

INSTRUCTIVO PARA LA CONFIGURACIÓN DEL DOBLE FACTOR DE AUTENTICACIÓN EN LOS SERVICIOS INFORMÁTICOS

División de Gestión Informática

1. Definición

La Universidad de Antioquia con el fin de mejorar las condiciones de seguridad digital de sus servicios informáticos, establece la configuración adicional en la autenticación de los usuarios mediante la implementación del Doble Factor de Autenticación (2FA), siendo este una capa adicional de seguridad que se suma a la contraseña del usuario.

Este 2FA será requerido, cada vez que intente acceder a los servicios informáticos, como lo son: correo electrónico institucional, OneDrive, Microsoft Teams entre otros, se le pedirá un segundo código de verificación. Este código se generará a través de cualquiera de las siguientes opciones:

- **Mensaje de texto:** se enviará por SMS a su número de teléfono móvil un código el cual deberá ingresar al momento de la solicitud del 2FA.
- **Llamada Telefónica:** Recibirá una llamada a su teléfono móvil o fijo con el código que deberá ingresar al momento de la solicitud del 2FA.
- **Microsoft Authenticator:** Una app que se podrá descargar e instalar en su teléfono móvil.

El presente instructivo describe los pasos a seguir para seleccionar el método de 2FA que cada usuario desee utilizar para el ingreso a las diferentes plataformas.

2. Contenido

2.1 Configuración del Doble Factor de Autenticación (2FA)

Para comenzar a utilizar el 2FA, sigue estos pasos:

1. **Accede a la plataforma:**
 - Puedes acceder a la plataforma de configuración de 2FA a través del enlace: <https://link.udea.edu.co/doblefactor> o iniciando sesión en cualquier plataforma de la Universidad que requiera autenticación, como el correo electrónico institucional, OneDrive o Microsoft Teams.
2. **Inicia sesión:**
 - Ingresa tu usuario completo (incluido el dominio, por ejemplo: usuario@udea.edu.co) y haz clic en "Siguiete" (Figura 1).
 - Ingresa tu contraseña y haz clic en "Iniciar sesión" (Figura 2).

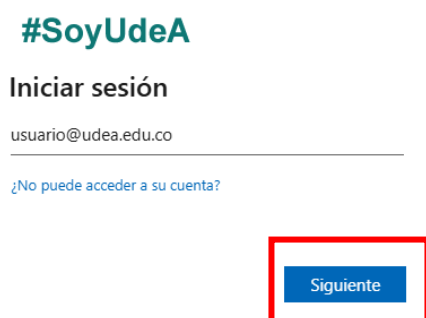


Figura 1



Figura 2

3. Verificación de seguridad:

- La plataforma te indicará que necesitas más información para garantizar la seguridad de tu cuenta. Haz clic en "Siguiete" (Figura 3).

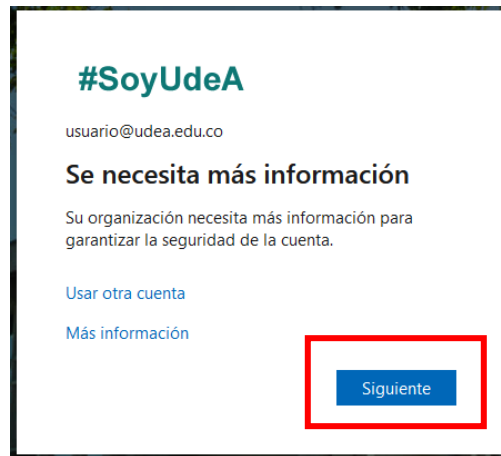


Figura 3

4. Selecciona tu método de 2FA:

- La plataforma te permitirá configurar varios métodos de 2FA según tu preferencia:
 - Mensaje de texto (SMS)
 - Llamada telefónica
 - Aplicación Microsoft Authenticator

2.1.1 Método 1: Mensaje de texto

1. Selecciona "Quiero configurar otro método":

- Después de la Figura 3, haz clic en la opción "Quiero configurar otro método" para elegir un método de 2FA diferente (Figura 4).

