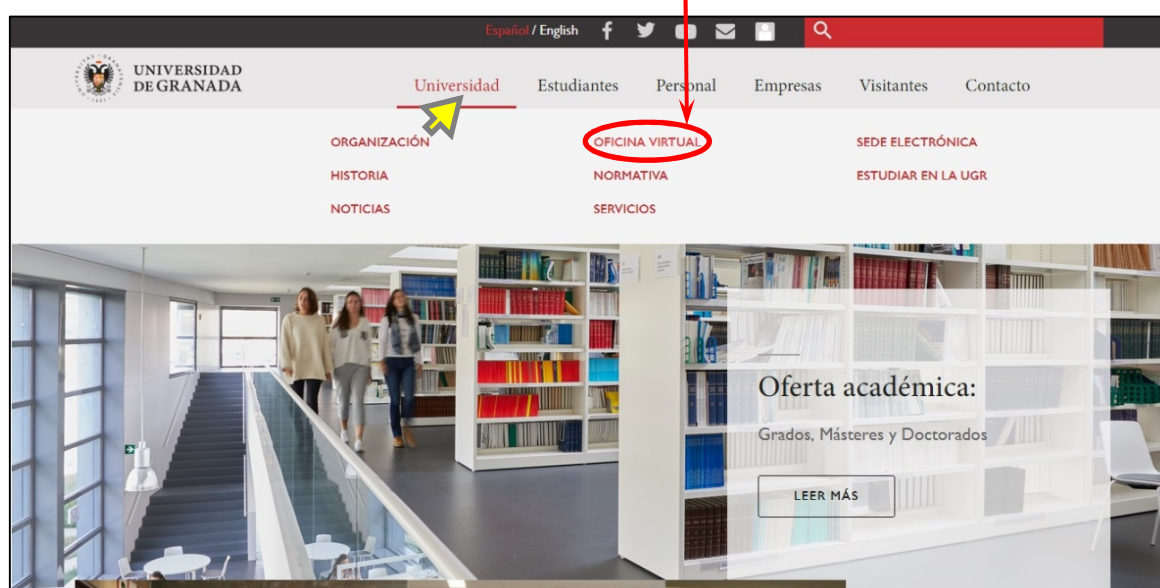


Manual to configure the second authentication factor of the Identified Access (Virtual Office)

The *Real Decreto 3/2010*, of January 8, which regulates the National Security Scheme in the Field of Electronic Administration, in its article 1.2 stipulates that this scheme *“is constituted by the basic principles and the minimum requirements demanded for an adequate protection of the information”*. University of Granada, in compliance with these principles and requirements, has implemented a double factor of authentication to the Identified Access (Virtual Office), among others.

Below we explain what it consists of.

To access to the Virtual Office we will proceed as usual, that is: we will go to the main website of University of Granada (<https://www.ugr.es/>) and we will place the cursor on the word/link "Universidad" on the top, and when the different options are displayed, we will click on *“OFICINA VIRTUAL”*.




Then we will access to the login screen by clicking on the red button *“ACCESO A OFICINA VIRTUAL”*. (*“Acceso a Oficina Virtual”* means *“Access to Virtual Office”*).



On the Identified Access (*Acceso Identificado*) screen we will login by entering our Identity Document number, with which we have registered/enrolled, in the *D.N.I.* field, and the four-digit PIN, that we obtain when we are doing the registration/enrolment, in the *Clave* field. If I am an Erasmus student, the four-digit PIN was provided by the person who did my registration/enrolment on that day. If we have already accessed and we have changed it, we must enter the new password that we have chosen in the *Clave* field.

With this we would have already accessed without the second authentication factor. But now we need to enter a second code. If it is the first time we access, we will see a screen with an explanation about the second authentication factor. Once we have seen the video and/or we have read the information we will click on the blue button "**SIGUIENTE**". ("*Siguiente*" means "*Next*").

From now on we begin to configure the second authentication factor. First thing we must do is to choose between the three options that are offered to us: a personal email account different from the university account, a Spanish mobile phone number (with 9 digits), or the numerical code of the university card or TUI (*Tarjeta Universitaria Inteligente* – Smart University Card). We must mark our choice and click on “SIGUIENTE”. If you are an international exchange student (Erasmus) or you do not live usually in Spain, we advise you to choose your personal email account.



Screen if you have an email account from University of Granada.



Screen if you DO NOT have an email account from University of Granada.

Option 1. Personal Email Account (different from the university account).

If we have chosen the first option, a personal email account (@hotmail.com, @gmail.com, @yahoo.fr, @outlook.com, @hotmail.es, etc...), we must enter it on the next screen and then click on “SIGUIENTE”.



