**🎯 SentinelCore**

**Seguridad Unificada con Toquens Dockerizados y Gestión Multimodal**

🗓 Fecha: [Tu fecha de presentación]  
👥 Audiencia: Equipo directivo, técnico y socios tecnológicos  
📍 Elaborado por: [Nombre del equipo]

**📌 Slide 1: Visión General**

* Plataforma SaaS modular de ciberseguridad.
* Tokens dockerizados y especializados.
* Comunicación dual: Dashboard Web + WhatsApp API.
* Activación remota de servicios internos y externos.
* Diseñada para servicios técnicos y PYMEs.

**📌 Slide 2: Problemas Detectados**

❌ Soluciones genéricas no se adaptan a las necesidades de PYMEs.  
❌ Falta de integración entre herramientas técnicas.  
❌ Comunicación lenta con el cliente ante incidencias.  
❌ Dificultad para escalar servicios técnicos.

**📌 Slide 3: Solución SentinelCore**

✅ Plataforma cloud-native accesible por navegador o WhatsApp.  
✅ Toquens independientes por tipo de análisis.  
✅ Activación y respuesta rápida desde dispositivos móviles.  
✅ Panel centralizado para técnicos y consultores.  
✅ Integración con servicios cloud y fabricantes.

**📊 Slide 4: Análisis de Mercado**

**Gráfico sugerido: mapa de calor o tabla comparativa por región**

| **Región** | **Crecimiento Ciberseguridad (CAGR 2025)** | **Oportunidad** |
| --- | --- | --- |
| Norteamérica | 12% | Alta demanda de SaaS técnico |
| Europa | 9% | Cumplimiento normativo (GDPR) |
| Asia-Pacífico | 15% | Alto crecimiento PYME digital |
| Latinoamérica | 11% | Alta adopción de WhatsApp, soluciones ágiles |

**🎯 Mercados clave: España, México, Colombia**

**🧠 Slide 5: Innovación Técnica**

* **Toquens dockerizados:** contenedores con lógica independiente.
* **Toquen de antesala:** analiza antes de almacenar.
* **WhatsApp Business API:** para alertas y respuestas inmediatas.
* **Activación de servicios externos:** ej. ClamAV Cloud, AWS Defender.
* **Estructura modular y escalable.**

**🛠️ Slide 6: Arquitectura General**

**Gráfico sugerido: Diagrama en capas o flujo modular**

plaintext

CopiarEditar

[Usuario: Dashboard / WhatsApp]

↓

[Dispatcher (API)]

↓

[Toquen de Antesala] → [Toquens Especializados] → [Mitigación] → [Informe + Notificación]

↓

[Integraciones: ClamAV, AWS, etc]

**📁 Slide 7: Estructura Técnica del Proyecto**

plaintext

CopiarEditar

sentinelcore/

├── api/ # API REST

├── core/ # Dispatcher, lógica

├── toquens/ # Dockerizados: PDF, Office, ClamAV...

├── partners/ # Integraciones externas

├── frontend/ # Vue.js Dashboard

├── whatsapp\_integration/ # Twilio API

├── reports/ # Informes PDF/HTML

├── docker/ # Dockerfiles

└── docker-compose.yml

📌 Cada toquen tiene lógica y despliegue independiente. Escalable.

**📈 Slide 8: Roadmap Técnico**

**Gráfico sugerido: Línea de tiempo horizontal**

* **Fase Alpha (0–2 meses):** ZAP, Toquens PDF, API WhatsApp
* **Fase Beta (2–5 meses):** Multicliente, dashboard, onboarding partners
* **Lanzamiento (6 meses):** multiidioma, Kubernetes, informes LLM

**📊 Slide 9: Comparativa Técnica**

**Gráfico sugerido: Barras comparativas**

| **Característica** | **Solución A** | **Solución B** | **SentinelCore** |
| --- | --- | --- | --- |
| Tokens independientes | ❌ | ❌ | ✅ Docker |
| Comunicación WhatsApp | ❌ | ❌ | ✅ API |
| Activación remota | ⚠️ | ❌ | ✅ |
| Integración partners | ❌ | ⚠️ | ✅ (AWS, ClamAV) |
| Rendimiento archivos/hora | 3,200 | 5,100 | **8,500** |

**🔄 Slide 10: Casos de Uso Reales**

**🏥 Clínica Dental**

* Problema: gestión de PDFs clínicos vulnerables
* Solución: detección automática, bloqueo y notificación por WhatsApp
* Resultado: 0 incidentes en 6 meses

**🛠️ MSP (Servicio Técnico)**

* 15 webs WordPress en mantenimiento
* Escaneo semanal automático con alertas vía WhatsApp
* Activación de parches desde panel

**🧩 Slide 11: Integraciones y Extensiones**

* 🔌 Integración con AWS Security Hub
* 🔌 ClamAV Cloud API
* 🔌 Soporte para plataformas externas (Azure, GCP)
* 🔁 Módulos adaptables según necesidades del cliente

**📚 Slide 12: Formación y Módulo Educativo**

* Simulaciones de ataques OWASP
* Recomendaciones MITRE ATT&CK
* Generador de informes guiado
* Manuales interactivos para técnicos
* Modo laboratorio para formación continua

**🛡️ Slide 13: Seguridad por Diseño**

**Gráfico sugerido: tabla o esquema de capas de seguridad**

| **Capa** | **Protección** |
| --- | --- |
| Comunicación | TLS 1.3 |
| Autenticación | OAuth2 + MFA |
| Contenedores | Sandboxing con gVisor |
| Datos | Encriptación AES-256 reposo/transito |

**💬 Slide 14: Preguntas Frecuentes**

* **¿Qué pasa si cae WhatsApp API?**  
  Backup por Telegram o canal web.
* **¿Dónde se almacenan los datos?**  
  Preferentemente en memoria; encriptado si persiste.
* **¿Soporta cumplimiento normativo?**  
  Sí: GDPR, HIPAA, LGPD.

**🧪 Slide 15: Demo Técnica en Vivo**

* Subida de archivo malicioso
* Detección por toquen
* Notificación inmediata por WhatsApp
* Activación de servicio externo desde el panel
* Generación de informe + logging

**📌 Slide 16: Conclusión**

✅ Seguridad enterprise sin necesidad de infraestructura.  
✅ Tokens aislados, escalables y fáciles de mantener.  
✅ Control centralizado + alertas inmediatas.  
✅ Ideal para técnicos, MSPs y PYMEs.  
✅ Listo para entrar en fase piloto.

**🤝 Slide 17: Siguientes Pasos**

* Implementación piloto gratuita por 30 días
* Taller formativo para técnicos
* Reunión de onboarding con partners técnicos
* Acceso a demo online + repositorio GitHub privado