2. Selecciona "Teléfono":

- En la siguiente pantalla, selecciona la opción "Teléfono" para configurar un número de teléfono celular (Figura 5).

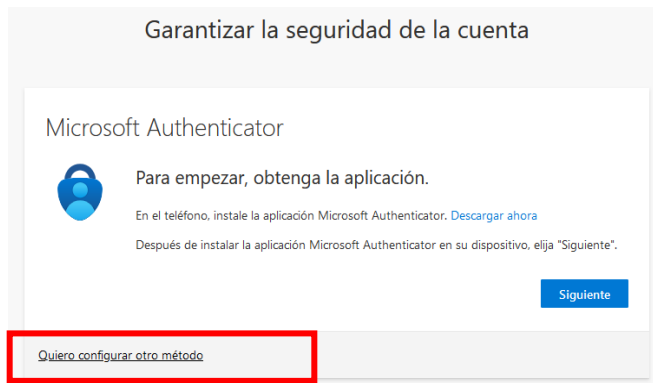


Figura 4

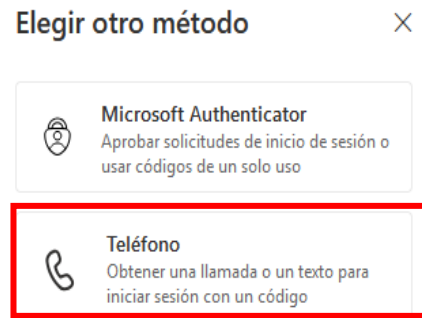


Figura 5

3. Ingresas tu número de teléfono:

- Selecciona el país, digita tu número de teléfono celular y selecciona el método "Recibir un código". Luego, haz clic en "Siguiente" (Figura 6).

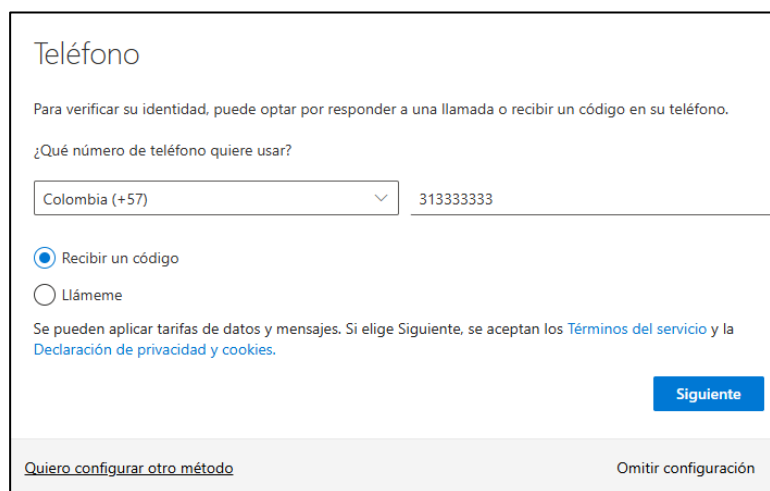


Figura 6

4. Verificación de seguridad (opcional):

- Es posible que la plataforma solicite una verificación adicional para confirmar que no eres un robot (Figura 7). Si es así, ingresa los caracteres que se muestran en tu pantalla y haz clic en "Siguiente".

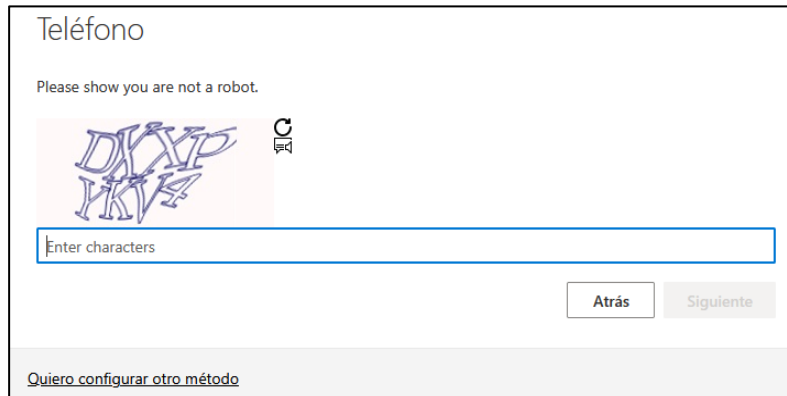


Figura 7

5. Ingresa el código de verificación:

- Se te enviará un código de verificación a tu teléfono celular mediante mensaje de texto. Ingresa el código y haz clic en "Siguiente" (Figura 8).



