1. Propósito y alcance

Este anexo describe los pasos generales para registrar, configurar y comprobar los tres métodos de autenticación aprobados por la Entidad: Microsoft Authenticator, Passkey (clave de paso) y Clave de paso con Authenticator. Las pantallas pueden variar según el dispositivo, la versión de la aplicación y la configuración institucional de Microsoft Entra ID.

Antes de iniciar el usuario debe contar con acceso a su cuenta institucional, un dispositivo compatible y conexión a internet. Realice el procedimiento únicamente desde las páginas y aplicaciones oficiales indicadas por la entidad. No comparta contraseñas, códigos de verificación ni solicitudes de aprobación con terceros.

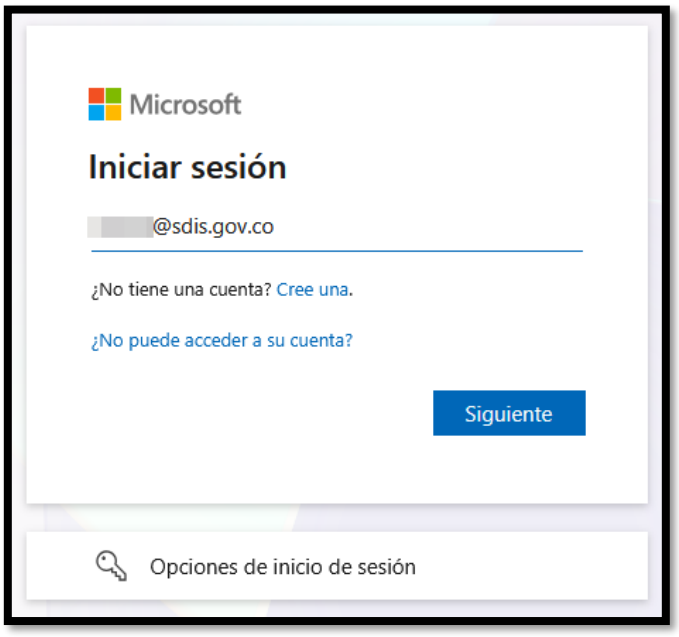
2. Métodos autorizados

Los métodos contemplados en este anexo son exclusivamente Microsoft Authenticator, Passkey (clave de paso) y Clave de paso con Authenticator. El SMS no se presenta como método autorizado en este documento. Si la pantalla ofrece SMS u otra opción no incluida en esta lista, no la seleccione y comuníquese con la Mesa de servicio.

2.1. Microsott Authenticator

Ingresar a la siguiente URL https://outlook.office.com/ con su cuenta de correo institucional y la contraseña asignada:

Imagen No. 01. Ingreso correo electrónico



Fuente: Microsoft.

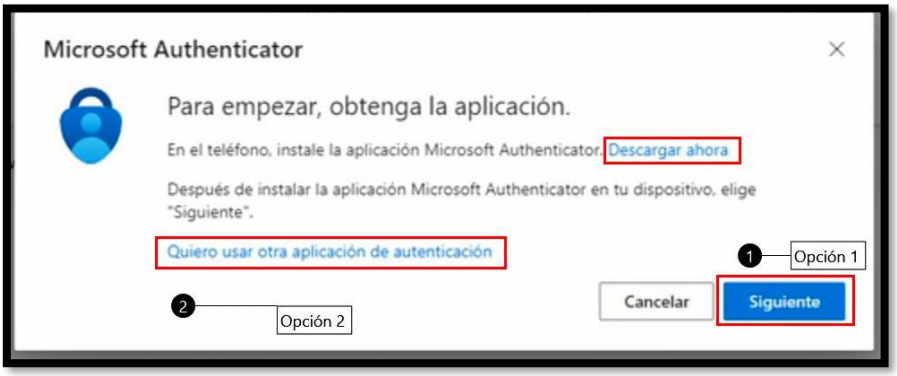
Imagen No. 02. Credenciales correo electrónico



Fuente: Microsoft.

Si aún no ha registrado un método de autenticación para su cuenta institucional, el sistema puede solicitar que configure *Microsoft Authenticator*. Siga las instrucciones que aparecen en pantalla. La disponibilidad de las opciones depende de la configuración habilitada por la entidad.

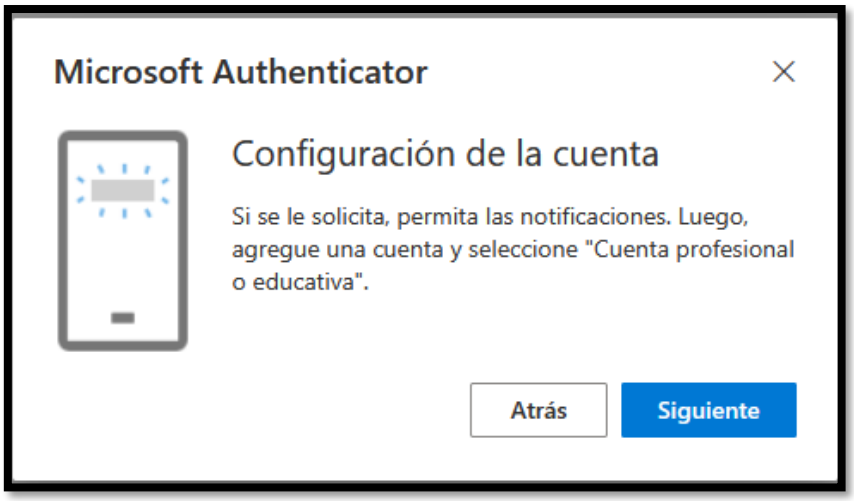
Imagen No. 03. Descarga y/o habilitación aplicación



Fuente: Microsoft.

