EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://www.santander.com.ar/personas	Checks	9 pruebas
Dominio	www.santander.com.ar	Hallazgos	16 totales
Fecha	18 de agosto de 2026 a las 21:53	Problemas	0 detectados

A

100/100

puntos de seguridad

RESUMEN EJECUTIVO

El análisis técnico de ciberseguridad realizado sobre el sitio web ha arrojado una puntuación perfecta de 100/100, lo que corresponde a una nota de A. Durante la evaluación se ejecutaron un total de 9 checks pasivos, obteniendo 2 resultados exitosos y ningún registro de advertencias o fallos de seguridad. La ausencia de hallazgos negativos en las pruebas realizadas indica que la superficie de exposición analizada cumple con los estándares de protección requeridos. Se concluye que el sitio es actualmente seguro bajo los parámetros de la auditoría pasiva.

Resumen de Riesgos

0	0	0	0	16
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

Robots.txt y Sitemap	100	OK	robots.txt y sitemap.xml presentes
Puertos Abiertos	100	OK	2 puerto(s) abierto(s), todos esperados

Robots.txt y Sitemap — 100/100

Estado: OK

robots.txt y sitemap.xml presentes

- INFO **robots.txt**
  Presente (439 bytes)
- INFO **Reglas robots.txt**
  11 Disallow, 0 Allow
- INFO **Sitemap en robots.txt**
  https://www.santander.com.ar/api/sitemap
- 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

No se detectaron vulnerabilidades durante el escaneo pasivo de seguridad. El sistema no presenta fallos de configuración en los puertos analizados ni exposición indebida de archivos de indexación. Al no haberse detectado CWEs, headers faltantes o endpoints expuestos en esta fase, el reporte de hallazgos se mantiene limpio.