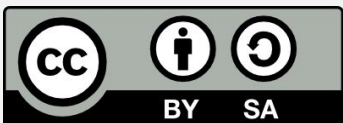


AUTENTICACIÓN DE DOS FACTORES EN GOOGLE (GMAIL) USANDO UNA LLAVE DE SEGURIDAD DE YUBICO



Esta obra está bajo una [Licencia Creative Commons Atribución-CompartirIgual 4.0 Internacional](https://creativecommons.org/licenses/by-sa/4.0/).

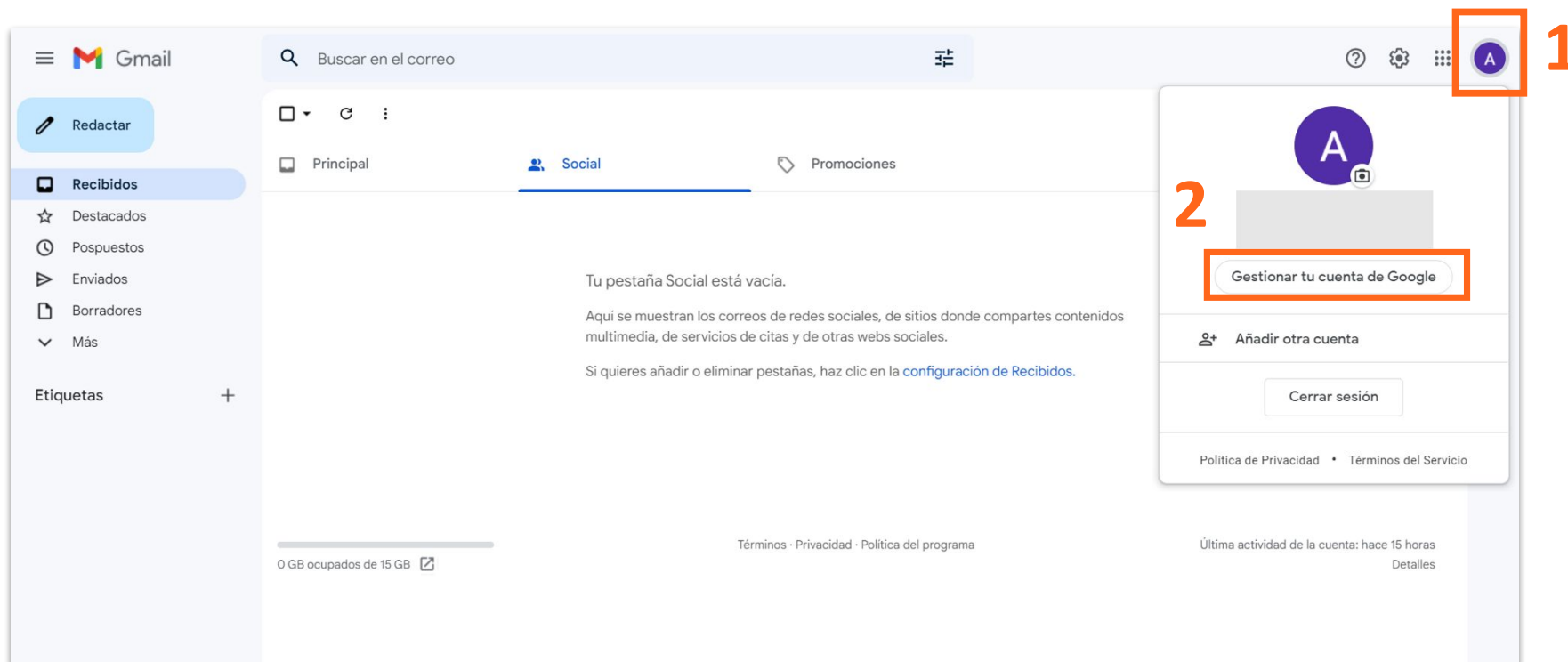
Última actualización: septiembre 2023

ACTIVAR 2FA EN GOOGLE (GMAIL)

¿Cómo activar la autenticación de dos factores en tu cuenta Google usando una Yubikey?

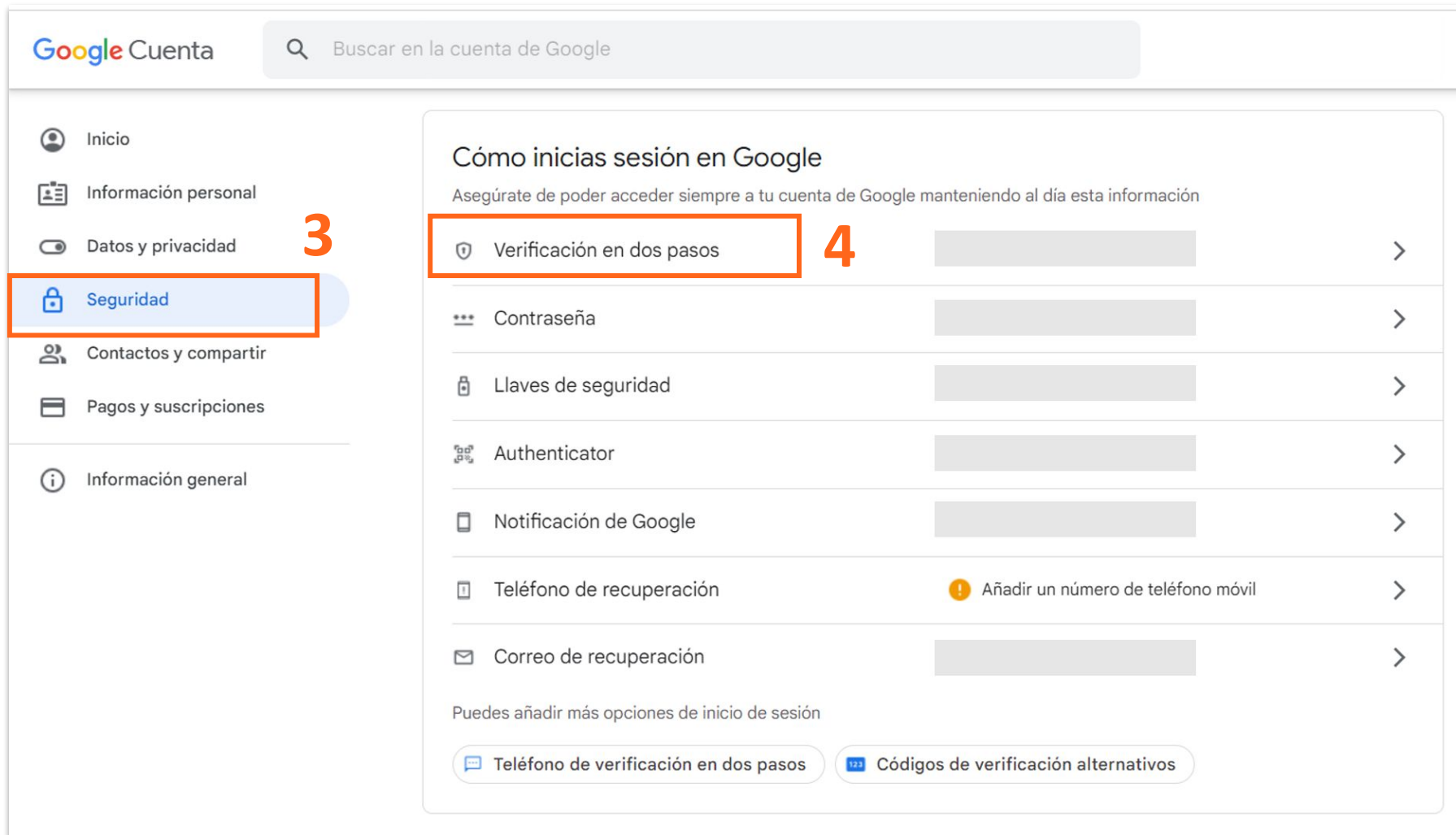
→ Ir al panel de Gestión de tu Cuenta de Google:

Bandeja de entrada del correo > Ícono de Cuenta > “Gestionar tu cuenta de Google”



ACTIVAR 2FA EN GOOGLE (GMAIL)

→ En el menú lateral izquierdo, selecciona **Seguridad** > “Verificación en dos pasos”



The screenshot shows the Google Account management interface. On the left, the 'Seguridad' (Security) menu item is highlighted with a red box and a large orange number '3'. The main content area is titled 'Cómo inicias sesión en Google' (How you sign in to Google). Within this area, the 'Verificación en dos pasos' (Two-step verification) option is highlighted with a red box and a large orange number '4'. Below this, a list of other security options is visible: Contraseña (Password), Llaves de seguridad (Security keys), Authenticator, Notificación de Google (Google notifications), Teléfono de recuperación (Recovery phone), and Correo de recuperación (Recovery email). At the bottom, there are buttons for 'Teléfono de verificación en dos pasos' (Two-step verification phone) and 'Códigos de verificación alternativos' (Alternative verification codes).

Google Cuenta

Buscar en la cuenta de Google

Inicio

Información personal

Datos y privacidad

Seguridad

Contactos y compartir

Pagos y suscripciones

Información general

Cómo inicias sesión en Google

Asegúrate de poder acceder siempre a tu cuenta de Google manteniendo al día esta información

Verificación en dos pasos

Contraseña

Llaves de seguridad

Authenticator

Notificación de Google

Teléfono de recuperación

Correo de recuperación

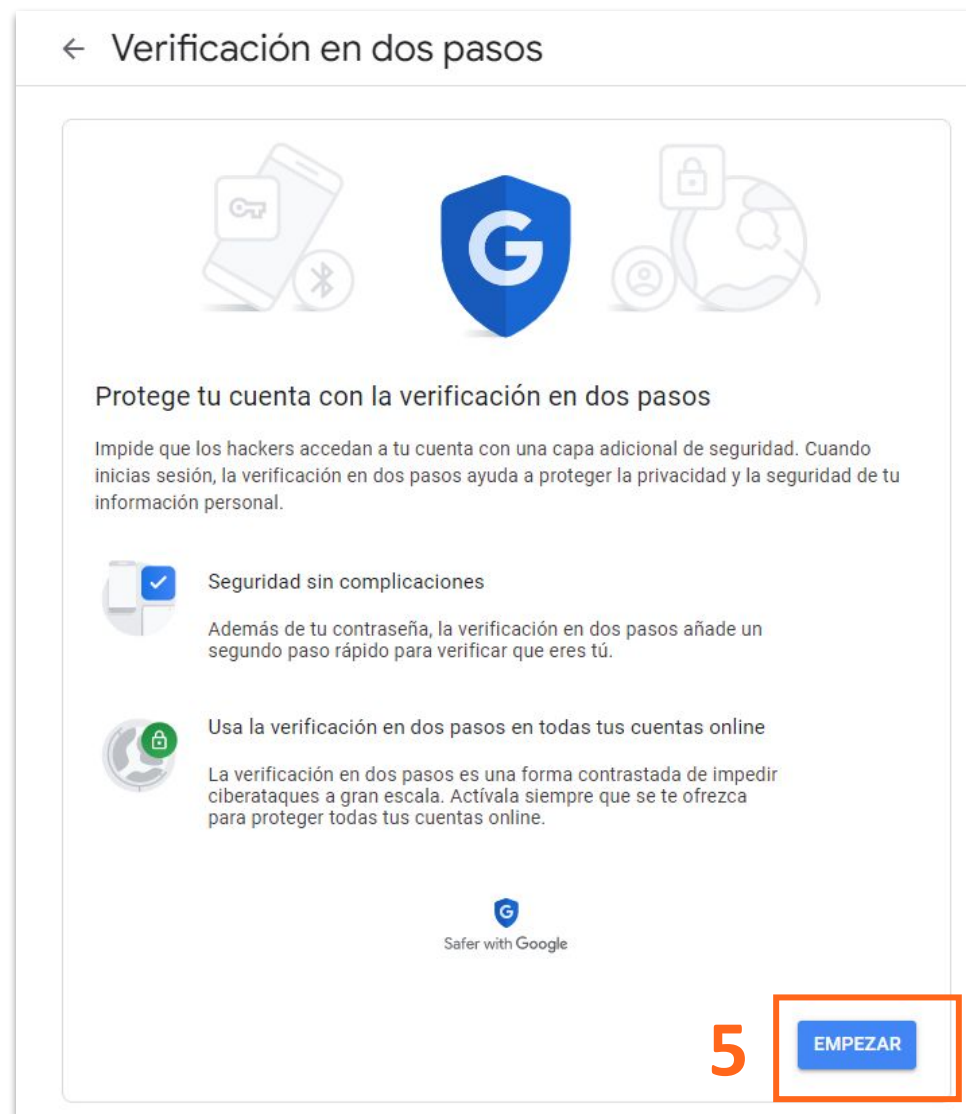
Puedes añadir más opciones de inicio de sesión

