PRORRECTORIA | DEI DIRECCIÓN ESTRATÉGICA INFORMÁTICA

INSTRUCTIVO

Casillas de Correo USACH

Autentificación en Dos Pasos

Santiago, diciembre de 2024

Departamento de Seguridad de la Información

CONTENIDO

INTRODUCCIÓN

La Universidad de Santiago de Chile, priorizando siempre la seguridad de la información, ha adoptado el **MFA (Autenticación Multifactor)** para proteger las casillas de correo y recursos digitales.

Las contraseñas por sí solas **ya no son seguras**, siendo vulnerables a accesos no autorizados, filtraciones, robo de información personal, ataques de fuerza bruta y *phishing

* Técnica de estafa en línea que consiste en enviar correos electrónicos falsos para robar información personal de los usuarios.

CÓMO FUNCIONA EL MFA (Autenticación Multifactor)

La Autenticación Multifactor (MFA) es un método de seguridad que requiere que los usuarios verifiquen su identidad utilizando dos o más factores diferentes antes de acceder a un sistema o cuenta. Esto agrega una capa adicional de protección frente a posibles amenazas, como el robo de contraseñas.

Los tres factores principales utilizados en MFA son:

- Algo que sabes: como una contraseña o un PIN.
- Algo que tienes: como un teléfono móvil, un token físico o una tarjeta inteligente.
- Algo que eres: como datos biométricos, como una huella dactilar, reconocimiento facial o escaneo de retina.

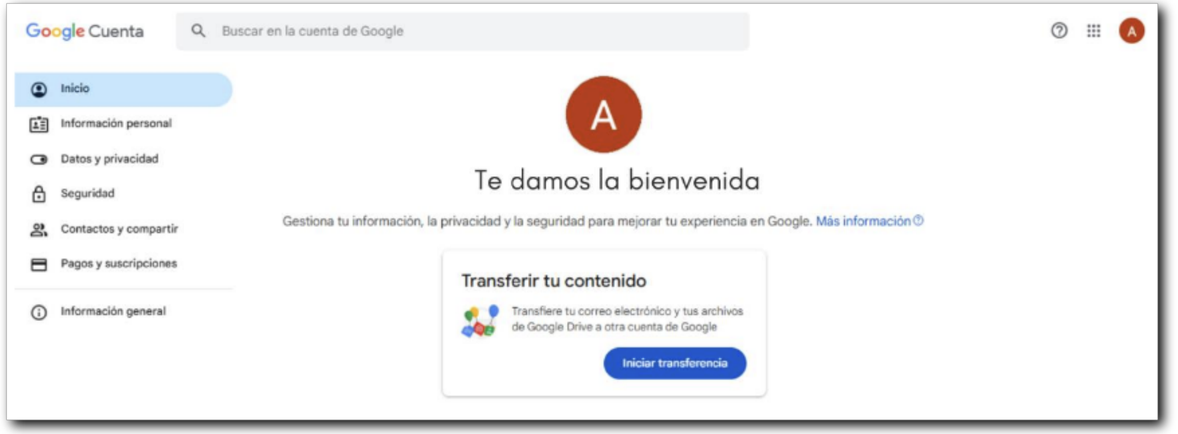
La USACH por ahora propone el uso de la 2° opción, verificación a través del teléfono móvil, que se detallará a continuación.

¿CÓMO ACTIVAR LA VERIFICACIÓN?