- *Opción 1: "Siguiente"* para la instalación y configuración del Microsoft Authenticator en el dispositivo móvil.
- Si no es posible instalar o configurar Microsoft Authenticator, no seleccione SMS ni otro método no autorizado. Comuníquese con la Mesa de Servicio para recibir orientación y gestionar la situación conforme al procedimiento de soporte y recuperación de acceso.

Imagen No. 04. Descarga y/o habilitación aplicación



Fuente: Microsoft

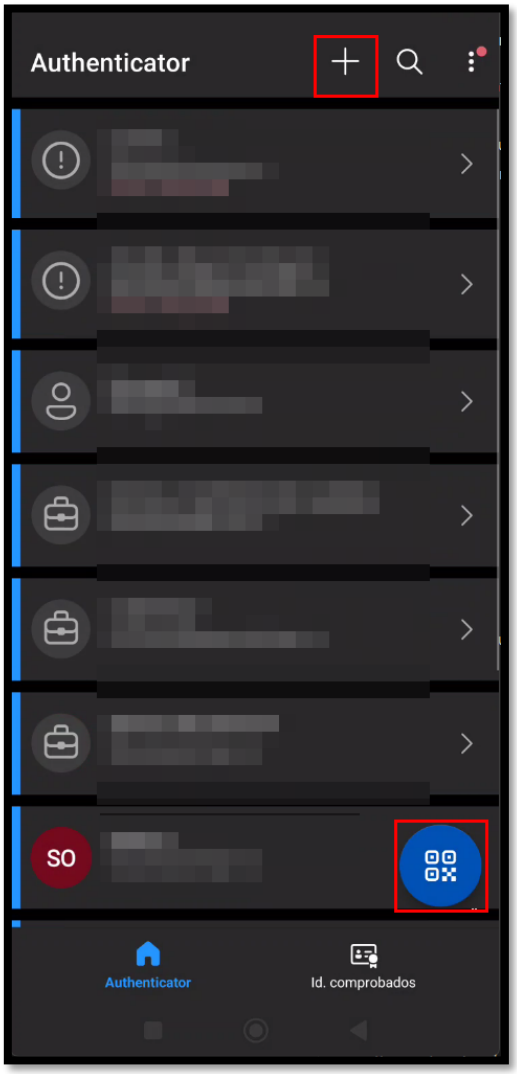
Imagen No. 05. Lectura código QR



Fuente: Microsoft.

Una vez descargada la aplicación Microsoft Authenticator a través de la Play Store o App Store, se procede a dar en la *Opción Siguiente*, en donde aparece la *Imagen No. 05*, para lo cual se debe abrir la aplicación Microsoft Authenticator previamente descargada para la lectura del Código QR, como se evidencia a continuación:

Imagen No. 06. Apertura de lectura código QR



Fuente. Imagen tomada de teléfono personal

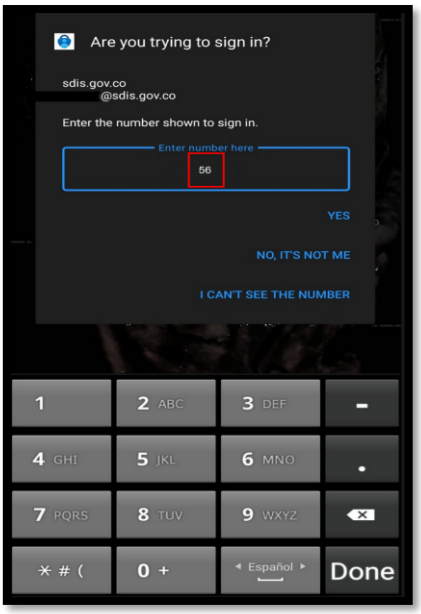
Una vez se esté dentro de la aplicación Microsoft Authenticator debe seleccionar en la parte inferior derecha como se muestra en la *Imagen No. 06*, el logo de *código QR*, en donde se da apertura a la cámara del teléfono para proceder a escanear el Código QR de la *Imagen No. 05,* en caso de que no aparezca, seleccionar el *Signo "+"* y escoger cuenta *Profesional o Educativa* y luego *Escanear Código QR.*

Imagen No. 07. Sincronización aplicación con teléfono personal



Fuente: Microsoft.

