**🧾 Informe de Viabilidad y Plan de Ejecución**

**Proyecto Final – SentinelCore**

**1. 📊 Análisis de Viabilidad**

**SentinelCore** es un proyecto viable, tanto en términos técnicos como organizativos, para un equipo de 4 personas en prácticas de fin de curso de ciberseguridad.  
Su principal innovación –el “toquen de antesala”– introduce una defensa proactiva previa al almacenamiento, ofreciendo un enfoque que no se encuentra en soluciones tradicionales centradas en la detección post-escritura.

* ✅ Modular: favorece el reparto del trabajo.
* ✅ Realizable con tecnologías conocidas: Python, SQLite, OWASP ZAP, Flask.
* ✅ Escalable: permite añadir más toquens y funcionalidades fácilmente.
* ✅ Enfocado: cada miembro puede trabajar en un módulo autónomo.

**2. 🧱 Plan de Ejecución por Fases**

**🔹 Fase 1: Análisis y Diseño (10h/persona)**

* Revisión técnica de herramientas a integrar.
* Diseño de arquitectura modular y comunicación entre toquens.
* Elección de tecnologías base (lenguaje, frameworks, base de datos).

**🔹 Fase 2: Desarrollo de Módulos (40h/persona)**

* Implementación del escáner web (OWASP ZAP, Wapiti).
* Desarrollo funcional del “toquen de antesala”.
* Creación de al menos 2 toquens especializados (ej. ClamAV + analizador PDF).
* Desarrollo de la interfaz básica (CLI o GUI web).

**🔹 Fase 3: Integración y Pruebas (20h/persona)**

* Conectar todos los módulos: GUI ↔ Toquens ↔ DB ↔ Escáneres.
* Validar flujo completo desde entrada de archivos hasta almacenamiento seguro.
* Pruebas funcionales, análisis de errores, logs y trazabilidad.

**🔹 Fase 4: Documentación y Presentación (10h/persona)**

* Manual de instalación y uso.
* Documentación interna de cada módulo.
* Informe técnico final + presentación con demo del sistema.

**3. ✅ Checklist General de Tareas**

* Establecer entorno de desarrollo (Git, virtualenv, entorno compartido).
* Implementar escáner web funcional (ZAP/Wapiti).
* Crear “toquen de antesala” que clasifique y redirija archivos.
* Desarrollar al menos 2 toquens especializados.
* Implementar interfaz CLI o web básica.
* Diseñar base de datos para guardar escaneos y acciones.
* Mostrar sugerencias de mitigación adaptadas a cada tipo.
* Generar informes automáticos en HTML o PDF.
* Documentar código y estructura.
* Validar el flujo completo con casos de prueba.
* Preparar presentación y demo del producto final.

**4. 🚀 Mejoras Estratégicas Sugeridas**

* Implementar autenticación (SSO, LDAP) para entornos corporativos.
* Añadir ML ligero para detección de anomalías en archivos.
* Contenerizar con Docker cada “toquen” y el sistema.
* Diseñar una API REST para interactuar con los toquens.
* Añadir un “modo laboratorio” para simular ataques y aprender mitigación.
* Crear una interfaz gráfica más visual con panel de control (futuro).