DATIC

DEPARTAMENTO DE ADMINISTRACIÓN
DE TECNOLOGÍAS DE INFORMACIÓN
Y COMUNICACIONES

MANUAL DE

CONFIGURACIÓN

Múltiple Factor de Autenticación (MFA)

2022

DATIC

DEPARTAMENTO DE ADMINISTRACIÓN DE TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIONES

VERSIÓN 1.0

MANUALES Y DOCUMENTACIÓN INSTITUCIONAL.

CONTENIDO

TEC | Tecnológico de Costa Rica

¿Qué es Autenticación Multifactor MFA[1] ?

Al iniciar una sesión en sus cuentas en línea, el proceso que llamamos *Autenticación* está demostrando al servicio que usted es quien dice ser.

Tradicionalmente, esto se ha hecho con un nombre de usuario y una contraseña. Sin embargo, esta ya no es la forma más segura de hacerlo. Los nombres de usuario suelen ser fáciles de descubrir, a veces son solo su dirección de correo electrónico. Como las contraseñas pueden ser difíciles de recordar, las personas tienden a elegir las sencillas o a usar la misma contraseña en muchos sitios diferentes.

Una forma de brindar mayor seguridad de ingreso a un sistema es utilizar la *Autenticación multifactor (MFA),* la cual es un procedimiento donde se le solicita al usuario una forma adicional de identificación al iniciar una sesión.

Si solo usa una contraseña para autenticar a un usuario, deja un vector desprotegido frente a los ataques. Si la contraseña es débil o se ha expuesto en otro lugar, un atacante podría usarla para obtener acceso. Al exigir una segunda forma de autenticación, se aumenta la seguridad, porque este factor adicional no es algo que resulte fácil de obtener o duplicar para un atacante. La MFA agrega una capa de protección al proceso de inicio de sesión.

La MFA ofrece una amplia gama de métodos de autenticación flexibles, como mensajes de texto, llamadas telefónicas, códigos de acceso únicos, entre otros. Esto permite satisfacer las necesidades específicas de cada usuario.

1 “MFA por sus siglas en inglés correspondientes a Multi-Factor Authentication”

Métodos de trabajo

El uso de MFA para el acceso al correo electrónico institucional, puede configurarse de varias formas, las cuales se detallan a continuación:

1. Uso de la app Microsoft Authenticator en modo Recibir notificaciones para verificación.

Con este modo de trabajo los inicios de sesión se aprueban desde la aplicación móvil mediante notificaciones directas al celular.

Al usuario se le envía una notificación al teléfono celular en la cual se le solicita la aprobación del inicio de sesión que está realizando o en caso de no reconocer este inicio de sesión se le da la posibilidad de denegarlo y así evitar el ingreso a su cuenta.

2. Uso de la app Microsoft Authenticator en modo Usar código de verificación.

Mediante el uso de la aplicación se genera un código de verificación (token) como segunda forma de autenticación. Este token debe ser digitado en el momento en que se solicite para garantizar su ingreso a la cuenta

3. Envío de mensaje de texto (SMS) al teléfono celular registrado.

Con este modo, el usuario recibe un código (token) en su teléfono celular mediante SMS. Este token debe ser digitado en el momento en que se le solicite para garantizar su ingreso a la cuenta

4. Llamada telefónica a teléfono registrado por el usuario.

El usuario recibe una llamada en el teléfono registrado en donde se le solicitará realizar alguna acción para verificar su identidad.

Para los modos 1 y 2 se requiere la instalación por parte del usuario de la app **Microsoft Authenticator**, la cual puede descargar desde la tienda de aplicaciones de su teléfono.

Ventajas y desventajas de los métodos de uso

MÉTODO	VENTAJAS	DESVENTAJAS
App Microsoft Authenticator, modo **Recibir notificación**	• Fácil de utilizar • Más seguro	• Requiere de instalación de app en el celular • El celular debe tener conexión a Internet para recibir las notificaciones • Configuración de la app tiene un nivel medio de dificultad
App Microsoft Authenticator, modo **Código de verificación**	• Fácil de utilizar • Más seguro • No requiere tener conexión a Internet	• Requiere de instalación de app en el celular • Configuración de la app tiene un nivel medio de dificultad
Envío de SMS	• Fácil de configurar • Fácil de utilizar • No requiere la instalación de software adicional en el teléfono celular • No requiere de un smartphone	• Los SMS pueden demorar mucho tiempo en llegar • Si su celular no tiene cobertura, los SMS no llegarán • Si sale del país debe pagar roaming para que le lleguen los SMS • No es muy seguro ya que al ser un SMS cualquiera que tenga acceso al teléfono podría ver el SMS
Llamada telefónica	• Fácil de configurar • Fácil de utilizar • No requiere la instalación de software adicional en el teléfono celular • No requiere de un smartphone	• Las llamadas pueden demorar mucho tiempo en llegar • Si su celular no tiene cobertura, no será posible que reciba la llamada • Si sale del país debe pagar roaming para recibir las llamadas de la plataforma • Si configura un teléfono fijo, debe estar siempre cerca de él para recibir la llamada • No es muy seguro ya que cualquiera podría contestar la llamada

