



INTRODUCCIÓN:

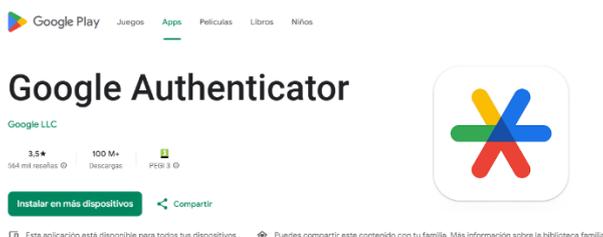
El presente manual permite la configuración de un Segundo Factor de Autenticación (2FA) en los servicios que Google proporciona a la UAL. Segundo Factor de Autenticación (2FA), Múltiple Factor de Autenticación (MFA) o Autenticación en Dos Pasos son términos equivalentes.

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

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

PASO 1: Instalar Google Authenticator en el móvil

¿Qué es Google Authenticator?



Google Authenticator es una aplicación creada por Google para proporcionar códigos para verificar tu identidad en sistemas con 2FA.

Puede descargarse en:

Google Play Store:

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

App Store de Apple:

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

Dependiendo del dispositivo que tengas Android o iPhone deberás ir a la tienda correspondiente e instalar la aplicación.

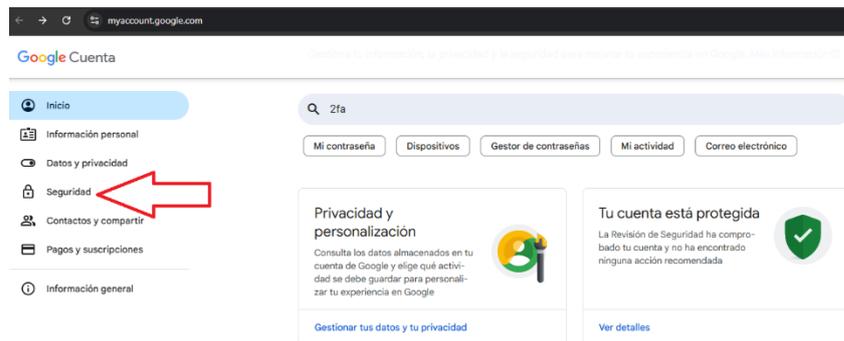
Se usará Google Authenticator para conectar tanto a los servicios de Google como a los de Microsoft.

PASO 2: Abrir sesión con la cuenta Google

Iniciar sesión con tu usuario y contraseña en cualquier servicio Google o mejor, directamente a la opción de gestión de la cuenta: <https://myaccount.google.com/>

PASO 3: Activación del 2FA

En el panel de navegación, selecciona **Seguridad**.



1.

En "Cómo inicias sesión en Google", selecciona **Activar la verificación en dos pasos**.

Cómo inicias sesión en Google

Asegúrate de poder acceder siempre a tu cuenta de Google manteniendo al día esta información

Verificación en dos pasos	La verificación en dos pasos está desactivada	>
Llaves de acceso y llaves de seguridad	Empezar a usar llaves de acceso	>
Contraseña	Última modificación: 1 ago 2024	>

Selecciona **"Authenticator"**.



← Verificación en dos pasos

Activar verificación en dos pasos

Segundos pasos

Asegúrate de poder acceder a tu cuenta de Google manteniendo al día esta información y añadiendo más opciones de inicio de sesión

- | | | | |
|---|--|---|---|
|  | Llaves de acceso y llaves de seguridad |  Añadir una llave de seguridad | > |
|  | Notificación de Google | | > |
|  | Authenticator |  Añadir aplicación Authenticator | > |
|  | Número de teléfono |  Añadir un número de teléfono | + |

Es posible que te solicite tu contraseña, introdúcela y selecciona **Siguiente**.

← Aplicación Authenticator

En vez de esperar a que lleguen mensajes de texto, puedes obtener códigos de verificación desde una aplicación de autenticación. Funciona aunque tu teléfono no tenga conexión.

Primero, descarga Google Authenticator desde [Google Play Store](#) o desde el [App Store de iOS](#).



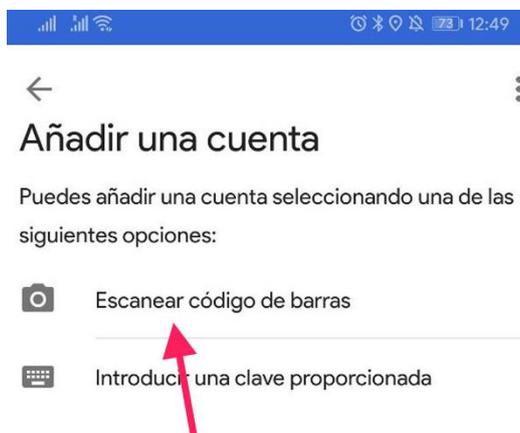
+ Configurar autenticador

Selecciona “Configurar Authenticator” y posteriormente genera un código QR a usar en los siguientes pasos.

PASO 4: Añadir el código a Google Authenticator

Abre Google Authenticator en tu móvil.

Dentro de Google Authenticator pulsa en "+ Agregar cuenta" > "Escanear código QR".



Escanea el código QR que aparece en la pantalla¹.

Configurar aplicación de autenticación

- En la aplicación Google Authenticator, toca el icono +.
- Elige Escanear un código QR.



[¿No puedes escanearlo?](#)

Confirma el código generado.

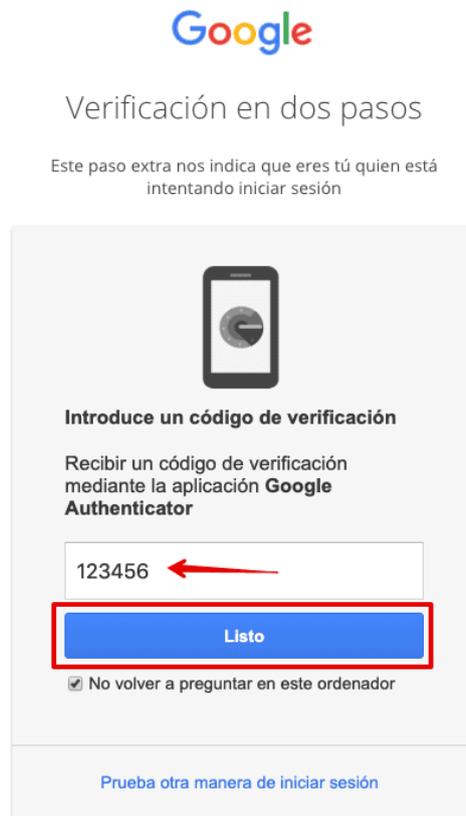


¹ Si no tienes acceso al código QR, puedes ingresar la clave manualmente en la aplicación.



PASO 5: Uso una vez configurado

Cuando iniciemos sesión en algún dispositivo nuevo (o no usado en algún tiempo) en el que se requiera el uso de servicios de Google, después de introducir nuestro usuario y contraseña, nos saltará una notificación para autorizar el inicio de sesión y deberemos introducir el código que nos ofrece Google Authenticator:



El código lo obtendremos en la App Google Authenticator, donde nos aparecerá un código para cada cuenta o servicios que hayamos configurado:

