



GPIT – PTI

# MANUAL DE CONFIGURACIÓN DOBLE FACTOR DE AUTENTICACIÓN DEL CORREO INSTITUCIONAL



UNAD  
GRUPO FUNCIONAL DE  
SEGURIDADINFORMATICA -  
GFSI  
13/03/2023

F-2-2-5  
3-05-02-2021



\*Aplica para las sedes José Celestino Mutis y José Acevedo y Gómez

## DOBLE FACTOR DE AUTENTICACIÓN

El **MFA (Multi-factor Authentication o Autenticación Multi-factorial)** proporciona una capa adicional de seguridad en la autenticación de usuarios en sistemas (AMAZON, s.f.). Mientras que los sistemas de autenticación tradicionales suelen requerir únicamente un nombre de usuario y una contraseña para acceder a una cuenta, la autenticación multifactorial añade una o más formas adicionales de autenticación, como por ejemplo una huella dactilar, una tarjeta de acceso o un token generado por una aplicación móvil, con el fin de verificar la identidad del usuario (MICROSOFT, 2023).

El objetivo de esta capa adicional de seguridad es proteger la cuenta de un usuario contra el acceso no autorizado y el robo de contraseñas. Si un usuario tiene una contraseña robusta y única, pero alguien más obtiene acceso a ella, no podrá acceder a la cuenta sin tener la información adicional requerida en el proceso de autenticación multifactorial. Por lo tanto, la implementación del MFA es una forma efectiva de mejorar la seguridad en la autenticación de usuarios y proteger la información confidencial (SALESFORCE, 2023).

## ALCANCE

El presente Manual tiene como finalidad informar y orientar a toda la plataforma humana de la UNAD sobre los cambios que será harán presente en los procesos de autenticación y acceso al correo institucional tras la implementación del doble factor de autenticación – MFA, el cual tiene como fin brindar mayores niveles de seguridad a la plataforma de correo y la información allí contenida.



Figura 1. Ingresamos a la Cuenta institucional

## PASO A PASO PARA LA CONFIGURACIÓN DEL MFA

Al momento de ingresar al correo como se muestra en la Figura 1, se mostrará en pantalla un mensaje para iniciar el proceso de activación del MFA, se da clic en el botón **INSCRIBIRSE**, como lo muestra la Figura 2:



Figura 2. Inicio del proceso del MFA

Posteriormente, se ingresa un número de celular como lo indica el recuadro rojo que está en la parte superior de la Figura 3, el cual actuará como medio para la segunda autenticación. Seguidamente, la cuenta de correo realizará validación ya sea por mensajes de texto o llamada telefónica al número celular designado.

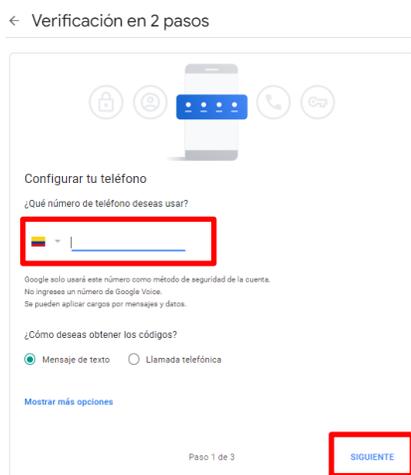
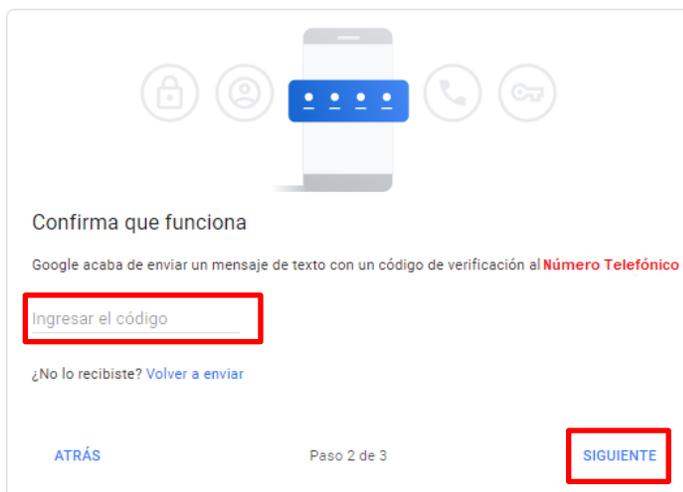


Figura 3. Paso 1 de 3 para la configuración del MFA

Una vez ingresado el número y haber dado clic en aceptar llegará un mensaje de texto o una llamada donde se entrega un código para su respectiva verificación, se ingresa el código como se muestra en la Figura 4.

Si por error se digita mal el código, se puede dar clic en el botón **atrás**, de lo contrario para continuar se da clic en **siguiente**.

