Rocketbot Studio : Migrar bots con Virtualizacion

Pasos a Seguir para la Migración de Bots de Virtualización

Virtualización en la Máquina Destino

Es recomendable realizar la virtualización directamente en la máquina o computadora final. Esto se debe a que la resolución de pantalla puede variar, lo que podría requerir ajustes en la configuración, similar a la máquina donde se realizó la virtualización inicialmente.

Consistencia de Imágenes de Referencia

Es posible que la imagen utilizada como referencia no sea la misma que la que se encuentra en la computadora de destino. En tal caso, será necesario capturar nuevamente las imágenes de referencia, incluyendo focos , como ejemplo, el comando “hacer clic en imagen” , etc.

Compatibilidad de Resolución y Zoom

Si la máquina en la que se trabaja es compatible tanto con la resolución como con el zoom utilizados al momento de capturar las pantallas en la referencia de virtualización, se deben seguir las siguientes consignas para asegurar una migración exitosa de los bots:

- **Registro de Comandos**
  Al grabar un comando en el entorno de virtualización, las imágenes se almacenarán en una carpeta específica dentro del directorio de Rocketbot, bajo el nombre correspondiente al bot, en la ruta Rocketbot/robots. Esta carpeta es crucial, ya que las imágenes se utilizan como comandos en Rocketbot Studio, tales como “hacer clic en imagen” y “esperar por imagen”.

- **Migración del Archivo .db**
  Para completar la migración del bot, es imprescindible transferir también el archivo .db. Este archivo es un componente básico del proceso de migración.

Consideraciones Finales

Asegurarse de seguir meticulosamente los pasos anteriores es esencial para lograr una migración exitosa de los bots de virtualización.

Una correcta transferencia de los componentes no solo garantizará que el bot funcione adecuadamente en su nuevo entorno, sino que también optimizará su rendimiento y facilitará futuras actualizaciones.

Adoptar un enfoque riguroso en este proceso es clave para minimizar cualquier inconveniente y asegurar un despliegue eficiente.

En caso de no entender algún concepto relacionado con la virtualización en Rocketbot Studio, se recomienda consultar la documentación : Documentación de Virtualización en Rocketbot.

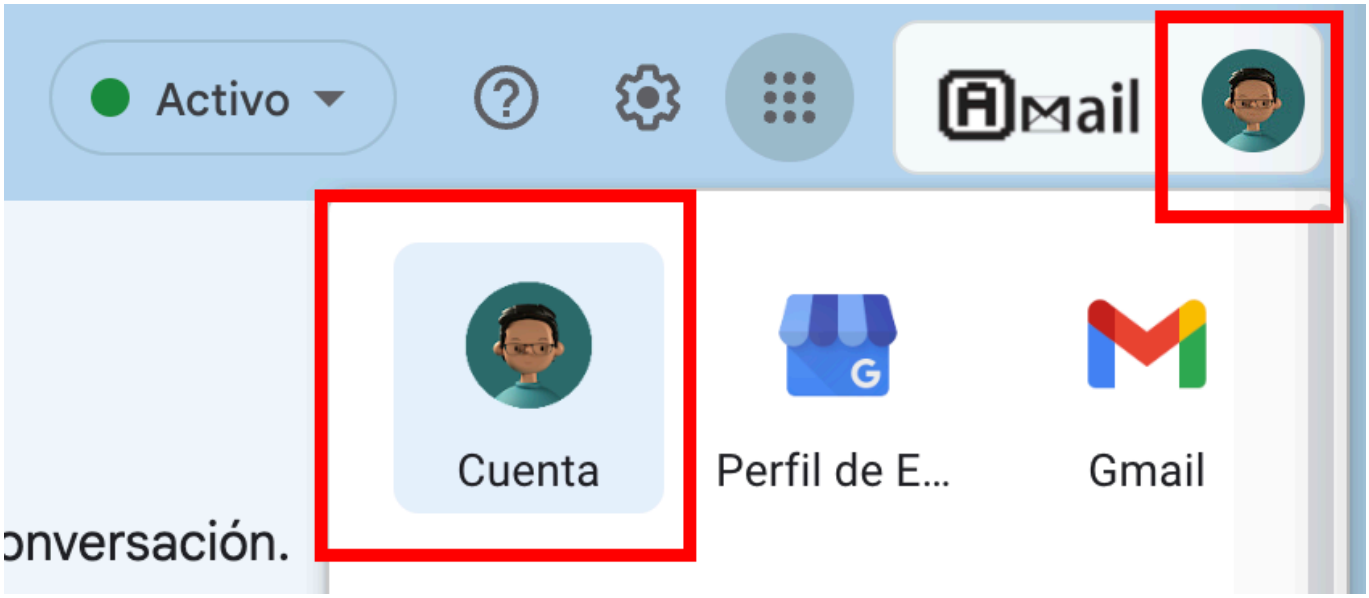
Crear contraseña de aplicación para Gmail

Una contraseña para una aplicación es un password de 16 letras que Google almacena en su cuenta y que da acceso al sistema sin necesidad de que se produzca una verificación en dos pasos.

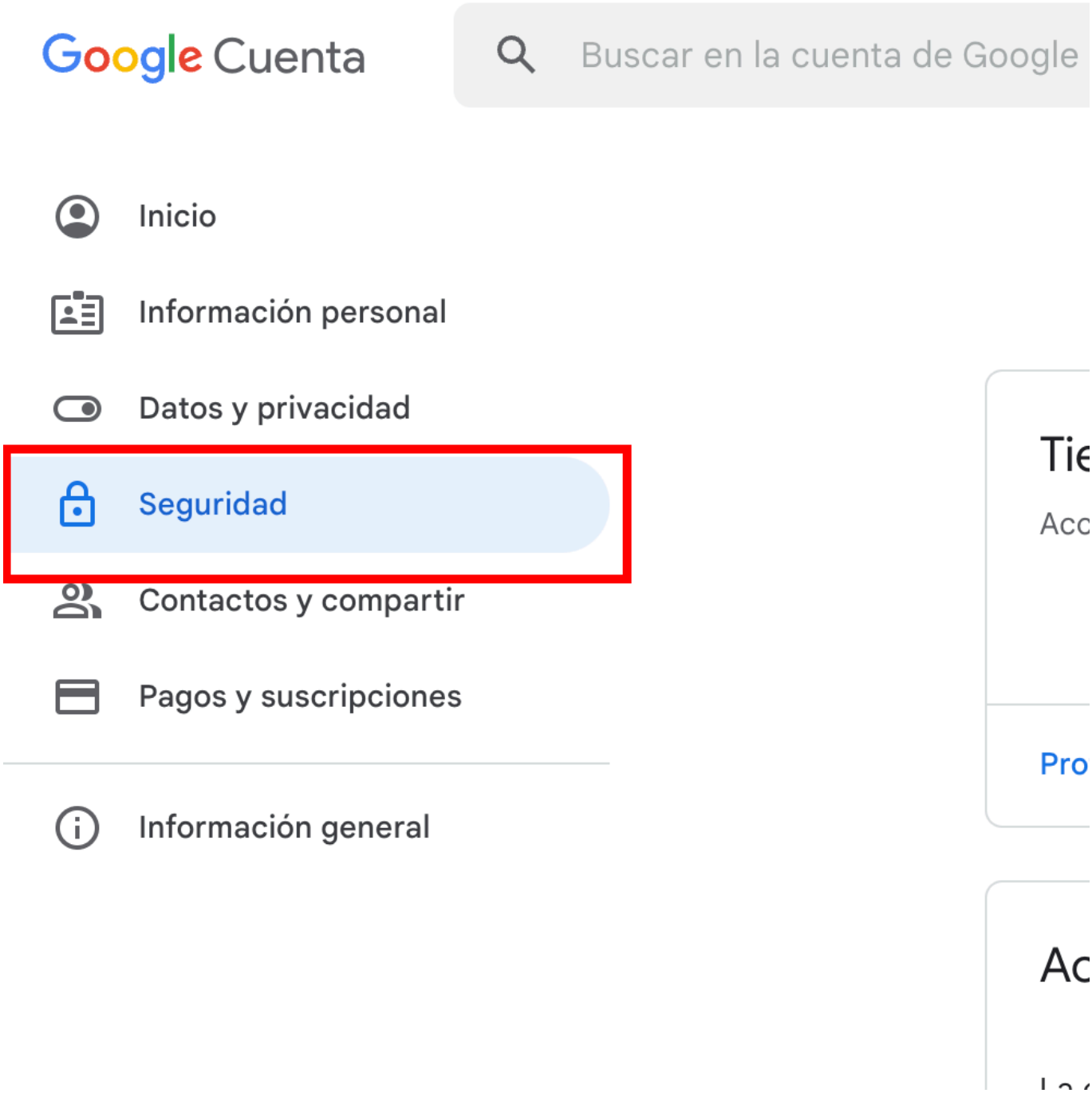
Para su configuración es necesario cumplir tener activo la verificación de segundo factor 2FA. En el caso de no tenerlo activado, no podrá crear una contraseña de aplicación. Para ello debemos de cumplir los siguientes pasos:

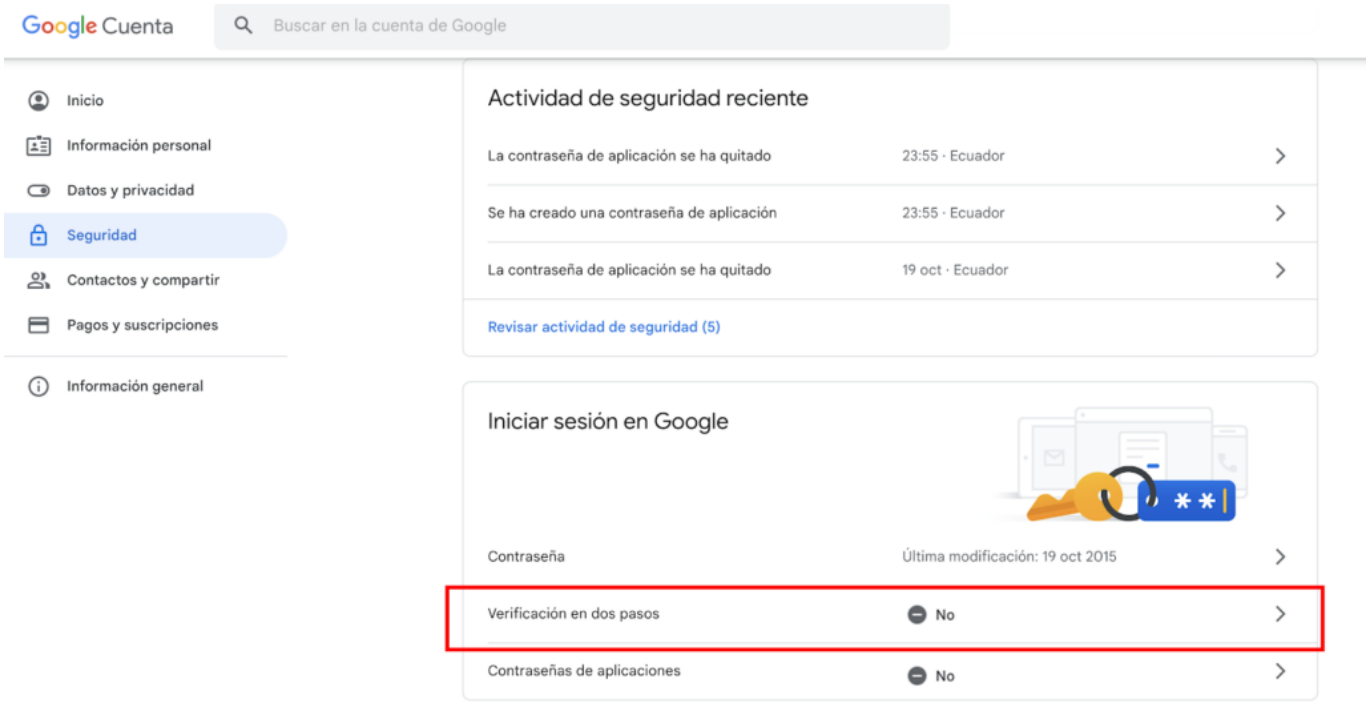
Primer Paso .- Activar verificación de segundo factor.