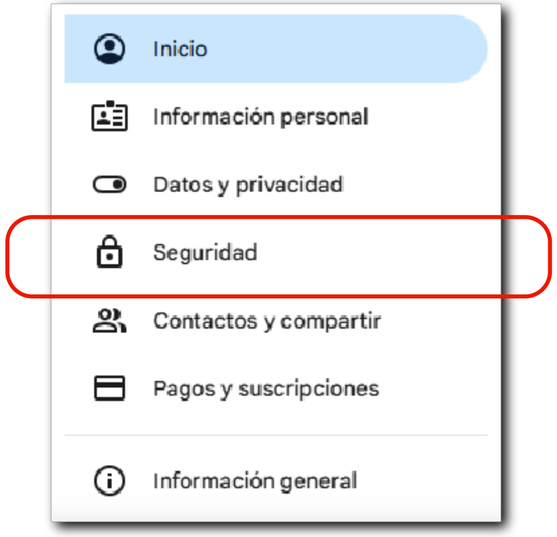
1. Ingresando al correo institucional, y haz “click” en el apartado correspondiente a tu perfil.

2. Ahora debe hacer “click” en el recuadro de **“Gestionar tu cuenta de Google”.**

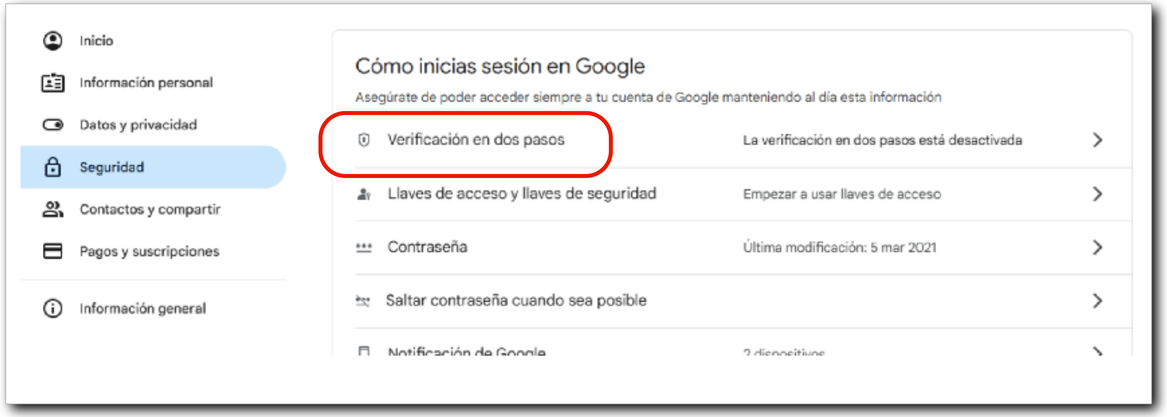
3. Luego, se abrirá otra ventana que mostrará la siguiente información:



4. Al costado izquierdo, haz click en seguridad.



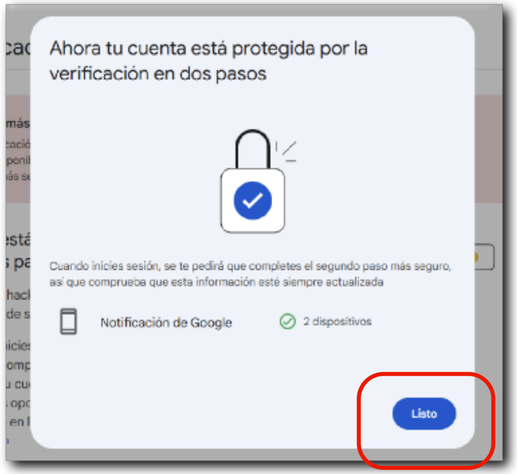
5. Deslizando la barra del costado derecho, se encontrará con la sección titulada **“Cómo inicias sesión en Google”**, y seleccionar **Verificación en dos pasos.**



