

## Configuración del Doble Factor de Autenticación en UAL Microsoft (Servicios de Microsoft para la UAL)

Autor	Servicio de Tecnologías de la Información y las Comunicaciones
Destinatario	Todos los usuarios de la UAL
Fecha creación	
Fecha última modificación	07/06/2022 18:47:00
Resumen del contenido	

### ¿Qué es el acceso mediante “doble factor de autenticación” (MFA), también llamado “verificación en dos pasos”?

Todos estamos acostumbrados a acceder a los servicios TIC usando simplemente un nombre de usuario y una contraseña, pero cada vez es más habitual (por ejemplo, en la banca online) que para hacer algunas operaciones nos exijan “algo más”: responder a una llamada, introducir un código que nos llega a nuestro móvil, etc. Eso es la verificación en dos pasos.

En este documento se detallan los pasos para activar la verificación en dos pasos en su cuenta de usuario de la UAL (tanto @ual.es como @inlumine.ual.es) para el acceso a los servicios de Microsoft (OneDrive, Office, Azure, etc.)

### ¿Qué necesito para la verificación en dos pasos cuando acceda a mis servicios de Microsoft?

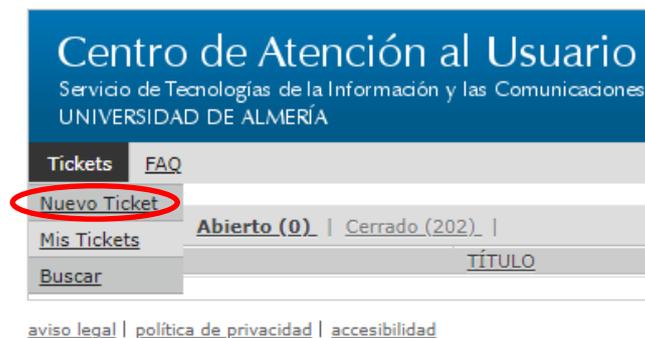
- **Disponer una cuenta de la UAL** ([usuario@ual.es](mailto:usuario@ual.es) o [usuario@inlumine.ual.es](mailto:usuario@inlumine.ual.es))
- **Tener el servicio UAL-Microsoft activado.** Puede comprobar si lo tiene o no activado, y activarlo si fuera necesario, entrando a Campus con su usuario y contraseña habituales, en la opción Inicio -> Servicios UAL-Microsoft
- **Disponer de un móvil que usaremos para verificar nuestra identidad**

## 1. Solicitar activación “doble factor de autenticación” (MFA)

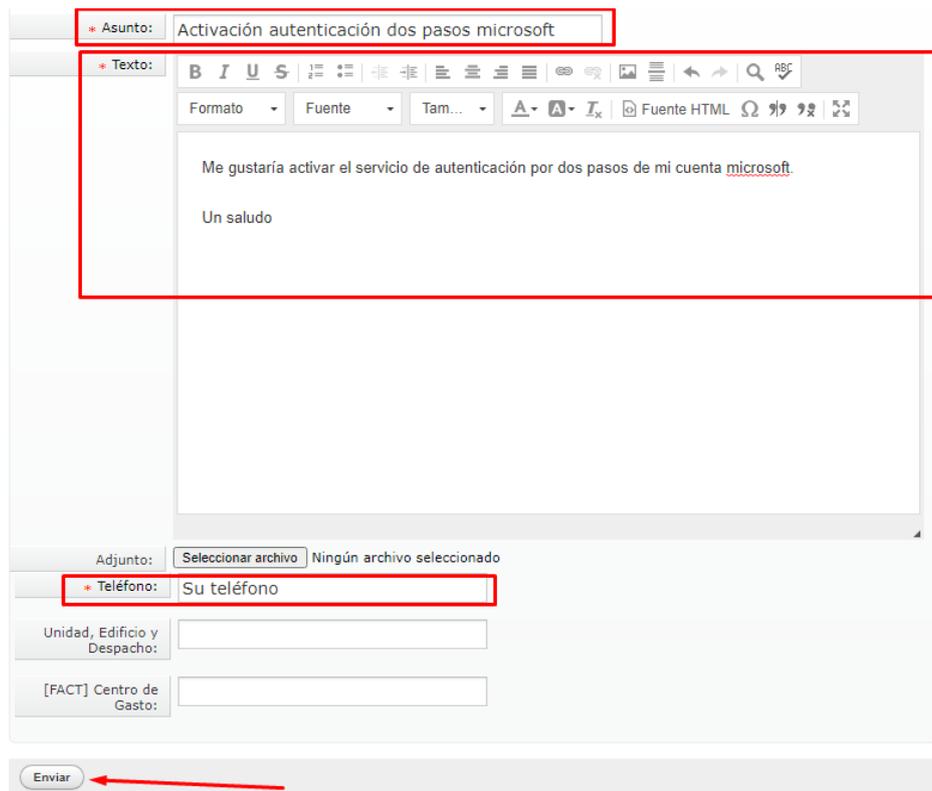
Para activar el servicio de verificación en 2 pasos de su cuenta Microsoft, debe solicitarlo a través del [Centro de Atención al Usuario del STIC](#). Inicie sesión con su cuenta de la Universidad de Almería (usuario, sin @ual.es o @inlumine.ual.es).