Lo primero que debes hacer es iniciar sesión en tu cuenta de Gmail, una vez conectado a tu cuenta, accede al menú de configuraciones. Lo encuentras en la parte superior derecha del navegador, en el círculo con tu avatar, luego debes elegir la opción «Cuenta de Google«

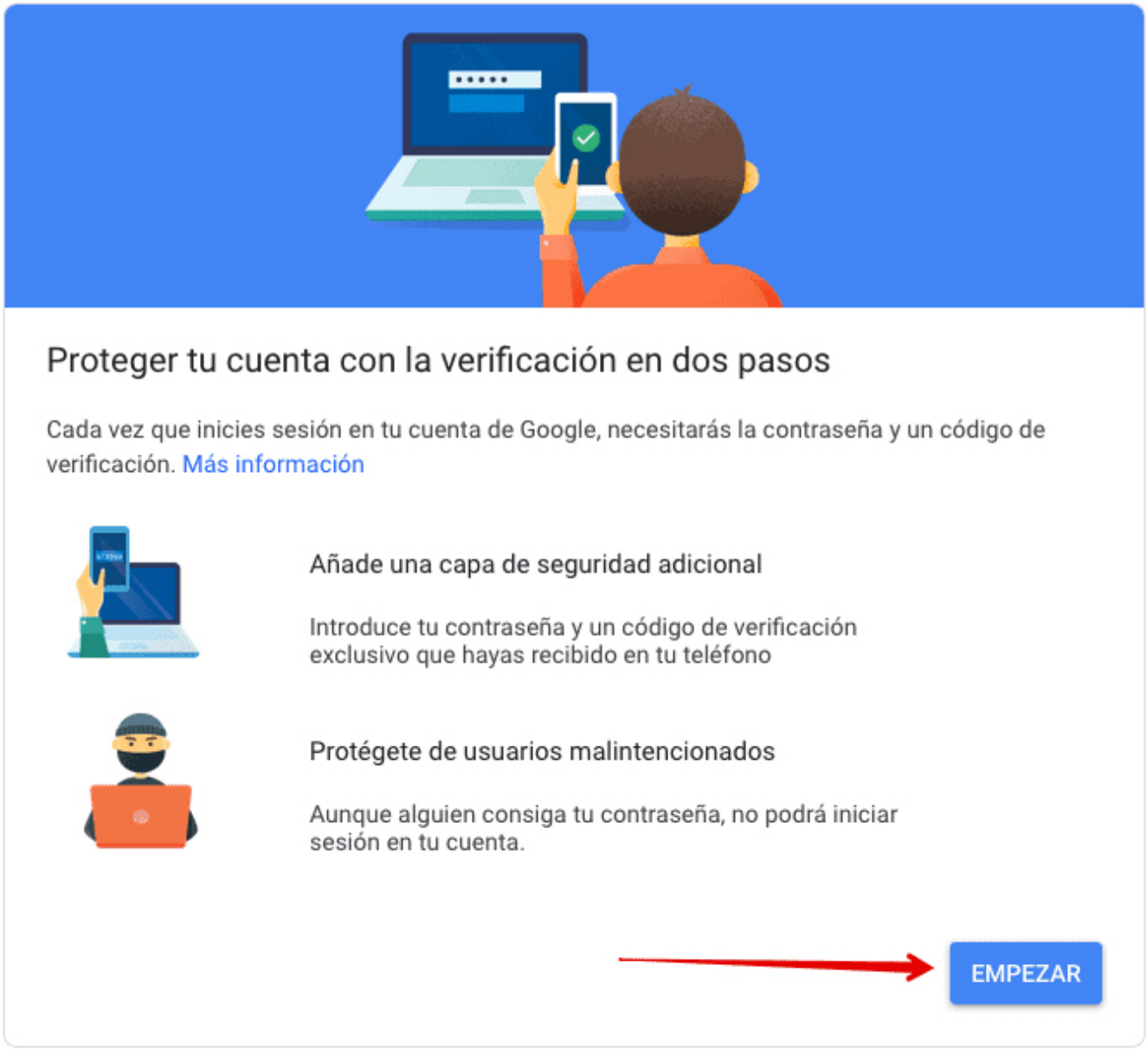


Te llevará a una pantalla de configuración de tu cuenta, donde tendrás que acceder al menú lateral»Seguridad»:



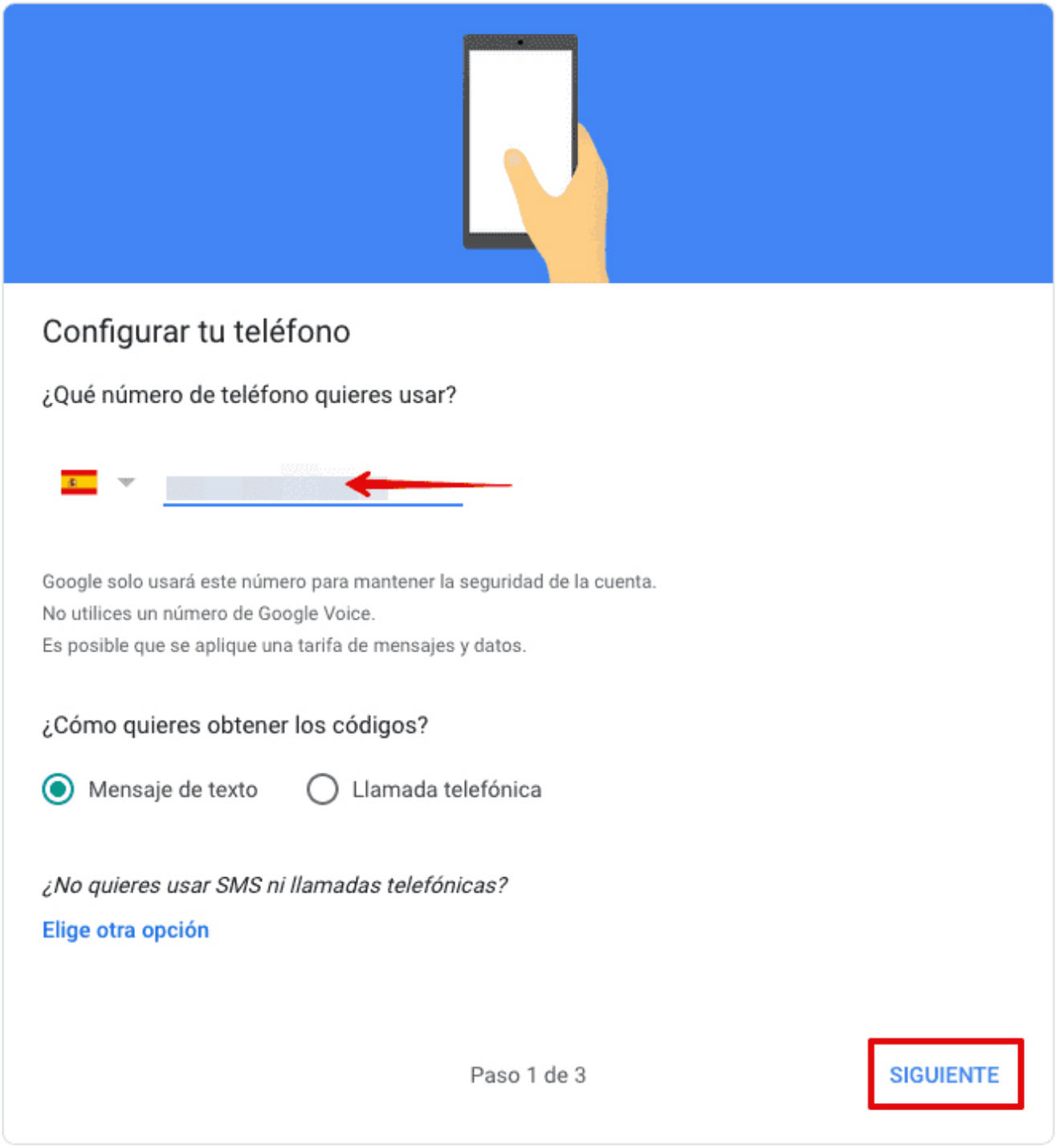


Verás una breve explicación sobre el doble factor de autenticación. Para iniciar este proceso haz clic en el botón «Empezar».

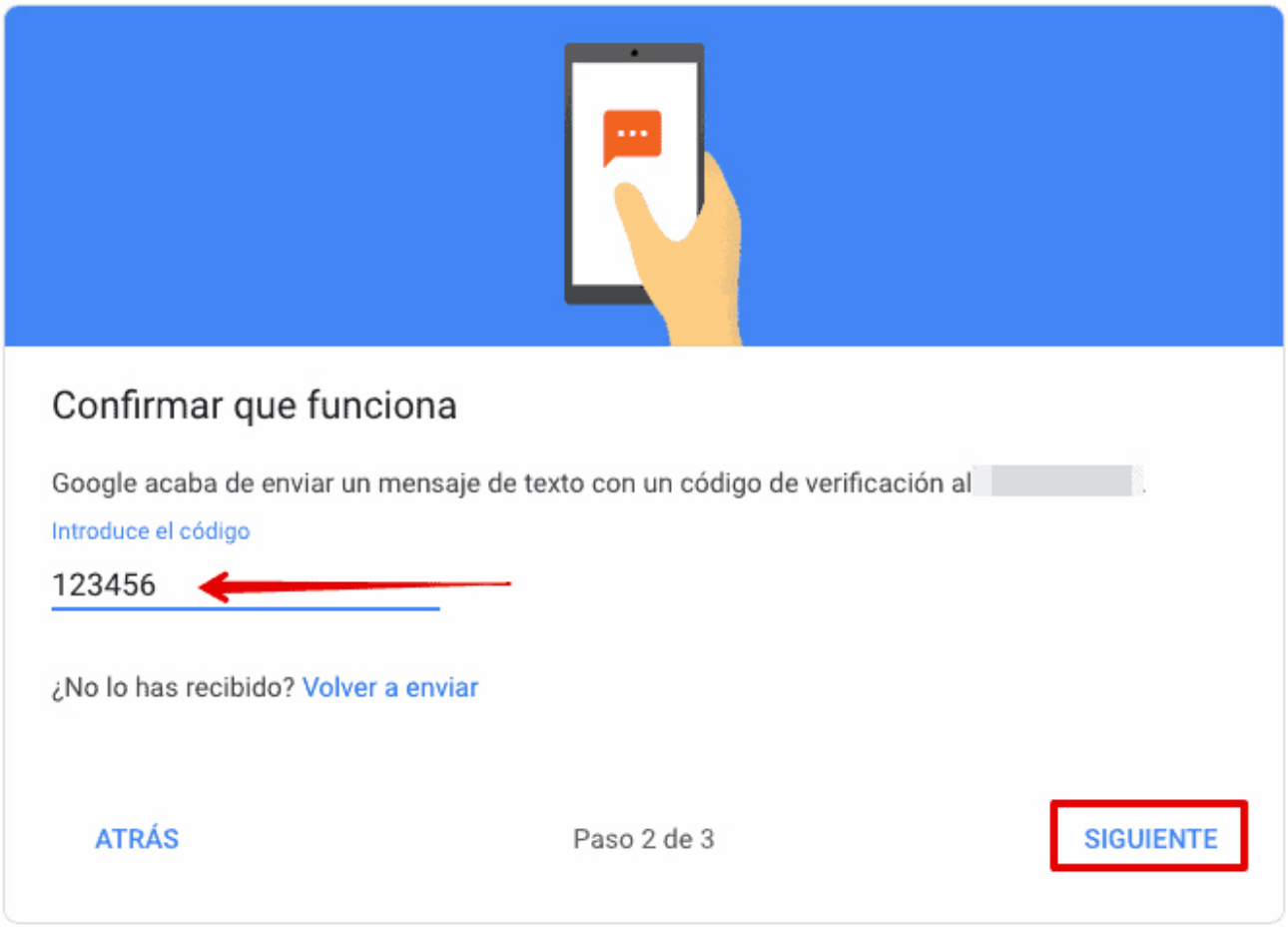


Vuelve a indicar la contraseña de tu cuenta en Google y haz clic en «Siguiente«:

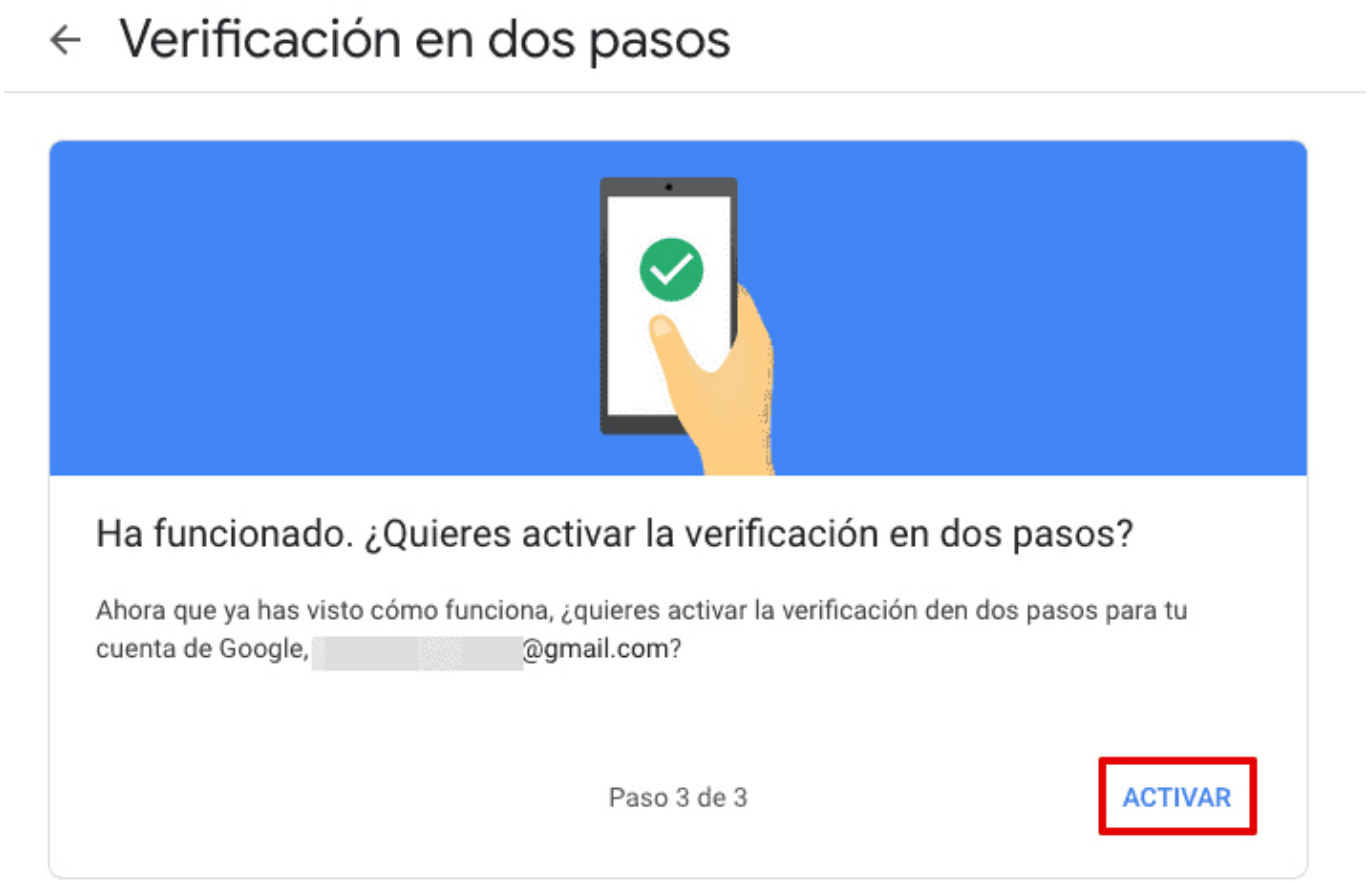
Introduce tu número de teléfono y la forma que deseas recibir los códigos, a continuación pulsa en «Siguiente«:



Google te enviará los códigos de confirmación. Introduce tu código, a continuación pulsa en «Siguiente«:



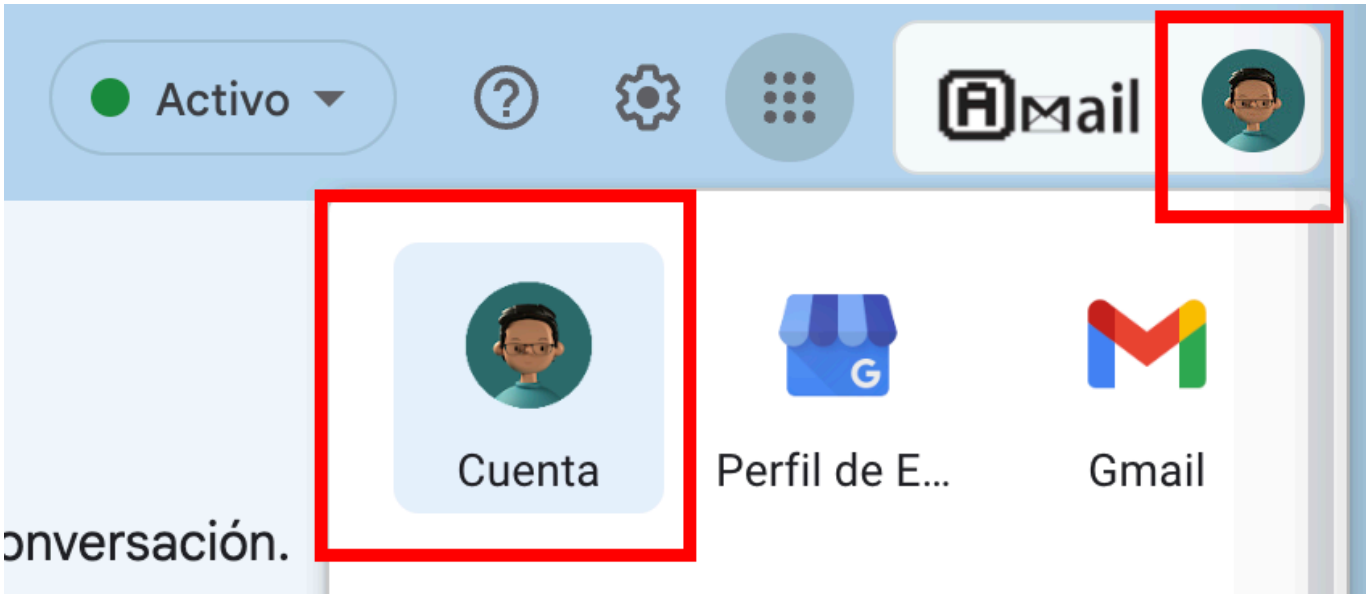
Una vez confirmado tu número de teléfono, puedes empezar a configurar el 2FA, para ello haz clic en «Activar«:



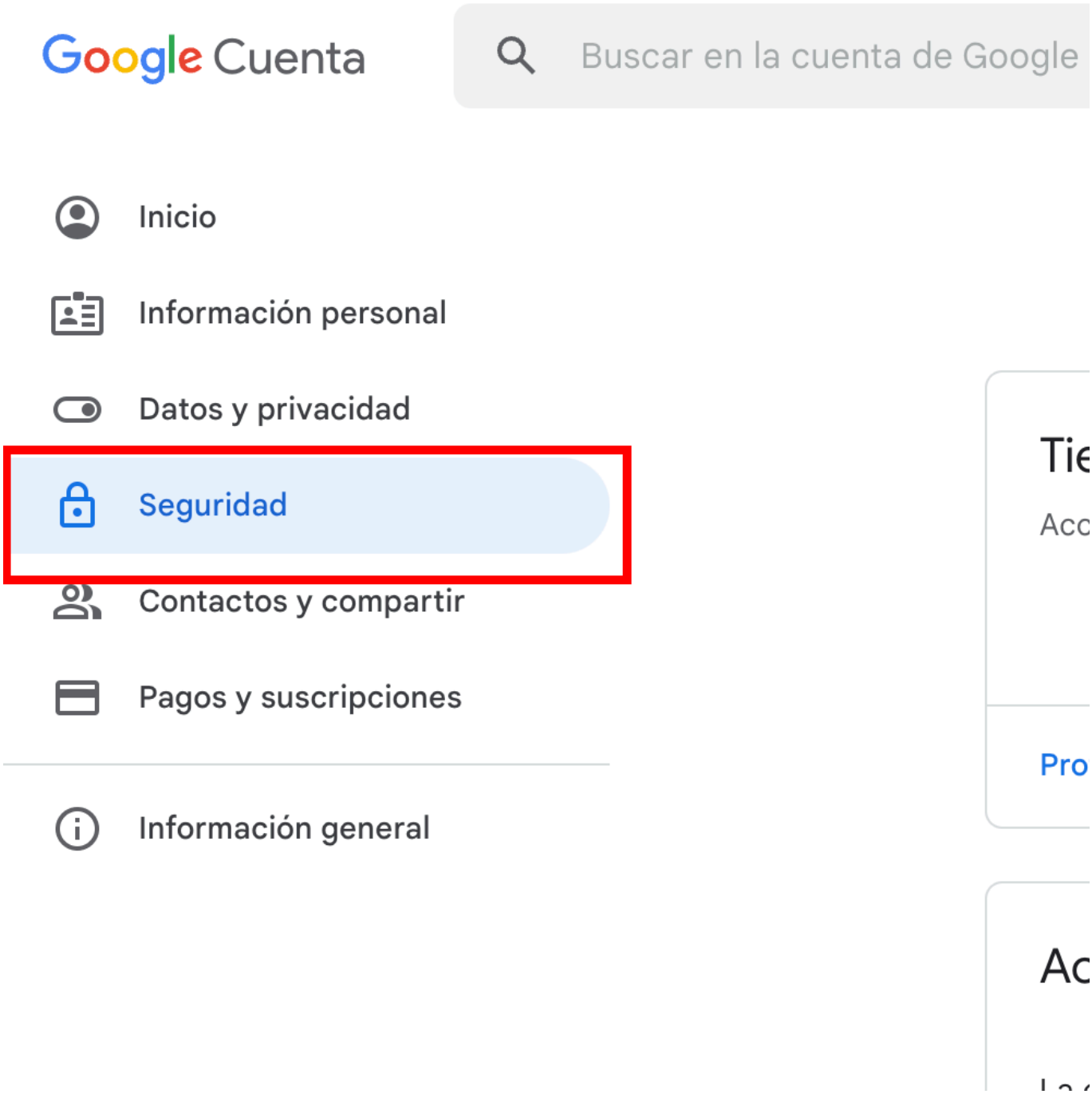
Listo, su cuenta de gmail.com es segura y cuenta con una segunda capa de seguridad para acceder a su correo.

