

**Centro de Investigación Científica y de Educación Superior
de Ensenada, Baja California**



DIRECCIÓN DE TELEMÁTICA

Guía de configuración para habilitar
doble factor de autenticación en el
correo electrónico institucional.

Versión 1.0

1 de agosto de 2026

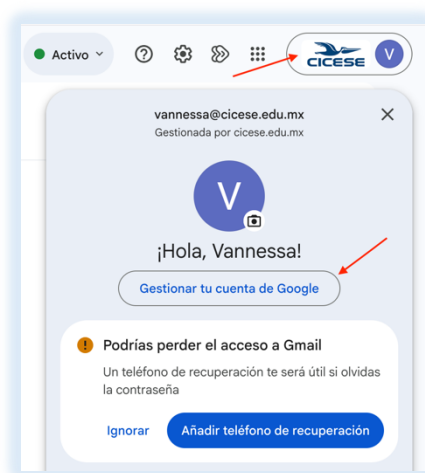
Guía de configuración para habilitar doble factor de autenticación en el correo electrónico institucional.

El doble factor de autenticación (2FA) es un método de seguridad que exige dos comprobaciones distintas para asegurar que quien intenta acceder a un sistema o servicio sea realmente quien dice ser.

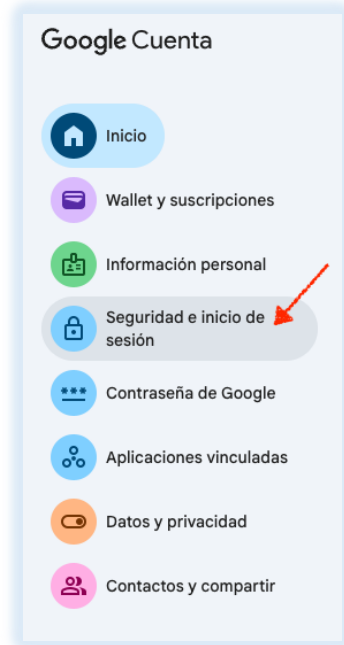
En el presente documento se explicarán los pasos a seguir para habilitar el doble factor de autenticación en el correo electrónico institucional.

1.- Debe acceder a su correo electrónico desde la interfaz web <https://gmail.com> con sus datos de acceso usuario@cicese.edu.mx y la contraseña correspondiente

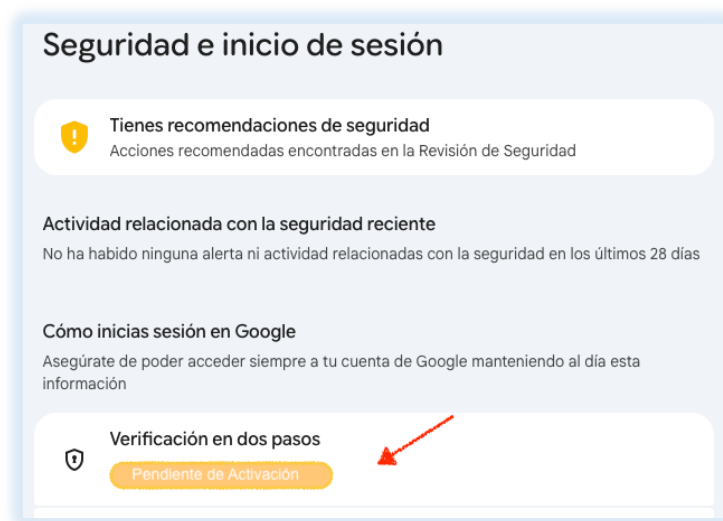
En la parte superior derecha debe hacer clic donde aparece el icono de CICESE y la imagen de su usuario. Enseguida debe hacer clic en el botón “Gestionar tu cuenta de Google”



2.- Haga clic en la opción “Seguridad e inicio de sesión”



3.- En la siguiente pantalla, ubique la sección “Cómo inicias sesión en Google - Verificación de dos pasos” y haga clic en el botón “Pendiente de activación”.



