

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



DIRECCIÓN DE TELEMÁTICA

Guía de configuración para Microsoft
Authenticator para acceso en dos
pasos.

Versión 1.0

17 de agosto de 2027

Guía de configuración de Microsoft Authenticator para acceso de dos pasos a cuentas de Microsoft 365.

Para un **usuario final de Microsoft 365**, la forma más segura y recomendada de habilitar Acceso Multifactor (MFA) o acceso de dos pasos, es mediante la aplicación **Microsoft Authenticator** en el teléfono móvil. Microsoft considera este método más seguro y cómodo que los SMS o llamadas telefónicas.

Antes de comenzar

Asegúrese de que:

- Tenga acceso a su cuenta de Microsoft 365.
- Tenga un teléfono Android o iPhone.
- Tenga acceso a su equipo de cómputo.
- En su STORE esté presente la aplicación **Microsoft Authenticator** para instalarla en su celular.

Microsoft Authenticator

Paso 1. Verificar si MFA ya está disponible para su cuenta

- A. En su navegador abra la página: <https://aka.ms/mysecurityinfo>. Verá una pantalla como la que se muestra en la figura 1.

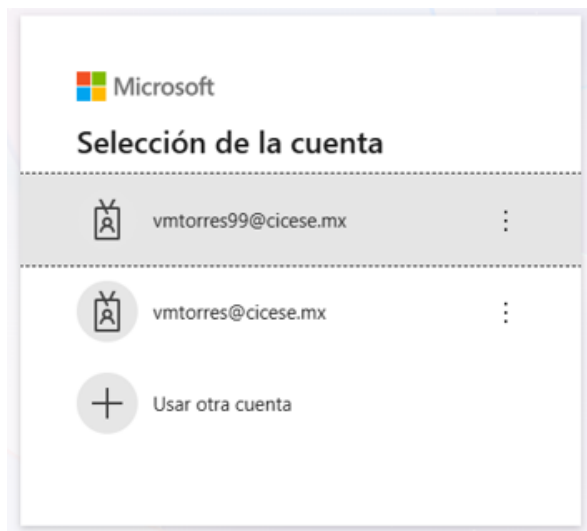


Figura 1.- Ingreso a Microsoft Security.

Seleccione una cuenta o elija usar otra cuenta.

- B. Inicia sesión con su cuenta corporativa, en este caso, la cuenta asociada a CICESE. Proporcione la contraseña de su usuario en Microsoft 365.

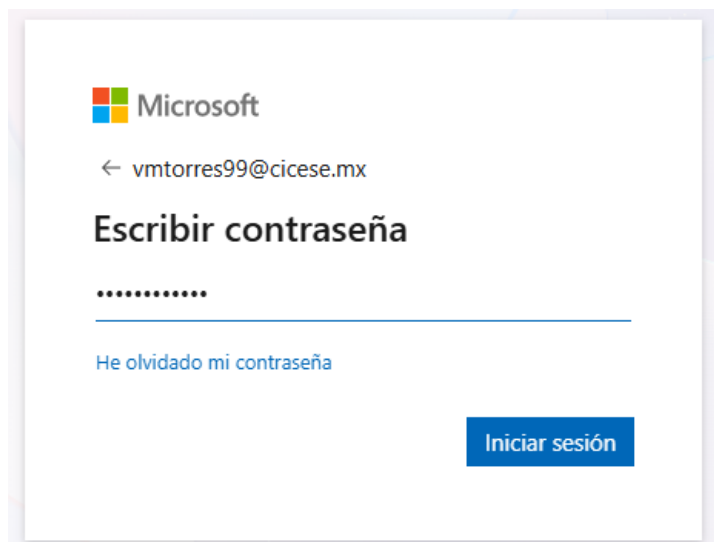


Figura 2.- Acceso por contraseña.

Microsoft verificará su identidad a través de un mensaje o una llamada (véase figura 3). La forma más usual es el envío de un mensaje al celular. Opte por esta forma para comprobar su identidad.

