1. ¿Por qué es importante?

El 2FA obliga al usuario a **tener algo** (normalmente una contraseña de un solo uso, OTP, por su significado en ingles One Time Password), aparte de **conocer algo** (contraseña habitual).

En caso de vulneración de la cuenta, el atacante necesitará la OTP para poder acceder.

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

2. Cómo activar 2FA

MUY IMPORTANTE: Comprobar que la hora es la correcta, tanto en el móvil como en el ordenador desde el que se va a hacer la activación del 2FA.

1. Descargar en el teléfono móvil, desde Google Play o desde AppStore, la aplicación Google Authenticator.

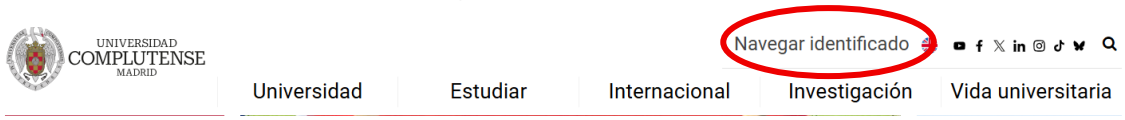
ANDROID

https://play.google.com/store/apps/details?id=com.google.android.apps.authenticator2&hl=es

IPHONE

https://apps.apple.com/es/app/google-authenticator/id388497605

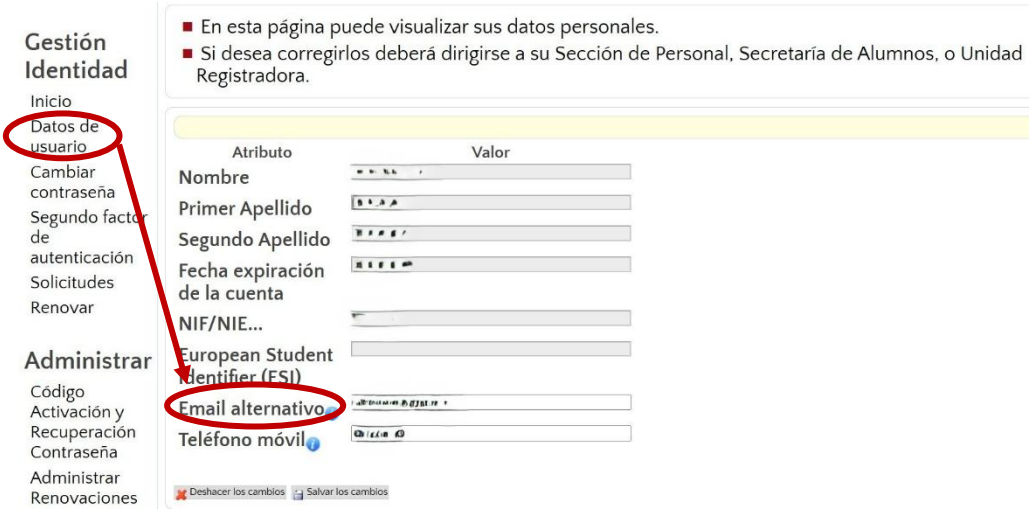
2._Desde el ordenador, entrar en la página de la UCM (www.ucm.es) y navegar identificado con el correo de la UCM y la contraseña de este.



Una vez identificados, pinchar en su nombre.

