

Microsoft Office 365

Doble factor de autenticación

El doble factor de autenticación (o autenticación en dos pasos) constituye una medida de seguridad importante, que adiciona una segunda capa de protección a la contraseña que empleamos. Una contraseña es algo que usted sabe, pero también algo que otras personas pueden saber o descubrir. Sin el doble factor de autenticación habilitado, cualquier persona que tenga conocimiento de su usuario y contraseña podrá acceder y hacer mal uso de su identidad.

Para poder acceder al servicio después de habilitar el doble factor de autenticación, requerirá de su contraseña y un segundo elemento para probar su identidad; en este caso algo que usted tiene (un número generado aleatoriamente por una aplicación en su celular).

¿Qué necesito?

- Credenciales de Microsoft 365 (numeroedocumento@icesi.edu.co numeroedocumento@u.icesi.edu.co) y contraseña de usuario único.
- Un dispositivo móvil (Institucional o personal), para instalar la aplicación de doble factor de autenticación.
- Un computador para poder hacer la configuración necesaria de la aplicación de doble factor.

Pasos para realizar la configuración del doble factor de autenticación

Prerrequisito:

Descarga e instalación de la aplicación de doble factor de autenticación


Antes de iniciar el proceso de configuración, se requiere la instalación de la aplicación de doble factor de autenticación de Microsoft. Luego podrá escanear el código QR según su sistema operativo, que lo llevará a las tiendas oficiales correspondientes.

En caso de que desee hacerlo usted mismo, busque la aplicación “**Microsoft Authenticator**”.

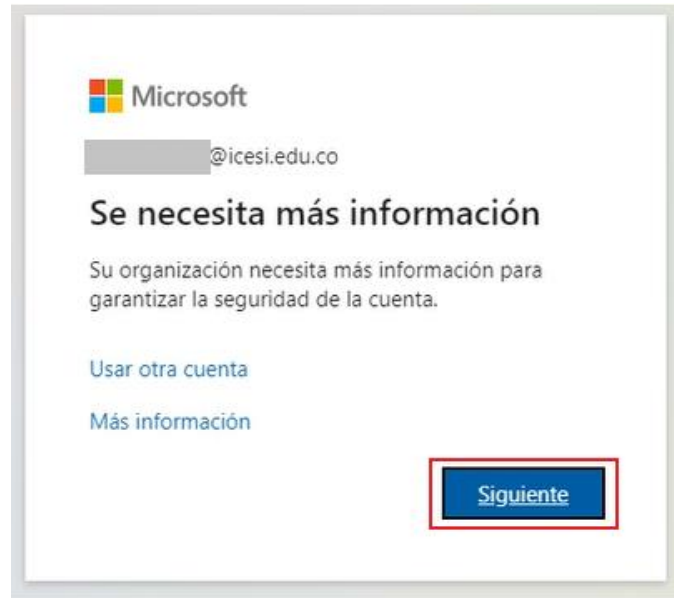


Microsoft Authenticator



Después de realizar este proceso, un nuevo ícono llamado “Authenticator” aparecerá en su dispositivo móvil:  , el cual necesitará posteriormente.

Paso 1. Iniciar sesión y empezar el proceso de configuración del doble factor: Ingrese a <https://login.microsoftonline.com>, y luego de iniciar sesión, aparecerá el siguiente aviso al tratar de ingresar al servicio. En este punto, damos clic en el botón de “Siguiente”.

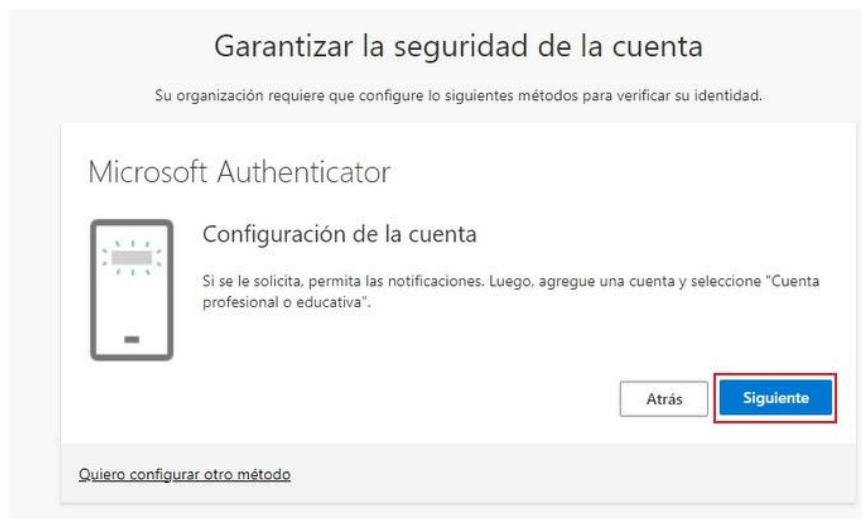


Paso 2. Configuración del doble factor de autenticación:

Llegará a la página llamada “Garantizar la seguridad de la cuenta”, donde se le pedirá que descargue la aplicación Microsoft Authenticator, que se menciona en el prerequisite de este documento. Después de instalada la aplicación dar clic en “Siguiete”.