Segundo Paso .- Configurar una contraseña de Aplicación

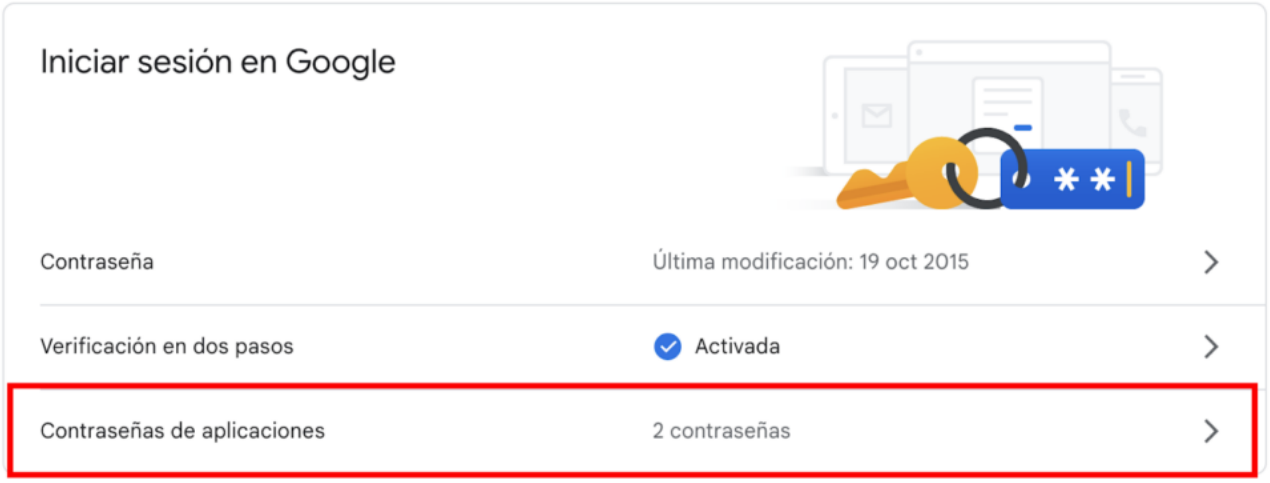
La contraseña de aplicación se encuentra en la misma sección de Gestionar tu cuenta.



En la parte media de la página, en la sección iniciar sesión en google, encontrarás una parte donde pone contraseñas de aplicación: ninguna. Haz clic en ninguna o en la flecha hacia la derecha

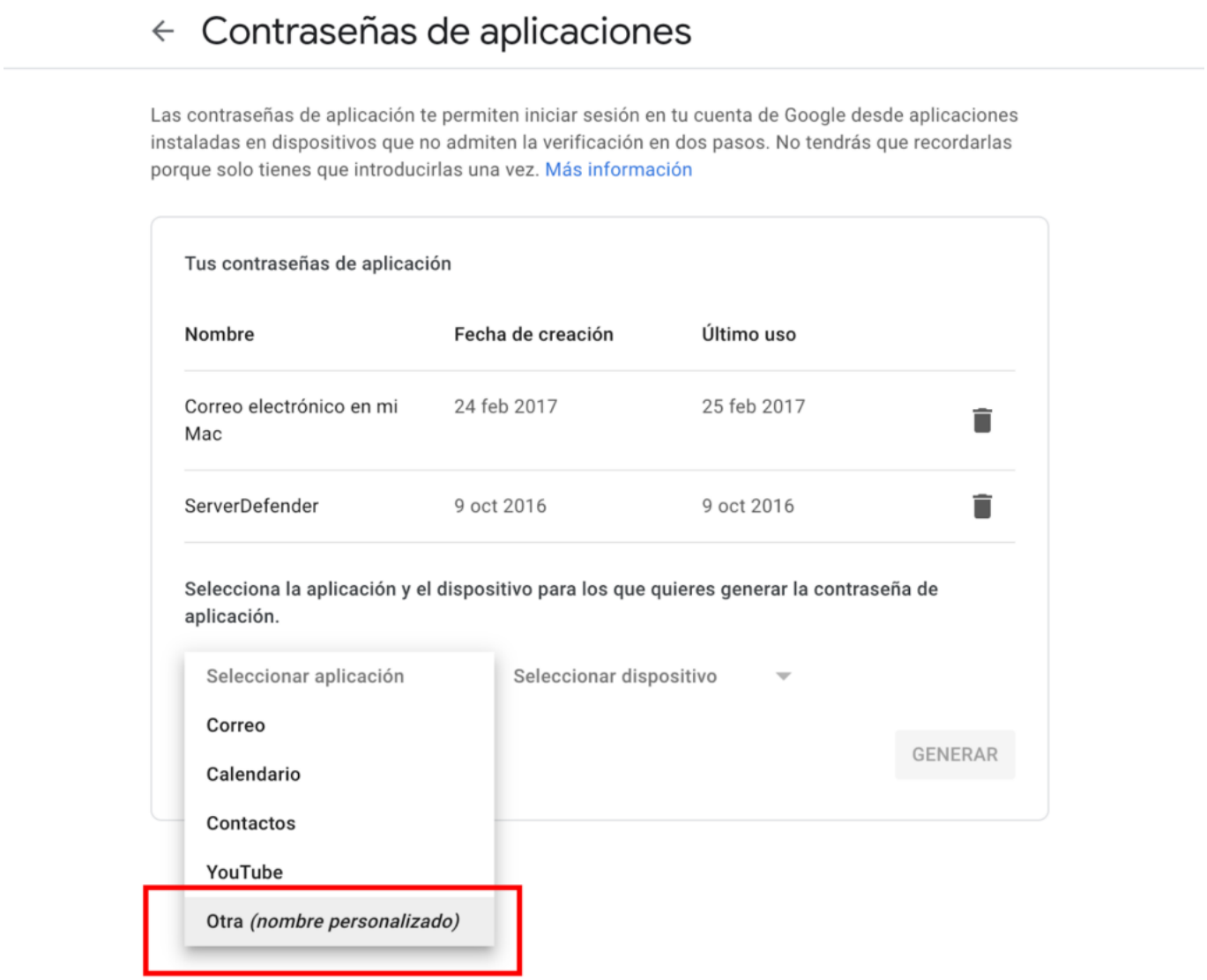


En esta imágen de referencia notamos que ya existen 2 contraseñas de aplicación creadas, pero en el caso de no tener ninguna contraseña creada se mostrará la palabra NInguna.

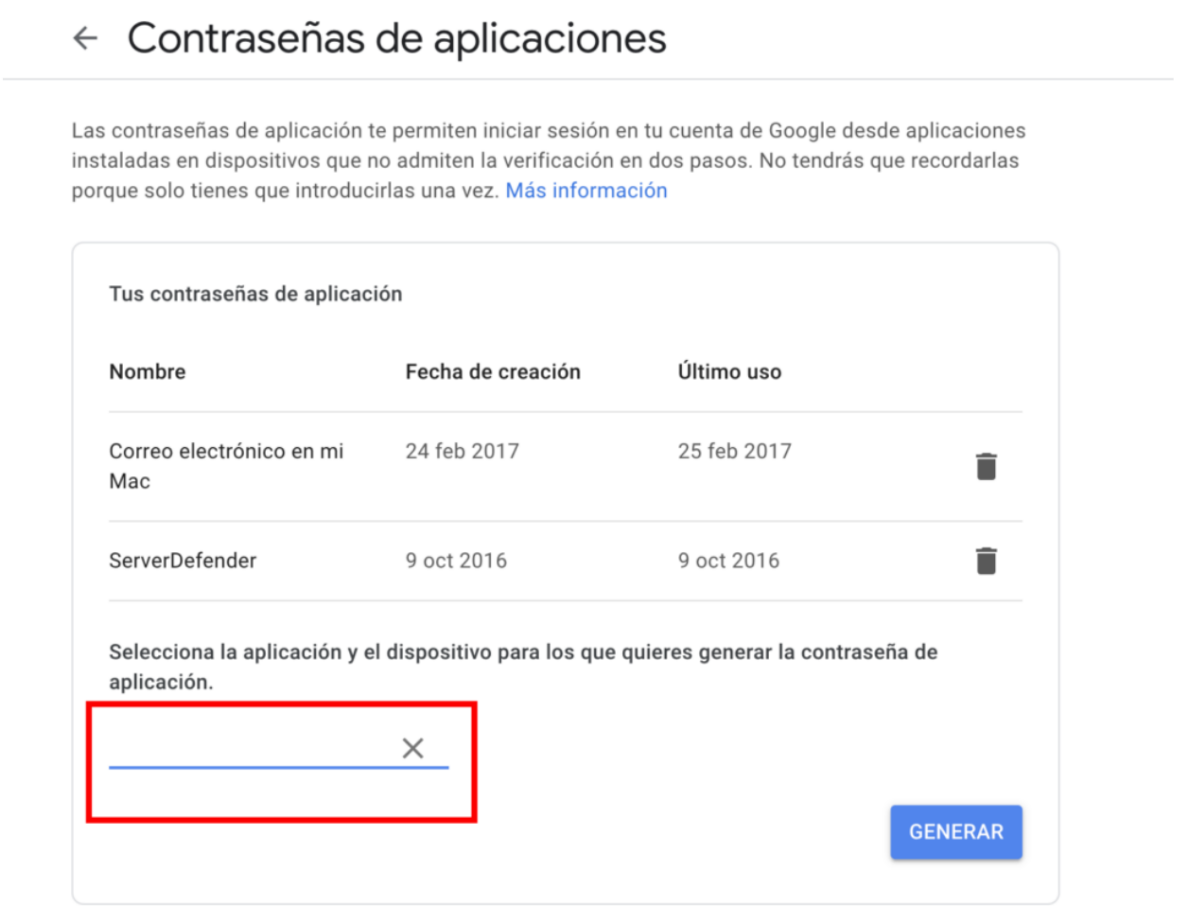


En la siguiente pantalla pedirá que vuelvas a poner tu contraseña, por seguridad. Debes poner tu contraseña actual. No se va a cambiar, vamos a crear una especial. Una vez pongas tu contraseña, la siguiente pantalla es la que permite crear la nueva contraseña de aplicación

