UNIVERSIDAD DISTRITAL
FRANCISCO JOSÉ DE CALDAS

INSTRUCTIVO PARA LA CONFIGURACIÓN DE MFA (AUTENTICACIÓN MULTIFACTOR) EN CUENTAS INSTITUCIONALES DE MICROSOFT®

SIGUD Sistema Integrado de Gestión

PROGRAMA RED UDNET

TABLA DE CONTENIDO

Tabla de ilustraciones

INSTRUCTIVO PARA LA CONFIGURACIÓN DE MFA (AUTENTICACIÓN MULTIFACTOR) EN CUENTAS INSTITUCIONALES DE MICROSOFT®

1. OBJETIVO

Definir el procedimiento para la configuración y consulta de la Autenticación Multifactor (MFA) en cuentas institucionales de Microsoft® pertenecientes a la Universidad Distrital Francisco Jose de Caldas, garantizando un acceso seguro a los servicios institucionales alojados en la plataforma colaborativa.

2. ALCANCE

Este instructivo está dirigido a todos los usuarios que cuentan con una cuenta institucional de Microsoft® 365 bajo el dominio udistrital.edu.co y que requieren acceder a los servicios institucionales alojados en la plataforma colaborativa.

Asimismo, tiene como propósito orientar a los usuarios en la configuración inicial, consulta del estado de registro de MFA, la configuración de nuevos métodos de autenticación y la actualización de los ya existentes. De esta manera, se busca fortalecer la seguridad en el acceso a los recursos institucionales y promover el uso adecuado de los mecanismos de verificación de identidad establecidos por la Universidad.

3. DEFINICION

Este instructivo aplica a todos los funcionarios, contratistas de prestación de servicios, docentes, estudiantes, egresados, pensionados, dependencias, proyectos curriculares, grupos académicos y de extensión, y, en general, a todas las personas que hagan uso de los servicios de correo electrónico institucional.

4. PREREQUISITOS

Antes de realizar la configuración o consulta de la Autenticación Multifactor (MFA) en su cuenta institucional de Microsoft®, el usuario deberá cumplir con los siguientes requisitos:

- Disponer de una cuenta institucional activa de Microsoft® 365 con dominio udistrital.edu.co.
- Conocer las credenciales de acceso de la cuenta institucional (usuario y contraseña).
- Disponer de un teléfono inteligente con sistema operativo Android o iOS para la instalación y configuración de la aplicación Microsoft Authenticator, cuando este sea el método de autenticación definido.
- Tener acceso al número de teléfono o dirección de correo electrónico registrados como métodos de recuperación o verificación de la cuenta.
- No presentar bloqueos, restricciones o condiciones que impidan el acceso a la cuenta institucional, tales como bloqueos de seguridad, exceso en la cuota de almacenamiento asignada o periodos prolongados de inactividad
- En caso de cambio, pérdida o actualización del dispositivo utilizado para la autenticación,

contar con acceso a un método de autenticación previamente registrado o solicitar el restablecimiento correspondiente a la Unidad Red UDNET.

5. RESPONSABLES

5.1. Usuario Final

- Mantener actualizada la información de autenticación asociada a su cuenta institucional, sea número de teléfono, correo electrónico o por la aplicación de autenticación de Microsoft (Microsoft Authenticator App).
- Configurar los métodos de Autenticación Multifactor (MFA) siguiendo el procedimiento establecido en este instructivo.
- Resguardar el dispositivo móvil o método de autenticación utilizado para la validación de identidad.
- Reportar oportunamente al Programa Red UDNET información cualquier inconveniente relacionado con el acceso, pérdida, cambio o reemplazo del dispositivo registrado para MFA.

6. PROCEDIMIENTO CONFIGURACIÓN DE METODOS DE INICIO DE SESIÓN POR PRIMERA VEZ

- Al iniciar sesión por primera vez con la cuenta institucional de Microsoft bajo el dominio udistrital.edu.co, asignada por el Programa Red UDNET, el sistema solicitará la configuración de un método de autenticación para proteger el acceso a la cuenta.

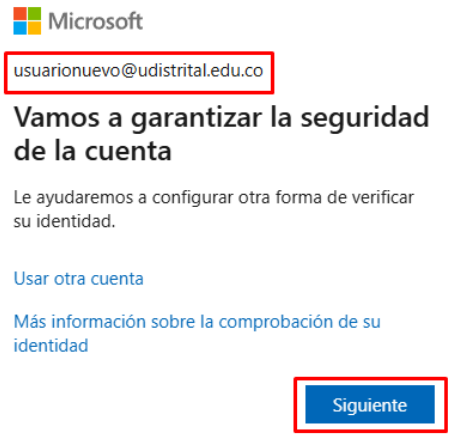

Ilustración 1. Aviso de configuración de seguridad en Microsoft

- Al hacer clic en Siguiente, Microsoft recomendará la instalación de la aplicación Microsoft Authenticator, dado que este es el método de autenticación principal definido por la Universidad para el acceso a los servicios institucionales.