6. Ingrese con su correo USACH.

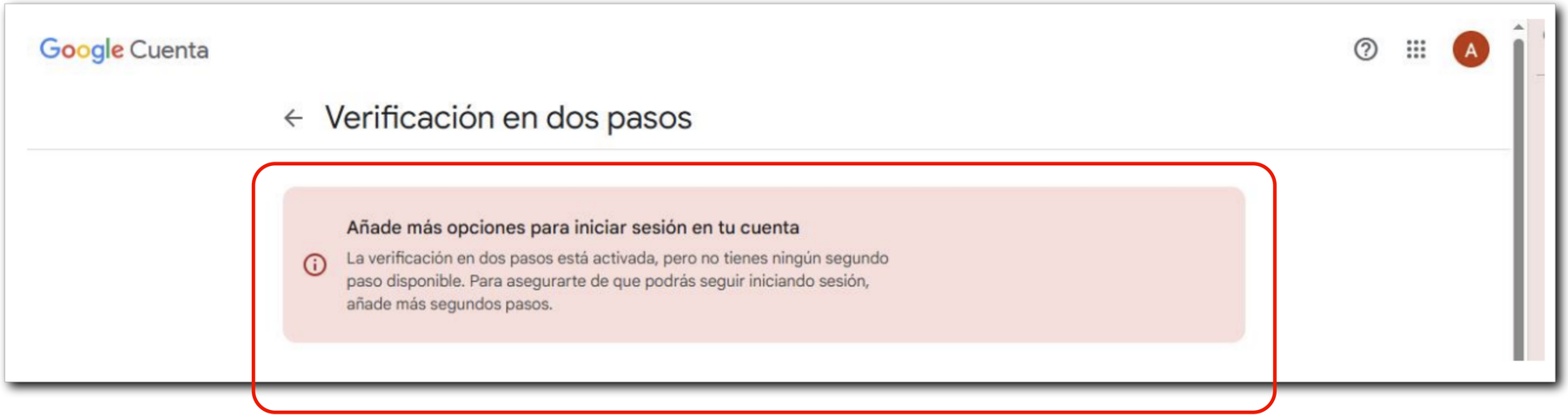
7. La página nuevamente lo redireccionará y se mostrará la siguiente pantalla, y seleccionamos la opción **Activar verificación en dos pasos.**

8. Se mostrará la siguiente pantalla, en donde debes hacer click en **Listo.**

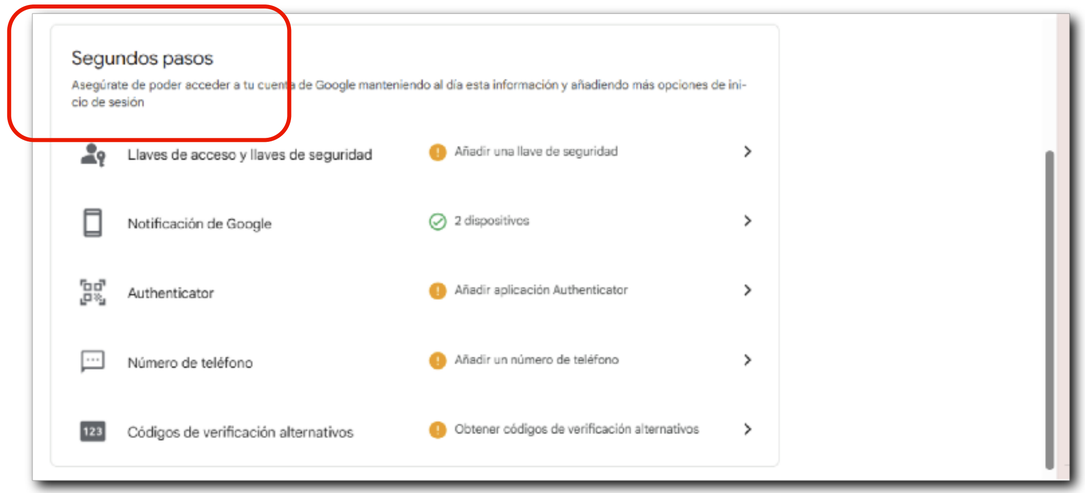


OPCIONES DE INICIO DE SESIÓN PARA MAYOR SEGURIDAD

Aunque la verificación ya se encuentre activada, **es importante añadir más opciones para iniciar sesión** en su cuenta para mayor seguridad. Por lo mismo, se mostrará este mensaje en rojo.



