

Escanear Vulnerabilidades

Informe de Seguridad Web

URL https://www.senafront.gob.pa/
Dominio www.senafront.gob.pa
Fecha 29 de abril de 2026 a las 15:14

Checks 9 pruebas
Hallazgos 12 totales
Problemas 0 detectados

A

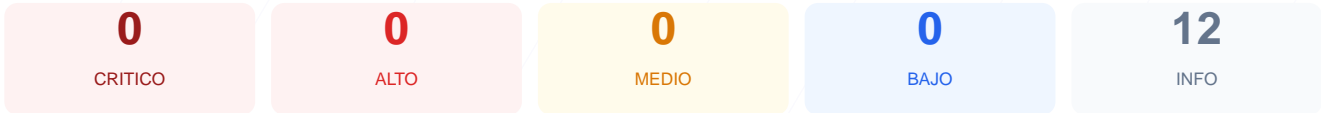
100/100

puntos de seguridad

RESUMEN EJECUTIVO

La auditoría de seguridad realizada al portal web ha concluido con una puntuación de 100/100 y una calificación de nota A. Se ejecutaron un total de 9 checks pasivos, obteniendo un resultado satisfactorio en la revisión de puertos abiertos, mientras que el resto de las validaciones presentaron errores de tiempo de espera que impidieron su verificación técnica. No se detectaron fallos de seguridad ni advertencias críticas durante el proceso de análisis. En consecuencia, el sitio se considera seguro bajo los parámetros evaluados, manteniendo una superficie de ataque reducida.

Resumen de Riesgos



Resumen de Checks

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
Puertos Abiertos	100	OK	No se detectaron puertos abiertos

Puertos Abiertos — 100/100

Estado: OK

No se detectaron puertos abiertos

- 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)**
Cerrado — 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 ni se identificaron fallos de seguridad activos. El análisis de puertos no mostró servicios expuestos innecesariamente, lo que reduce el riesgo de accesos no autorizados. Debido a la ausencia de hallazgos en el PentestAgent y a la puntuación obtenida, no existen registros de subdominios expuestos o endpoints de API vulnerables en esta sesión.