CONFIGURACIÓN DE APLICACIONES PARA LA GESTIÓN DE CÓDIGOS DE 2FA: AUTHY

Esta obra está bajo una Licencia Creative Commons Atribución-CompartirIgual 4.0 Internacional.

Última actualización: septiembre 2023

AUTHY

Características:

- Sin costo
- Funciona sin conexión a internet
- Múltiples dispositivos y sincronización entre ellos
- Buena usabilidad. Facilidad de asociación de códigos 2FA a cuentas
- Posibilidad de activación de respaldos cifrados en los servidores de Authy

AUTHY

https://authy.com/



ÍNDICE

CONFIGURACIÓN DE AUTHY

1. Descargar Authy
2. Registro de cuenta
3. Activar respaldos
4. Permitir multidispositivos
5. Activar Protección de la aplicación
6. Agregar cuenta

CONEXO

DESCARGAR

1. Descargar la aplicación “Authy”

Authy es multidispositivo, es decir, puedes descargarlo en diferentes equipos con diferentes sistemas operativos como **Android, iPhone, Windows, macOS y Linux.** Los cambios que hagas en un dispositivo se sincronizarán en los restantes.

Para comenzar, te recomendamos que descargues Authy en tu teléfono celular.

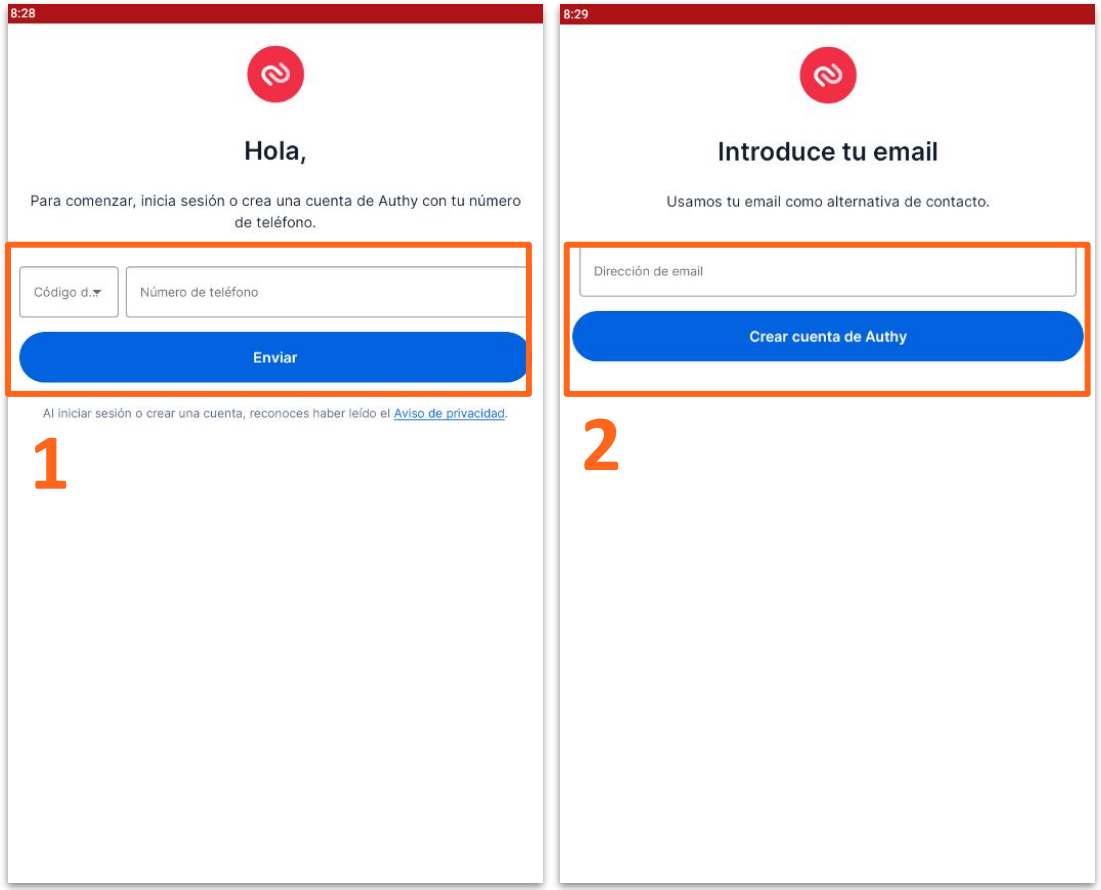




REGISTRO DE CUENTA

2. Registro de cuenta

Para el registro de cuenta debes agregar tu número de teléfono celular y tu correo electrónico.