1. Baja con la barra derecha (scroll) hasta llegar a **“Segundos pasos”.**



2. Las opciones recomendables para incorporar son:

- Authenticator
- Número de teléfono

Para ambas alternativas, es importante destacar que **es necesario el uso del celular**.

Puede añadir tanto una de las opciones, como ambas, ya que **no son excluyentes entre sí.**

IMPORTANTE

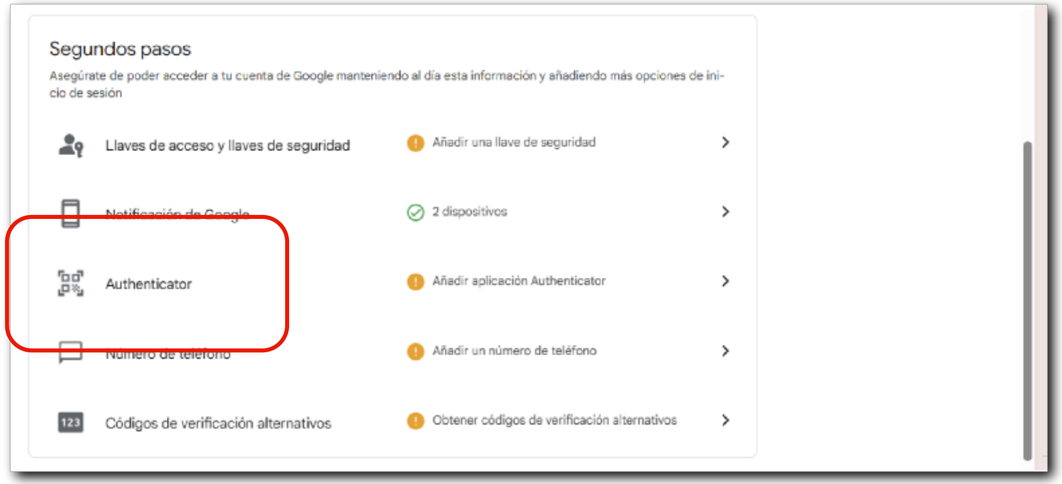
En el caso de pérdida o robo de su celular

Si bien es importante elegir alguna de las opciones anteriores, también es recomendable activar la opción de **“Códigos de Verificación Alternativos”** como respaldo, ya que, en el caso de perdida o robo de su celular, con solo la opción de Authenticator o Número de teléfono activadas, no podrá acceder a su correo institucional.

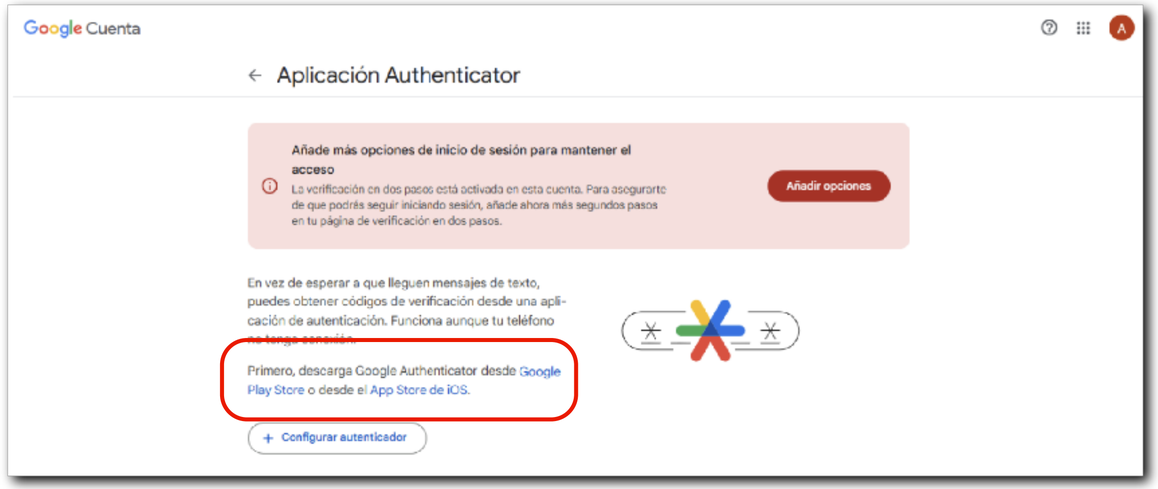
→ Para activar la opción Códigos de Verificación Alternativos, puede seguir cualquiera de los 3 pasos que se detallan a continuación.

