Universidad unab

# ¡Dos es mejor que uno!

*Doble factor de identificación*

## Autenticación de doble factor para evitar accesos indeseados y suplantación de identidad.

La autenticación de doble factor (o autenticación en dos pasos) constituye una medida de seguridad importante que añade una segunda capa de protección a la contraseña que empleamos. Agregar esta capa adicional de seguridad hace que sea mucho más difícil para un ciberdelincuente vulnerar las cuentas de los usuarios.

## ¿Qué pasa cuando usamos un mecanismo de doble factor de autenticación?

La autenticación de doble factor o verificación en dos pasos agrega un nivel adicional de seguridad al proceso de acceso al correo electrónico, ya que requiere que el usuario se identifique de 2 maneras diferentes:

la primera es generalmente una contraseña y la segunda se puede elegir entre varios modos, por ejemplo: SMS o un código de seguridad numérico. Gracias a esto, es mucho más difícil que alguien, averiguando la contraseña, pueda acceder a su correo

Ilustrado con un ejemplo, es similar a colocar un sistema de alarma para llegar a tu casa, usualmente usarás una llave para entrar a la vivienda, pero además también tendrás que introducir un código, de lo contrario, no podrás acceder.

## ¿Qué se soluciona con la doble autenticación?

Los ciberdelincuentes se dan a la tarea de buscar nuestras contraseñas para poder acceder a nuestros servicios, robarnos datos, extorsionarnos, etc. Pueden encontrar las contraseñas de varias maneras:

- Intentando adivinarlas por fuerza bruta, es decir, probando todas las combinaciones posibles.
- Engañándonos con técnicas de ingeniería social para que se las entreguemos (phishing).
- Infectándonos por malware, que tiene la funcionalidad de robar contraseñas.
- Por malas prácticas del usuario, como no cerrar la sesión del correo electrónico o apuntar las contraseñas en un papel quedando a la vista de alguien con malas intenciones.

**Con la doble autenticación se mitigan en gran medida los ataques anteriores,** pues el ciberdelincuente tendría que hacerse también con el segundo factor.

## ¿Siempre tendré que autenticarme con los dos factores?

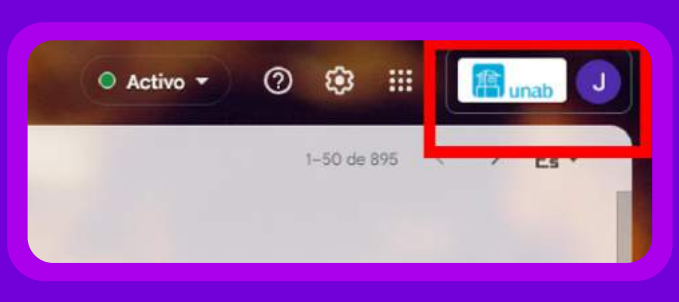
No, el segundo factor se activará cuando se autentique en un equipo diferente al utilizado habitualmente.

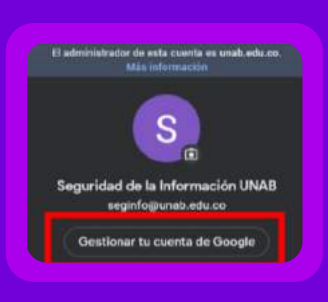
## ¿Esto significa que estoy completamente a salvo?

No. Por definición, ningún sistema conectado a la red es 100% seguro. Sin embargo, has reducido el riesgo de robo de datos al agregar un nivel adicional de seguridad.

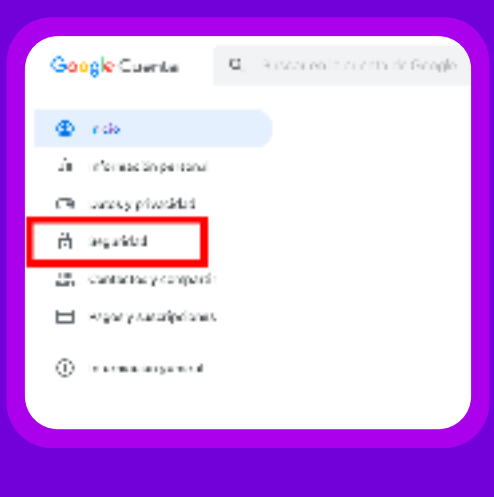
# ¿Cómo lo hago?

**1.** Ingresa al sitio de administración de la cuenta haciendo clic en el enlace Gestionar en tu cuenta de Google. que se visualiza al hacer clic en la letra inicial o fotografía de tu cuenta de correo.




**2.** Ingresa a la opción Seguridad de Google.




**3.** Activa la verificación en dos pasos en la sesión de acceso a Google. Ubicar la sección de “Métodos para verificar que eres tú”.


Finalmente ingresa el número de celular y/o correo electrónico al que deseas que llegue la solicitud de aceptación y/o rechazo para ingresar al correo. (El Correo que ingreses en esta opción debe ser una cuenta diferente al correo UNAB).

Recuerda, la seguridad es compromiso de todos.

**Seguridad de la información - UNAB**