Puerto 8080 (HTTP-Alt)**
  ABIERTO — Servidor web alternativo / proxy
- INFO **Puerto 27017 (MongoDB)**
  Cerrado — Base de datos MongoDB expuesta

## Analisis de Seguridad

**VULNERABILIDADES DETECTADAS**

[MEDIUM] Permissions-Policy: La cabecera esta ausente, lo que impide restringir el acceso del navegador a APIs sensibles como la camara, el microfono o la geolocalizacion.
[LOW] Server header expuesto: Se detecto la cabecera Server: cloudflare, lo cual revela informacion sobre la infraestructura tecnologica y facilita el reconocimiento por parte de atacantes.
[MEDIUM] HSTS max-age: La directiva HSTS tiene un valor de 0 dias, invalidando la proteccion que obliga al navegador a usar siempre conexiones seguras en futuras visitas.
[MEDIUM] Recurso HTTP (Contenido Mixto): Se identificaron 3 llamadas a recursos bajo el protocolo inseguro HTTP (http://b.tigo.com/MTData2), lo que permite ataques de hombre en el medio.
[MEDIUM] Bloqueo total en robots.txt: El archivo bloquea la indexacion de todo el sitio mediante Disallow: /, lo cual puede afectar la visibilidad y ocultar estructuras de directorios de forma ineficiente.
[LOW] Ruta sensible en robots.txt: Se hace referencia a la ruta admin, lo que proporciona a potenciales atacantes pistas directas sobre la ubicacion de paneles de administracion.
[MEDIUM] Puerto 8080 (HTTP-Alt) abierto: Este puerto suele utilizarse para servicios web secundarios o de administracion y representa una superficie de ataque adicional si no esta debidamente protegido.