



¿CÓMO ACTIVAR EL DOBLE FACTOR DE AUTENTIFICACIÓN?



UNIVERSIDAD PARA MAYORES

UNIVERSIDAD COMPLUTENSE DE MADRID

¿POR QUÉ ES IMPORTANTE EL SEGUNDO FACTOR?

El 2FA obliga al usuario a **tener algo** (normalmente una contraseña de un solo uso, como el Google Authenticator), aparte de **conocer algo** (contraseña habitual).

En caso de vulneración de la cuenta, el atacante necesitará la OTP (Contraseña de un solo uso en inglés) para poder acceder.

Esta medida ralentiza el acceso de los usuarios legítimos, pero prácticamente bloquea el acceso a los usuarios no legítimos.



Antes de empezar, es importante saber que hay **dos opciones** para iniciar sesión en tu cuenta UCM:

- el **Segundo Factor de Autenticación**
- o con el **Certificado Digital o Clave PIN**, puedes utilizarlo si ya lo usas para autenticarte en otras Administraciones.

Acceso Web Unificado a la UCM (Web SSO)

Identificarse correctamente en esta página le habilitará la entrada en la mayoría de las aplicaciones y en los servicios en la nube @UCM.

DIRECCIÓN DE CORREO UCM

CONTRASEÑA

CLAVE SEGUNDO FACTOR DE AUTENTICACIÓN

Confiar en este equipo

INICIAR SESIÓN

[¿Olvidó la contraseña?](#)

OTROS MEDIOS DE AUTENTICACIÓN

Certificado Digital

Cl@ve

1

**ACTIVAR SEGUNDO FACTOR
DE AUTENTICACIÓN**

Ve al apartado 1 (página 5)

2

**SEGUNDO FACTOR DE
AUTENTICACIÓN EN EL
MÓVIL**

Ve al apartado 2 (página 14)

3

**SEGUNDO FACTOR DE
AUTENTICACIÓN EN EL
ORDENADOR**

Ve al apartado 2 (página 21)

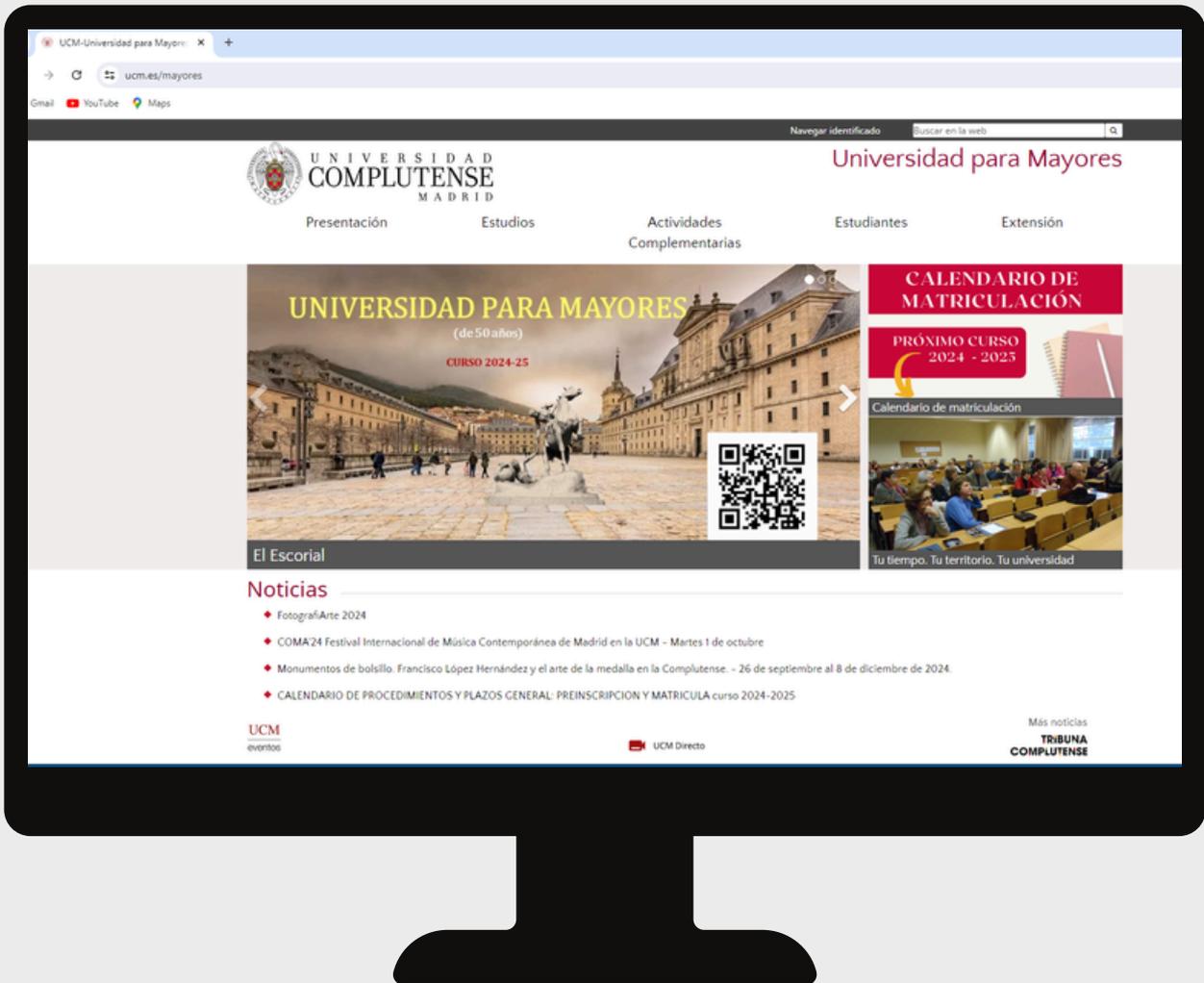


1

ACTIVAR SEGUNDO FACTOR DE AUTENTICACIÓN

1

Entramos en 'ucm.es/mayores'



2

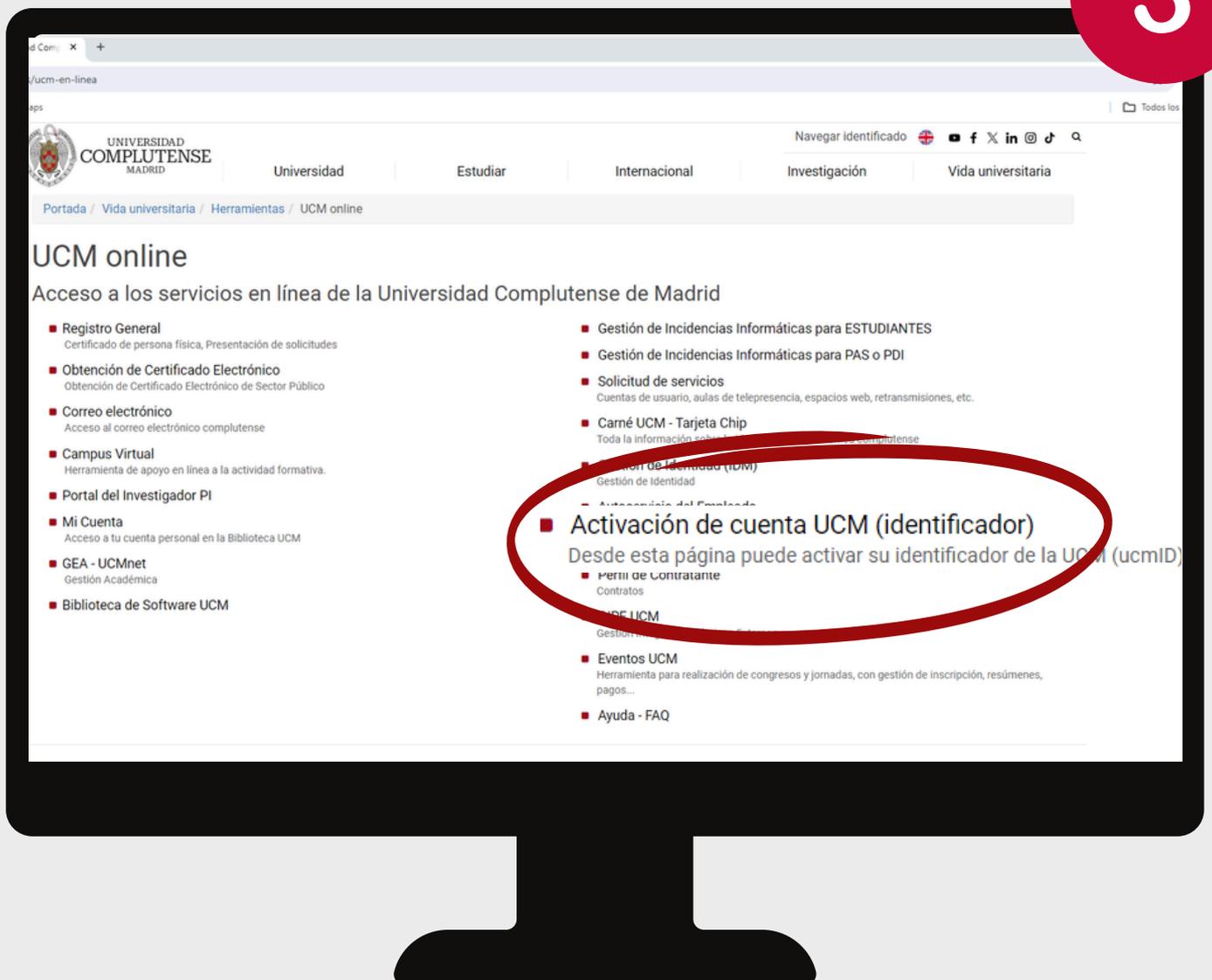
Bajamos hasta **abajo** del todo y **pinchamos en 'UCM en línea'**

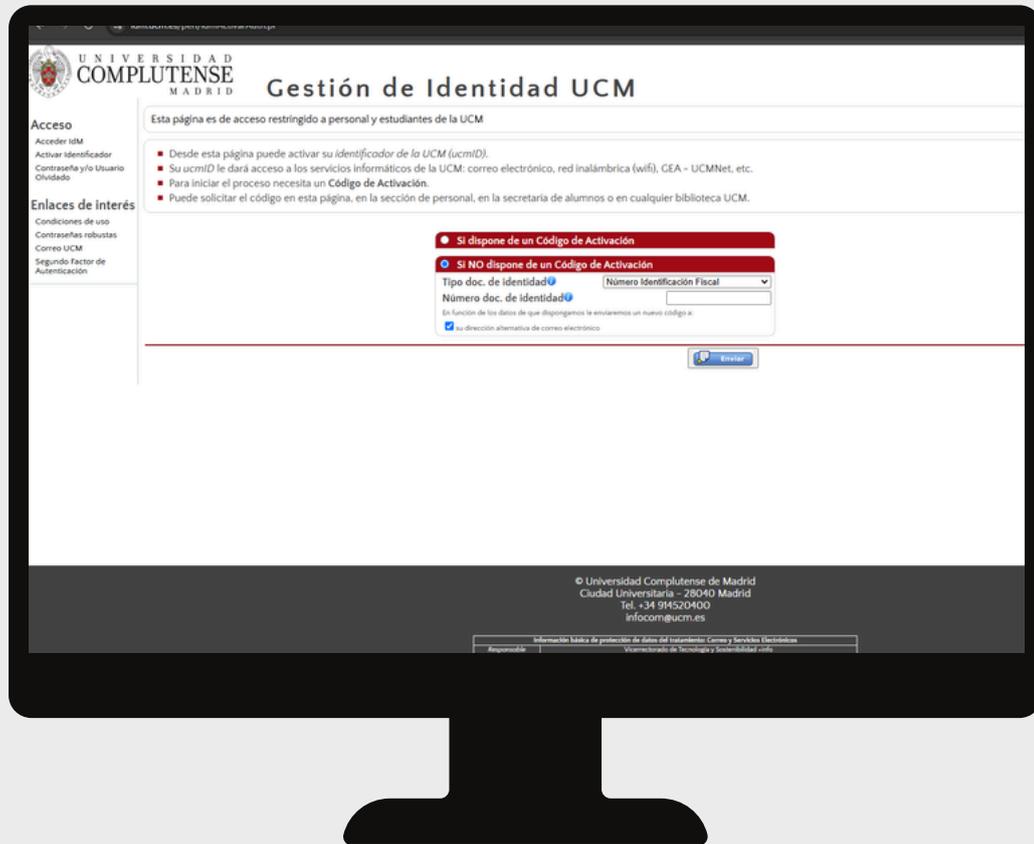


UCM en línea

Pinchamos en 'Activación de cuenta UCM (identificador)