4.- En la siguiente ventana se verán las características de acceso a tu cuenta, selecciona 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



Contraseña
Última modificación: 11:46



Saltar contraseña cuando sea posible



Teléfono de recuperación
Añadir un número de teléfono móvil



Correo de recuperación
Añadir una dirección de correo electrónico

Puedes añadir más opciones de inicio de sesión

 Llaves de acceso y llaves de seguridad

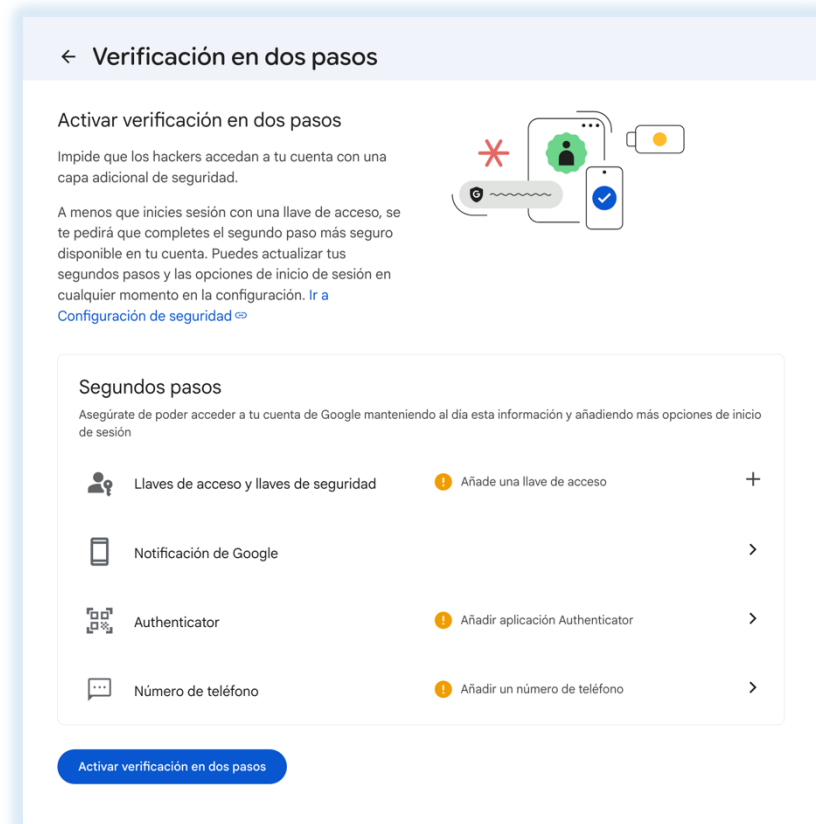
 Authenticator

 Notificación de Google

 Teléfono de verificación en dos pasos

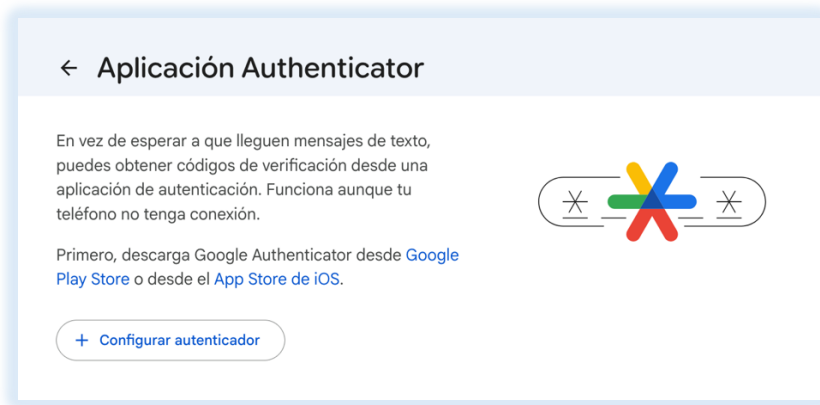
5.- Enseguida se mostrarán las diferentes opciones que puede utilizar como segundo factor de autenticación. Puede elegir cualquiera de ellas y seguir las instrucciones que se proporcionan por Google.

Recomendado: “Authenticator”.



6.- Configuración de segundo factor “Authenticator”,

6.1.- Se desplegará una imagen como la siguiente.