Ilustración 2. Instalar Microsoft Authenticator

- En caso de no contar con la posibilidad de instalar la aplicación Microsoft Authenticator en un dispositivo móvil, podrá seleccionar la opción "**Otras opciones**" para configurar un método alternativo de autenticación.

Ilustración 3. Instalar Microsoft Authenticator - Otras opciones

- Se desplegará la ventana **"Agregar un método de inicio de sesión"**, en la cual podrá seleccionar uno de los siguientes mecanismos de autenticación:

    - **Microsoft Authenticator (Recomendado):** Aplicación móvil que permite aprobar solicitudes de inicio de sesión mediante notificaciones o códigos de verificación de

un solo uso. Es el método más seguro y recomendado para validar la identidad del usuario.

- **Teléfono:** Permite recibir códigos de verificación mediante mensaje de texto (SMS) o llamada telefónica al número registrado.
- **Correo electrónico:** Método utilizado principalmente para procesos de recuperación y restablecimiento de contraseña. No se recomienda como mecanismo principal de autenticación multifactor.

Nota:
Para las cuentas institucionales de Microsoft, se recomienda seleccionar Microsoft Authenticator, ya que proporciona un mayor nivel de seguridad y permite aprobar las solicitudes de acceso de forma rápida y sencilla desde un dispositivo móvil.

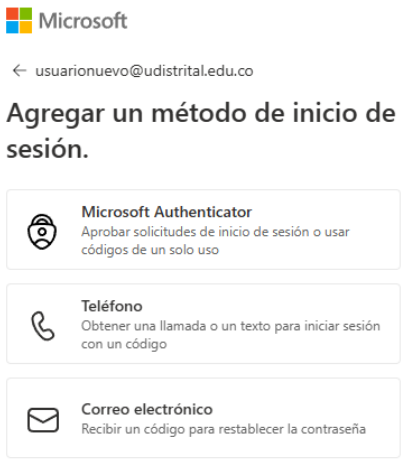

Ilustración 4. Agregar un método de inicio de sesión

- Para efectos de este instructivo, se seleccionará la opción "**Microsoft Authenticator"**. Al continuar, el sistema mostrará un código QR que deberá ser escaneado desde la aplicación previamente instalada en el dispositivo móvil.

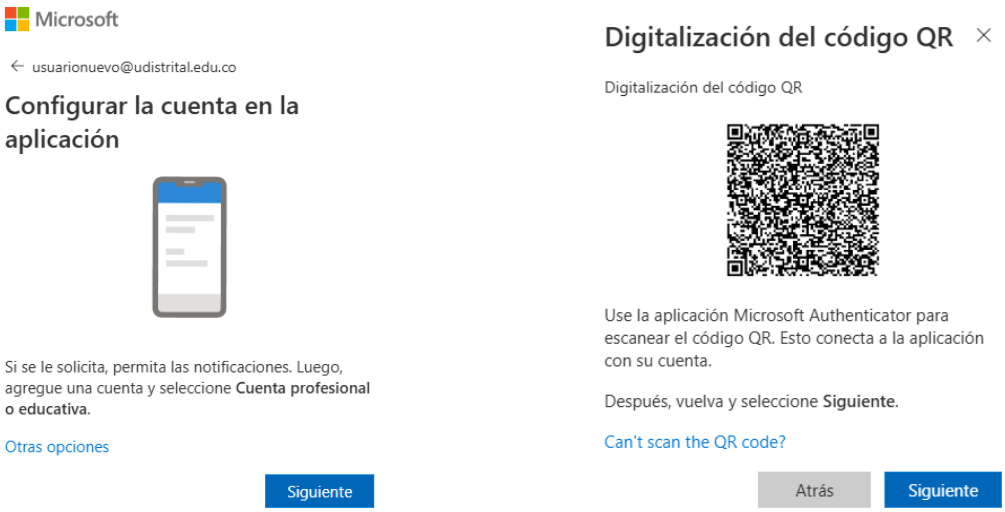

Ilustración 5. Escaneo código QR

- Una vez escaneado el código QR y vinculada correctamente la cuenta institucional con la aplicación, Microsoft solicitará la validación del registro mediante la introducción de un número mostrado en pantalla dentro de la aplicación Microsoft Authenticator.