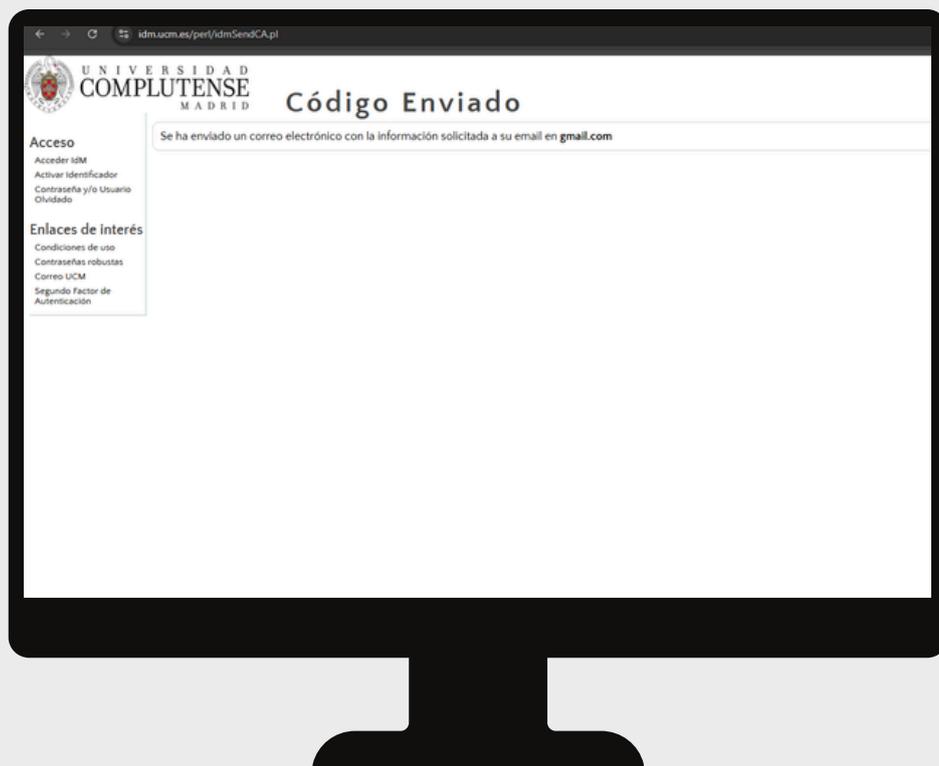
3

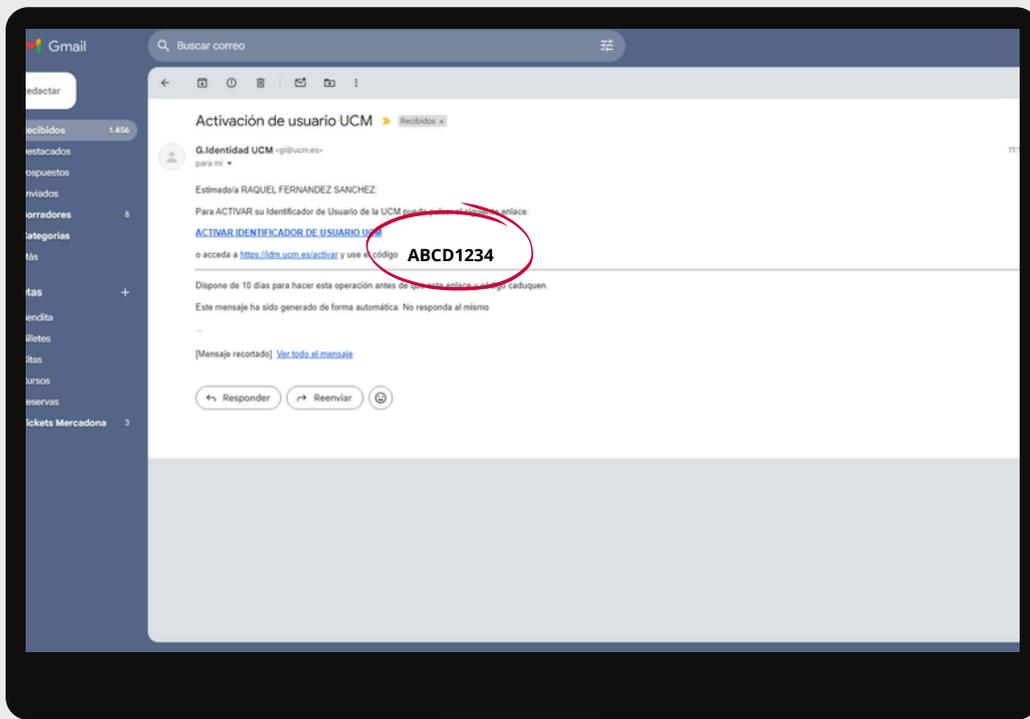




4

Le damos a 'Si no dispone de un Código de Activación' y ponemos el DNI

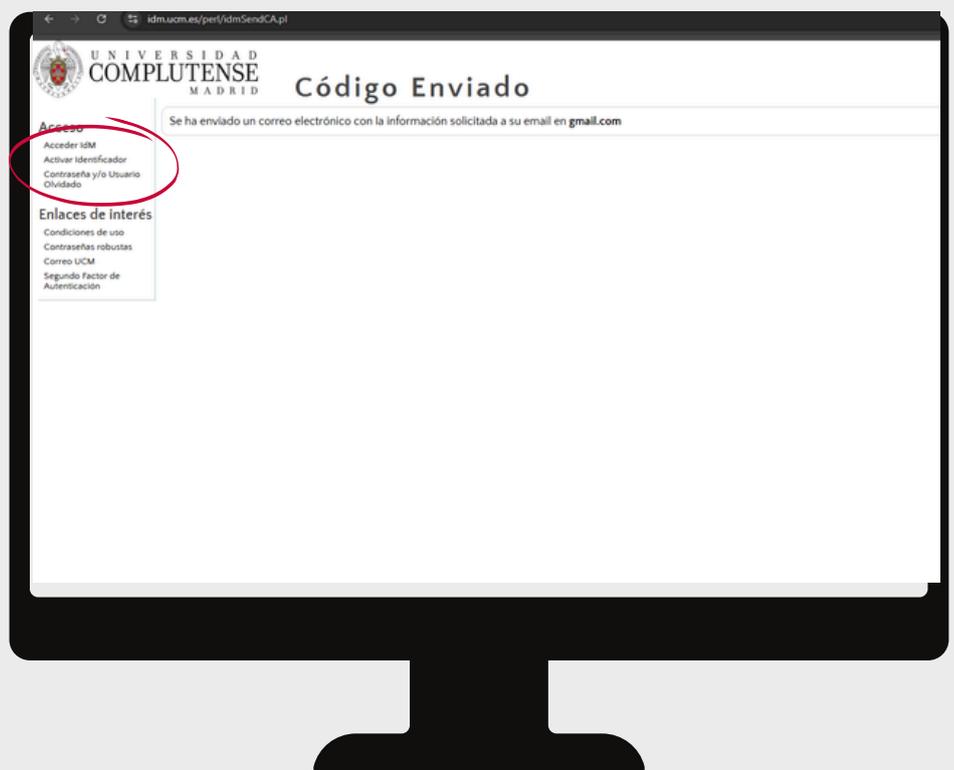




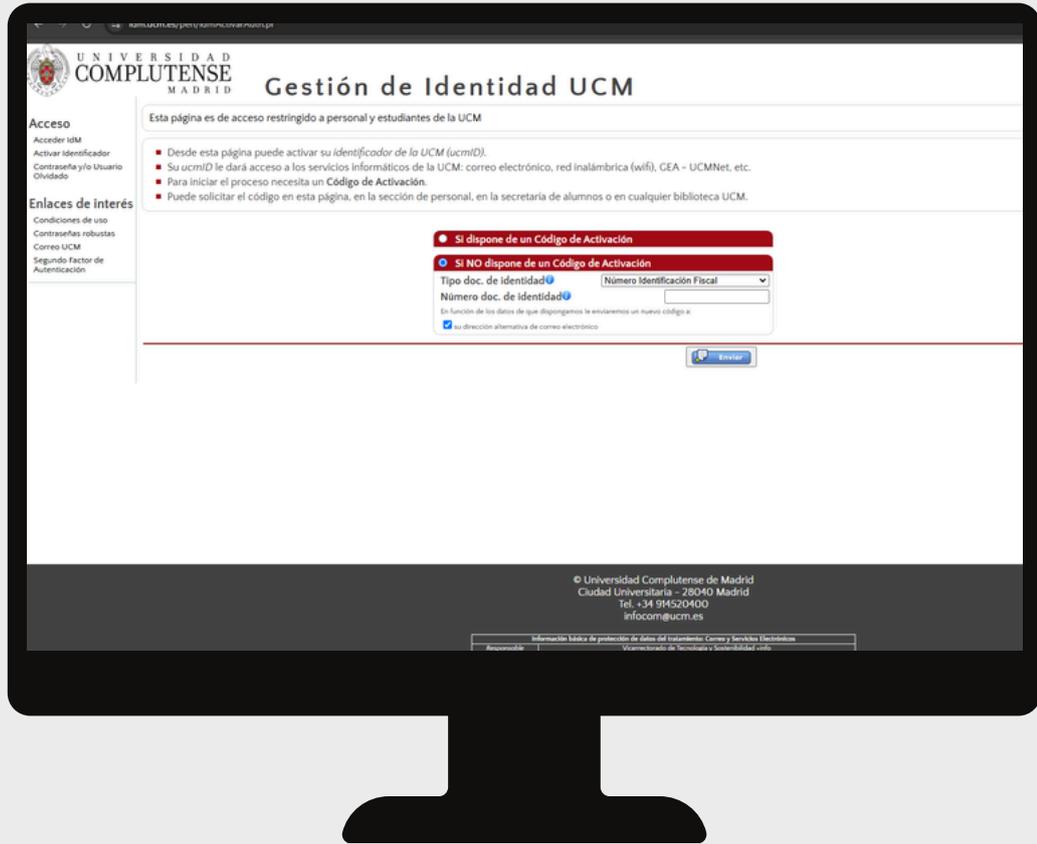
Comprueba
el SPAM

5

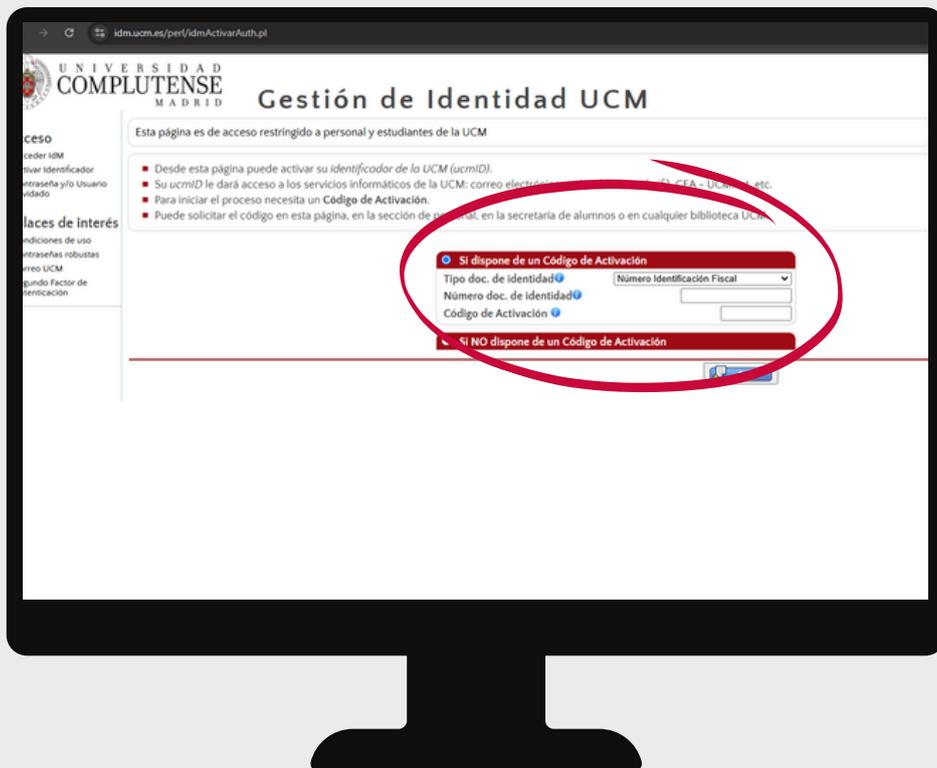
Apunta este código, vuelve a la página de 'Gestión de Identidad', pincha en '**Activar Identificador**', situado en la columna izquierda.



