

PLAN DE PRUEBAS REGRES.IN (REST ASSURE)

1. ALCANCE DE PRUEBAS

El alcance de pruebas incluye la HU-001 y la HU-002. Para ello se probaran cada uno de los criterios de aceptación como vemos a continuación.

- Alcance de las pruebas HU-001 – Login exitoso en la pagina.
- Alcance de las pruebas HU-002 – Login no exitoso por ausencia de contraseña.

2. ESTRATEGIA DE PRUEBAS

HU-001: Login de usuario exitoso

- CA-1
El servicio deberá contar con una aplicación que permita hacer el registro, la cual deberá recibir el usuario y la contraseña ingresada para consumir el servicio.
- CA-2
La aplicación deberá enviar al cliente un token en caso de que la cuenta se haya registrado exitosamente.

HU-002: Login de usuario fallido.

- CA-3
La aplicación deberá enviar al cliente un mensaje de error en caso de errar el usuario o la contraseña al consumir el servicio.

3. ANÁLISIS DE RIESGOS

Criterio de Aceptación	Probabilidad (1-5)	Impacto (1-5)	Nivel de Riesgo	Tipo de Ejecución
El servicio deberá contar con una aplicación que permita hacer el registro, la cual deberá recibir el usuario y la contraseña ingresada para consumir el servicio	1	5	5	Automatizado
La aplicación deberá enviar al cliente un token en caso de que la cuenta se haya registrado exitosamente.	3	1	3	Automatizado
La aplicación deberá enviar al cliente un mensaje de error en caso de errar el usuario o la contraseña al consumir el servicio	3	1	3	Automatizado

4. ESTRATEGIA DE PRUEBA

De acuerdo a la identificación de los riesgos en la matriz de riesgos, se abordaran primero las historias de usuario con mayor riesgo. Por lo tanto se probara inicialmente la HU-001 y posterior se probara la HU-002.

HU-001: Login de usuario exitoso

- CA-1
Se debe verificar que el servicio cuente con una aplicación adecuada para recibir los datos del usuario (usuario y contraseña).
- CA-2
Se debe verificar que se recibe en el cliente un token indicando su autenticación correcta en el servicio.

HU-002: Login de usuario fallido.

- CA-3
Se debe verificar que la aplicación envíe al cliente un mensaje de error en caso de errar el usuario o la contraseña en la sección de login.

Estrategia de datos

Se debe contar con al menos un nombre de usuario y contraseña validos para realizar la verificación. De preferencia seria ideal contar con una base de datos dummy de usuarios y contraseñas previamente registrados en la aplicación.

5. CRONOGRAMA DE ENTREGAS O DESPLIEGUE

Se debe entregar la aplicación y los datos de usuario a QA por lo menos tres días antes de la finalización del sprint.

6. OTROS TIPOS DE PRUEBAS

Se recomienda también realizar los siguientes tipos de pruebas:

- Pruebas de rendimiento
- Pruebas de seguridad

7. REQUERIMIENTOS

Se requiere para la ejecución la base de datos dummy con los datos de usuario (nombre de usuario y contraseña), o en su defecto al menos un usuario debidamente registrado en la aplicación.

8. ACUERDOS

Tan pronto se detecte un bug adicional, este sera ingresado de forma inmediata al bug tracker para su respectiva corrección. Adicionalmente se enviara un correo electrónico indicando detalles del error al equipo de desarrollo y al Product Owner en caso de revisiones administrativas