Teléfono de verificación en dos pasos

Códigos de verificación alternativos

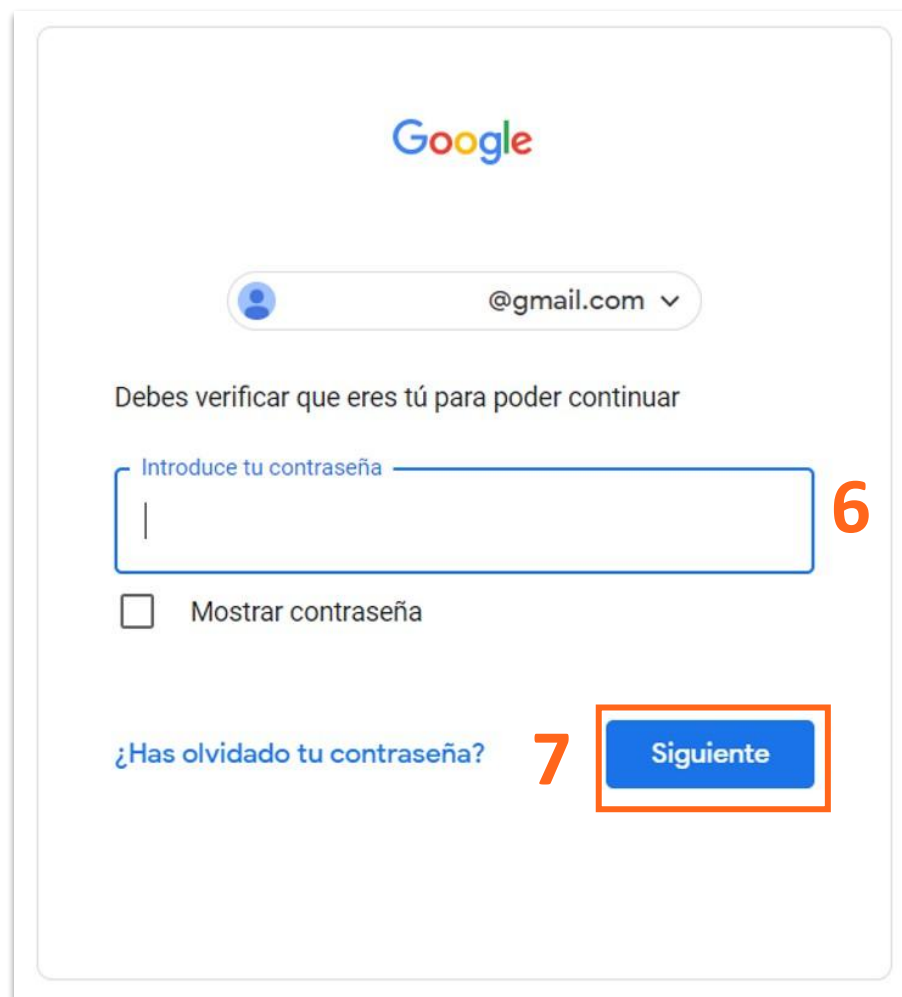
ACTIVAR 2FA EN GOOGLE (GMAIL)

→ Clic en “Empezar”



ACTIVAR 2FA EN GOOGLE (GMAIL)

→ Introduce tu contraseña > Clic en “Siguiente”



Google

@gmail.com ▾

Debes verificar que eres tú para poder continuar

Introduce tu contraseña

☐ Mostrar contraseña

¿Has olvidado tu contraseña?

6

7 Siguiente

ACTIVAR 2FA EN GOOGLE (GMAIL)

- Verifica si tu dispositivo se encuentra en la lista de dispositivos de confianza >
Clic en "Continuar"

8

← Verificación en dos pasos



Usa tu teléfono como segundo paso para iniciar sesión

Después de introducir tu contraseña, se enviarán mensajes de Google de forma segura a todos los teléfonos en los que hayas iniciado sesión. Solo tienes que tocar la notificación para revisarla e iniciar sesión.

Estos dispositivos pueden recibir mensajes

[¿No ves tu dispositivo?](#)

[Mostrar más opciones](#)

9 **CONTINUAR**

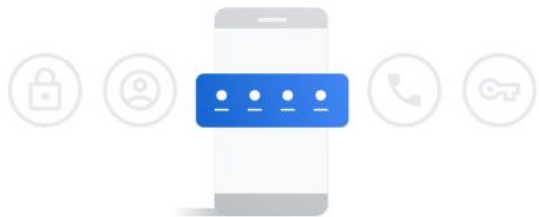
ACTIVAR 2FA EN GOOGLE (GMAIL)

Si te aparece la opción de recibir un código a través de un mensaje de texto:

→ Haz clic en “Usar otra opción de seguridad”

Nota: no es recomendable activar la recepción de un código vía SMS como segundo factor de autenticación

← Verificación en dos pasos



Ya casi has terminado. Añade una opción de seguridad

Si pierdes tu teléfono o no puedes realizar el segundo paso, necesitarás una opción de seguridad para acceder a tu cuenta.



Google solo usará este número para mantener la seguridad de la cuenta.
No utilices un número de Google Voice.
Es posible que se aplique una tarifa de mensajes y datos.

¿Cómo quieres obtener los códigos?

☒ Mensaje de texto ☐ Llamada telefónica

USAR OTRA OPCIÓN DE SEGURIDAD **10** **ENVIAR**

ACTIVAR 2FA EN GOOGLE (GMAIL)

Se te presentará la opción de descargar un lista de 10 códigos de verificación alternativa de un sólo uso.

Te recomendamos almacenar **tus códigos de seguridad** en un lugar seguro, ya que pueden funcionar como un método alternativo del segundo factor de autenticación,

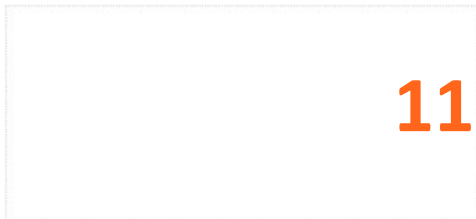
→ **Copia los códigos de verificación y pégalos en tu administrador de contraseña > Clic en "Siguiete"**

← Verificación en dos pasos



Guarda tus códigos de seguridad para poder acceder siempre a tu cuenta

Los códigos de verificación alternativos son contraseñas de un solo con las que puedes iniciar sesión cuando no tengas tu teléfono a mano. Cada uno de los códigos solo puede utilizarse una vez.



11

IMPRIMIR

DESCARGAR

USAR NÚMERO DE SEGURIDAD COMO ALTERNATIVA

12 SIGUIENTE

ACTIVAR 2FA EN GOOGLE (GMAIL)

Recuerda: Una vez que descargues la lista de **códigos de seguridad de un solo uso**, lo ideal es almacenarlos en un lugar seguro como tu administrador de contraseñas, **Bitwarden o 1Password**

En Bitwarden: Abre tu caja fuerte desde la extensión > Ubica el elemento asociado a los datos de tu cuenta de Google y selecciónalo > Haz clic en "Editar" > Baja a la sección de Notas > Copia los códigos de seguridad > Guardar

The image shows a sequence of five steps to activate 2FA in Google (Gmail) using Bitwarden:

- 1**: Click the Bitwarden extension icon in the browser toolbar.
- 2**: Select the entry "Cuenta Correo Gmail Perso..." from the list of "ENTRADAS".
- 3**: Click the "Editar" button in the top right of the entry details panel.
- 4**: Click into the "NOTAS" (Notes) field to add security codes.
- 5**: Click the "Guardar" (Save) button in the top right of the edit panel.

Nota: No olvides borrar el archivo de texto que descargaste en tu computadora con los códigos de seguridad de un solo uso

ACTIVAR 2FA EN GOOGLE (GMAIL)

En 1Password: Abre tu caja fuerte desde la extensión > Ubica el elemento asociado a los datos de tu cuenta de Google y selecciónalo > Haz clic en el **Menú** > **"Editar"** > Serás dirigido a la versión web > Ve a la sección de **Notas** > Copia los códigos de seguridad > **"Guardar"**.

The screenshot illustrates the process of editing a Google account entry in the 1Password browser extension. The interface is divided into several sections:

- Top Bar:** Includes a search bar labeled "Buscar en 1Password" and a button labeled "+ Nuevo elemento".
- Left Panel:** Displays a list of suggestions. One entry, "Google Prueba Con... conexoprueba@gmail.com", is highlighted with an orange box and labeled with the number 2.
- Right Panel (Entry Details):** Shows the details for the selected entry. It includes fields for "Nombre de usuario" (conexoprueba@gmail.com), "contraseña" (masked with dots), "página web" (https://accounts.google.com), and "Sección" (nuevo campo). A "Guardar" button is located in the top right corner, labeled with the number 6.
- Menu:** A menu is open over the entry, showing options like "Editar", "Escanear código QR", "Añadir a favoritos", "Cambiar contraseña", "Abrir en una nueva ventana", "Compartir...", "Copiar enlace privado", "Archivar", and "Eliminar". The "Editar" option is highlighted with an orange box and labeled with the number 4.
- Notes Section:** At the bottom, there is a section labeled "notas" with a text input field, labeled with the number 5.

Orange boxes and numbers (1, 2, 3, 4, 5, 6) indicate the sequence of steps to follow:

1. Click the 1Password extension icon in the browser toolbar.
2. Select the Google account entry from the suggestions list.
3. Click the menu icon (three dots) next to the entry.
4. Click the "Editar" option in the menu.
5. Enter the security codes in the "notas" field.
6. Click the "Guardar" button to save the changes.

Nota: No olvides borrar el archivo de texto que descargaste en tu computadora con los códigos de seguridad de un solo uso

ACTIVAR 2FA EN GOOGLE (GMAIL)

→ Clic en "Activar"

← Verificación en dos pasos



¿Quieres activar la verificación en dos pasos?

Segundo paso: **Notificación de Google (predeterminado)**

Opción de seguridad: **Códigos de verificación alternativos**

No se cerrará la sesión de en estos dispositivos

Es posible que se cierren las sesiones en los demás dispositivos. Para volver a iniciarlas, necesitarás la contraseña y el segundo paso.

13

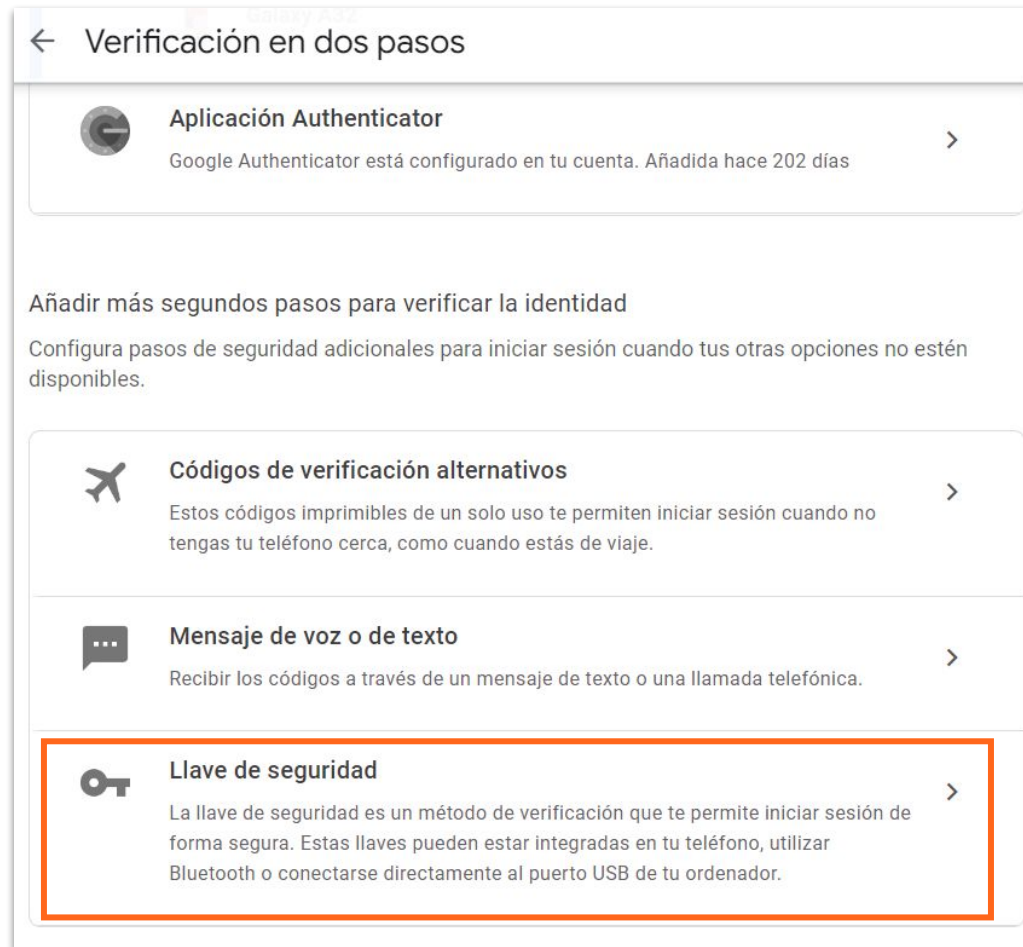
ACTIVAR

ACTIVAR 2FA EN GOOGLE (GMAIL)