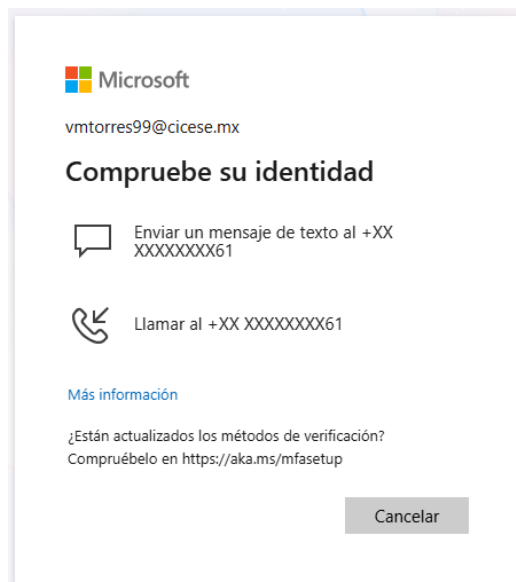
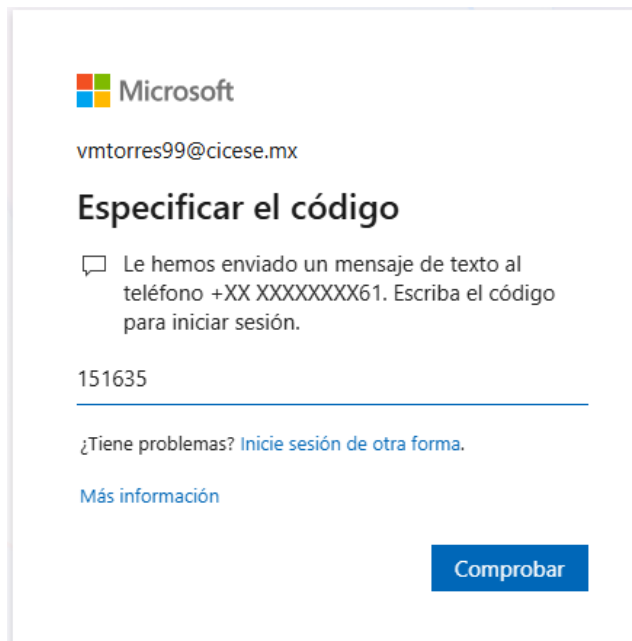


Figura 3.- Verificación de identidad.

En la siguiente página, proporcione el código que habrá llegado a su celular (véase figura 4).



Microsoft

vmtorres99@cicese.mx

Especificar el código

Le hemos enviado un mensaje de texto al teléfono +XX XXXXXXXX61. Escriba el código para iniciar sesión.

151635

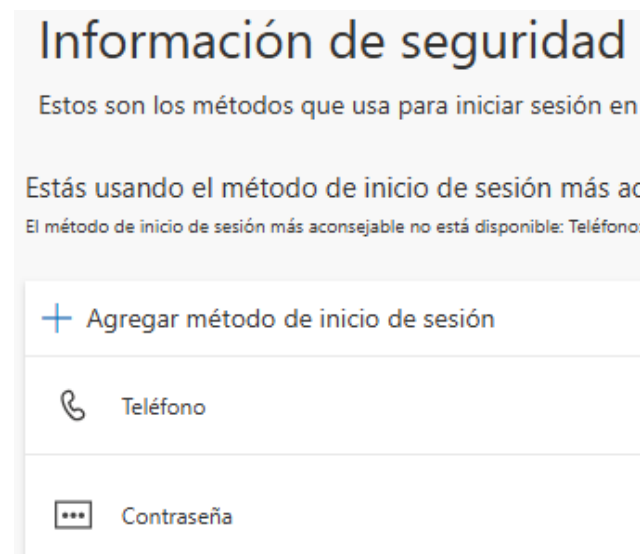
¿Tiene problemas? [Inicie sesión de otra forma.](#)

[Más información](#)

[Comprobar](#)

Figura 4.- Ingreso del código de acceso.

- C. Una vez validado el ingreso, observará en la página una sección con información de seguridad (véase figura 5).