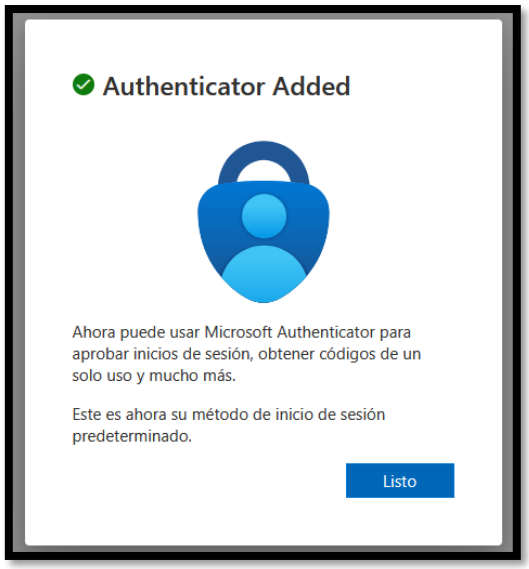
Imagen No. 08. Sincronización aplicación con teléfono personal - 2



Fuente. Imagen tomada de teléfono personal

Posterior a la lectura del código QR con el teléfono personal se *notifica un número aleatoriamente* el cual debe introducirse en el *teléfono personal* para poder sincronizar exitosamente la aplicación con el teléfono personal, una vez se confirme que dicho número son iguales queda sincronizado el teléfono y la aplicación para los inicios de sesión del correo electrónico.

Imagen No. 09. Finalización sincronización aplicación y teléfono



Fuente: Microsoft.

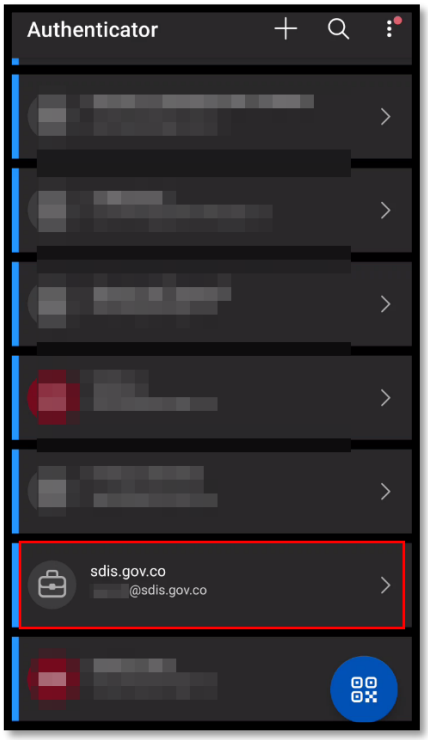
Como resultado del procedimiento de vinculación, se confirma que la aplicación Microsoft Authenticator se ha agregado correctamente y que el proceso de sincronización ha finalizado satisfactoriamente, tal como se evidencia en la *Imagen No. 9*. Este resultado permite disponer de un mecanismo de autenticación asociado al teléfono personal, mediante el cual el usuario podrá aprobar solicitudes de inicio de sesión y generar códigos de verificación de un solo uso, según las opciones habilitadas para su cuenta. La configuración de esta herramienta representa un avance importante en el fortalecimiento de la seguridad de la cuenta institucional, dado que permite complementar las credenciales de acceso con mecanismos adicionales de verificación de identidad. De esta manera, se reduce la dependencia exclusiva de las contraseñas y se dificulta que una persona no autorizada acceda a la cuenta únicamente mediante el conocimiento de dichas credenciales.

En conclusión, la finalización de la sincronización establece las condiciones necesarias para utilizar Microsoft Authenticator como parte del proceso de autenticación, favoreciendo un acceso más seguro y una mejor protección de la información institucional. Sin embargo, es importante tener presente que la seguridad del mecanismo también depende del uso responsable del dispositivo vinculado, de la revisión cuidadosa de las solicitudes de autenticación y de la aprobación exclusiva de aquellas que correspondan a intentos de acceso legítimos. Por consiguiente, la correcta configuración de esta herramienta, acompañada de buenas prácticas de seguridad digital, contribuye a mitigar los riesgos de acceso no autorizado y a fortalecer la protección de la identidad digital del usuario.

2.2. Passkey (Clave de paso)

Para crear una Passkey (clave de paso) mediante Microsoft Authenticator, una vez sincronizada la cuenta institucional, ingrese a la cuenta *SDIS.GOV.CO* en la aplicación y seleccione *"Crea una clave de paso"*, como se evidencia a continuación:

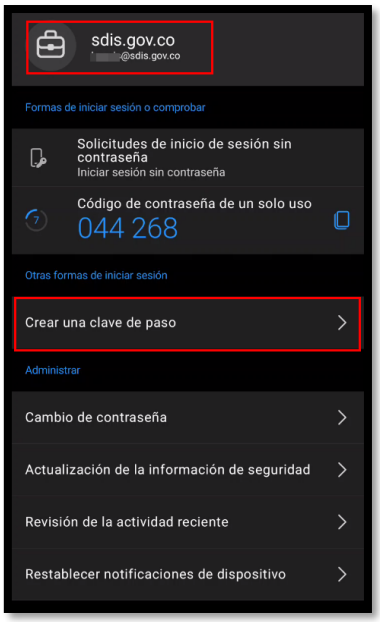
Imagen No. 10. Ingreso Authenticator SDIS.GOV.CO en Authenticator