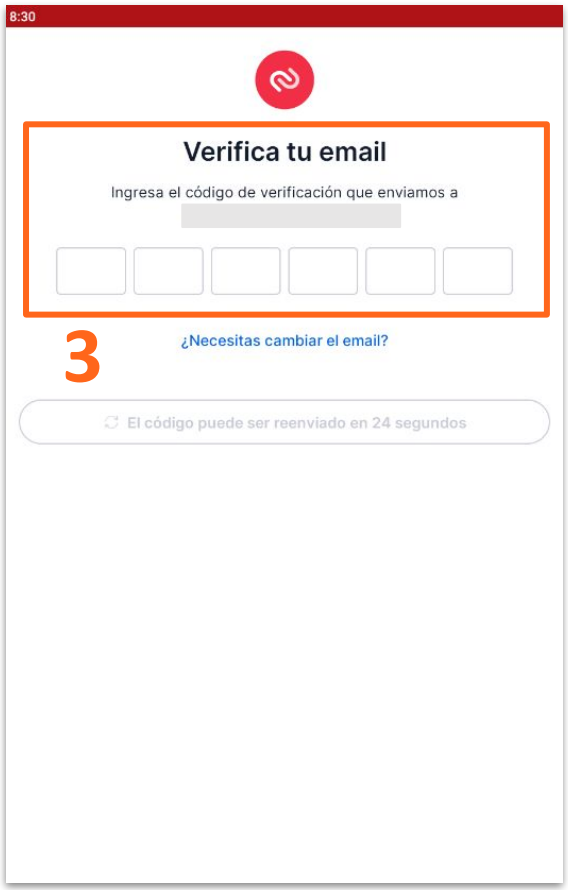
- ➔ Introduce tu número de teléfono y haz clic en "**Enviar**"
- ➔ Introduce tu correo electrónico y haz clic en "**Crear cuenta de Authy**"