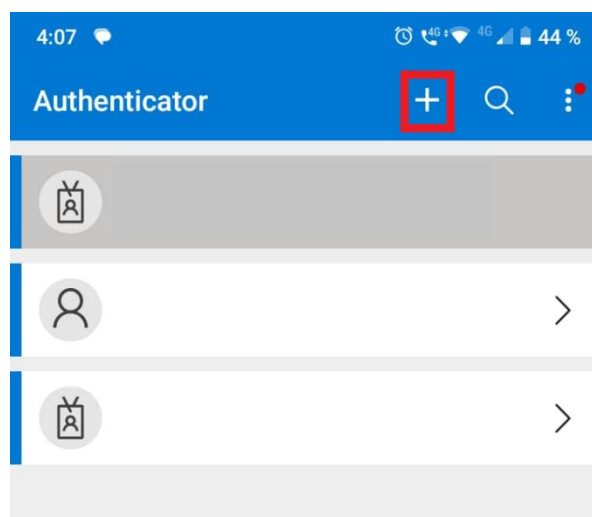


Deberá configurar la cuenta en la aplicación Microsoft Authenticator; esta configuración la hará según el paso 3. Después de configurada, dar clic en “Siguiente”.

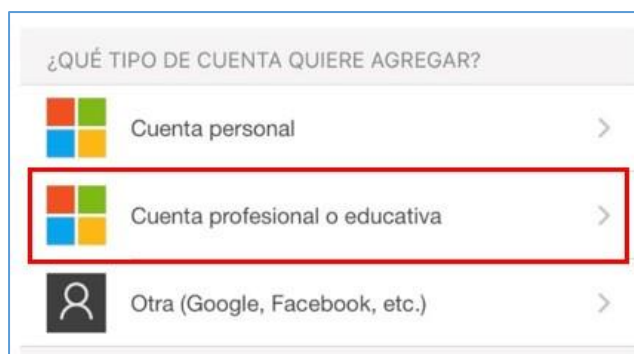


Paso 3. Configuración de la aplicación Microsoft Authenticator:

En este punto, en el navegador nos mostrará un código QR que debemos escanear con la aplicación Microsoft Authenticator, la cual se ha instalado previamente. Tome su celular, abra la aplicación y salte las pantallas de bienvenida que aparezcan, hasta que aparezca la correspondiente a “¿Preparado para agregar su primera cuenta?”. En este punto haga clic en la opción “Agregar cuenta” o en el botón “+” en la parte superior.

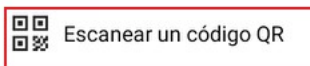


Posteriormente, debe seleccionar la opción “Cuenta profesional o educativa”:



Y escoja la opción “Escanear un código QR”. **Nota:** Si le solicita permisos para acceder a la cámara, por favor pulse en el botón Aceptar.

Agregar una cuenta profesional o educativa



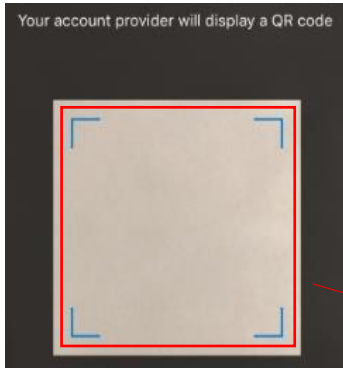
Iniciar sesión

CANCELAR

Nota: Si su dispositivo cuenta con cámara para el escaneo del código QR seguir al paso 4, de lo contrario ir al paso 5.

Paso 4. Escanear código QR:

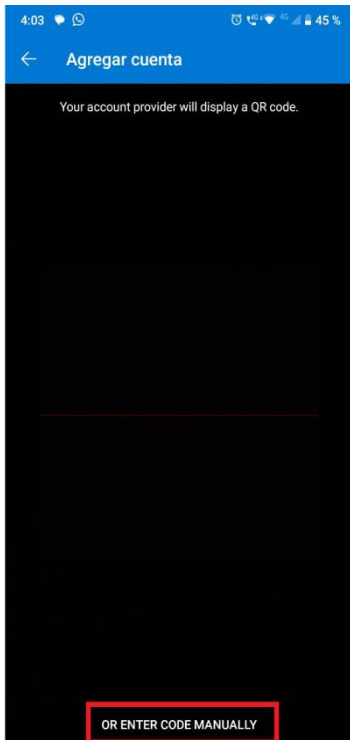
Tome su celular y apunte a la página que aparece en su pantalla. Encadre el código QR (la imagen que aparece resaltada como ejemplo en la imagen inferior) para que quede dentro del cuadro que aparece en su celular. Si en su celular aparece un código de seis dígitos, pulse el botón “Siguiente”, continuar al paso 6.