ANEXO 1: ACTIVAR OPCIÓN DE AUTHENTICATOR

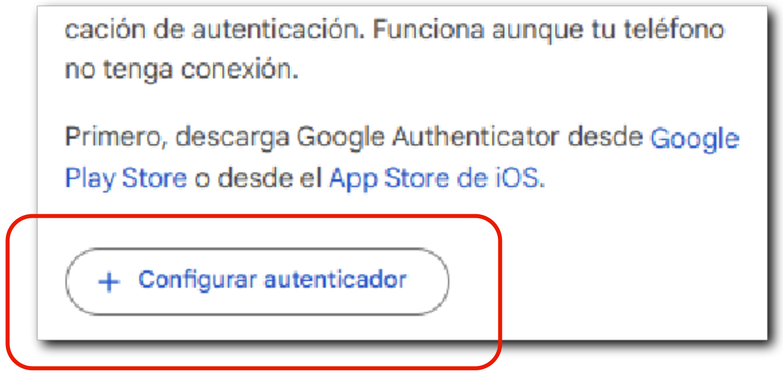
1. Desde la misma pantalla Segundos Pasos, hacer click en **Authenticator**



2. Aparecerá la siguiente pantalla, en donde se indica que debes descargar la aplicación de **“Google Authenticator”** en tu celular.

