|  |  |  |  |
| --- | --- | --- | --- |
| CU-001 | Acceder a la Aplicación | | |
| Versión | 1.0 (14/02/2022) | | |
| Dependencias | * Bloqueo Usuario * Generación Token * Generación Alerta | | |
| Precondición | El usuario ha sido registrado previamente por un administrador, por lo cual el usuario cuenta con un username y un password. | | |
| Descripción | El sistema deberá de comportarse como se describe en el siguiente caso de uso cuando un usuario intente acceder a la aplicación introduciendo sus credenciales de acceso. | | |
| Secuencia nominal | Paso | Acción | |
| 1 | El usuario introduce sus credenciales en el formulario del login (username y password) y solicita acceso a la aplicación. | |
| 2 | El sistema realiza una búsqueda para un usuario que cumpla con las credenciales introducidas. | |
| 3 | El sistema genera un token que permitirá el acceso a todas las operaciones de la aplicación. | |
| 4 | El sistema redirige al usuario a la página principal de la aplicación. | |
| Excepciones | Paso | Acción | |
| 3 | Si el usuario introduce un username valido pero el password es incorrecto. | |
| E.1 | El sistema tiene un contador interno que actualiza el numero de intentos de acceso realizados. |
| E.2 | El sistema muestra una alerta al usuario notificando que las credenciales son incorrectas. |
| E.3 | El usuario debe de volver al paso 1 y corregir las credenciales. |
| 3 | Si el usuario introduce un username valido pero el password es incorrecto y lleva mas de 3 intentos de acceso. | |
| E.1 | El sistema realizara el bloqueo del usuario. |
| E.2 | El sistema realizara el despliegue de una alerta |
| E.3 | Se cancela el caso de uso |
| Comentarios | El número de intentos por acceso son 3 y pueden cambiar en el futuro o ser reseteados por día, el token de acceso generado no es visible por el usuario y solo es un medio de autenticación para acceder a las Apis. | | |

|  |  |  |  |
| --- | --- | --- | --- |
| CU-002 | Recuperación de contraseña | | |
| Versión | 1.0 (14/02/2022) | | |
| Dependencias | * Send token recover * Autentificación username | | |
| Precondición | El usuario ha sido registrado previamente por un administrador, por lo cual el usuario cuenta con un username y un password, pero ha olvidado el password lo que le impide acceder a la aplicación. | | |
| Descripción | El sistema deberá de comportarse como se describe en el siguiente caso de uso cuando un usuario intente recuperar su contraseña. | | |
| Secuencia nominal | Paso | Acción | |
| 1 | El usuario se encuentra en la vista de login y selecciona el enlace para recuperar contraseña. | |
| 2 | El sistema lo redirige a un formulario donde se le es solicitado su email para ser ingresado al sistema. | |
| 3 | El sistema busca el email con el cual identifica a un usuario. | |
| 4 | El sistema envía un token para poder acceder al cambio de contraseña. | |
| 5 | El usuario consulta su correo y obtiene el token. | |
| 6 | El sistema solicita al usuario token, nueva contraseña y confirmación de contraseña | |
| 7 | El sistema valida que el token sea correcto y que las contraseñas sean iguales | |
| 8 | El sistema redirige al login. | |
| Postcondiciones | El usuario puede realizar el caso de uso CU-001. | | |
| Excepciones | Paso | Acción | |
| 3 | Si el usuario introduce un email que no existe. | |
| E.1 | El sistema desplegará una alerta al usuario |
| E.2 | El usuario debe de volver al paso 2 y corregir el email. |
| 7 | Si el usuario introduce un token incorrecto. | |
| E.1 | El sistema desplegará una alerta. |
| E.2 | El sistema vuelve a solicitar los datos del paso 6 |
| Comentarios | En caso de solicitar un token para recuperación de contraseña este tiene un tiempo de vida de 30 min si no es utilizado se debe de generar uno nuevo. Criterios de aceptación para una nueva contraseña (8 caracteres, número, ($#./+-) ). | | |