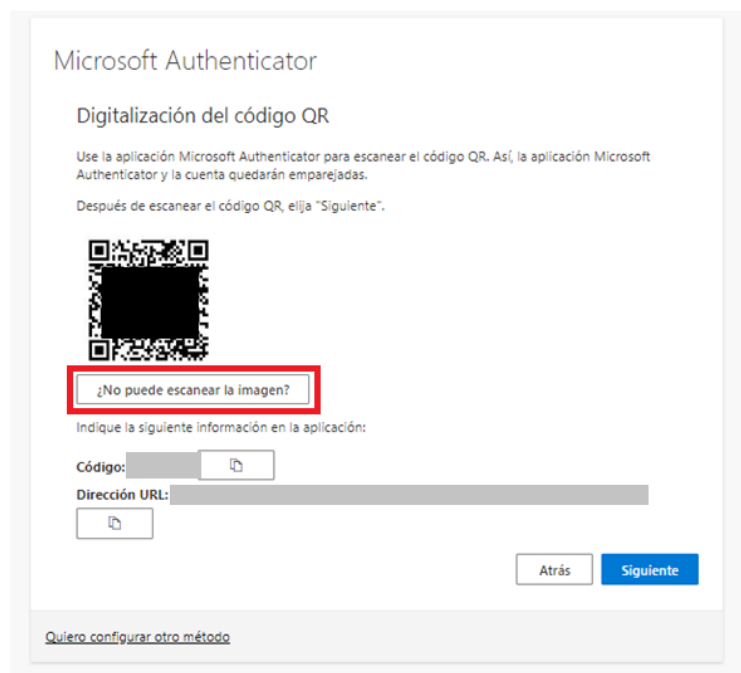
Paso 5. Método alternativo de emparejamiento:

Después de seleccionar “Escanear un código QR” en el paso 3, seleccionar “or enter code manually”, para realizar el emparejamiento manual. A su vez en el navegador seleccionar “¿No puede escanear la imagen?”, donde se desplegará un código y dirección URL, las cuales deberá copiar.

En su celular

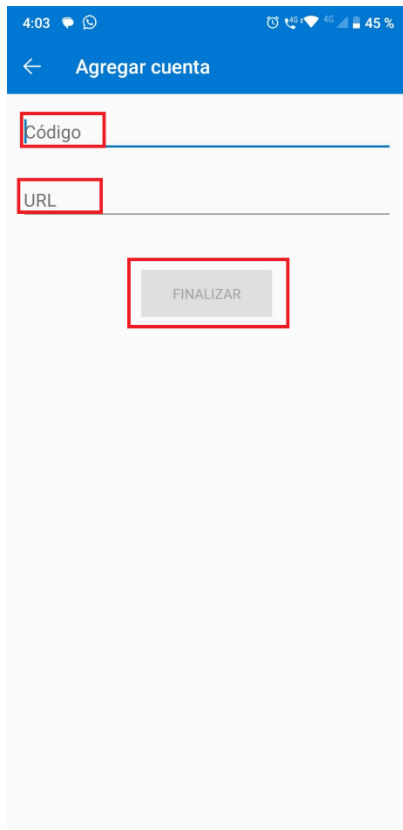


En su computador o celular



A continuación en su celular ingresar el código y dirección URL copiada anteriormente y pulse el botón “Finalizar”. En su navegador, pulsar el botón “Siguiente”:

En su celular



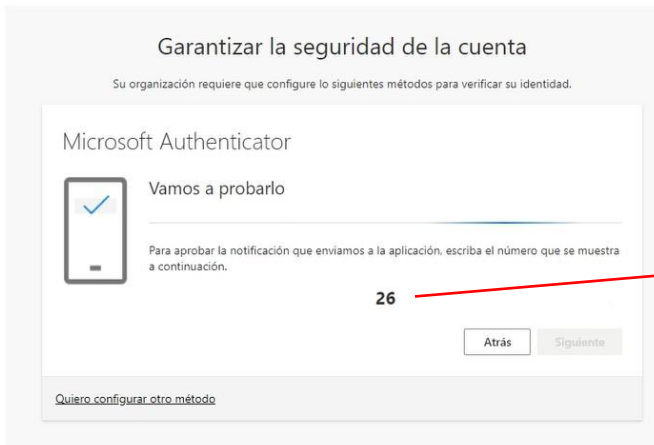
En su computador o celular



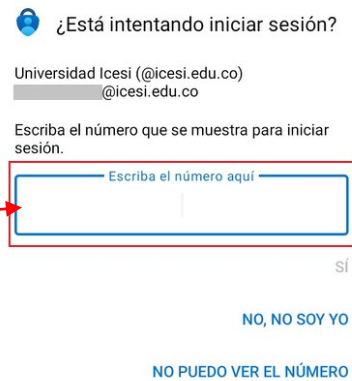
Paso 6. Comprobación de configuración:

Luego de pulsar el botón “Siguiete”, aparecerá en pantalla un número de verificación, que deberá de ingresarlo en la aplicación.

