MY ACCOUNT

User Guide

IT Services and Applications Management

Information Systems Department

San Jorge University

Content

1. Introduction

The aim of this application is to centralise the management of the accounts of University users allowing them to activate their accounts and change or reset their password.

2. Password Expiration

This policy does not apply to students.

Passwords are valid for one year. After this period, the account will be blocked, therefore the password must be changed before this occurs. Reminder emails will be sent 15 and 7 days before the account is blocked.

If the password expires and the account is blocked, you must reset the password to recover it (see point 6 of this document).

3. Application access

Go to https://micuenta.usj.es

To manage your account, first login, indicating your USJ username.

Image1. Login

4. Activate account

Once the username is entered, the application proceeds to perform the following actions:

1. Verification of the username.

   - The username cannot be left blank.
   - Do not include @usj.es at the end.
   - It can only contain alphanumeric characters and the special characters . - _

2. Verifying the user and obtaining their data:

3. If the user is inactive, an email containing an activation link is sent.

   The mail is sent to an alternative email account, that is, the user's **personal email account.** If the user does not have a defined alternative email, this email cannot be sent. A message will appear to contact:

   - *Dirección y Desarrollo de Personas (Human Resources)* if the user is a member of staff.
   - *Secretaría General Académica (Academic Registry)* if the user is a student or a graduate.
   - *Unidad de Orientación Profesional y Empleo* (*Careers Advice Unit)* if the user is a professional tutor or an institution.

Image2. Email sent for account activation.

This link is valid for 2 hours from the time of being sent. After this time it will no longer be valid and the process must be repeated to receive a new mail.

Image3. Mail that the user receives to perform the activation.

Clicking on the link redirects the application and a screen is displayed for the user to enter their new password twice.

Passwords should follow these guidelines:

- The length must be equal to or greater than 8 characters and less than 13 characters.

- It must contain at least one upper case letter, one lower case letter, one number and one special character of the following: ! " # $ % & ' ( ) * + , - . / : ; < = > ? @ [ ] ^ _ ` { | } ~

- It cannot be the same as the last 3 passwords used.

- The application informs the user the same repeated character is written more than once in a password but it is not a prerequisite.
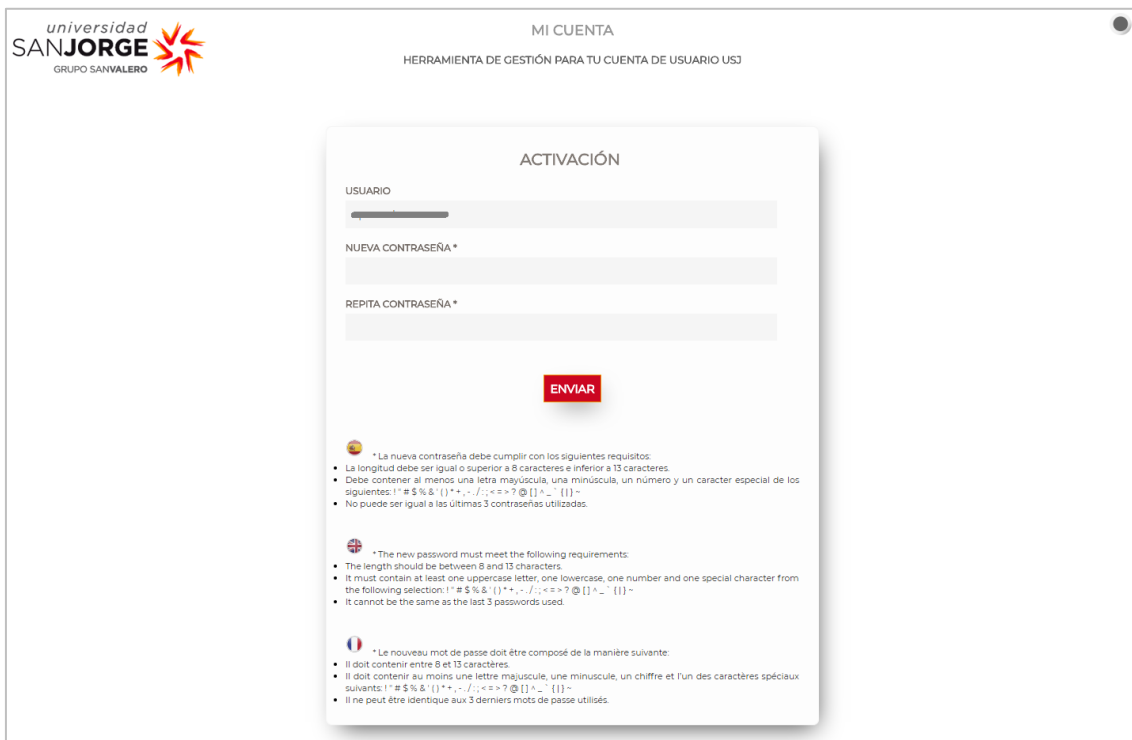
Image4. Activation after clinking the link.

The following is verified in the data validation form:

- The two passwords entered cannot be left blank.

- The two passwords entered must be exactly the same.

- Passwords must follow the guidelines given above.

