



## 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 inglés 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

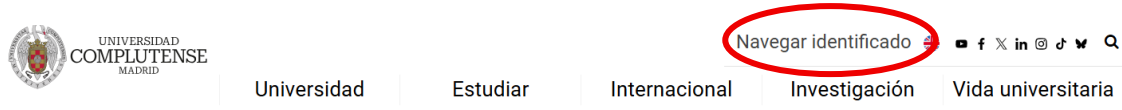
<https://play.google.com/store/apps/details?id=com.google.android.apps.authenticator2&hl=es>



IPHONE

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

2. Desde el ordenador, entrar en la página de la UCM ( [www.ucm.es](http://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](http://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.

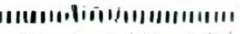
■ En esta página puede visualizar sus datos personales.  
■ Si desea corregirlos deberá dirigirse a su Sección de Personal, Secretaría de Alumnos, o Unidad Registradora.

Atributo	Valor
Nombre	<input type="text"/>
Primer Apellido	<input type="text"/>
Segundo Apellido	<input type="text"/>
Fecha expiración de la cuenta	<input type="text"/>
NIF/NIE...	<input type="text"/>
European Student Identifier (ESI)	<input type="text"/>
<b>Email alternativo</b>	<input type="text"/>
Teléfono móvil	<input type="text"/>

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.

**Gestión de Identidad UCM**

■ Hola 

■ Desde esta página puede activar el segundo factor de autenticación para acceder a los servicios protegidos por el Acceso Web Unificado a la UCM (SSO).

■ Para poder usar este servicio necesitará disponer de un teléfono inteligente con la hora sincronizada correctamente, en el que además haya instalado una aplicación para generar claves temporales. Por ejemplo: Google Authenticator (Android/iOS) o FreeOTP (Android/iOS).

■ Si activa el servicio, cuando el servicio de SSO le solicite autenticarse, además de la clave de acceso actual le solicitará una clave generada desde la aplicación y que sólo es válida por un corto período de tiempo.

■ La aplicación móvil necesita cargar una clave inicial que se genera exclusivamente para Ud. Para activar el segundo factor de autenticación escanee desde la aplicación móvil que vaya a usar el código QR que se muestra más abajo con su clave privada, genere una clave temporal y proceda a validarla en el formulario. También puede añadir la clave privada manualmente en la aplicación, para lo que dispone del botón de copia de la misma. Si el proceso se completa correctamente, habrá activado el segundo factor de autenticación.

■ Para desactivar el segundo factor de autenticación use el botón que se muestra más abajo.

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.

UNIVERSIDAD  
COMPLUTENSE  
MADRID

### 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?](#)

**Si se utiliza tarjeta o DNle, debe introducirse en el lector adecuado antes de continuar.**

Una vez que se haya autenticado no será necesario identificarse de nuevo para acceder a otros recursos.  
Para desconectarse, recomendamos que cierre su navegador (cerrando todas las ventanas).

[Más información](#)

### 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](http://www.ucm.es))
- 2 Arriba a la derecha - Navegar identificado



- 3 Olvidó la contraseña

**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: login@ucm.es

CONTRASEÑA

CLAVE SEGUNDO FACTOR DE AUTENTICACIÓN

Confiar en este equipo

**INICIAR SESIÓN**

¿Olvidó la contraseña?

**OTROS MEDIOS DE AUTENTICACIÓN**

Certificado Digital Cl@ve

**Si se utiliza tarjeta o DNle, debe introducirse en el lector adecuado antes de continuar.**

Una vez que se haya autenticado no será necesario identificarse de nuevo para acceder a otros recursos.  
Para desconectarse, recomendamos que cierre su navegador (cerrando todas las ventanas).

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

**UNIVERSIDAD COMPLUTENSE MADRID**

## Gestión de Identidad UCM

Esta página es de acceso restringido a personal y estudiantes de la UCM

- Desde esta página puede establecer una nueva contraseña de acceso a los SSII de la UCM.
- Debe disponer de un **Código de Recuperación**.
- Los usuarios pueden solicitar el código en esta página, en la sección de personal o secretaría de su centro, o en cualquier biblioteca UCM.

**Acceso**

- Acceder IdM
- Activar Identificador
- Contraseña y/o Usuario
- Olvidado

**Enlaces de interés**

- Accede con un Código de Recuperación
- Si NO dispone de un Código de Recuperación

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

● Accede con un Código de Recuperación

○ Si NO dispone de un Código de Recuperación

Tipo doc. de identidad

Número doc. de identidad

su dirección alternativa de correo electrónico

- 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.