Especialización en Back End II

Mesa de trabajo

- Ejercitación grupal
- Nivel de complejidad: medio 🔥🔥

Objetivos

- Afirmar conceptos de tokens y refresh tokens

Consigna

Supongamos que trabajamos en una **empresa de servicios financieros** que está desarrollando una aplicación web para que los usuarios puedan consultar sus movimientos y saldos bancarios. Para autenticar y autorizar las peticiones de los usuarios a nuestra API REST, se está utilizando **Keycloak** como proveedor de identidad.

Teniendo en cuenta este escenario, la empresa de servicios financieros necesita que realicemos las siguientes tareas:

1. Configurar y registrar un **cliente** en Keycloak que será el que luego asignaremos a la aplicación web que desarrollaremos.
2. Crear un **usuario** admin con su respectiva contraseña.
3. Antes de desarrollar nuestra aplicación, queremos probar que efectivamente Keycloak devuelva los datos necesarios, por lo que, mediante **Postman** simularemos una request con la autenticación del usuario usando el protocolo **OpenID Connect (OIDC)** y obtendremos un **access token válido**.
4. Una vez obtenido el **access token**, procederemos a corroborar si es posible generar y obtener el correspondiente **refresh token**.

Si todo sale bien... ¡Listo! Hemos finalizado las pruebas previas al desarrollo de nuestra aplicación. Para validar que efectivamente las hemos realizado, la empresa necesita que

efectuemos un **documento de pruebas** con capturas de pantalla que validen el proceso que estuvimos haciendo en formato de informe.

5. Documentar el proceso realizado, explicando a la empresa cada paso implementado y la respuesta obtenida por aparte de Keycloak.