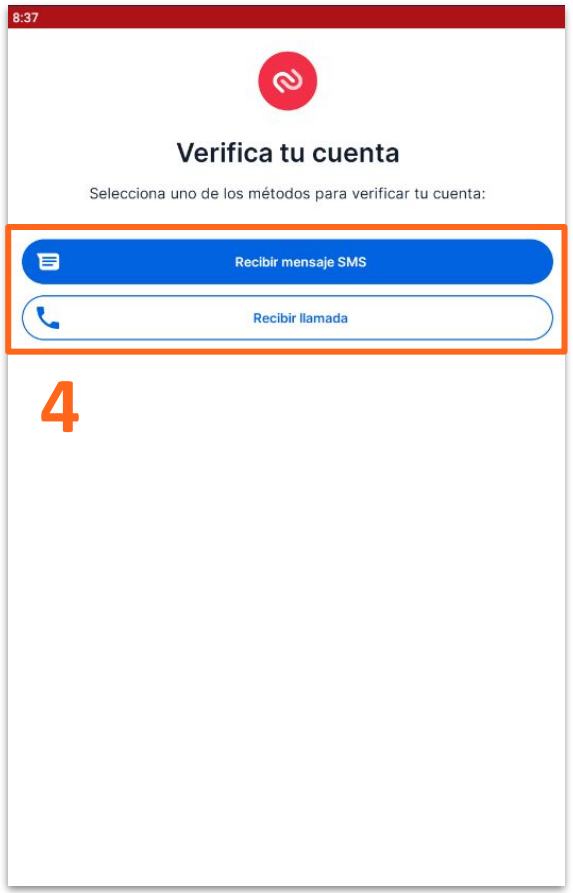


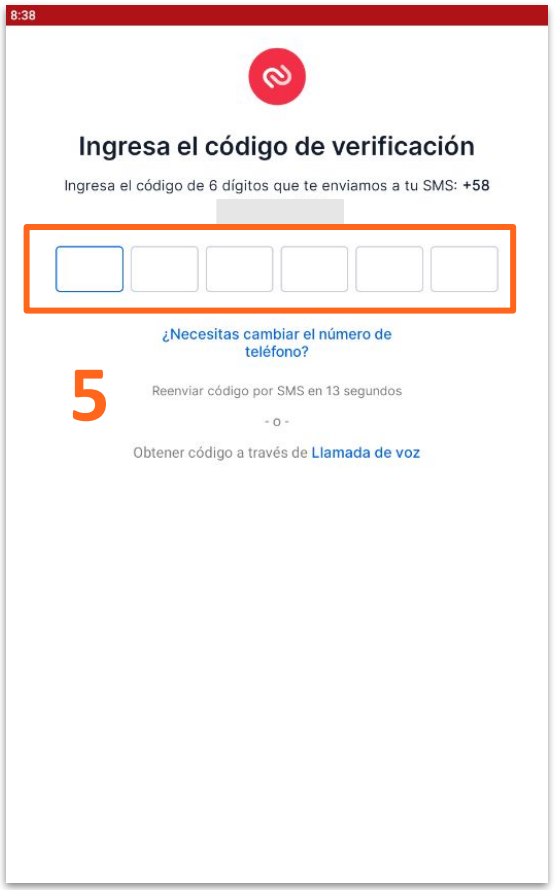
REGISTRO DE CUENTA

2. Registro de cuenta

➔ Authy te enviará un código a tu correo electrónico para verificarlo y luego un SMS para verificar tu teléfono y cuenta.