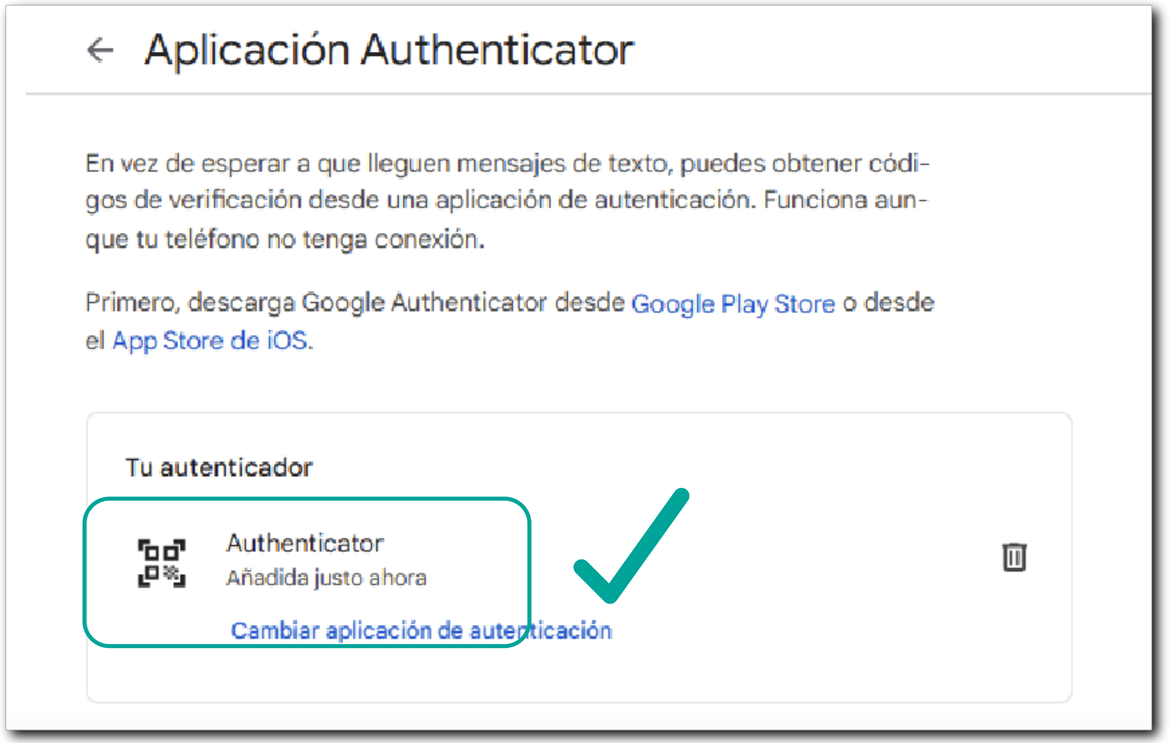


3. Una vez instalada la aplicación en su dispositivo, seleccionar **“Configurar autenticador”**.



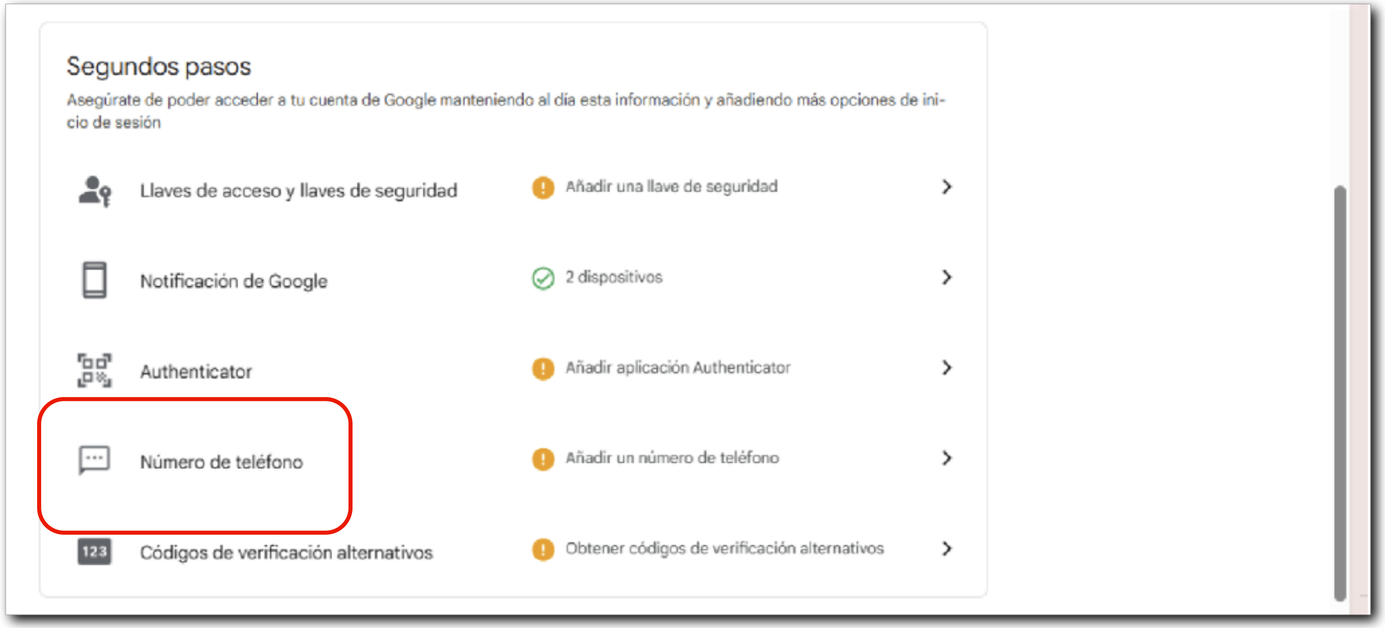
4. **Escanee el Código QR** presente en su pantalla del computador y una vez realizada esta operación, ingrese los códigos que aparecerán en su celular.