Figura 8

6. Confirmación:

- Se mostrará un mensaje de confirmación del 2FA (Figura 9). Haz clic en "Siguiente" para confirmar que tu método preferido de 2FA se ha configurado correctamente (Figura 10).

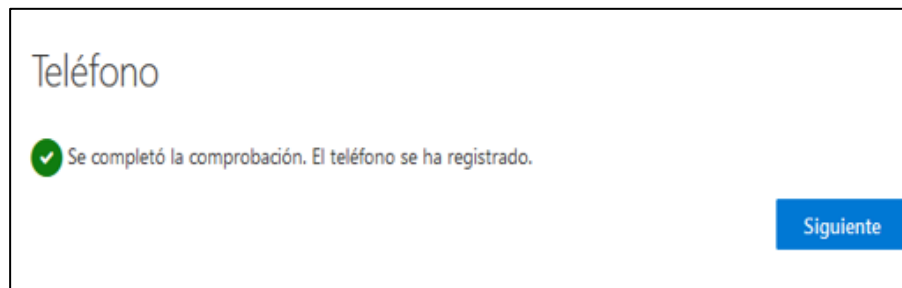


Figura 9

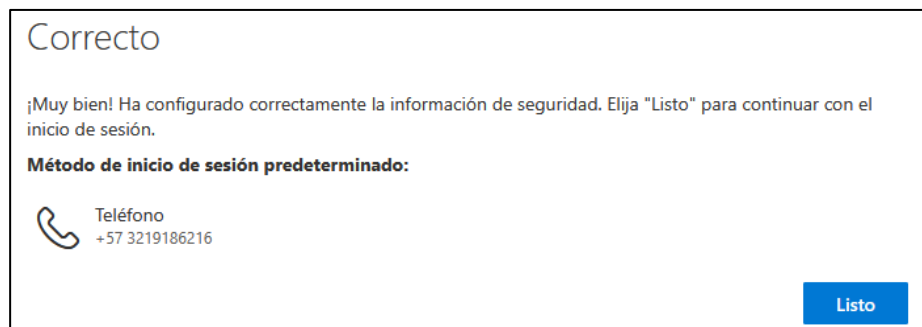


Figura 10

2.1.2 Método 2: Llamada telefónica

1. Selecciona "Quiero configurar otro método":

- Haz clic en la opción "Quiero configurar otro método" para elegir un método de 2FA diferente (Figura 11).

2. Selecciona "Teléfono":

- En la siguiente pantalla, selecciona la opción "Teléfono" para configurar un número de teléfono fijo o celular (Figura 12).

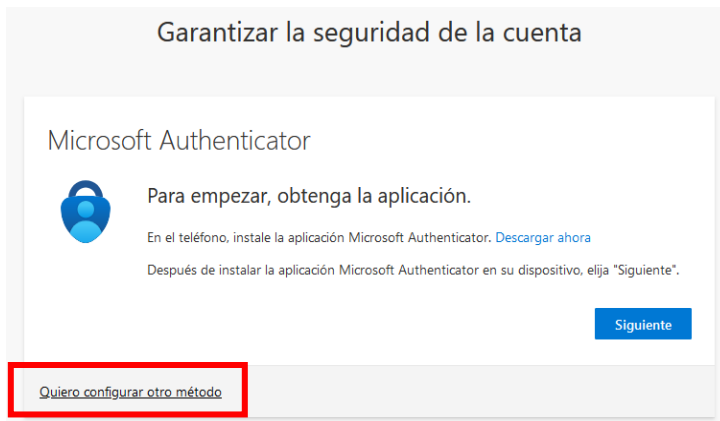


Figura 11

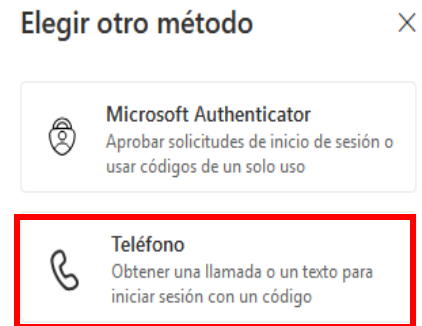


Figura 12

3. Ingresa tu número de teléfono:

- Selecciona el país, digita tu número de teléfono fijo o celular y selecciona el método "Llámame". Luego, haz clic en "Siguiente" (Figura 13).