Configuración de Segundo factor de Autenticación

A continuación va a configurar donde quiere recibir el código para el Segundo Factor de Autenticación.

Importante:

El valor introducido únicamente se utilizará para recibir el código de doble autenticación de Acceso Identificado.

Correo Electrónico distinto a su correo personal @ugr.es:

SIGUIENTE →

Then a screen will appear to enter the code that has been sent to the email account that we have just indicated on the previous screen. Something to keep in mind is the possibility that our mail manager has been moved the mail with the code to Spam folder or a similar one. We will introduce the code and then click on “SIGUIENTE”.



Configuración de Segundo factor de Autenticación

Para comprobar que ha introducido correctamente el medio de recepción de la clave para el segundo factor de autenticación se ha enviado una clave al **Correo Electrónico no Institucional** que está configurando.

Valor recibido en xxxxxxxx@hotmail.com:

Importante: Si no recibe el correo mire en la carpeta de SPAM

SIGUIENTE →

¿Ha pasado más de un minuto y no ha recibido el código en xxxxxxxx@hotmail.com?

[Reenviar Clave](#) Quedan 2 intentos

Option 2. Spanish Mobile Phone Number.

If we have chosen the second option, a Spanish mobile phone number, on the next screen we have to enter our mobile phone number (remember: 9 digits) and then click on “SIGUIENTE”.

Then on the next screen we have to enter the code that has been sent by SMS to our mobile phone. We will enter the code and click on “SIGUIENTE”.

UNIVERSIDAD DE GRANADA

Acceso Identificado

Configuración de Segundo factor de Autenticación

A continuación va a configurar donde quiere recibir el código para el Segundo Factor de Autenticación.

Importante:
El valor introducido únicamente se utilizará para recibir el código de doble autenticación de Acceso Identificado.

Número del teléfono móvil en el que desea recibir el SMS:
(Teléfono de 9 dígitos)

SIGUIENTE →

Screen for entering our mobile phone number.

UNIVERSIDAD DE GRANADA

Acceso Identificado

Configuración de Segundo factor de Autenticación

Para comprobar que ha introducido correctamente el medio de recepción de la clave para el segundo factor de autenticación se ha enviado una clave al Teléfono (SMS) que está configurando.

Valor recibido en 123456789 :

Importante: Tenga en cuenta que el SMS puede demorarse unos segundos en llegar

SIGUIENTE →

[¿Ha pasado más de un minuto y no ha recibido el código en 123456789 ?](#)

[Reenviar Clave](#) Quedan 2 intentos

Screen for entering the code received on our mobile phone indicated above.

Whether we have chosen the first option (personal email account) or the second one (Spanish mobile phone), once we have entered the received code, on next screen we have to choose the default shipping method of the second authentication factor.

If we have a university email account the usual thing is that this is the shipping method marked by default. In any case we can choose the personal email account (different from the university account) or the mobile phone number as the default shipping method of the second authentication factor. Either way, once we have chosen the default shipping method of the second authentication factor, we must **re-enter** the four-

digit PIN or the password that we used at the beginning (*see page 2 of this manual*) and click on "SIGUIENTE".

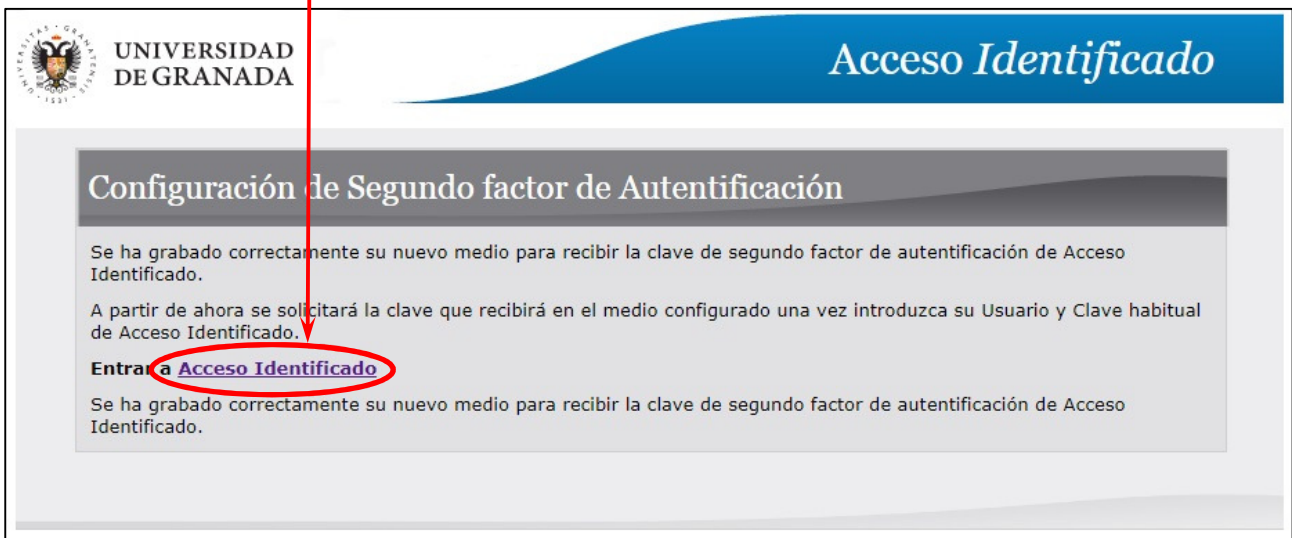
Screen to choose between university email account and personal email account.

