

MANUAL DE RESTABLECIMIENTO DE CONTRASEÑA Y MFA

Tabla de contenido

1.OBJETO	3
2.ALCANCE.....	3
3.PROCEDIMIENTO	3
4.RESTABLECIMIENTO DE CONTRASEÑA DE LA CUENTA INSTITUCIONAL.....	9

Tabla de imágenes

Ilustración 1 Configuración Microsoft Authenticator	4
Ilustración 2 Instalar Microsoft Authenticator	5
Ilustración 3 Configuración de la cuenta	5
Ilustración 4 Código QR	6
Ilustración 5 Método autenticación numero 1.....	7
Ilustración 6 Método autenticación numero 2.....	8
Ilustración 7 Método de autenticación aprobado.....	8
Ilustración 8 Datos institucionales.....	9
Ilustración 9 Paso de comprobación 1	10
Ilustración 10 Ingreso del código de verificación.....	10
Ilustración 11 Paso de comprobación 2	11
Ilustración 12 Validación del código de verificación	11
Ilustración 13 Registro de nueva contraseña.....	12
Ilustración 14 Restablecimiento exitoso de contraseña	12
Ilustración 15 Confirmación del restablecimiento de contraseña	13

1. OBJETO

Describir de forma clara, precisa y ordenada los pasos necesarios para realizar el cambio de contraseña de las cuentas institucionales mediante la página web de autoservicio, garantizando un proceso seguro, eficiente y alineado con los lineamientos establecidos por el Departamento de Tecnologías de la Información (DTI) de la Universidad Piloto de Colombia.

2. ALCANCE

Este procedimiento aplica a los estudiantes, docentes y personal administrativo de la Universidad Piloto de Colombia que requieran realizar el cambio o restablecimiento de la contraseña de sus cuentas institucionales mediante la página web de autoservicio. Comprende las actividades necesarias para acceder a la plataforma, verificar la identidad del usuario y establecer una nueva contraseña, garantizando un proceso seguro y conforme a los lineamientos definidos por el Departamento de Tecnologías de la Información (DTI).

3. PROCEDIMIENTO

El cambio de contraseña de las cuentas institucionales se realizará a través de la página web de autoservicio, siguiendo un procedimiento estandarizado que garantice la seguridad de la información, la autenticidad del usuario y el correcto acceso a los servicios institucionales.

3.1 CONFIGURACIÓN DEL DOBLE FACTOR DE AUTENTICACIÓN

Abra el navegador web de su preferencia e ingrese a la dirección <https://aka.ms/mfasetup> Inicie sesión con su cuenta institucional. A continuación, se mostrará una ventana solicitando la configuración del doble factor de autenticación; seleccione la opción “Siguiente” para continuar con el proceso.



Ilustración 1 Configuración Microsoft Authenticator

3.2 Una vez seleccionada la opción “Siguiente”, deberá descargar la aplicación Microsoft Authenticator en su dispositivo móvil. Después de instalar el aplicativo, regrese al asistente de configuración del doble factor de autenticación y seleccione nuevamente la opción “Siguiente” para continuar con la vinculación de la aplicación Microsoft Authenticator.



Ilustración 2 Instalar Microsoft Authenticator

3.3 En la ventana “Configurar la cuenta en la aplicación”, seleccione la opción “Siguiente” para continuar con el proceso de configuración del doble factor de autenticación.



Ilustración 3 Configuración de la cuenta

3.4 Ingrese a la aplicación Microsoft Authenticator previamente instalada en su dispositivo móvil. Seleccione el ícono de código QR ubicado en la parte inferior de la aplicación para agregar una nueva cuenta. Posteriormente, escanee el código QR que se muestra en la pantalla de configuración del doble factor de autenticación. Una vez realizado el escaneo, la cuenta quedará vinculada automáticamente y el doble factor de autenticación quedará sincronizado con la aplicación Microsoft Authenticator.



Ilustración 4 Código QR

3.5 Después de seleccionar la opción “Siguiente”, se enviará una notificación a la aplicación Microsoft Authenticator en el dispositivo móvil. Abra la notificación y escriba el número que se muestra en la pantalla del equipo. Posteriormente, seleccione la opción “Sí” o “Aprobar” (según corresponda) y, si el dispositivo lo solicita, auténtíquese mediante su contraseña, PIN o huella dactilar para autorizar el acceso a la cuenta.



