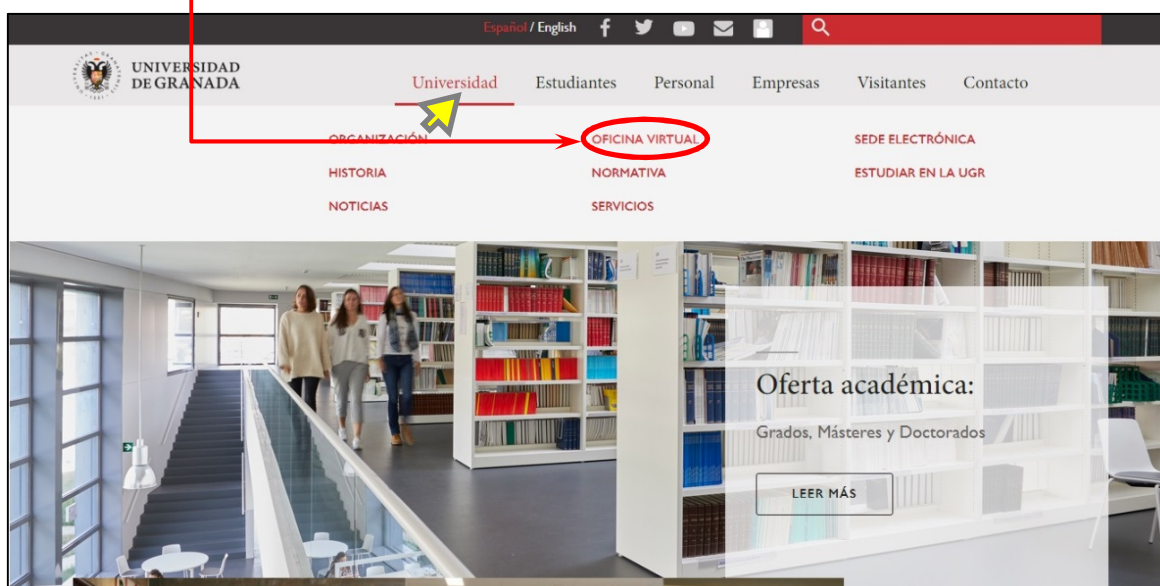


Manual para configurar el segundo factor de autenticación en el Acceso Identificado (Oficina Virtual)

El Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el Ámbito de la Administración Electrónica, establece en su artículo 1.2 que dicho esquema *“está constituido por los principios básicos y requisitos mínimos requeridos para una protección adecuada de la información”*. La Universidad de Granada, en cumplimiento de estos principios y requisitos, ha implantado un doble factor de autenticación en los accesos, entre otros, al acceso identificado a la Oficina Virtual.

A continuación explicamos en qué consiste.

Para acceder a la Oficina Virtual se procederá como viene siendo habitual, esto es: iremos a la página web principal de la Universidad de Granada (<https://www.ugr.es/>) y situaremos el cursor sobre la palabra “Universidad” en la parte superior y, cuando se desplieguen las diversas opciones, haremos clic en “OFICINA VIRTUAL”.



A continuación accederemos a la pantalla de acceso haciendo clic en el botón rojo “ACCESO A OFICINA VIRTUAL”.



En la pantalla de Acceso Identificado nos identificaremos introduciendo en el campo *D.N.I.* el número del documento de identidad con el que estemos matriculados/as (DNI sin letra, NIE, Pasaporte, etc...), y en el campo *Clave* el PIN de cuatro cifras que obtenemos al hacer la matrícula (si soy Erasmus, me lo proporcionaron en Secretaría el día de la matrícula) o, si ya hemos accedido y lo hemos cambiado, la contraseña que hayamos decidido.

Con esto ya habríamos accedido sin el segundo factor de autenticación. Pero ahora es necesario introducir un segundo código. Si es la primera vez que accedemos aparecerá una página con un vídeo explicativo del segundo factor de autenticación. Una vez hayamos visto el vídeo y/o leído la información haremos clic en el botón "SIGUIENTE".

Configuración de Segundo factor de Autenticación

¿Qué es el Segundo Factor de Autenticación

Es un nuevo protocolo de seguridad implantado por la Universidad de Granada para la protección de datos de carácter personal, que sirve para verificar la identidad del usuario. De esta manera, a partir de ahora, a los usuarios que se autentifiquen en el Acceso Identificado, el sistema les solicitará introducir un código adicional que recibirán de forma inmediata en correo electrónico o teléfono móvil. A este código se le conoce como Doble Factor de Autenticación.

