

Escanear Vulnerabilidades

Informe de Seguridad Web

URL https://digitec.com.ec
Dominio digitec.com.ec
Fecha 5 de mayo de 2026 a las 20:31

Checks 9 pruebas
Hallazgos 44 totales
Problemas 11 detectados

C

61/100

puntos de seguridad



RESUMEN EJECUTIVO

El análisis de ciberseguridad realizado al dominio digitec.com.ec arroja una puntuación de 61/100, lo que representa una nota de C. Tras la ejecución de 9 comprobaciones pasivas, el sistema determinó que 6 resultaron satisfactorias, 1 presenta advertencias y 2 presentan fallos críticos. La ausencia total de cabeceras de seguridad y la falta de redirección automática hacia protocolos cifrados comprometen la integridad de la comunicación con el usuario. Debido a estas omisiones técnicas en la configuración del servidor, el sitio se clasifica actualmente como vulnerable ante ataques de interceptación y secuestro de clics.

Resumen de Riesgos



Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 45 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	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 45 dias

- INFO **Certificado valido**
El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
45 dias restantes (expira: 2026-06-20T01:33:02.000Z)
- INFO **Fecha de emision**
Emitido desde: 2026-03-22T00:34:25.000Z
- 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: cloudflare — 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 — 0/100

Estado: **FALLO**

No hay redireccion HTTP a HTTPS

- **ALTO** **HTTP !' HTTPS redireccion**
HTTP 521 — No redirige a HTTPS
- **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

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 (1806 bytes)
- INFO **Reglas robots.txt**
9 Disallow, 2 Allow
- MEDIO **Bloqueo total**
robots.txt bloquea todo el sitio con Disallow: /
- INFO **Sitemap en robots.txt**
https://digitec.com.ec/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

[HIGH] Content-Security-Policy: Falta esta cabecera fundamental para prevenir ataques de ejecución de scripts maliciosos (XSS) e inyección de datos.

[HIGH] X-Frame-Options: Su ausencia permite que el sitio sea embebido en marcos externos, facilitando ataques de clickjacking.

[HIGH] Strict-Transport-Security: No se ha configurado HSTS, lo que impide que el navegador fuerce conexiones seguras de forma permanente.

[HIGH] Redirección HTTP a HTTPS: El servidor no redirige el tráfico no cifrado automáticamente, devolviendo un error HTTP 521 en el proceso.

[MEDIUM] Puerto 8080 (HTTP-Alt): Este puerto se encuentra abierto, lo que representa un vector de ataque adicional al exponer un servicio alternativo.

[MEDIUM] X-Content-Type-Options: Al faltar esta cabecera, el navegador podría interpretar archivos de forma incorrecta mediante el sniffing de tipos MIME.

[MEDIUM] Referrer-Policy: No existe control sobre la información de referencia que el sitio envía a otros dominios al navegar.

[MEDIUM] Permissions-Policy: No se restringen las capacidades del navegador como el acceso a cámara, micrófono o geolocalización.

[MEDIUM] Bloqueo en robots.txt: El archivo de configuración bloquea la indexación total del sitio, lo que puede ser una configuración errónea de visibilidad.

[LOW] Server header expuesto: La cabecera revela el uso de tecnología Cloudflare, proporcionando pistas sobre la infraestructura a posibles atacantes.