Ingresa a la lista de **“Segundos pasos disponibles”**

→ **Clic en “Llaves de seguridad” para iniciar la configuración.**

1



ACTIVAR 2FA EN GOOGLE (GMAIL)

Se abrirá el asistente de configuración de las llaves de seguridad

→ **Selecciona “Añadir Llave de seguridad”**

← Llaves de seguridad

Las llaves de seguridad son un segundo paso más seguro. [Más información ?](#)

Puedes ver todas tus llaves de seguridad y llaves de acceso en la página de configuración de tus llaves de acceso. [Ir a la configuración de llaves de acceso](#)

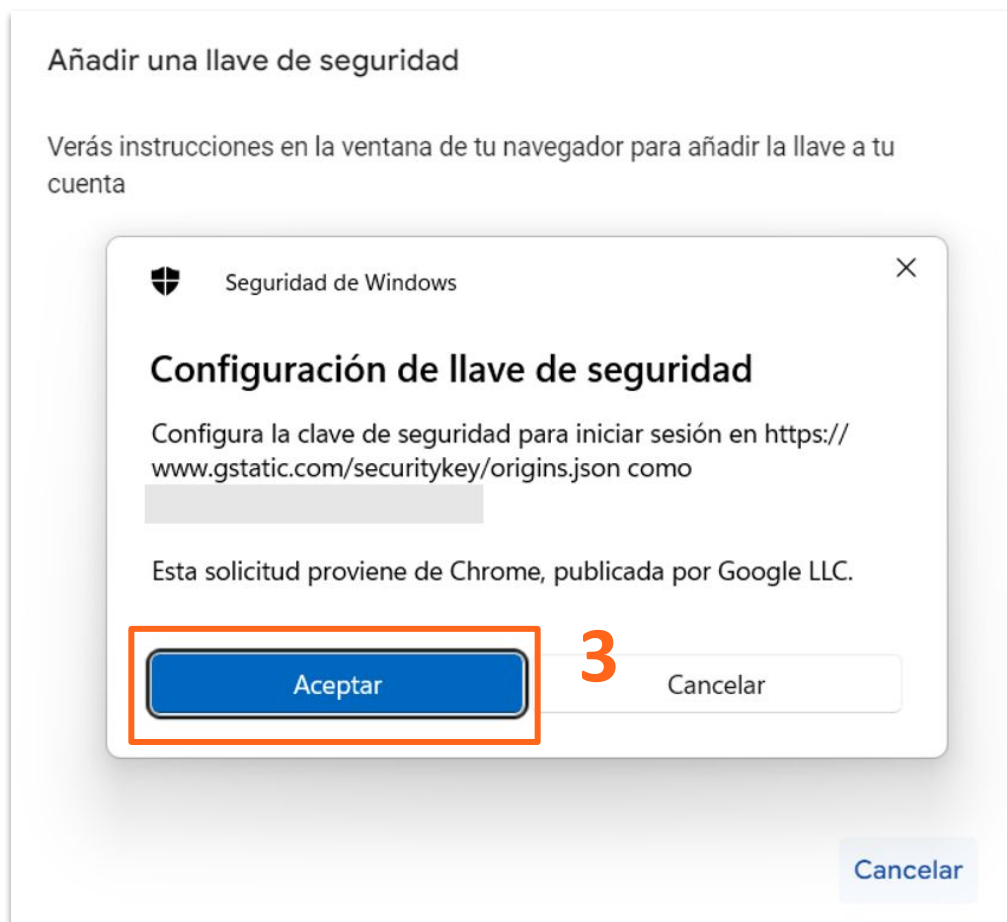
+ Añadir llave de seguridad

2



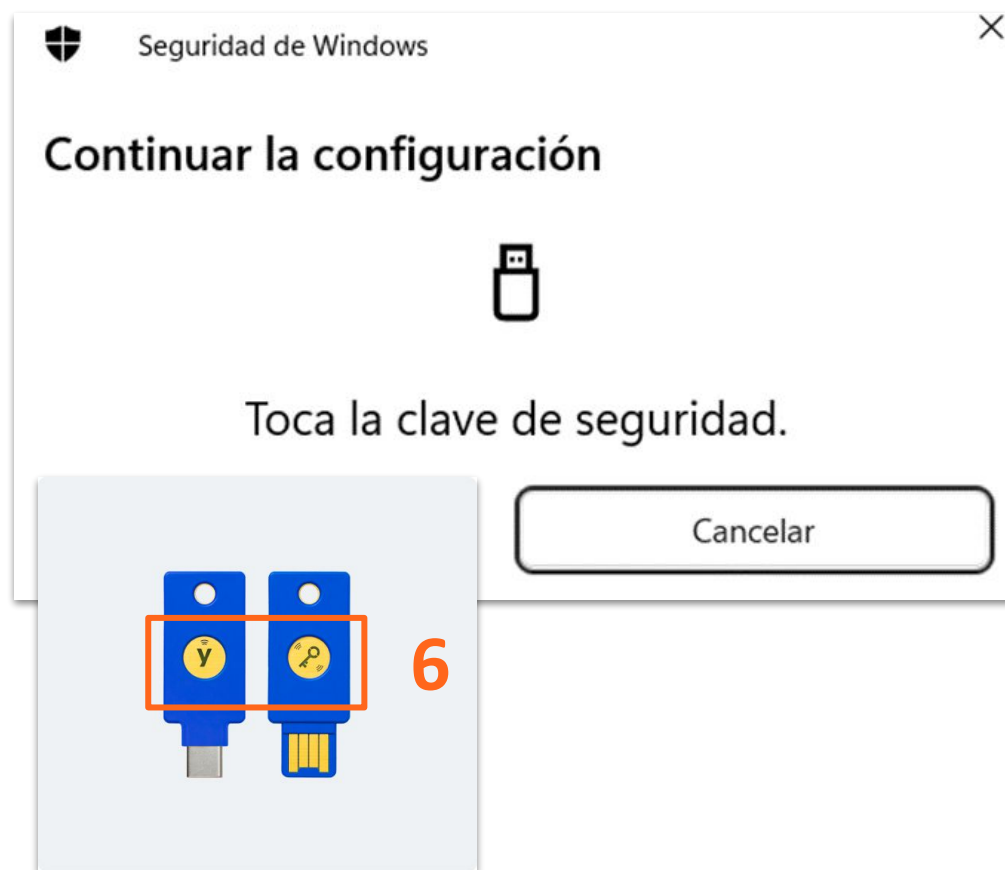
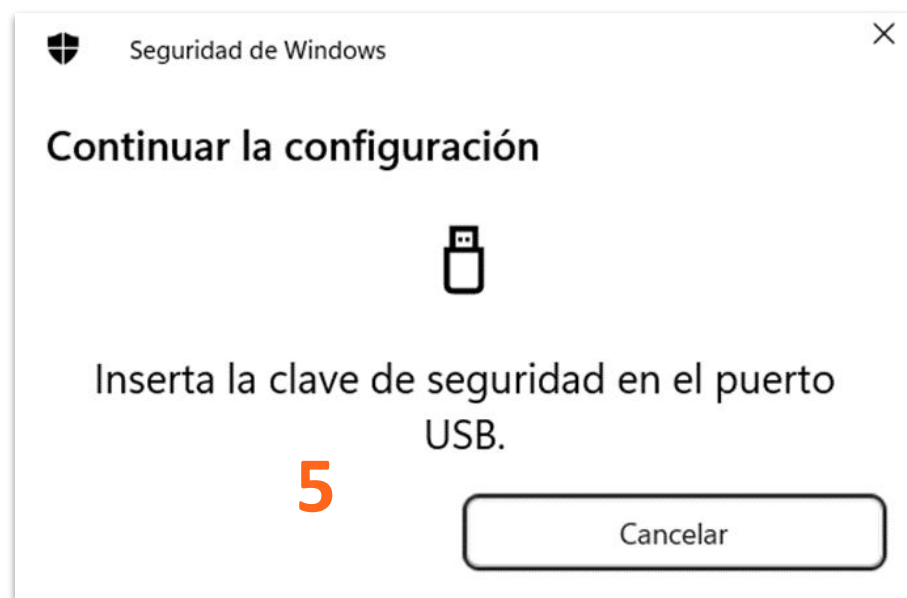
ACTIVAR 2FA EN GOOGLE (GMAIL)

- Clic en "Aceptar" para iniciar con la configuración de la Llave Yubico
- Clic en "Aceptar" para habilitar permisos de lectura de la Llave Yubico



ACTIVAR 2FA EN GOOGLE (GMAIL)

- Inserta tu Llave Yubico
- Toca tu Llave Yubico en el símbolo



ACTIVAR 2FA EN GOOGLE (GMAIL)

→ Asigna un nombre a tu Llave Yubico “Llave Principal” > Clic en “Siguiente”

Indica el nombre de tu llave

Pon un nombre a tu llave para que puedas identificarla más tarde

Nombre de la llave de seguridad

7

0 / 20

8

Siguiente

ACTIVAR 2FA EN GOOGLE (GMAIL)

→ Has añadido tu Llave Yubico como segundo factor de autenticación > Clic en “Siguiente”

Security key is added



2-Step Verification is on for your account and your security key is ready to use.

Keep your security key with you so you can always sign into your Google Account.

9

[Back](#)

[Next](#)

ACTIVAR 2FA EN GOOGLE (GMAIL)

- Clic en “Añadir Llave de Seguridad” para configurar tu Llave Yubico de Backup
- Repite los pasos de la diapositiva 12 a la 17 y asigna un nombre “Llave Backup”

← Security keys

Security keys are a more secure second step. You can add a physical key or use your phone's built-in key. [Learn more](#)