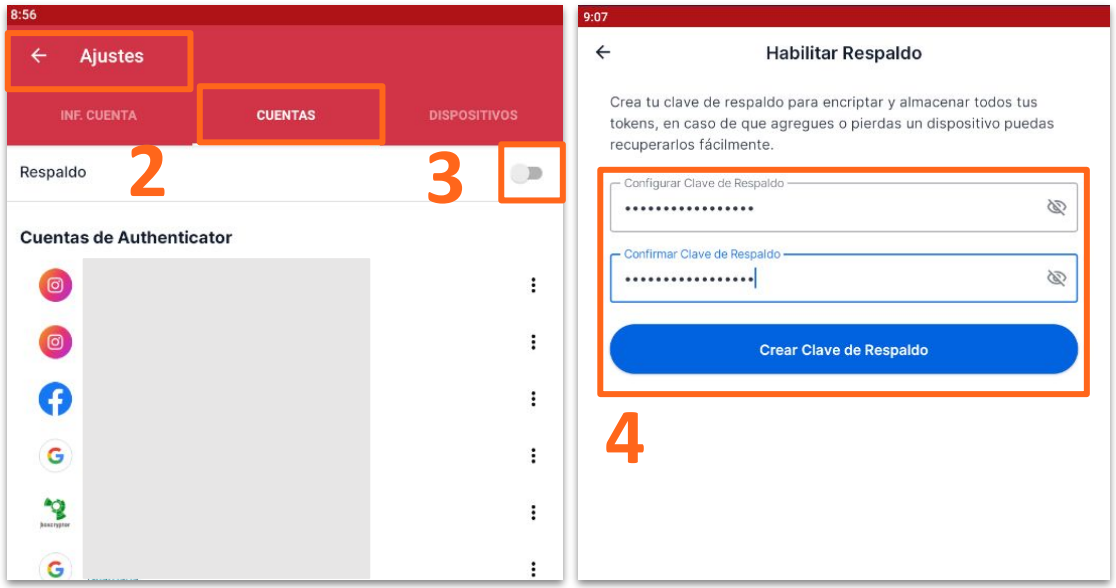


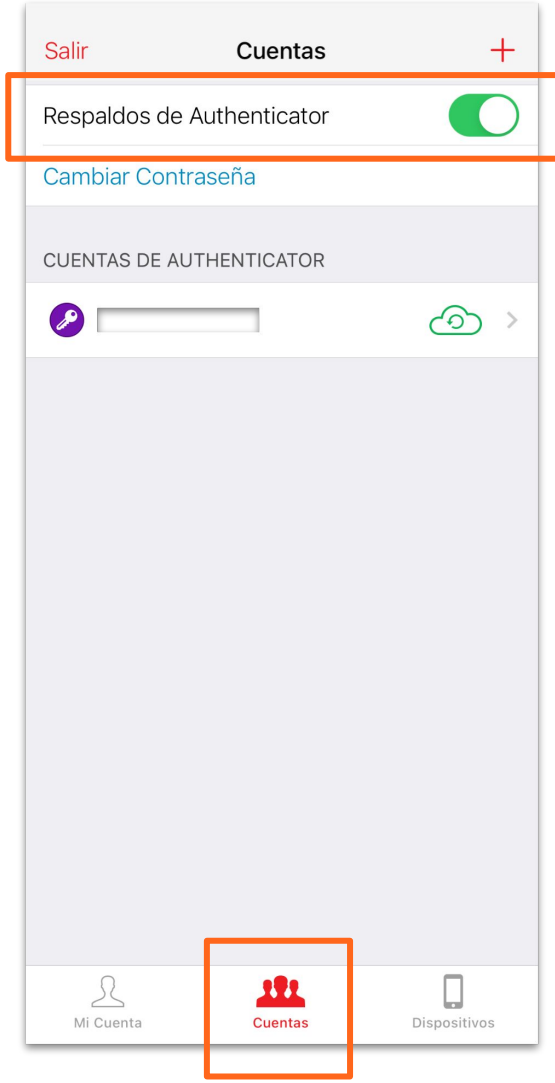
RESPALDOS

3. Activar respaldos

Desde el menú de **"Ajustes"** puedes activar la creación de **respaldos cifrados en los servidores de Authy.** Esto es una alternativa para recuperar tus códigos de doble factor en caso de pérdida, robo o extravío de los dispositivos donde hayas configurado la aplicación.

Para activar los respaldos debes **configurar una contraseña**. Considera que esta debe tener todas las **características de seguridad** para que no se convierta en una puerta de entrada para los atacantes.