6

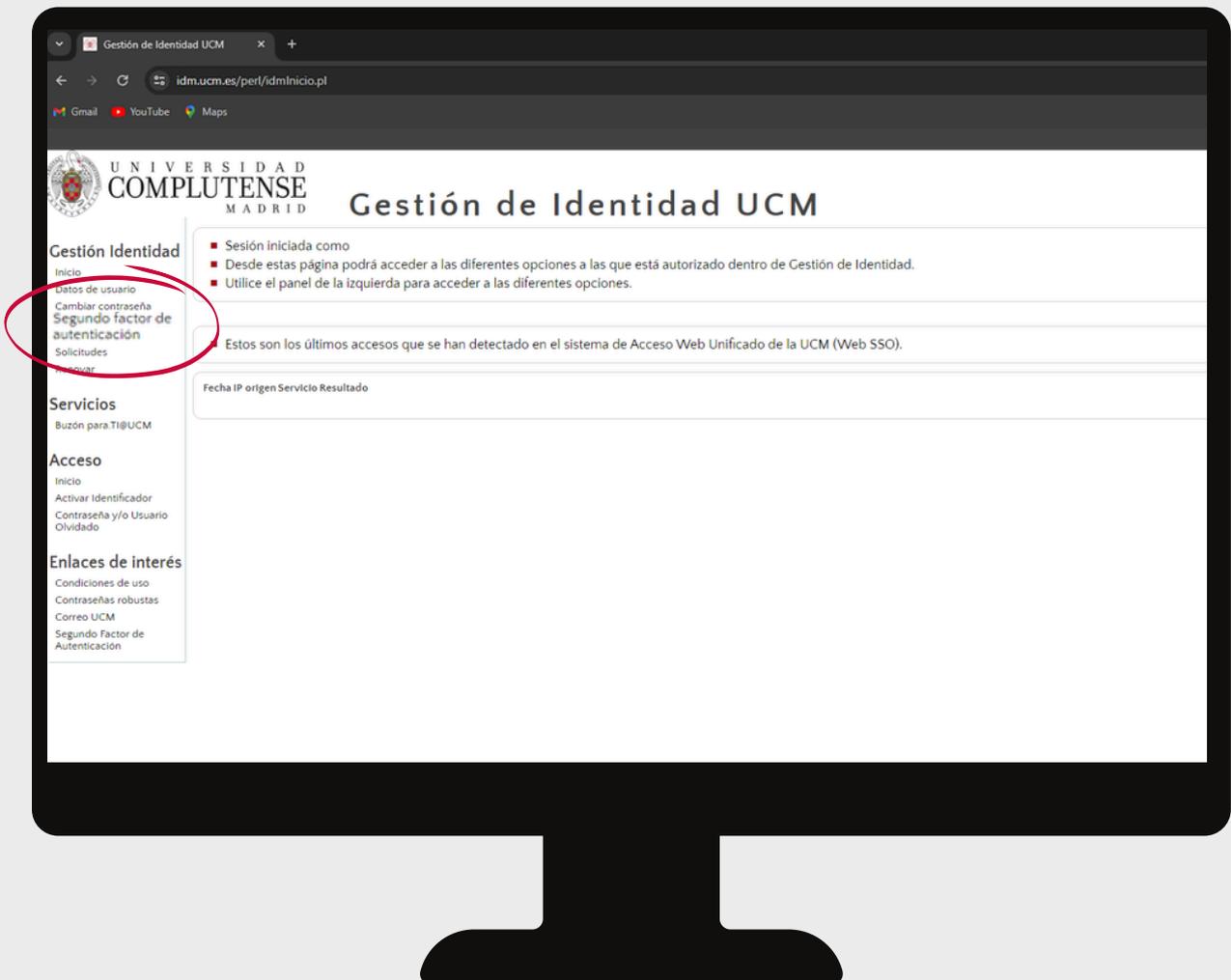


Pincha en 'SI dispone de Código de Activación' y rellena los datos



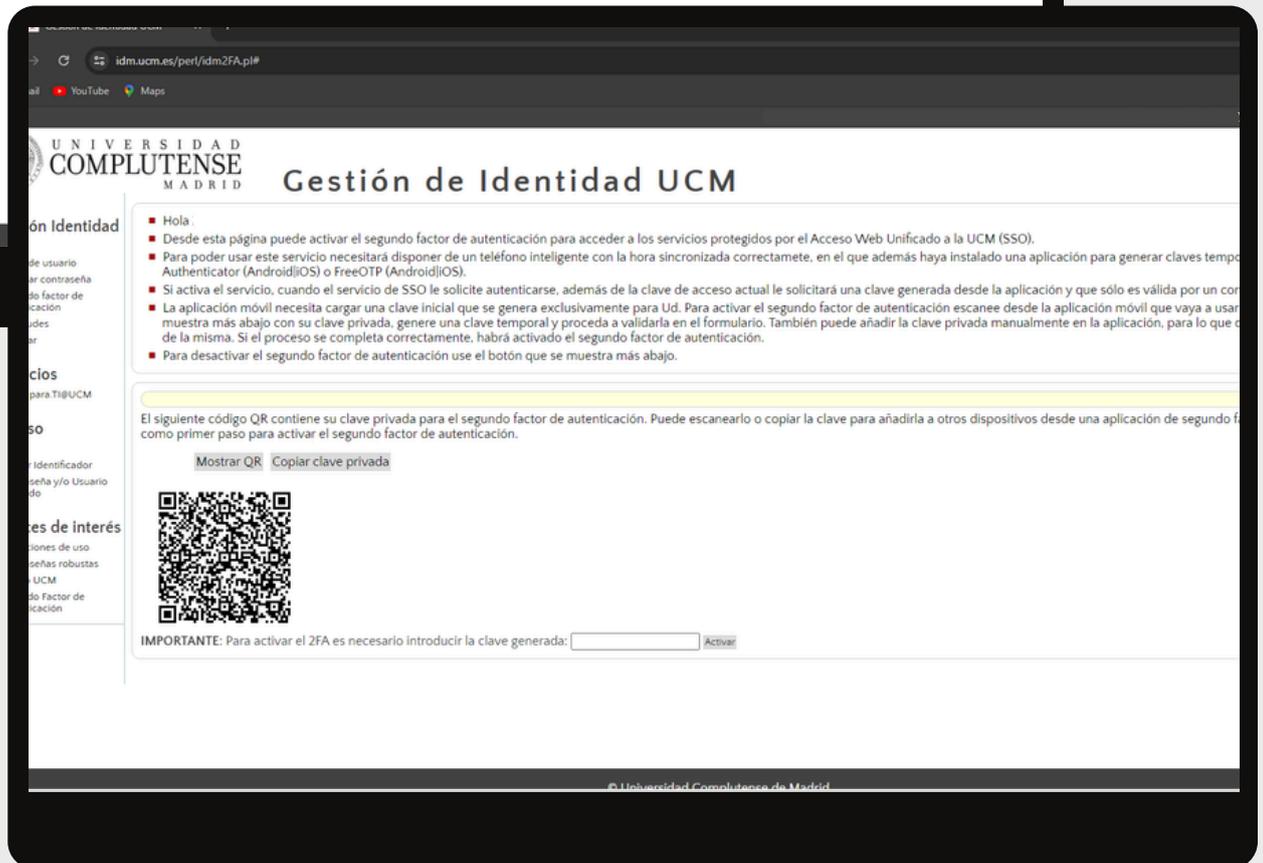
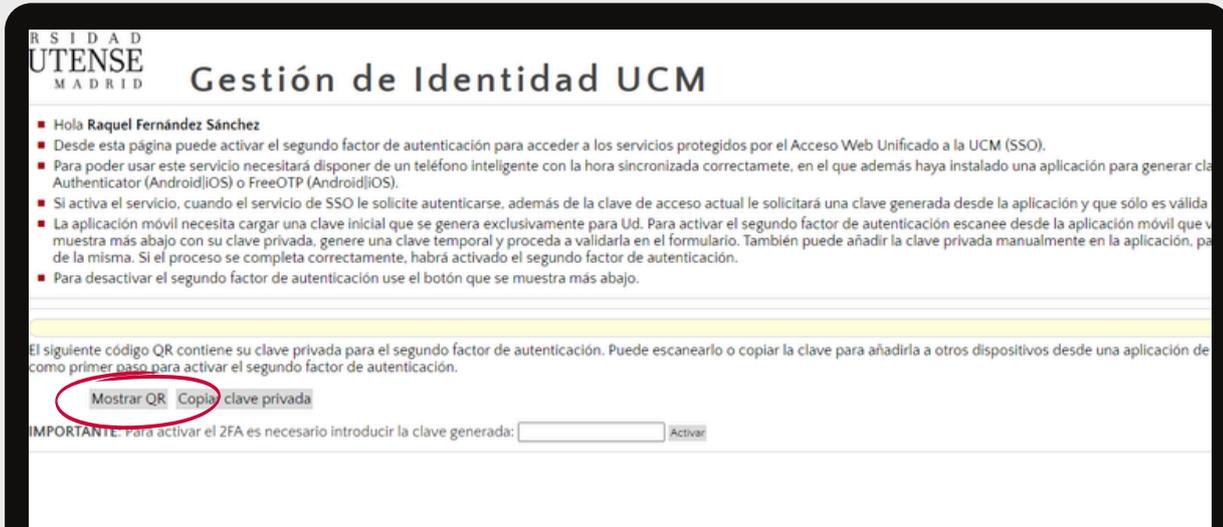
7

Pinchamos en '**Segundo factor de autenticación**' que aparece en la columna izquierda, la 4^o opción.