Haga clic “Nuevo ticket” poniendo el puntero encima de “Tickets”.



Cree un ticket solicitando activar la verificación en dos pasos, y recibirá la respuesta del STIC (vía ticket CAU) donde le indicarán que ya ha sido activado el doble factor de autenticación o verificación en dos pasos.



\* Asunto: Activación autenticación dos pasos microsoft

\* Texto:

Me gustaría activar el servicio de autenticación por dos pasos de mi cuenta [microsoft](#).

Un saludo

Adjunto:  Ningún archivo seleccionado

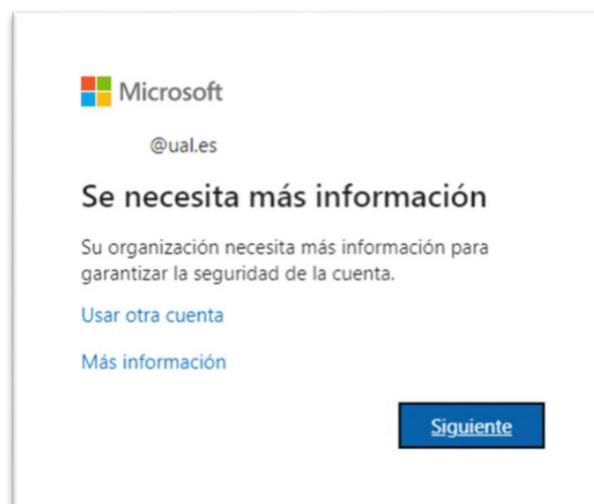
\* Teléfono: Su teléfono

Unidad, Edificio y Despacho:

[FACT] Centro de Gasto:

## 2. Activar “doble factor de autenticación” (MFA)

Vaya a la web [portal.office.com](https://portal.office.com) para iniciar sesión. Indique su usuario ([usuario@ual.es](mailto:usuario@ual.es) o [usuario@inlumine.ual.es](mailto:usuario@inlumine.ual.es)) y contraseñas habituales de la UAL.



Comprobación de seguridad adicional

Proteja su cuenta agregando más comprobación de teléfono a su contraseña. Ver vídeo para saber cómo proteger su cuenta