Menú ⋮ > Ajustes > Cuentas > Activar Respaldo > Crear clave de respaldo

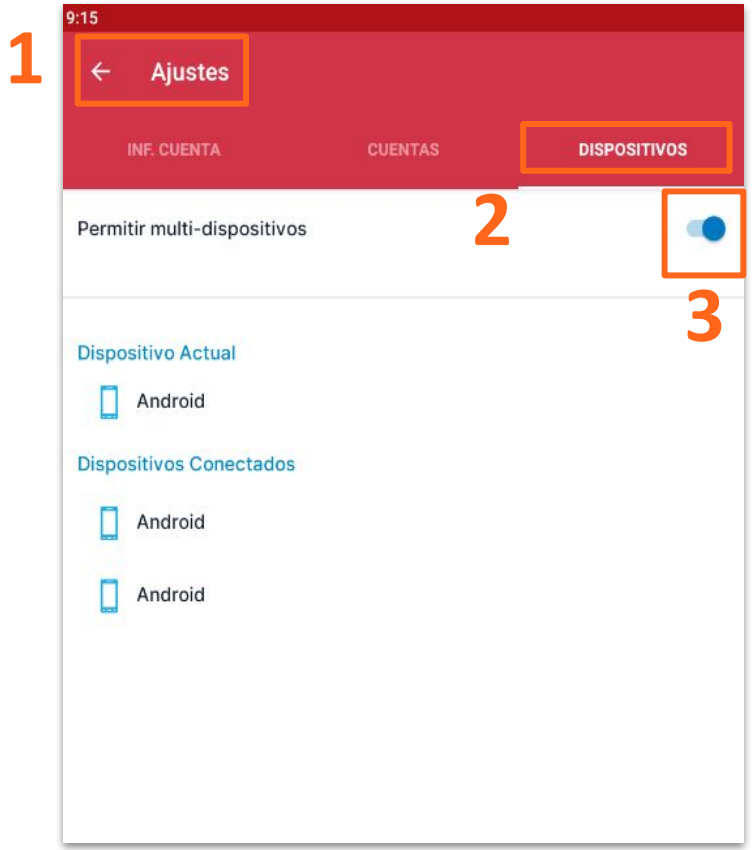
MULTIDISPOSITIVOS

4. Permitir multidispositivos

La característica “Multi-dispositivos” se puede utilizar para permitir que varios dispositivos de confianza utilicen la misma cuenta Authy. Esta puede ser una buena opción cuando tienes varios dispositivos, como un teléfono móvil y una computadora.

Después de que se activen los respaldos y hayas configurado Authy en los dispositivos de confianza que necesites, es conveniente que **deshabilites** la característica **“permitir Multi-dispositivos”** para evitar el riesgo de que un tercero no autorizado agregue un nuevo dispositivo. Esto aún te permitirá acceder a tu cuenta desde todos los dispositivos existentes.





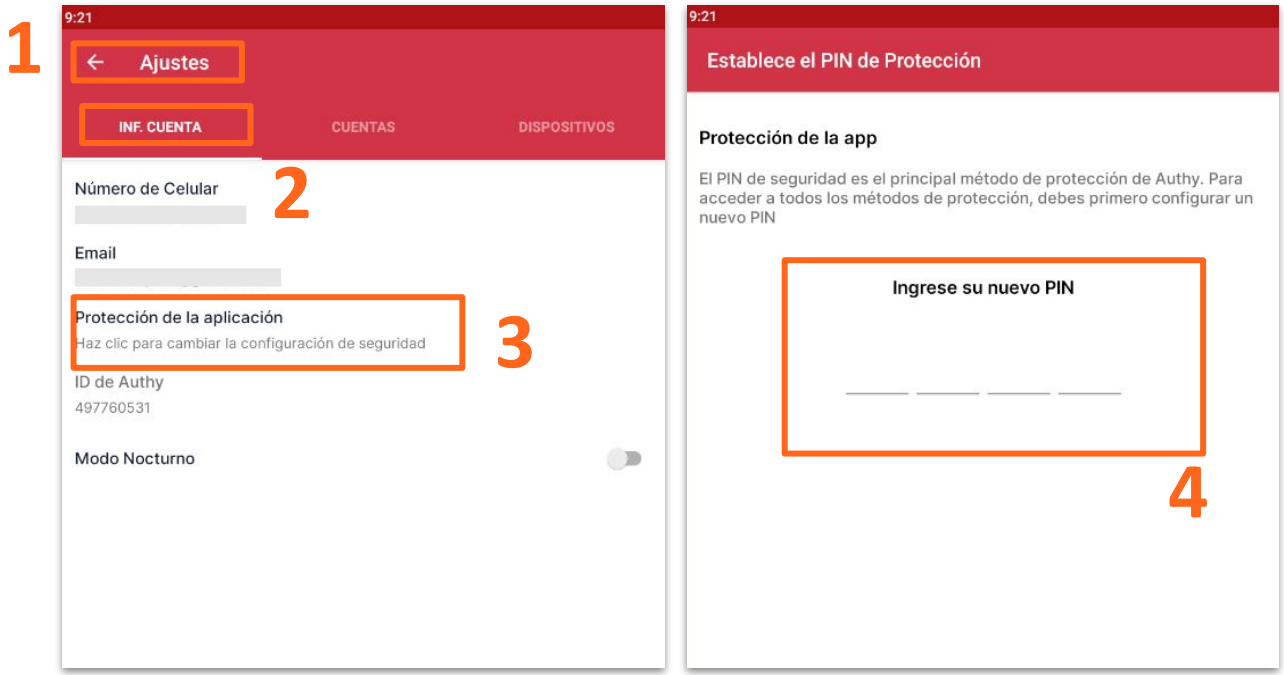
Menú ⋮ > Ajustes > Dispositivos > Permitir Multi-dispositivos