En su computador o celular



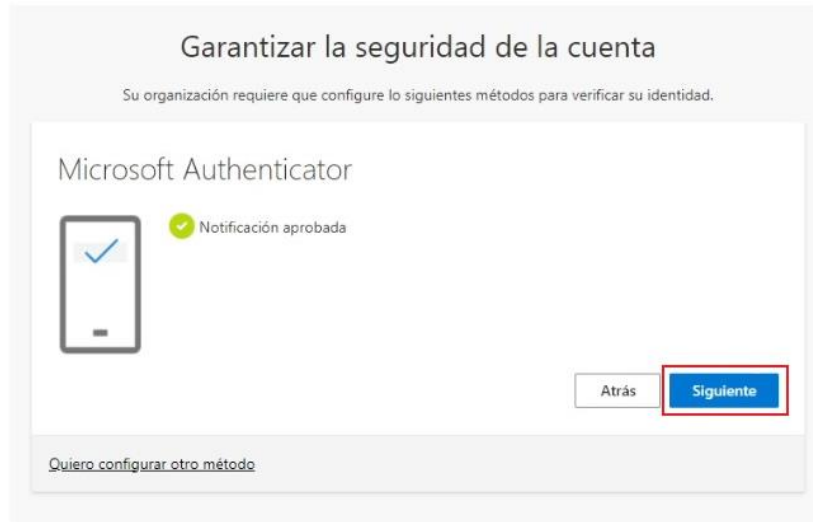
En su celular



Nota: En caso de que no logre ver el número de verificación en su celular, dar clic en “No puedo ver el número”.



Después de haber ingresado correctamente el número de verificación en la aplicación, aparecerá en pantalla que la notificación fue aprobada, a continuación, pulse el botón “Siguiente”.



Al concluir satisfactoriamente la configuración, dar clic en “Listo”, para continuar con el inicio de sesión.



En este punto ha quedado configurado el doble factor de autenticación. A partir de este momento, al digitar sus credenciales en alguno de los servicios de Microsoft 365, le pedirá aprobar la solicitud de inicio de sesión; por lo cual, debe abrir la aplicación de Microsoft Authenticator en su celular y escribir el número que se muestra para iniciar sesión.

Preguntas frecuentes

¿Cada cuánto me va a pedir el doble factor de autenticación?

La frecuencia de solicitud del código dependerá de cuál es la aplicación que esté usando.

Si inicia sesión desde un navegador, por ejemplo: Chrome o Edge (vía web):

Acceso por navegador con caché, cada 7 días.

Acceso por navegador sin caché (o en modo incógnito), cada que intente autenticarse.

Si inicia sesión desde una aplicación:

Cada 90 días, a menos que una actualización de la aplicación obligue a que se deba suministrar de nuevo las credenciales.

Ejemplos de inicios de sesión desde aplicaciones:

- Outlook (Windows, Android, Mac/iOS).
- Mac Mail.
- Aplicaciones de Office.
- Aplicación de Microsoft Teams (no versión web)
- Cliente OneDrive
- App de Flow para dispositivos móviles

En cualquier caso, si Microsoft detecta una situación de riesgo (por ejemplo, con múltiples intentos fallidos de inicio de sesión, inicios de sesión desde lugares diferentes al habitual), podrá solicitar el código de doble factor de autenticación. De igual manera, si se cierra sesión en cualquier caso y se vuelve a iniciar, también solicitará el código.

Si cambio mi contraseña de usuario único, ¿vuelve a pedir el doble factor? Sí, ya que para Microsoft el cambio de contraseña obliga a un cierre de las sesiones activas. Por ende, en el próximo inicio de sesión, solicitará el código generado por la aplicación de Microsoft Authenticator.

¿Qué hago si pierdo mi dispositivo móvil?

Debes contactar de inmediato a Soporte Syri a los teléfonos +57 (602) 5552334 extensión 4200 o acudir al punto de atención en el primer piso del edificio C, para que se revoque el permiso de acceso del equipo perdido y se pueda realizar de nuevo el proceso de configuración del doble factor con un nuevo dispositivo móvil.