**METODOLOGÍA**

El desarrollo del componente de inicio de sesión con OAuth 2.0 para el proyecto Creavi ha seguido la metodología MODESEC: Modelo para el desarrollo de software educativo basado en competencias, adaptando la documentación cuidadosamente para asegurar que se aborden de manera efectiva los aspectos de funcionalidad, seguridad y facilidad de uso del componente al momento de iniciar sesión con tres proveedores diferentes de OAuth 2.0 como lo son GitHub, Facebook y Google en Creavi, los cuales son los más comunes. Aplicado durante tres etapas clave del ciclo de desarrollo en los cursos de Desarrollo de Software 1, 2 y 3. Este enfoque asegura que se aborden tanto los desafíos técnicos como las necesidades de los usuarios y administradores, priorizando la seguridad y la experiencia del usuario.

1. **Planificación y Análisis de Requisitos**

El primer paso fue entender los problemas actuales y las necesidades de los usuarios de Creavi. Nos enfocamos en detectar puntos débiles a través de análisis de los flujos existentes. Gracias a esto, encontramos estos dos problemas:

* La dificultad de los usuarios para registrarse debido a que deben ser registrados directamente por un Administrador de Creavi en este caso Usuario por Usuario lo cual retrasa el proceso.
* La incapacidad de los administradores para integrar fácilmente nuevos proveedores de autenticación.

Gracias a MODESEC, identificamos posibles riesgos desde el principio, y pensamos en la integración de OAuth 2.0 para simplificar los flujos de inicio de sesión, garantizando seguridad y facilidad de uso. En esta etapa se proporcionó un marco para priorizar riesgos y garantizar que el diseño contempla aspectos técnicos y funcionales fundamentales desde el inicio.

En el primer curso, el enfoque estuvo en el análisis y la documentación, estableciendo una base sólida para los desarrollos posteriores:

* Definición de Casos de Uso: Se identificaron las interacciones principales entre los usuarios y el sistema, como el inicio de sesión, registro y selección de métodos de autenticación.
* Modelado de Datos: Se diseñó un esquema detallado que abarcara tanto la estructura de la información del usuario como su protección mediante mecanismos de cifrado.
* Riesgos y Objetivos: Se analizaron problemas clave, como formularios de registro extensos y la falta de flexibilidad en la integración de nuevos proveedores de autenticación, definiendo los objetivos del proyecto y posibles mitigaciones.

**2. Persistencia de Datos con Backend – Base de Datos**

Aquí se enfocó en la implementación técnica en el lado del servidor y la base de datos, abordando aspectos críticos como:

* Configuración de Clientes OAuth: Se aseguraron conexiones seguras con los proveedores de autenticación.
* Gestión de Tokens: Se implementaron validaciones estrictas para proteger la información sensible y evitar accesos no autorizados.

El diseño modular permite una implementación ágil y escalable, haciendo que cada parte del sistema pudiera ser desarrollada, evaluada y mejorada de forma independiente. Esto también facilitó la realización de revisiones continuas, asegurando que cada componente del sistema fuera robusto y estuviera alineado con los requisitos de seguridad.

En el segundo curso, el equipo abordó la implementación técnica del backend, asegurando la persistencia de datos y la seguridad en los flujos de autenticación:

* Base de Datos: Se desarrolló una estructura robusta para almacenar información de usuarios y tokens de acceso, implementando cifrado para datos sensibles.
* Integración de OAuth 2.0: Se configuraron clientes y flujos de autorización para interactuar con proveedores de autenticación, reforzando las validaciones en la emisión y uso de tokens.

Esta fase destacó por su enfoque en garantizar que el backend fuera capaz de manejar de forma eficiente y segura la autenticación y autorización, pero, el equipo present ciertos problemas en cuanto a validar los datos en la base que al final se lograron solucionar de manera eficiente.

**3. Implementación Técnica**

La fase de implementación técnica se dividió en dos partes: el backend y el frontend. En el backend, se configuraron clientes OAuth 2.0 que interactúan con los proveedores de autenticación, y se implementaron estrictas validaciones en el manejo de los tokens.

En el frontend, el enfoque se centró en crear una interfaz de usuario intuitiva que simplificará el proceso de inicio de sesión, permitiendo a los usuarios seleccionar fácilmente entre varios proveedores de autenticación sin perder la seguridad del sistema.

En el curso actual, el equipo se encuentra trabajando en el frontend, con un enfoque en la experiencia del usuario y la integración visual del componente:

* Diseño de Interfaz: La interfaz de usuario se está desarrollando para ser intuitiva, permitiendo a los usuarios acceder a múltiples opciones de autenticación de manera sencilla y rápida.
* Pruebas de Usabilidad: Se realizan ajustes basados en la retroalimentación de pruebas con usuarios, optimizando elementos visuales y flujos de interacción.
* Integración de OAuth 2.0: Se conectan los flujos de autenticación desarrollados en el backend con el cliente, asegurando que la seguridad no se vea comprometida en la experiencia del usuario.

Este curso representa la culminación del desarrollo, donde se consolidan los avances de las etapas anteriores en una experiencia cohesiva y segura.

**4. Pruebas y Validación**

La fase de pruebas es fundamental en el enfoque MODESEC. Las pruebas también incluyeron pruebas de integración, que aseguraron que el sistema de autenticación se integrará correctamente con otras partes de la plataforma Creavi, como el sistema de gestión de usuarios y la base de datos.

**5. Mantenimiento y Escalabilidad**

Finalmente, la metodología MODESEC facilitó la planificación del mantenimiento continuo para el sistema. El enfoque modular y flexible de MODESEC también garantiza que el sistema sea escalable, permitiendo la adición de nuevas funcionalidades de manera eficiente y con mínimo impacto en el rendimiento o la seguridad.