Configuración del segundo método de autenticación usando la app Microsoft Authenticator

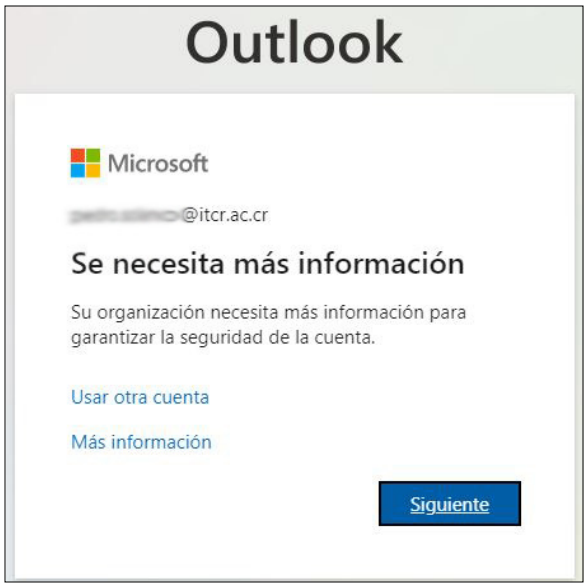
Pasos previos

- Cierre todos los navegadores (Firefox, Chrome, Edge, etc.) que tenga abiertos en la computadora.
- Asegúrese de tener a mano usuario y contraseña de su correo TEC.
- Descargue la app "Microsoft Authenticator" en su teléfono desde la tienda de apps de su teléfono celular.

Configuración

1. Ingrese al correo institucional vía web por medio del siguiente enlace: www.tec.ac.cr/correo

2. Al ingresar, le debe aparecer la siguiente ventana:



Haga clic en el botón *"Siguiente"*.

3. En la siguiente ventana, haga clic donde dice *Teléfono de autenticación* y seleccione *Aplicación Móvil*. *Ver Figura 1*.