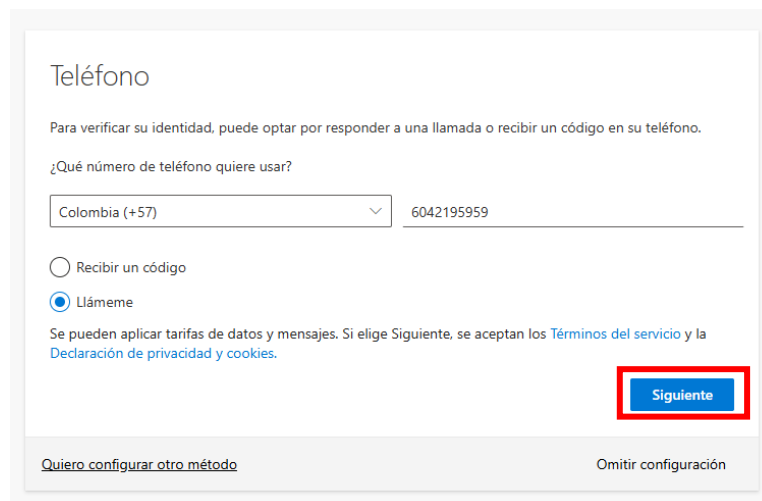


Figura 13

4. Verificación de seguridad (opcional):

- Es posible que la plataforma solicite una verificación adicional para confirmar que no eres un robot (Figura 14). Si es así, ingresa los caracteres que se muestran en tu pantalla y haz clic en "Siguiente".

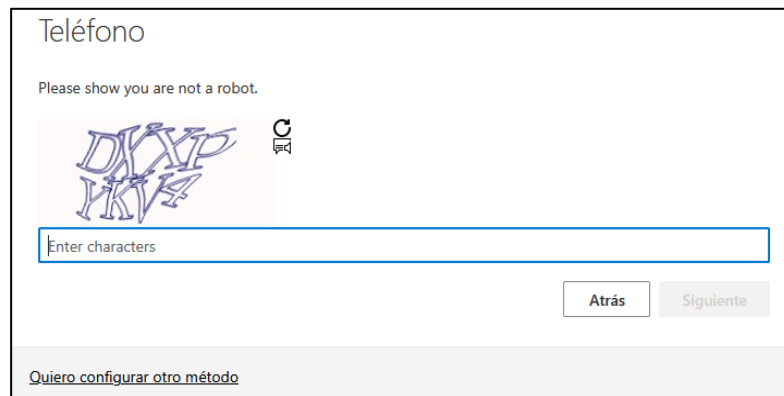


Figura 14

5. Recibe la llamada y presiona la tecla (#):

- Recibirás una llamada telefónica (Figura 15). Contesta la llamada y presiona la tecla numeral (#) para confirmar.



Figura 15

6. Confirmación:

- Se mostrará un mensaje de confirmación del 2FA (Figura 16). Haz clic en "Siguiente" para confirmar que tu método preferido de 2FA se ha configurado correctamente (Figura 17).