8

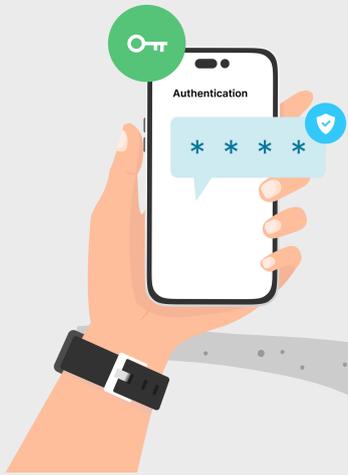
Una vez hecho esto, pinchamos en **'Mostrar QR'** y **dejamos esta página abierta.**



2 OPCIONES:

MÓVIL

Página 14

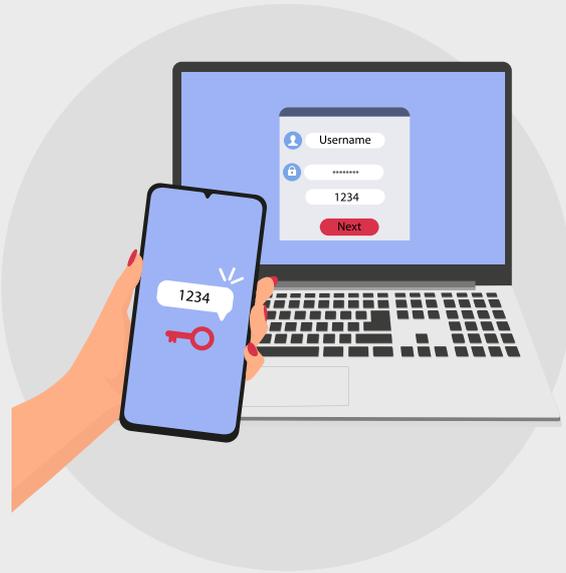


ORDENADOR

Página 21

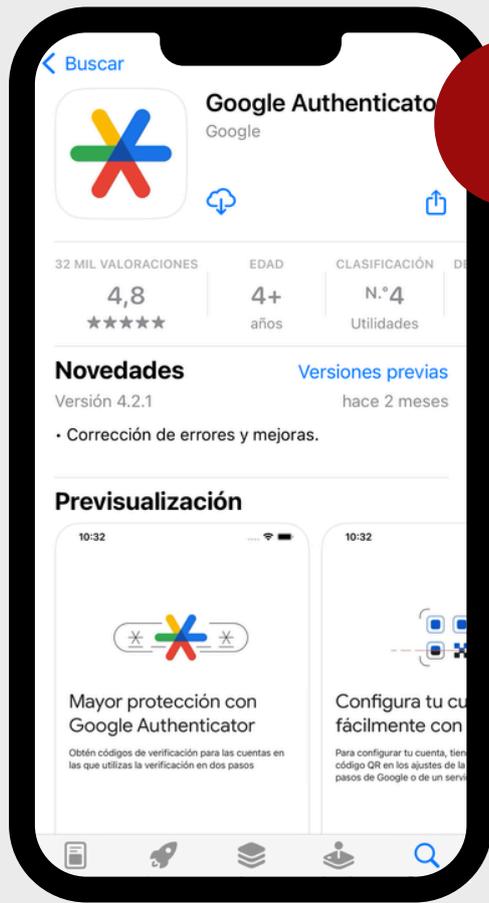


Una vez hecho esto, puede elegir **introducir los códigos de un solo uso** o bien a través del **móvil** o bien con el **ordenador**. A continuación, te enseñamos el **paso a paso** de cómo hacerlo.



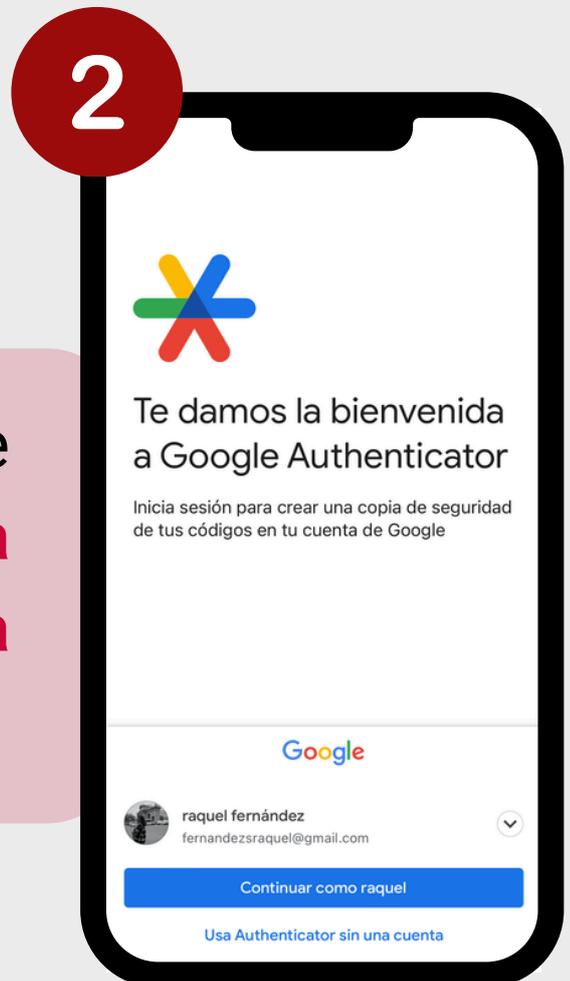
2

**SEGUNDO FACTOR DE
AUTENTICACIÓN EN EL
MÓVIL**



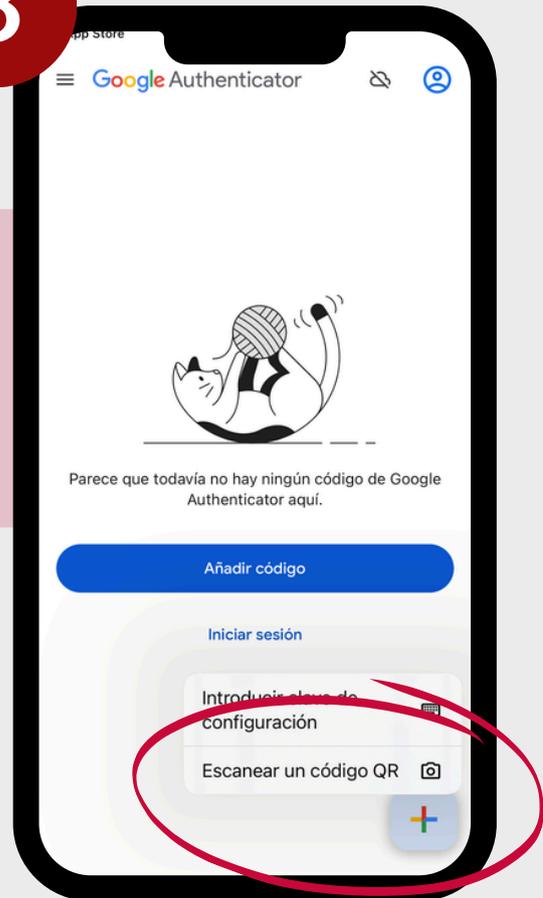
Ahora nos vamos al móvil y descargamos la Aplicación **'GOOGLE AUTHENTICATOR'**.

Una vez descargada le damos a **'Usa Authenticator sin una cuenta'**

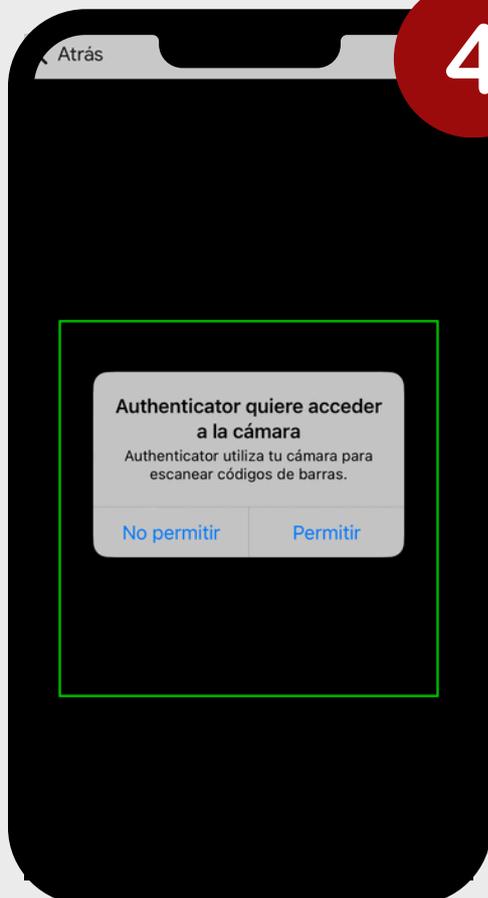


3

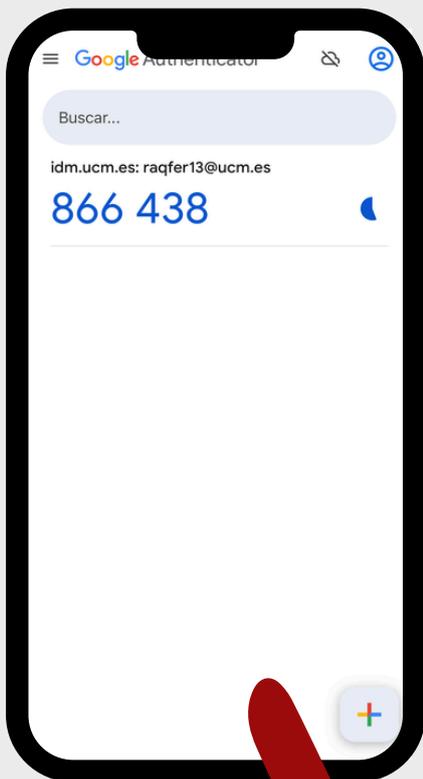
Pinchamos en el '+' y en 'Escanear un código QR'



4

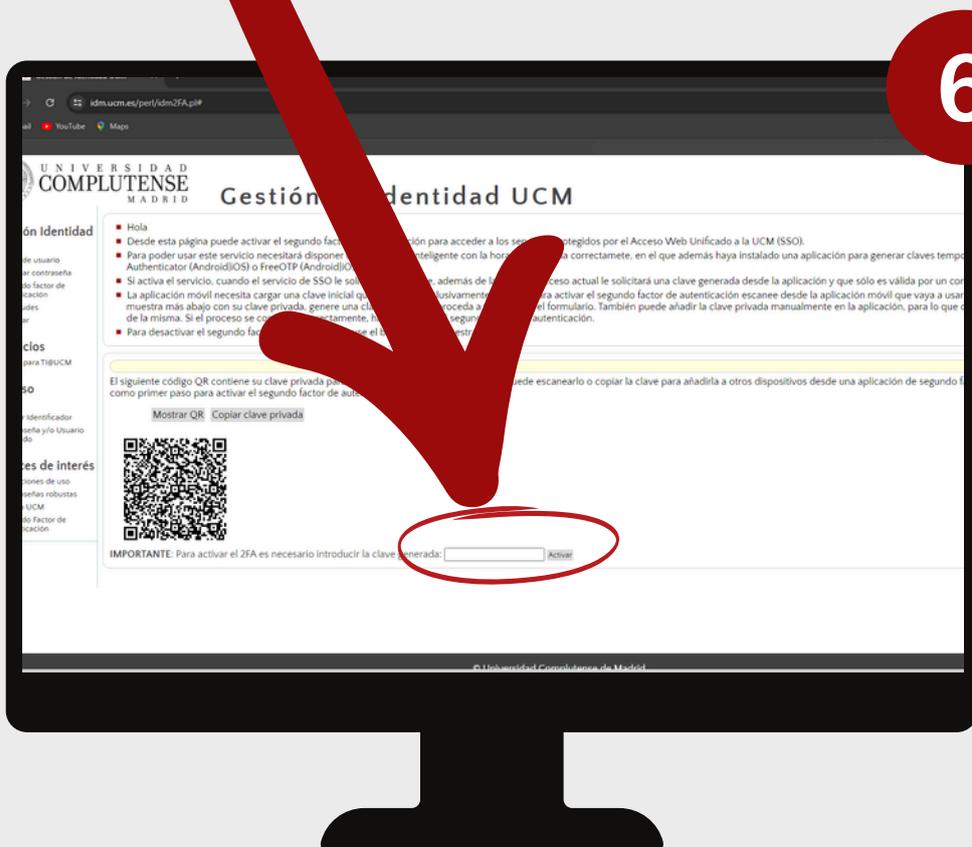


Damos **permiso** para **acceder a la cámara**



5

Estos **códigos** se **renuevan** cada 30 segundos, es decir, que son **temporales**.