Screen to choose between university email account and mobile phone number.

When we have done the choice of the default shipping method for sending the code of the second authentication factor will appear a screen informing us that the choice has been done with success. On this screen there is a link called "[Acceso Identificado](#)" to access again to our Identified Access.

Until now what we have done is to configure the second authentication factor of our Identified Access. Therefore we will not have to do this procedure again when we want to access to our Identified Access (also known as Virtual Office).

Next step will be to re-access to our Identified Access and check that it works properly by clicking on the link "[Entrar a Acceso Identificado](#)".



Once we logged as we have seen at page 2 of this manual, that is, by entering our Identity Document number in the *D.N.I.* field and the four-digit PIN or the password in the *Clave* field, will appear a screen asking for the code of the second authentication factor.

Here we will enter the code that we have received; no matter the shipping method we have chosen (university email account, personal email account or mobile phone). If we **do not want to be required** this code for next accesses during **next 30 days** we should mark the check box before clicking on "ENVIAR". ("*Enviar*" means "*Send*").



Once the "ENVIAR" button is clicked we will access to our Identified Access and we could make use of all the procedures that we need such as university scholarship requesting, creating an university email account if we didn't have one yet, upload a passport-size photo to our file, check our marks, etc...

Option 3. Numerical code of the university card or TUI.

If we have chosen the third option, the numerical code of the university card or TUI (*Tarjeta Universitaria Inteligente* – Smart University Card) we will find this code on the back of our TUI right under the barcode, as we can see in the following image.



TUI numerical code.

On next screen we must enter the hidden numbers by asterisks of the numerical code of our university card **in the same order**. If we **do not want to be required** this code for next accesses during **next 30 days** we should mark the **check box** before clicking on "**ENVIAR**", as we have just seen with the previous two options.

The screenshot shows the 'Acceso Identificado' page for the 'Servicio de consulta y gestión Web. Segundo Factor de Autenticación'. It asks the user to 'Indique los dígitos de su tarjeta TUI UGR (bajo código de barras) que faltan: *23***7'. There is a text input field for 'Código:'. Below it, there is a checkbox that is currently unchecked. A red circle highlights this checkbox, and a red arrow points from the text in the previous paragraph to it. The text next to the checkbox says: 'Para su comodidad recomendamos que marque esta casilla si desea que no se solicite esta segunda clave en este navegador durante 30 días (se establecerá una cookie para tal fin)'. Below the checkbox is a blue 'ENVIAR' button with a right-pointing arrow. At the bottom, there are links for '¿No dispone de su tarjeta TUI UGR?', 'Reenviar Clave a xxxxxxxx@correo.ugr.es', and 'Información sobre Doble Factor de Autenticación en Acceso Identificado'. A yellow mouse cursor is pointing at the 'ENVIAR' button.

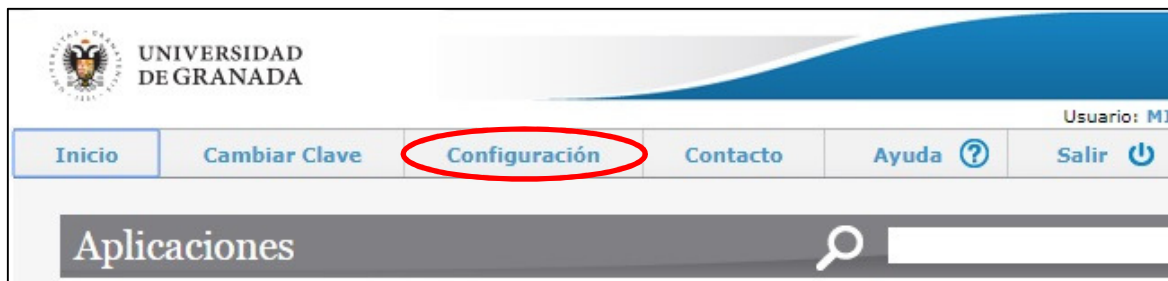
Therewith the explanation of how to set the second authentication factor of the Identified Access has finished. From now on each time that we want to access to our Identified Access the first authentication will be as it has been until now, by entering our Identity Document number in the *D.N.I.* field and the four-digit PIN or the password in the *Clave* field, and the second authentication, at least every 30 days, by entering the code that we will receive on our email account (personal or institutional) or on our mobile phone, or entering the asked numbers of the numerical code of our university card, depending on the choice that we did.