Your security keys



Llave Principal (Added: Just now)
Last used: –

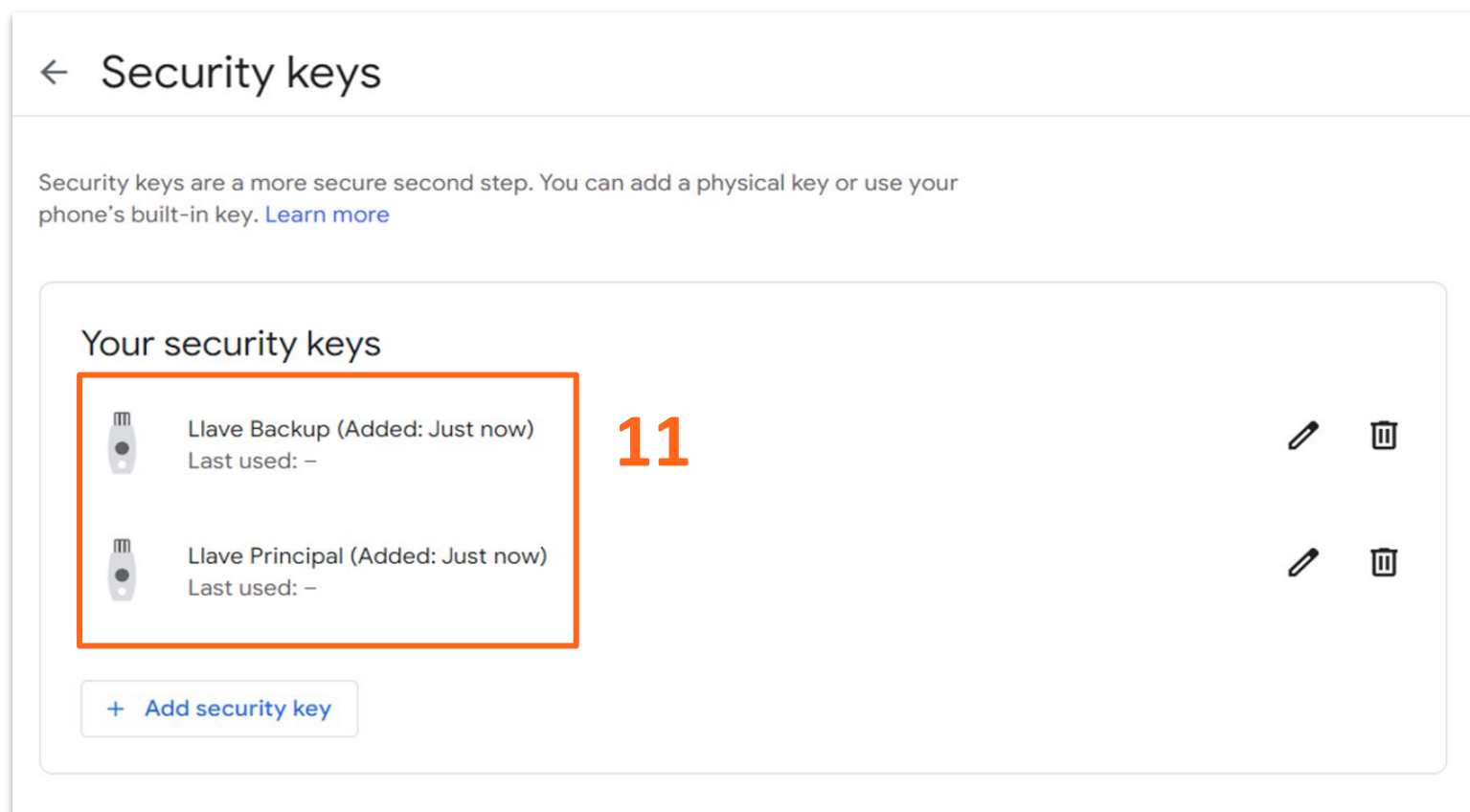


+ Add security key

10

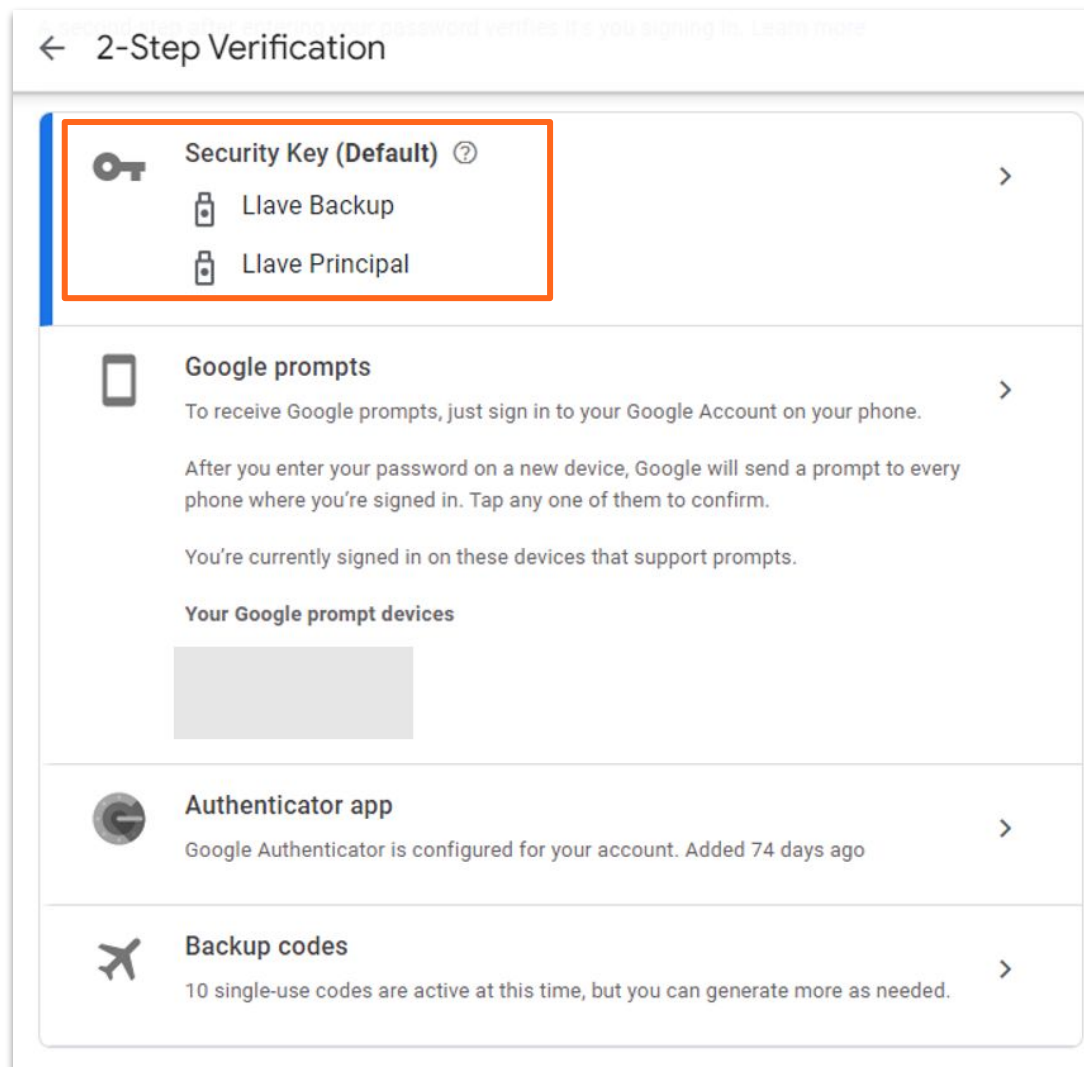
ACTIVAR 2FA EN GOOGLE (GMAIL)

- Tendrás configurada tu Llave Yubico Principal y de Backup como segundo factor de autenticación



ACTIVAR 2FA EN GOOGLE (GMAIL)

La Llave de seguridad se colocará de forma predeterminada como segundo factor de autenticación



ACTIVAR 2FA EN GOOGLE (GMAIL)

Recuerda: Una vez activado el 2FA, si previamente tenías configurado un número de teléfono para recibir los códigos de seguridad a través de un mensaje de texto (SMS), **te recomendamos eliminarlo**

Para hacerlo:

Vuelve al apartado de “Verificación en dos pasos” > Métodos Activos > Mensaje de voz o de texto > Editar > Elimina tú número de teléfono

1

← Verificación en dos pasos

3

Mensaje de voz o de texto

Verificado

Los códigos de verificación se envían a través de mensajes de texto.

2 AÑADIR TELÉFONO

Añadir más segundos pasos para verificar la identidad

Configura pasos de seguridad adicionales para iniciar sesión cuando tus otras opciones no estén disponibles.

Códigos de seguridad

Estos códigos imprimibles de un solo uso te permiten iniciar sesión cuando no tengas tu teléfono cerca, como cuando estás de viaje.

CONFIGURAR

Aplicación Authenticator

Usa la aplicación Authenticator para recibir códigos de verificación gratuitos aunque tu teléfono esté sin conexión. Disponible para Android y iPhone.

CONFIGURAR

ACTIVAR 2FA EN GOOGLE (GMAIL)

Recuerda: En la sección **“Cómo inicias sesión en Google”**, revisa que no tengas asociado un **“Teléfono de recuperación”** para verificar tu identidad. No es recomendable recibir códigos de verificación mediante mensajes de texto (SMS) o llamadas telefónicas. Además revisar que el correo electrónico de recuperación configurado, sea uno seguro

The screenshot shows the Google Account management interface. On the left, a sidebar contains links to 'Inicio', 'Información personal', 'Datos y privacidad', 'Seguridad', 'Contactos y compartir', 'Pagos y suscripciones', and 'Información general'. The 'Seguridad' link is highlighted with a blue box and an orange number '1'. The main content area is titled 'Cómo inicias sesión en Google' (highlighted with an orange box and number '2') and includes the subtitle 'Asegúrate de poder acceder siempre a tu cuenta de Google manteniendo al día esta información'. Below this, a list of security options is shown: 'Verificación en dos pasos', 'Contraseña', 'Llaves de seguridad', 'Authenticator', 'Notificación de Google', 'Teléfono de recuperación' (with a yellow warning icon and the text 'Añadir un número de teléfono móvil'), and 'Correo de recuperación'. The 'Teléfono de recuperación' and 'Correo de recuperación' items are grouped together in an orange box with the number '3'. At the bottom, there are buttons for 'Teléfono de verificación en dos pasos' and 'Códigos de verificación alternativos'.

Google Cuenta

1

2

3

Puedes añadir más opciones de inicio de sesión

Teléfono de verificación en dos pasos Códigos de verificación alternativos

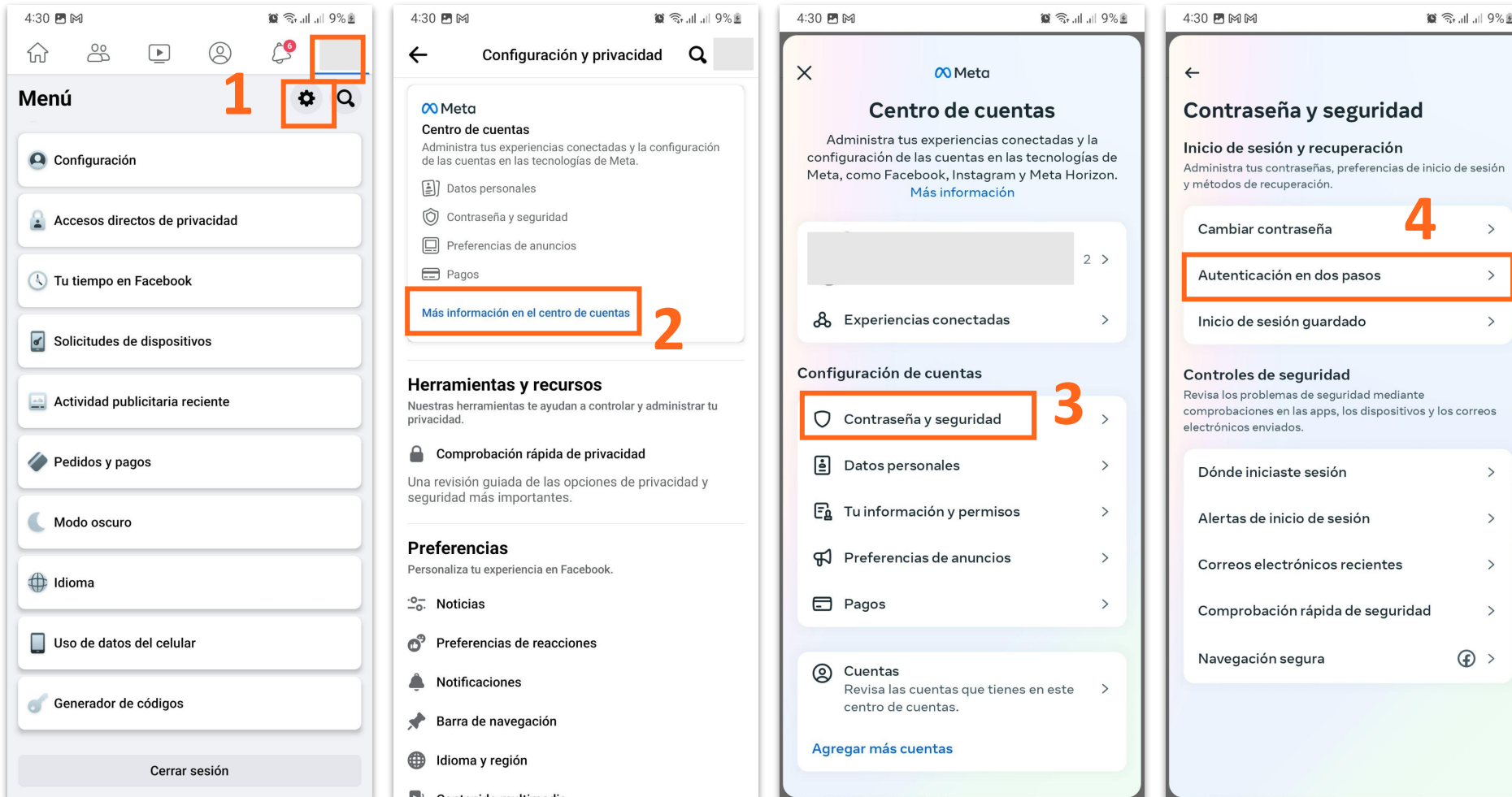
ACTIVAR 2FA EN (RRSS)