#### ← Verificación en 2 pasos



Confirma que funciona

Google acaba de enviar un mensaje de texto con un código de verificación al **Número Telefónico**

Ingresar el código

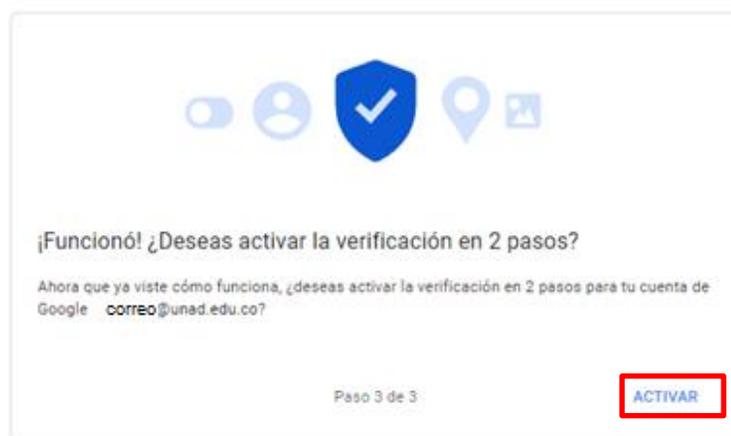
¿No lo recibiste? [Volver a enviar](#)

ATRÁS Paso 2 de 3 SIGUIENTE

Figura 4. Paso 2 de 3 para la configuración del MFA

Después de que se corrobora el código ingresado, se indicará si se desea activar la característica MFA y se da clic en **activar** como se muestra en la Figura 5:

#### ← Verificación en 2 pasos



¡Funcionó! ¿Deseas activar la verificación en 2 pasos?

Ahora que ya viste cómo funciona, ¿deseas activar la verificación en 2 pasos para tu cuenta de Google correo@unad.edu.co?

Paso 3 de 3 ACTIVAR

Figura 5. Paso 3 de 3 para la configuración del MFA

Seguidamente aparecerá una ventana donde se informa que la segunda verificación queda activada y también se visualizará el número telefónico al cuál llegará el código como segunda autenticación para cada ingreso que se realice a la cuenta de correo.

← Verificación en 2 pasos

Se activó la Verificación en 2 pasos el 10 mar 2023. DESACTIVAR

Segundos pasos disponibles

Cuando accedas, con el segundo paso se verificará tu identidad una vez ingresada la contraseña.

[Más información](#)

**Nota:** Si accedes a tu Cuenta de Google en un teléfono apto, se agregarán los mensajes de Google como otro método para realizar la verificación en 2 pasos.

**Mensaje de texto o de voz (Predeterminado)** ⓘ

**Número Telefónico Verificado**

Los códigos de verificación se envían por mensaje de texto

Agrega más segundos pasos para verificar tu identidad

Configura pasos de seguridad adicionales para poder acceder incluso si las otras opciones no están disponibles.

- Códigos de copia de seguridad**

Estas contraseñas de uso único y para imprimir te permiten acceder a tu cuenta cuando no tienes tu teléfono a mano, por ejemplo, si estás de viaje.
- Mensajes de Google**

Para recibir mensajes de Google, accede a tu Cuenta de Google en el teléfono.

Después de que ingreses la contraseña en un dispositivo nuevo, Google enviará un mensaje a todos los teléfonos en los que hayas accedido a tu cuenta. Presiona cualquiera de ellos para confirmar tu identidad.

No accediste en ningún dispositivo que admite mensajes de Google.
- App del Autenticador**

Usa una app de autenticación para obtener códigos de verificación sin cargo, incluso cuando el teléfono esté sin conexión. Disponible para Android y iPhone.
- Llave de seguridad**

Una llave de seguridad es un método de verificación que te permite acceder a tu cuenta de forma segura. Puede estar integrada en tu teléfono, usar la conexión Bluetooth o insertarse directamente en un puerto USB de la computadora.

Figura 6. Confirmación de número telefónico a dónde llegara el segundo paso del MFA

**En caso de omitir la activación del MFA, después del 30 de abril se mostrará en pantalla lo que se indica en la Figura 7, para este caso por favor informar la situación presentada mediante la **MESA DE AYUDA**.**



Figura 7. Bloqueo del correo institucional

## BIBLIOGRAFÍA

AMAZON. (s.f.). *¿Qué es la autenticación multifactor (MFA)?* Obtenido de <https://aws.amazon.com/es/what-is/mfa/>

MICROSOFT. (15 de 02 de 2023). *Ayudar a proteger el acceso a los recursos con la autenticación multifactor.* Obtenido de [https://www.microsoft.com/es-es/security/business/identity-access/azure-active-directory-mfa-multi-factor-authentication#:~:text=La%20autenticaci%C3%B3n%20multifactor%20\(MFA\)%20agrega,que%20reciben%20en%20su%20tel%C3%A9fono.](https://www.microsoft.com/es-es/security/business/identity-access/azure-active-directory-mfa-multi-factor-authentication#:~:text=La%20autenticaci%C3%B3n%20multifactor%20(MFA)%20agrega,que%20reciben%20en%20su%20tel%C3%A9fono.)

SALESFORCE, H. (20 de 01 de 2023). *Preguntas más frecuentes sobre la autenticación de múltiples factores de Salesforce.* Obtenido de <https://help.salesforce.com/s/articleView?id=000388806&type=1>