# Caso de Uso UC-02: Iniciar Sesión

## Información General

|  |  |
| --- | --- |
| ID | UC-02 |
| Nombre | Iniciar Sesión |
| Actores | Recepcionista (Web) Cliente (App Móvil) |
| Descripción | Permite a un usuario existente autenticarse en la aplicación web o en la app móvil introduciendo sus credenciales. |
| Precondiciones | 1. El usuario ya debe haberse registrado. 2. Disponer de credenciales válidas (usuario/clave). |
| Postcondiciones | 1. Se crea o renueva la sesión del usuario. 2. Se emite un token JWT (o cookie de sesión) para futuras peticiones autenticadas. |
| Nivel | Primario |

## Flujo Principal A: Recepcionista (Web)

1. En la página de login de la web, ingresa usuario y contraseña.
2. Pulsa “Iniciar Sesión”.
3. Sistema valida campos no vacíos, consulta usuario y compara contraseña.
4. Si es correcto, crea sesión (cookie o token) y redirige al Dashboard.
5. Se muestra mensaje de bienvenida con nombre de usuario.

## Flujo Principal B: Cliente (App Móvil)

1. En la app, cliente ve pantalla de Login con Email y Contraseña.
2. Introduce credenciales y pulsa “Entrar”.
3. App envía datos al endpoint /api/auth/login.
4. Backend verifica formato, consulta cliente y valida contraseña.
5. Si es válido, devuelve token JWT.
6. App guarda token y navega a la pantalla de Mis Citas.

## Flujos Alternativos / Excepciones

* Credenciales incorrectas: muestra 'Usuario o contraseña inválidos'.
* Cuenta inactiva/bloqueada: muestra 'Cuenta inactiva. Contacte al administrador.'.
* Campos vacíos/formato erróneo: muestra 'Por favor complete todos los campos correctamente.'.
* Error de red/servidor: muestra 'No se pudo conectar. Intente de nuevo.'.

## Reglas de Negocio

* Después de 3 intentos fallidos, la cuenta se bloquea durante 15 minutos.
* El token JWT tendrá una vigencia configurada (p.ej. 1 hora).
* Se implementará un endpoint de refresh de token (opcional).