Meta

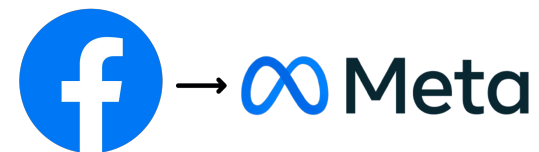


Activa la 2FA en tus cuentas de redes sociales: Facebook e Instagram:

Ingresa al centro de cuentas de Meta desde Facebook: Menú de ajustes > Ícono de configuración > Más información en el centro de cuentas > Contraseña y seguridad > Autenticación en dos pasos



ACTIVAR 2FA EN (RRSS)



Activa la 2FA en tus cuentas de redes sociales: Facebook e Instagram:

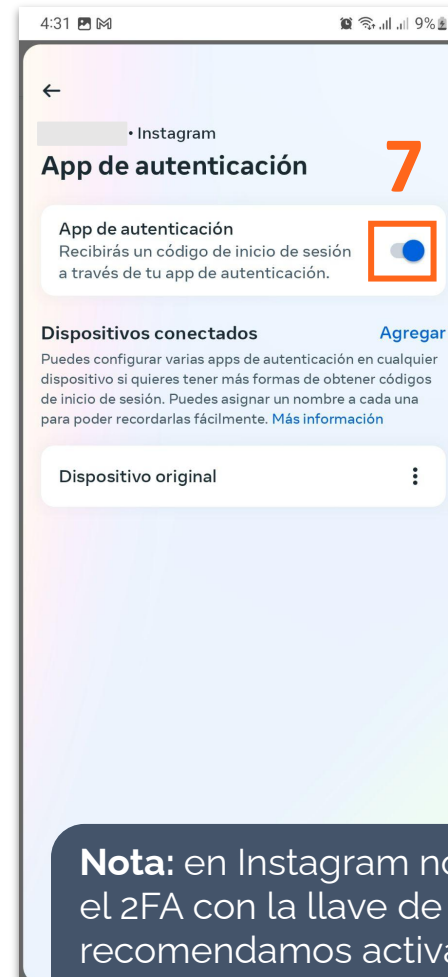
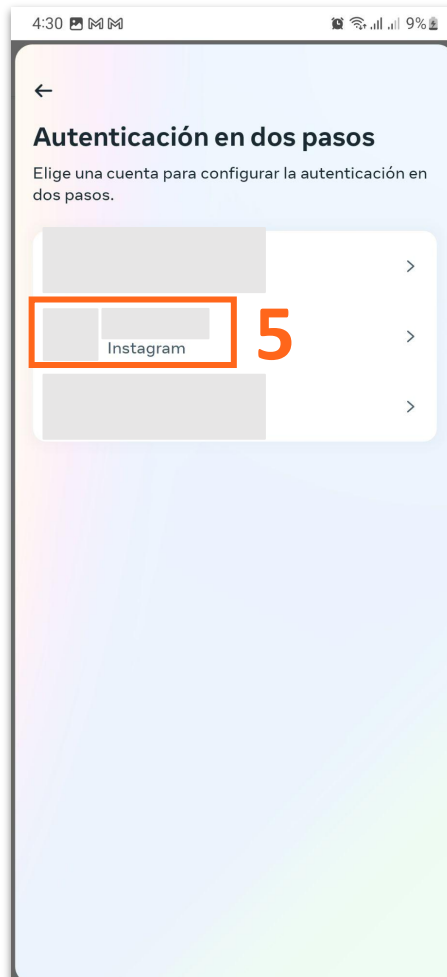
Selecciona la cuenta a la que le activarás el 2FA: Facebook > Coloca tu contraseña > Selecciona Llave de seguridad > Activa este método utilizando una llave principal y una llave de respaldo



ACTIVAR 2FA EN (RRSS)

Activa la 2FA en tus cuentas de redes sociales: Facebook e Instagram:

Selecciona la cuenta a la que le activarás el 2FA: Instagram > Selecciona App de autenticación > Activa este método escaneando el código QR con tu aplicación.



Nota: en Instagram no puedes activar el 2FA con la llave de seguridad, te recomendamos activarlo con la App de autenticación

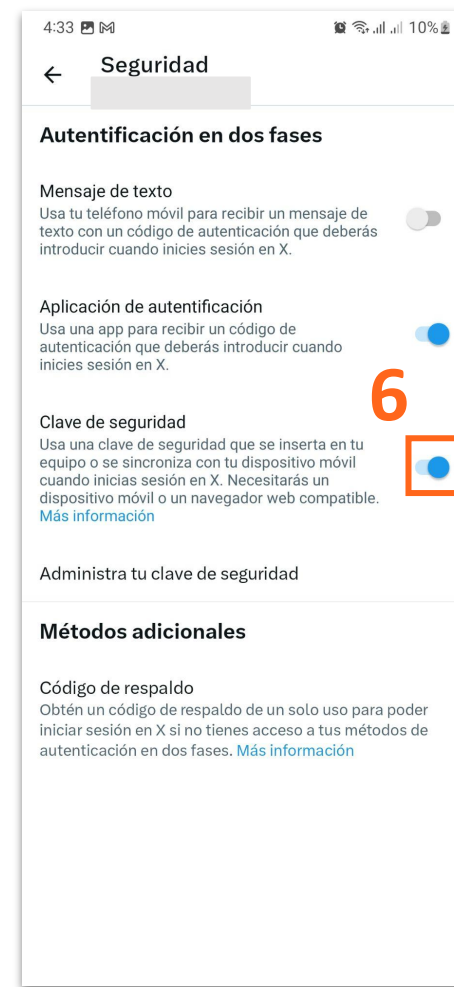
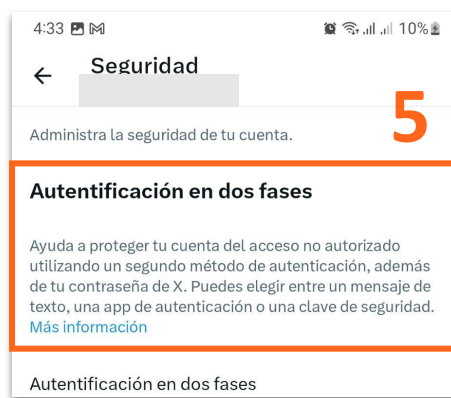
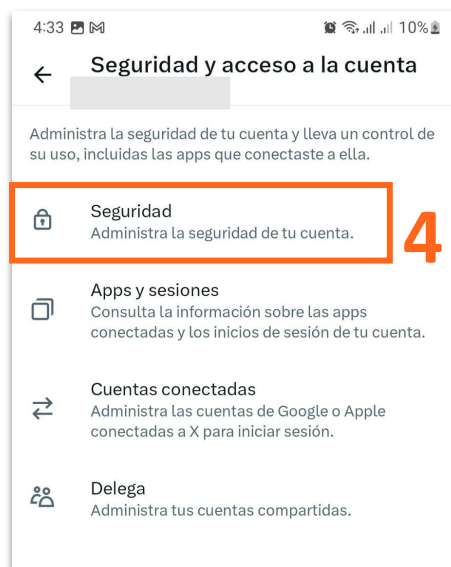
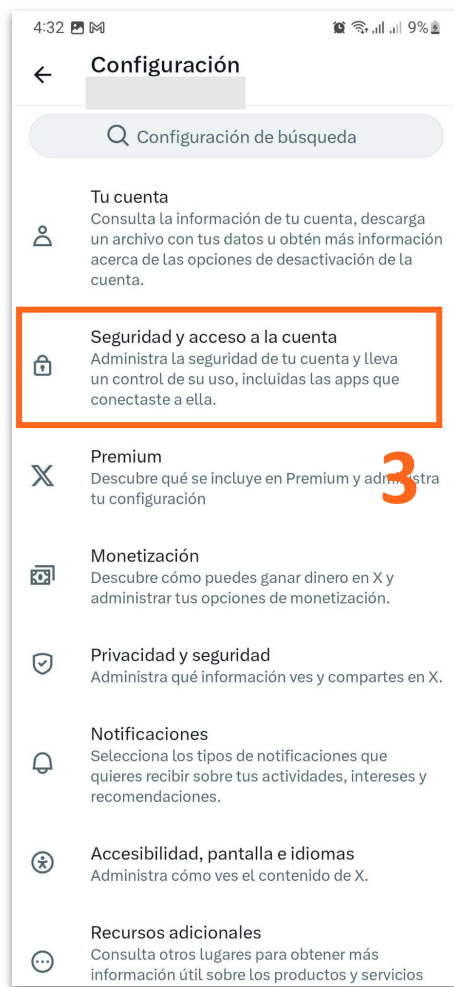
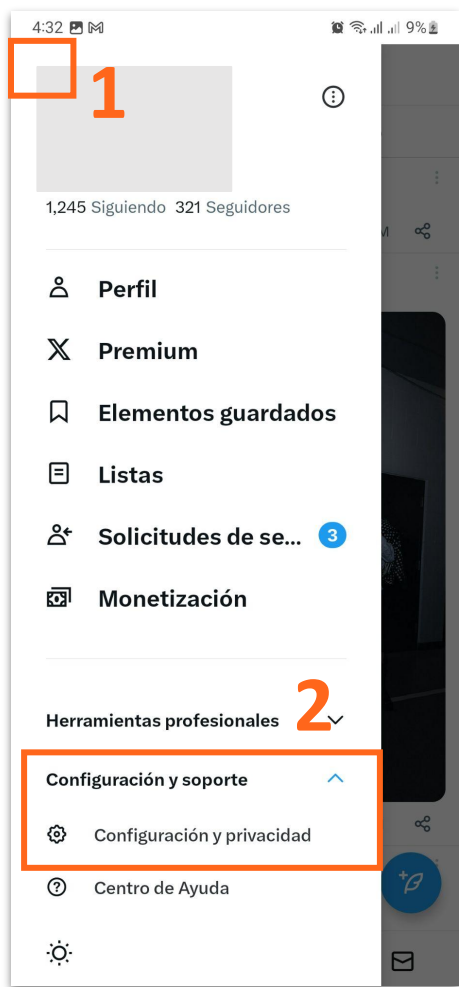
ACTIVAR 2FA EN (RRSS)

Nota: Recuerda eliminar tu número de teléfono como información de contacto para recuperar el acceso a tu cuenta o como método de 2FA (ver siguientes diapositivas).



