

Manual de Usuario de Multifactor Autenticación MFA para el portal de MasterConsultas.

Contenido

¿Qué es MFA?.....	2
¿Por qué es necesaria la autenticación multifactor (MFA)?.....	2
¿Cuáles son los beneficios de la autenticación multifactor?.....	2
Implementación de la aplicación Google Authenticator para el sitio de MasterConsultas .	2
Funcionamiento básico en el portal de MasterConsultas.....	3
Instalación de la aplicación de Google Authenticator en el dispositivo móvil del usuario .	3
Acceder a MasterConsultas y registrar el dispositivo móvil por primera vez.....	5
Pasos para el registro de MFA (Multifactor Authentication).....	7
Ingresar a MasterConsultas con la cuenta de usuario del portal y con la cuenta de MFA ya registrada.....	11
Administración de dispositivos registrados en la cuenta de MFA.....	13
Apéndice A, Cambiar los nombres de los dispositivos asociados en la aplicación Google Authenticator.....	14

¿Qué es MFA?

La autenticación multifactor (MFA) es un proceso de registro en dos pasos que requiere que los usuarios ingresen algo más de información que simplemente una contraseña. Por ejemplo, junto con la contraseña, los usuarios deberán ingresar un código que se envía a su correo electrónico, responder a una pregunta secreta o escanear una huella dactilar. Una segunda forma de autenticación puede ayudar a evitar el acceso no autorizado a una cuenta si la contraseña del sistema se ha visto expuesta.

¿Por qué es necesaria la autenticación multifactor (MFA)?

La seguridad digital es fundamental en el mundo de hoy, ya que tanto empresas como usuarios almacenan información confidencial en línea. Este tipo de autenticaciones actúan como una capa adicional de seguridad, fomentando mejores prácticas de resguardo de información y previniendo estafas o robos de datos sensibles.

Las empresas que utilizan autenticación multifactor pueden validar identidades de usuarios y brindar un acceso rápido y práctico a los usuarios autorizados.

¿Cuáles son los beneficios de la autenticación multifactor?

- **Reduce el riesgo de seguridad**

La autenticación multifactor reduce los riesgos derivados de errores humanos, contraseñas extraviadas y dispositivos perdidos.

- **Permite iniciativas digitales**

Para ofrecer una plataforma digital con confianza, incorporamos esta autenticación multifactor para proteger sus datos, generando un entorno de interacción en línea aún más seguro.

- **Mejora la respuesta de seguridad**

De esta manera es posible configurar un sistema de autenticación multifactor para enviar activamente una alerta en cuanto se detecten intentos sospechosos de inicio de sesión. Esto ayuda a responder rápidamente a ciberataques, minimizando cualquier daño potencial

Implementación de la aplicación Google Authenticator para el sitio de MasterConsultas

Google Authenticator es una aplicación disponible en móviles Android y iOS que nos permite añadir un nivel adicional de seguridad a nuestras cuentas. Forma parte del grupo de apps que habilitan la verificación en dos pasos.

➔ Funcionamiento básico en el portal de MasterConsultas



imagen 1

En la *imagen 1* se muestran cuatro pasos para acceder a la aplicación MasterConsultas:

1. Se accede al portal MasterConsultas con el usuario y contraseña del portal.
2. Se accede a la aplicación Google Authenticator para obtener la clave de acceso, que se compone de seis dígitos.
3. Se introduce la clave de acceso en el portal de MasterConsultas, obtenida desde la aplicación Google Authenticator.
4. Una vez introducida la clave de acceso, validada en el portal de MasterConsultas, se accede a dicho portal.

➔ Instalación de la aplicación de Google Authenticator en el dispositivo móvil del usuario

Para poder acceder al portal de MasterConsultas junto con la autenticación multifactor de Google Authenticator, se requiere lo siguiente:

1. Tener una cuenta de acceso al portal de MasterConsultas con su respectiva contraseña.
2. Contar con un dispositivo móvil (celular) con Sistema Operativo Android o IOS.
3. Poseer acceso a internet desde el dispositivo Móvil.
4. Tener una Cuenta Google para poder descargar e instalar la aplicación Google Authenticator.