¿Por qué se solicita este Segundo Factor de Autenticación?

La Universidad de Granada está certificada en cumplimiento con el Esquema Nacional de Seguridad, a partir de ahora ENS, Real Decreto 3/2010. Dentro del ENS aparecen unas medidas de protección que hemos de cumplir. Con el tipo de certificación obtenida, categoría media, se nos pide que pongamos en la autenticación un doble factor para asegurar la identidad de la persona que hace uso del servicio.

Todas las administraciones públicas deben cumplir el ENS, actualmente todas se están adecuando al sistema c@ve, nosotros de momento utilizamos un método que nos ha parecido menos restrictivo.

Según estudios se ha demostrado que la protección solo con password ya no es segura, es cuestión de tiempo romperla. Con el segundo factor de autenticación aumentamos la seguridad.

¿Me van a solicitar el código de Segundo Factor de Autenticación siempre que acceda mediante Acceso Identificado?

Después de identificarse por primera vez mediante el Segundo Factor, puede evitar que el sistema le requiera el código de verificación durante un mes marcando la casilla correspondiente que le aparecerá en pantalla. Con ello, el sistema estará reconociendo su dispositivo como un equipo de confianza. Transcurrido un mes, por seguridad, el sistema le volverá a requerir el código de Segundo Factor.

¿Cómo se configura el Segundo Factor de Autenticación?

Si dispone de cuenta de correo de la UGR, la recepción del código de verificación se realizará por defecto en esta cuenta. Pero también deberá elegir una segunda vía para la verificación, optando por la forma que le resulte más cómoda, entre las siguientes posibilidades:

- Otra cuenta de correo personal diferente a la de la UGR.
- Identificación mediante el número del código de barras de su tarjeta universitaria TUI UGR.
- Recepción del código de verificación en su teléfono móvil mediante SMS.

No obstante, puede cambiar su configuración de medios de recepción de la clave del Segundo Factor de Autenticación en cualquier momento utilizando el botón "Configuración" que encontrará en la parte superior de la pantalla de Acceso Identificado.

¿Cómo accedo si aún no tengo cuenta de correo personal de la UGR?

En el caso de que aún no disponga de una cuenta de correo de la UGR, deberá elegir como medio para la recepción de la clave del segundo factor de autenticación otra cuenta de correo personal o su teléfono móvil. En el caso de que cree automáticamente una nueva cuenta de correo de la UGR, esta se configurará como un medio más para la recepción de dicho código.

¿Puedo cambiar la configuración de medios elegidos por defecto para la recepción del código?

Si, puede cambiar su configuración de medios de recepción de la clave del Segundo Factor de Autenticación en cualquier momento utilizando el botón "Configuración" que encontrará en la parte superior de la pantalla de Acceso Identificado.

SIGUIENTE

A partir de ahora comenzamos a configurar el segundo factor de autenticación. Lo primero que debemos hacer es elegir entre las tres posibilidades que se nos ofrecen: una cuenta de correo electrónico personal distinta a la de la universidad, un número de teléfono móvil español (con 9 dígitos), o el código numérico del carnet universitario o TUI (Tarjeta Universitaria Inteligente). Debemos marcar nuestra elección y hacer clic en “SIGUIENTE”. Nuestro consejo es que si eres un/a estudiante de intercambio internacional (Erasmus) o no resides habitualmente en España elijas la cuenta de correo electrónico personal.

The screenshot shows the 'Configuración de Segundo Factor de Autenticación' page for users with an institutional email account. The page header includes the University of Granada logo and the text 'UNIVERSIDAD DE GRANADA' and 'Acceso Identificado'. The main heading is 'Configuración de Segundo Factor de Autenticación'. Under 'Configuración Actual', it states: 'Por defecto la clave que solicitará Acceso Identificado la recibirá en:'. A bullet point indicates: 'Cuenta de correo institucional (xxxxxxxxxx@correo.ugr.es)'. An 'Importante' section follows, stating: 'Es necesario que configure un segundo método de envío de la clave para prevenir posibles problemas al acceder a su correo electrónico para consultar la clave que le será enviada.' Below this, a section titled 'Indique un medio de envío alternativo a su correo institucional:' contains three radio button options: 'Correo Electrónico Externo (distinto a su correo personal @correo.ugr.es)', 'Teléfono Móvil mediante el envío de un SMS', and 'Código numérico (bajo el código de barras) de Tarjeta Universitaria TUI UGR'. The first option is selected and circled in red. A blue 'SIGUIENTE' button with a right arrow is at the bottom right.