Fuente. Imagen tomada de teléfono personal

Una vez ingresado a la opción SDIS:GOV:CO, seleccionamos *Crea una Clave de Paso* en donde se despliega una ventana *Imagen No. 11*, en donde se inicia sesión, aprobando dicho inicio con se visualiza en la *Imagen No. 12*, como se evidencia a continuación:

Imagen No. 11. Creación clave de paso Authenticator SDIS.GOV.CO.



Fuente. Imagen tomada de teléfono personal

Imagen No. 12. Inicio sesión para crear clave de paso



Fuente. Imagen tomada de teléfono personal

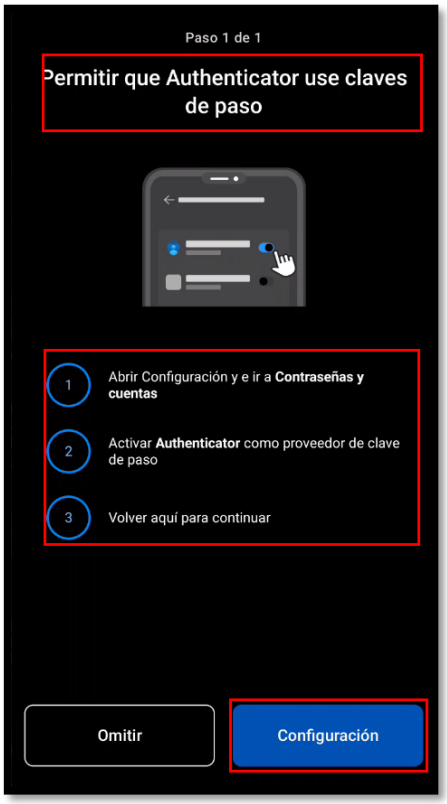
Imagen No. 13. Aprobación inicio de sesión clave de paso



Fuente. Imagen tomada de teléfono personal

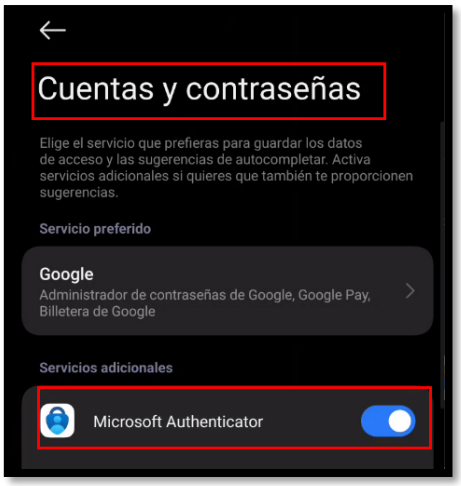
Posterior a la aprobación del inicio de sesión *Imagen No. 13*, se procede a permitir que el Authenticator use las claves de paso para poder iniciar sesión, *Imagen No. 14*, para lo cual, se debe habilitar en el apartado *cuentas y contraseñas* de la configuración del teléfono los *servicios adicionales* de Microsoft Authenticator, *Imagen No. 15*, como se evidencia a continuación:

Imagen No. 14. Permisos de claves de paso Authenticator



Fuente. Imagen tomada de teléfono personal

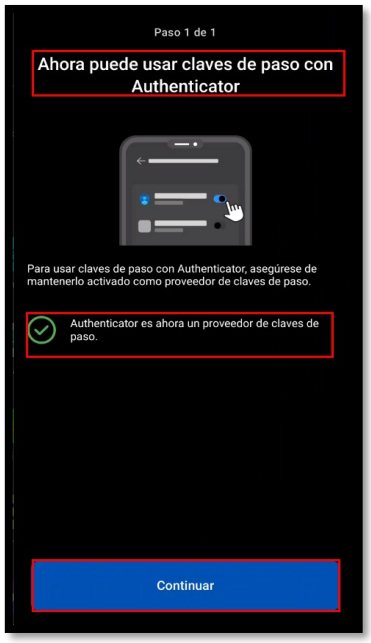
Imagen No. 15. Habilitación servicios adicionales Microsoft Authenticator



Fuente. Imagen tomada de teléfono personal

Una vez habilitado los servicios adicionales de la *Imagen No. 15*, queda configurado Microsoft Authenticator como proveedor de clave de paso *Imagen No. 16*, como se evidencia a continuación:

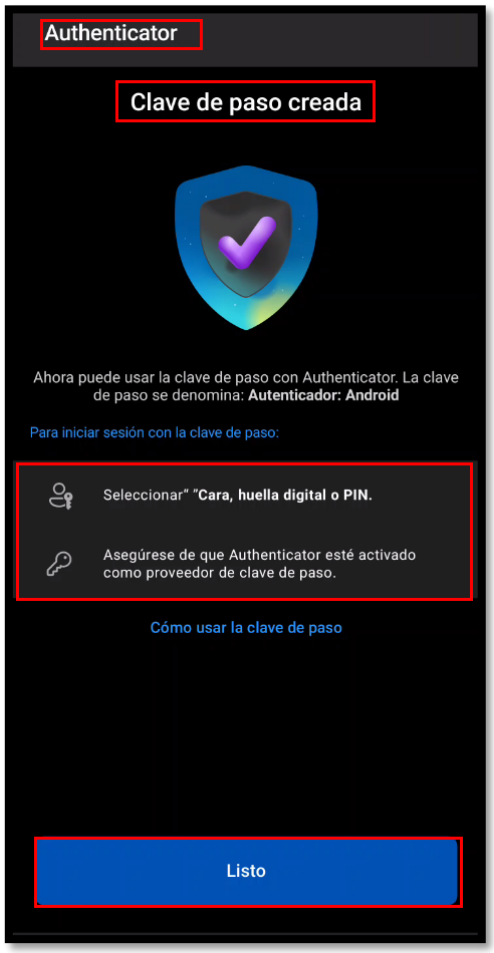
Imagen No. 16. Confirmación de Authenticator como proveedor de clave de paso



Fuente: Imagen tomada de teléfono personal

Posteriormente, al oprimir continuar, aparece la *Imagen No. 17*, en donde se confirma la creación de la clave de paso para la autenticación a través de la selección de los mecanismos disponibles es el teléfono celular, como se evidencia a continuación:

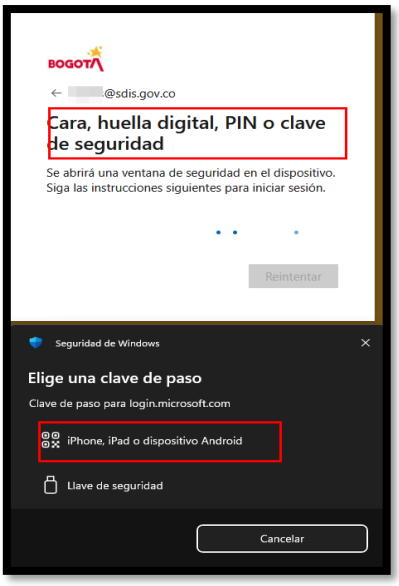
Imagen No. 17. Confirmación de creación de clave de paso



Fuente. Imagen tomada de teléfono personal

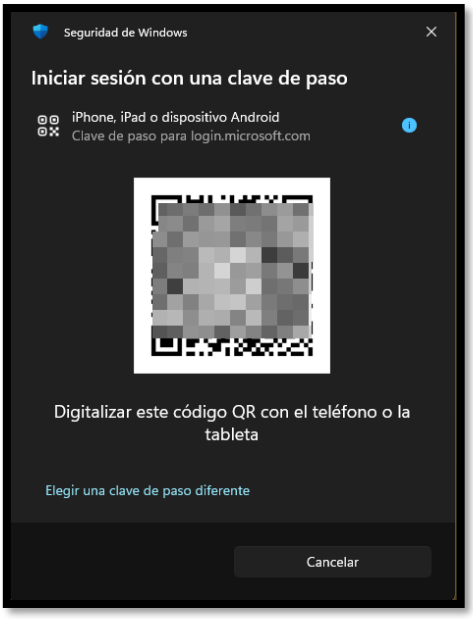
Una vez que se ha configurado la opción de clave de paso, cuando intente ingresar a la cuenta de correo electrónico aparece una ventana emergente solicitando la clave de paso que se ha generado, para lo cual, se selecciona la opción *iPhone, iPad o Dispositivo Android*, *Imagen No. 18*, donde una vez seleccionada aparece una ventana con *Código QR,* el cual debe escanear desde el teléfono celular activando el Bluetooth en los casos en los que se requiera realizar conexión desde otro dispositivo, siguiendo los pasos de la *Imagen No. 19*, como se evidencia a continuación:

Imagen No. 18. Ventana Emergente para Inicio de Sesión



Fuente. Imagen tomada de teléfono personal

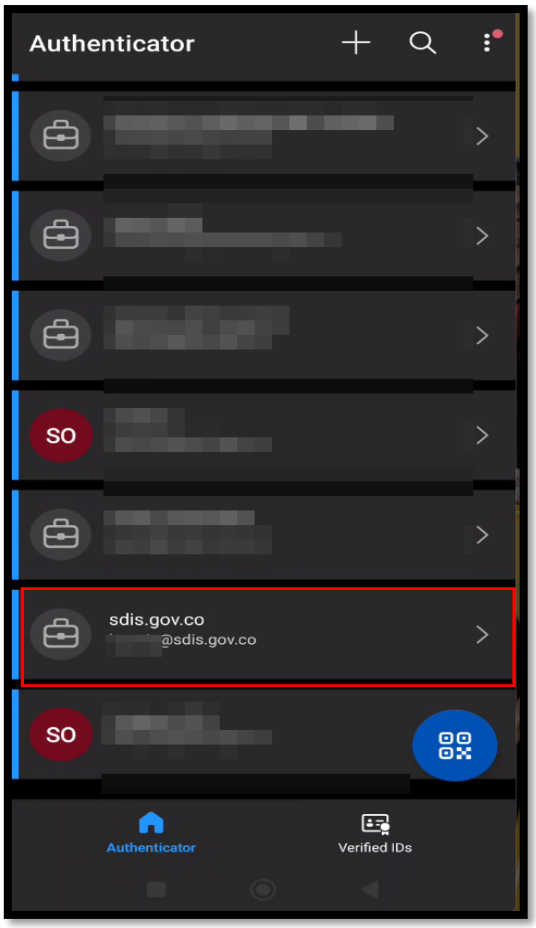
Imagen No. 19. Selección llave de paso Microsoft Authenticator



Fuente. Imagen tomada de teléfono personal

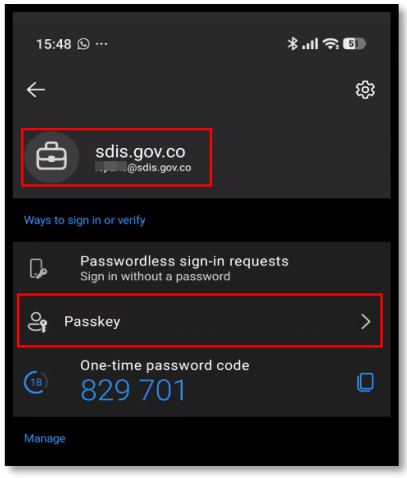
Dentro de la Aplicación Microsoft Authenticator, ingresa al apartado *SDIS.GOV.CO Imagen No. 20*, posteriormente ingrese a *clave de paso o Passkey*, *Imagen No. 21*, en donde una vez dentro, en la parte inferior derecha aparece el *símbolo de código de QRs*, *Imagen No. 22*, el cual seleccionamos, y se nos abrirá la cámara del teléfono celular y escaneamos el *Código QR* de la *Imagen No. 19*, como se evidencia a continuación:

Imagen No. 20. Escaneo código QR desde Microsoft Authenticator



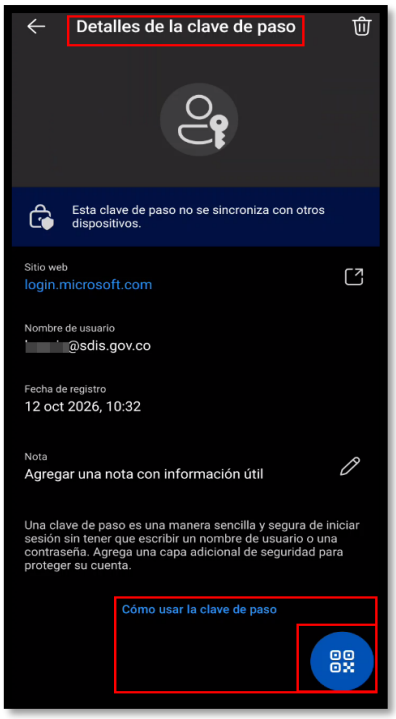
Fuente. Imagen tomada de teléfono personal

Imagen No. 21. Escaneo código QR desde Microsoft Authenticator



Fuente. Imagen tomada de teléfono personal

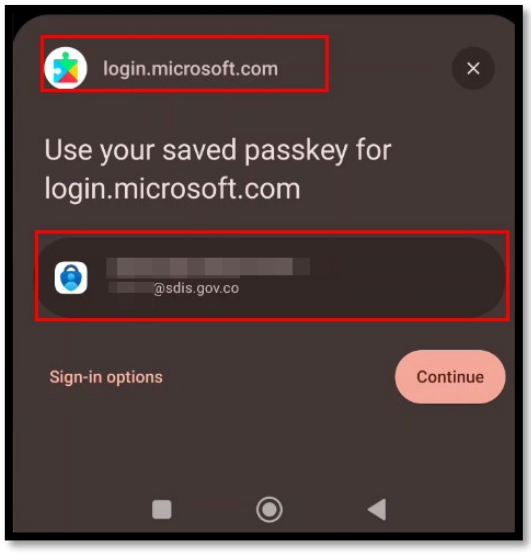
Imagen No. 22. Selección símbolo QR – clave de paso



Fuente. Imagen tomada de teléfono personal

Posteriormente al escaneo exitoso del Código QR, aparece en el teléfono celular una ventana emergente, *Imagen No. 23*. la cual muestra la *clave de paso* previamente creada en Microsoft Authenticator, en donde al seleccionarla, logra iniciar correctamente sesión del correo electrónico.