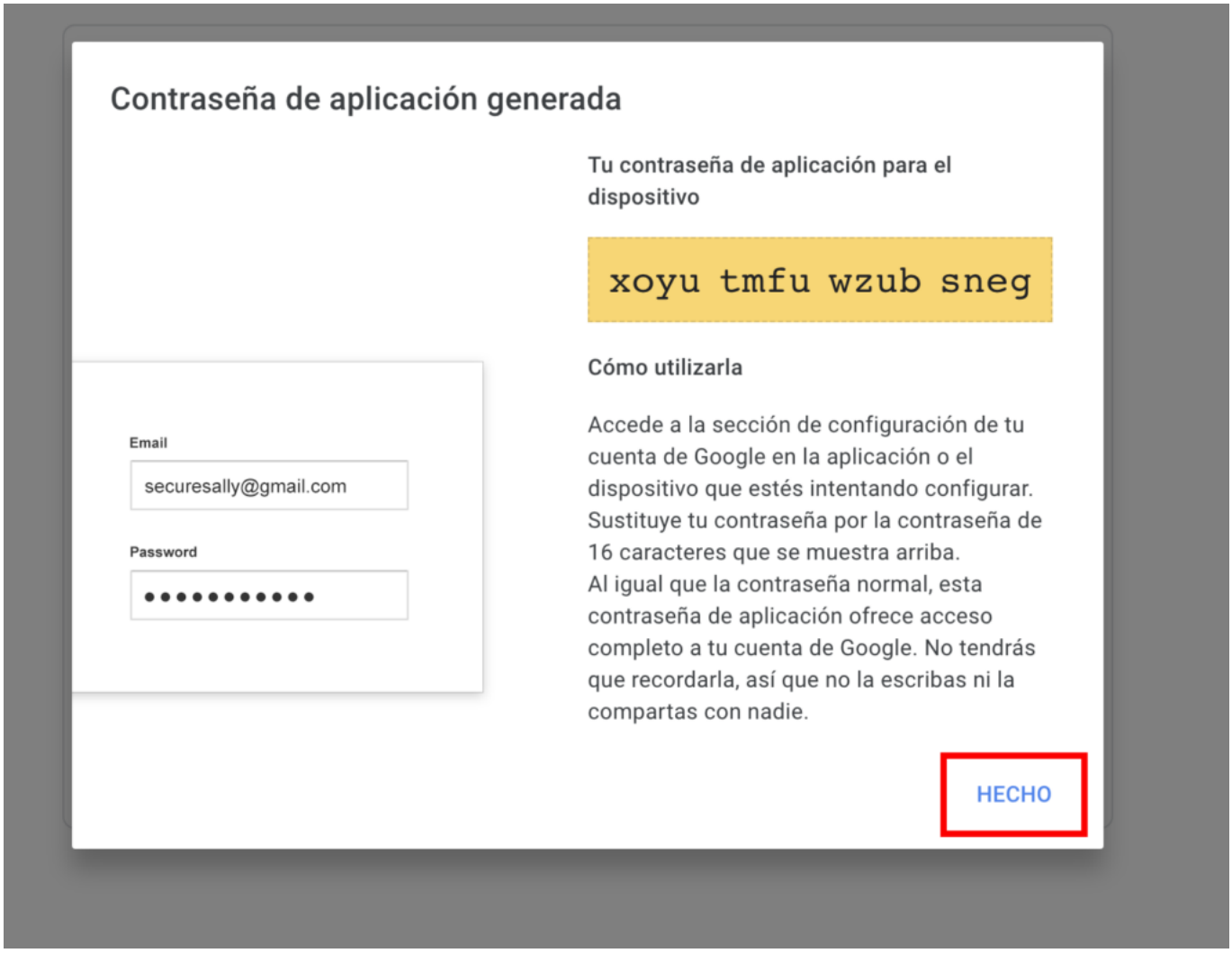
Puedes seleccionar en Otros (nombre personalizado) con la finalidad de asignarle un nombre.



Al dar clic , debemos colocar el nombre y pulsa el botón generar



Ahora por fin has creado una nueva contraseña de aplicación exclusiva para enviar emails desde cualquier App . Solamente, no sustituye a tu contraseña de gmail.



Datos para Configuración

Luego de crear la contraseña de aplicación, podrá configurar su cuenta en el portal. Los datos de envio son los siguiente:

1. Correo/Usuario: sucorreo@gmail.com (en el caso de google apps sería @sudominio.com)
2. Contraseña: La generada en el segundo paso.
3. Servidor SMTP : smtp.gmail.com
4. Puerto: 587
5. TLS : SI
6. Autenticación SMTP : SI

Aqui estan los links de los modulos donde se pueden ejecutar estas acciones :

Email Advaced : https://market.rocketbot.com/module/emailAdvanced

Gmail : https://market.rocketbot.com/module/gmail_

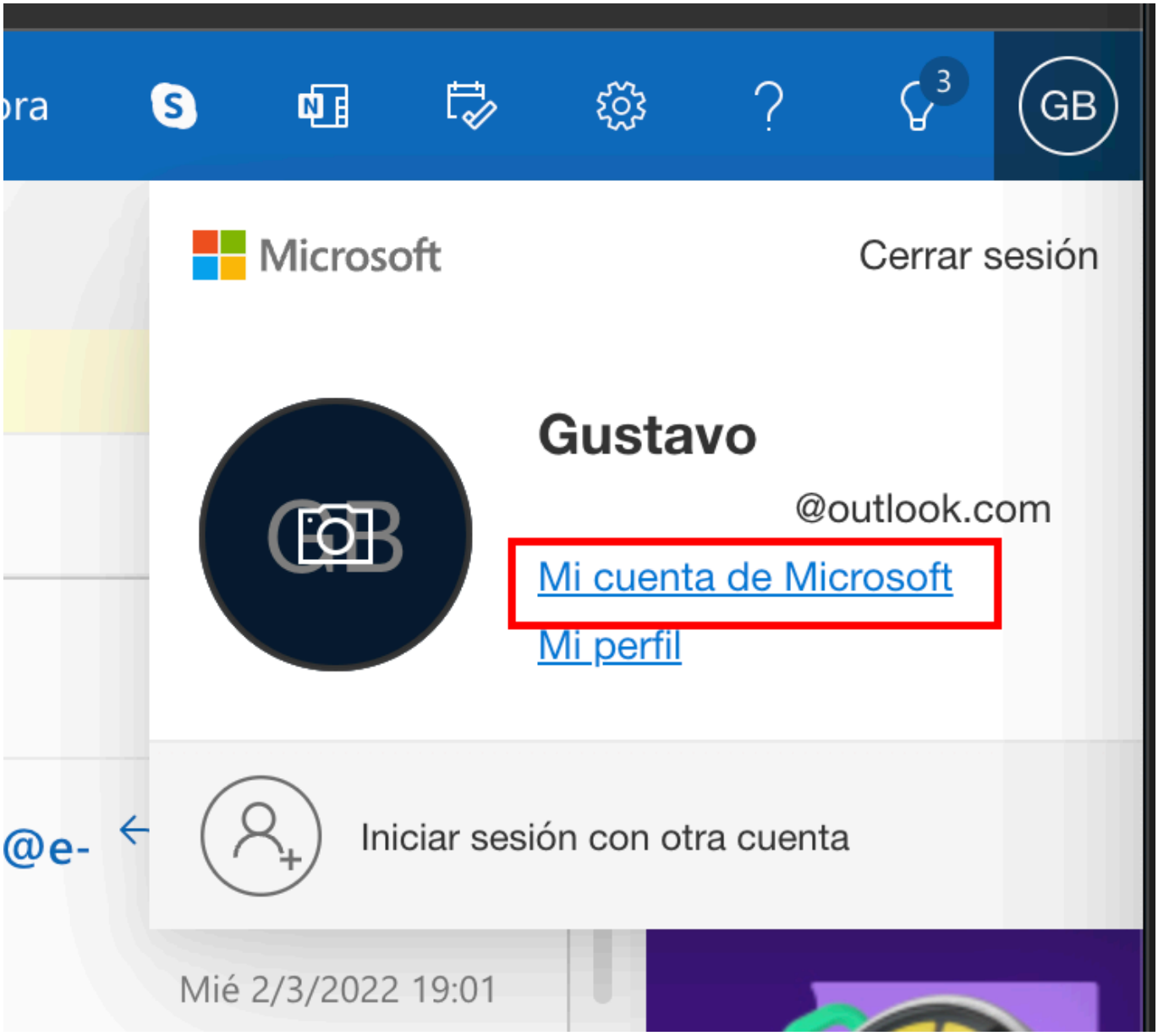
Crear contraseña de aplicación para Outlook

Una contraseña para una aplicación es un password que Outlook almacena en su cuenta y que da acceso al sistema sin necesidad de que se produzca una verificación en dos pasos.

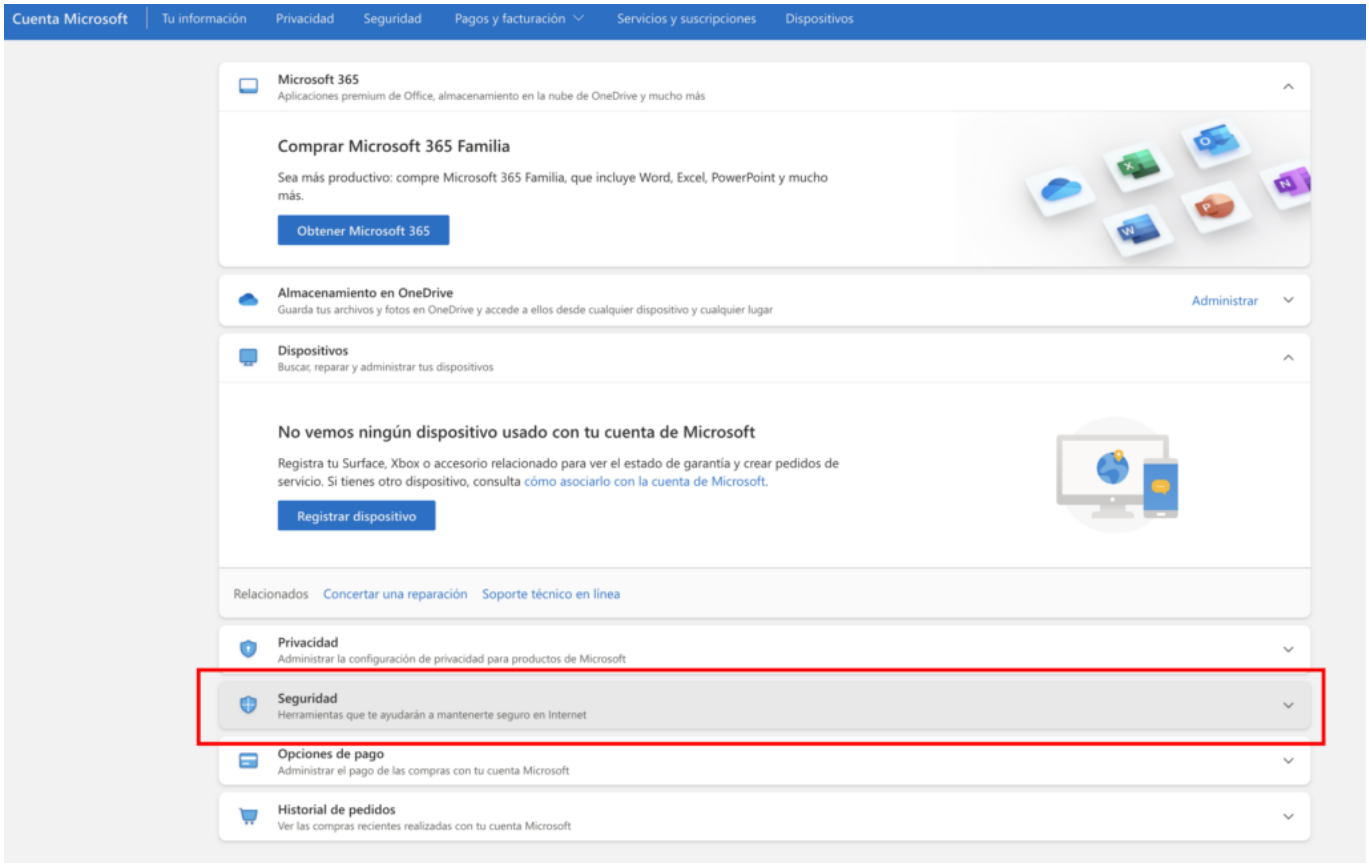
Para su configuración es necesario cumplir tener activo la verificación de segundo factor 2FA. En el caso de no tenerlo activado, no podrá crear una contraseña de aplicación. Para ello debemos de cumplir los siguientes pasos:

Primer Paso .- Activar verificación de segundo factor.