Pantalla si se tiene cuenta de correo institucional de la Universidad de Granada.

The screenshot shows the 'Configuración de Segundo Factor de Autenticación' page for users without an institutional email account. The page header includes the University of Granada logo and the text 'UNIVERSIDAD DE GRANADA' and 'Acceso Identificado'. The main heading is 'Configuración de Segundo Factor de Autenticación'. Below the heading, it asks: 'Indique donde quiere recibir el código para el Segundo Factor de Autenticación:'. Three radio button options are listed: 'Correo Electrónico Externo (distinto a su correo personal @ugr.es)', 'Teléfono Móvil mediante el envío de un SMS', and 'Código numérico (bajo el código de barras) de Tarjeta Universitaria TUI UGR'. The first option is selected and circled in red. A blue 'SIGUIENTE' button with a right arrow is at the bottom right.

Pantalla si NO se tiene cuenta de correo institucional de la Universidad de Granada.

Opción 1. Correo Electrónico Externo.

Si hemos optado por la cuenta de correo electrónico personal (@hotmail.com, @gmail.com, @yahoo.fr, @outlook.com, @hotmail.es, etc...) en la siguiente pantalla deberemos introducirla y hacer clic en “SIGUIENTE”.



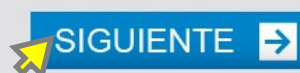
Configuración de Segundo factor de Autenticación

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:



A continuación nos aparecerá una pantalla para introducir el código que nos ha sido enviado a la cuenta de correo electrónico que hemos indicado. Hay que tener en cuenta que es posible que el email con el código sea derivado por nuestro gestor de correo a una carpeta de Correo No Deseado o de SPAM. Introduciremos el código y haremos clic en “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 xxxxxxxxx@hotmail.com:

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



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

[Reenviar Clave](#) Quedan 2 intentos

Opción 2. Teléfono Móvil mediante el envío de un SMS.

Si hemos optado por el teléfono móvil en la siguiente pantalla deberemos introducir el número de nuestro teléfono móvil y hacer clic en “SIGUIENTE”.

Posteriormente nos aparecerá una pantalla para introducir el código que nos ha sido enviado al teléfono móvil que hemos indicado. Introduciremos el código y haremos clic en “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.

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

SIGUIENTE →

Pantalla de introducción del número de teléfono móvil.



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

Pantalla de introducción del código recibido en el teléfono móvil indicado anteriormente.

Tanto si hemos optado por el correo electrónico externo como si hemos optado por el teléfono móvil, una vez introducido el código recibido nos aparecerá una pantalla en la que se nos solicitará la elección del medio de envío predeterminado del segundo factor de autenticación.

Aquí lo habitual será que venga marcado por defecto la cuenta de correo electrónico institucional (la de la Universidad de Granada), a no ser que no se haya creado aún. En cualquier caso se puede optar por que el medio predeterminado para el envío del segundo factor de autenticación sea la cuenta de correo electrónico externo o el número de teléfono móvil. En ambos casos, una vez elegido el medio predeterminado, se deberá **introducir de nuevo** el PIN/Clave del Acceso Identificado que ya introdujimos al

principio (*si soy Erasmus, el que me proporcionaron en Secretaría el día de la matrícula*) y hacer clic en "SIGUIENTE".

UNIVERSIDAD DE GRANADA Acceso Identificado

Configuración de Segundo factor de Autenticación

La validación ha sido correcta. Se va a proceder a grabar su nuevo medio de envío del segundo factor de Autenticación para el Acceso Identificado de la Universidad de Granada. Los datos que se van a grabar son:

- Medio de Envío: **Correo Electrónico Externo (distinto a su correo personal @ugr.es)**
- Valor: **xxxxxxxxx@hotmail.com**

Medio de Envío Predeterminado:

Seleccione el medio de envío en el que por defecto quiere recibir el código para la autenticación:

Cuenta de Correo Institucional (xxxxxxxx@correo.ugr.es)

Correo Electrónico no Institucional(xxxxxxxx@hotmail.com)

PIN/Clave de su Usuario de Acceso Identificado:

SIGUIENTE →

Pantalla de elección entre el correo electrónico institucional y el correo electrónico externo.

