

MANUAL DE CONFIGURACIÓN DE MFA GOOGLE AUTHENTICATOR



INTRODUCCIÓN

Este documento ofrece una guía paso a paso para la descarga, instalación y configuración inicial de la aplicación Google Authenticator en dispositivos móviles (Android e iOS), como gestor de códigos de verificación en dos pasos (MFA) soportado por la institución.

Requisitos previos

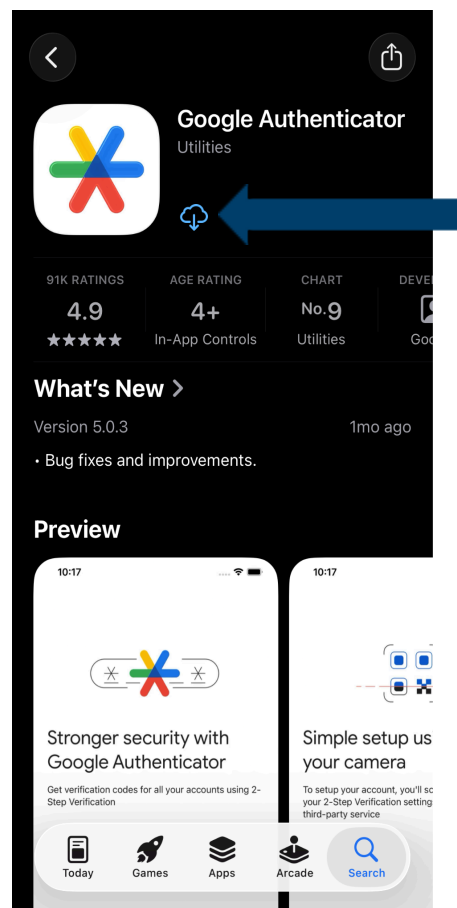
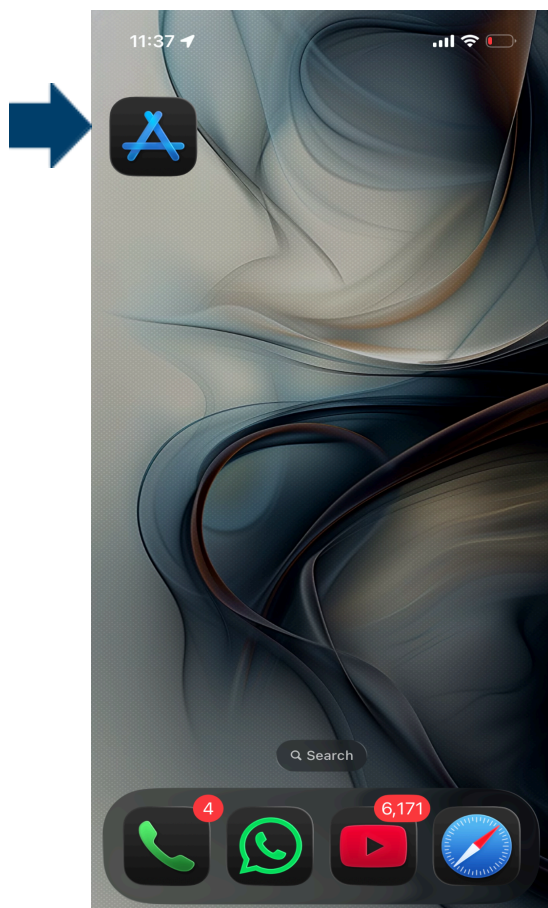
- Teléfono inteligente con sistema operativo Android o iOS.
- Conexión activa a Internet (Wi-Fi o datos móviles).
- Cuenta de Google para respaldo opcional de credenciales en la nube.

PROCEDIMIENTO

1. Para descargar y comenzar con la instalación de la aplicación abra la tienda de aplicaciones de su dispositivo móvil e instale la aplicación oficial desarrollada por Google.

En Android: Ingrese a Google Play Store y busque “Google Authenticator”.