Changing the setting of the second authentication factor.

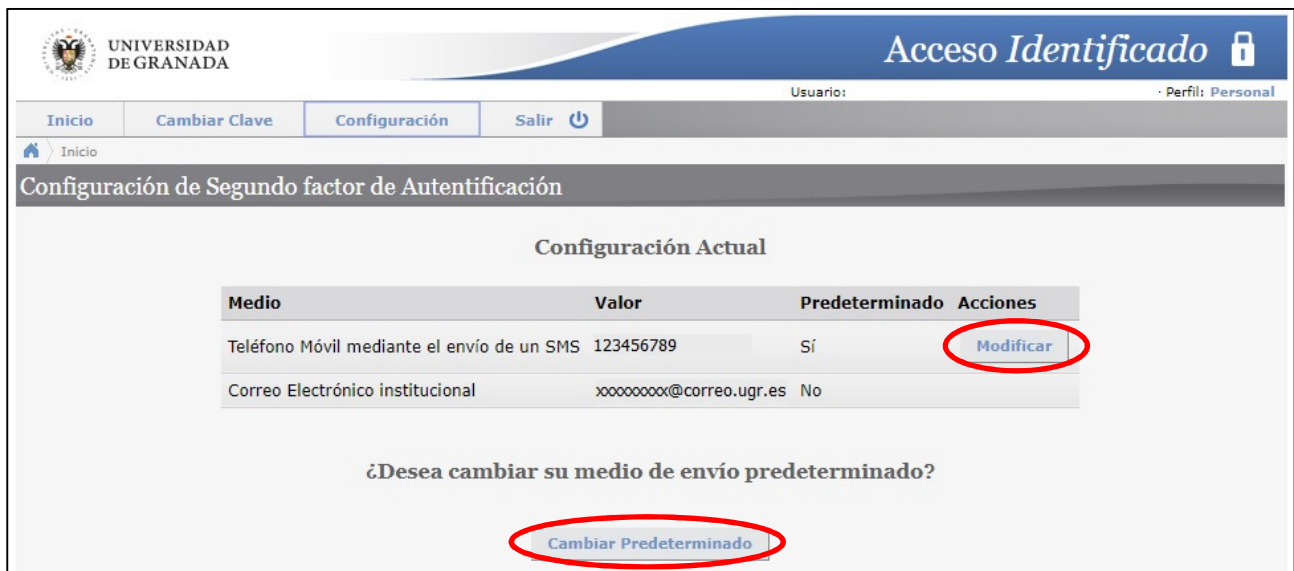
Let's imagine that at first we chose as second authentication factor the email account that we have at yahoo but we have just created an email account at gmail and we are going to use as main email account the last one; or that we are a first-year student and we have just collected our university card and now we would like to change the second authentication factor because we think that with the university card it's easier; or that we have finished our university degree and we had as default shipping method our university email account but we will no longer use it as often. Can we change the settings of the second authentication factor once configured in first time?

The answer to this question is **YES**.

For this we must access to our Identified Access. On the top row we can see different options/links. To the right of "Cambiar Clave" option, that allows us to change the original PIN for another PIN or an alphanumeric password, is the "Configuración" option/link. ("Cambiar Clave" means "Change Key" and "Configuración" means "Setting").



If we click on "Configuración" the following screen will appear:



This screen shows us the shipping methods of authentication that we have available with the current settings and it offers to us two possibilities:

- Changing default shipping method of the second authentication factor by clicking on the button "Cambiar Predeterminado".
- Changing the second authentication factor by clicking on the button "Modificar".

Changing default shipping method.

In the shipping method list we can see a column called "*Predeterminado*". If the shipping method is the default the value on that column is "*Si*" (Yes). In any other case the value on that column is "*No*". Every time we click on "*Cambiar Predeterminado*" the "*Si*" value changes to the row of the new default shipping method. ("*Predeterminado*" means "*Default*").

Changing the second authentication factor.

In the shipping method list we can see a column called "Acciones" also. If there is a button in the row of the shipping method means that we can change it. For this we must click on "*Modificar*" and we will see very similar screens to the ones that we have seen before to set the second authentication factor. This way we can choose both the default method among the three possibilities (personal email account, mobile phone or numerical code of the university card) and the email account or the mobile phone number if we have chosen one of the first two respectively.