Ilustración 6. Prueba de funcionamiento

- Si el proceso se realiza correctamente, el método de autenticación quedará registrado y asociado a la cuenta institucional, permitiendo completar los futuros inicios de sesión mediante autenticación multifactor.

Ilustración 7. Vinculación exitosa

7. PROCEDIMIENTO CONFIGURACIÓN DE UN NUEVO REGISTRO MFA

Este procedimiento permite al usuario agregar un nuevo método de Autenticación Multifactor (MFA) en su cuenta institucional de Microsoft® 365, con el fin de habilitar un segundo factor de verificación que refuerce la seguridad en el acceso a los servicios institucionales.

7.1 Agregar Microsoft Authenticator

- Ingrese a la información de seguridad desde el portal de seguridad de Microsoft mediante la dirección proporcionada por la Universidad - https://mysignins.microsoft.com/security-info
- Haga clic en la opción “Agregar método de inicio de sesión”.

Ilustración 8. Agregar método de inicio de sesión

- Se desplegará la ventana **"Agregar un método de inicio de sesión"**, en la cual podrá seleccionar el mecanismo que utilizará para la autenticación multifactor (MFA). Las opciones disponibles son las siguientes:

  - **Microsoft Authenticator (Recomendado):** Aplicación móvil que permite aprobar solicitudes de inicio de sesión mediante notificaciones o códigos de verificación de un solo uso. Es el método más seguro y recomendado para validar la identidad del usuario.
  - **Token de hardware:** Dispositivo físico que genera códigos de seguridad temporales. Durante el inicio de sesión, el usuario deberá ingresar el código mostrado en el dispositivo para completar la autenticación.
  - **Teléfono:** Permite recibir códigos de verificación mediante mensaje de texto (SMS) o llamada telefónica al número registrado.
  - **Teléfono alternativo:** Permite registrar un número telefónico adicional como mecanismo de respaldo para la autenticación.
  - **Teléfono del trabajo:** Permite recibir llamadas de verificación en el número telefónico institucional o laboral registrado.
  - **Correo electrónico:** Método utilizado principalmente para procesos de recuperación y restablecimiento de contraseña. No se recomienda como mecanismo principal para la autenticación multifactor.

Nota:
Para las cuentas institucionales de Microsoft, se recomienda seleccionar Microsoft Authenticator, ya que ofrece un mayor nivel de seguridad y permite aprobar las solicitudes de acceso de manera rápida y sencilla desde un dispositivo móvil.

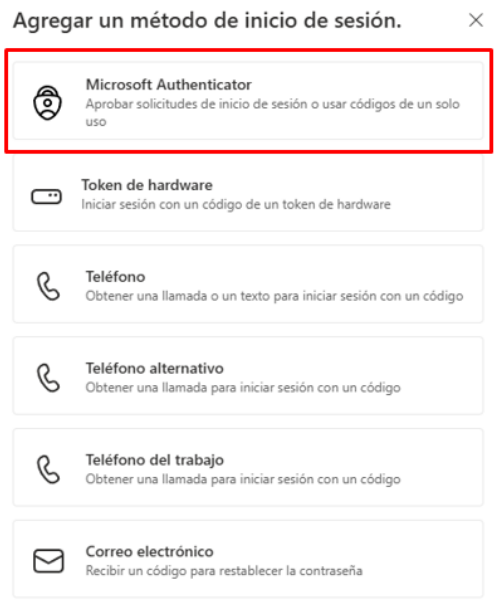

Ilustración 9. Agregar método de inicio de sesión – Microsoft Authenticator

- Al seleccionar “Microsoft Authenticator” el sistema le mostrará el nombre de la aplicación y las tiendas oficiales de donde se puede descargar la aplicación en caso de no tenerla.

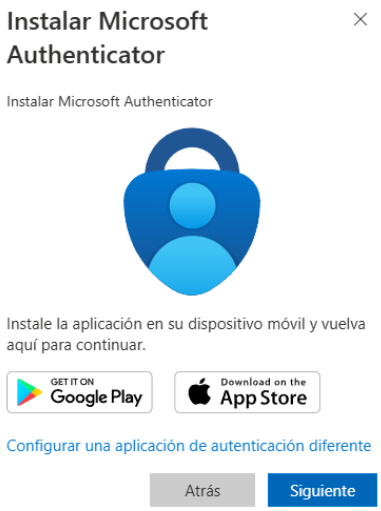

Ilustración 10. Instalar Microsoft Authenticator al agregar un nuevo método de sesión

- El siguiente paso es “Digitalización del código QR”, en donde debe abrir la aplicación “Microsoft Authenticator” y escanear el QR que le aparecerá en pantalla