Información de seguridad

Estos son los métodos que usa para iniciar sesión en

Estás usando el método de inicio de sesión más aconsejable

El método de inicio de sesión más aconsejable no está disponible: Teléfono

[+ Agregar método de inicio de sesión](#)

[Teléfono](#)

[Contraseña](#)

Figura 5.- Información de seguridad del usuario.

- D. Revise si aparece la opción Microsoft Authenticator eligiendo la opción **Agregar método de inicio de sesión**. Esta opción debe aparecer como se muestra en la figura 6.

Agregar un método de inicio de sesión.



Microsoft Authenticator

Aprobar solicitudes de inicio de sesión o usar códigos de un solo uso



Token de hardware

Iniciar sesión con un código de un token de hardware



Teléfono alternativo

Obtener una llamada para iniciar sesión con un código



Teléfono del trabajo

Obtener una llamada para iniciar sesión con un código



Correo electrónico

Recibir un código para restablecer la contraseña

Obtén más información sobre cada método [para ayudarte a elegir](#).

Figura 6.- Métodos de inicio de sesión

Si estas opciones aparecen, ya se puede registrar MFA.

Paso 2. Configurar Microsoft Authenticator

En el teléfono

- Instale **Microsoft Authenticator**.
- Abra la aplicación.
- Permita las notificaciones.
- No agregue la cuenta todavía; lo hará después de escanear el código QR.

En la computadora

- Acceda a <https://aka.ms/mysecurityinfo>
- Haga clic en **Agregar método**.
- Seleccione **Aplicación Authenticator**.
- Seleccione **Agregar**.
- Aparecerá un código QR.

En el teléfono

- A. En Microsoft Authenticator pulse +.
- B. Seleccione **Cuenta profesional o educativa**.
- C. Seleccione **Escanear código QR**.
- D. Escanee el código mostrado en el navegador.

Paso 3. Realizar la prueba de autenticación

Al finalizar:

- A. Microsoft enviará una notificación al teléfono.
- B. Apruebe la solicitud.
- C. El asistente mostrará la confirmación de registro.

Paso 4. Configure sus aplicaciones de Microsoft 365

Outlook

- A. Cierre la sesión de su cuenta, si está abierta.
- B. Cierre Outlook completamente.
- C. Vuelva a abrirlo.
- D. Introduzca el nombre de usuario.
- E. Introduzca la contraseña.
- F. Una notificación llegará a su celular a través de Microsoft Authenticator.
- G. Apruebe la solicitud en Authenticator.

Teams

- A. Cierre sesión si ya estaba iniciada.
- B. Inicie sesión nuevamente.
- C. Complete la validación MFA.

Los pasos son similares a los mostrados en **Outlook**.

OneDrive

- A. Haga clic en el icono de OneDrive.
- B. Configure la cuenta nuevamente si es necesario.
- C. Complete el desafío MFA.

Aplicaciones Office (Word, Excel, PowerPoint)

- A. Abra cualquier aplicación.
- B. Vaya a **Archivo > Cuenta**.

- C. Si aparece una advertencia de autenticación, vuelva a iniciar sesión.
 - D. Complete el MFA.
-

Paso 5. Verifique que MFA realmente está funcionando

Haga una prueba controlada:

- A. Vaya a <https://portal.office.com>
- B. Cierre sesión.
- C. Borre la sesión del navegador o use una ventana privada.
- D. Inicie sesión nuevamente.

Deberá observar:

Usuario
↓
Contraseña
↓
Notificación Microsoft Authenticator
↓
Acceso a Microsoft 365
"" 【1-8f3147】

Recomendaciones de seguridad

- Utilice Microsoft Authenticator en lugar de SMS.
- Registre al menos dos métodos de autenticación.
- Mantenga actualizado su número telefónico.
- Nunca apruebe una solicitud MFA que no haya usted iniciado. Si recibe una notificación inesperada, recházela y cambia la contraseña inmediatamente.
- Si cambia de teléfono, agregue el nuevo dispositivo antes de eliminar el anterior. Y si cambia de número telefónico, actualícelo.