Plan de Pruebas para el Microservicio de Autenticación y Autorización

1. **Pruebas Unitarias**

-**Objetivo:** Verificar que cada función y método del microservicio de autenticación opere de manera aislada y correcta.

-Casos de Prueba:

- Verificar que el método de registro crea un nuevo usuario con los datos correctos (nombre, email, contraseña).

- Probar que el método de login devuelve un token válido cuando se proporcionan credenciales correctas.

- Verificar que el método de login retorna un error adecuado cuando las credenciales son incorrectas.

- Comprobar que la función de validación de contraseñas identifica correctamente contraseñas seguras e inseguras.

2. **Pruebas de Integración**

- **Objetivo:** Asegurar que los diferentes componentes del microservicio interactúan correctamente y que la comunicación con otros microservicios (como el de Gestión de Usuarios) es adecuada.

- **Casos de Prueba:**

- Validar que, al registrarse, el nuevo usuario es añadido correctamente a la base de datos de usuarios.

- Comprobar que, al iniciar sesión, se verifique la existencia del usuario en la base de datos.

- Probar que un usuario no autenticado no puede acceder a rutas protegidas que requieren un token.

- Verificar que el microservicio de Autenticación se comunique correctamente con el microservicio de Gestión de Usuarios para obtener detalles adicionales de los usuarios después del login.

3. **Pruebas de Carga**

-**Objetivo:** Evaluar si el microservicio puede manejar múltiples solicitudes de login y registro simultáneamente sin degradación del rendimiento.

- Casos de Prueba:

- Enviar múltiples solicitudes de registro (por ejemplo, 500 registros en 1 minuto) y medir el tiempo de respuesta.

- Realizar pruebas de carga para iniciar sesión con varios usuarios simultáneamente (por ejemplo, 1000 inicios de sesión en 1 minuto) y comprobar la estabilidad del sistema.

4. **Pruebas de Seguridad**

-**Objetivo:** Validar que la información del usuario esté protegida y que solo los usuarios autorizados puedan acceder a sus propios datos.

- **Casos de Prueba:**

- Intentar acceder a las rutas de login y registro sin proporcionar datos y verificar que el sistema responda adecuadamente.

- Probar que un atacante no pueda acceder al sistema mediante inyecciones SQL o ataques de fuerza bruta en el login.

- Verificar que las contraseñas se almacenen de manera segura (por ejemplo, mediante hashing) y que no se expongan.

- Asegurarse de que los tokens de acceso expiren después de un tiempo razonable y que no se pueda reutilizar un token expirado.

5. **Pruebas de Usabilidad**

- **Objetivo:** Asegurar que la funcionalidad de login y registro sea intuitiva y fácil de usar.

- **Casos de Prueba:**

- Verificar que los mensajes de error sean claros y útiles en caso de un registro o inicio de sesión fallido.

- Comprobar que el formulario de registro tenga validaciones adecuadas (por ejemplo, formato de email, longitud de contraseña).

- Validar que la interfaz de usuario sea clara y permita a los usuarios completar el registro e inicio de sesión sin confusión.

6. **Pruebas de Compatibilidad**

- **Objetivo**: Asegurar que el microservicio funcione correctamente en múltiples dispositivos y navegadores.

- **Casos de Prueba:**

- Probar el proceso de login y registro en diferentes navegadores (Chrome, Firefox, Safari, Edge).

- Verificar la accesibilidad del microservicio desde dispositivos móviles y tabletas.

- Comprobar que las respuestas del sistema (errores y confirmaciones) se muestren correctamente en todos los dispositivos.

7. **Pruebas de Regresión**

-**Objetivo:** Confirmar que las actualizaciones y cambios en el microservicio no rompan las funcionalidades existentes.

-**Casos de Prueba:**

- Repetir las pruebas de registro y login después de realizar cambios en el código.

- Verificar que las funcionalidades anteriores de login y registro sigan funcionando como se espera tras una actualización.

- Comprobar que las configuraciones de seguridad (como el hashing de contraseñas) se mantengan efectivas tras cambios.