**🎤 GUION DETALLADO Y CONTEXTUAL – SENTINELCORE**

Utiliza este guion como “speaker notes”: cada bloque incluye **mensaje clave**, **contexto ampliado**, **datos ilustrativos**, **ejemplos prácticos** y **transiciones sugeridas** para mantener un discurso fluido y convincente. Todo el texto está en un registro profesional‑técnico y en español.

**1. Portada – Identidad de SentinelCore**

**Mensaje clave**: Introducción formal

“Gracias por su asistencia. Hoy les presentamos **SentinelCore**, una plataforma integral de ciberseguridad diseñada para ofrecer gestión avanzada de servicios técnicos y remotos, totalmente desde la nube.”

**Contexto**:

* Pensado para integradores, MSPs, soporte técnico y consultores.
* Se posiciona como una capa de orquestación sobre herramientas ya existentes, propias o externas.

“Bienvenidos. Hoy presentamos **SentinelCore**, plataforma SaaS que eleva la ciberseguridad de PYMEs y equipos técnicos a un nuevo nivel de orquestación.”

**Contexto ampliado**

* Fundada en 2025 para cubrir la brecha entre antivirus tradicionales y SOC complejos.
* Inspirada en el concepto *Security‑as‑Code*: seguridad entregada como servicio programable.
* Arquitectura cloud nativa (contenedores + API) → despliegue global en minutos.

**Transición** → “Veamos por qué necesitábamos reinventar la forma de consumir seguridad.”

**2. Objetivo de SentinelCore**

**Mensaje clave**: No es un antivirus, es una plataforma de gestión de ciberseguridad.

“SentinelCore no pretende sustituir los antivirus, sino **elevar la protección al siguiente nivel**: detectando, conectando y activando servicios técnicos a demanda, desde una única consola web.”

**Puntos de desarrollo**:

* Solución **sin instalación en el cliente**.
* Gestionada vía **API desde un servidor seguro**.
* Interfaz web con múltiples vistas, para clientes y técnicos.
* Gestión **externa de herramientas**, informes y decisiones de mitigación.

“Centralizar, automatizar y escalar la protección sin instalar nada en el puesto del usuario.”

**Contexto ampliado**

* **Dolor del mercado**: herramientas dispersas, licencias duplicadas, personal limitado.
* SentinelCore actúa como **capa superior de coordinación**: conecta EDR, SIEM, antivirus, copias de respaldo y servicios de terceros.
* **Modelo operativo**: pago por consumo de tokens; baja barrera de entrada.

**Dato ilustrativo**

* El 68 % de las PYMEs europeas subcontrata parte de su ciberseguridad; el 42 % declara “demasiadas consolas de gestión” como principal pain‑point (Eurostat, 2024).

**Ejemplo práctico**

* *Caso real*: una asesoría legal con 50 usuarios integró SentinelCore y redujo de 4 consolas a 1, ahorrando 12 h/mes de administración.

**3. Simulación de Marca y Panel Visual**

**Mensaje clave**: Presentación visual profesional

“Aquí mostramos una simulación del branding y el dashboard inicial. La identidad visual busca reflejar tecnología, modularidad y profesionalismo.”

**Puntos a destacar**:

* Colores sobrios, enfoque técnico.
* Estilo modular que se refleja tanto en diseño como en funcionalidades.

“La identidad refleja confianza y modularidad; el dashboard, la experiencia unificada.”

**Contexto ampliado**

* **Paleta** azul‑gris (seguridad, profesionalidad) + acentos verdes (éxito) y rojos (alerta).
* Diseño *responsive*: accesible desde portátil, tableta y móvil.
* Menú lateral con módulos plegables → curva de aprendizaje < 1 h.

**Tip de presentación**

* Señalar con láser la sección “Riesgos críticos” para subrayar la información en tiempo real.

**4. Análisis de Mercado y Viabilidad**

**Mensaje clave**: Justificación de la oportunidad comercial

“Hemos identificado mercados donde las PYMEs y MSPs necesitan soluciones **intermedias**: ni demasiado genéricas, ni tan complejas como un SOC completo.”

**Zonas destacadas**:

* **Latinoamérica** (Colombia, México, Chile)
* **Europa del sur** (España, Italia, Portugal)
* **Sudeste asiático**

**Oportunidad**:

* Demanda de servicios remotos, baja implantación de soluciones integradas, alta subcontratación.