Configuración de Segundo factor de Autenticación

La validación ha sido correcta. Se va a proceder a grabar su nuevo medio de envío del segundo factor de Autenticación para el Acceso Identificado de la Universidad de Granada. Los datos que se van a grabar son:

- Medio de Envío: **Teléfono Móvil mediante el envío de un SMS**
- Valor: **123456789**

Medio de Envío Predeterminado:

Seleccione el medio de envío en el que por defecto quiere recibir el código para la autenticación:

Cuenta de Correo Institucional (xxxxxxxx@correo.ugr.es)

Teléfono (SMS)(123456789)

PIN/Clave de su Usuario de Acceso Identificado:

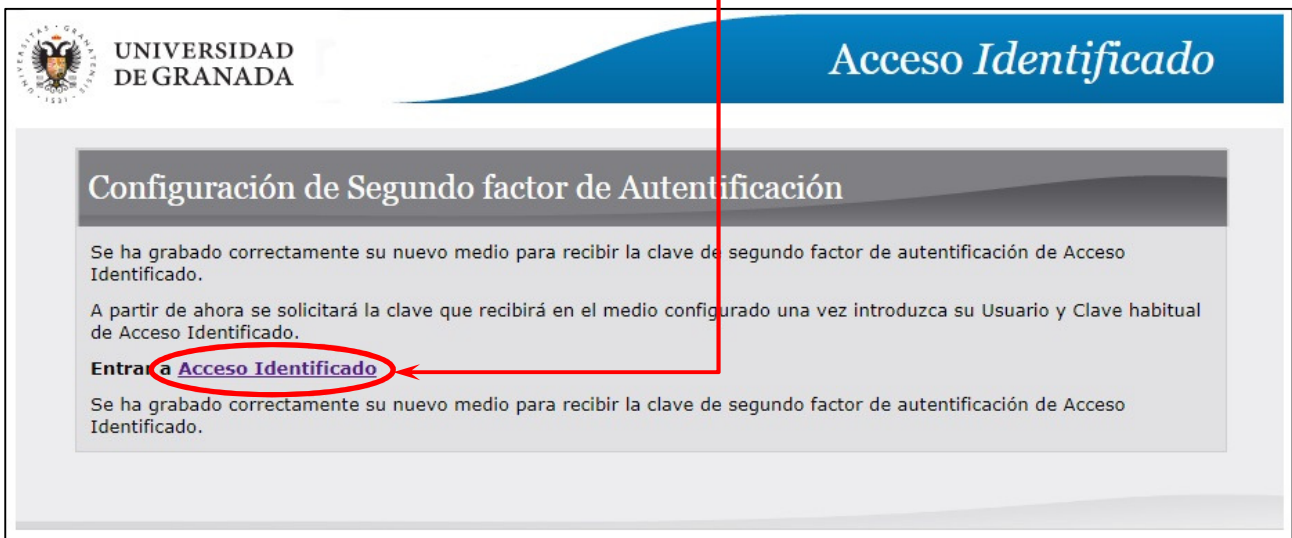
SIGUIENTE →

Pantalla de elección entre el correo electrónico institucional y el número de teléfono móvil.

Una vez hecha la elección del medio predeterminado para el envío del código del segundo factor de autenticación, nos aparecerá una pantalla informándonos de que se ha grabado correctamente nuestra elección y con el enlace para entrar de nuevo al Acceso Identificado.

Hasta ahora lo que hemos hecho ha sido configurar el segundo factor de autenticación de nuestro Acceso Identificado. Por lo tanto este procedimiento no lo tendremos que volver a realizar cuando queramos entrar a nuestro Acceso Identificado.

El siguiente paso será volver a entrar en nuestro Acceso Identificado y comprobar que funciona correctamente. Para ello haremos clic en el enlace “Entrar a Acceso Identificado”.



Una vez introducido el número del documento de identidad con el que estemos matriculados/as (DNI sin letra, NIE, Pasaporte, etc...) y el PIN/Clave de nuestro Acceso Identificado nos aparecerá la pantalla que nos pedirá el segundo factor de autenticación.