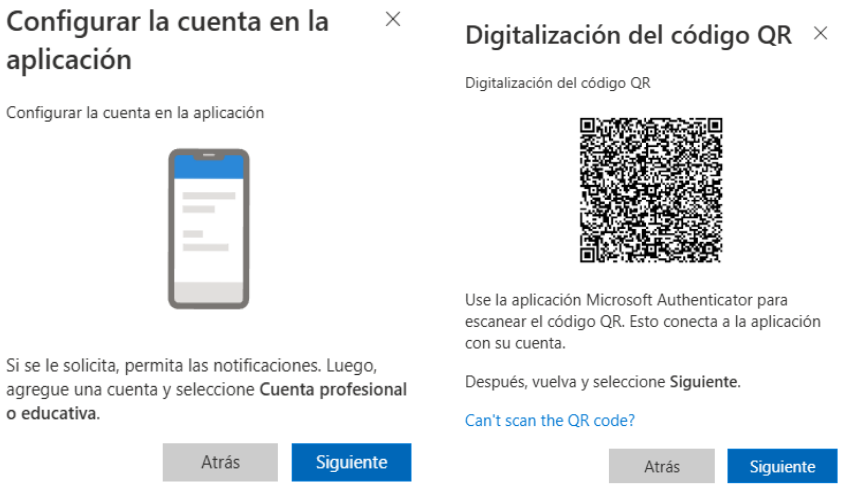

Ilustración 11. Escaneo código QR en agregar un nuevo método de sesión

- Una vez escaneado el código QR en la aplicación móvil, debe dar clic en “Siguiente” y escribir el número que le aparece en la pantalla titulada “Vamos a probarlo”.

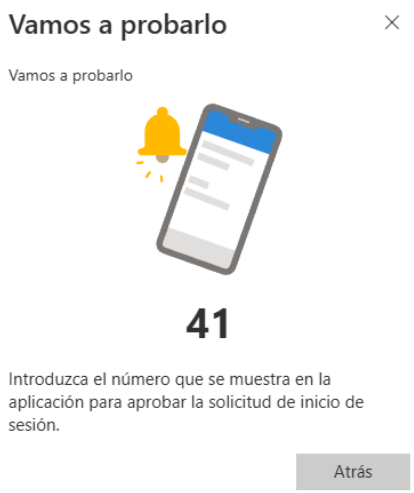

Ilustración 12. Prueba de funcionamiento al agregar un nuevo método de sesión

- Si la vinculación es correcta se agregará el método escogido.

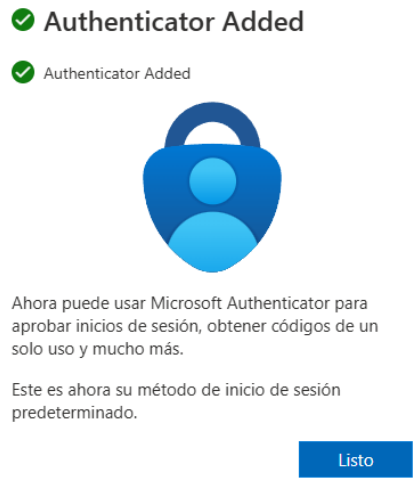

Ilustración 13.Vinculación exitosa al agregar un nuevo método de sesión

- Finalmente puede validar si el método de inicio de sesión fue agregado en la pantalla de "Información de seguridad". Para este caso se tiene acceso a la cuenta institucional desde dos dispositivos móviles diferentes.

  Nota: Este método es especialmente útil cuando dos o más personas requieren acceso a la misma cuenta de correo electrónico. Además, permite registrar múltiples métodos de autenticación multifactor (MFA), facilitando la recuperación y el acceso seguro a la cuenta.

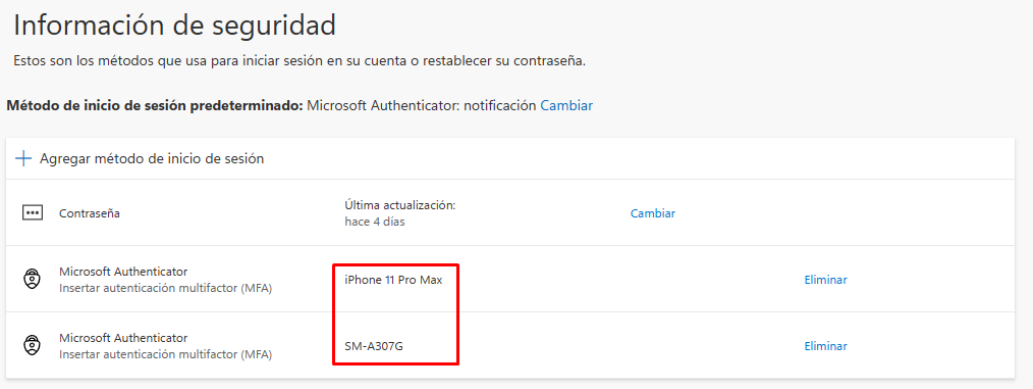

Ilustración 14. Validación de información tras agregar nuevo método de inicio de sesión