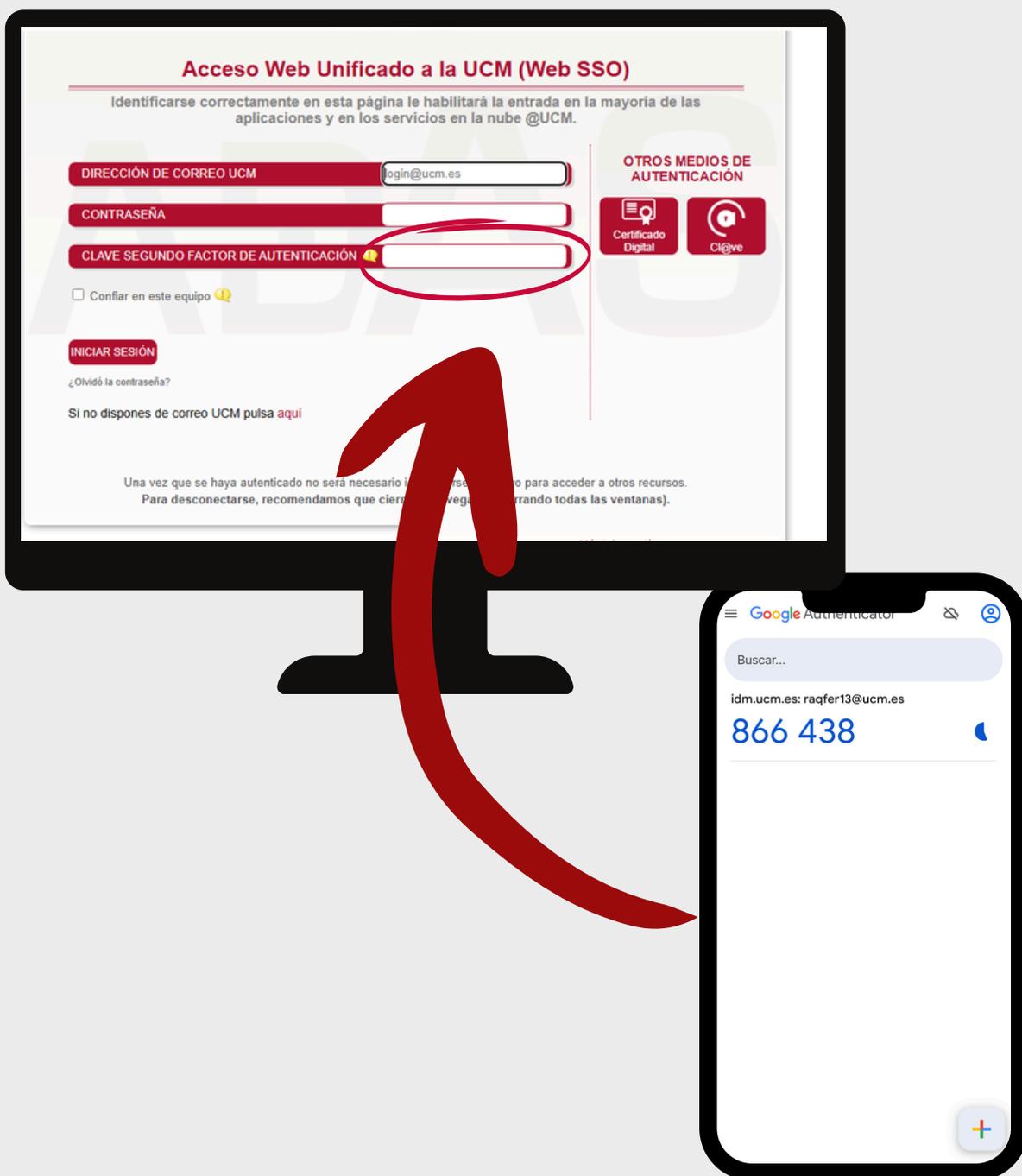


6

Introducimos el código del móvil y le damos a **'ACTIVAR'**.

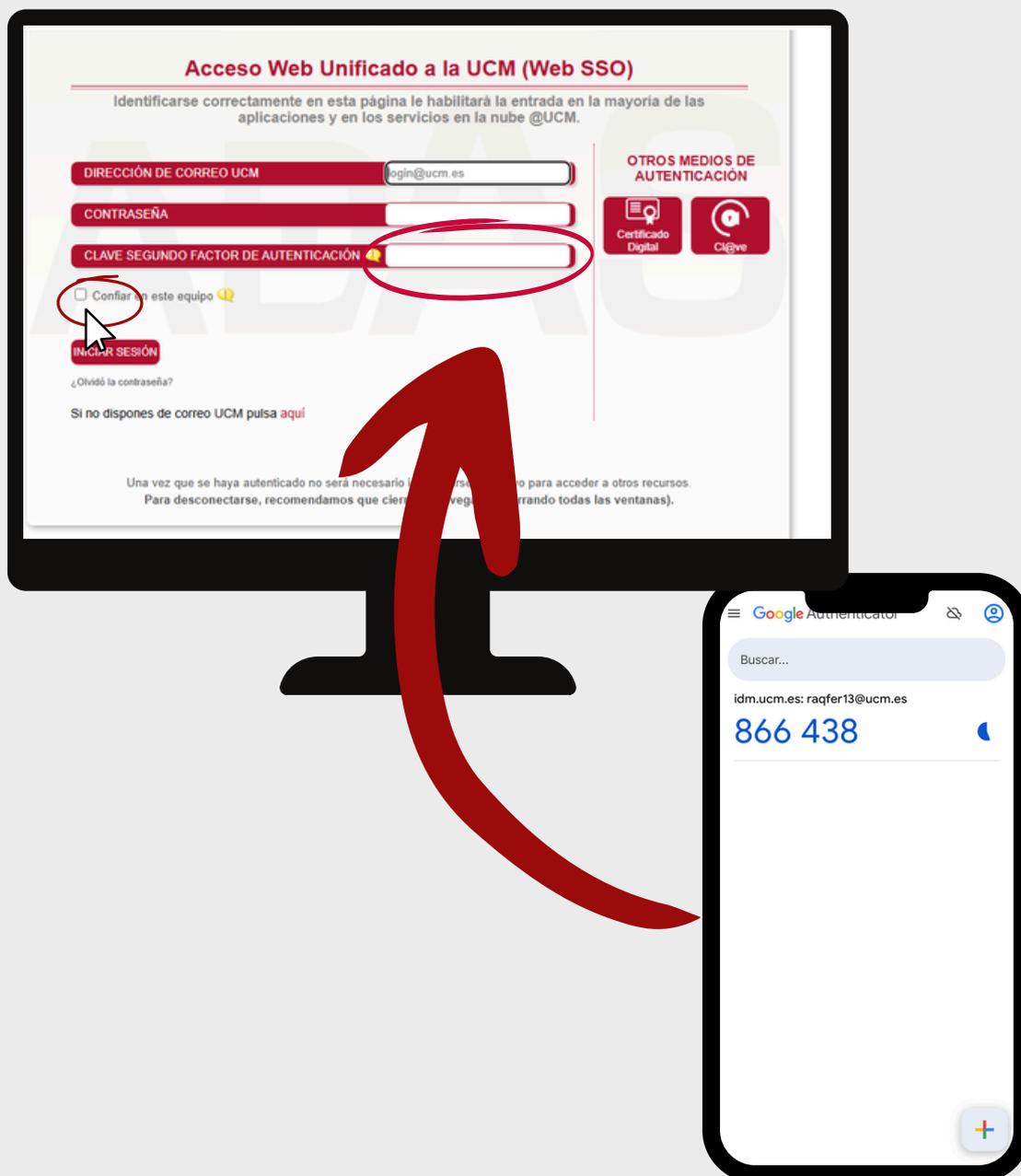
Para iniciar sesión, introducimos el correo UCM y la contraseña junto con el Código de Autenticación.

7



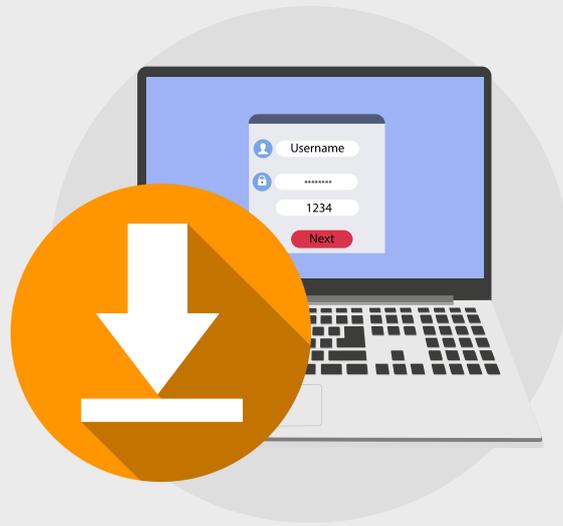
Si le damos a **'Confiar en equipo'**, no nos pediría el Segundo Factor durante 15 días.

8





Si hemos seguido correctamente estos pasos, ya tenemos activado el Segundo Factor de Autenticación.



3

**SEGUNDO FACTOR DE
AUTENTICACIÓN EN EL
ORDENADOR**

En este caso tienes que descargar una **extensión**:

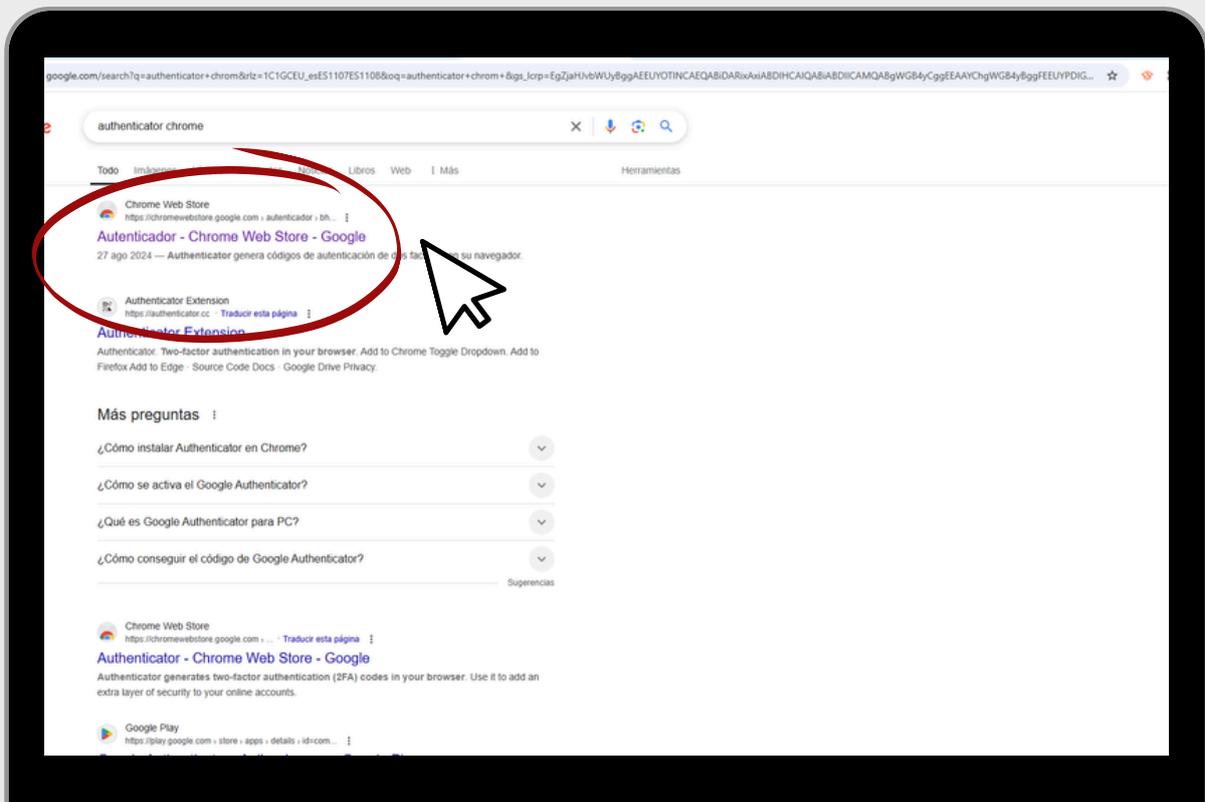
Es una app que se añade a **Chrome**, para generar las contraseñas de un solo uso, cada vez que necesites iniciar sesión.