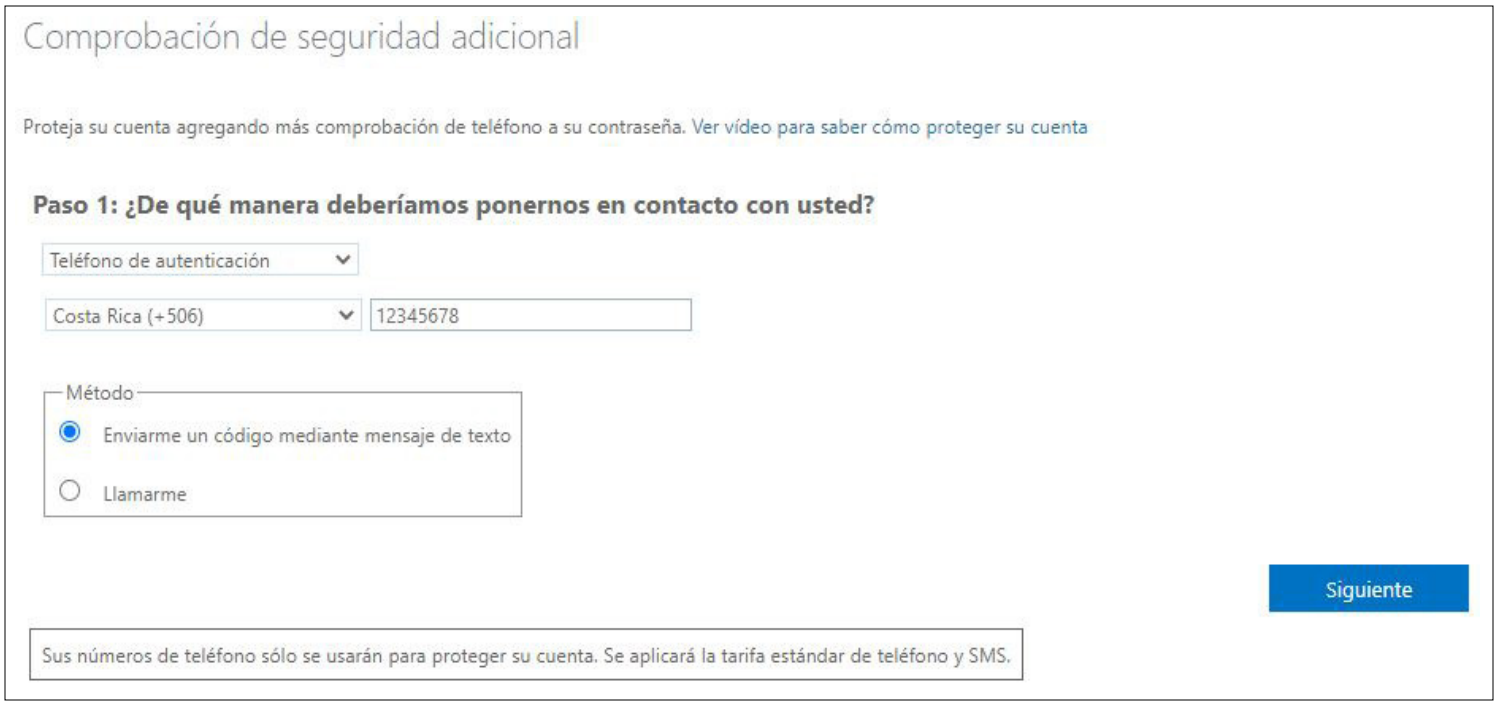


Figura 1.

4. Cuando seleccionamos *Aplicación Móvil* se muestran dos opciones para configurar la app. *Ver figura 2*.

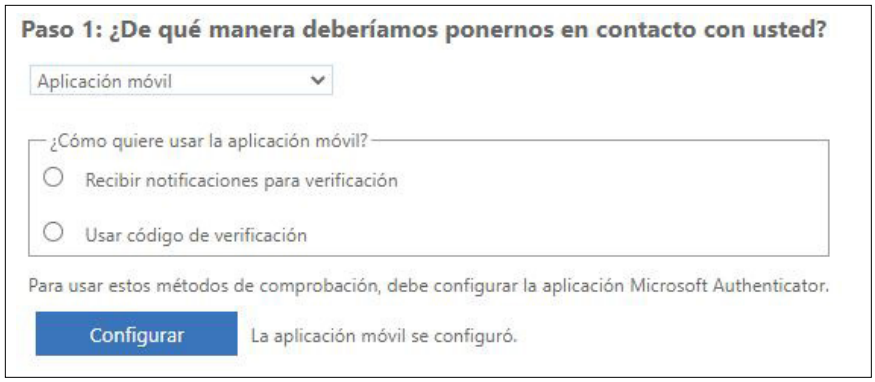


Figura 2.

Seleccione el método que mejor se adapte a su forma de trabajo; tenga en consideración la tabla de ventajas y desventajas sobre los métodos.

a. Método: Recibir notificaciones para verificación

- Seleccionamos la opción *Recibir notificaciones para verificación*
- En el teléfono celular, abra la app *Microsoft Authenticator*
    - Acepte el contrato
    - Luego seleccione *Agregar cuenta*
    - Ahora seleccione *Cuenta profesional o educativa*
    - Posteriormente seleccione *Escanear código QR*
    - En caso de que la app pida permiso para abrir la cámara, permítalo. *Ver figura 3.*