MULTIDISPOSITIVOS

5. Activar Protección de la aplicación

La característica “Protección de la aplicación” se activa para agregar un nivel de seguridad al acceso de los códigos de doble factor necesarios para iniciar sesión en las cuentas configuradas. Puedes activarla mediante un **PIN de cuatro dígitos,** o a través de tus **Datos Biométricos (Huella).**

Nota: Este PIN de seguridad es diferente a la contraseña que se utiliza para acceder a los respaldos en la Nube

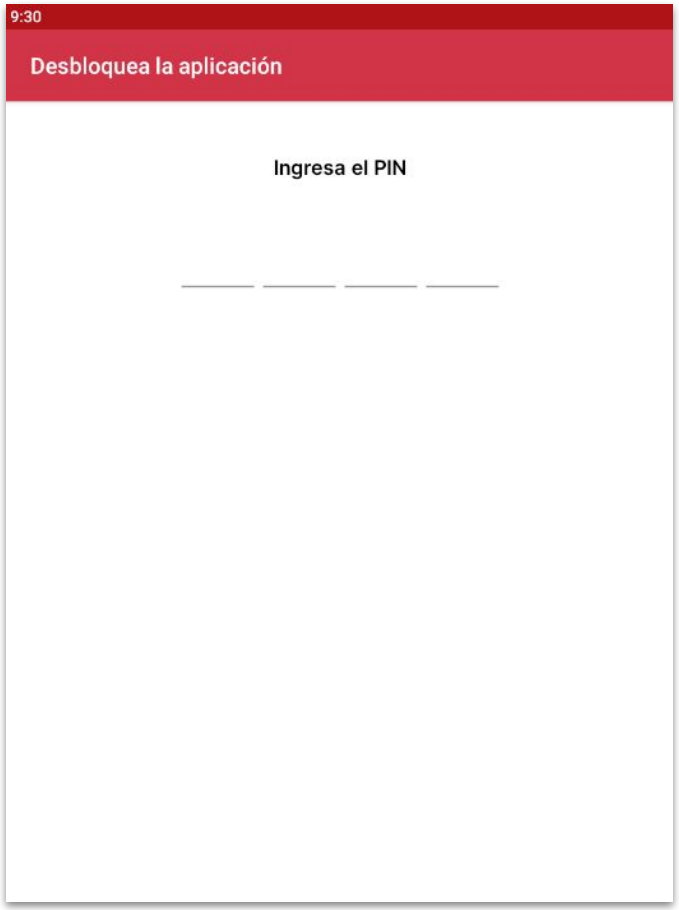


Menú ⋮ > Ajustes > Inf. Cuenta > Protección de la aplicación > Crear PIN

MULTIDISPOSITIVOS

5. Activar Protección de la aplicación

Luego de activarlo, cada vez que ingreses a la aplicación, te solicitará tu PIN o tu huella dactilar.