No te preocupes si te suena algo técnico, es sencillo y aquí te explicamos el paso a paso.



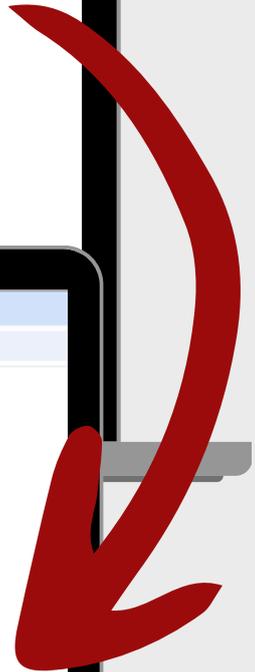
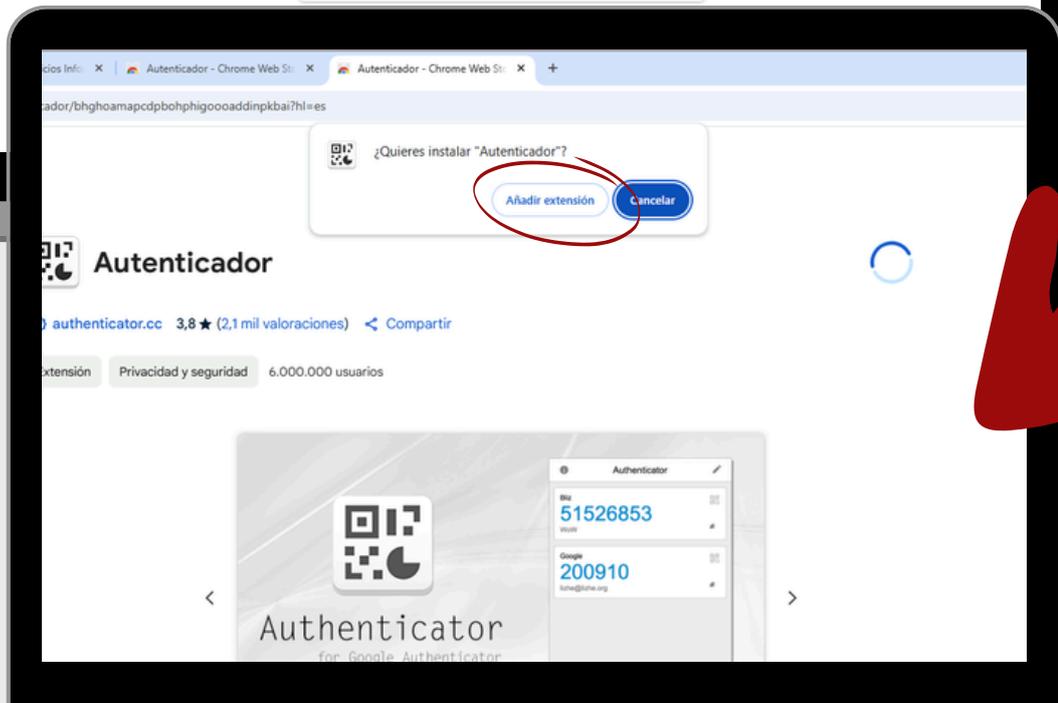
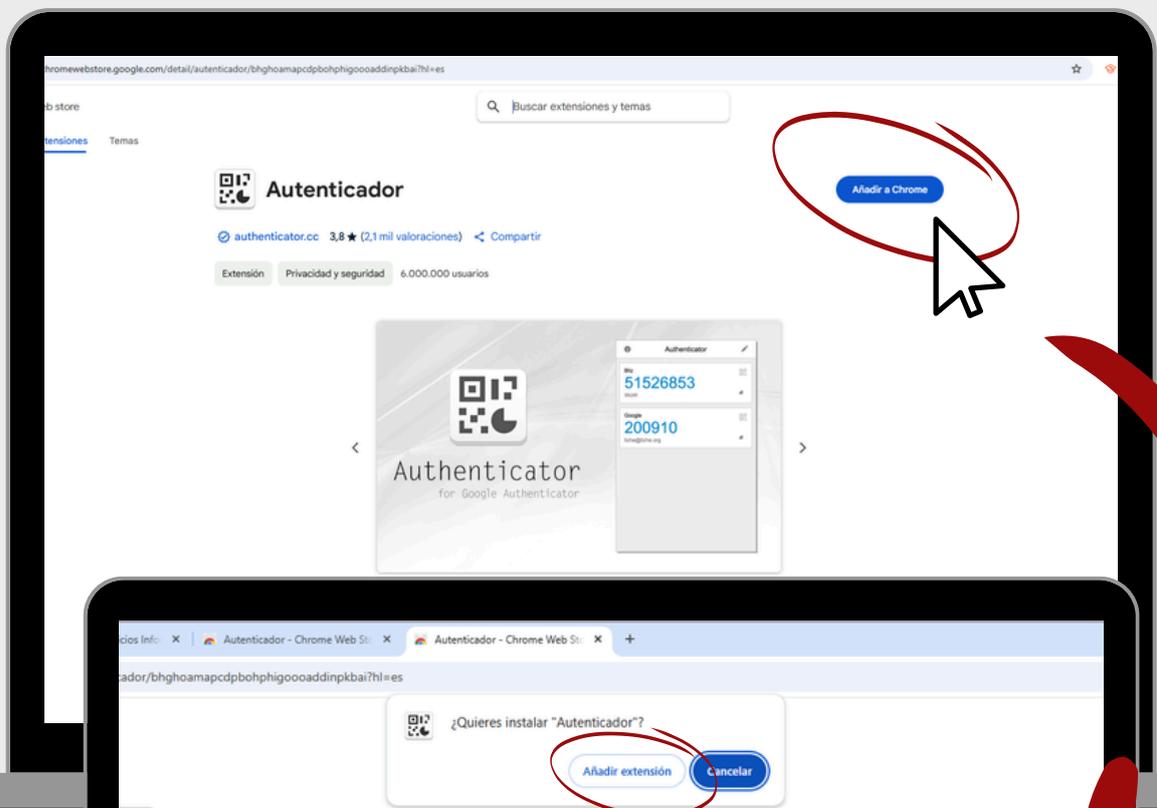
1

En el navegador Chrome busca **“authenticator chrome”** o pinchas aquí.

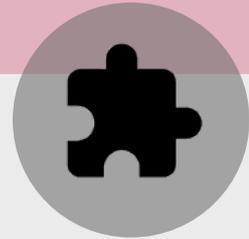


2

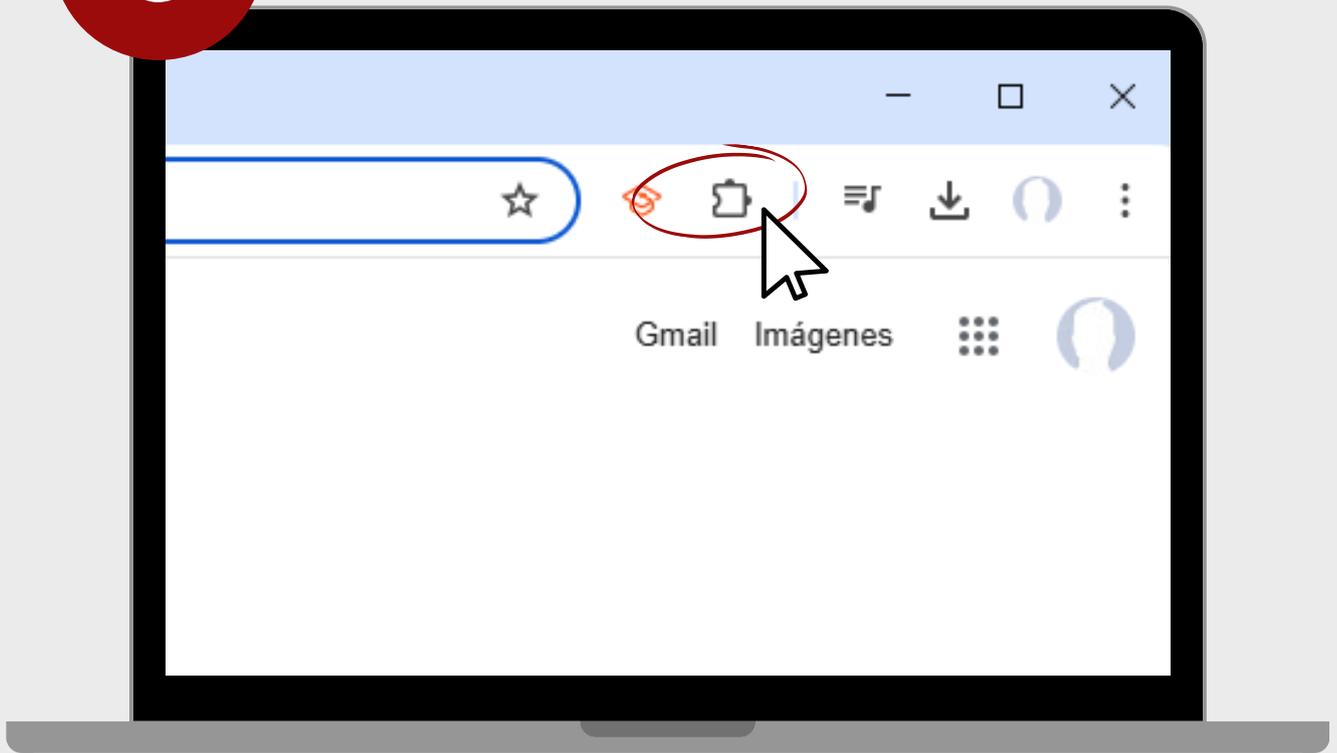
Clickea en **“Añadir a Chrome”**, y después en **“Añadir extensión”**



Para **encontrar y fijar la extensión**, pincha en este icono ubicado en la esquina superior derecha:

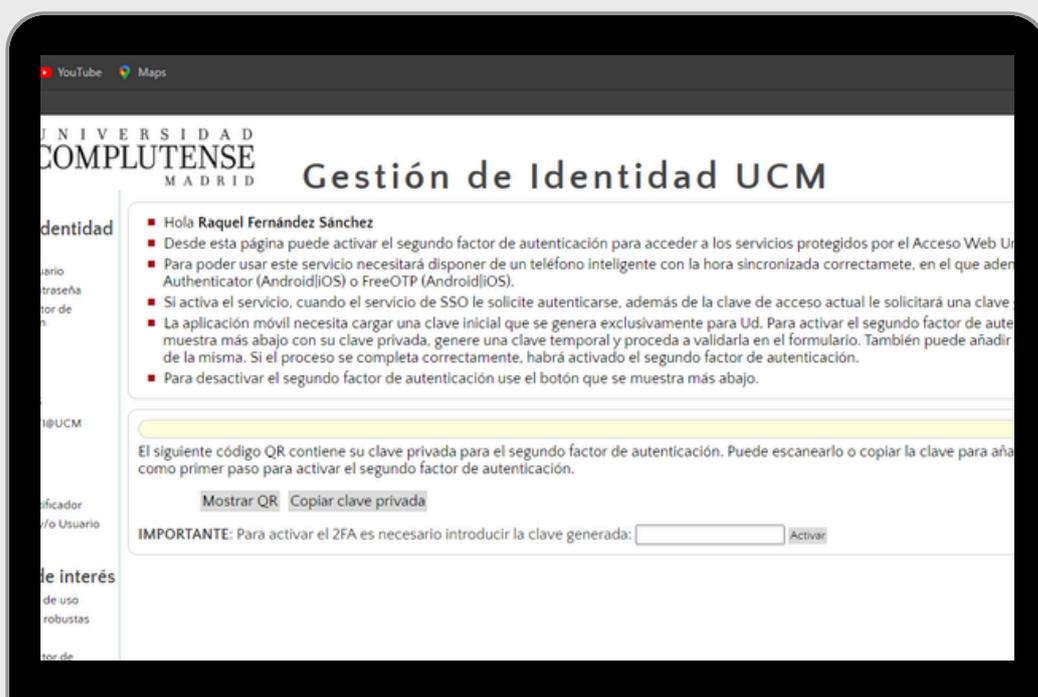


3



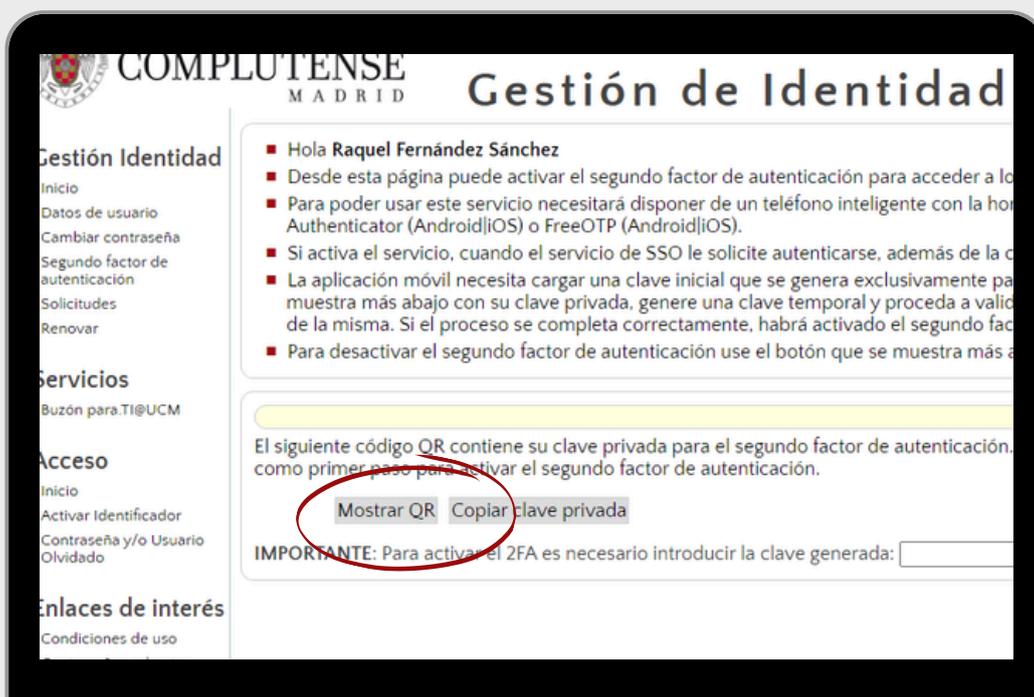
Vuelve a la página del segundo factor de autenticación

4



5

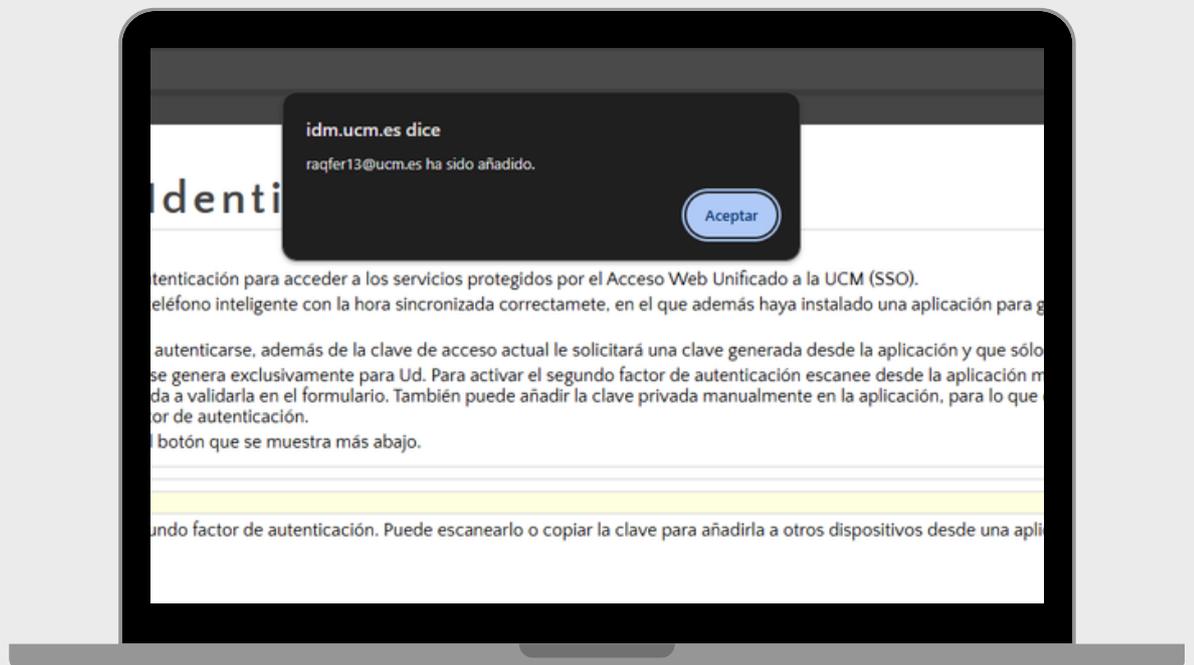
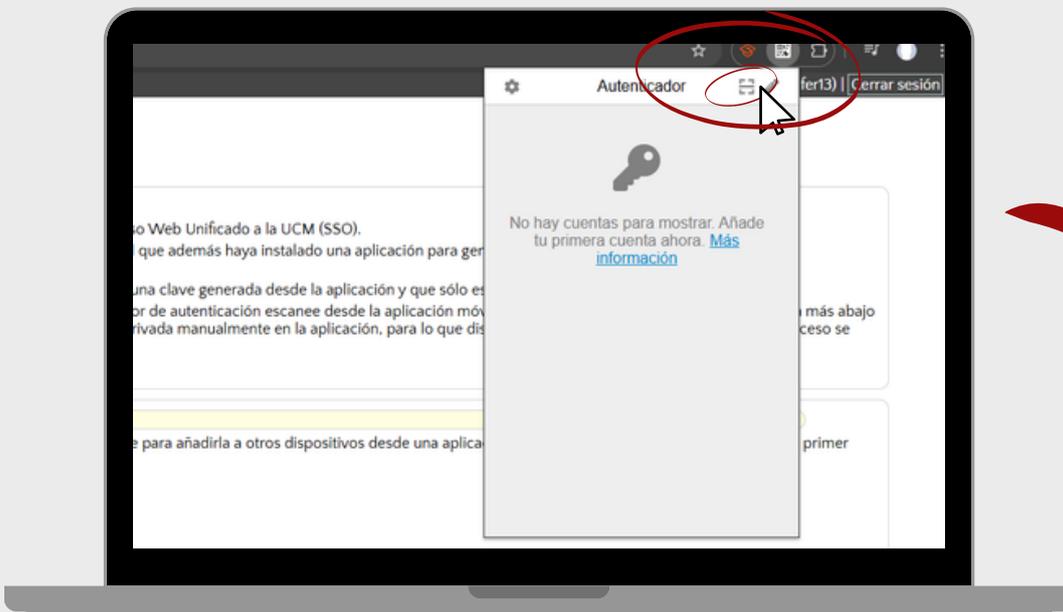
Clickea en “Mostrar QR”



Comprueba que la hora del PC y del móvil coincida para poder continuar

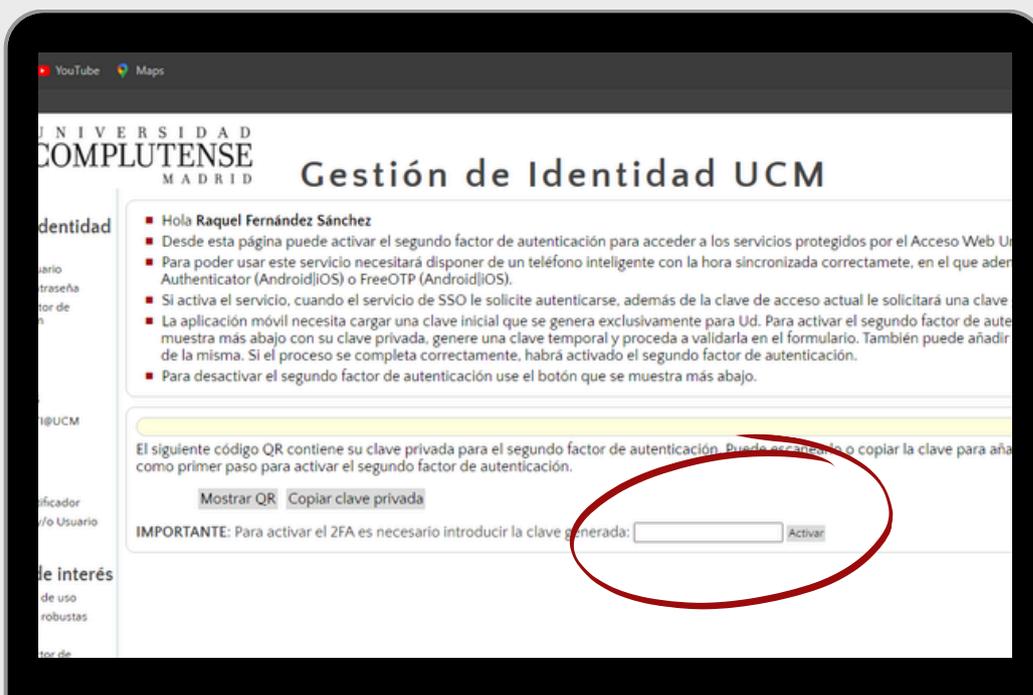
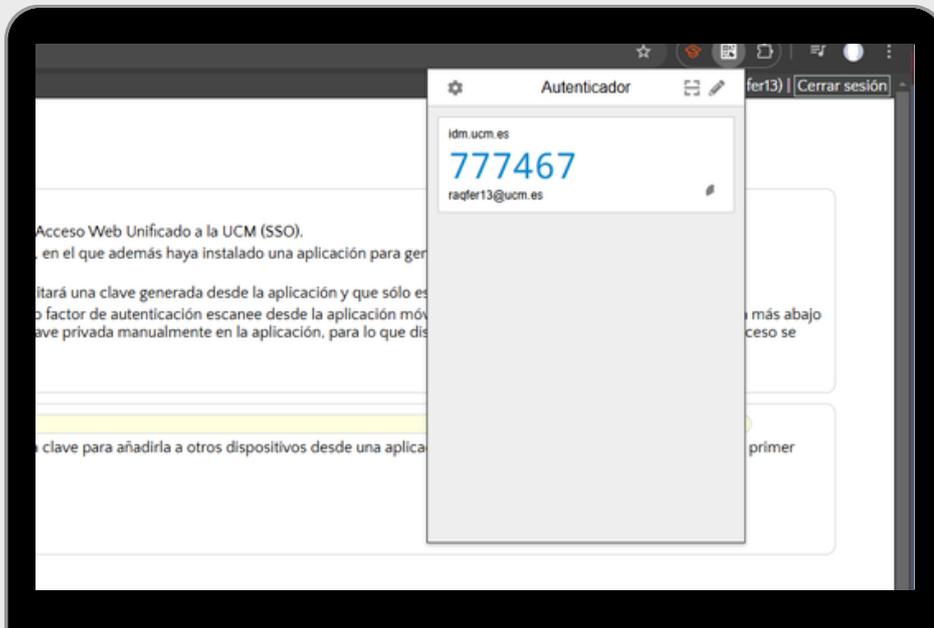
6

Pulsa en la extensión y en el icono de "Escanear QR". Selecciona el QR con el puntero, aparecerá una ventana avisándote de que tu correo "usuario@ucm" ya se ha añadido.



