Boletín Informativo

GIDT

MANUAL DE INSTALACIÓN **DOBLE FACTOR DE AUTENTICACIÓN DEL CORREO INSTITUCIONAL Y DE GMAIL**

Universidad Nacional Abierta y a Distancia

"Por la Calidad Educativa y La Equidad Social"

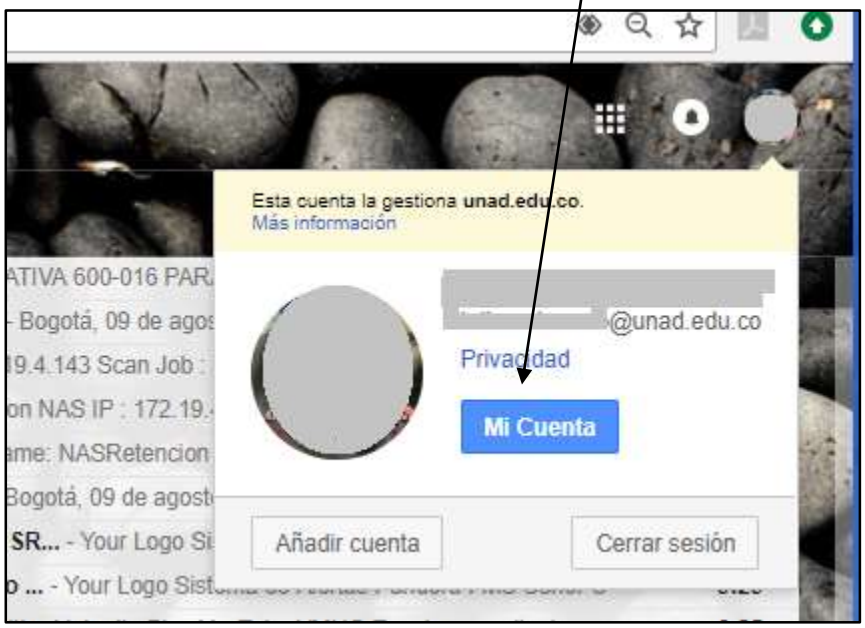
UNAD

GRUPO FUNCIONAL DE SEGURIDAD INFORMATICA - GFSI

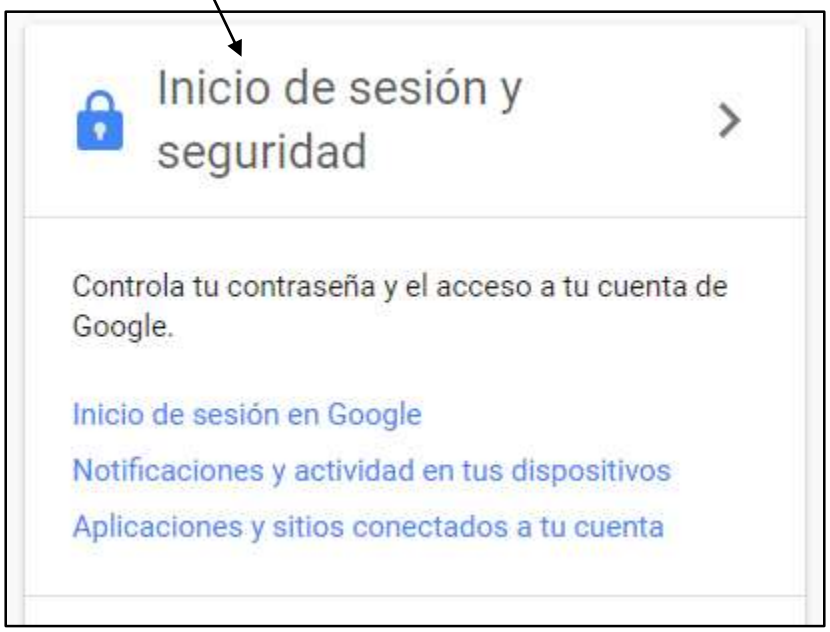
29/03/2021

Cuando estemos dentro de la bandeja de nuestro correo institucional, haremos click en la parte superior derecha en el ícono con círculo relleno, como se aprecia a continuación:

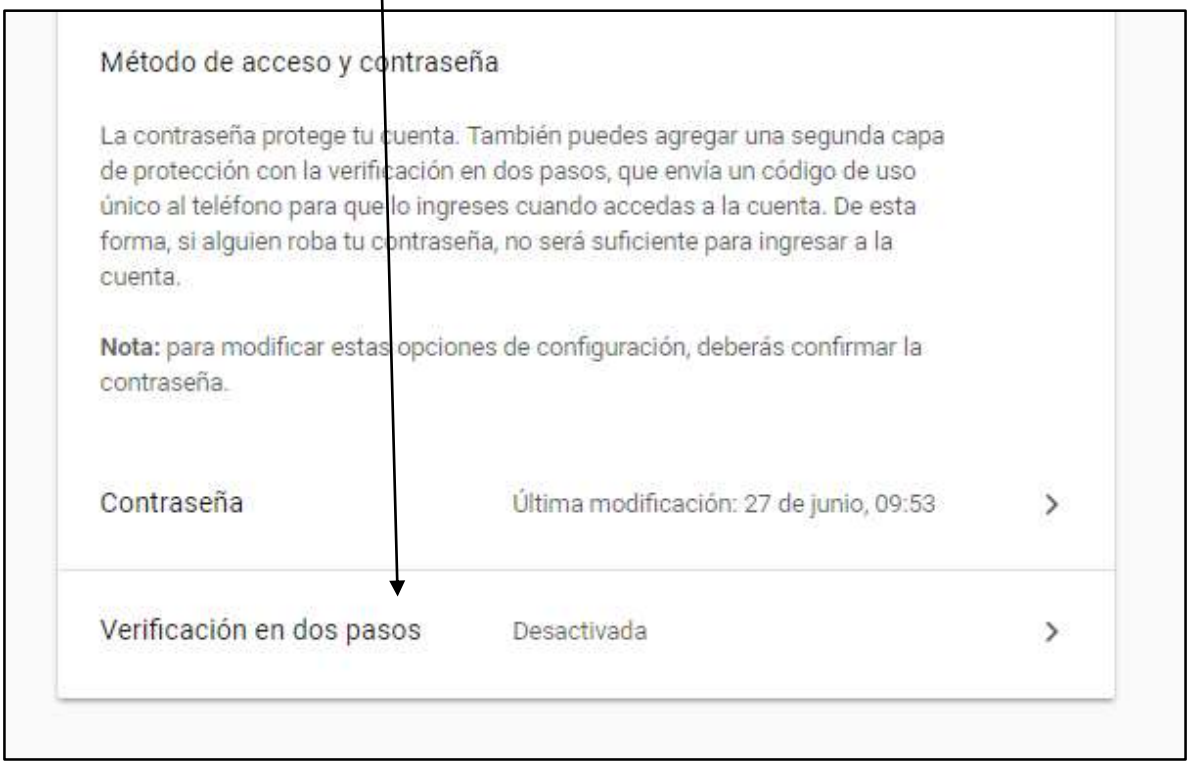
Una vez hemos hecho click nos aparecerá la siguiente ventana en donde haremos click en "**Mi Cuenta**", como se aprecia a continuación:



Al hacer click nos aparecerá la siguiente ventana en donde haremos click en "**Inicio de sesión y seguridad**":