Aquí introduciremos el código que hayamos recibido, ya sea a través del correo electrónico institucional, del correo electrónico externo o del teléfono móvil, y si queremos que **no nos sea requerido** este código en los próximos accesos durante **los siguientes 30 días**, marcaremos la casilla de verificación antes de hacer clic en “ENVIAR”.



Una vez hecho clic en el botón “ENVIAR” accederemos a nuestro Acceso Identificado y podremos realizar los trámites que necesitemos, como puede ser solicitar una beca propia, crearnos una cuenta de correo electrónico institucional en el caso de que no la tengamos aún, subir una foto tamaño carnet a nuestra ficha, consultar nuestro expediente, etc...

Opción 3. Código numérico (bajo el código de barras) de Tarjeta Universitaria TUI UGR.

Si hemos optado por el código numérico que aparece en nuestro carnet universitario o TUI (Tarjeta Universitaria Inteligente) directamente nos iremos a la parte trasera de nuestra TUI y localizaremos el número debajo del código de barras, tal y como se muestra en la siguiente imagen.



Código numérico de la TUI.

En la siguiente pantalla deberemos introducir los números que aparecen ocultos por un asterisco en el mismo orden y, si queremos que durante los 30 días siguientes el sistema no nos vuelva a solicitar el código del segundo factor de autenticación, marcaremos la casilla de verificación antes de hacer clic en “ENVIAR”, como acabamos de ver en las dos opciones anteriores.

The image is a screenshot of a web page titled 'Acceso Identificado' for the 'UNIVERSIDAD DE GRANADA'. The main heading is 'Servicio de consulta y gestión Web. Segundo Factor de Autenticación'. Below this, there is a prompt: 'Indique los dígitos de su tarjeta TUI UGR (bajo código de barras) que faltan: *23***7'. There is a text input field labeled 'Código:'. Below the input field, there is a checkbox with the text: '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)'. A red circle highlights the checkbox, and a red arrow points from the text above to it. Below the checkbox is a blue 'ENVIAR' button with a right-pointing arrow. At the bottom, there are two links: '¿No dispone de su tarjeta TUI UGR?' and 'Reenviar Clave a xxxxxxxx@correo.ugr.es'. A third link at the bottom reads 'Información sobre Doble Factor de Autenticación en Acceso Identificado'.

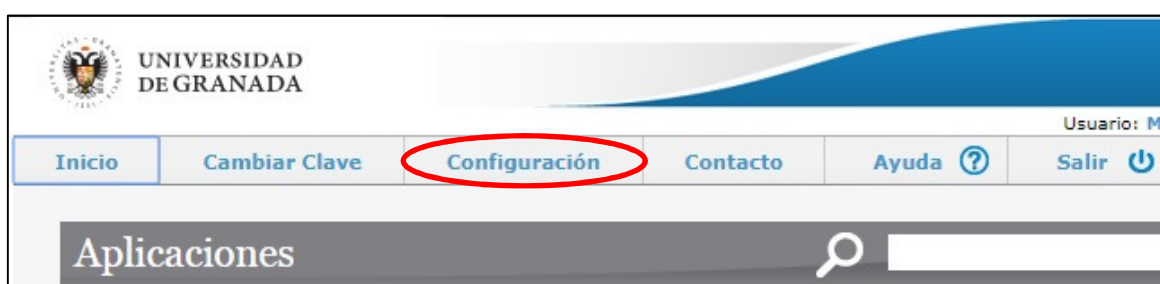
Con esto queda explicada la forma de configurar el segundo factor de autenticación del Acceso Identificado. Una vez hecho esto, cada vez que vayamos a entrar en nuestro Acceso Identificado tendremos que utilizar como primera autenticación nuestro documento de identidad y nuestro PIN/Clave, y como segunda autenticación, al menos cada 30 días, el código que recibiremos en la cuenta de correo electrónico o el número de teléfono móvil elegidos como medio predeterminado, o los números del código numérico de nuestra TUI si esta ha sido nuestra elección.

Cambio de la configuración del segundo factor de autenticación.

