



UTN.BA

UNIVERSIDAD TECNOLÓGICA NACIONAL
FACULTAD REGIONAL BUENOS AIRES

Verificación en 2 pasos

Aclaración: Esta documentación está orientada específicamente para cuentas de **Google institucionales**. Es posible que algunas opciones o configuraciones varíen respecto a cuentas personales. En caso de no encontrar alguna opción mencionada, comunicate con soporte.

¿Qué es la Verificación en 2 Pasos?

La **Verificación en 2 Pasos** (también conocida como autenticación de dos factores) es una medida adicional de seguridad que protege tu cuenta de Google en caso de que tu contraseña sea robada o comprometida. Al activarla, deberás confirmar tu identidad con un segundo paso de verificación cada vez que inicies sesión.

Esto significa que, además de tu **contraseña**, necesitarás un **código adicional** o una **aprobación desde un dispositivo de confianza** para poder acceder. De esta manera, si alguien obtiene tu contraseña, no podrá acceder sin ese segundo factor de autenticación.

¿Por qué es importante activarla?

Activar la Verificación en 2 Pasos en tu cuenta institucional ayuda a:

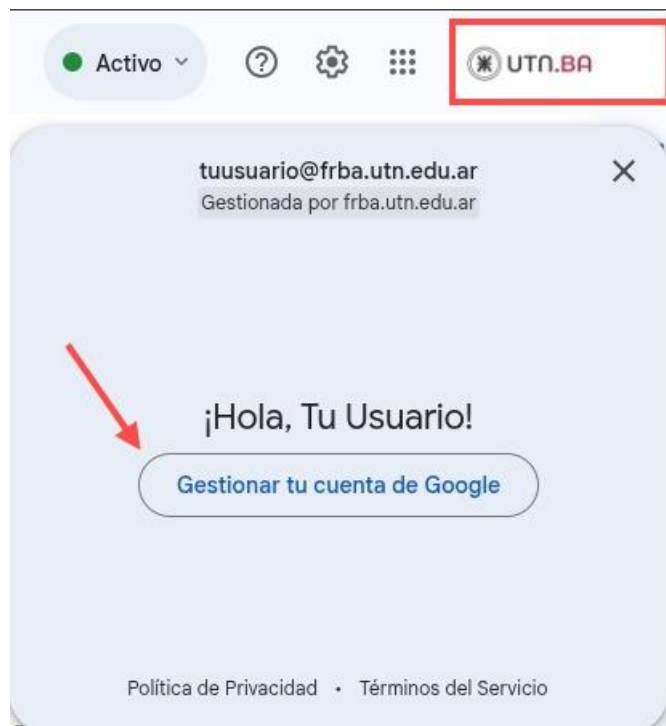
- **Prevenir accesos no autorizados**, incluso si se conoce tu contraseña.
- **Proteger información confidencial** vinculada a tu cuenta institucional.
- **Cumplir con políticas de seguridad** de la institución

Pasos para activar la Verificación en 2 Pasos

Paso 1: Ingresar a tu cuenta

1. Abrió [Gmail](#) desde tu navegador o dispositivo móvil.
2. En la parte superior derecha, hacé clic sobre tu foto de perfil.
3. Luego, seleccioná la opción "**Gestionar tu cuenta de Google**".

(Aquí va una imagen con un cuadro resaltando la foto de perfil y una flecha hacia "Gestionar tu cuenta de Google")