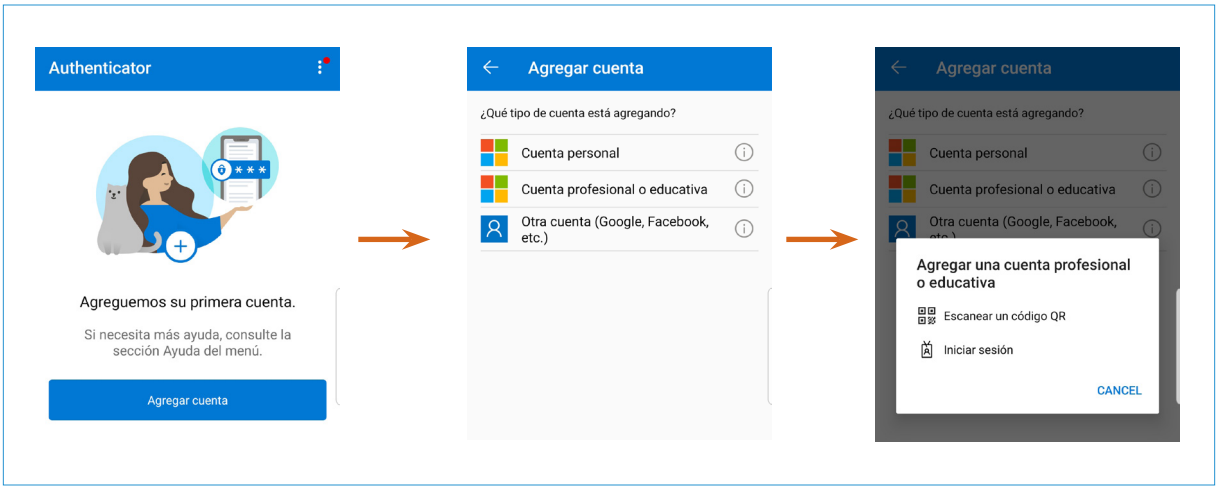


Figura 3.

- En la página de correo, haga clic en el botón *Configurar.*

Al hacer clic se desplegará un código QR el cual debe escanear con la app. *Ver figura 4.*

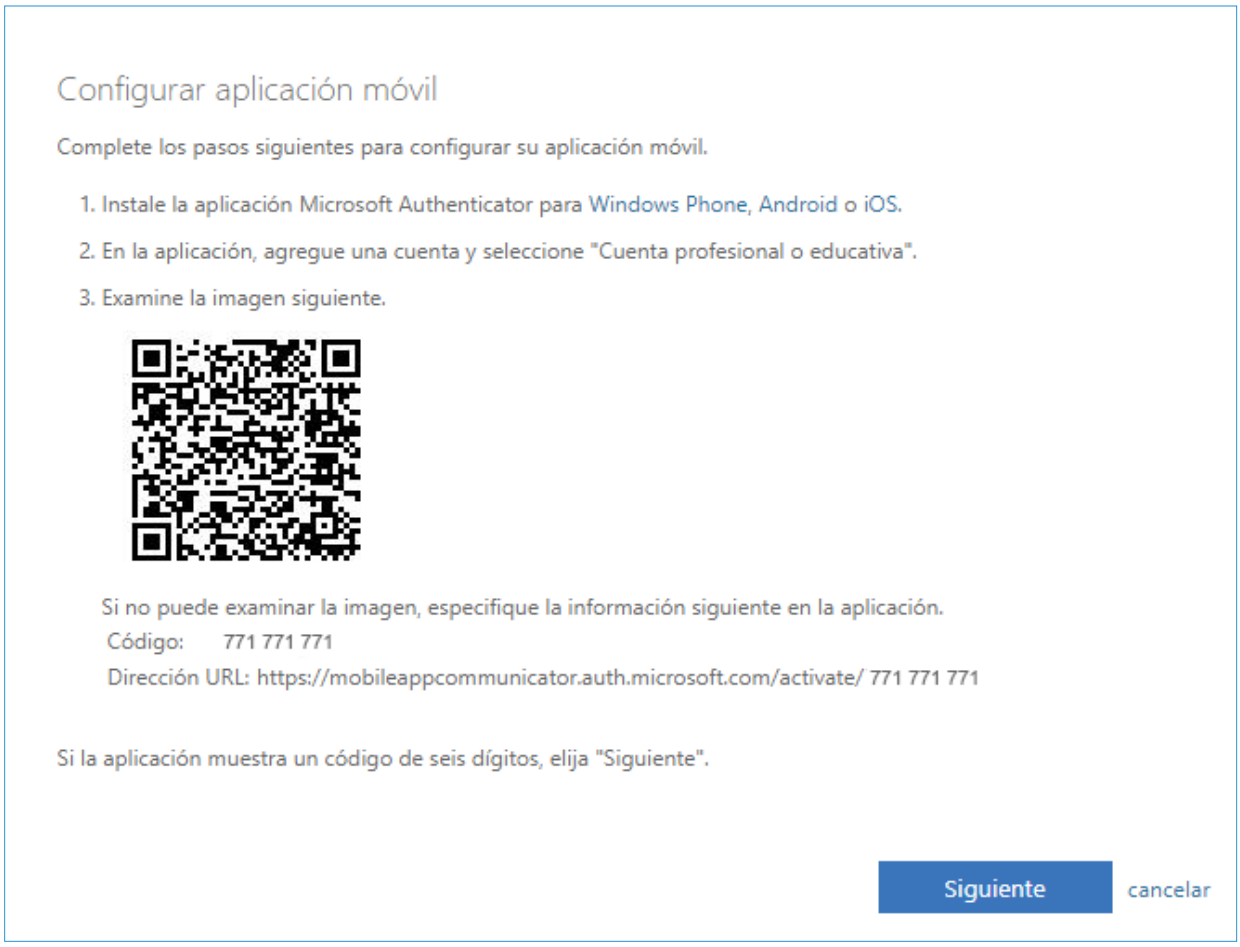


Figura 4.

