

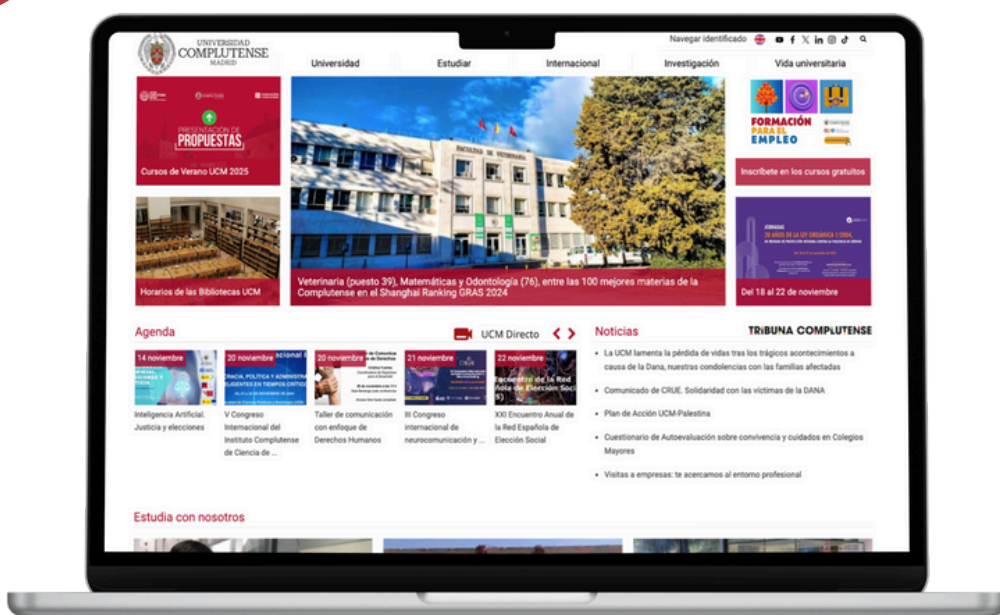
# SEGUNDO FACTOR DE AUTENTIFICACIÓN (2FA)

La autenticación de dos factores añade una capa adicional de seguridad a tu cuenta UCM. Aunque alguien consiga tu contraseña, no podrá iniciar sesión sin tener también acceso a tu teléfono móvil. Esto hace que tu cuenta sea mucho más segura.



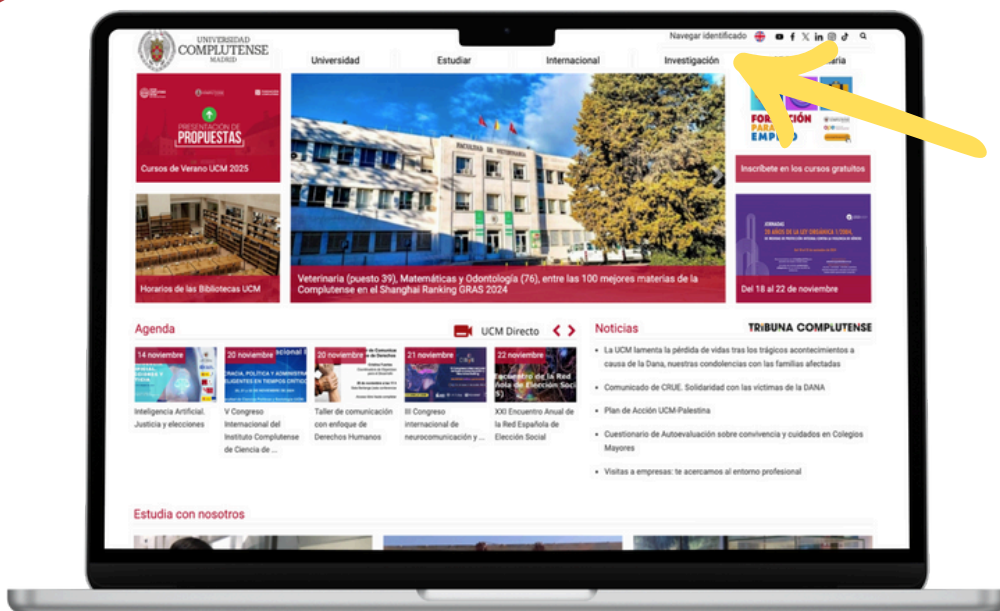
1

[www.ucm.es](http://www.ucm.es)