Ilustración 5 Método autenticación numero 1

3.6 Una vez completada la autenticación, el sistema solicitará configurar un segundo método de verificación como respaldo para el acceso a la cuenta. Verifique que el código de país corresponda a Colombia (+57), ingrese su número de teléfono celular y seleccione el método de verificación de su preferencia (llamada telefónica o mensaje de texto). A continuación, seleccione "Siguiente". Si eligió la opción de llamada telefónica, recibirá una llamada automática en la que deberá presionar la tecla numeral (#) para confirmar la verificación y completar la configuración del segundo método de autenticación.

U2Piloto

jose-figueroa2@upc.edu.co

Adición del número de teléfono

Compruebe que es usted con una llamada o un código de texto en el teléfono.

Código de país
Colombia (+57)

Phone number
3217

Elegir cómo comprobar

☒ Envío de un código por mensaje de texto

☐ Llamada

Se pueden aplicar tarifas de datos y mensajes. Si presiona siguiente, acepta los [Términos del servicio](#) y la [Declaración de privacidad y cookies](#).

[Otras opciones](#)

[Omitir configuración](#)

Seguiente

Ilustración 6 Método autenticación numero 2

3.7 Una vez aprobada la verificación, el sistema mostrará una ventana indicando que el número de teléfono se agregó correctamente como método de autenticación de respaldo. Seleccione la opción “Listo” para finalizar el proceso de configuración del doble factor de autenticación (MFA) de su cuenta institucional.

U2Piloto

jose-figueroa2@upc.edu.co

Números de teléfono agregado

Ahora puede recibir un código cada vez que inicie sesión.

Listo

Ilustración 7 Método de autenticación aprobado

4. RESTABLECIMIENTO DE CONTRASEÑA DE LA CUENTA INSTITUCIONAL

Abra el navegador web de su preferencia e ingrese a la dirección <https://aka.ms/sspr> para acceder al portal de cambio o restablecimiento de contraseña. Posteriormente, registre su correo institucional, complete la verificación CAPTCHA y haga clic en “Siguiente” para continuar con el procedimiento.



The screenshot shows the 'U2 Piloto' account recovery interface. At the top, the logo 'U2 Piloto' is displayed with 'UNIVERSIDAD DE COLOMBIA' in smaller text. Below the logo, the heading 'Vuelva a su cuenta' is followed by the question '¿Quién es usted?'. A paragraph of instructions states: 'Para recuperar su cuenta, escriba su nombre de usuario o correo electrónico y los caracteres que encontrará en la imagen o el audio de abajo.' Below this, there is a text input field labeled 'Correo electrónico o nombre de usuario *' containing the text 'jose-figueroa2@upc.edu.co'. A note below the field provides an example: 'Ejemplo: usuario@contoso.onmicrosoft.com o usuario@contoso.com'. To the right of the input field is a CAPTCHA image showing the text 'YRAN PPW' in a stylized font. Below the CAPTCHA is another text input field containing 'YRANPPW'. A label below this field reads 'Escribe los caracteres de la imagen o los palabras del audio *'. At the bottom, there are two buttons: a blue 'Siguiente' button and a grey 'Cancelar' button.

Ilustración 8 Datos institucionales

4.1 Una vez seleccionada la opción “Siguiente”, deberá escoger uno de los métodos de verificación configurados previamente para autorizar el cambio de contraseña. Seleccione la opción “Enviar mensaje de texto a mi teléfono móvil”, ingrese el número de celular registrado y seleccione la opción “Texto”.

U2 Piloto
UNIVERSIDAD DE COLOMBIA

Vuelva a su cuenta

paso de comprobación 1 > paso de comprobación 2 > elegir una contraseña nueva

Elija el primer método de contacto que debemos usar para la comprobación:

- ☒ Enviar mensaje de texto a mi teléfono móvil
- ☐ Llamar al teléfono móvil
- ☐ Aprobar la notificación en la aplicación de autenticación
- ☐ Introducir el código de la aplicación de autenticación

Para proteger su cuenta necesitamos que introduzca su número de teléfono móvil completo (*****09) a continuación. Recibirá un mensaje de texto con un código de verificación que se puede usar para restablecer la contraseña.

321

Texto

Ilustración 9 Paso de comprobación 1

4.2 Después de seleccionar la opción “Texto”, el sistema solicitará ingresar el código de verificación enviado mediante mensaje de texto al número registrado. Digite el código recibido y, finalmente, seleccione la opción “Siguiente” para continuar con el proceso de cambio de contraseña.