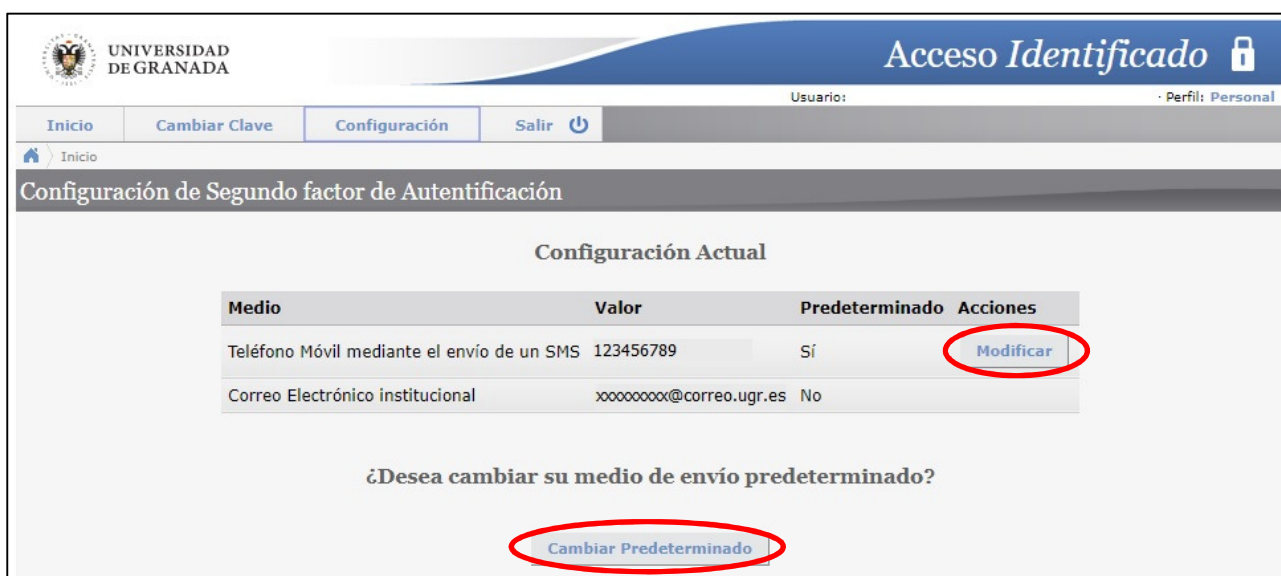
Imaginemos que en su momento elegimos como segundo factor de autenticación la cuenta de correo electrónico externo que teníamos con yahoo, pero nos hemos creado una cuenta de correo de gmail y es la que queremos utilizar como cuenta principal; o que somos estudiantes de primer curso y acabamos de recoger la TUI, y ahora que la tenemos nos gustaría cambiar el medio de autenticación por la TUI que nos parece más sencillo; o que hemos finalizado los estudios y teníamos como medio predeterminado la cuenta de correo electrónico institucional que ya no vamos a utilizar con tanta frecuencia. ¿Podemos cambiar la configuración del segundo factor de autenticación una vez configurado la primera vez?

La respuesta a esta pregunta es **SÍ**.

Para ello hemos de entrar a nuestro Acceso Identificado. En la parte superior del mismo, a la derecha de la opción “Cambiar Clave” que nos permite cambiar el PIN inicial por otro PIN o por una clave alfanumérica, tenemos la opción “Configuración”.



Si hacemos clic en “Configuración” nos aparecerá la siguiente pantalla:



Esta pantalla nos muestra los medios de autenticación que tenemos disponibles en la configuración actual, y nos ofrece dos posibilidades:

- Cambiar el segundo factor de autenticación predeterminado mediante el botón “Cambiar Predeterminado”.
- Modificar el segundo factor de autenticación mediante el botón “Modificar”.

Cambiar medio predeterminado.

Si hacemos clic en el botón “Cambiar Predeterminado”, en la lista de medios, concretamente en la columna “Predeterminado”, vemos que hay un *Sí* en el medio predeterminado y un *No* en el resto. Cada vez que hagamos clic en el botón “Cambiar Predeterminado” cambiará el *Sí* al siguiente medio, dejando al resto con el valor *No*.

Modificar el segundo factor de autenticación.

Si hacemos clic en el botón “Modificar” que hay en la columna “Acciones” de la lista de medios disponibles nos irán apareciendo pantallas muy similares a las que ya hemos visto anteriormente para la elección del medio de envío del segundo factor de autenticación. De esta forma podremos tanto elegir el medio predeterminado entre las tres opciones (correo electrónico externo, teléfono móvil mediante el envío de un SMS o código numérico de la TUI), como especificar la cuenta de correo electrónico externa o el número del teléfono móvil si elegimos alguna de las dos primeras respectivamente.