Pasos de Instalación

1. Desde la aplicación móvil, abrir la aplicación Google Play.

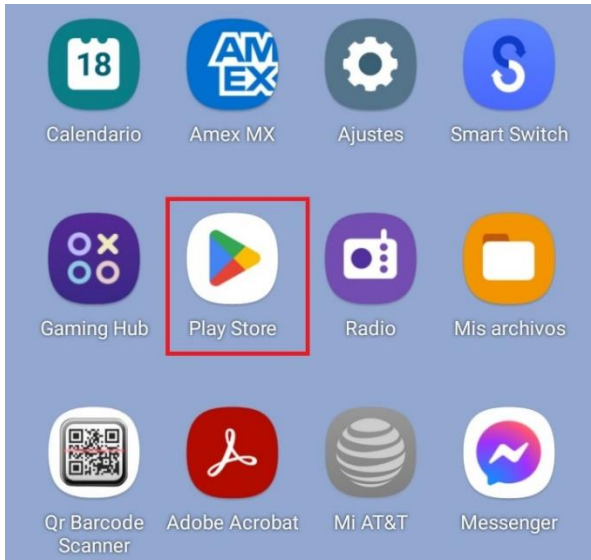


imagen 2

- 1.1. En el catálogo de aplicaciones de Google Play, buscar la aplicación Google Authenticator. Instalar la aplicación siguiendo los tres pasos de instalación mostrados en la siguiente imagen.



imagen 3

- 1.2. Verificar que la aplicación se encuentre instalada en el dispositivo móvil, como se muestra en la imagen4 con el ícono de la aplicación.



imagen 4

- 1.3. Abrir la aplicación y comprobar su correcto funcionamiento.



imagen 5

➔ Acceder a MasterConsultas y registrar el dispositivo móvil por primera vez

Para el acceso al portal de MasterConsultas se ingresa con la cuenta y contraseña del usuario.

imagen 6

El portal de acceso a MasterConsultas muestra dos leyendas:

1. ¡ATENCIÓN! Desde el día dd-mm-aaaa es obligatorio contar con un segundo factor de autenticación mediante la aplicación de Google Authenticator en su dispositivo móvil, donde deberá estar previamente registrado. Más información sobre cómo usar la aplicación haciendo click aquí. (Link al tutorial de Google Authenticator).

2. Obtenga el manual de usuario de segundo factor de autenticación MFA haciendo click aquí.
(Link de acceso para descargar y visualizar este manual de usuario)

Pasos para el registro de MFA (Multifactor Authentication)

Primero se debe acceder al portal con el usuario y contraseña de la cuenta:

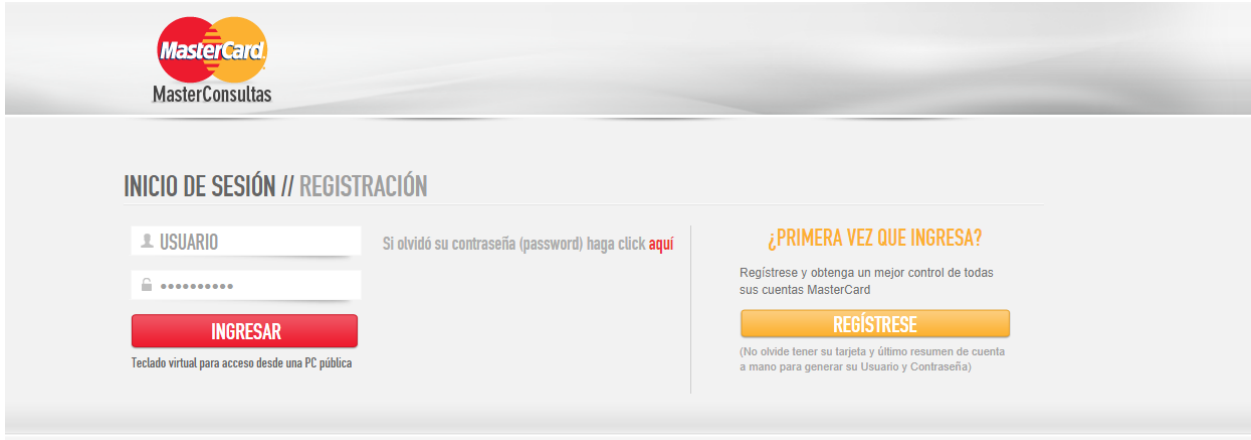


imagen 7

Una vez que se accede portal de MasterConsultas con el usuario y contraseña, el portal comprueba si la cuenta del usuario ya está registrada con el registro de multifactor de autenticación asociada a Google Authentication.