Imagen No. 23. Selección clave de paso creada para inicio de sesión



Fuente. Imagen tomada de teléfono personal

Una vez seleccionada la clave de paso creada previamente, se procede a completar el proceso de autenticación mediante la opción Continuar, con el fin de acceder al servicio de correo electrónico, permitiendo de esta manera, verificar la identidad del usuario utilizando la credencial previamente registrada, sin necesidad de introducir ni recordar una contraseña convencional.

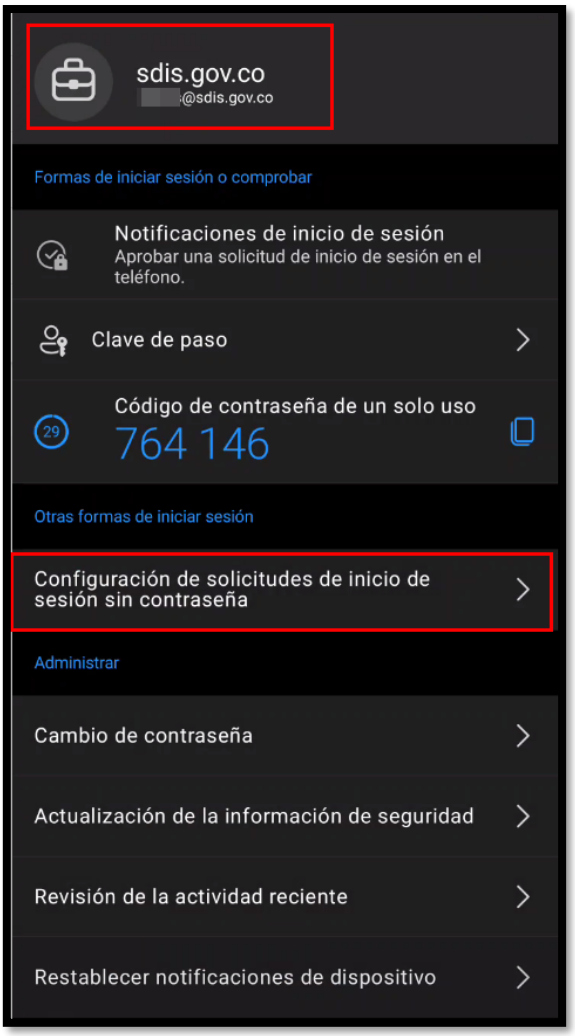
En este sentido, la implementación de este mecanismo de autenticación contribuye a mejorar la experiencia de acceso y a fortalecer la seguridad de la cuenta, al reducir la dependencia de las contraseñas tradicionales y la exposición a riesgos asociados con su reutilización, pérdida o divulgación. Asimismo, las claves de paso permiten una autenticación más sencilla y resistente a ataques de suplantación de identidad (phishing), siempre que se utilicen correctamente y se mantengan protegidos el dispositivo y los mecanismos de desbloqueo asociados.

En conclusión, la selección de la clave de paso constituye un paso fundamental para demostrar el funcionamiento del método de autenticación implementado y evidenciar sus ventajas en términos de seguridad, facilidad de uso y reducción de la dependencia de las contraseñas.

2.2.1. Clave de Paso con Authenticator

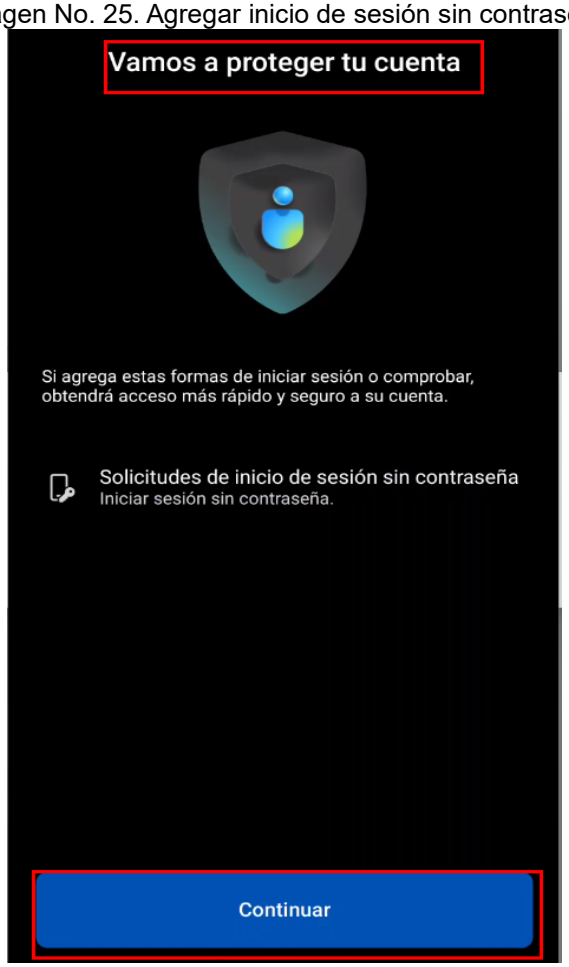
Para habilitar la opción de clave de paso con autenticación desde la aplicación Microsoft Authenticator una vez sincronizada la cuenta institucional, ingrese al Authenticator SDIS.GOV.CO, y seleccione Configuración de Solicitudes de inicio de sesión Sin contraseña, como se evidencia a continuación en la *Imagen No. 24:*