5. Una vez realizados todos los pasos, se mostrará la siguiente página principal, indicando que el proceso se encuentra completo.

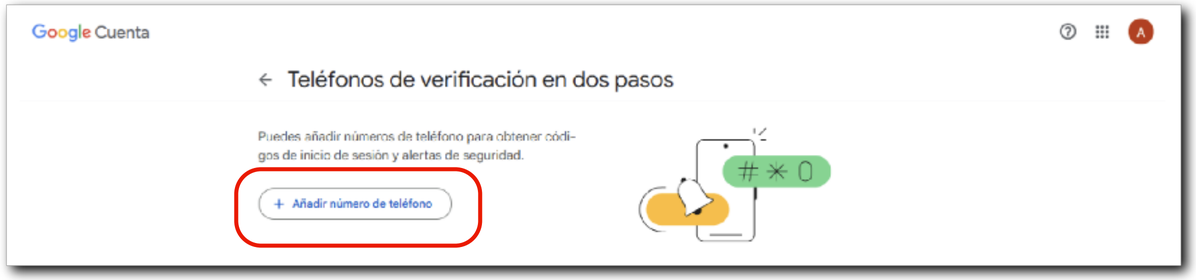


ANEXO 2: ACTIVAR OPCIÓN DE NÚMERO DE TELÉFONO

1. Desde la pantalla de **“Segundos pasos”**, seleccione la opción de **Número de teléfono.**



2. Ahora, debemos hacer click en **“Añadir número de teléfono”**.

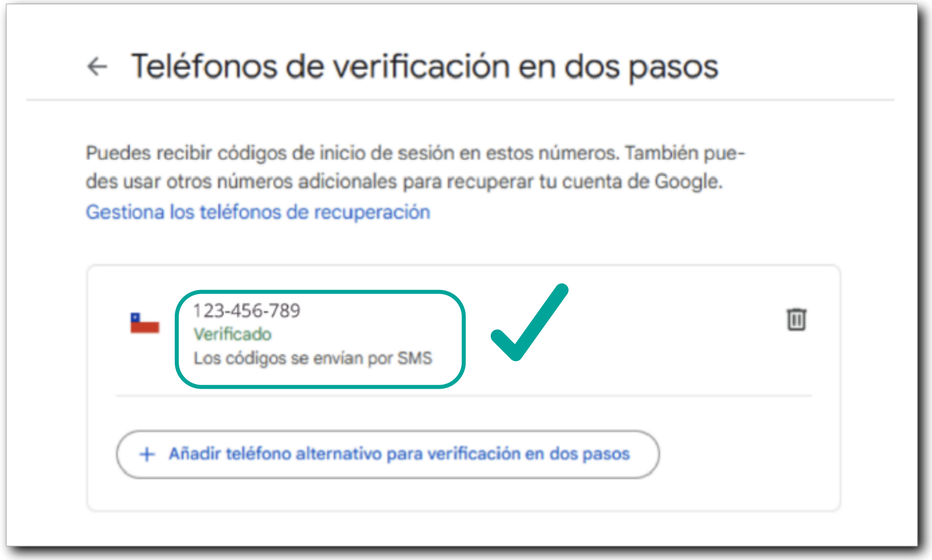


3. Aquí debemos ingresar nuestro n° de celular, y seleccionar el medio por el cual preferimos que nos envíen los códigos de activación. Luego has click en **Siguiente.**

