**Implementación del Componente de Inicio de Sesión con OAuth 2.0 en CREAVI**

Daniel David Doria Diaz, Kissy Carolina Manjarrez Murillo, Jabib Roberto Manzur Lemos, Daniel Alejandro Márquez Araujo

**Resumen**

Este documento describe el diseño, desarrollo e implementación de un componente de inicio de sesión con OAuth 2.0 para la plataforma CREAVI. A través de este protocolo de autorización, se busca mejorar la seguridad, facilitar la autenticación para los usuarios y permitir a los administradores integrar nuevos proveedores de inicio de sesión de forma ágil. Siguiendo la metodología MODESEC, se detallan las etapas desde el análisis de requisitos hasta la implementación final, garantizando que el componente cumpla con los estándares más altos de seguridad y usabilidad.

**Introducción**

En un entorno digital donde la autenticación y la seguridad son primordiales, el protocolo OAuth 2.0 se presenta como una solución robusta para autorizar el acceso a aplicaciones sin exponer las credenciales de los usuarios. Este proyecto se centra en la creación de un componente para CREAVI que permite a los usuarios autenticarse mediante proveedores externos como Google o Facebook, simplificando el proceso y aumentando la seguridad de las cuentas.

El desarrollo de este componente responde a dos necesidades clave: simplificar el registro y autenticación para los usuarios, y brindar a los administradores la capacidad de gestionar y personalizar los métodos de inicio de sesión.

**Metodología (MODESEC)**

La metodología MODESEC se utilizó para estructurar el desarrollo del componente. Esta metodología enfatiza la seguridad en cada fase del desarrollo. A continuación, se detallan las etapas clave:

Modelado de amenazas: Identificación de riesgos potenciales, como suplantación de identidad y accesos no autorizados.

Definición de requisitos: Se establecieron requerimientos funcionales, como soporte para múltiples proveedores OAuth 2.0, y no funcionales, como tiempo de respuesta inferior a un segundo.

Diseño: Se definió un modelo basado en diagramas de flujo y casos de uso para garantizar la correcta interacción entre el frontend y backend.

Implementación segura: Se emplearon estándares de cifrado y validación de tokens para garantizar la integridad y confidencialidad de los datos.

Pruebas: Se llevaron a cabo pruebas de usabilidad, rendimiento y seguridad con usuarios finales y desarrolladores.

Mantenimiento: Se documentó el proceso para facilitar futuras actualizaciones y garantizar la sostenibilidad del componente.

**Etapas del Desarrollo**

**1. Análisis y diseño de la aplicación**

En esta etapa se identificaron las necesidades de los usuarios y administradores. Los usuarios requerían opciones de inicio de sesión simplificadas, mientras que los administradores necesitaban herramientas para gestionar nuevos proveedores. Se definieron los flujos de autorización y los diagramas de uso correspondientes.

**2. Persistencia de datos con backend**

Se implementaron en el servidor los flujos de autorización, almacenamiento seguro de tokens y medidas de seguridad para proteger los datos. Se configuraron los endpoints de autorización y token siguiendo las mejores prácticas de OAuth 2.0.

**3. Desarrollo frontend**

Se diseñaron interfaces intuitivas que permiten a los usuarios seleccionar su proveedor de inicio de sesión preferido. Para los administradores, se desarrolló un módulo que les permite agregar, editar y eliminar proveedores de forma sencilla.

**Conclusión**

El componente de inicio de sesión con OAuth 2.0 para CREAVI mejora significativamente la experiencia del usuario y refuerza la seguridad de la plataforma. La implementación de esta solución no solo resuelve los problemas actuales de autenticación, sino que también permite la integración futura con nuevos proveedores, adaptándose a las necesidades dinámicas de la plataforma.

Este proyecto demuestra cómo la combinación de protocolos avanzados como OAuth 2.0 y metodologías estructuradas como MODESEC pueden garantizar soluciones tecnológicas seguras y escalables.