Una vez que el código QR sea leído por la app, aparecerá una línea con el título TEC y abajo su dirección de correo. *Ver figura 5.*

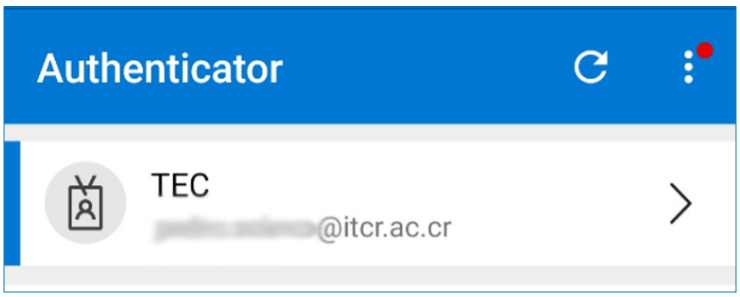


Figura 5.

• Posteriormente, en la computadora se debe hacer clic en el botón *Siguiente,* el cual llevará hacia una ventana que indica que se está enviando una notificación al teléfono celular (similar a la que se muestra) para validar su inicio de sesión; usted debe aprobarla o denegarla. *Ver figura 6.*

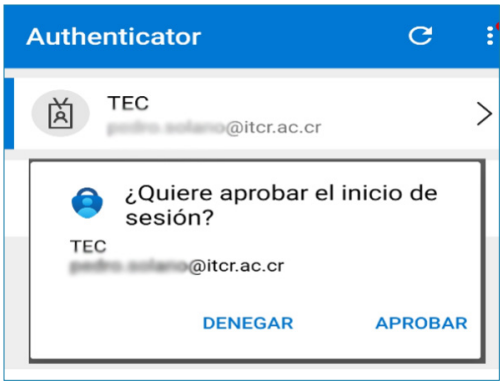


Figura 6.

• Una vez que se aprueba la solicitud de inicio de sesión, el sistema solicitará ingresar un número de teléfono el cual será utilizado en caso de que no tengamos acceso a la app y necesitemos ingresar a los servicios Microsoft en línea. *Ver figura 7.*

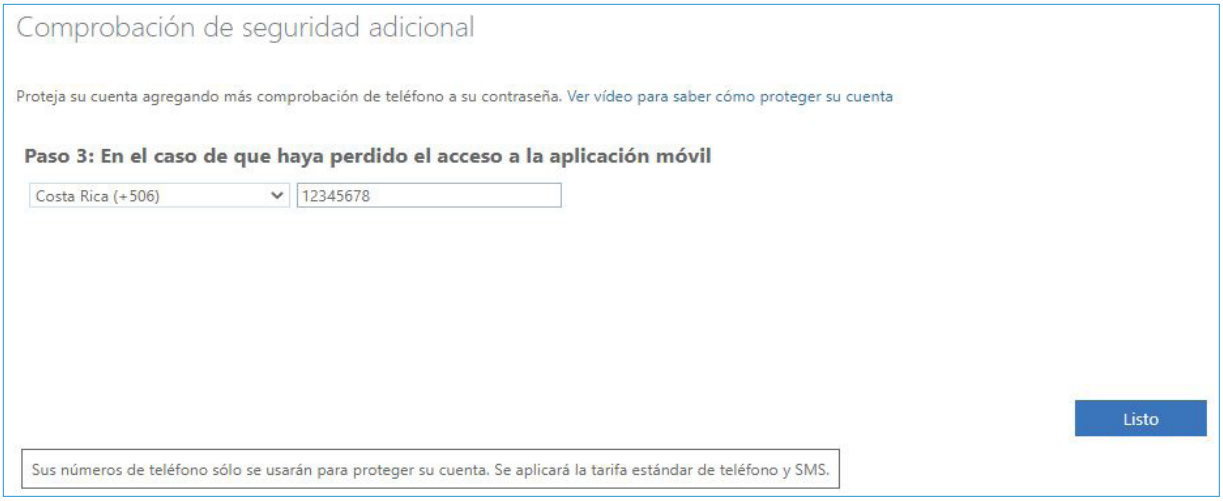


Figura 7.

Se debe seleccionar código de área o región -Costa Rica (+506)- y luego escribir el número de teléfono al que la plataforma lo contactará.