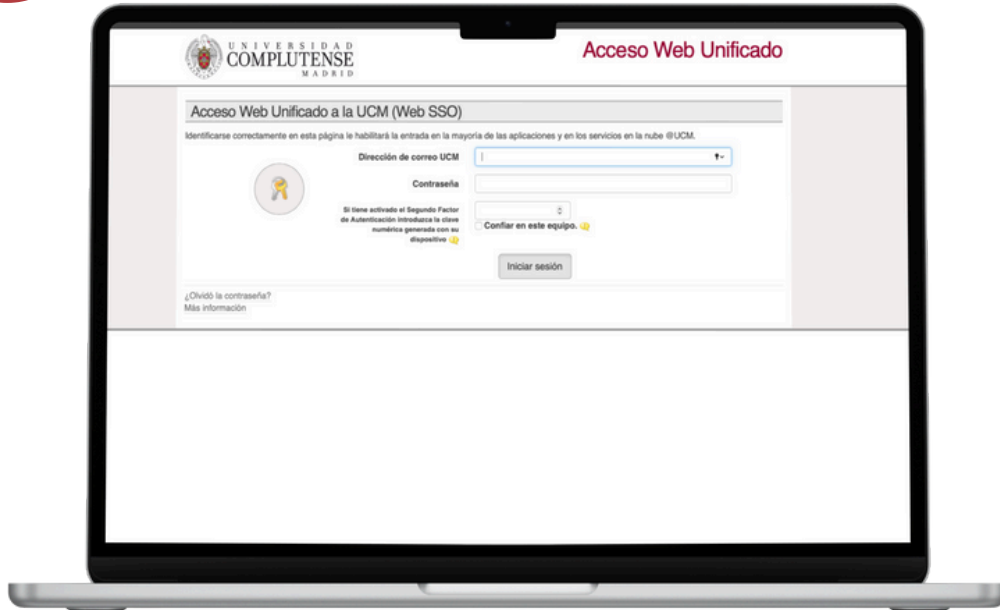
2

‘Navegar Identificado’.



3

## Inicia sesión con tu cuenta UCM.

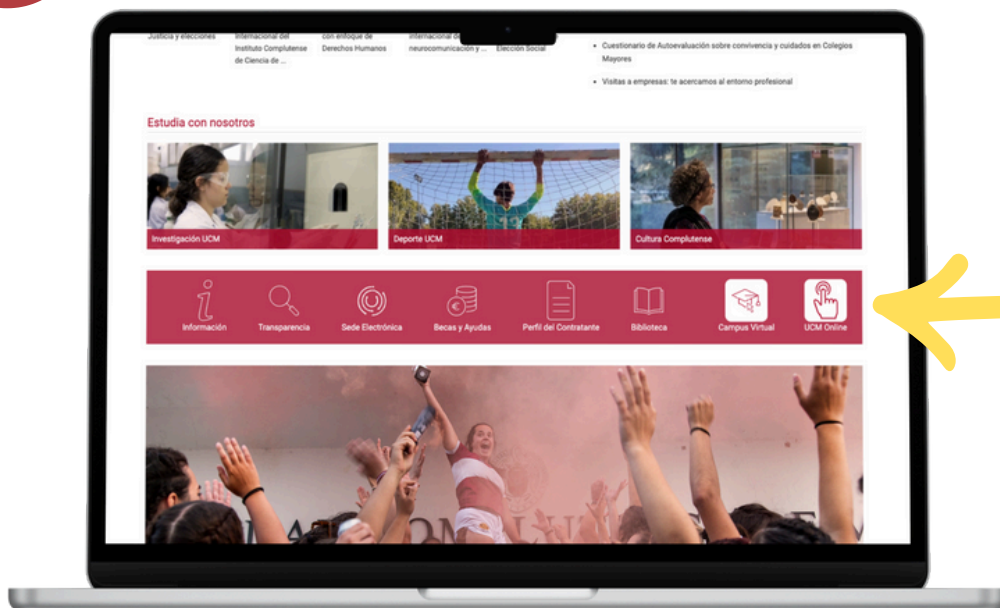


El nombre de usuario elegido + «@ucm.es» es la dirección de correo electrónico completa (por ejemplo, si seleccionas «danram12», tu correo electrónico es «danram12@ucm.es»).