4. Complete la acción necesaria.

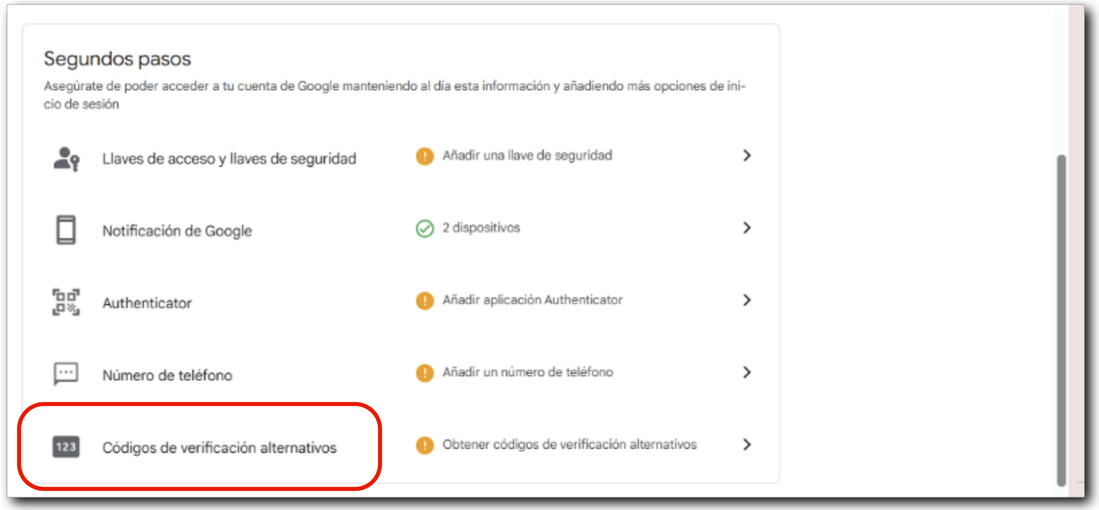
- Si eligió la alternativa de **“Mensaje de texto”:** Debe completar con el código enviado a su celular.
- Si eligió la alternativa de **“Llamada de voz”**: Le habrán llamado para entregarle el código correspondiente con el fin de verificar que es usted el dueño/a de su dispositivo.

5. Una vez realizados todos los pasos, se mostrará la siguiente página principal, indicando que el proceso se encuentra completo:



ANEXO 3: ACTIVAR LA OPCIÓN DE CÓDIGOS DE VERIFICACIÓN ALTERNATIVOS

1. Desde la pantalla de **“Segundos pasos”** haga click en la opción de **Códigos de Verificación Alternativos.**

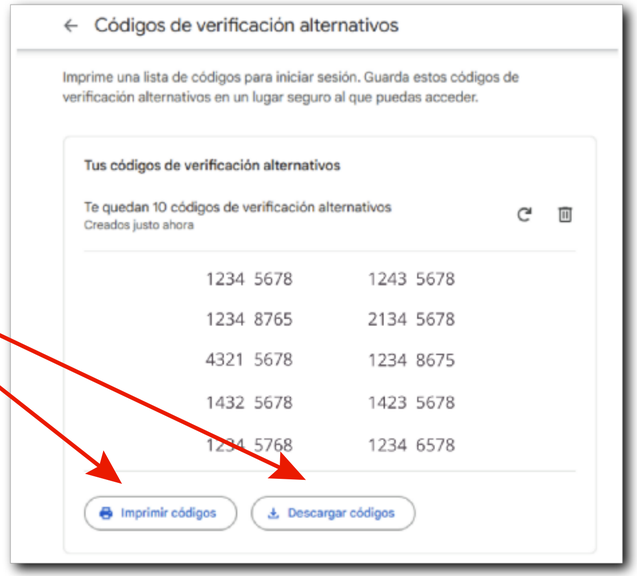


2. Ahora debe seleccionar la opción **“Obtén códigos de seguridad”**.

3. Aparecerán todos los códigos son diversos entre sí y que, además, son diferentes para cada persona.

Puede seleccionar cualquiera de las 2 opciones, ya sea imprimir o descargar los códigos.

Una vez realizados todos los pasos, el proceso se encuentra terminado. ✓



USACH

PRORRECTORIA

DEI
DIRECCIÓN ESTRATÉGICA
INFORMÁTICA