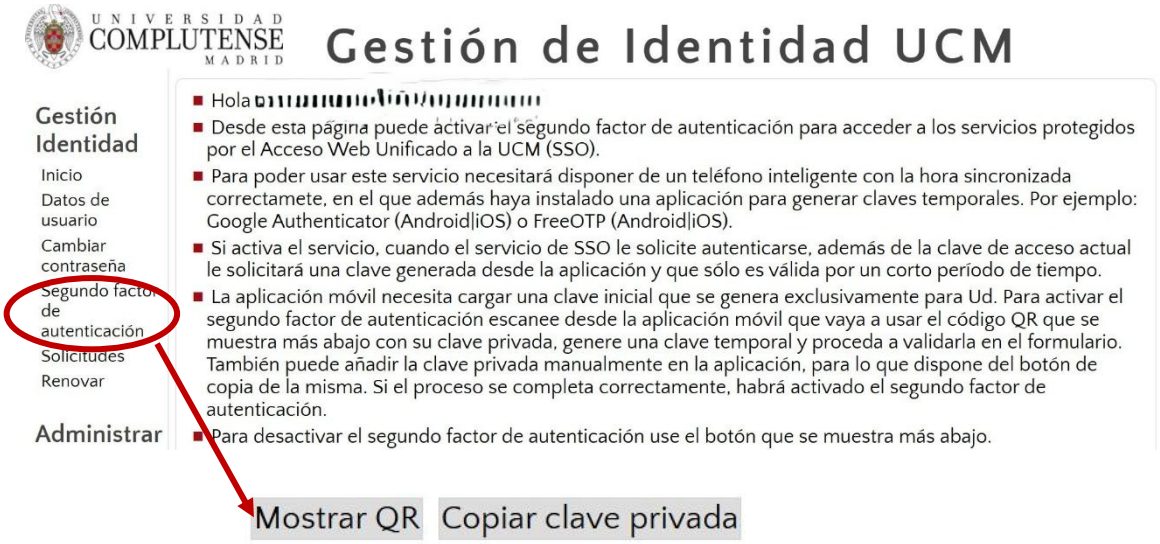
3._Acceder a Gestión de Identidad (IDM) idm.ucm.es

MUY IMPORTANTE: Comprobar que tiene un email alternativo en Datos de Usuario (columna de la izquierda). De no ser así, incluirlo y salvar los cambios.



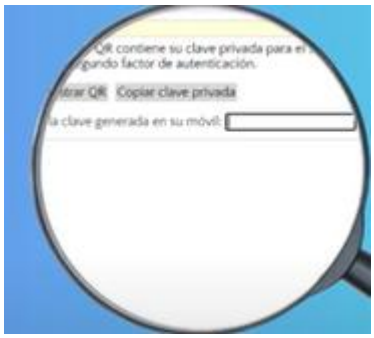
Esto facilitará problemas en caso de tener algún incidente con el Segundo Factor (2FA).

4. _Pinchar en Segundo Factor de Autenticación en la columna de la izquierda y a continuación Mostrar QR.



5._Desde el móvil abrir la aplicación Google Authenticator, con cuenta UCM o sin una cuenta, y escanear el código QR del ordenador (en el móvil se abre automáticamente la cámara para escanear el código del ordenador y a partir de este momento, cada vez que se abra en el móvil la aplicación "Google Authenticator" se generará un número que dura unos segundos).

MUY IMPORTANTE: Después de abrir la aplicación se introduce el código en la casilla correspondiente para activar el 2FA.



Desde el momento en que el 2FA esté activado, siempre que se quiera acceder a nuestra cuenta, hay que abrir en el móvil la aplicación "Google Authenticator" e introducir ese código en el cuadro de "Segundo factor de autenticación". Si se marca la casilla de "confiar en este equipo" no pedirá el 2FA durante 14 días en el dispositivo en el que se esté accediendo.

3. Problemas frecuentes

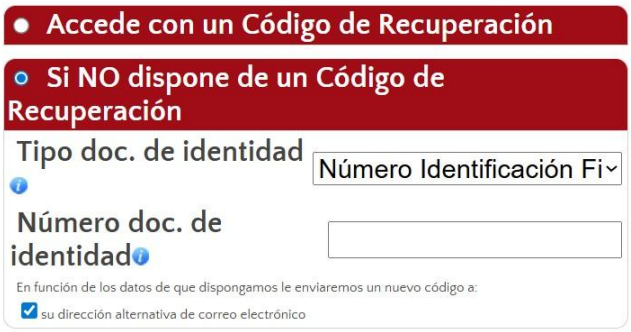
- **ERROR CON EL CÓDIGO 2FA: Comprobar que la fecha y hora es la correcta.**
- **CAMBIO DE DISPOSITIVO:** Para volver a instalar la aplicación Authenticator

1 Acceder a la página de la UCM (www.ucm.es)
2 Arriba a la derecha - Navegar identificado

3 Olvidó la contraseña

4 Marcar la opción “Si no dispone de un código de Recuperación”

5 Indique el Tipo de documento de identidad y el número de dicho documento



6 Se le enviará un Código de Reseteo a su dirección de correo electrónico alternativa y un enlace para acceder de nuevo a Gestión de Identidad.
Desde ahí debe volver **a desactivar el 2FA y volver a activarlo** siguiendo los pasos anteriormente explicados en esta ayuda.