Posteriormente se debe hacer clic en *Listo* para finalizar la configuración.

b. Método: Usar código de verificación

- Seleccionamos la opción *Recibir notificaciones para Usar Código de verificación*
- En el teléfono celular, abrir la app *Microsoft Authenticator*
  - Aceptar el contrato
  - Luego seleccione *Agregar cuenta*
  - Luego seleccione *Cuenta profesional o educativa*
  - Posteriormente seleccione *Escanear código QR*
  - En caso de que la app pida permiso para abrir la cámara, permitirlo. *Ver figura 8.*

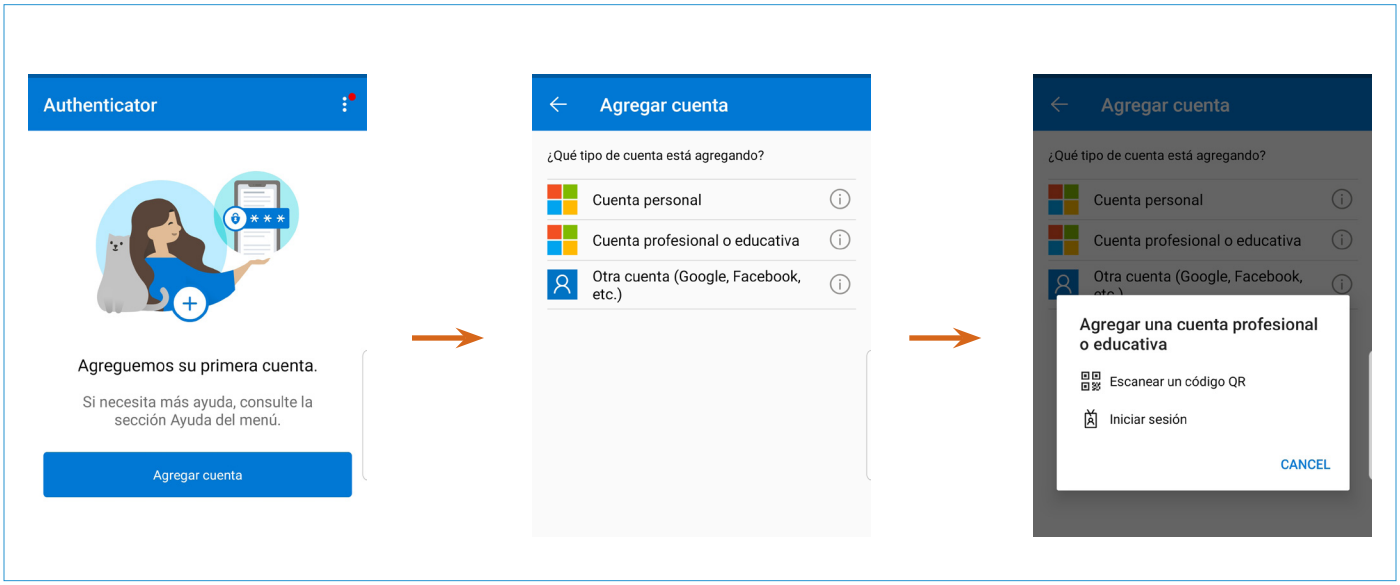


Figura 8.

- En la página de correo, hacer clic en el botón *Configurar.*
- Al hacer clic se desplegará un código QR el cual debe escanear con la app. *Ver figura 9.*