7.2 Agregar número de teléfono nuevo

- Ingrese a la información de seguridad desde el portal de seguridad de Microsoft mediante la dirección proporcionada por la Universidad - https://mysignins.microsoft.com/security-info
- Haga clic en la opción “Agregar método de inicio de sesión”.

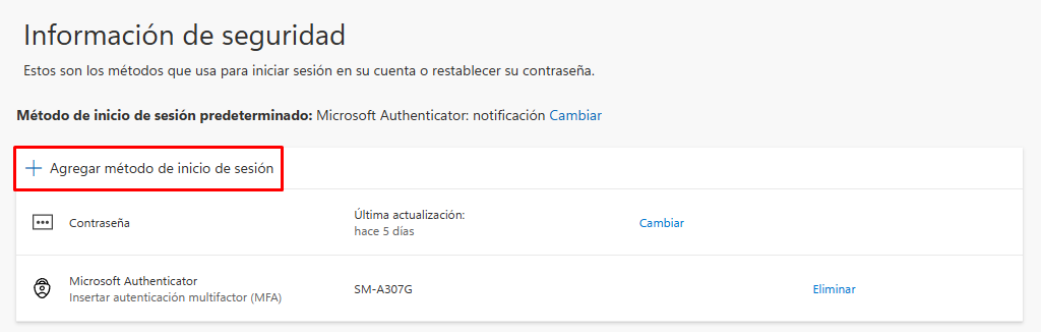

Ilustración 15. Agregar un método de inicio de sesión – Teléfono

- Se desplegará la ventana **“Agregar un método de inicio de sesión”**, en la cual podrá seleccionar el mecanismo que utilizará para la autenticación multifactor (MFA). En este caso es “Teléfono, Teléfono alternativo o Teléfono del trabajo”.

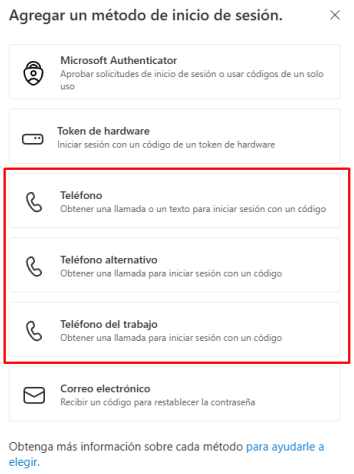

Ilustración 16. Agregar método de inicio de sesión – Teléfono

- Al seleccionar "Teléfono, Teléfono alternativo o Teléfono del trabajo" el sistema le mostrará el formulario para agregar el nuevo número de teléfono. En donde debe diligenciar por completo los siguientes datos:

    - **Código de país:** debe seleccionar Colombia o en su defecto el país en donde se encuentre.
    - **Phone number o Número de teléfono:** debe ingresar el número de teléfono.
    - **Elegir como comprobar:** debe seleccionar una de las opciones "Envió de un código por mensaje de texto" o "Llamada".

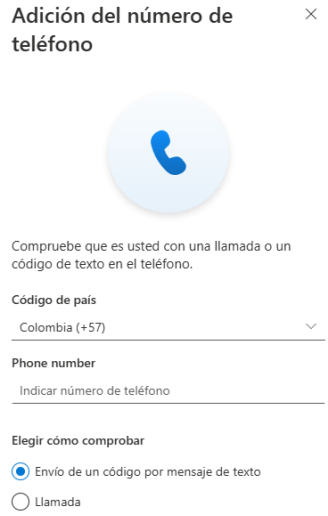

Ilustración 17. Adición del número de teléfono

- Al ingresar el código enviado por Microsoft o contestar la llamada, el sistema agregara el número de teléfono.

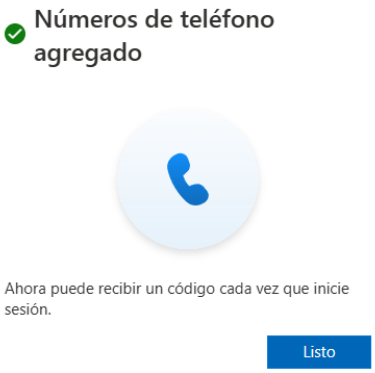

Ilustración 18. Número de teléfono agregado

- Finalmente puede verificar el número agregado en la pantalla de Información de seguridad.

