**Informe Final de Alcance**

**Proyecto PlatSentinel – Plataforma Modular de Seguridad como Servicio (SaaS)**  
*(Compilado a partir de toda la conversación y del contenido completo del archivo PlatSentinel.zip)*

**1. Resumen ejecutivo**

PlatSentinel es una **plataforma SaaS de ciberseguridad modular** que orquesta, en una única consola web, un catálogo de micro‑servicios (“tokens”) ejecutados en contenedores Docker.  
La solución está orientada a:

* **MSPs, equipos de soporte técnico y PYMEs reguladas** que precisan más que un antivirus pero menos que un SOC completo.
* **Integradores y fabricantes** que desean exponer sus propias herramientas como micro‑servicios plug‑and‑play.

El presente informe define con detalle **alcance, arquitectura, módulos, roadmap y recomendaciones de mejora**, condensando la información de los nueve documentos Word y las iteraciones de diseño realizadas en el chat.

**2. Objetivos del proyecto**

| **Nº** | **Objetivo** | **Métrica de éxito** |
| --- | --- | --- |
| 1 | Centralizar la operación de seguridad en un panel único | 90 % de tareas resueltas desde el dashboard |
| 2 | Desplegar servicios en **tokens Docker** aislados | MTTR < 20 min; rollback instantáneo |
| 3 | Ofrecer **control remoto** vía API y canal WhatsApp/App | Latencia comando‑respuesta ≤ 5 s |
| 4 | Entregar la plataforma **sin instalar agentes** en el cliente | 0 software persistente en endpoints |
| 5 | Facilitar integración de terceros (marketplace) | ≥ 25 partners certificados en 18 meses |

**3. Alcance funcional**

**3.1 Módulos (tokens) incluidos en la fase MVP**

| **Categoría** | **Token** | **Descripción breve** |
| --- | --- | --- |
| Análisis de red | token.nmap | Descubrimiento de puertos y servicios |
| Análisis web | token.nikto | Detección de vulnerabilidades HTTP |
| Malware | token.virustotal | Hash lookup en VT y sandbox opcional |
| Vulnerabilidades | token.openvas | Escaneo CVE sobre rangos definidos |
| Respuesta | token.firewall‑isolate | Bloqueo IP/host a demanda |
| Backup | token.backup‑s3 | Copia rápida en almacenamiento S3 |
| Inteligencia | token.threat‑intel | IOCs diarios desde feeds OSINT |

*(Derivado de* ***herramientas2.docx*** *y* ***planificaciónydiseño.docx****)*

**3.2 Servicios de plataforma**

* **API REST/JSON** v1 – todas las acciones del GUI están expuestas.
* **Dashboard web** (React + Tailwind) – multitenant, login MFA.
* **Bot WhatsApp Business** – comandos /scan, /report, /isolate, etc.
* **App móvil (Flutter)** –  idéntico flujo que WhatsApp para quienes no usen ese canal.
* **Motor de orquestación** – Kubernetes ligero; auto‑escala tokens.

**3.3 Fuera de alcance (v1)**

* Integración nativa con entornos OT/ICS – planificada para la fase 2026.
* Soporte de cumplimiento específico (PCI‑DSS, HIPAA) – se ofrecerá via partners.

**4. Arquitectura técnica**

[ Cliente / App / WhatsApp ]

│ (HTTPS / WebSocket / Cloud API)

▼

┌───────────────┐

│ API Gateway │ ↔ OAuth2 / JWT

└───────────────┘

│

▼

┌───────────────────────────┐

│ Orquestador de Tokens │──► Lanza contenedores Docker en pool

└───────────────────────────┘

│

▼

┌───────────────┐

│ Backend │─┬─► Postgres (meta)

│ (FastAPI) │ │ Redis (colas)

└───────────────┘ │ MinIO (artefactos)

│ │

▼ ▼

┌───────────────┐ ┌───────────────┐

│ Dashboard UI │ │ Integraciones │ (SIEM, EDR, Jira…)