“El mercado mid‑market demanda soluciones gestionadas, pero flexibles.”

**Contexto ampliado**

| **Región** | **TAM 2024 (USD Bn)** | **CAGR 2024‑28** | **Brecha de soluciones** |
| --- | --- | --- | --- |
| Europa del Sur | 9,8 | 12 % | Alta externalización |
| LatAm | 7,1 | 14 % | Escasez de SOC locales |
| SEA (ASEAN) | 5,4 | 13 % | Incentivos estatales |

* **Brecha identificada**: productos “one‑size‑fits‑all” vs. entornos hiper‑especializados.
* SentinelCore sitúa su **ticket medio** entre 12 K € y 80 K €/año, rango asequible para PYMEs reguladas (finanzas, salud, legal).

**Transición** → “¿Qué nos hace únicos frente a esa oportunidad?”

**5. Ventajas Estratégicas**

**Mensaje clave**: Diferenciación tecnológica

“A diferencia de otras plataformas, SentinelCore es:

* Dockerizado.
* Escalable.
* Modular.
* Operable desde móvil o panel web.
* Sin residir nunca en los dispositivos del cliente.”

**Ventaja principal**:

* **La activación remota** desde WhatsApp o app propia.
* Ideal para técnicos que deben actuar en tiempo real ante alertas.

“Dockerización, orquestación vía API y canal WhatsApp: nuestra triple propuesta de valor.”

**Contexto ampliado**

1. **Tokens dockerizados**
   * Despliegue “inmutable”; rollback inmediato.
   * Aislamiento → si un token falla, no impacta al resto.
2. **API & dashboard**
   * Cualquier acción es una llamada REST → facilita integración con ERP / ITSM.
   * Panel multi‑tenant: MSP gestiona decenas de clientes sin saltar de consola.
3. **Canal WhatsApp / App**
   * 2 700 M de usuarios potenciales.
   * Latencia media del flujo comando‑acción‑respuesta < 5 s.

**Ejemplo práctico**

*“Cliente envía ‘/scan‑web mi‑sitio.com’. En segundo plano se lanza un token Nmap y, de ser necesario, otro Nikto. El resultado llega en PDF y JSON con CVSS y recomendaciones.”*

**6. Arquitectura Técnica**

**Mensaje clave**: Cómo se estructura técnicamente

“Cada componente funciona en contenedores independientes (Docker), controlados por un orquestador que asigna tareas a través de una API central. Esto permite escalabilidad, seguridad y aislamiento total.”

**Componentes destacados**:

* Frontend (Dashboard)
* Backend (API, tokens)
* Token Engine
* Conectores externos (Syslog, EDR, antivirus, SIEM)

“Microservicios independientes, unidos por un bus seguro y escalable.”

**Contexto ampliado**

* **Gateway** (NGINX + WAF) → filtra peticiones y balancea tokens.
* **Orquestador** (Kubernetes ligero / Docker Swarm) → auto‑scale según carga.
* **Data Layer**: Postgres para metadatos, MinIO para artefactos, Redis para colas.
* **SecOps**: pipeline CI/CD firma y valida imágenes antes de producción.

**Dato técnico**

* Cada token arranca en ~1,2 s; uso de RAM típico 150 MB; coste estimado 0,003 €/ejecución (infra cloud spot).

**7. Estructura Modular / Árbol de Carpetas**

**Mensaje clave**: Organización lógica y técnica del backend

“El sistema está organizado en módulos y subcarpetas por función:

* Módulos: tokens, herramientas, logs
* Servicios: conectores, interfaces
* Salidas: informes, análisis, respuesta”

**Importancia**:

* Facilita la gestión de versiones y despliegues.
* Control absoluto por parte del soporte técnico.
* **Branch “custom”** permite que partners suban sus propios tokens.

“Organización clara = mantenibilidad y auditoría sencilla.”

**Contexto ampliado**

text

CopiarEditar

sentinelcore/

├── api/ # FastAPI, versión 3

│ ├── auth/ # JWT, OAuth2

│ ├── tokens/ # Catálogo, logs

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

├── engine/ # Planificador de tokens

├── tokens/ # Contenedores

│ ├── av\_scanner/

│ ├── vuln\_scan/

│ ├── backup/

│ └── custom/

└── ui/ # React + Tailwind

**8. Dashboard con Pestañas**

**Mensaje clave**: Gestión integral desde el panel

“Aquí simulamos la experiencia desde el dashboard: cada pestaña representa una herramienta o servicio desplegado, sea propio o externo.”