U2 Piloto
UNIVERSIDAD DE COLOMBIA

Vuelva a su cuenta

paso de comprobación 1 > paso de comprobación 2 > elegir una contraseña nueva

Elija el primer método de contacto que debemos usar para la comprobación:

- ☒ Enviar mensaje de texto a mi teléfono móvil
- ☐ Llamar al teléfono móvil
- ☐ Aprobar la notificación en la aplicación de autenticación
- ☐ Introducir el código de la aplicación de autenticación

Se ha enviado a su teléfono un mensaje de texto con un código de verificación.

988243

Siguiente

Intentelo de nuevo
Ponerse en contacto con el administrador

Ilustración 10 Ingreso del código de verificación

4.3 Como segundo método de comprobación, seleccione la opción “Aprobar la notificación en la aplicación de autenticación”. Posteriormente, seleccione “Enviar notificación” para recibir la solicitud de aprobación en la aplicación Microsoft Authenticator y continuar con el proceso de verificación.



Ilustración 11 Paso de comprobación 2

4.4 Después de seleccionar la opción “Enviar notificación”, recibirá una solicitud de aprobación en la aplicación Microsoft Authenticator. Ingrese el código que se muestra en la pantalla de configuración del cambio de contraseña y confirme la autenticación mediante su huella dactilar o PIN. Una vez validada la solicitud, el sistema lo redirigirá automáticamente a la pantalla para ingresar la nueva contraseña.



Ilustración 12 Validación del código de verificación

4.5 A continuación, ingrese y confirme la nueva contraseña que desea establecer para el acceso a las plataformas institucionales. Una vez validada la información, seleccione la opción “Finalizar” para completar el proceso. El cambio de contraseña se aplicará automáticamente a todas las plataformas institucionales.



Ilustración 13 Registro de nueva contraseña

4.6 Una vez seleccionada la opción “Finalizar”, se mostrará un mensaje de confirmación indicando que el restablecimiento de contraseña se realizó exitosamente.



Ilustración 14 Restablecimiento exitoso de contraseña

4.7 Por último, recibirá en su correo institucional una notificación confirmando que el restablecimiento de contraseña fue realizado exitosamente.

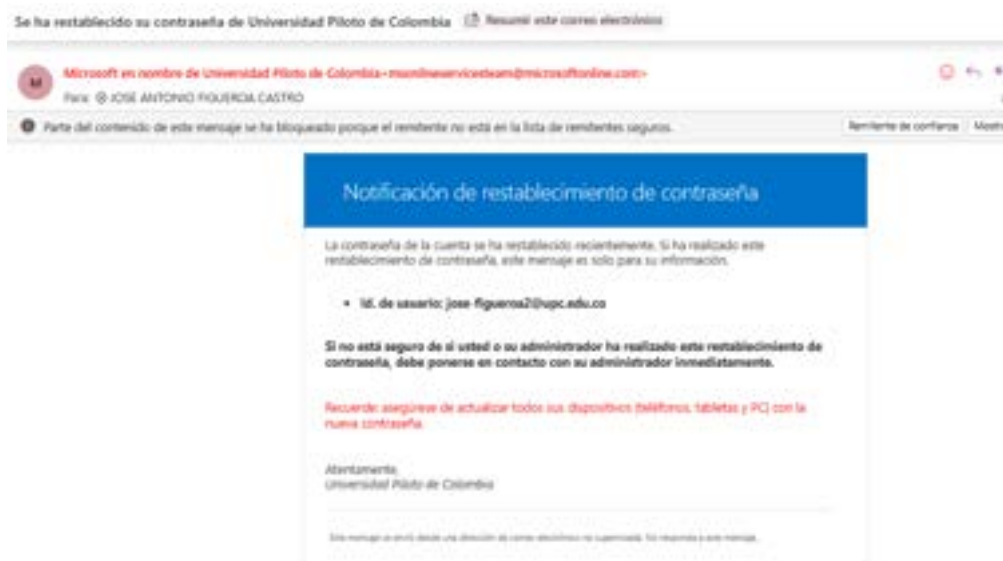


Ilustración 15 Confirmación del restablecimiento de contraseña

NOTA: En caso de cambio de número celular o si los métodos de autenticación configurados no se encuentran disponibles, deberá enviar una solicitud al Centro de Servicios de Tecnología – Citius al correo Citius@unipiloto.edu.co, solicitando el restablecimiento del doble factor de autenticación (MFA) para realizar nuevamente la configuración.