**Paso 1: ¿De qué manera deberíamos ponernos en contacto con usted?**

Teléfono de autenticación

Seleccione su país o región

Método

Enviarme un código mediante mensaje de texto

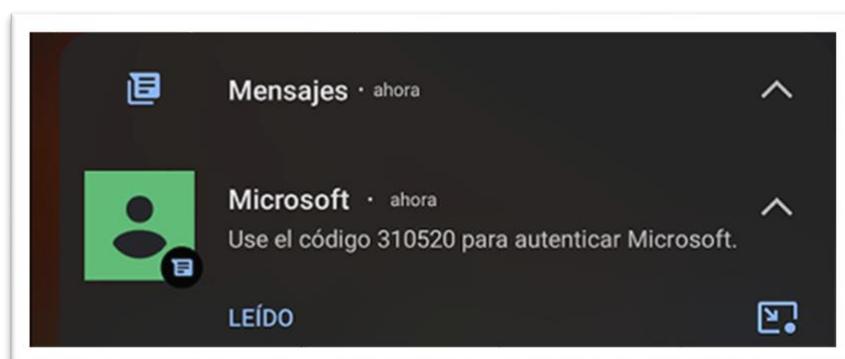
Llámarme

[Siguiente](#)

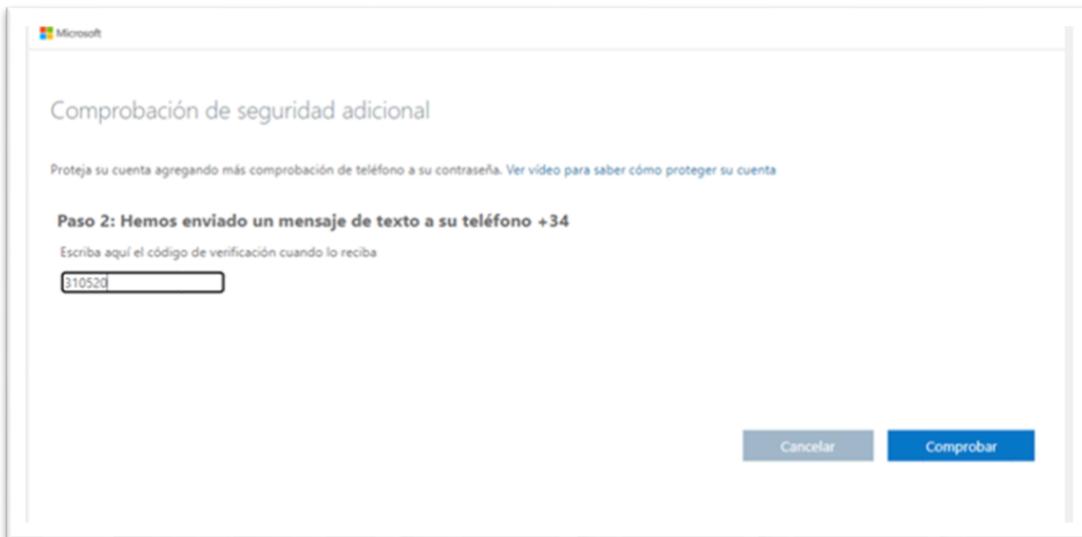
Sus números de teléfono sólo se usarán para proteger su cuenta. Se aplicará la tarifa estándar de teléfono y SMS.

©2022 Microsoft Legal | Privacidad

Indicamos nuestro número de teléfono y seleccionamos el método para obtener el código, en este ejemplo, por SMS.

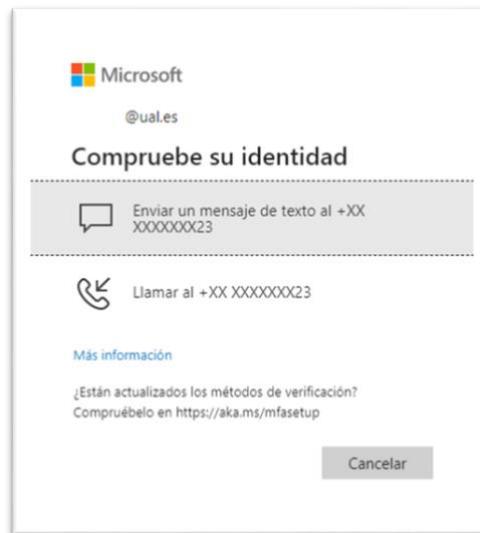


Copiamos el código que nos indica el mensaje de Microsoft (nunca pulsar un enlace que venga dentro de un SMS)