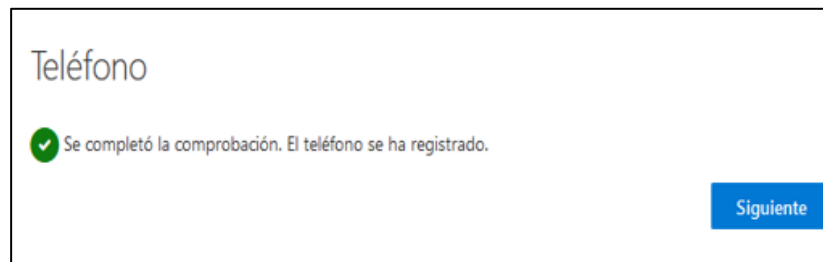


Figura 16

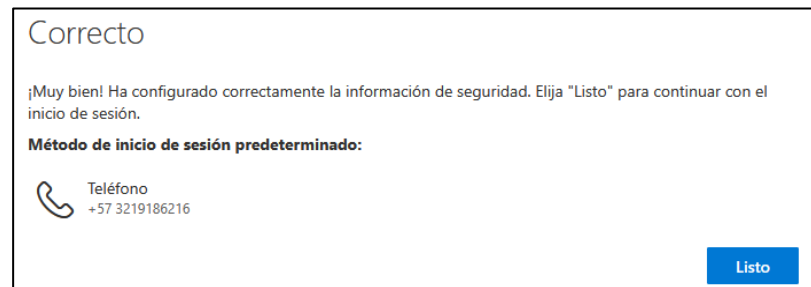


Figura 17

Consideraciones importantes:

1. **Teléfono celular:** Si utilizas un número de teléfono celular, puedes seleccionar cualquiera de los dos métodos de 2FA (mensaje de texto o llamada telefónica). Asegúrate de tener tu dispositivo a la mano cuando se te envíe el código o recibas la llamada.
2. **Teléfono fijo:** Si utilizas un número de teléfono fijo, solo podrás seleccionar la llamada telefónica como método de 2FA. Además, deberás estar en el lugar donde se encuentra el teléfono fijo para contestar la llamada.

Recomendación:

Se recomienda configurar un teléfono celular para recibir mensajes de texto o llamadas, ya que ofrece mayor flexibilidad y movilidad.

2.1.3 Método 3: Configurar Aplicación Microsoft

Authenticator

1. Instala la aplicación:

- Si aún no tienes la aplicación Microsoft Authenticator instalada en tu dispositivo móvil, descárgala desde la tienda de aplicaciones correspondiente (Android o iOS).

2. Accede a la configuración de 2FA:

- Haz clic en la opción "Siguiente" para elegir Microsoft Authenticator como método de 2FA.

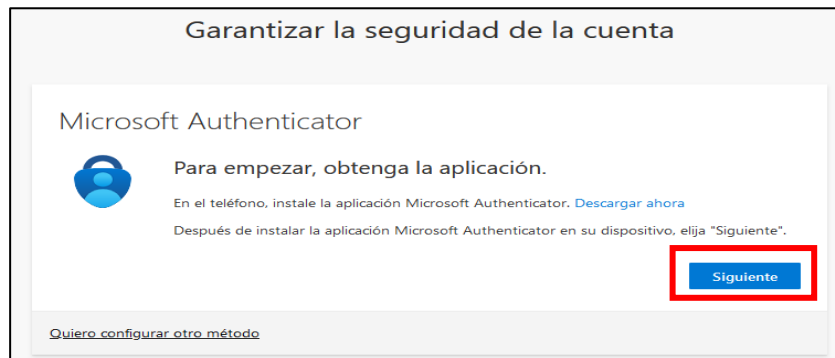


Figura 18

3. Escanea el código QR:

- La plataforma te mostrará un código QR (Figura 19). Abre la aplicación Microsoft Authenticator en tu dispositivo móvil y escanea este código para vincular tu cuenta.

Microsoft Authenticator

Digitalización del código QR

Use la aplicación Microsoft Authenticator para escanear el código QR. Así, la aplicación Microsoft Authenticator y la cuenta quedarán emparejadas.

Después de escanear el código QR, elija "Siguiente".



¿No puede escanear la imagen?

Atrás

Siguiente

Figura 19

4. Acepta los términos y accede a la app:

- Abre la aplicación Microsoft Authenticator en tu dispositivo, si es la primera vez que inicias la aplicación verás la información para aceptar el tratamiento de datos personales como se ilustra en la figura 20. Y haz clic en continuar para ver la pantalla de inicio como se ilustra en la figura 21. donde debes hacer clic en escanear código QR.