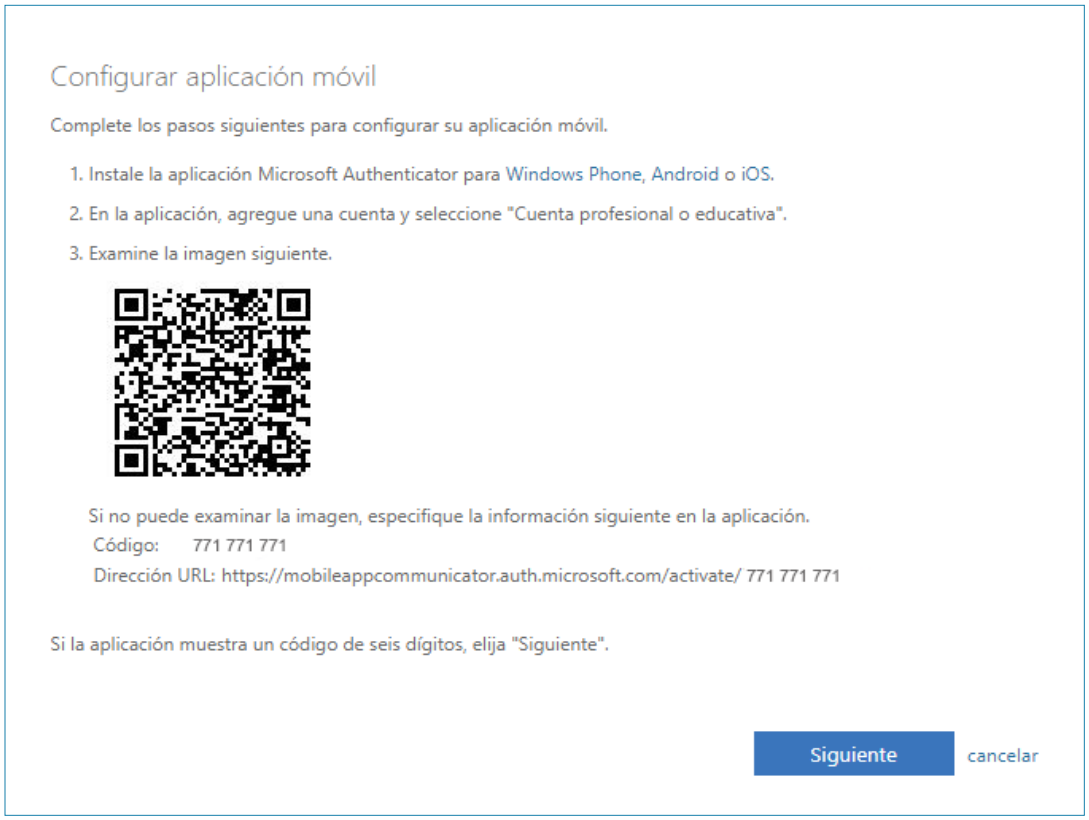


Figura 9.

- Una vez el código QR sea leído por la app, aparecerá el título TEC y abajo su dirección de correo. *Ver figura 10.*

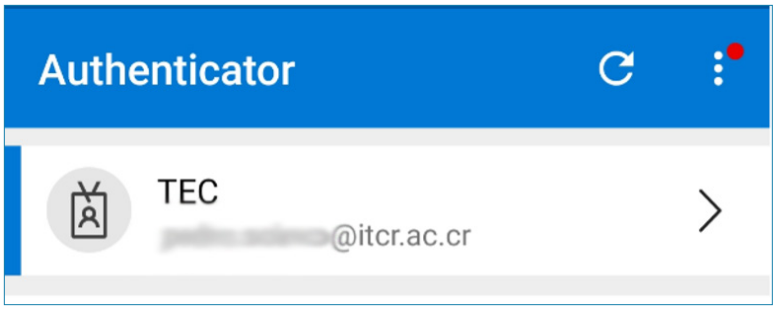


Figura 10.

- Posteriormente, en la computadora se debe hacer clic en el botón *Siguiente* el cual nos llevará hacia una ventana que solicita el código que se está generando en la app.

Para obtener este código, debe ingresar a la app y seleccionar su cuenta. En este punto, se estará desplegando un código de seis dígitos, el cual debe digitar en la página web donde se le solicita. El código se autogenera cada 30 segundos. *Ver figura 11*.

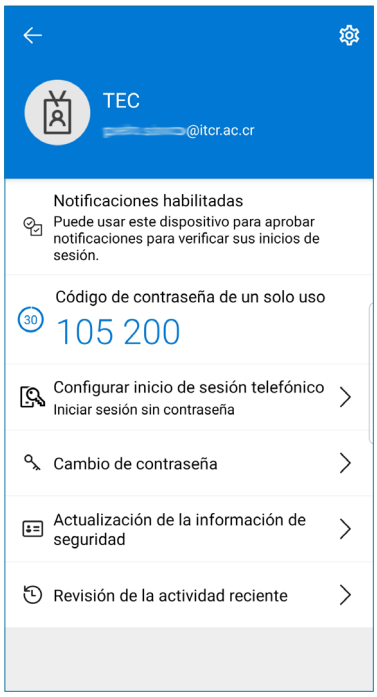


Figura 11.

