

Área de Tecnologías de la Información y la Comunicación

INTRODUCCIÓN:

El presente manual permite la configuración de un Segundo Factor de Autenticación (2FA) en los servicios que Microsoft proporciona a la UAL. Segundo Factor de Autenticación (2FA) , Múltiple Factor de Autenticación (MFA) o Autentificación en Dos Pasos son términos equivalentes.

Puedes encontrar toda la información necesaria, así como este manual en la web: <u>https://www.ual.es/2fa</u>

El requisito imprescindible es tener una cuenta activa de la UAL, bien como Estudiante, PDI o PTGAS.

PASO 0: Solicitar vía ticket al CAU del ATIC la activación

Solicitar al CAU del ATIC en https://caustic.ual.es la activación del 2FA para los servicios proporcionados por Microsoft, no se podrá empezar el procedimiento antes de que se haya obtenido la confirmación por parte del ATIC de su activación.

PASO 1: Instalar GOOGLE AUTHENTICATOR

Descarga la aplicación GOOGLE AUTHENTICATOR en tu dispositivo móvil.

Abre la aplicación y acepta los permisos.

PASO 2: Abrir sesión con la cuenta Microsoft

Inicia sesión en Microsoft (https://portal.office.com) en tu ordenador. Se te pedirá información adicional para acceder. Selecciona "Siguiente" para continuar:





Área de Tecnologías de la Información y la Comunicación

Por defecto se te ofrecerá configurar el 2FA usando "Microsoft Authenticator". Para usar Google Authenticator (el recomendado por el ATIC), elije la opción "Quiero usar otra aplicación de autenticación" y selecciona "Siguiente" hasta que se le muestre el código QR:

	Garantizar la seguridad de la cuenta
	Aplicación de autenticación
	Digitalización del código QR
Microsoft Authenticator	Use la aplicación de autenticación para escanear el código QR Así, la aplicación de autenticación y la cuenta quedarán emparejadas.
	Después de escanear el código QR, elija "Siguiente".
Para empezar, obtenga la aplicación.	
En el teléfono, instale la aplicación Microsoft Authenticator. Descargar ahora	
Después de instalar la aplicación Microsoft Authenticator en su dispositivo, elija "Siguiente".	
Quiero usar otra aplicación de autenticación	¿No puede escanear la imagen?
Siguiente	Atris Siguiente
	Quiero configurar otro método
Quiero configurar otro método	

PASO 3: Añadir la cuenta a GOOGLE AUTHENTICATOR

A continuación, abre Google Authenticator en su móvil.

Pulsa el signo "+" para agregar tu cuenta Microsoft (usuario@ual.es / usuario@inlumine.ual.es) o "Añadir código" si no tienes otra cuenta previamente. Selecciona "Escanear un Código QR" (usaremos el código obtenido en la ventana anterior).







Área de Tecnologías de la Información y la Comunicación

Se te mostrará un código de 6 dígitos temporal (token) similar al de la imagen.

Google Authenticator	÷
100 676	

PASO 4: Verificar en Microsoft

Regresa a la pantalla de Microsoft 365 en tu ordenador (donde se muestra todavía el QR) y selecciona "Siguiente".

Introduce el código de 6 dígitos anterior. Si es correcto, aparecerá un mensaje confirmando que todo está listo y la cuenta Microsoft quedará vinculada a Google Authenticator.

Garantizar la seguridad de la cuenta

Método 2 de 2: Listo		
Aplicación	Correo electrónico	
Correcto		
¡Muy bien! Ha configurado correctamente la información de seguridad. Elija "Listo" para continuar con el inicio de sesión.		
Método de inicio de sesión predeterminado:		
Aplicación de autenticación		
Correo electrónico		
	Listo	

A partir de ahora, cuando inicies sesión en Microsoft deberás introducir el código o token que mostrará Google Authenticator.