

Bogotá, 24 de marzo 2023

CIRCULAR INFORMATIVA 109-003

PARA: COMUNIDAD UNADISTA

DE: Gerencia de Plataformas Infraestructura Tecnológica - GPIT

ASUNTO: Activación doble factor de autenticación al correo electrónico institucional

La Gerencia de Plataformas e Infraestructura Tecnológica - GPIT, en el marco de sus buenas prácticas y en aras de proteger la información institucional, previene a sus usuarios sobre nuevos métodos que utilizan los ciberdelincuentes en busca de obtener datos sensibles, consiguiendo información personal, financiera, y credenciales de acceso a los correos electrónicos, de la misma manera se informa las herramientas para combatirlos.

En esta ocasión, la GPIT invita a la comunidad UNADISTA a activar el servicio ofrecido por Google, en el dominio (@unad.edu.co) el cual permite configurar el acceso a la cuenta de correo mediante autenticación de doble factor (MFA): "*contraseña habitual del usuario*" más verificación de identidad a través de un dispositivo móvil o correo electrónico alternativo, con el fin de garantizar que solamente el usuario principal sea quien pueda acceder a la cuenta.

Es importante señalar, que la implementación es de forma obligatoria e iniciará a partir del 24 de marzo y se extenderá hasta el 30 de abril del presente año.

En caso de omitir la activación del MFA, su cuenta será bloqueada y no podrá acceder al correo institucional, hasta que realice la respectiva activación.

Se adjunta Manual MFA para realizar esta configuración en las cuentas de correo institucional.

"**Código mediante mensaje de texto**", es decir, que, para poder acceder al correo, deberá ingresar un código que llegará por medio de un SMS al móvil registrado, para comprobación de identidad, lo que da confianza a verificar la identidad cuando se inicia sesión en la cuenta como se muestra en la Figura 1.

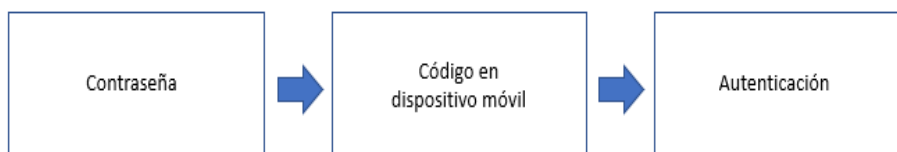


Figura 1. Proceso de autenticación

Con esta medida se pretende:

- ✚ Minimizar el riesgo de acceso no autorizado a las cuentas de correos institucionales
- ✚ Minimizar el riesgo de suplantación de identidad
- ✚ El uso de un nivel adicional de seguridad sobre las cuentas de correos institucionales
- ✚ Evitar la sustracción de información institucional y/o personal

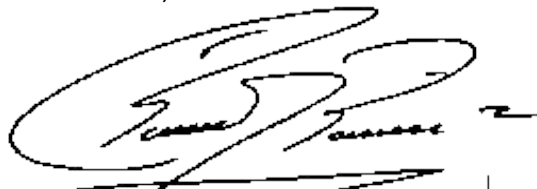
Recomendaciones para tener contraseñas seguras:

1. Tener mínimo 10 caracteres
2. Incluir caracteres especiales, mayúsculas, minúsculas y números
3. No incluir datos sensibles o personales (nombres, ciudades, fechas)
4. Que sea fácil de memorizar para que no las tenga que anotar
5. Cambiarla cada 60 o 90 días
6. No suministrar la contraseña a terceros (Familiares, amigos u otros)
7. Caracteres permitidos (@ [] ^ _ ! " # \$ % & ' () * + , - . / : ; { } < > = | ~ ? A-Z a-z 0-9

En caso de alguna inquietud sobre el proceso de la activación del MFA, por favor realizar la solicitud a través de la aplicación <https://mesadeayuda.unad.edu.co/>, donde el equipo de soporte técnico de la GPIT a nivel nacional estará dispuesto para atender estas solicitudes.

Agradecemos su amable atención

Cordial Saludo,



RAFAEL ANTONIO RAMÍREZ RODRIGUEZ
Gerente de Plataforma e Infraestructura Tecnológica – GPIT
UNAD

Elaborado por: Grupo de Seguridad de la Información

Anexo: Se anexa Manual de Instalación Doble Factor de Autenticación del correo institucional.