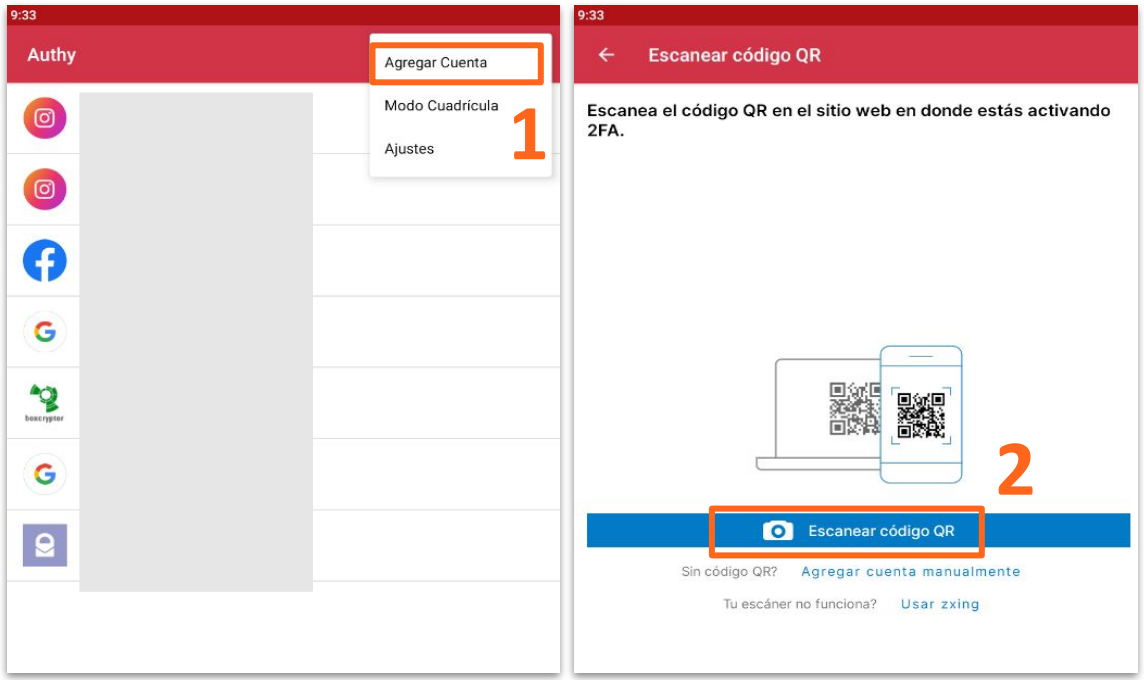
AGREGAR CUENTA

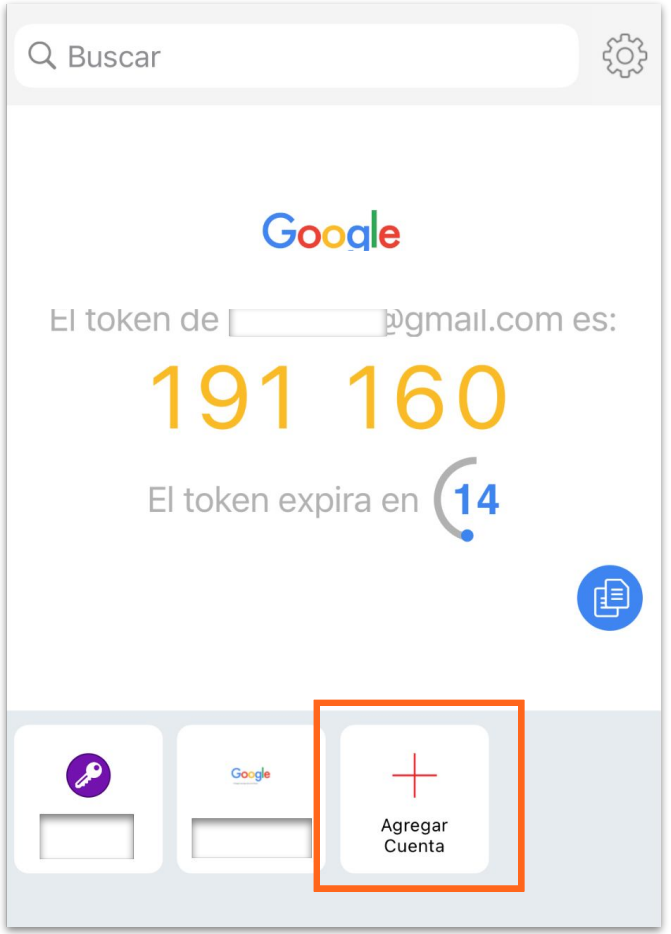
6. Agregar cuenta

La activación de la autenticación de dos factores se realiza con cada cuenta de usuario que tengas (y que permita activar esta característica).

Para agregar una cuenta en Authy presiona:

Menú ⋮ > Agregar cuenta > Escanear código QR





AGREGAR CUENTA

Así se verá la aplicación “Authy” en tu teléfono móvil cuando hayas activado la autenticación de dos factores en varias de tus cuentas de usuario.

El número de 6 dígitos asociado a cada cuenta, será el código de doble factor que de ahora en adelante necesitarás para iniciar sesión (además de tu contraseña).

