**Informe de Viabilidad, Plan de Ejecución y Checklist**

**Proyecto:** SentinelCore – Plataforma Centralizada de Herramientas de Seguridad Informática1.

**1. Análisis de Viabilidad**

**Técnica**

* **Modularidad:** El proyecto se basa en una arquitectura modular, permitiendo desarrollar y probar cada componente (“toquen”) de forma independiente, lo que facilita el trabajo en equipo y la escalabilidad1.
* **Integración:** Es viable integrar herramientas open source (OWASP ZAP, Wapiti, Nmap, ClamAV, etc.) mediante APIs o CLI, lo que reduce la carga de desarrollo propio y aumenta la robustez del sistema1.
* **Innovación:** El “toquen de antesala” añade una capa de prevención proactiva poco común en soluciones actuales, aportando diferenciación real1.
* **Automatización:** Es factible automatizar el flujo de análisis y mitigación, apoyándose en bases de datos de vulnerabilidades y recomendaciones (OWASP, MITRE ATT&CK)1.

**Organizativa**

* **Trabajo en equipo:** La división modular permite repartir tareas según especialidad/interés, fomentando la colaboración y la revisión cruzada1.
* **Aprendizaje:** El proyecto es ideal para prácticas de fin de curso, ya que abarca integración de herramientas, desarrollo seguro, automatización y documentación1.

**Económica**

* **Coste:** Uso de herramientas open source y recursos gratuitos, minimizando el coste económico1.
* **Infraestructura:** Puede ejecutarse en entornos locales y cloud gratuitos para pruebas (por ejemplo, VMs educativas, servicios cloud con free tier)1.

**Riesgos y Mitigación**

* Complejidad en la integración de múltiples herramientas → Solucionable con una buena definición de interfaces y pruebas unitarias.
* Seguridad de la propia plataforma → Aplicar buenas prácticas de desarrollo seguro y revisión por pares.

**2. Plan de Ejecución (Equipo de 4 personas)**

**Fases Principales**

1. **Planificación y Diseño (1-2 semanas)**
   * Definición de arquitectura modular.
   * Selección de herramientas a integrar.
   * Diseño de la interfaz y flujo de usuario.
2. **Desarrollo de Módulos**
   * **Módulo 1:** Integración de escáner web (OWASP ZAP/Wapiti).
   * **Módulo 2:** Desarrollo del “toquen de antesala” y toquens especializados.
   * **Módulo 3:** Interfaz web/dashboard y base de datos de resultados.
   * **Módulo 4:** Generación de informes y recomendaciones de mitigación.
3. **Integración y Pruebas**
   * Integración de todos los módulos.
   * Pruebas unitarias y de integración.
   * Simulación de escenarios de ataque y validación de respuestas.
4. **Documentación y Presentación**
   * Manual de usuario y documentación técnica.
   * Preparación de la presentación final y demo funcional.

**Asignación Sugerida de Roles**

| **Persona** | **Rol Principal** | **Responsabilidades** |
| --- | --- | --- |
| 1 | Integración de escáneres y pentesting | OWASP ZAP, Nmap, Wapiti, automatización |
| 2 | “Toquen de antesala” y toquens | Desarrollo de módulos de análisis de archivos |
| 3 | Interfaz web y base de datos | Dashboard, almacenamiento y visualización |
| 4 | Informes, mitigación, documentación | Generación de reportes y recomendaciones |
| Todos | Testing, integración, revisión cruzada | Pruebas, integración y mejora continua |

**3. Checklist de Trabajos a Realizar**

**Planificación**

* Definir alcance y arquitectura modular1.
* Seleccionar herramientas de análisis y APIs.
* Asignar roles y tareas.

**Desarrollo**

* Implementar integración con escáner web (OWASP ZAP/Wapiti).
* Desarrollar el “toquen de antesala” (análisis y redirección de archivos).
* Crear toquens especializados según tipo de archivo/sistema.
* Desarrollar la interfaz web/dashboard básica.
* Configurar base de datos ligera (SQLite).
* Implementar generación de informes HTML/PDF.
* Integrar recomendaciones de mitigación (basadas en OWASP/MITRE).
* Añadir automatización de pruebas de penetración.

**Pruebas**

* Pruebas unitarias de cada módulo.
* Pruebas de integración de todo el sistema.
* Simulación de ataques y validación de respuestas.
* Pruebas de usabilidad en la interfaz.

**Documentación**

* Manual de usuario y guía de instalación.
* Documentación técnica de arquitectura y módulos.
* Registro de incidencias y mejoras propuestas.

**Mejoras y Extensiones**

* Integración de nuevos escáneres o módulos (cloud, APIs).
* Incorporar LLMs para generación automática de textos explicativos.
* Añadir autenticación y gestión de usuarios.
* Mejorar visualización y reporting (gráficas, dashboards avanzados).
* Adaptar la solución para despliegue en cloud/híbrido.

**4. Mejoras Propuestas**

* **Automatización avanzada:** Integrar scripts que, previa autorización, puedan corregir vulnerabilidades simples de forma automática1.
* **Educación y formación:** Añadir recursos didácticos y explicaciones contextuales para cada vulnerabilidad, ideal para equipos en formación1.
* **Extensibilidad:** Diseñar la arquitectura para que sea fácil añadir nuevos “toquens” o integrar nuevas herramientas según evolucionen las amenazas1.
* **Cumplimiento normativo:** Incluir chequeos automáticos de cumplimiento con normativas (GDPR, LOPD, etc.) en los informes1.
* **Protección de subdominios y entornos internos:** Implementar medidas activas para evitar la indexación y exposición de recursos internos1.

**Conclusión:**  
El proyecto SentinelCore es viable y ofrece un enfoque innovador y educativo, ideal para un equipo de estudiantes en prácticas de seguridad informática. Su arquitectura modular, la integración de herramientas líderes y el mecanismo de “toquen de antesala” lo posicionan como una solución diferenciadora y escalable12.

1. <https://ppl-ai-file-upload.s3.amazonaws.com/web/direct-files/attachments/49893040/6da1f2cd-a9ef-4570-aac4-da35da646969/Borrador_Proyecto-Alcance.docx>
2. [projects.security\_tools](https://www.perplexity.ai/search/projects.security_tools)
3. <https://repository.ucatolica.edu.co/entities/publication/a6c64cc2-1be8-4270-b2de-47da374282cd>
4. <https://m.riunet.upv.es/bitstream/handle/10251/190634/Lacalle%20-%20Diseno%20y%20desarrollo%20de%20una%20arquitectura%20de%20Internet%20de%20las%20Cosas%20de%20Nueva%20Generacion%20or....pdf?sequence=1&isAllowed=y>