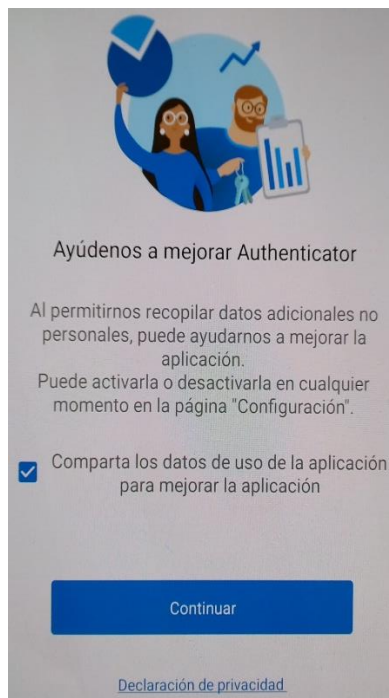


Figura 20

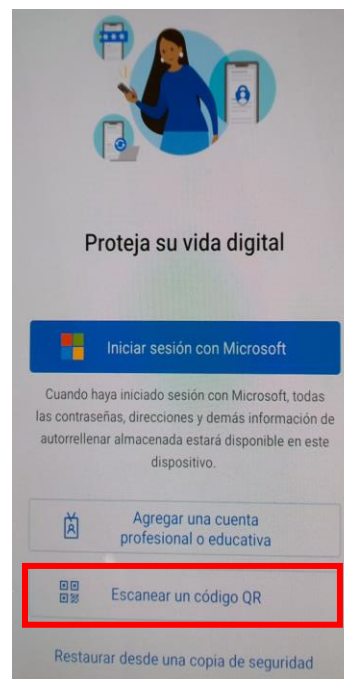


Figura 21

5. Añadir nueva cuenta:

- Si ya tienes la aplicación instalada y deseas agregar una cuenta nueva, debe hacer clic en la opción escanear QR como se ilustra en la en la figura 22.

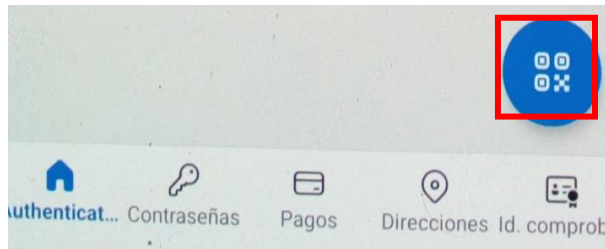


Figura 22

6. Espera la sincronización:

- Al escanear el código QR, verás una pantalla como la que se ilustra en la figura 23. Debe esperar a que se sincronice y se cierre automáticamente; de esta forma, ya tendrás la cuenta vinculada con la aplicación.

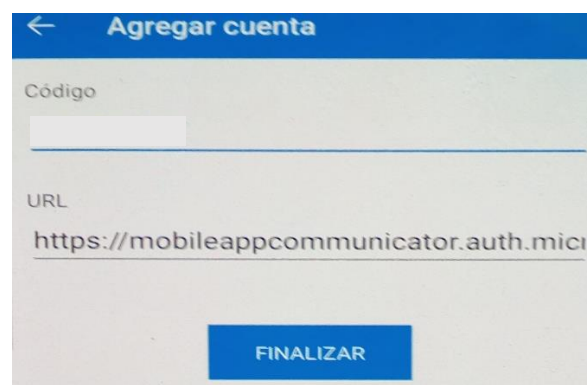


Figura 23

7. Finaliza la configuración:

- Para finalizar la configuración, haz clic en "Siguiete" (Figura 24).



Figura 24

8. Ingresa el código de verificación:

- La aplicación enviará una notificación para que ingreses el código que se muestra en la pantalla (Figura 25).