Configuración del segundo método de autenticación usando la app en modo Envío de mensaje de texto (SMS)

Pasos previos:

1. Cierre todos los navegadores (Firefox, Chrome, Edge, etc.) que tenga abiertos en su computadora.

2. Asegúrese de tener a mano usuario y contraseña de su correo TEC.

Instalación

1. Ingrese al correo institucional vía web por medio del siguiente enlace: www.tec.ac.cr/correo

2. Al ingresar debe aparecer la siguiente ventana (*ver figura 12*)

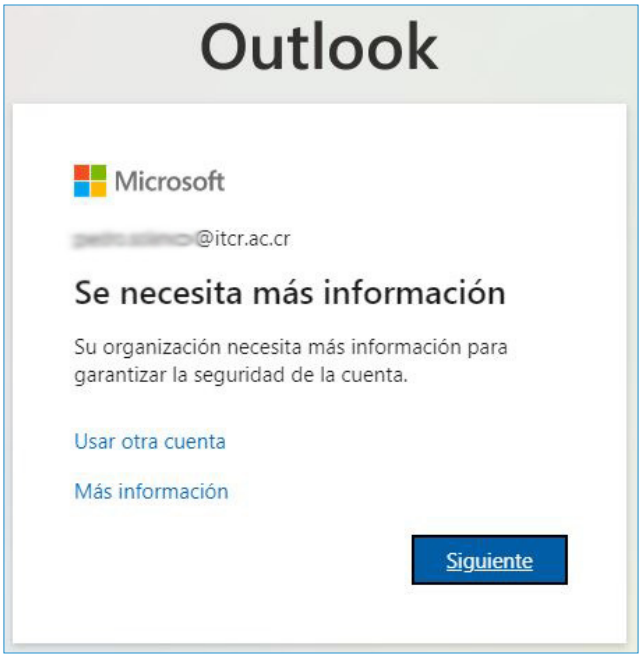


Figura 12.

Haga clic en el botón *Siguiente*.

3. En la siguiente ventana se muestra la configuración para envío de mensaje por medio de SMS.

- Se debe seleccionar el código de país o región (Costa Rica (+506)) y luego escribir el número de teléfono al cual se enviará el SMS. Este número de teléfono debe ser un número celular.

- Posteriormente se debe seleccionar la opción:

  Enviarme un código mediante mensaje de texto.

- Una vez que completes los datos se debe hacer clic en el botón *Siguiente*. *Ver figura 13.*

Figura 13.

- Cuando hacemos clic en *Siguiente*, se nos solicita el código de verificación que fue enviado a nuestro teléfono celular; digítelo en el espacio y haga clic en *Comprobar. Ver figura 14.*

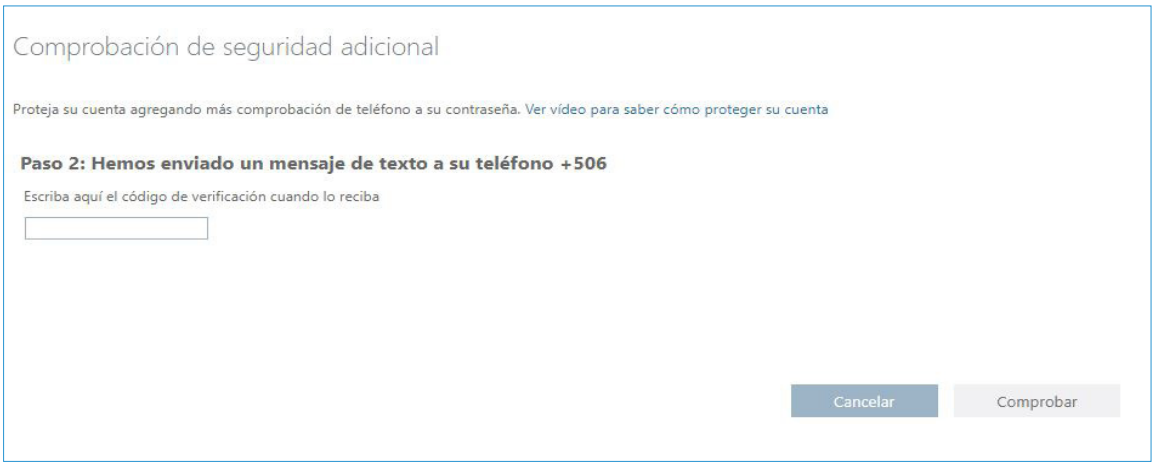


Figura 14.

Una vez que la comprobación es correcta haga clic en el botón *Listo* para continuar e ingresar al correo electrónico.

El doble factor de autenticación será necesario para poder ingresar a cualquier servicio Microsoft 365 desde la web *(correo electrónico, MS Forms, MS Teams, OneDrive, etc.).*

De igual forma las aplicaciones de escritorio pueden solicitar en algún momento la validación del segundo factor.

Para aclarar cualquier duda o consulta puede llamar a la extensión 9500, o escribir a soporte@itcr.ac.cr

DATIC

DEPARTAMENTO DE ADMINISTRACIÓN
DE TECNOLOGÍAS DE INFORMACIÓN
Y COMUNICACIONES

SOPORTE@ITCR.AC.CR