Ilustración 19. Número de teléfono nuevo agregado

7.3 Agregar correo electrónico nuevo

- Ingrese a la información de seguridad desde el portal de seguridad de Microsoft mediante la dirección proporcionada por la Universidad - https://mysignins.microsoft.com/security-info
- Haga clic en la opción “Agregar método de inicio de sesión”.

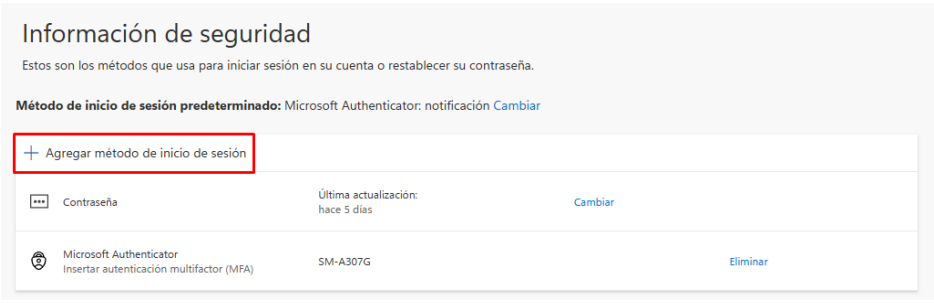

Ilustración 20. Agregar un método de inicio de sesión – Correo electrónico

- Se desplegará la ventana **"Agregar un método de inicio de sesión"**, en la cual podrá seleccionar el mecanismo que utilizará para la autenticación multifactor (MFA). En este caso es "Correo electrónico".

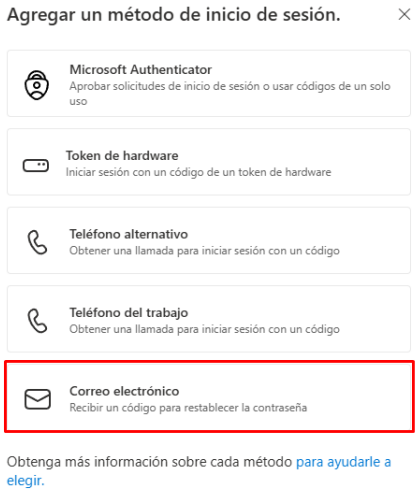

Ilustración 21. Agregar método de inicio de sesión – Correo electrónico

- Al seleccionar "Correo electrónico" el sistema le mostrará el formulario para agregar el nuevo correo electrónico.

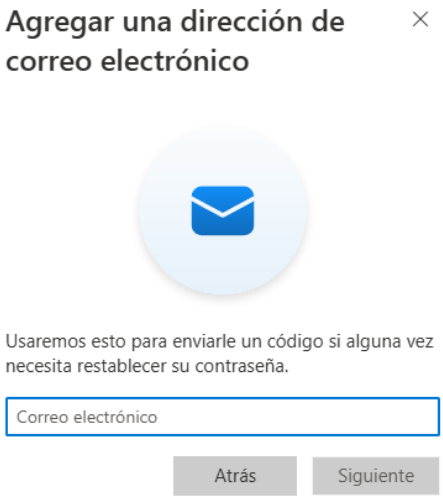

Ilustración 22. Agregar una dirección de correo electrónico

- Al ingresar el código enviado por Microsoft a su correo.

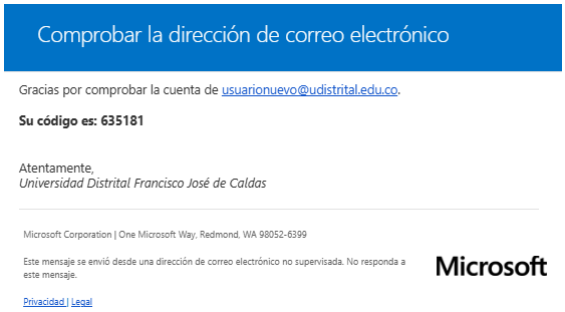

Ilustración 23. Código de verificación en correo electronico

- Si el código que se ingreso es correcto, se agregara a su información de seguridad.

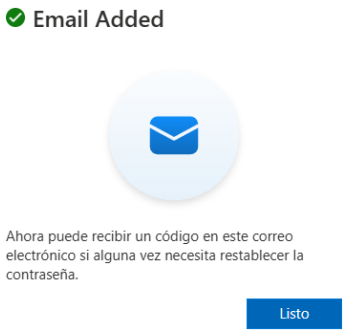

Ilustración 24. Número de teléfono agregado

- Finalmente puede verificar el número agregado en la pantalla de Información de seguridad.

