

10 DE JUNIO DE 2021

**CIRCULAR
UNA-CGT-CIRC-010-2021**

PARA: COMUNIDAD UNIVERSITARIA

DE: CENTRO DE GESTIÓN TECNOLÓGICA (CGT)

**ASUNTO: RECORDATORIO. RECUPERACIÓN DE CONTRASEÑA DE
CORREO ELECTRÓNICO INSTITUCIONAL PARA FUNCIONARIOS**

Estimada comunidad universitaria:

Debido a las numerosas solicitudes recibidas en relación con el extravío de la contraseña de correo electrónico institucional para funcionarios, el Centro de Gestión Tecnológica (CGT) procede a recordar el procedimiento para la recuperación de esta contraseña de forma desconcentrada, a cargo del interesado.

El funcionario debe iniciar la sesión requerida en el siguiente enlace web:

<https://myaccount.google.com/u/0/?hl=es>

Posteriormente, se procede a ingresar al apartado “Seguridad”, y en esta opción se debe ubicar el apartado de “Correo electrónico de recuperación” o “Teléfono de recuperación”. En ambos casos, se asume que estos elementos pertenecen al usuario, y que futuros cambios de estos de estos datos de contacto deben reflejarse de forma oportuna en este apartado.

Lo anterior permite incluir un correo electrónico alternativo y/o número de teléfono celular, que serán utilizados por Google en caso de que el interesado desee recuperar su contraseña por alguno de los métodos señalados.

Respetuosamente, se solicita a la comunidad universitaria proceder con esta configuración.

Segundo factor de autenticación

Se aprovecha la oportunidad para indicar que, para reforzar la seguridad de este servicio, se puede habilitar un segundo factor de autenticación (2FA), o una segunda contraseña, cuya funcionalidad es idéntica a la utilización de claves dinámicas o tokens bancarios utilizados en internet. Por lo tanto, en cada ocasión que se utilice alguna facilidad de Google asociada al correo electrónico institucional, la plataforma solicitará la contraseña principal, y



posteriormente una segunda contraseña correspondiente al segundo factor de autenticación (2FA). El 2FA, se habilita en el mismo apartado de “Seguridad”, habilitando la opción de “Verificación en dos pasos”.

Existen varias formas de utilizar el 2FA, siendo una de las más populares la instalación en el teléfono del software “Google Authenticator” para obtener de forma aleatoria la segunda contraseña. Esta opción se recomienda para aquellas personas que deseen incrementar la seguridad de su correo electrónico, y que utilicen de forma correcta e informada esta tecnología.

Para más información:

https://www.google.com/landing/2step/?hl=es_419#tab=why-you-need-it

<https://support.google.com/accounts/answer/185839?co=GENIE.Platform%3DDesktop&hl=es>

Atentamente,

Maykol Phillips Seas
Director