La contraseña es la misma que elegiste al crear tu cuenta.

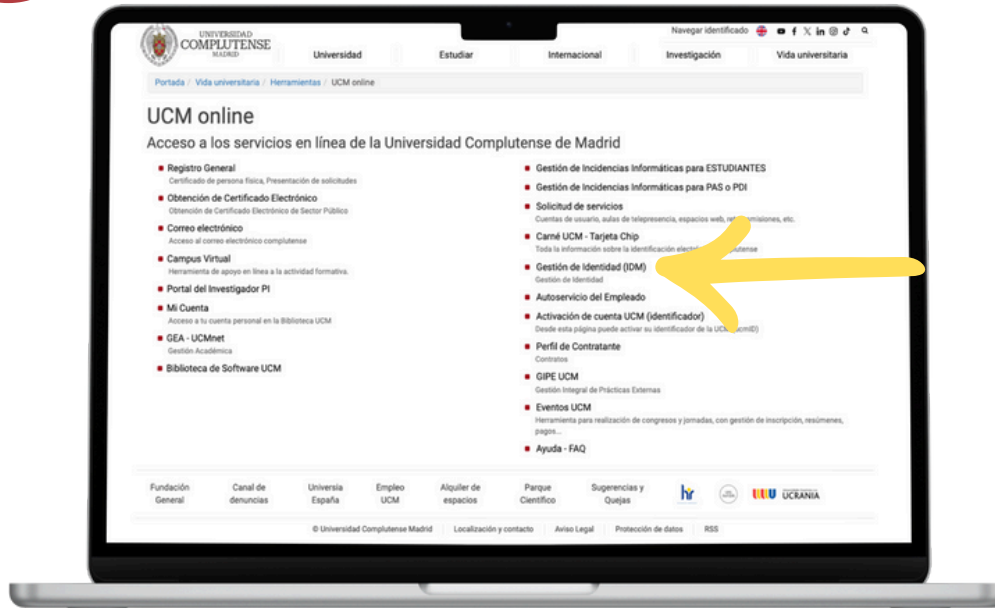
4

## UCM ONLINE



5

## Gestión de Identidad (IDM)



6

## Segundo Factor de Autenticación



TEN TU TELÉFONO A MANO YA QUE NECESITARÁS UTILIZARLO PARA EL SIGUIENTE PASO



7

## 'Mostrar QR' button

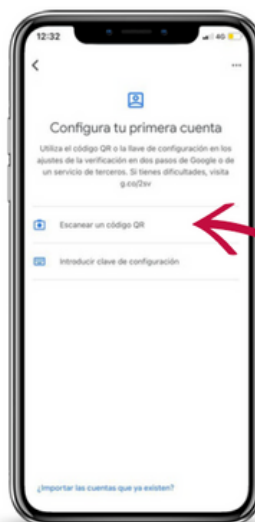


8



Con tu teléfono,  
descarga la aplicación  
«GoogleAuthenticator  
» de Google Play o  
AppStore.