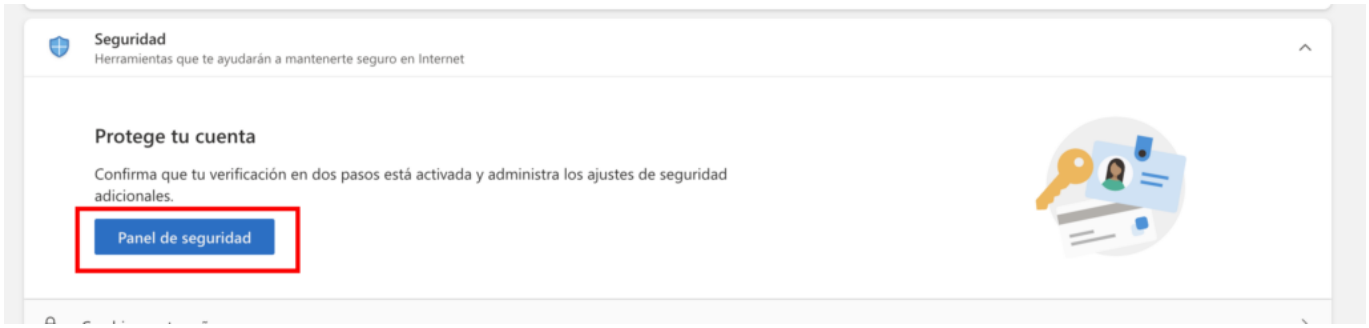
Lo primero que debes hacer es iniciar sesión en tu cuenta de Outlook, una vez conectado a tu cuenta, accede al menú de tu cuenta. Lo encuentras en la parte superior derecha del navegador, en el cícurlo con tu avatar, luego debes elegir la opción «Mi cuenta de Microsoft«



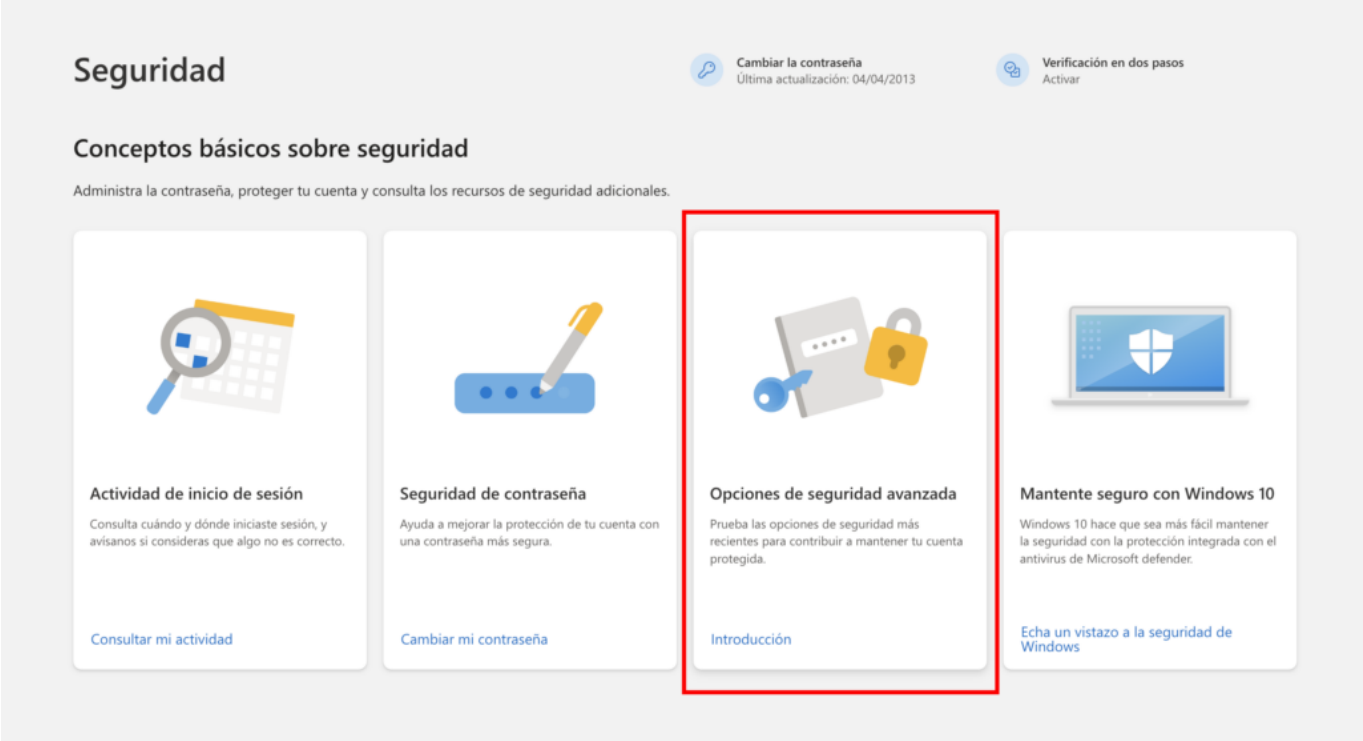
Te llevará a una pantalla, donde tendrás que acceder a la opción de »Seguridad»



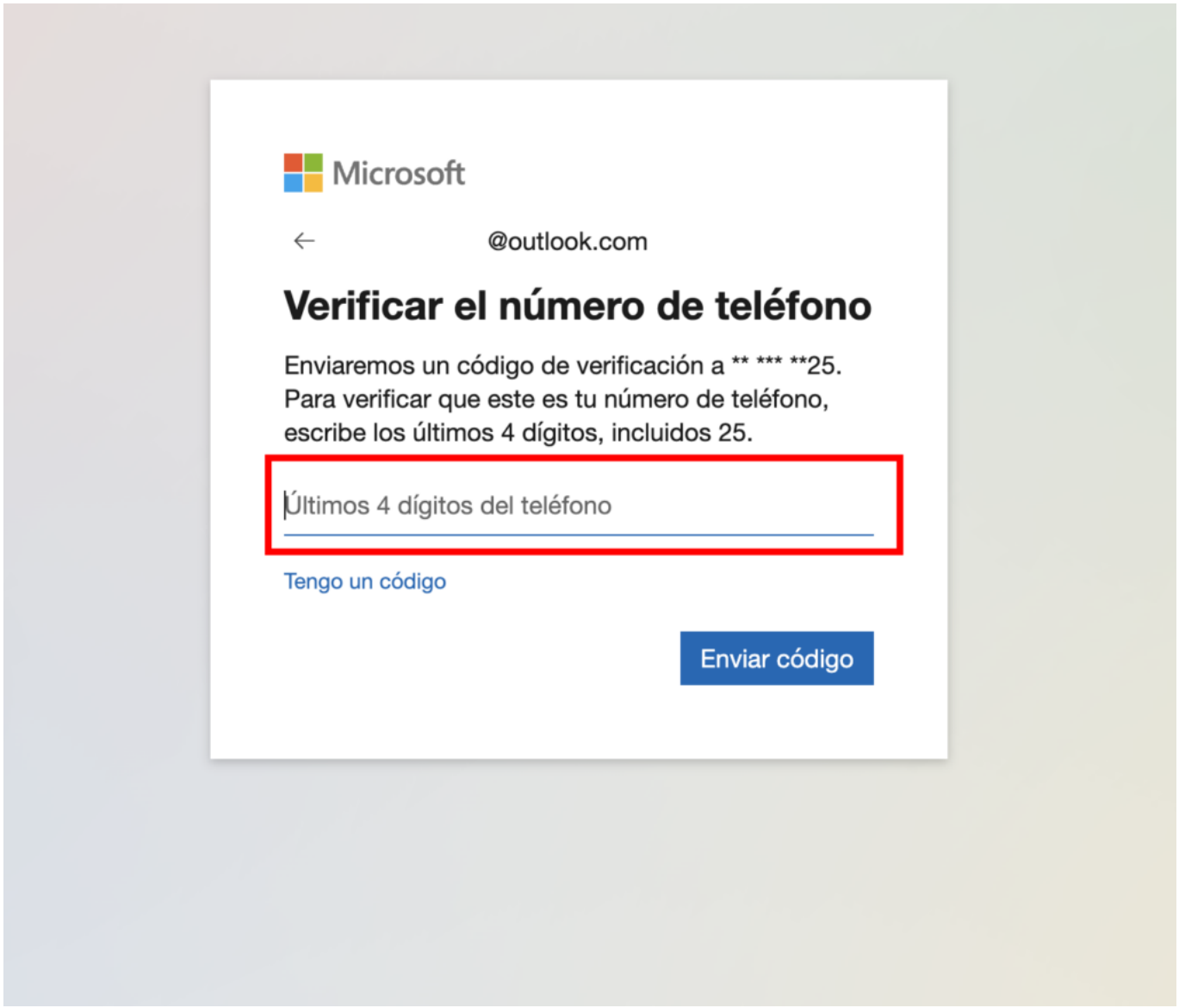
Al presionar te mostrará una opción para acceder presionando en el botón de »Panel de seguridad»:



Serás redireccionado al panel de Seguridad, donde podrás ver las opciones de conceptos básicos. Para iniciar este proceso haz clic en la opción **«Opciones de seguridad avanzada».**