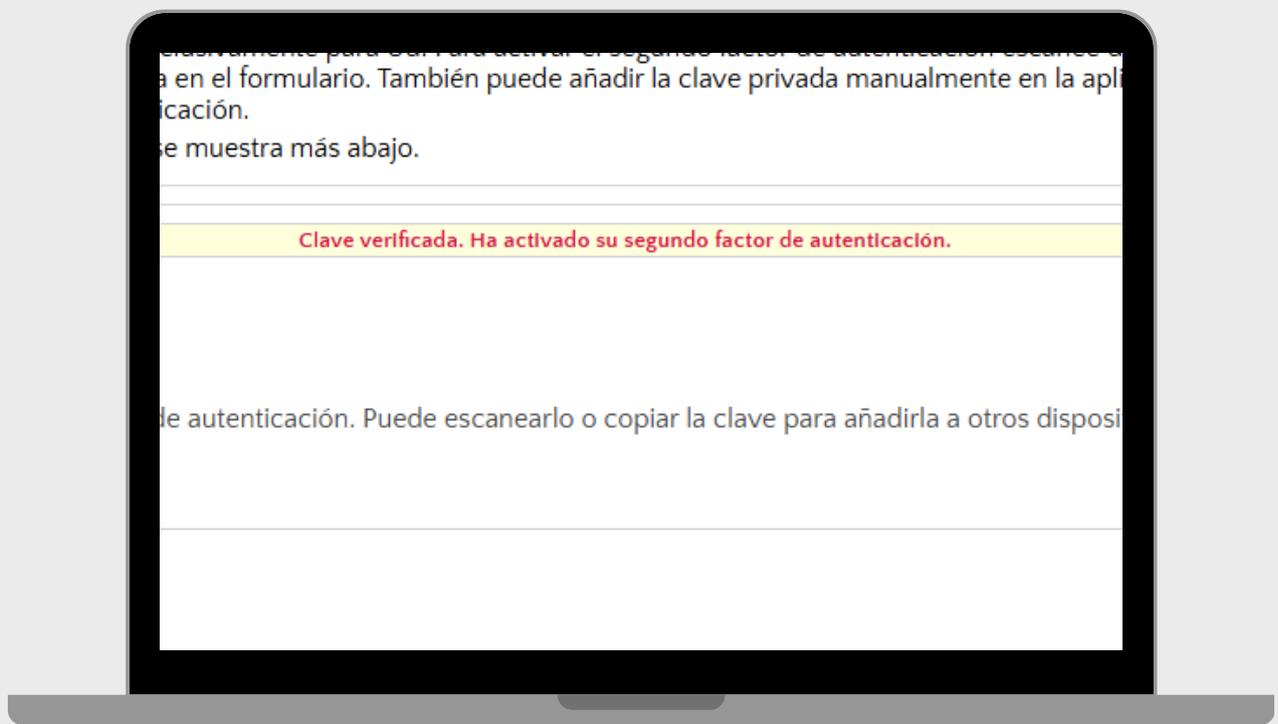
7

Copia la clave generada y haz clic en activar.



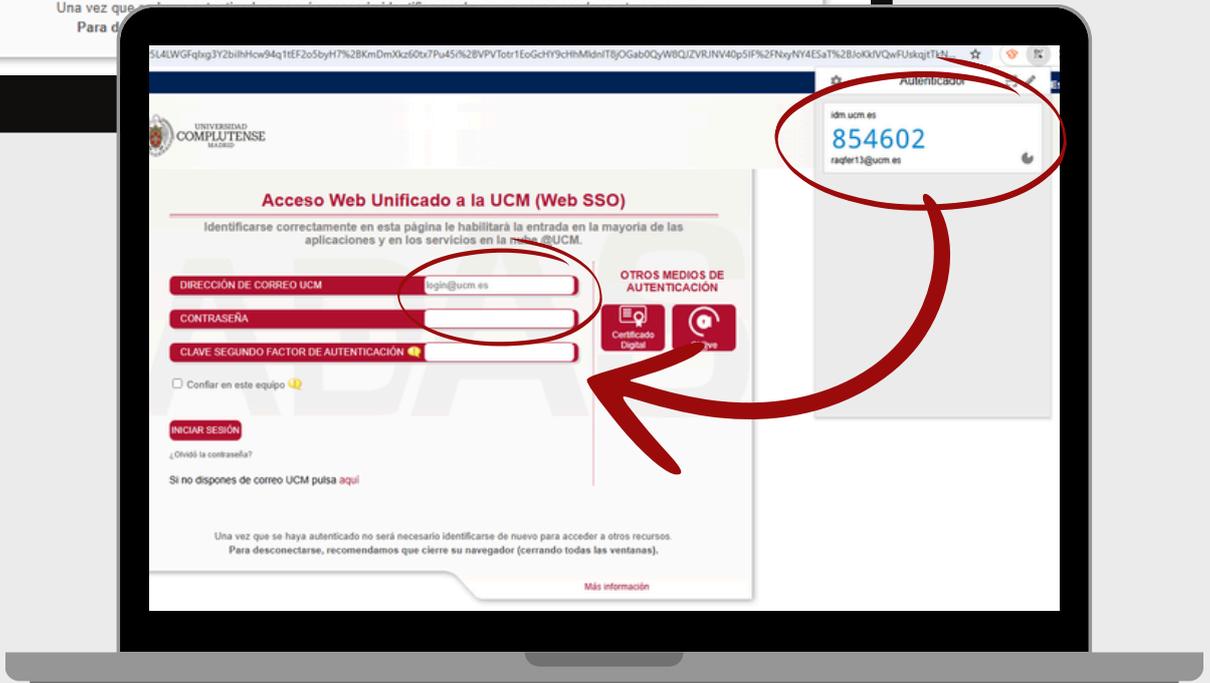
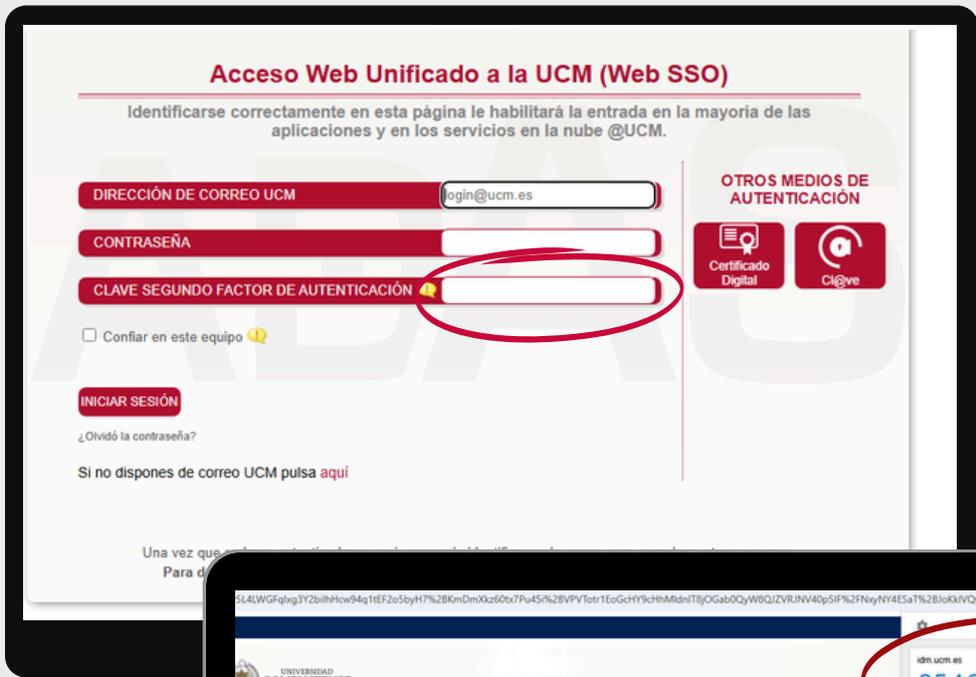
8

Y ya estaría activado el segundo factor de autenticación.



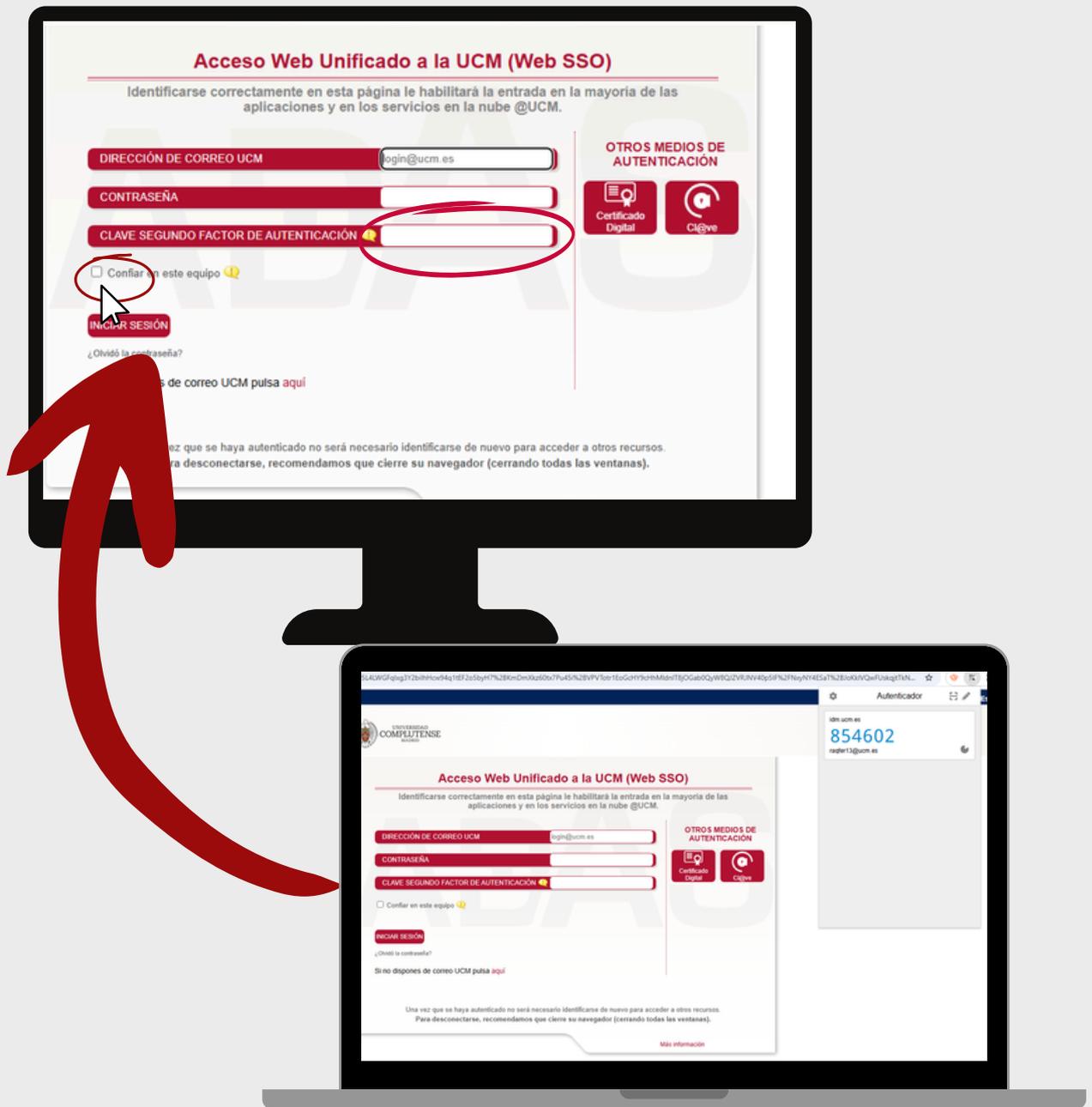
Para iniciar sesión, introducimos el correo UCM y la contraseña junto con el Código de Autenticación, que aparecerá si le damos al icono de 'Extensión'.

9



Si le damos a **'Confiar en equipo'**, no nos pediría el Segundo Factor durante 15 días.

10





Si hemos seguido correctamente estos pasos, ya tenemos activado el Segundo Factor de Autenticación en el ordenador.



UNIVERSIDAD PARA MAYORES

UNIVERSIDAD COMPLUTENSE DE MADRID