

Escanear Vulnerabilidades

Informe de Seguridad Web

URL	https://es.t-mobile.com/_smetrics_t-mobile_com/ee/va6/v1/interact?configId=...-b3054e0ebas
Dominio	es.t-mobile.com
Fecha	12 de septiembre de 2026 a las 16:26
Problemas	8 detectados

C

69/100

puntos de seguridad

RESUMEN EJECUTIVO

El análisis de seguridad técnica realizado al sitio web arroja una puntuación de 69/100, lo que corresponde a una calificación de grado C. Se completaron 9 comprobaciones pasivas de las cuales 7 resultaron satisfactorias y 2 presentaron fallos críticos de configuración. A pesar de contar con un cifrado de conexión válido, la infraestructura carece de protecciones esenciales contra ataques de interceptación y suplantación. Debido a la ausencia de cabeceras de seguridad fundamentales, el sitio se considera vulnerable y requiere intervención inmediata para mitigar riesgos de integridad.

Resumen de Riesgos

0	3	4	1	38
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 139 dias
Cabeceras de Seguridad	20	FALLO	Solo 1/6 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	100	OK	robots.txt y sitemap.xml presentes
Puertos Abiertos	100	OK	2 puerto(s) abierto(s), todos esperados

SSL/TLS — 100/100

Estado: OK

Certificado valido, expira en 139 dias

- INFO Certificado valido
El certificado SSL es valido y de confianza
- INFO Dias hasta expiracion
139 dias restantes (expira: 2027-01-29T23:59:59.000Z)
- INFO Fecha de emision
Emitido desde: 2026-01-30T00:00:00.000Z
- INFO Puerto 443
Conexion HTTPS establecida correctamente en puerto 443

Cabeceras de Seguridad — 20/100

Estado: FALLO

Solo 1/6 presentes. Faltan: Content-Security-Policy, X-Frame-Options, 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
- INFO

Strict-Transport-Security
Presente: max-age=31536000 ; preload
- 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 dirige a HTTPS
- INFO

HSTS (Strict-Transport-Security)
HSTS activo: max-age=31536000 ; preload
- BAJO

HSTS includeSubDomains
HSTS no cubre subdominios
- INFO

HSTS max-age
max-age=31536000 (365 días)
- 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 — 100/100

Estado: OK

robots.txt y sitemap.xml presentes

- INFO **robots.txt**
Presente (3501 bytes)
- INFO **Reglas robots.txt**
53 Disallow, 1 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://es.t-mobile.com/sitemap.xml>
- INFO **security.txt**
Presente en /.well-known/security.txt — Buena practica

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: La ausencia de esta cabecera facilita ataques de inyección de código y Cross-Site Scripting (XSS) al no restringir el origen del contenido.

[HIGH] X-Frame-Options: El sitio es susceptible a ataques de clickjacking, permitiendo que un atacante cargue la página en marcos invisibles para engañar al usuario.

[HIGH] Redirección HTTP a HTTPS: No existe una transición automática hacia la conexión segura y el servidor devuelve errores 403, lo que compromete la disponibilidad y el cifrado del tráfico.

[MEDIUM] X-Content-Type-Options: La falta de esta directiva permite el MIME-type sniffing, lo que podría llevar al navegador a ejecutar archivos con contenido malicioso oculto.

[MEDIUM] Referrer-Policy: No se define el control de la información de procedencia, lo que puede exponer datos de navegación privados a dominios de terceros.

[MEDIUM] Permissions-Policy: El sitio no restringe el acceso a APIs del navegador como la cámara, micrófono o ubicación, aumentando la superficie de exposición.

[MEDIUM] Divulgación en robots.txt: El archivo expone la ruta "admin", proporcionando a posibles atacantes información sobre la ubicación de directorios internos sensibles.