Ilustración 25. Correo electrónico nuevo agregado

8. PROCESIMIENTO DE ACTUALIZACIÓN O CAMBIO DE REGISTRO MFA

Este procedimiento aplica cuando el usuario requiere actualizar, reemplazar o recuperar los métodos de Autenticación Multifactor (MFA) asociados a su cuenta institucional de Microsoft® 365.

8.1 Cambio de teléfono móvil, correo electrónico o la aplicación de Microsoft Authenticator

8.2 Pérdida, daño o reemplazo del dispositivo

Si el usuario pierde el dispositivo móvil, este presenta fallas o ha sido reemplazado y no cuenta con acceso a ningún método de autenticación registrado, no podrá completar el proceso de inicio de sesión.

- En este caso, deberá solicitar el restablecimiento de los métodos MFA al Programa Red UDNET mediante los canales oficiales de atención, sea por teléfono, correo electrónico o por medio de la plataforma IRIS. En donde el Programa Red UDNET restablecerá por completo todos los métodos registrados por el usuario.
- Una vez efectuado el restablecimiento, el usuario deberá registrar nuevamente sus métodos de autenticación siguiendo el procedimiento descrito en el **ítem 6** de este instructivo.

8.3 Actualización de número telefónico o correo electrónico

Cuando se requiera modificar un número telefónico o dirección de correo electrónico registrados como método de autenticación, el usuario deberá acceder a la sección Información de seguridad.

- Seleccione el método que desea actualizar y realice los cambios correspondientes.
- Finalizada la actualización, se recomienda realizar una prueba de autenticación para verificar el correcto funcionamiento del método registrado.

9. PROCEDIMIENTO DE CONSULTA DE MFA

El siguiente procedimiento permite al usuario verificar el estado de los métodos de Autenticación Multifactor (MFA) asociados a su cuenta institucional de Microsoft® 365, así como consultar los dispositivos y mecanismos de autenticación registrados.

9.1 Acceso a la información de seguridad

- Inicie sesión con su cuenta institucional utilizando su usuario y contraseña.
- Ingrese al portal de seguridad de Microsoft mediante la dirección proporcionada por la Universidad - https://mysignins.microsoft.com/security-info o siguiendo los siguientes pasos:

    - Ubicarse en el menú de usuario ubicado en la esquina superior derecha de la pantalla, donde se visualizan las iniciales del usuario. Desde este menú, seleccione la opción **“Ver cuenta”** para acceder a la configuración y administración de la cuenta institucional.

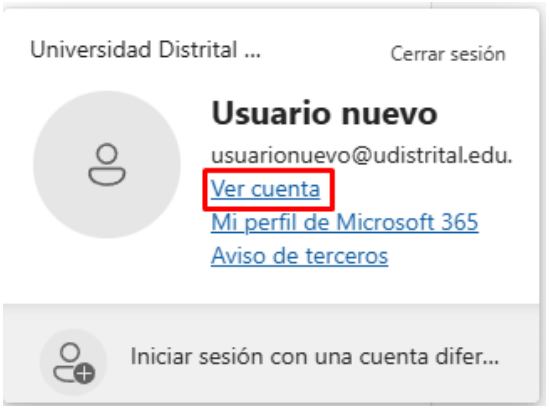

Ilustración 26. Ver cuenta de usuario

- Haga clic en la opción “Información de seguridad”, donde podrá visualizar todos los métodos de autenticación configurados en su cuenta.

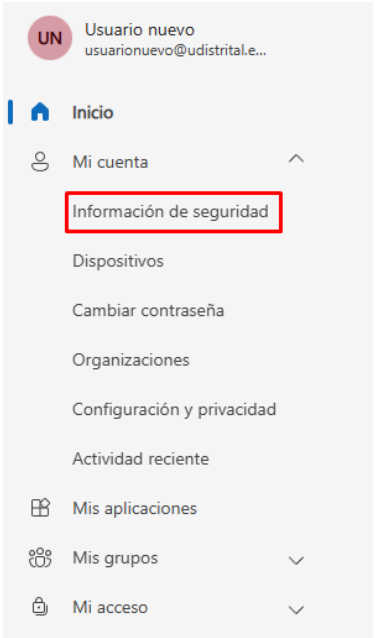

Ilustración 27. Menú lateral de información de usuario

- Finalmente, en este espacio podrá ver todos los métodos de autenticación configurados en su cuenta.