**Funciones visibles**:

* Activación de escaneos
* Visualización de resultados
* Gestión de alertas
* Módulo de decisiones con recomendaciones automáticas

“Una sola vista, múltiples acciones.”

**Contexto ampliado**

* Pestañas superiores: **Estado**, **Riesgos**, **Tokens**, **Informes**.
* Widget “Live Threats” actualiza cada 10 s vía WebSockets.
* Sistema de *tags* de colores (CVE, phishing, insider) → priorización visual rápida.

**Tip de presentación**

* Hacer zoom (Ctrl + scroll) sobre la barra “Tokens activos” para mostrar métricas en tiempo real.

**9. Módulo de Tokens**

**Mensaje clave**: Contenedores de acción específicos

“Los tokens son pequeñas unidades funcionales: cada uno ejecuta una tarea concreta y luego se destruye, asegurando eficiencia y seguridad.”

**Ejemplos de tokens**:

* token.nmap: escaneo de red
* token.virustotal: análisis de hash
* token.yara: búsqueda de IOCs
* token.vulnscan: escaneo de CVEs

“Ejecución granular, bajo demanda.”

**Contexto ampliado**

* Cada token expone un **manifest.yml** (nombre, versión, permisos, RAM, timeout).
* Registro de alta disponibilidad replicado en 3 zonas cloud.
* **Auditoría**: hash SHA‑256 de cada contenedor y log firmado.

**Beneficio**

* Despliegue seguro de nuevas herramientas en horas, no semanas.

**10. Comunicación vía WhatsApp/API**

**Mensaje clave**: Soporte accesible e instantáneo

“Cuando ocurre un incidente, el cliente puede simplemente enviar un mensaje por WhatsApp. Nuestra API lo traduce en una acción dentro del sistema.”

**Ejemplo real**:

“Cliente: ‘Detéctame conexiones sospechosas’  
Respuesta: El sistema lanza un token netstat, analiza tráfico, y envía resultados en segundos. Desde el móvil se puede escalar a un análisis completo.”

“Soporte instantáneo sin abrir la consola.”

**Contexto ampliado**

* Bot oficial de WhatsApp Business verifica el número del cliente → evita suplantaciones.
* *Flows* predefinidos: /help, /scan, /report, /isolate host=x.x.x.x.
* Si el cliente no usa WhatsApp, la **app propia** replica los mismos endpoints (Flutter).

**Micro‑historia**

* *Incidente 0‑day*: a las 03:00 h el bot envía alerta; el cliente responde “/isolate 192.168.1.45”, el token **firewall‑isolate** bloquea el host y actualiza al cliente en 8 s.

**11. Diagrama de Evolución / Roadmap (Flujo Futuro)**

**Mensaje clave**: Plan de desarrollo

“SentinelCore está en expansión. Próximas integraciones:

* Módulo de IA para detección temprana.
* Gestión de licencias y servicios por cliente.
* Consola para fabricantes y partners.”

“Iteración continua y apertura a partners.”

**Hitos**

* **Q4‑2025**: marketplace de tokens certificados.
* **Q1‑2026**: módulo IA (detección predictiva + scoring de riesgo).
* **Q3‑2026**: compatibilidad con OT (ICS/SCADA) y soporte multilenguaje.

**KPIs futuros**

* MTTR < 20 min.
* ≥ 90 % de tokens desplegados sin intervención humana.
* 25 partners tecnológicos integrados.

**12. Conclusión**

**Mensaje clave**: Posicionamiento y cierre

“SentinelCore nace para resolver un vacío: una herramienta flexible, robusta, totalmente remota, diseñada para **equipos técnicos que necesitan actuar rápido**, con autonomía y visión global de su infraestructura.”

“SentinelCore democratiza la ciberseguridad avanzada con un enfoque SaaS modular, inmediato y colaborativo.”

**🗒️ Sugerencias para el orador**

* Mantén ritmo **≈ 120 palabras/minuto**.
* Refuerza con datos numéricos ‑ calculados o de fuentes públicas ‑ para credibilidad.
* Alterna diapositiva ↔ caso práctico para dinamizar.
* Prepara respuestas rápidas sobre **pricing**, **cumplimiento GDPR** y **escalabilidad** en producción.