**Proyecto:** Plataforma Centralizada de Seguridad Informática (WEB&CLOUD)

**Visión General**

Desarrollar una aplicación integral que centralice herramientas de análisis de vulnerabilidades para entornos web y cloud, incorporando un innovador sistema de "toquen de antesala" para el procesamiento seguro de archivos antes de su almacenamiento.

**Componentes Clave**

**1. Sistema de Toquen de Antesala**

- Arquitectura modular: Cada toquen es un módulo especializado generado durante la instalación

- Procesamiento previo: Analiza archivos entrantes antes del almacenamiento en disco

**- Funcionalidades:**

- Análisis de tipo de archivo y contenido

- Enrutamiento a toquens especializados

- "Inoculación" de archivos (sanitización/neutralización de amenazas)

- Sistema colaborativo entre toquens para defensa en profundidad

**2. Módulos de Análisis**

- Escaneo web: SQLi, XSS, CSRF, etc.

- Cloud Security: Configuraciones erróneas, permisos IAM, exposición de datos

- OSINT: Recopilación de información de fuentes abiertas

**3. Motor de Mitigación**

- Recomendaciones accionables basadas en hallazgos

- Integración con herramientas de remediación

- Guías paso a paso para corrección

**Innovación Tecnológica**

**Arquitectura de Toquens**

1. Toquen Maestro: Coordina el flujo de análisis

2. Toquens Especializados:

- Documentos (PDF, Office)

- Ejecutables

- Multimedia

- Contenedores/empaquetados

3. Toquen de Cuarentena: Manejo de archivos sospechosos

**Proceso de Inoculación**

1. Análisis estático/dinámico

2. Reconstrucción segura del archivo

3. Firma digital del contenido procesado

4. Almacenamiento en zona segura

***Roadmap***

**Fase 1 (0-3 meses)**

- Diseño arquitectura toquens

- MVP del toquen de antesala

- Integración con 2-3 scanners básicos

**Fase 2 (4-6 meses)**

- Desarrollo de toquens especializados

- Panel de visualización de resultados

- Sistema de recomendaciones inicial

**Fase 3 (7-12 meses)**

- Integración cloud completa

- Automatización de remediación

- API para integración con SIEMs

**Consideraciones de Seguridad**

- Aislamiento de procesos de análisis

- Firmado digital de todos los toquens

- Rotación periódica de claves de toquens

- Auditoría de interacciones entre toquens

Este proyecto representa un enfoque innovador en la seguridad proactiva, combinando análisis tradicional con un sistema de pre-procesamiento que reduce significativamente la superficie de ataque antes incluso que los datos alcancen el almacenamiento persistente.