Imagen No. 24. Configuración Inicio de sesión sin contraseña aplicación



Fuente. Imagen tomada de teléfono personal

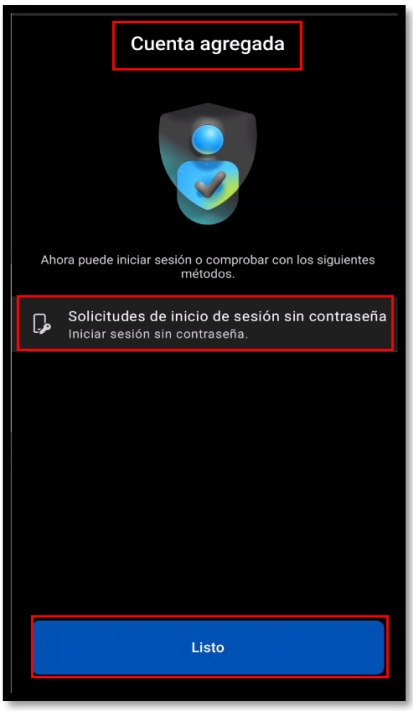
Imagen No. 25. Agregar inicio de sesión sin contraseña



Fuente. Imagen tomada de teléfono personal

Posteriormente, seleccione continuar, *Imagen No. 25*, en donde se despliega una ventana notificando que la *Configuración de inicio de sesión sin contraseña ha sido exitosa*, *Imagen No. 26.* Adicionalmente, cuando se realiza la prueba de inicio de sesión de correo electrónico, se muestra un código en el dispositivo con el que se inicia sesión, y que se debe digitar en el teléfono celular en la ventana emergente que aparece de la Aplicación Microsoft Authenticator, una vez se *confirme el número de aprobación*, se inicia sesión de manera exitosa de la cuenta institucional.

Imagen No. 26. Configuración finalizada



Fuente. Imagen tomada de teléfono personal

Imagen No. 27. Inicio de sesión exitoso



Fuente. Imagen tomada de teléfono personal

Como resultado del proceso de configuración, se evidencia la incorporación exitosa de la cuenta y la habilitación del mecanismo de autenticación sin contraseña, tal como se observa en la *Imagen No. 26.* Posteriormente, la *Imagen No. 27* muestra una solicitud de aprobación de inicio de sesión mediante la aplicación Microsoft Authenticator, en la que se presenta un código numérico que debe ser validado conforme al procedimiento de autenticación establecido.

Estas evidencias permiten documentar las etapas de configuración y verificación de la identidad, demostrando cómo la integración de mecanismos de autenticación modernos contribuye a fortalecer la protección de la cuenta institucional. En particular, el uso de claves de paso reduce la dependencia de las contraseñas tradicionales, mientras que la aprobación mediante una aplicación de autenticación incorpora una verificación adicional que ayuda a prevenir accesos no autorizados.

En términos de seguridad, este procedimiento representa una mejora frente a los métodos basados exclusivamente en contraseñas, debido a que combina facilidad de uso con mecanismos adicionales de protección de la identidad digital.

En conclusión, la implementación de estos mecanismos constituye un avance en el fortalecimiento de la seguridad del acceso al correo electrónico institucional, al promover métodos de autenticación más robustos y reducir los riesgos asociados con el uso indebido de credenciales. Su efectividad depende, además, de la protección de los dispositivos vinculados, la verificación de las solicitudes de acceso y la aprobación exclusiva de aquellas que hayan sido iniciadas legítimamente por el usuario.

3. Validación posterior a la configuración

Después de configurar cualquiera de los métodos, realice una prueba de inicio de sesión siguiendo las indicaciones del sistema. Confirme que el método aparece registrado en las opciones de seguridad de la cuenta y que el acceso se completa correctamente. Si la prueba falla, no repita aprobaciones que no haya iniciado; contacte a la Mesa de Servicio.

3.1. Pérdida, cambio o indisponibilidad del dispositivo

Si pierde el dispositivo, cambia de teléfono o no puede utilizar el método registrado, reporte la situación por los canales institucionales de soporte. La recuperación o el restablecimiento del acceso debe realizarse después de validar la identidad del usuario y por personal autorizado, dejando la trazabilidad correspondiente. No solicite ni acepte que se deshabilite permanentemente la autenticación multifactor como solución ordinaria.

4. Recomendaciones de Seguridad

- Apruebe únicamente las solicitudes de autenticación que usted haya iniciado.
- No comparta códigos, claves de paso, contraseñas ni capturas que contengan información de autenticación.
- Mantenga actualizado el sistema operativo y la aplicación Microsoft Authenticator.
- Reporte de inmediato solicitudes inesperadas, pérdida del dispositivo o indicios de acceso no autorizado.
- Use únicamente los métodos habilitados y autorizados por la entidad.