Note que PRIMERO deberá instalar en su teléfono CELULAR una aplicación como *Google Authenticator* o *Microsoft Authenticator* o similar. Asegúrese de tenerla instalada y enlazada a su cuenta **cicese.edu.mx**

Una vez que termine la instalación y configuración de Authenticator en su celular, regrese a la página web y haga clic en el botón “Configurar Authenticator”

6.2.- En la siguiente pantalla, se le proveerán un **código QR** que deberá escanear en la aplicación Authenticator que previamente instaló en su celular.



6.2.- La aplicación Authenticator en su celular le proveerá un **código de 6 dígitos** que debe ingresar en la página web y hacer clic en el botón ‘Verificar ‘.

Configurar aplicación de autenticación

Introduce el código de seis dígitos que se muestra en la aplicación

[Atrás](#) [Cancelar](#) [Verificar](#)

6.3.- Ahora se mostrará una pantalla como la siguiente donde debe hacer clic en el botón “Activar”.

← Aplicación Authenticator

**Activar verificación en dos pasos**
Para iniciar sesión con tu aplicación de autenticación, activa la verificación en dos pasos. [Activar](#)

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.

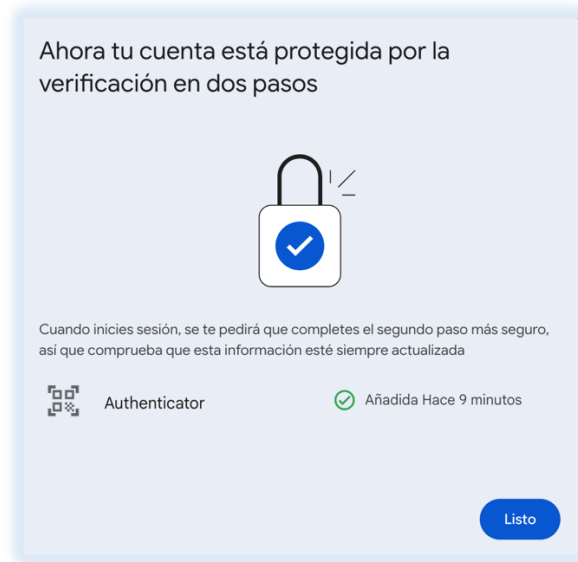
Primero, descarga Google Authenticator desde [Google Play Store](#) o desde el [App Store de iOS](#).

Tu autenticador

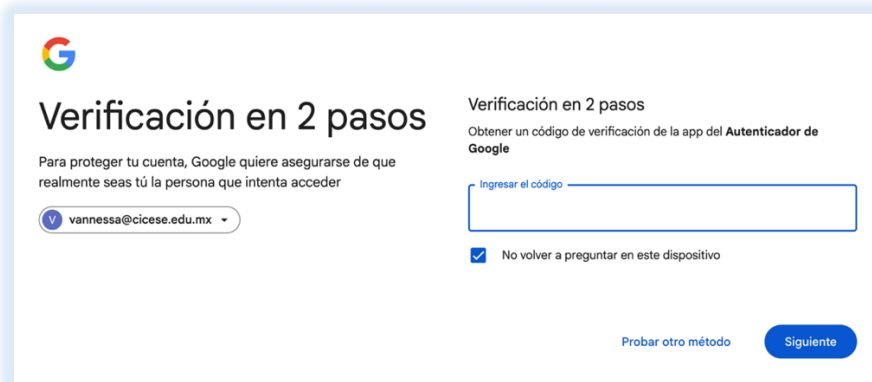
 Authenticator
Añadida justo ahora 

[Cambiar aplicación de autenticación](#)

6.4.- en la siguiente pantalla se recibe la confirmación de éxito en la configuración de doble factor utilizando Authenticator, solo debe hacer clic en el botón “Listo”.



6.5.- En este momento, el navegador hará un reinicio de sesión y deberá ingresar el código generado por la aplicación Authenticator instalada en su celular. Si es un dispositivo o computadora que solo usted utiliza puede palomear la casilla “No volver a preguntar en este dispositivo” en caso de ser un equipo de uso común o público deberá deshabilitarla.



6.6.- A continuación, se le permite el acceso confirmando que ya se ha añadido Authenticator como otro factor de verificación.