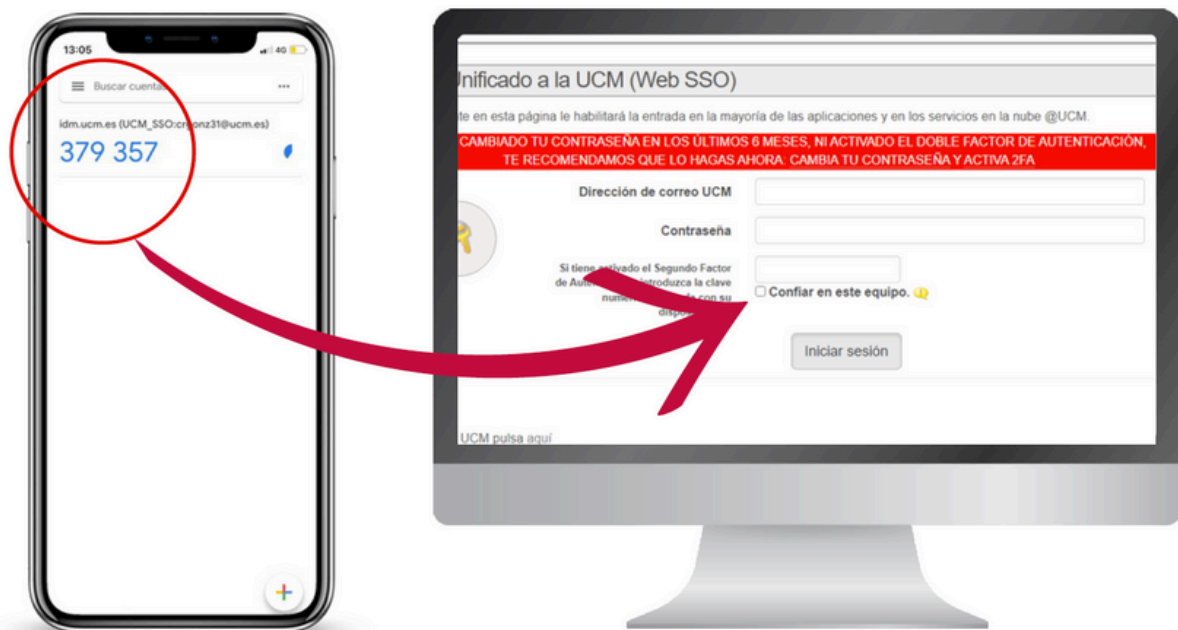
9



Abre la  
aplicación y haz  
clic en  
«Escanear  
código QR».



A partir de ahora, cada vez que queramos acceder a nuestra cuenta, tendremos que abrir la aplicación 'Google Authenticator' en nuestro teléfono y se generará un número que durará unos segundos. Lo escribiremos en el campo 'Segundo factor de autenticación'. Si marcamos la casilla «Confiar en este equipo», no tendremos que introducir el segundo factor de autenticación durante 14 días.



## Por favor, recuerde el procedimiento...

- **Descargar APP:** Descargue la aplicación de contraseña de un solo uso basada en el tiempo (TOTP) en su teléfono móvil. Recomendamos *FreeOTP Authenticator* o *Google Authenticator*.
- **Escanee el código QR:** Vaya al servicio de gestión de identidades (<https://idm.ucm.es>) y haga clic en «Autenticación de dos factores». Escanee el código QR de la página con tu aplicación móvil.
- **Generar un código:** La aplicación generará ahora un código único cada 30 segundos.
- **Introduce el código:** Introduce el código de la aplicación en la página web.

**Ya está. Ya ha activado la autenticación de doble factor. Cada vez que inicie sesión en un servicio UCM, se pedirá tu contraseña y un código temporal de su aplicación.**

Antes de activarla, recomendamos que añada una dirección de correo electrónico alternativa a su información de usuario en Gestión de identidades (<https://idm.ucm.es>).

### ¿Cómo desactivarla?

1. <https://idm.ucm.es>.
2. Segundo Factor de Autentificación.
3. Desactivar



### ¿Qué pasa si pierdo el teléfono o borro la app?

Puede recuperar la cuenta utilizando su dirección de correo electrónico alternativa. Si no tiene una dirección de correo electrónico alternativa, tendrá que acudir a un departamento de la universidad (como una oficina de servicios estudiantiles o la biblioteca) para restablecer la contraseña.

### ¿Por qué utilizar la autenticación de doble factor?

Al utilizar la autenticación de dos factores, está protegiendo su información personal y garantizando la seguridad de su cuenta UCM. Es un paso sencillo que puede marcar una gran diferencia.

## Beneficios del correo electrónico UCM:

Su dirección de correo electrónico UCM es su cuenta de correo electrónico oficial de la universidad. Desbloquea el acceso a diversos recursos y servicios universitarios, incluyendo:

- Biblioteca
- Campus Virtual
- Wifi



- Utilice siempre su dirección de correo electrónico UCM completa para acceder a los servicios universitarios.
- No comparta las credenciales de acceso con nadie para mantener la seguridad de la cuenta.
- Deberá esperar 24 horas para acceder al correo UCM una vez que lo haya solicitado.

¡Enhorabuena! Siguiendo estos pasos, estará en el buen camino para utilizar su activación del «Segundo Factor de Autenticación» y disfrutar de todas las ventajas que ofrece.

Si tiene alguna pregunta, envíenos un correo electrónico a: [erasmus1@ucm.es](mailto:erasmus1@ucm.es)



OFICINA DE RELACIONES  
INTERNACIONALES  
UNIVERSIDAD COMPLUTENSE DE MADRID