

# Escanear Vulnerabilidades

Informe de Seguridad Web

URL https://aserta.com.mx  
Dominio aserta.com.mx  
Fecha 27 de mayo de 2026 a las 14:30

Checks 9 pruebas  
Hallazgos 18 totales  
Problemas 3 detectados

# F

## 37/100

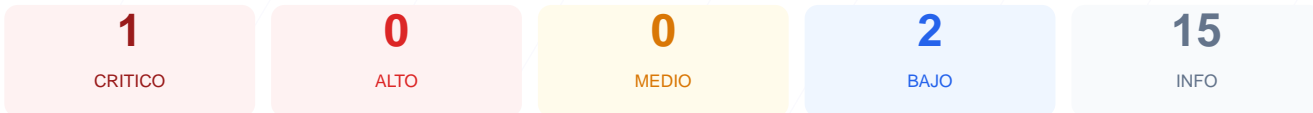
puntos de seguridad



### RESUMEN EJECUTIVO

La auditoría de seguridad realizada al dominio aserta.com.mx arrojó una puntuación crítica de 37/100, lo que corresponde a una calificación de grado F. Se ejecutaron 9 comprobaciones pasivas, de las cuales solo una resultó exitosa, mientras que se identificaron dos fallos críticos en la infraestructura básica y múltiples errores de acceso. La imposibilidad de validar el cifrado de datos y las cabeceras de seguridad fundamentales representa un riesgo alto para la integridad de los usuarios. En su estado actual, el sitio web se considera vulnerable y no cumple con los estándares mínimos de ciberseguridad industrial.

### Resumen de Riesgos



### Resumen de Checks

SSL/TLS	0	FALLO	Certificado SSL no valido
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
Robots.txt y Sitemap	20	FALLO	Faltan robots.txt y sitemap.xml
Puertos Abiertos	100	OK	1 puerto(s) abierto(s), todos esperados

### SSL/TLS — 0/100

Estado: FALLO

Certificado SSL no valido

- CRITICO** Certificado valido  
El certificado SSL NO es valido
- INFO** Dias hasta expiracion  
117 dias restantes (expira: 2026-09-21T23:59:59.000Z)
- INFO** Fecha de emision  
Emitido desde: 2025-08-21T00:00:00.000Z
- INFO** Puerto 443  
Conexion HTTPS establecida correctamente en puerto 443

### Robots.txt y Sitemap — 20/100

Estado: FALLO

Faltan robots.txt y sitemap.xml

- BAJO** robots.txt  
Error al acceder

## Puertos Abiertos — 100/100

---

Estado: OK

1 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 — Envío de correo
- **INFO** **Puerto 80 (HTTP)**  
Cerrado — 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 autenticación 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

[CRÍTICA] Certificado SSL no válido: El certificado de seguridad ha fallado las pruebas de validación, lo que significa que la comunicación entre el usuario y el servidor no está cifrada y puede ser interceptada.

[BAJA] Archivo robots.txt ausente o inaccesible: El sitio no proporciona instrucciones a los motores de búsqueda, lo que puede exponer rutas sensibles o afectar el indexado.

[BAJA] Archivo sitemap.xml ausente o inaccesible: La falta de un mapa del sitio dificulta la auditoría de la estructura web y la navegación de servicios legítimos de rastreo.