Once validated correctly, the application proceeds to assign the entered password and activate the account. Once the entire process is completed, the correct activation of the account or any possible error is reported on the screen.
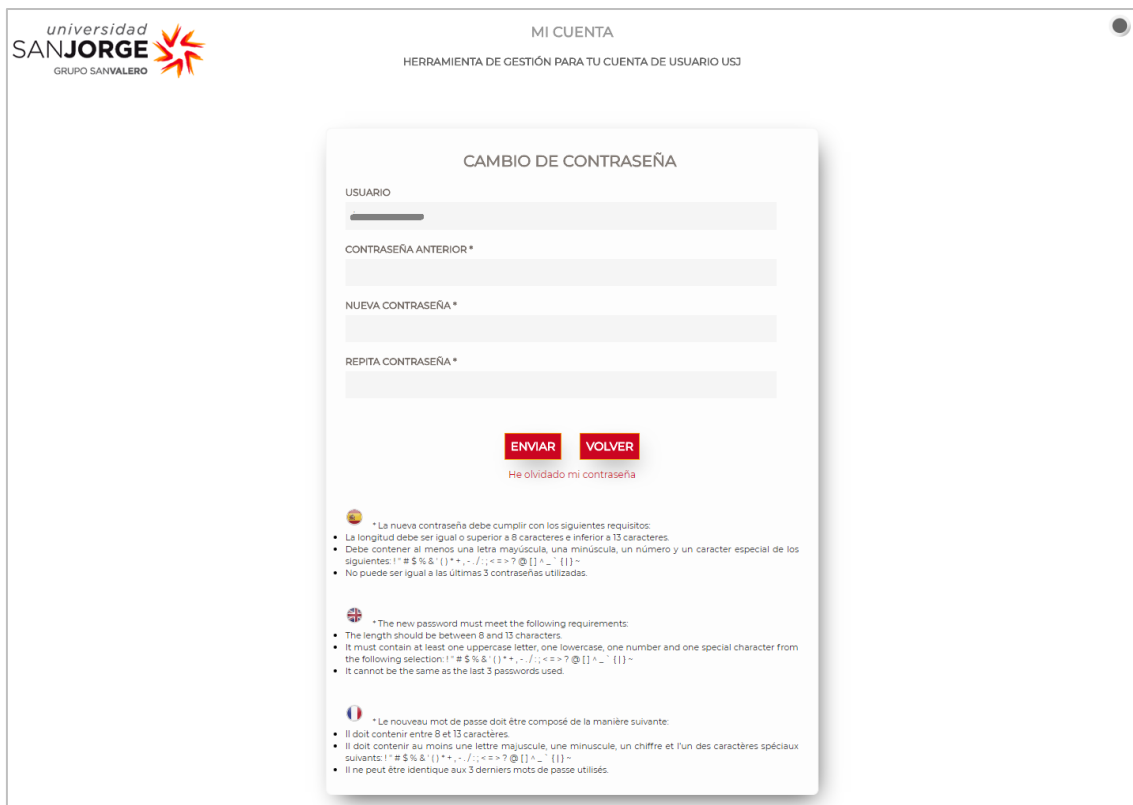

Image5. User activated correctly.

5. Change password

Once the username is entered, the application proceeds to perform the following actions:

1. **Verification of the username.**

   - The username cannot be left blank.

   - Do not include @usj.es at the end.

   - It can only contain alphanumeric characters and special characters - _

2. **Verifying the user and obtaining their data:**

3. **If the user is active, the user is redirected to the change their password.**

The user is prompted to enter their old password and their new password twice.

Image6. Change password.

Passwords should follow these guidelines:

- The length must be equal to or greater than 8 characters and less than 13 characters.

- It must contain at least one upper case letter, one lower case letter, one number and one special character of the following: ! " # $ % & ' ( ) * + , - . / : ; < = > ? @ [ ] ^ _ ` { | } ~

- It cannot be the same as the last 3 passwords used.

- The application informs when in a password the same repeated character is written more than once but it is not a prerequisite.

The following is verified in the data validation form:

- The three passwords entered cannot be left blank.

- The two new passwords entered must be exactly the same.

- Passwords must follow the guidelines given above.

- The previous password must be correct.

Once correctly verified, the application proceeds to assign the entered password and the correct change of password or any possible error is reported on the screen.

Image7. Password changed correctly.

6. Reset password

Once the username is entered, the application proceeds to perform the following actions:

1. Verification of the username.

   - The username can not be left blank.
   - Do not include @usj.es at the end.
   - It can only contain alphanumeric characters and special characters - _

2. Verifying the user and obtaining their data:

3. If the user is active, the user is redirected to the change their password.

In the change password screen there is the option to reset it. To do this, click on the "**He olvidado mi contraseña**" (I have forgotten my password) link.

An email containing a link to reset the password is sent.

The mail is sent to an alternative email account, that is, the user's **personal email account.** If the user does not have a defined alternative email, this email cannot be sent. A message will appear to contact:

   - *Dirección y Desarrollo de Personas* (*Human Resources)* if the user is a member of staff.
   - *Secretaría General Académica* (*Academic Registry)* if the user is a student or a graduate.
   - *Unidad de Orientación Profesional y Empleo* (*Careers Advice Unit)* if the user is a professional tutor or an institution.

Image8. Email sent to reset password.

Clicking on the link redirects the application and a screen is displayed for the user to enter their new password twice.

Image9. Mail that the user receives to reset password.

Passwords should follow these guidelines:

- The length must be equal to or greater than 8 characters and less than 13 characters.

- It must contain at least one upper case letter, one lower case letter, one number and one special character of the following: ! " # $ % & ' ( ) * + , - . / : ; < = > ? @ [ ] ^ _ ` { | } ~

- It cannot be the same as the last 3 passwords used.

- The application informs when in a password the same repeated character is written more than once but it is not a prerequisite.

Image10. Reset password.

The following is verified in the data validation form:

- The two passwords entered cannot be left blank.

- The two passwords entered must be exactly the same.

- Passwords must follow the guidelines given above.

Once correctly verified, the application proceeds to assign the entered password and the correct change of password or any possible error is reported on the screen.

Image11. Password reset correctly.