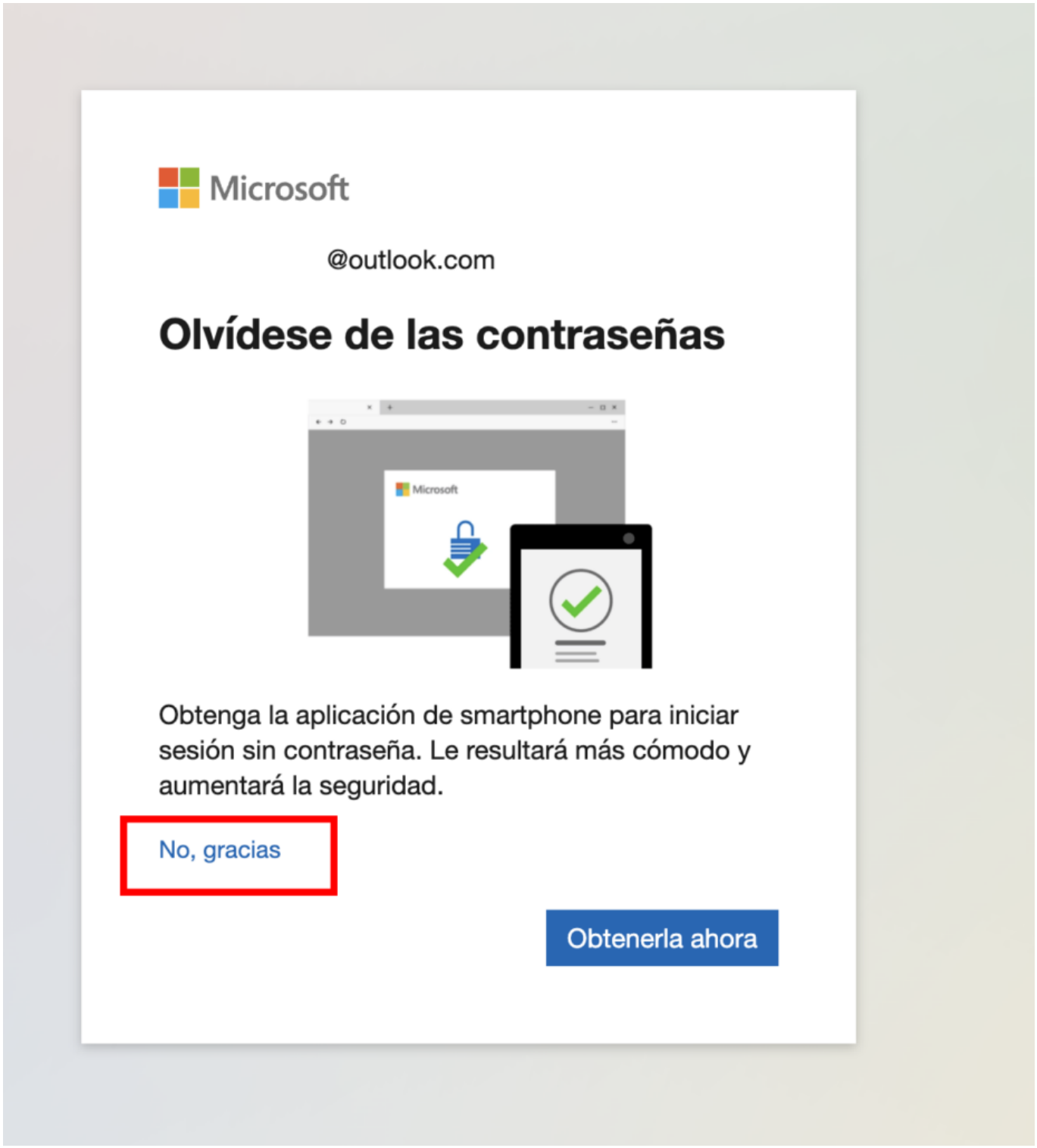
Luego de eso se le pedirá que confirme el número de telefono asociado a su cuenta, por lo cual debe ingresar los 4 últimos digitos para continuar.



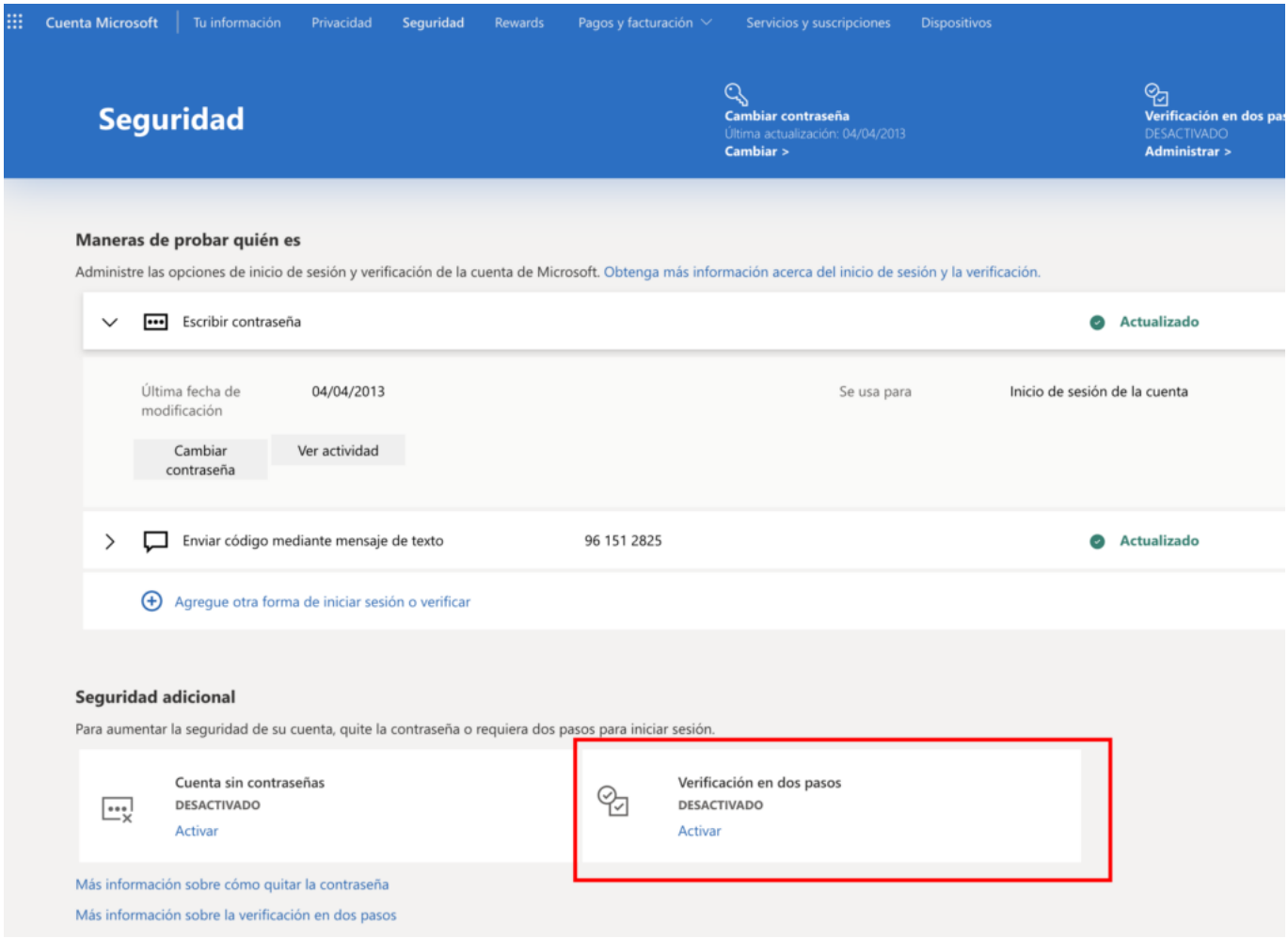
Con la finalidad de poder explicar el método más siemple para la verificación de segundo factor, escogeremos la opción de «**No, gracias**» del panel de opciones.

Importante:

Cómo alternativa Outlook le ofrecerá utilizar su aplicación móvil para generar las contraseñas. Puede optar por ese procedimiento en el caso de que desee.



Al finalizar, se nos mostrará la siguiente pantalla de Seguridad, en donde podrá notar que la **Verificación en dos pasos** se encuentra **DESACTIVADA** , por lo que procedemos a dar clic en **«Activar»**

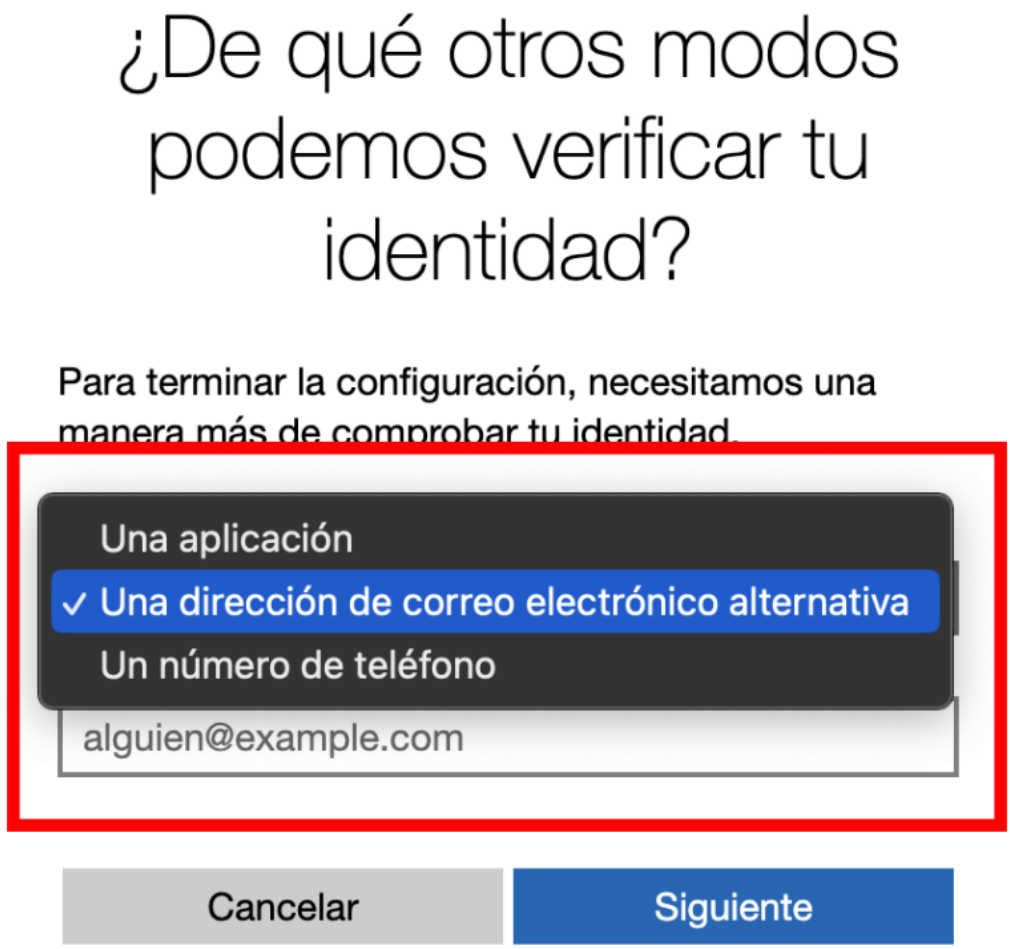


Al dar clic en la opción de Activar, se nos mostrará un nuevo cuadro de dialogo con diferentes opciones para verificar el acceso a la cuenta.