└───────────────┘ └───────────────┘

* Arranque medio de un token: **1,2 s** (medido en pruebas de carga)
* Consumo RAM medio: **150 MB**/token
* RPO backups – 15 min; RTO tokens críticos – < 5 min

*(Basado en* ***Arquitectura\_Modular\_PlatSentinel.docx*** *y* ***planificaciónydiseño.docx****)*

**5. Estructura de carpetas (repositorio)**

PlatSentinel/

├── api/ # FastAPI 3.1

│ ├── auth/ # OAuth2

│ ├── tokens/ # Catálogo + logs

│ └── integrations/ # Slack, Jira, SIEM

├── engine/ # Schedulers y workers

├── tokens/ # Contenedores Docker

│ ├── core/ # Soporte oficial

│ └── partners/ # Marketplace

├── ui/ # React/Tailwind

└── docs/ # Arquitectura, guías, IaC

**6. Plan de proyecto**

| **Fase** | **Periodo** | **Entregables** | **Hitos** |
| --- | --- | --- | --- |
| **Kick‑off** | Ago 2025 | Documento alcance (este informe) | Equipo multidisciplinar asignado |
| **Desarrollo MVP** | Sep–Dic 2025 | API, dashboard, 6 tokens, bot WhatsApp | Demo funcional |
| **Pilotos controlados** | Ene–Mar 2026 | 3 clientes piloto, métricas MTTR | Informe de mejoras |
| **Marketplace & IA** | Abr–Jul 2026 | Portal de partners, scoring predictivo | 10 tokens externos |
| **Expansión LATAM/APAC** | Ago 2026– | Localización, soporte multi‑idioma | 25 partners & 5 MSPs |

**7. Análisis de mercado (síntesis)**

* Mercado global mid‑market ≈ **42 Bn USD** (2024), CAGR 12 %.
* Brecha clara entre “antivirus doméstico” y “SOC Premium” → oportunidad.
* Factores de adopción: **escalabilidad**, pago por uso, **soporte remoto**.
* Regulaciones (NIS2, DORA, LGPD‑BR) empujan a contratación de servicios gestionados.

**8. Riesgos y mitigaciones**

| **Riesgo** | **Impacto** | **Prob.** | **Mitigación** |
| --- | --- | --- | --- |
| Fallo en un token crítico | Medio | Bajo | Health‑checks + reinicio automático |
| Sobrecoste cloud | Medio | Medio | Auto‑escalado + spot instances |
| Brecha API | Alto | Bajo | WAF + pruebas DAST continuas |
| Reticencia a WhatsApp | Bajo | Medio | App móvil con misma API |

**9. Recomendaciones de mejora (próximos 12 meses)**

1. **Zero‑Trust by design**: incorporar mTLS entre tokens y backend.
2. **Firma de contenedores (Cosign)** para garantizar integridad.
3. **Módulo ML** que correlacione eventos y proponga runbooks automáticos.
4. **Terraform‑provider oficial** → despliegue en infra híbrida de clientes grandes.
5. **Dashboards pre‑construidos** en Grafana/ELK exportables para auditorías.
6. **Programa de certificación de partners** con pruebas funcionales y sello “PlatSentinel‑Ready”.

**10. Conclusión**

El alcance aquí definido coloca a PlatSentinel como una **plataforma SaaS modular, extensible y orientada a la acción**, capaz de:

* Reducir drásticamente la complejidad operativa de las PYMEs.
* Permitir a los equipos de soporte técnico **activar, medir y remediar** sin cambiar de consola.
* Escalar con el negocio, gracias a una arquitectura de tokens Docker orquestados y a un modelo “pay‑as‑you‑grow”.

Con la hoja de ruta y las recomendaciones descritas, PlatSentinel queda preparado para su fase de piloto y posterior comercialización a gran escala.

**Fin del informe**