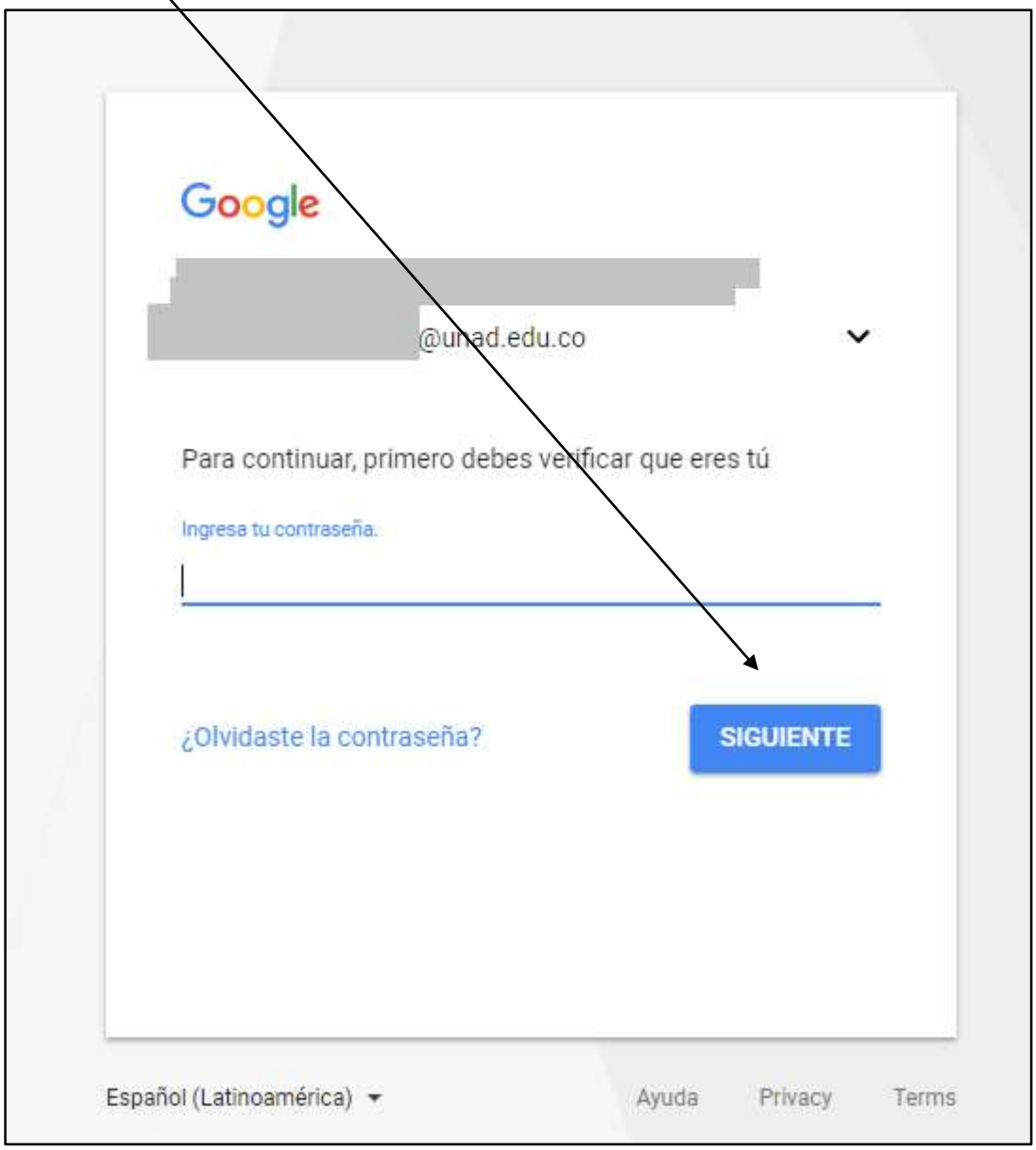


Seguidamente nos aparecerá una ventana donde escogeremos la opción "**verificación en dos pasos**", que inicialmente se visualiza como desactivada, como se aprecia a continuación:

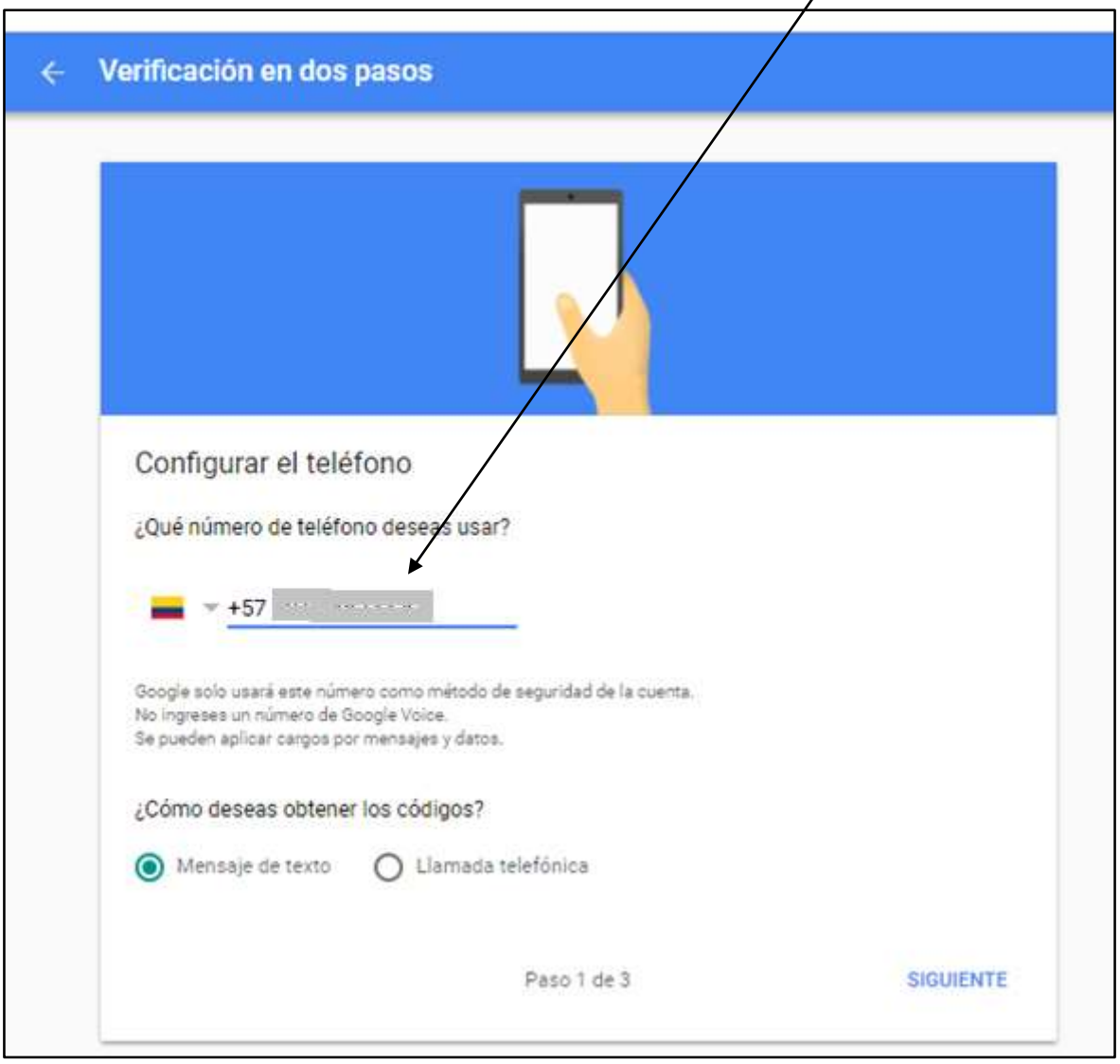


Al hacer click en la opción anterior, nos aparecerá la siguiente ventana en donde haremos click en "**empezar**", como se puede apreciar en la siguiente gráfica:

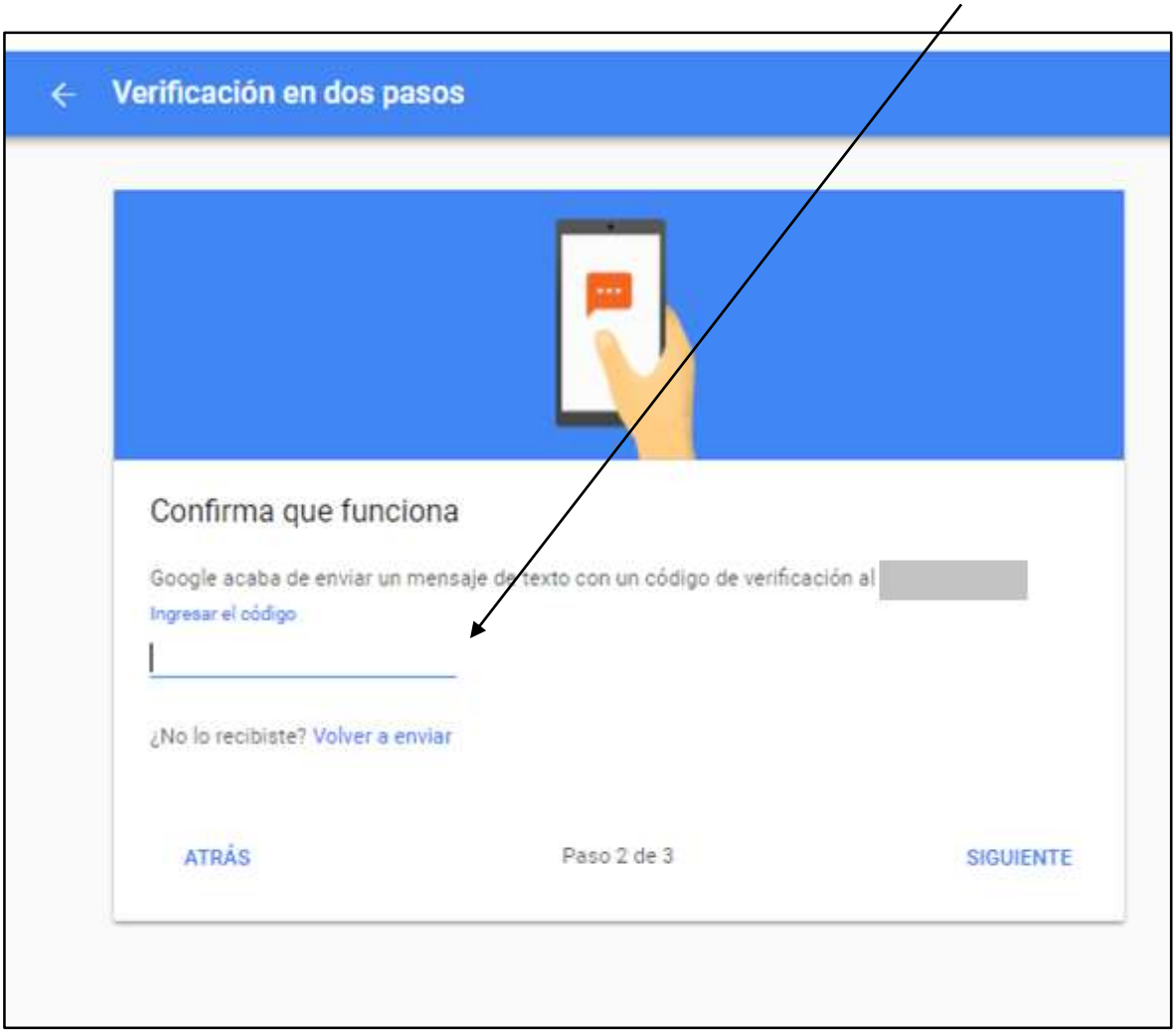
Una vez hemos hecho click en esta opción nos aparecerá una nueva ventana en la cual GMAIL nos pide nuevamente ingresar las credenciales (clave) de nuestro correo institucional, después haremos click en "**siguiente**", como se aprecia a continuación:



Seguidamente nos pedirá que número telefónico usaremos para recibir el mensaje de texto con el código numérico o recibir una llamada, recomendamos escoger la opción “**mensaje de texto**”, una vez digitado el número telefónico del móvil haremos click en “**siguiente**”, como se puede apreciar a continuación:



A continuación GMAIL nos avisará que se ha enviado un código de verificación al número telefónico escrito anteriormente, el cual debemos revisar y digitar y hacer click en “**siguiente**”, como se puede apreciar en la siguiente gráfica:

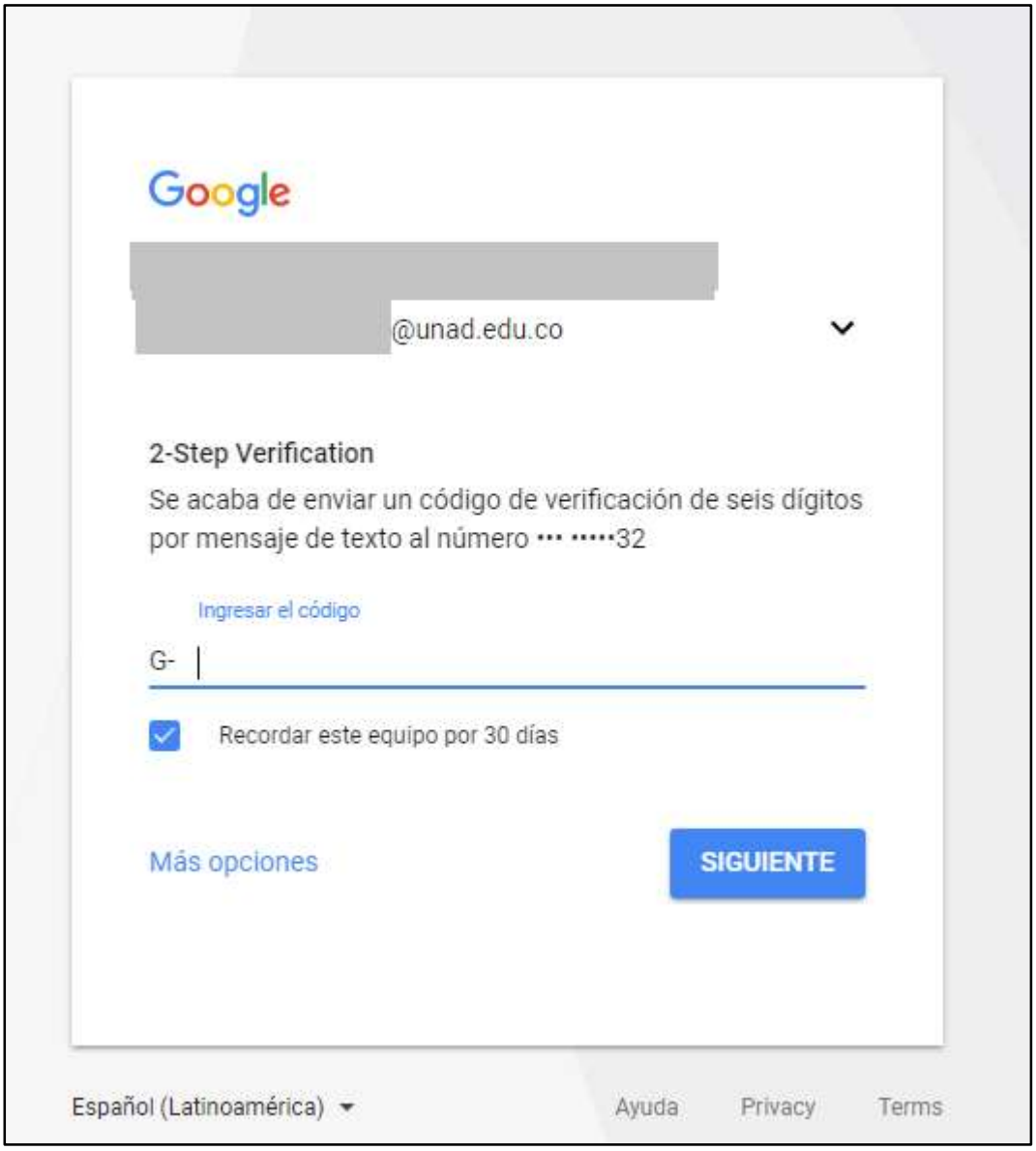


Nota: Nos aparece el código con la letra G al principio, solo debemos digitar el número telefónico.

Una vez hemos introducido el código numérico y hecho click en siguiente, nos aparecerá una ventana que nos preguntará si funcionó el proceso de verificación en dos pasos para nuestra cuenta de correo. A continuación pulsaremos click en "**Activar**", como se puede apreciar en la siguiente gráfica:

Seguidamente nos aparecerá una ventana que nos avisará desde cuando la verificación en dos pasos queda activada, para el ejemplo quedó desde el 10 de agosto del 2.017.

Para validar que se ha implementado correctamente la verificación en dos pasos, nuevamente iniciamos sesión en GMAIL y a continuación nos pedirá nuevamente otro código numérico que ya habremos recibido en nuestro número telefónico móvil, el cual tendremos que digitar y hacer click en "**siguiente**".



Y eso es todo.

NOTAS:

a) Cada vez que iniciemos sesión generará por seguridad un código numérico en nuestreo móvil, ese será nuestro segundo factor de autenticación al correo institucional.
b) GMAIL nos preguntará si queremos recordar nuestro pc por 30 días, para evitar digitar el código de autenticación, por seguridad es mejor no recordar. Es mejor digitar un código nuevo cada vez que iniciemos sesión.
c) Si entramos a nuestro correo institucional desde otro pc, móvil, o equipo diferente, nos pedirá el código de verificación.
d) Podriamos habilitar siguiendo los pasos anteriores, un segundo teléfono móvil para recibir el código de verificación en caso de que el servicio del primer móvil esté temporalmente fuera de servicio.
e) Podriamos configurar alertas de seguridad, en el evento que un hacker tenga mis credenciales de acceso, pero no tenga el código de verificación, en ese caso nos llegará como mensaje de texto a nuestro móvil la alerta configurada, o simplemente nos llegará un nuevo código numérico, si no estamos realizando una sesión para entrar a nuestro correo, posiblemente otra persona lo esté intentando.

Este mecanismo de autenticación no es infalible, pero le da otro nivel de seguridad a la manera como iniciamos sesión a nuestro correo institucional. Y así minimizamos el riesgo de suplantación de identidad y de acceso no autorizado a nuestra cuenta de correo.

Atentamente,

Grupo Funcional de Seguridad Informática, UNAD