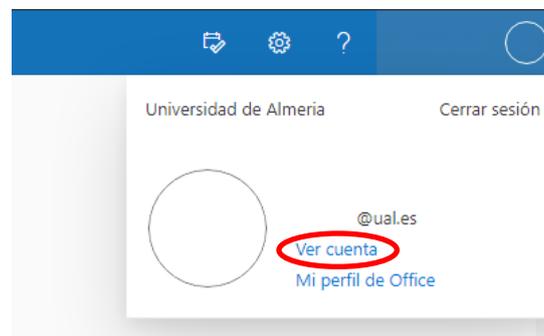
### 3. Configuramos “doble factor de autenticación” (MFA)

La próxima vez que iniciemos sesión satisfactoriamente en un equipo no reconocido por el sistema, nos saldrá esta pantalla para identificarnos con el móvil.

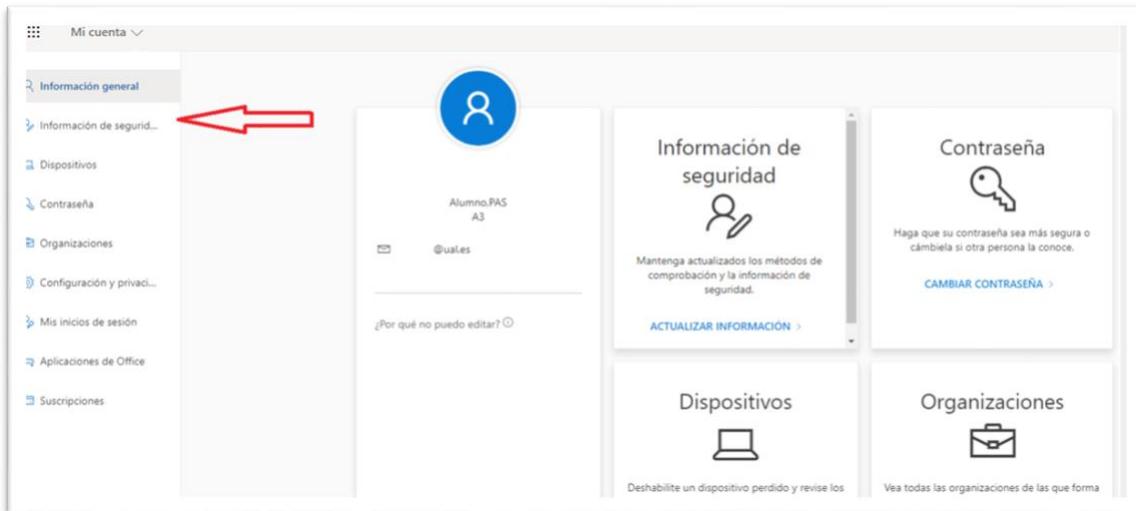


#### 4. Opciones de segunda verificación (MFA)

Partiendo de la web de [portal.office.com](http://portal.office.com), en la esquina superior derecha, haciendo clic en nuestro nombre, pulsamos en “Ver cuenta”



Llevándonos a esta web, donde podemos configurar nuestra cuenta de Microsoft y hacemos clic en “Información de seguridad”.



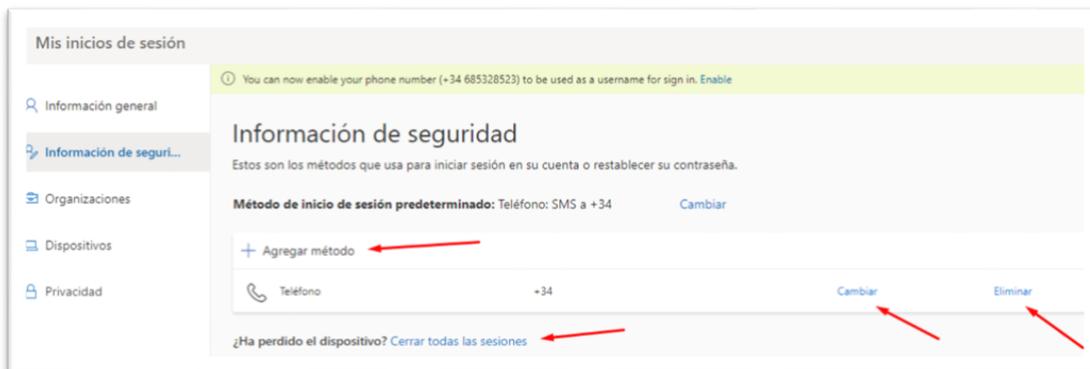
Aquí podremos:

**Cambiar** dentro del mismo teléfono si queremos el código por SMS o por locución en una llamada.

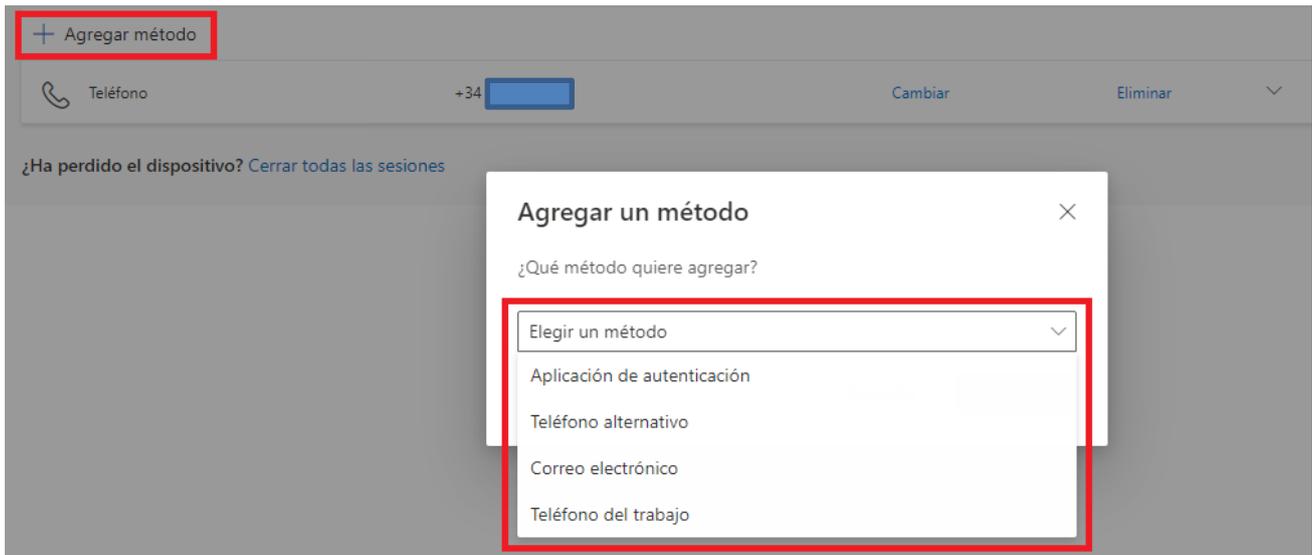
**Cambiar** o añadir teléfonos para poder iniciar sesión.

**Añadir métodos** alternativos de verificación para iniciar sesión.

**Cerrar sesión** por pérdida del dispositivo.

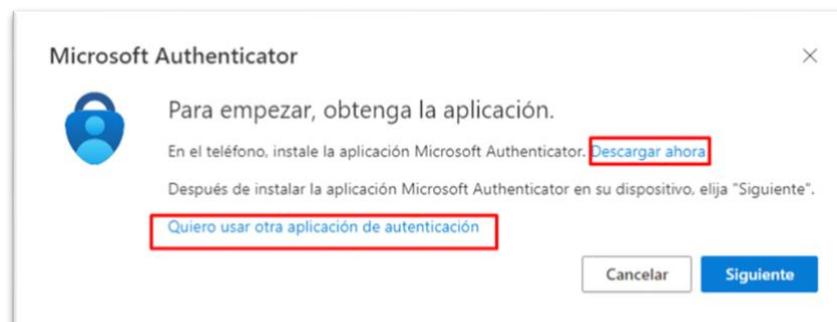


Si nos centramos en “Agregar método”, disponemos estas opciones:

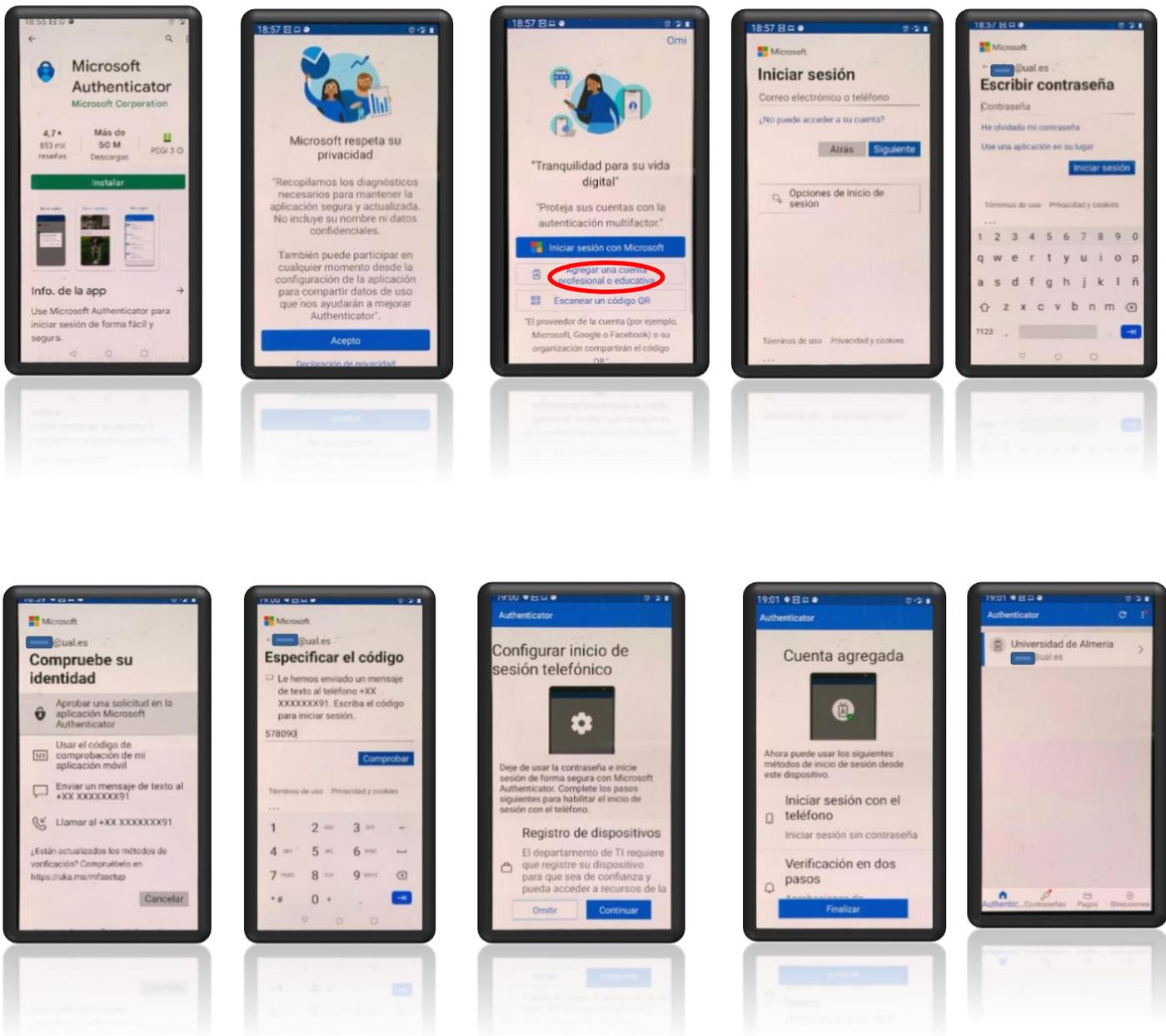


- **Teléfono alternativo:** Añadimos otro teléfono válido para ser usado para iniciar sesión
- **Correo electrónico:** Se usa un correo para recibir el código.
- **Teléfono del trabajo:** Esta opción contempla poner el teléfono de una centralita + una extensión para que nos llame a nuestro entorno laboral (**no es el caso de la UAL**)
- **Aplicación de autenticación:** Nos permite usar aplicaciones desde nuestro móvil para verificar nuestra identidad:

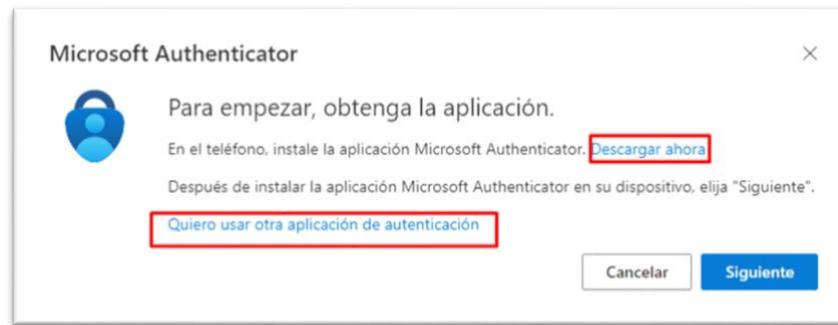
Tenemos la opción de usar la Aplicación de Microsoft, y descargarla



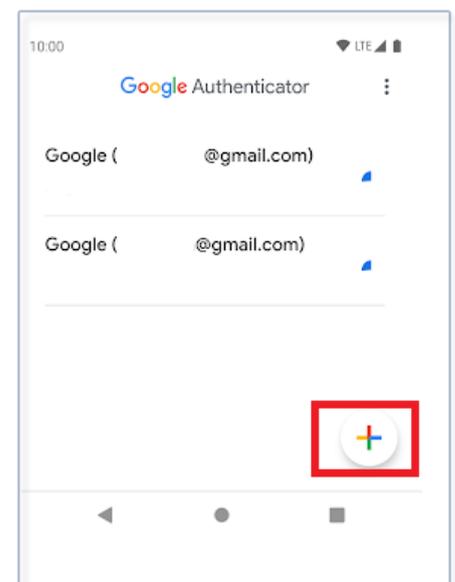
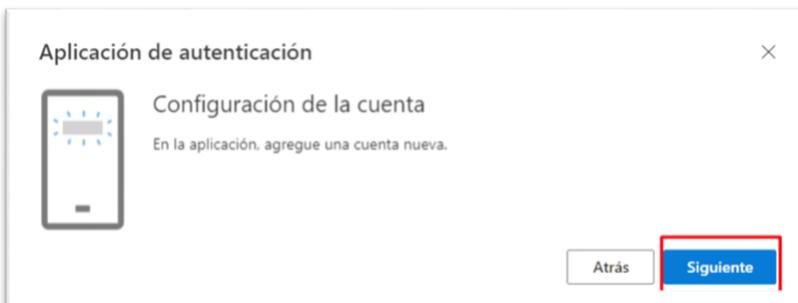
En las capturas siguientes aparecen los pasos a seguir para configurarla en Android:



También podremos usar otra aplicación, seleccionando “Quiero usar otra aplicación de autenticación”.



Buscamos nuestra aplicación preferida de autenticación (Ej: Google Authenticator) y añadir nuestra cuenta Microsoft para poder iniciar sesión.



Escaneamos el código y ya tendríamos el código para añadir el Authenticator en su cuenta de Microsoft, solo escribiendo el código de nuestro Authenticator igual que en la captura.



### Aplicación de autenticación ✕



#### Especificar el código

Escriba el código de 6 dígitos que se muestra en la aplicación Authenticator.

Especificar el código