Activa la 2FA en tus cuentas de redes sociales: X

X: Menú de ajustes > Configuración y soporte > Configuración y privacidad > Seguridad y acceso a la cuenta > Seguridad > Autenticación en dos fases > Activa la Clave de seguridad con una llave principal y una de respaldo



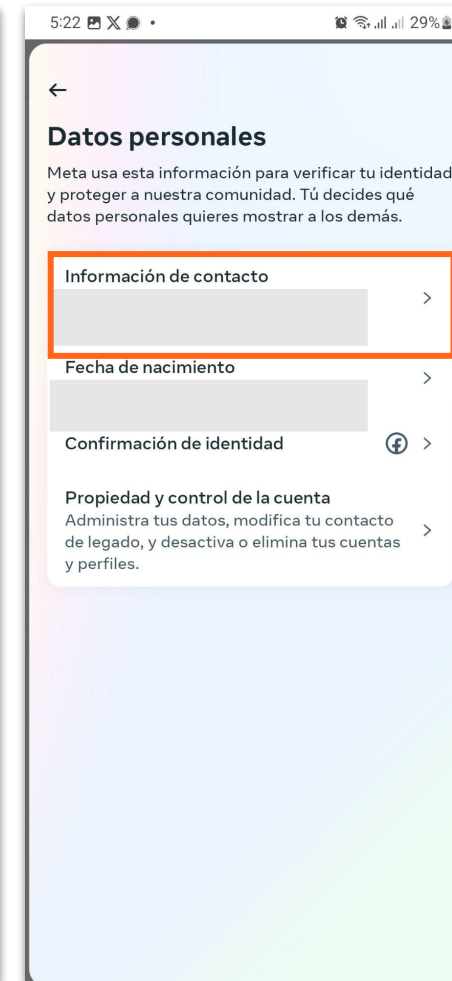
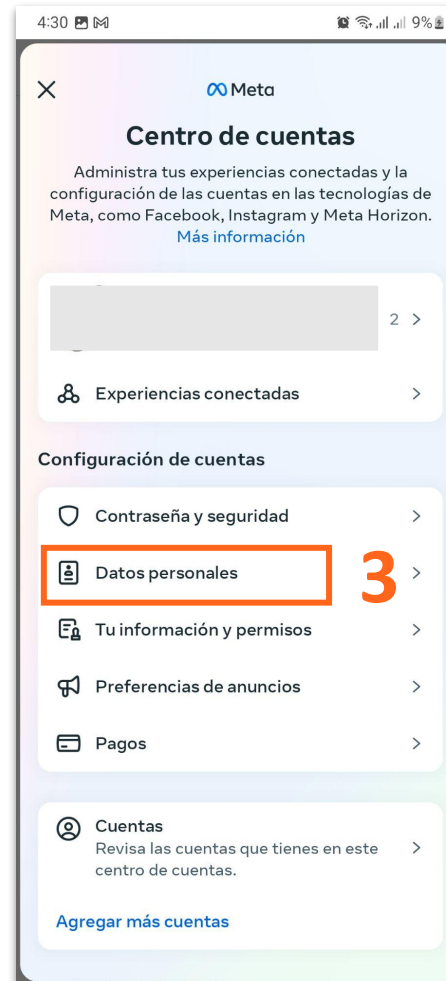
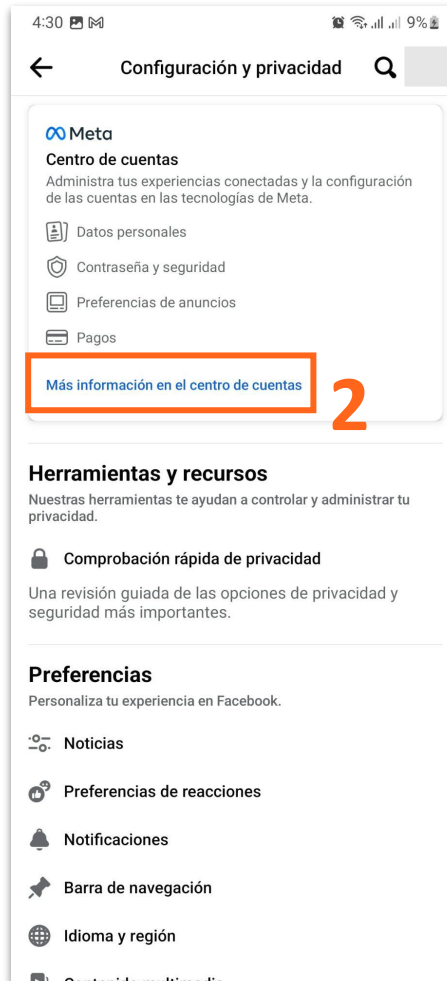
ACTIVAR 2FA EN (RRSS)

Meta



Eliminar número de teléfono como 2FA o alternativa de recuperación de cuenta:

Facebook e Instagram (Meta): Menú de ajustes > Ícono de configuración > Más información en el centro de cuentas > Datos personales > Información de contacto

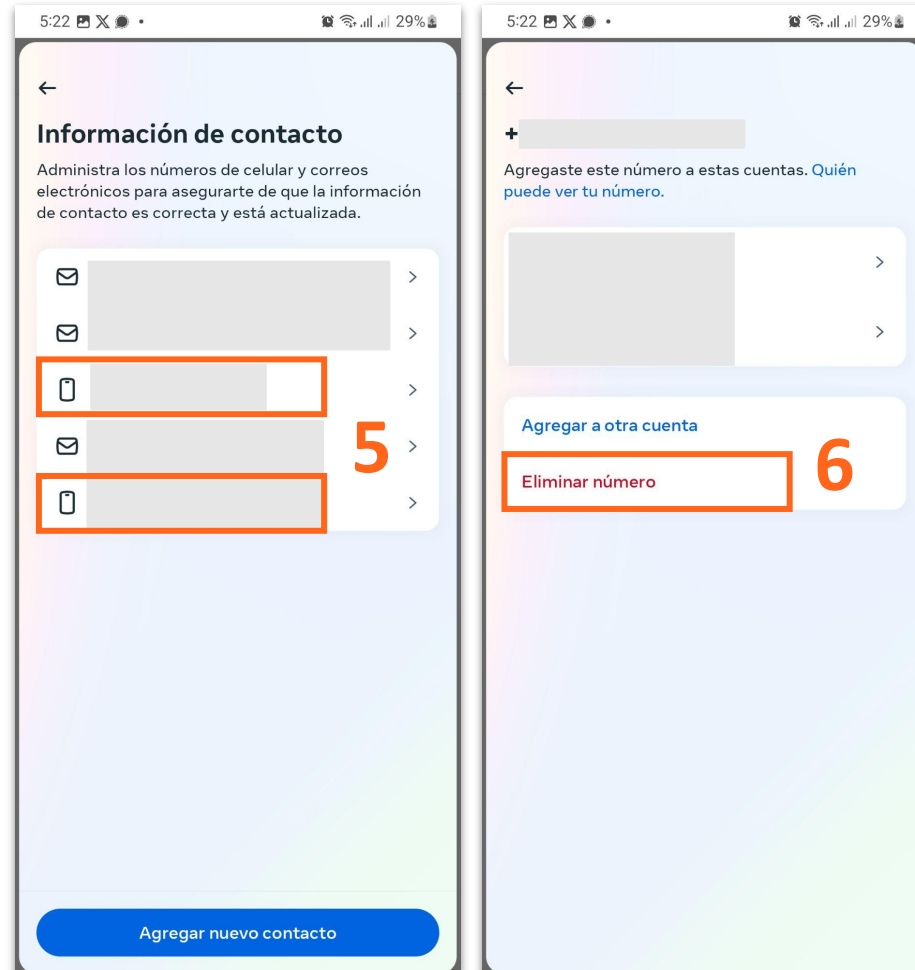


ACTIVAR 2FA EN (RRSS)

Eliminar número de teléfono como 2FA o alternativa de recuperación de cuenta:

Facebook e Instagram (Meta): Selecciona los números de teléfono > Eliminar número

Meta

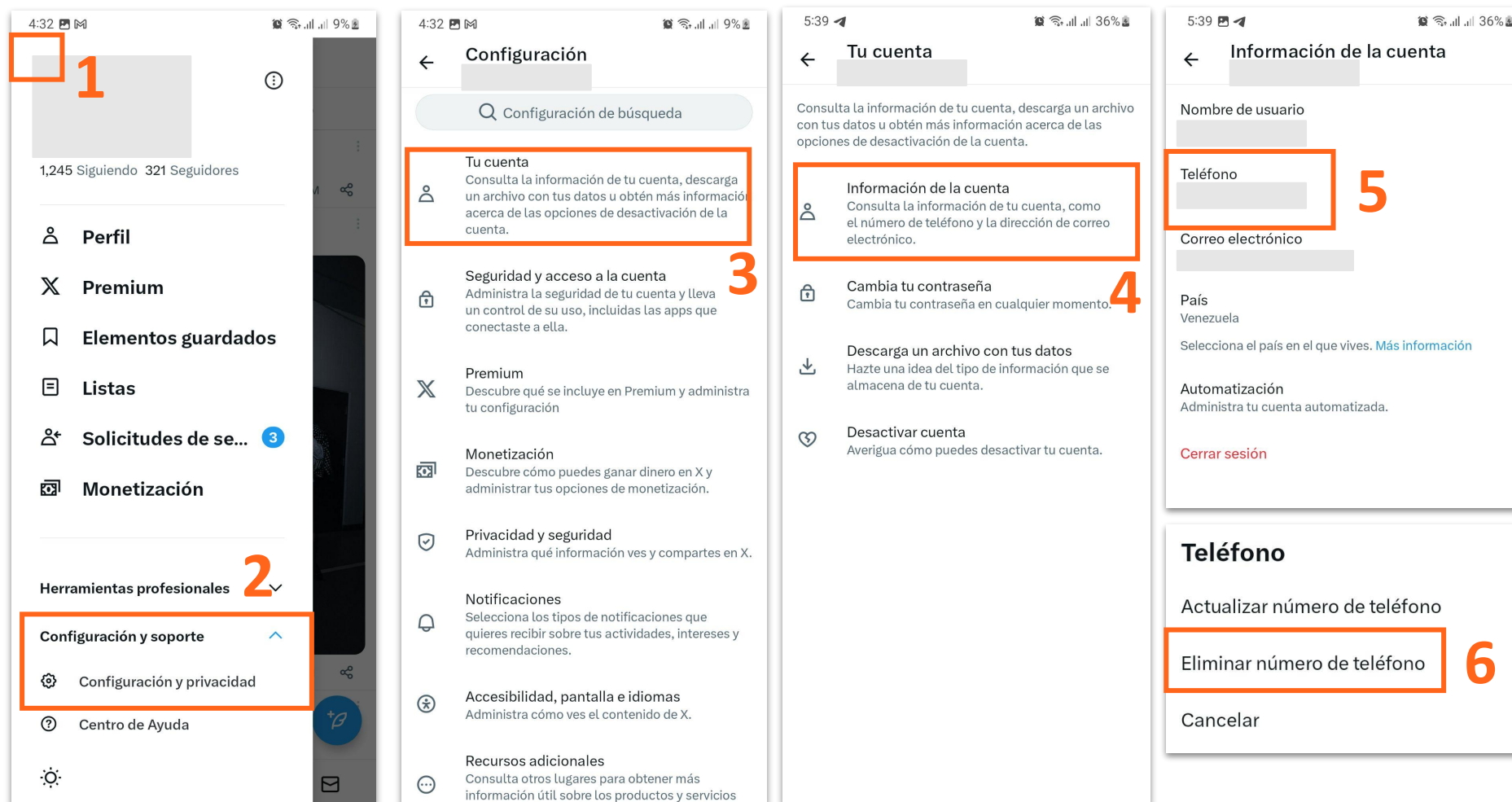


ACTIVAR 2FA EN (RRSS)



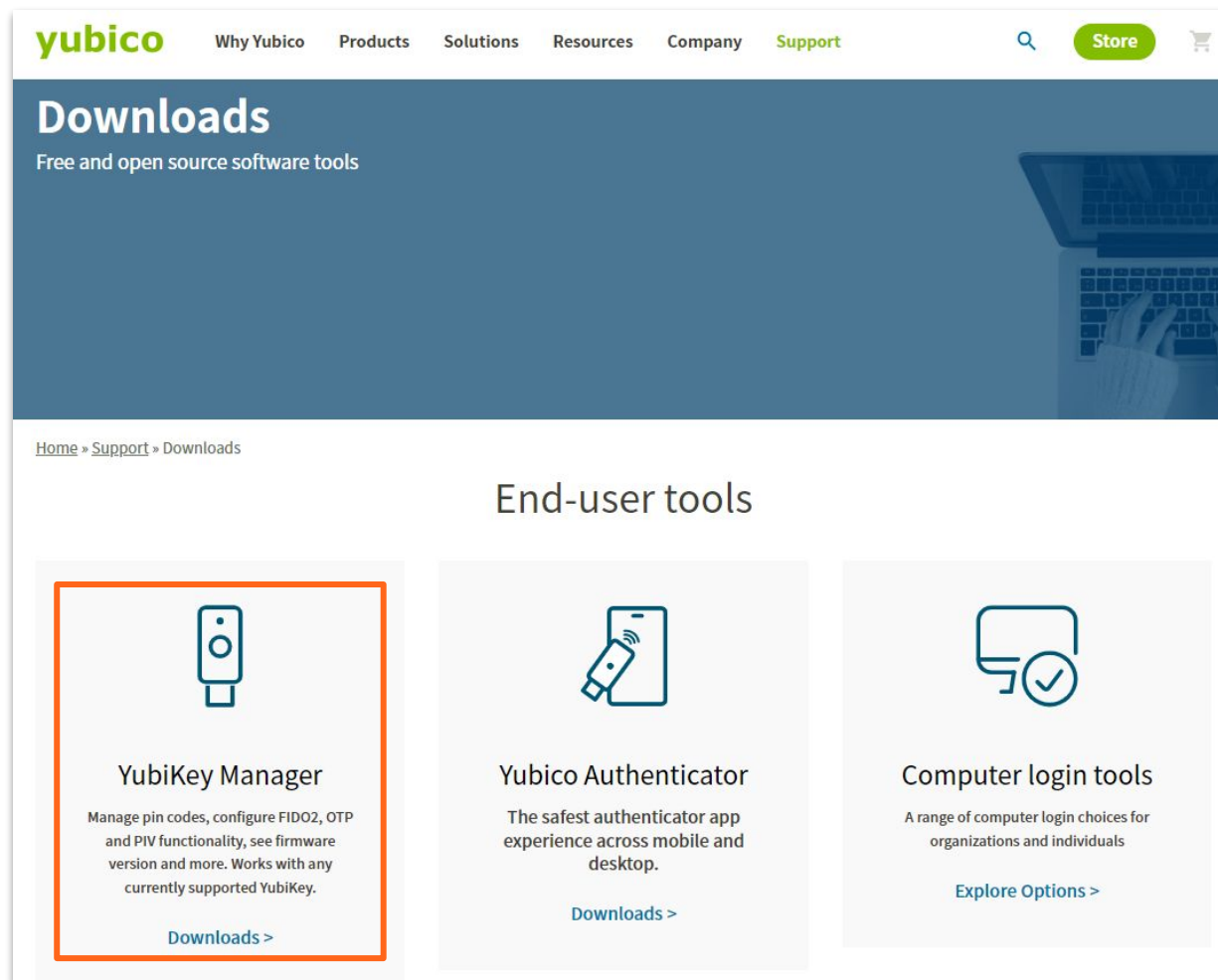
Eliminar número de teléfono como 2FA o alternativa de recuperación de cuenta:

X: Menú de Ajuste > Configuración y soporte > Configuración y privacidad > Tu cuenta > Información de la cuenta > Teléfono > Eliminar número de teléfono



ADMINISTRADOR YUBIKEY

1. Ingresa a: <https://www.yubico.com/support/download/> y selecciona "YubiKey Manager"



The screenshot shows the Yubico website's 'Downloads' section. The header includes the Yubico logo and navigation links: 'Why Yubico', 'Products', 'Solutions', 'Resources', 'Company', and 'Support'. A search icon and a 'Store' button are also present. The main heading is 'Downloads' with the subtitle 'Free and open source software tools'. Below this, a breadcrumb trail reads 'Home » Support » Downloads'. The section is titled 'End-user tools' and features three cards. The first card, 'YubiKey Manager', is highlighted with an orange border and contains an icon of a YubiKey, the title 'YubiKey Manager', a description about managing pin codes and FIDO2/OTP, and a 'Downloads >' link. The second card, 'Yubico Authenticator', has an icon of a smartphone with a YubiKey, the title 'Yubico Authenticator', a description about a safe authenticator app, and a 'Downloads >' link. The third card, 'Computer login tools', has an icon of a computer monitor with a checkmark, the title 'Computer login tools', a description about login choices, and an 'Explore Options >' link.

yubico Why Yubico Products Solutions Resources Company Support

Downloads

Free and open source software tools

[Home](#) » [Support](#) » Downloads

End-user tools



YubiKey Manager

Manage pin codes, configure FIDO2, OTP and PIV functionality, see firmware version and more. Works with any currently supported YubiKey.

[Downloads >](#)



Yubico Authenticator

The safest authenticator app experience across mobile and desktop.

[Downloads >](#)



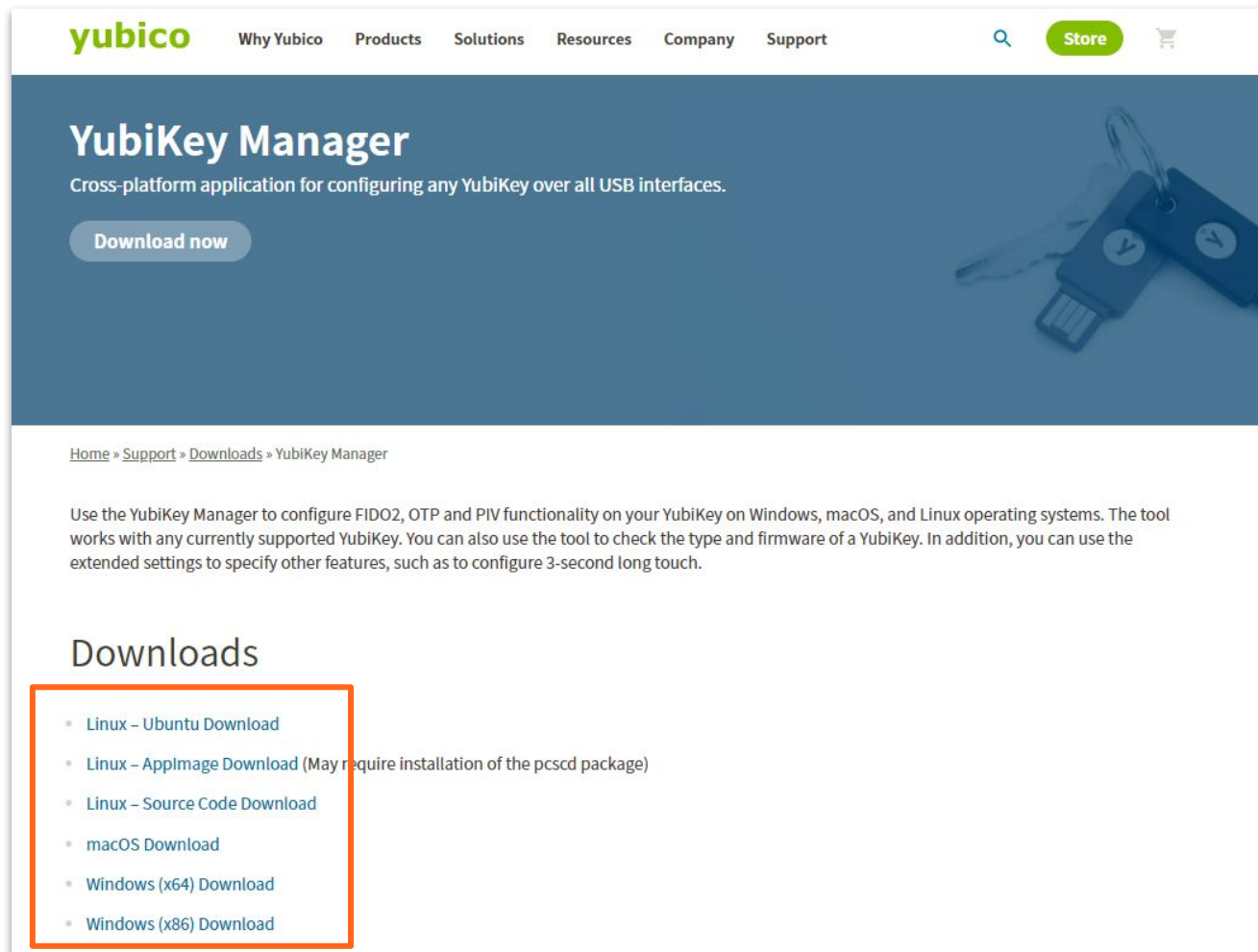
Computer login tools

A range of computer login choices for organizations and individuals

[Explore Options >](#)

ADMINISTRADOR YUBIKEY

2. Selecciona el link de acuerdo a tu sistema operativo > Espera que culmine la descarga



yubico Why Yubico Products Solutions Resources Company Support

YubiKey Manager

Cross-platform application for configuring any YubiKey over all USB interfaces.

[Download now](#)

[Home](#) » [Support](#) » [Downloads](#) » YubiKey Manager

Use the YubiKey Manager to configure FIDO2, OTP and PIV functionality on your YubiKey on Windows, macOS, and Linux operating systems. The tool works with any currently supported YubiKey. You can also use the tool to check the type and firmware of a YubiKey. In addition, you can use the extended settings to specify other features, such as to configure 3-second long touch.

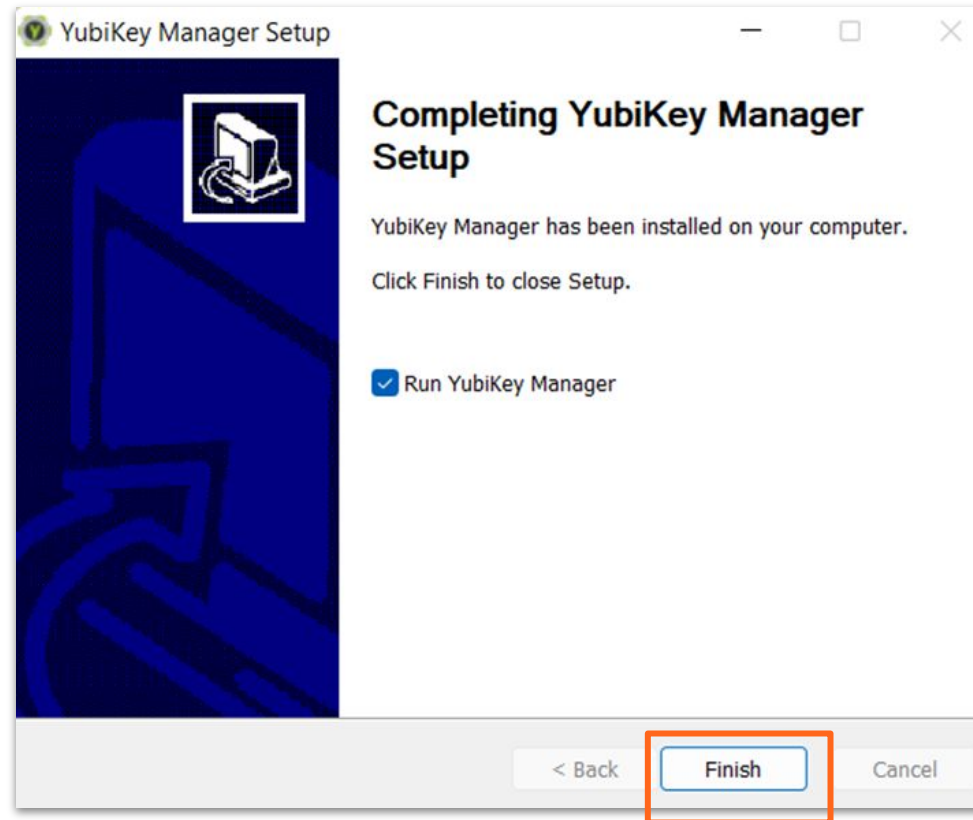
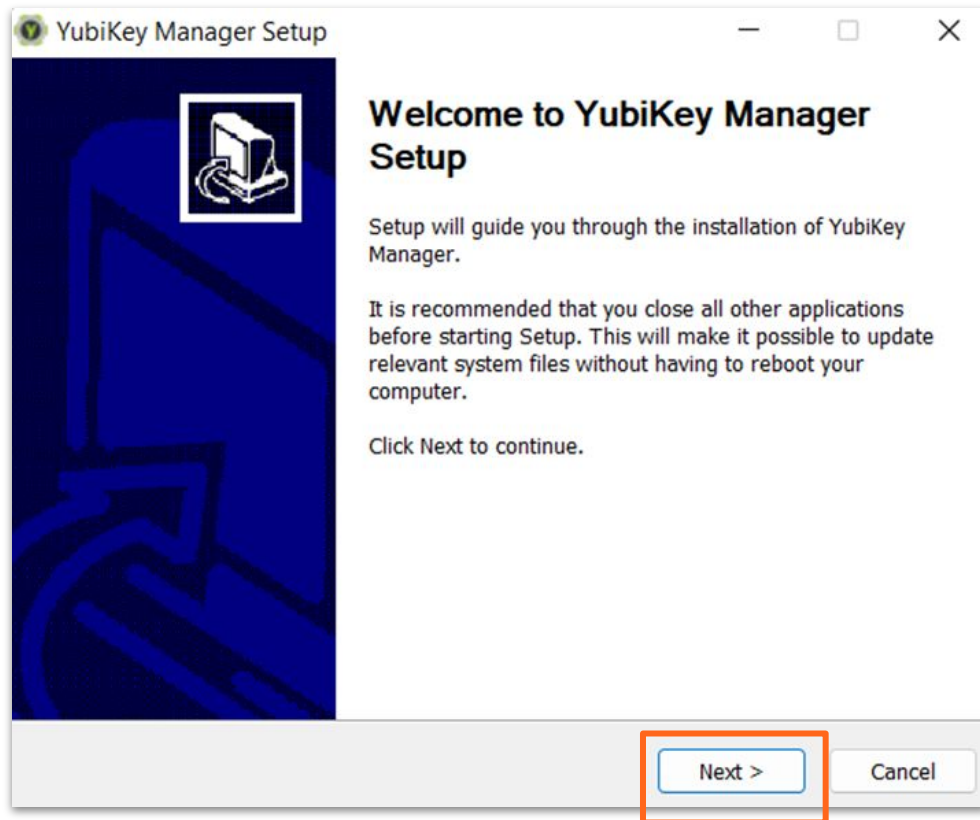
Downloads