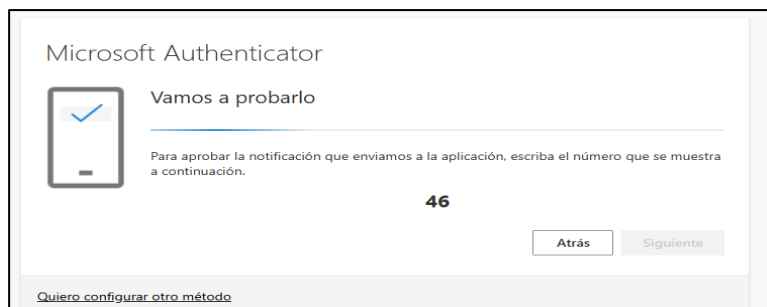


Figura 25

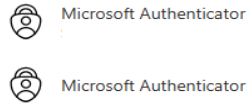
9. Confirmación:

- Se mostrará un mensaje de confirmación indicando que el proceso ha finalizado. En ese momento, ya estará configurado el método de Microsoft Authenticator (Figura 26).

Correcto

¡Muy bien! Ha configurado correctamente la información de seguridad. Elija "Listo" para continuar con el inicio de sesión.

Método de inicio de sesión predeterminado:



Listo

Figura 26

2.1.4 Registrar método alternativo de 2FA

Se recomienda establecer al menos dos métodos de 2FA. Si pierdes el acceso a uno de ellos, podrás seguir utilizando el otro para acceder a los servicios informáticos.

1. Accede a la configuración de 2FA:

- Ingresa al siguiente enlace: <https://link.udea.edu.co/doblefactor>
- Haz clic en la opción "Ver cuenta" (Figura 27).
- Luego, haz clic en "Información de seguridad" (Figura 28).

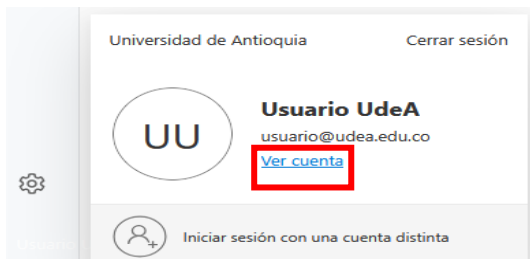


Figura 27

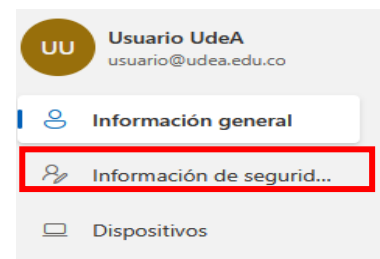


Figura 28

2. Agrega un nuevo método:

- Haz clic en la opción "Agregar método de inicio de sesión" (Figura 29).
- Selecciona el método de tu elección (Figura 30).

Instructivo para la configuración del doble factor de autenticación en los servicios informáticos

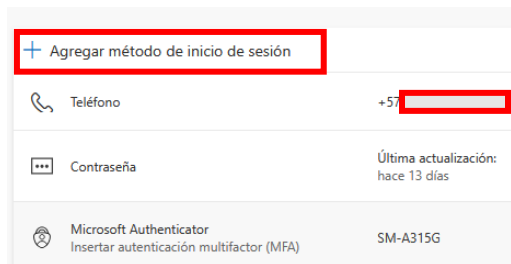


Figura 29

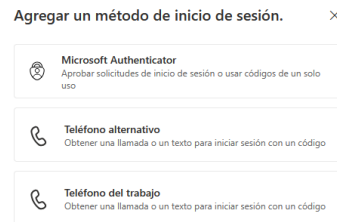


Figura 30

Nota:

- Tenga en cuenta que contar con métodos adicionales de 2FA, puede garantizar nuestro acceso a las diferentes plataformas como Correo electrónico institucional, en caso de pérdida o daño de nuestros dispositivos móviles.

3. Nota de cambio.

- No aplica para la primera versión.

<p>Elaboró: Equipo de trabajo División de Gestión Informática</p>	<p>Revisó: Julio César García Castrillón Analista de Procesos División de Estrategia y Organización</p>	<p>Aprobó: Jaime Ignacio Montoya Giraldo Director Dirección de Planeación y Desarrollo Institucional</p>
<p>Fecha: 13-FEB-2025</p>	<p>Fecha: 19-FEB-2025</p>	<p>Fecha: 20-FEB-2025</p>