Proyecto *(preliminar)*

Desarrollo de Aplicaciones Seguras 2026

Sistema de gestión segura de identidades y secretos

En el contexto de las organizaciones actuales, la correcta gestión de identidades, autentificación, autorización y secretos digitales es un elemento crítico de la seguridad de la información. Más allá del simple almacenamiento de datos, estos sistemas deben garantizar que únicamente los usuarios autorizados accedan a la información adecuada, en el momento adecuado, y que todas las acciones relevantes queden registradas y puedan ser auditadas.

El objetivo de este proyecto es el diseño y desarrollo de una plataforma para la gestión segura de identidades y secretos dentro de una organización; permitiendo, entre otros, la autenticación de usuarios, la gestión de sesiones, el control de acceso a la información y el almacenamiento seguro de secretos (por ejemplo, contraseñas, credenciales u otra información sensible), considerando distintos roles y niveles de acceso. El proyecto debe abordarse desde una perspectiva de diseño y desarrollo seguros, prestando especial atención a la superficie de ataque, al modelado de riesgos y a la aplicación de mecanismos de mitigación adecuados.

La implementación práctica puede centrarse únicamente en las partes del sistema que se consideren más relevantes o interesantes desde el punto de vista de la seguridad, pudiendo dejar otros componentes descritos a nivel de diseño conceptual, siempre que estén correctamente justificados.

- Aspectos a incorporar:
  - Arquitectura cliente/servidor.
  - Autentificación y gestión de sesión seguras.
  - Tráfico y almacenamiento seguros (cifrado).
  - Gestión de identidades y/o secretos (crear, editar, borrar, etc.)
  - Roles o diferentes niveles de acceso a la información.
  - Posibilidad de compartir identidades y/o secretos entre usuarios o grupos.
  - Justificar las herramientas empleadas desde el punto de vista de la seguridad.

- Aspectos a considerar y evaluar:
  - Sistemas de *backup* y *logging* de eventos.
  - Infraestructura adecuada y escalabilidad del sistema.
  - Técnicas de ingeniería del software.
  - Minimización de dependencias externas, sencillez de diseño e implementación.

- Puede haber otros aspectos opcionales a propuesta del estudiantado *(consensuar primero con el profesor)*.

Indicaciones

- Se realizará en grupo (aprox. 4 personas)
- Se podrá aplicar un enfoque híbrido que comprenda aspectos de diseño teórico, *implementación y desarrollo*, integración de tecnologías, etc.
- El diseño comprenderá el sistema completo, pero la implementación puede ser de una parte más reducida.
- La evaluación consistirá en la entrega de una memoria del proyecto (junto con los materiales prácticos asociados) y la nota se dividirá entre la entrega (30% de la nota final) y revisiones (el otro 30%).

Revisiones

- Las características de las revisiones se indicarán con suficiente antelación.
- En la revisión participarán todos los componentes del equipo, indicando el reparto de trabajo.
- Habrá dos revisiones: una a mitad de cuatrimestre (10% de la nota final) y otra al final (20% de la nota final).

Memoria del proyecto

- Longitud máxima 20 páginas, formato y tamaño de letra razonable.
- Guía de contenido en página siguiente.
- Entrega en PDF (no en papel).
- Se pasará por *Turnitin* (antiplagio).

Guía de contenido para la memoria

(puede haber otro contenido adicional):

- Portada *(título, autores)*

- Resumen *(máx. 1 página)*

- Introducción
    - ...
    - Preliminares *(breve explicación de conceptos adicionales, si fueran necesarios)*
    - Objetivos *(contestar a la pregunta ¿qué se va a diseñar/desarrollar y con qué objetivo?)*
    - Estado del arte *(breve, consiste en estudiar y comparar el proyecto con otros sistemas o servicios similares o dentro del mismo contexto funcional)*

- Descripción
    - ...
    - Descripción de la funcionalidad
    - Planificación *(cronología aproximada y división del trabajo)*
    - Diseño seguro *(comentario conectando con el tema 1 de teoría)*:
        - *Adaptación del modelo SDL*
        - *Superficie de ataque y principios de resiliencia aplicables*
        - *Metodología y herramientas para el modelado del riesgo*
        - *Tácticas de mitigación del riesgo*

- Resultados
    - ...
    - Implementación *(descripción de la implementación realizada y aspectos asociados)*
    - Desarrollo seguro *(comentario conectando con el tema 2 de teoría, indicando características, tecnologías y herramientas para evitar vulnerabilidades en el código)*
    - Expectativas de seguridad y privacidad:
        - *Límites de seguridad (en qué condiciones el proyecto es seguro y en cuáles no)*
        - *Elementos criptográficos (qué se ha empleado y para qué)*
        - *Elementos de seguridad de la información (qué se ha empleado y para qué)*

- Conclusión
    - ...
    - *Contestar a la pregunta ¿Qué se ha realizado?*
    - *Destacar aspectos positivos y relevantes del proyecto*
    - *Establecer posibles trabajos futuros*