Paso 2: Ir a la sección de Seguridad

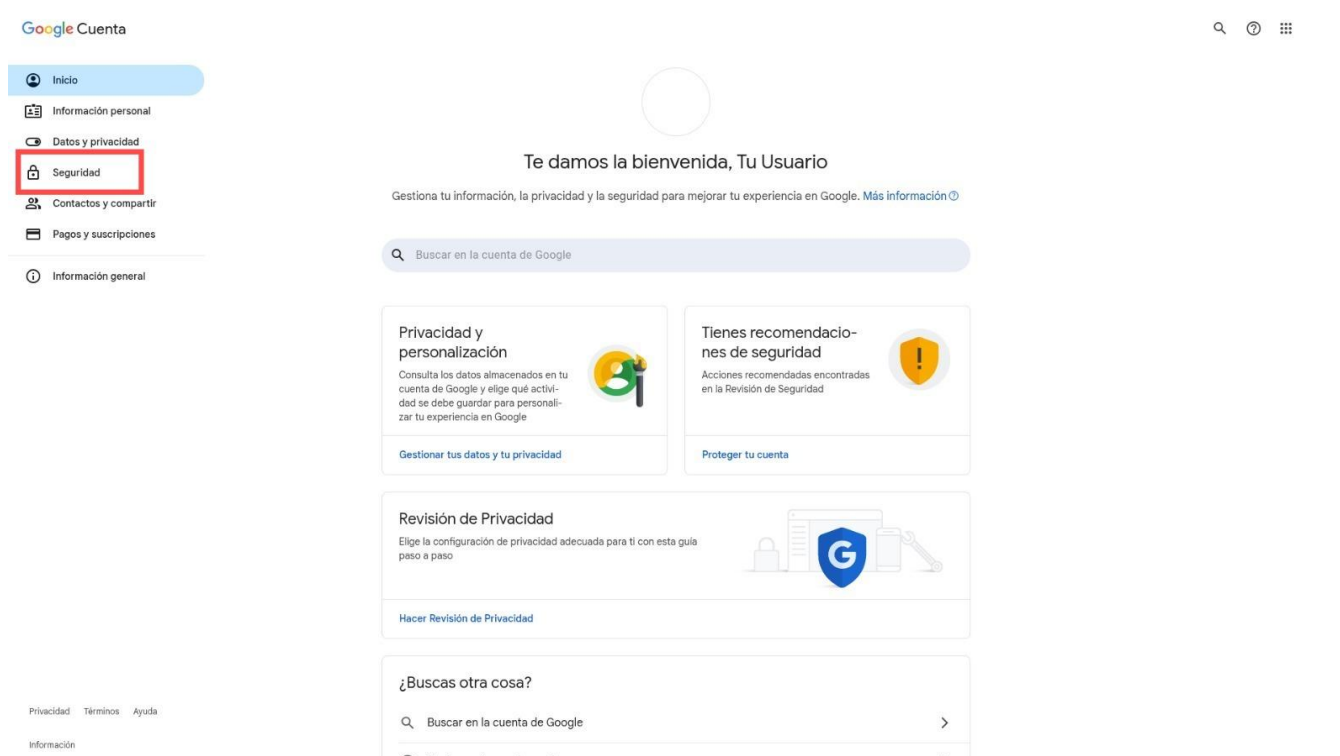
Una vez que accedas a la configuración de tu cuenta de Google, serás redirigido al panel general.

1. En el menú lateral izquierdo, seleccioná la pestaña **“Seguridad”**.

Importante:

- En computadoras de escritorio, la opción estará visible directamente en el menú de la izquierda.
- En teléfonos móviles, es posible que debas desplazarte hacia los costados o buscar la opción de seguridad entre las secciones del centro de la pantalla.

(Aquí va una imagen señalando la opción “Seguridad” en una computadora)



Paso 3: Activar la Verificación en 2 Pasos

1. Dentro de la sección de **Seguridad**, buscá el apartado llamado **“Cómo accedes a Google”** o **“Cómo inicias sesión en**

Google”.

2. Hacer clic en la opción “**Verificación en 2 pasos**”.
3. Es posible que el sistema te pida volver a ingresar tus credenciales:
 - Ingresá tu **usuario del SIA** y tu **contraseña** institucional.
4. Luego, seleccioná la opción para **activar la Verificación en 2 pasos**.

(Aquí va una imagen mostrando dónde se encuentra la opción “Verificación en 2 pasos”)

← Verificación en dos pasos

Activar verificación en dos pasos

Impide que los hackers accedan a tu cuenta con una capa adicional de seguridad.

A menos que inicies sesión con una llave de acceso, se te pedirá que completes el segundo paso más seguro disponible en tu cuenta. Puedes actualizar tus segundos pasos y las opciones de inicio de sesión en cualquier momento en la configuración. [Ir a Configuración de seguridad](#) ⇌



Activar verificación en dos pasos

Segundos pasos

Asegúrate de poder acceder a tu cuenta de Google manteniendo al día esta información y añadiendo más opciones de inicio de sesión



Llaves de acceso y llaves de seguridad



Añadir una llave de seguridad



Notificación de Google



0 dispositivos



Authenticator



Añadir aplicación Authenticator



Paso 4: Elegir el método de verificación

Una vez activada, se te pedirá que elijas un segundo método de verificación.

Las opciones más comunes son:

- **Notificación de Google:**
Cada vez que intentes iniciar sesión, recibirás una notificación en tu dispositivo de confianza. Solo cuando apruebes esa notificación se permitirá el acceso.
- **Google Authenticator u otra app de códigos:**
Podés usar una aplicación que genera códigos temporales de 6 dígitos.

(Aquí va una imagen mostrando las distintas opciones de verificación)

Segundos pasos

Asegúrate de poder acceder a tu cuenta de Google manteniendo al día esta información y añadiendo más opciones de inicio de sesión



Llaves de acceso y llaves de seguridad



Añadir una llave de seguridad



Notificación de Google



4 dispositivos



Authenticator



Añadir aplicación Authenticator



Códigos de verificación alternativos



Obtener códigos de verificación alternativos



¡Listo! Tu cuenta ya tiene la Verificación en 2 Pasos activada.



A partir de ahora, cada vez que accedas a tu cuenta institucional desde un nuevo dispositivo o navegador, se requerirá este segundo paso de autenticación para mayor seguridad.

🔄 Revisión #3

★ Creado 23 junio 2025 09:23:53 por Massimo Andres Cibeira Occhiuzzi

✎ Actualizado 23 junio 2025 10:31:58 por Massimo Andres Cibeira Occhiuzzi