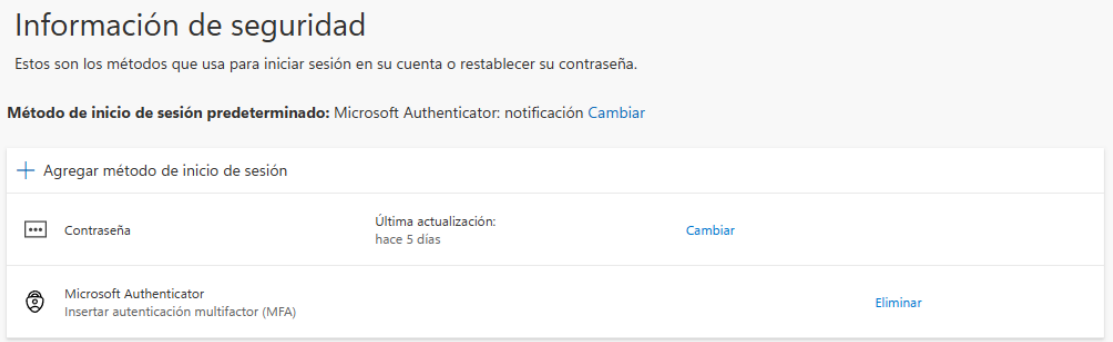

Ilustración 28. Información de seguridad

10. CONSIDERACIONES DE SEGURIDAD

Con el fin de proteger la información institucional y garantizar la seguridad de las cuentas de Microsoft® 365, los usuarios deberán tener en cuenta las siguientes recomendaciones:

- Mantener actualizados los métodos de Autenticación Multifactor (MFA) registrados en la cuenta institucional.
- Registrar, cuando sea posible, más de un método de autenticación (por ejemplo, Microsoft Authenticator y un número telefónico de respaldo), con el fin de facilitar la recuperación del acceso en caso de pérdida o cambio del dispositivo principal.
- No elimine un método de autenticación activo hasta verificar que el nuevo método se encuentre configurado y funcionando correctamente.
- No compartir con terceros los códigos de verificación, notificaciones de aprobación, números de validación ni ningún otro mecanismo utilizado para la autenticación multifactor.
- Aprobar únicamente las solicitudes de autenticación que hayan sido iniciadas directamente por usted. Si recibe una solicitud inesperada, deberá rechazarla inmediatamente y en caso de que sea recurrente reportar la situación al Programa Red UDNET.
- Proteger el dispositivo móvil utilizado para la autenticación mediante mecanismos de seguridad como contraseña, PIN, patrón de desbloqueo o autenticación biométrica.
- Mantener actualizada la aplicación Microsoft Authenticator y el sistema operativo del dispositivo móvil para garantizar el correcto funcionamiento de los mecanismos de seguridad.
- No instalar aplicaciones de autenticación provenientes de fuentes no oficiales. Se recomienda descargar Microsoft Authenticator únicamente desde las tiendas oficiales de Android o iOS.
- Informar oportunamente al Programa Red UDNET en caso de pérdida, robo, daño o reemplazo del dispositivo utilizado para la autenticación.
- Verificar periódicamente la información de seguridad registrada en la cuenta institucional para asegurar que los métodos de autenticación configurados sean correctos y se encuentren bajo el control del usuario.

11. GLOSARIO

- **Autenticación Multifactor (MFA):** Método de seguridad que requiere dos o más factores de verificación como una aplicación de autenticación, mensaje de texto, llamada telefónica o

llave de seguridad, para confirmar la identidad de un usuario antes de conceder acceso a una cuenta o servicio.

- **Registro MFA:** Proceso mediante el cual un usuario configura uno o más métodos de autenticación multifactor para su cuenta institucional.
- **Microsoft 365:** Plataforma de servicios en la nube de Microsoft que integra herramientas de productividad, colaboración, correo electrónico y almacenamiento de información.
- **Microsoft Authenticator:** Aplicación de autenticación desarrollada por Microsoft que permite aprobar solicitudes de inicio de sesión y generar códigos de verificación para la autenticación multifactor.
- **Cuenta Institucional:** Cuenta de usuario asignada por la institución con dominio udistrital.edu.co para el acceso a los servicios tecnológicos, aplicaciones y recursos corporativos o académicos.

12. CONTROL DE CAMBIOS

FECHA	VERSIÓN	DESCRIPCIÓN
23/06/2026	01	Se crea “Instructivo para la configuración de MFA (Autenticación Multifactor) en cuentas institucionales de Microsoft”
ELABORÓ	**REVISÓ**	**APROBÓ**
Santiago Lopez Gomez CPS Red de Datos 23/06/2026	Stefany Arias CPS UDNET y OATI 23/06/2026	Alejandro Paolo Daza Corredor Jefe Oficina Asesora de Tecnologías e Información 23/06/2026