

Requerimientos del Inicio de Sesión

Requerimientos funcionales

1. Pantalla de inicio de sesión

- El sistema debe mostrar una pantalla titulada “Inicia Sesión”.
- La pantalla debe contener los campos:
 - Correo electrónico
 - Contraseña
- Debe haber un botón “Iniciar sesión”.
- Debe mostrarse un enlace con el texto “¿No tienes una cuenta? Regístrate” que lleve a la pantalla de registro.
- En la parte superior debe mostrarse el logotipo “Otaklar” y un menú de navegación con las opciones:
 - Inicio
 - Planes
 - Sobre Nosotros

2. Campo Correo electrónico

- RF2.1 El usuario debe poder capturar su correo en el campo Correo electrónico.
- RF2.2 Antes de procesar el inicio de sesión, el sistema debe eliminar espacios en blanco al inicio y al final del valor capturado (trim()).
- RF2.3 El valor capturado se utilizará para comparar con la propiedad email de cada usuario obtenido desde la API.
- RF2.4 Si el correo (después del trim) no coincide exactamente con el correo de ningún usuario registrado, el sistema debe considerar el intento como credenciales inválidas.

3. Campo Contraseña

- RF3.1 El usuario debe poder capturar una contraseña en el campo Contraseña.
- RF3.2 El valor capturado en el campo Contraseña se utilizará para comparar con la propiedad contraseña de cada usuario obtenido desde la API.
- RF3.3 Si la contraseña no coincide exactamente con la contraseña asociada al correo electrónico, el sistema debe considerar el intento como credenciales inválidas.
- RF3.4 Si cualquiera de los campos (correo o contraseña) se deja vacío, la autenticación debe fallar y se debe mostrar el mensaje de error general de credenciales inválidas.

4. Navegación posterior al inicio de sesión

- RF7.1 Despues de un inicio de sesión exitoso, el sistema debe permitir redirigir al usuario a la página principal o a la sección correspondiente (según se implemente), tras mostrar el mensaje de éxito “Redirigiéndote.”.
- RF7.2 La redirección no debe realizarse si las credenciales son inválidas.

Requerimientos no funcionales

1. Usabilidad

- RNF1.1 El sistema debe proporcionar mensajes de error claros y en español, por ejemplo:
 - “Credenciales invalidas.” cuando el correo y/o contraseña no coincidan.
- RNF1.2 Los mensajes de éxito o error deben mostrarse en un área visible justo debajo del formulario, utilizando estilos de alerta (por ejemplo, verde para éxito, rojo para error).
- RNF1.3 El enlace “¿No tienes una cuenta? Regístrate” debe estar claramente visible para facilitar la navegación a la pantalla de registro.

2. Rendimiento

- RNF2.1 La verificación de credenciales debe realizarse de forma asíncrona mediante fetch sin bloquear la interfaz.
- RNF2.2 El tiempo de respuesta entre hacer clic en “Iniciar sesión” y mostrar el mensaje de éxito o error debe ser, idealmente, menor a 1 segundo en el entorno local.

3. Seguridad

- RNF3.1 Las contraseñas no deben mostrarse en texto claro en la interfaz (el campo debe ser de tipo password).
- RNF3.2 En un entorno real, la comunicación con la API de usuarios debe realizarse sobre un canal seguro (HTTPS).
- RNF3.3 No se deben registrar en consola las contraseñas en texto plano en un sistema en producción; cualquier traza de depuración debe eliminarse antes de desplegar.

4. Mantenibilidad

- RNF4.1 Los textos de mensajes de alerta (éxito y error) deben centralizarse para evitar inconsistencias si se modifican.
- RNF4.2 El código debe utilizar nombres de variables claros (email, passwd, users) que faciliten su lectura y mantenimiento.

5. Compatibilidad

- RNF5.1 La solución debe funcionar en navegadores modernos.
- RNF5.2 La interfaz debe verse correctamente en resoluciones de escritorio estándar, manteniendo el formulario centrado.