Usted puede escoger cualquiera de las 3 opciones que muestran a continuación. A continuación escogeremos la forma más sencilla de verificación de correo el cual es **Una dirección de correo electrónico alternativa.**

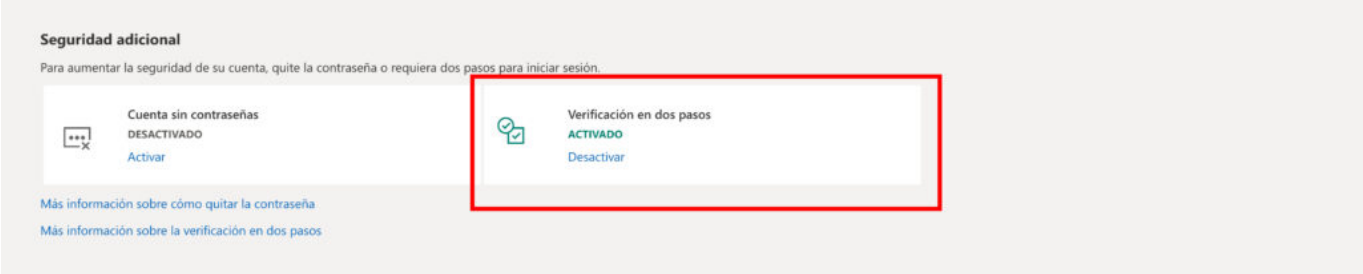
Importante:

Puede también escoger la opción de aplicación el cual le pedirá tener instalado una aplicación móvil. Ejemplo: Microsoft Authenticator o Google Authenticator.



Luego de colocar la cuenta de correo solo debe dar clic en siguiente y recibirá un email indicando la clave que debe agregar para validar su cuenta.

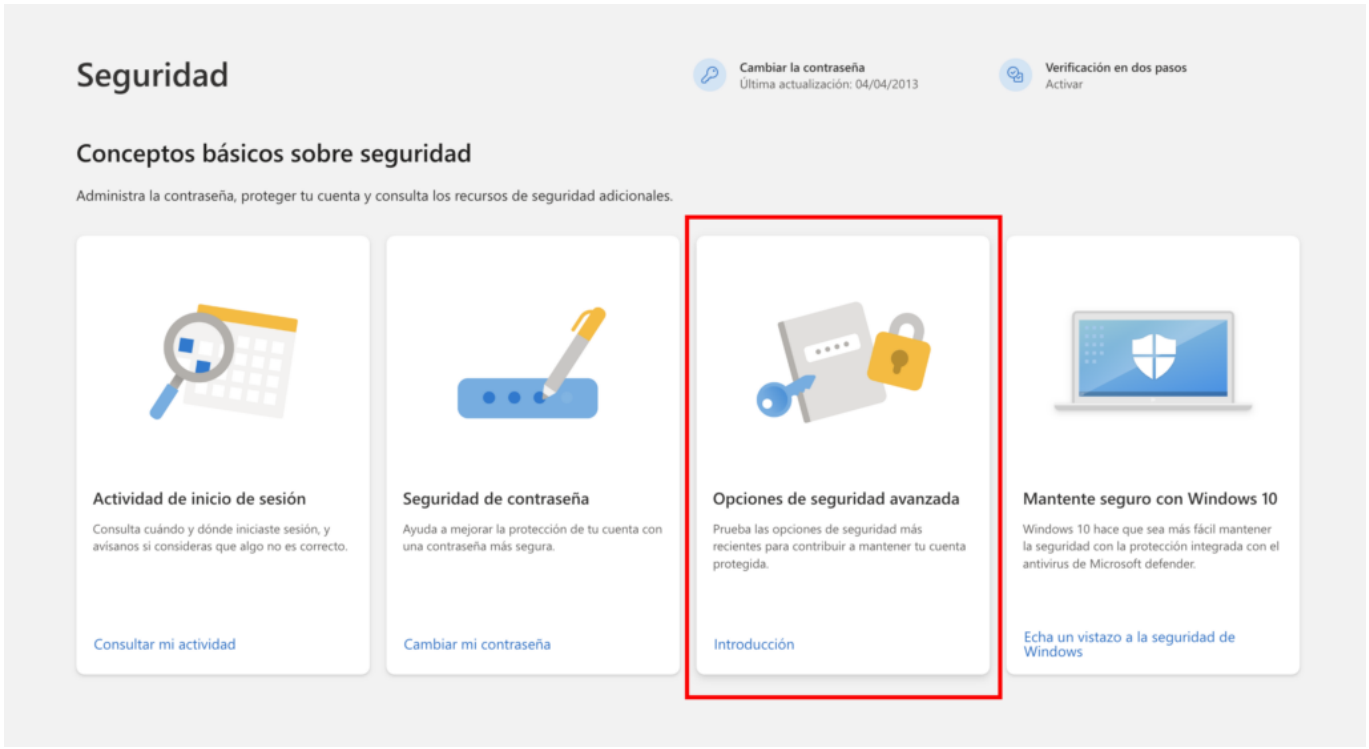
Luego de confirmar el código, su cuenta tendrá activada la **Verificación de dos pasos.**



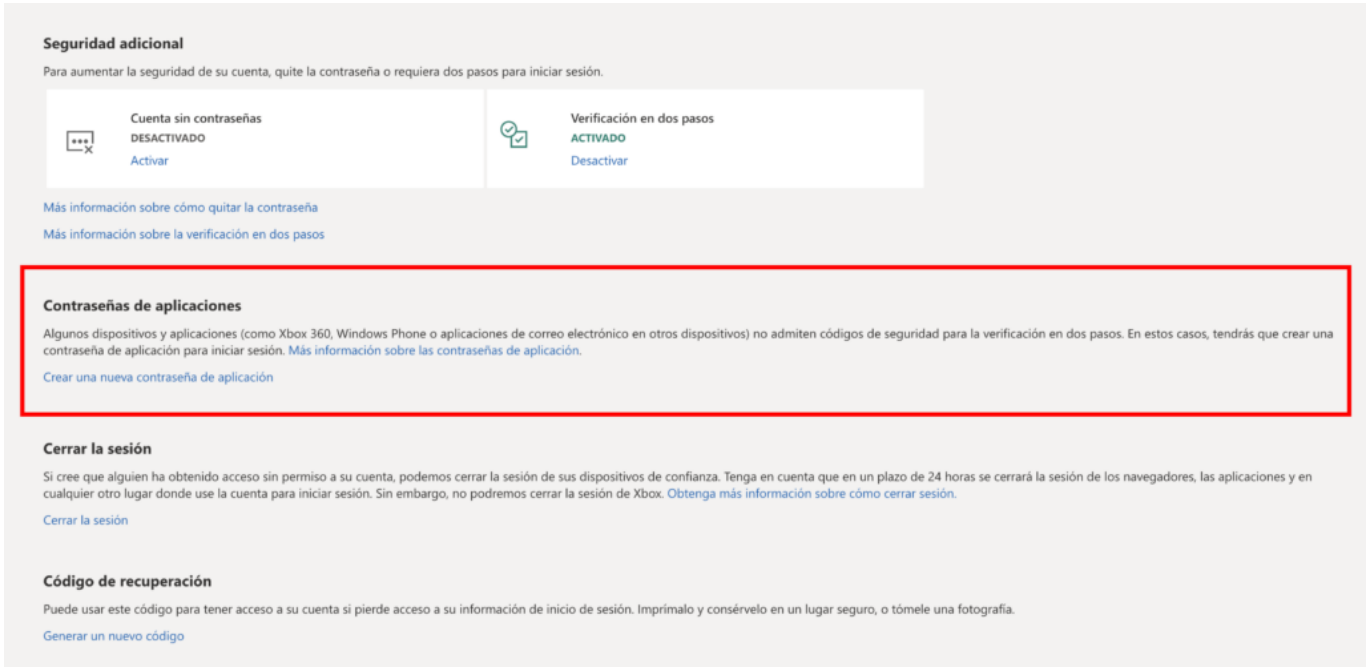
Segundo Paso.- Configurar una contraseña de Aplicación

Para crear una nueva contraseña de aplicación para una aplicación o dispositivo, sigue los pasos que se indican a continuación. Puedes repetir estos pasos de creación de una contraseña de aplicación para todas las aplicaciones o dispositivos que necesites.

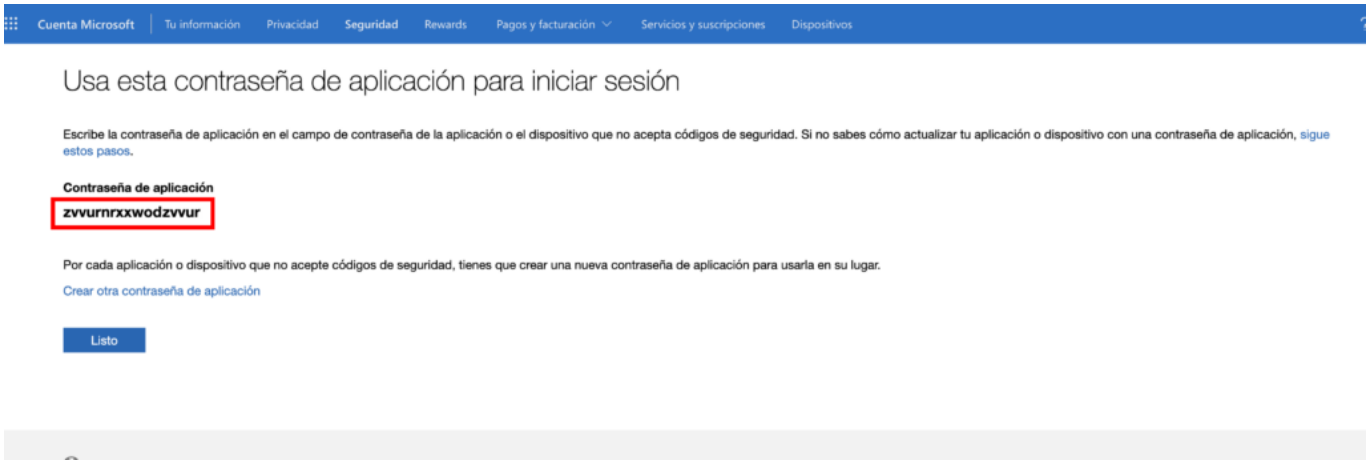
Dirígete a la página Conceptos básicos sobre seguridad e inicia sesión en tu cuenta de Microsoft y seleccionamos **«Opciones de Seguridad».**



En **Contraseñas de aplicación**, selecciona **«Crear una nueva contraseña de aplicación»**.



Se genera una nueva contraseña de aplicación que aparece en la pantalla.



Datos para Configuración

Luego de crear la contraseña de aplicación, podrá configurar su cuenta en el portal. Los datos de envio son los siguiente:

1. Correo/Usuario: sucorreo@outlook.com (en el caso de Office365 sería @sudominio.com)
2. Contraseña: La generada en el segundo paso.
3. Servidor SMTP : **outlook.office365.com**
4. Puerto: **587**
5. TLS : **SI**
6. Autenticación SMTP : **SI**

Aqui estaran disponibles los links a los modulos donde se puedan aplicar estas acciones :

Email Advanced : https://market.rocketbot.com/module/emailAdvanced

Outlook 365 : https://market.rocketbot.com/module/Outlook365

Rocketbot Transaction Framework

RTFramework de Rocketbot es una plantilla que organiza proyectos RPA en módulos reutilizables. Gestiona transacciones y excepciones, asegurando robustez, mantenibilidad y escalabilidad en la automatización de procesos.

Click relativo en Objeto

Haga clic en un objeto usando sus coordenadas relativas desde su elemento más cercano

---

Arrastrar a la imagen

Hace clic donde está el mouse y arrastra a una posición específica mientras lo sostiene.

Mover a la imagen

Mueve el mouse a una imagen específica.

Ejecutar archivo Powershell

Abra y ejecute el archivo '.ps1'

Ejecutar archivo de script de Visual Basic

Abre y ejecuta el archivo '.vbs' pasando los argumentos necesarios

---

Obtener Proceso

Obtiene los procesos que coincidan con el filtro.