- [Linux – Ubuntu Download](#)
- [Linux – Appliance Download](#) (May require installation of the pcsd package)
- [Linux – Source Code Download](#)
- [macOS Download](#)
- [Windows \(x64\) Download](#)
- [Windows \(x86\) Download](#)



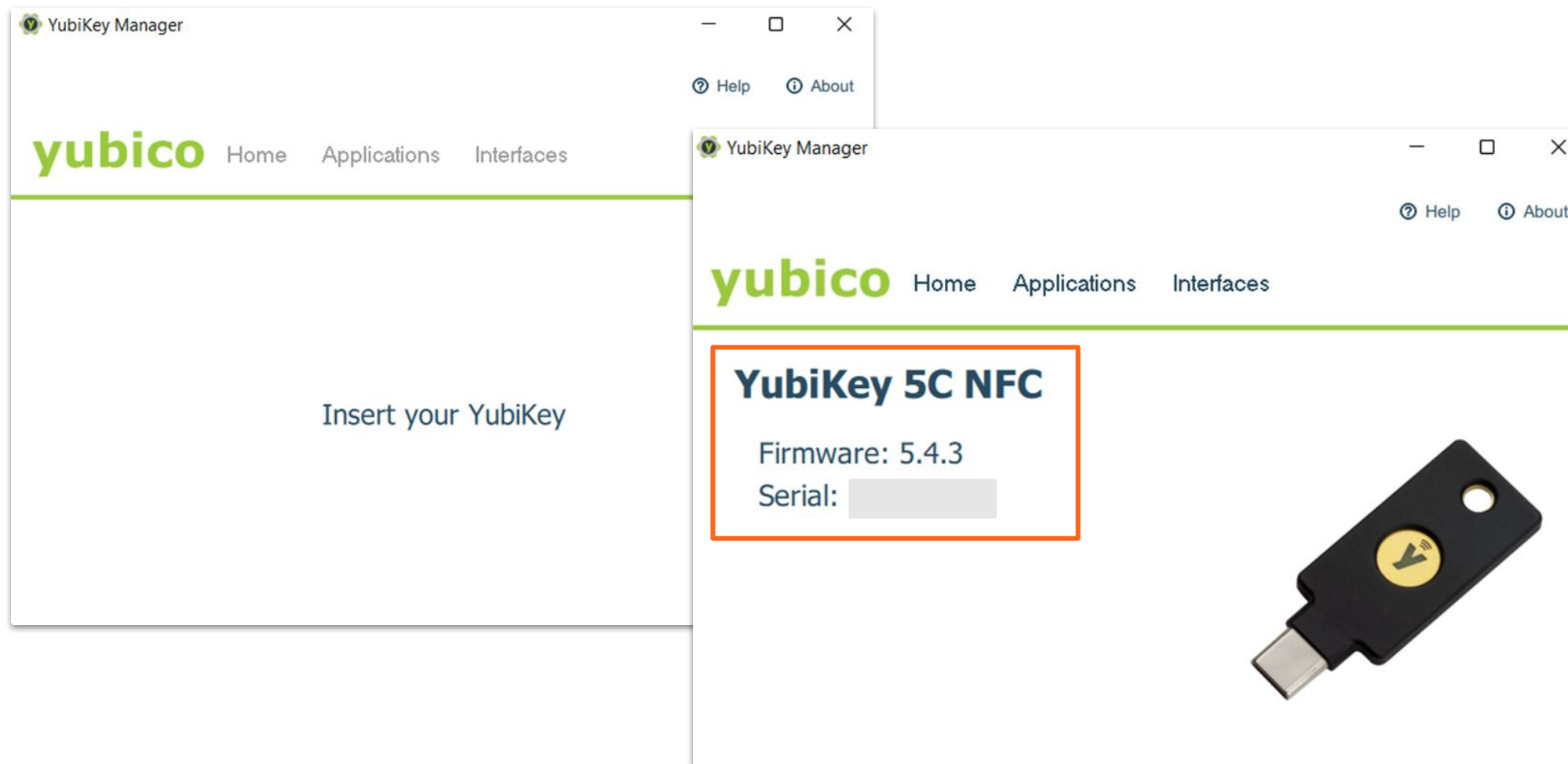
ADMINISTRADOR YUBIKEY

3. Ejecuta el instalador, acepta los permisos y continua por el menú de instalación hasta finalizar.



ADMINISTRADOR YUBIKEY

4. Conecta tu Llave Yubico, la aplicación la reconocerá automáticamente



ADMINISTRADOR YUBIKEY

5. Clic en "Aplicaciones" > Clic en "FIDO2" > Clic en "Ser PIN"

The image displays two screenshots of the YubiKey Manager web application. The first screenshot shows the main dashboard with the 'Applications' menu item highlighted in the top navigation bar. A dropdown menu is open, showing 'Configure FIDO2 Application', 'OTP', 'FIDO2', and 'PIV'. The 'FIDO2' option is highlighted. The second screenshot shows the 'FIDO2' configuration page. Under the 'FIDO2 PIN' section, it states 'No PIN is set' and a 'Set PIN' button is highlighted with a red box. To the right, there is a 'Reset' section with a 'Reset FIDO' button. The background of the interface includes a YubiKey 5C NFC device and a blue-tinted image of a desk with a smartphone and a coffee cup.

YubiKey Manager

yubico Home Applications Interfaces

YubiKey 5C NFC

Firmware: 5.4.3
Serial: 19887649

Configure FIDO2 Application
OTP
FIDO2
PIV

YubiKey Manager

YubiKey 5C NFC (19887649) Help About

yubico Home Applications Interfaces

FIDO2

Home / FIDO2

FIDO2 PIN

No PIN is set

Set PIN

Reset

Restore defaults

Reset FIDO

< Back

ADMINISTRADOR YUBIKEY

6. Introduce un PIN de por lo menos 4 caracteres > "Set PIN" > El FIDO2 PIN quedará establecido

YubiKey Manager

YubiKey 5C NFC (19887649) ? Help ? About

yubico Home Applications Interfaces

Set FIDO2 PIN

Home / FIDO2 / Set PIN

The FIDO2 PIN must be at least 4 characters

New PIN _____

Confirm PIN _____

< Back

✓ Set PIN

YubiKey 5C NFC (19887649) ? Help ? About

Home Applications Interfaces

FIDO2 PIN

A PIN is set, 8 retries left

Change PIN

Reset

Restore defaults

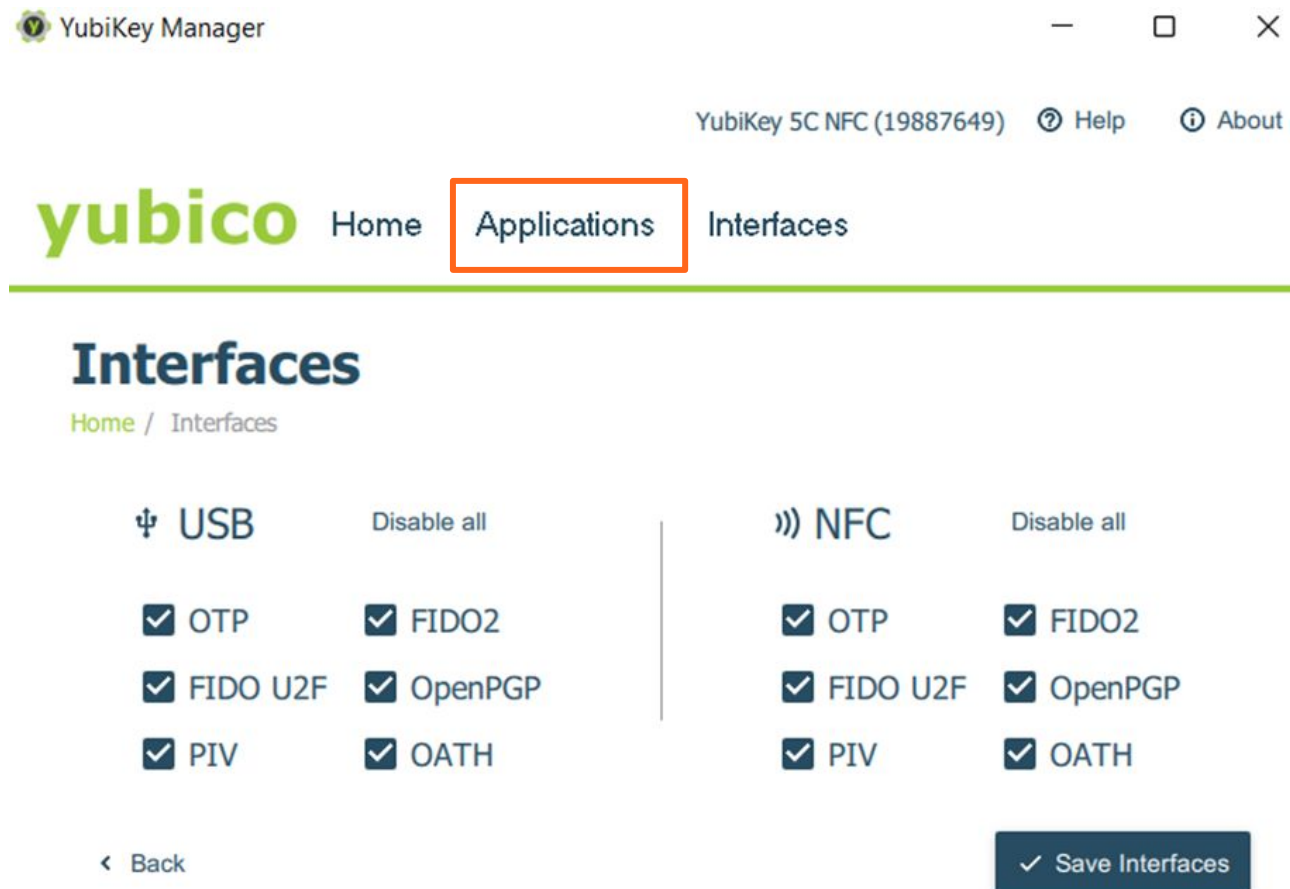
Reset FIDO

< Back

FIDO2 PIN was set

ADMINISTRADOR YUBIKEY

7. En la pestaña "Interfaces" podrás habilitar o deshabilitar las funciones disponibles de tu YubiKey



The screenshot shows the YubiKey Manager web application. At the top, there's a header with the YubiKey Manager logo, the device name 'YubiKey 5C NFC (19887649)', and links for 'Help' and 'About'. Below the header is a navigation bar with the 'yubico' logo and tabs for 'Home', 'Applications' (which is highlighted with an orange border), and 'Interfaces'. The main content area is titled 'Interfaces' and shows a breadcrumb 'Home / Interfaces'. It is divided into two columns: 'USB' and 'NFC'. Each column has a 'Disable all' link and a list of protocols with checkboxes. For USB, the protocols are OTP, FIDO U2F, PIV, FIDO2, OpenPGP, and OATH. For NFC, the protocols are OTP, FIDO U2F, PIV, FIDO2, OpenPGP, and OATH. All checkboxes are currently checked. At the bottom left is a '< Back' link, and at the bottom right is a 'Save Interfaces' button.

YubiKey Manager

YubiKey 5C NFC (19887649) ? Help i About

yubico Home Applications Interfaces

Interfaces

Home / Interfaces

USB	Disable all
☒ OTP	☒ FIDO2
☒ FIDO U2F	☒ OpenPGP
☒ PIV	☒ OATH

NFC	Disable all
☒ OTP	☒ FIDO2
☒ FIDO U2F	☒ OpenPGP
☒ PIV	☒ OATH

< Back

✓ Save Interfaces