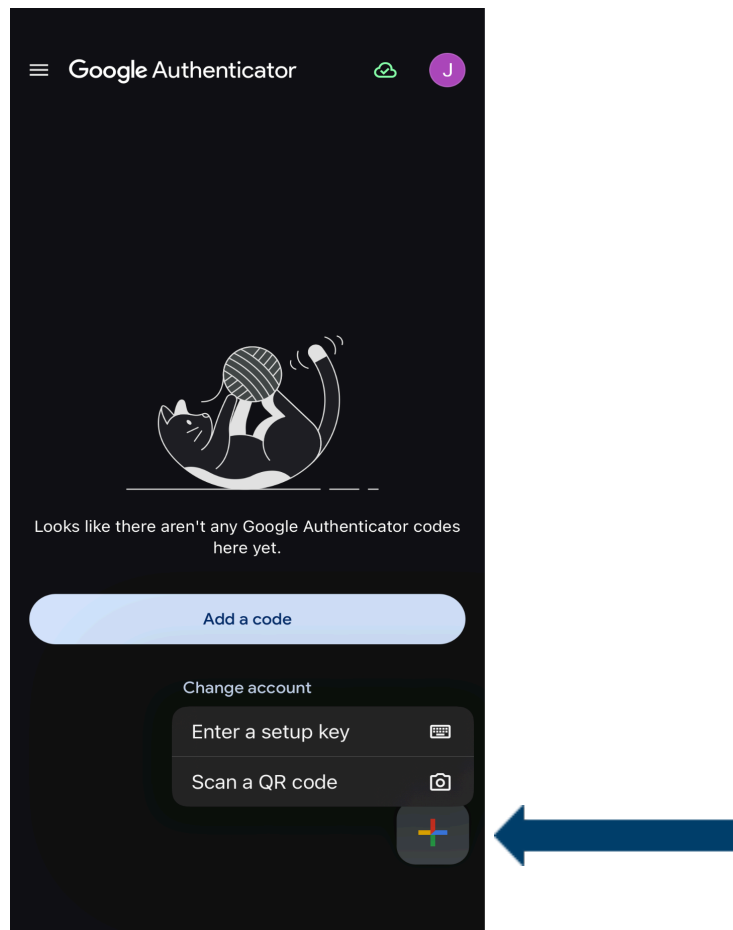
En iOS (iPhone): Ingrese a App Store y busque “Google Authenticator”.



2. Al abrir la aplicación por primera vez, presione en “Comenzar” o “Get Started”. Se le solicitará iniciar sesión con su cuenta de Google institucional o personal.

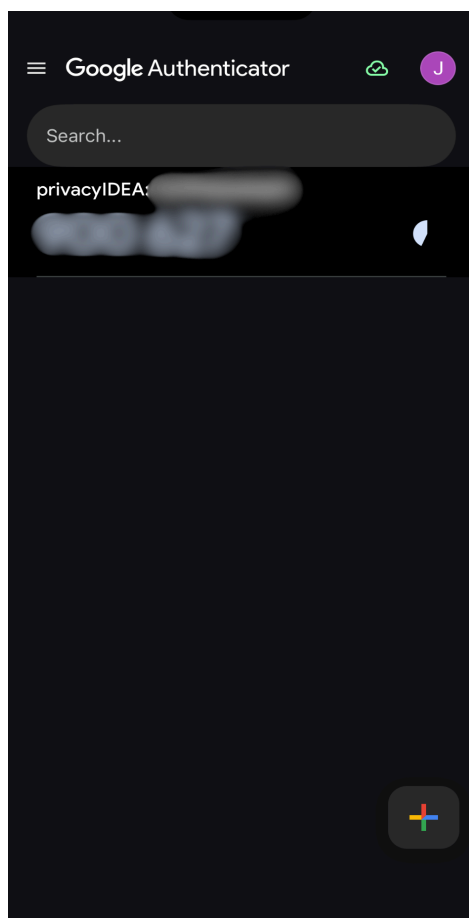
NOTA: Mantener su cuenta sincronizada permite respaldar sus tokens en la nube de forma segura en caso de daño, cambio o pérdida del teléfono.

3. Para vincular una cuenta institucional, presione el botón flotante con el símbolo “+” ubicado en la esquina inferior derecha de la pantalla (ver figura).



4. Para realizar el escaneo de un código QR, en el menú desplegable, seleccione la opción “Escanear código QR” o “Scan a QR code” (ver figura). Si es la primera vez que utiliza la aplicación, el sistema operativo le solicitará permiso para acceder a la cámara; acepte dicho permiso y apunte la lente hacia el código QR mostrado en la pantalla de su computadora (portal institucional).
5. Una vez escaneado el código, este quedará agregado de inmediato. Verifique que en la lista principal aparezca el nombre del servicio institucional junto con un código

numérico de 6 dígitos y un icono de reloj o temporizador que se renueva cada 30 segundos (ver figura).



NOTA IMPORTANTE: Nunca comparta los códigos generados ni capturas de pantalla de sus tokens con terceros. El personal de la Dirección de Telemática nunca le solicitará su código temporal por correo o llamada telefónica.