En este ejemplo, el usuario **no tiene cuenta asociada**, por lo que se muestra la siguiente página para registrar el MFA, que consiste en 3 sencillos pasos.

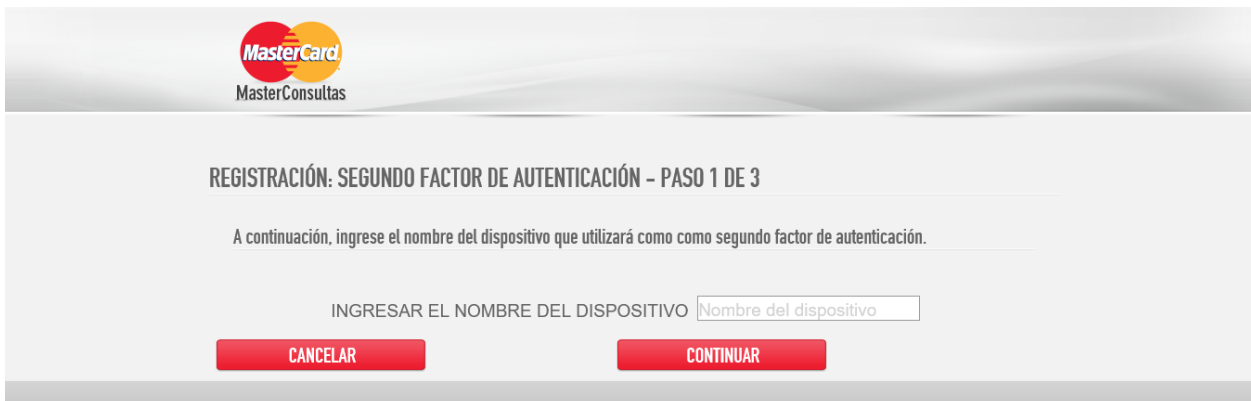


imagen 8

Paso 1 de 3: Se debe **introducir un nombre** en el campo “INGRESAR EL NOMBRE DEL DISPOSITIVO”, con la finalidad de asociar dicho nombre con el dispositivo que se utilizará para la autenticación con la cuenta del usuario. Se puede ingresar cualquier valor alfanumérico, guiones “-“ y guion inferior “_” o espacios en blanco. Cualquier otro carácter que sea introducido no es válido.

Por ejemplo: Motorola 45

A continuación, ingrese el nombre del dispositivo que utilizará como segundo factor de autenticación.


INGRESAR EL NOMBRE DEL DISPOSITIVO

CANCELAR **CONTINUAR**

imagen 9


Clickear [Continuar](#). En cualquier momento puede cancelar la operación y regresar a la página de inicio de MasterConsultas.

Paso 2 de 3: Se debe [registrar](#) el factor de autenticación en el dispositivo móvil, ya sea escaneando el QR o ingresando la clave de configuración.


MasterConsultas

REGISTRACIÓN: SEGUNDO FACTOR DE AUTENTICACIÓN - PASO 2 DE 3

Escanee el siguiente código QR con la aplicación Google Authenticator instalada en su dispositivo:



Código QR que escanea con la Aplicación Google Authenticator instalada en su dispositivo móvil.

Ante inconvenientes con el escaneo, ingrese la siguiente clave de configuración en la aplicación Google Authenticator instalada en su dispositivo: **DERIC8E6JVD2CNEKMQO3UY7NOKILMH**

Clave de configuración que se puede introducir con la aplicación Google Authenticator instalada en el dispositivo móvil.

Una vez obtenido el código de seis dígitos en la aplicación Google Authenticator ingrésela en el siguiente campo

Introducir la clave de 6 dígitos que proporciona la aplicación Google Autenticación en el dispositivo móvil.

Por último, haga click en **CONTINUAR**.

CANCELAR **CONTINUAR**

Imagen 10

a) Abrir la aplicación Google Authenticator instalado en el dispositivo móvil:



imagen 11

b) **Clickear** en *Agregar un código*. Se mostrará la siguiente pantalla del dispositivo móvil:

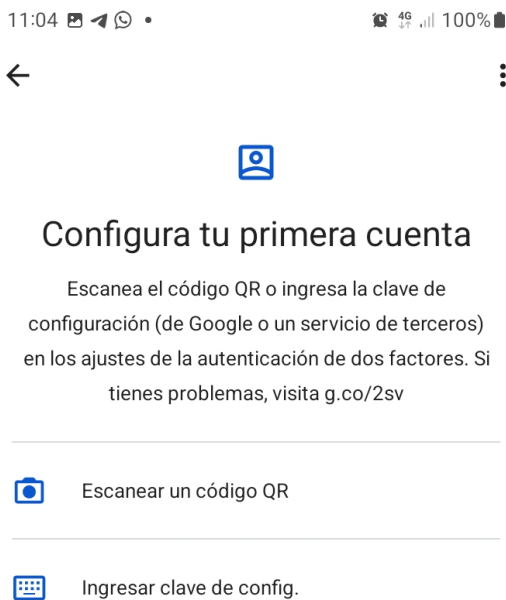


imagen 12

Se tienen dos opciones:

- i. Seleccionar *Escanear un código QR* y, a continuación, escanear el código QR mostrado en la pantalla de MasterConsultas

- ii. Seleccionar *Ingresar clave de config.* e ingresar la clave que figura en la pantalla (en este ejemplo es N5WUYM4BL2VZX3SWVL6RV6B36XSJBQI2). Introducir el nombre del dispositivo, que debe ser el mismo nombre que se colocó en el paso 1.

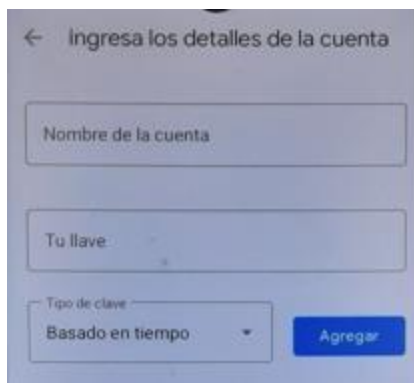


imagen 13

- c) Una vez realizada la captura vía QR o vía clave de configuración, la aplicación Google Authenticator del dispositivo móvil mostrará una **clave de seis dígitos**. Esta clave debe ser ingresada en MasterConsultas en el campo que señala la leyenda: **“AHORA INGRESE EL CÓDIGO OBTENIDO DEL DISPOSITIVO DE 6 DÍGITOS”** (imagen 9). **Clickear aceptar**. Nota: se dispone de 40 segundos para ingresar el código. Una vez excedido el tiempo Google Authenticator generará un nuevo código.

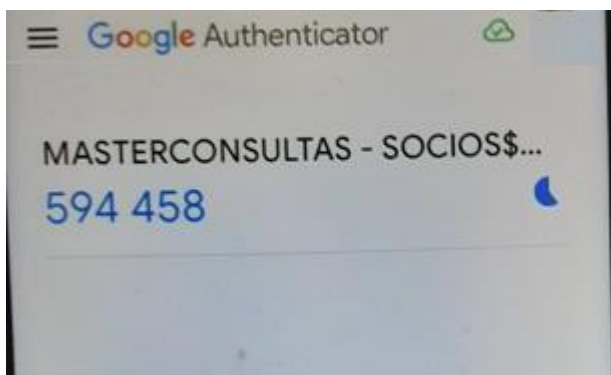


imagen 14

Paso 3 de 3. Una vez que el dispositivo se ha registrado correctamente, se debe **introducir la clave de seis dígitos** generada con Google Authenticator en el portal de MasterConsultas.



imagen 15

Cabe señalar que, en el paso 2, los 6 dígitos que se solicitan son para activar el dispositivo en la aplicación de Google Authenticator, en este paso se introduce “INGRESE EL CÓDIGO DE 6 DÍGITOS” para acceder al portal de MasterConsultas.

Ingresar el código de 6 dígitos con la aplicación de Google Authenticator del dispositivo móvil, tal como se muestra en la imagen 15, de donde se genera el código de 6 dígitos.

Finalmente se accede a la página principal MasterConsultas.

Ingresar a MasterConsultas con la cuenta de usuario del portal y con la cuenta de MFA ya registrada

Paso 1. Ingresar el usuario y contraseña del portal de MasterConsultas.



Imagen 16

Paso 2. Después de introducir el usuario y contraseña de la página de inicio de MasterConsultas, aparece la siguiente página.



Imagen 17

La página muestra el listado de dispositivos registrados la aplicación de Google Authenticator. Notar que en el apartado anterior se registró el dispositivo con el nombre Motorola 45 y este aparece en la lista. Seleccionar el dispositivo deseado.

Paso 3. A continuación se muestra la siguiente página.



Imagen 18

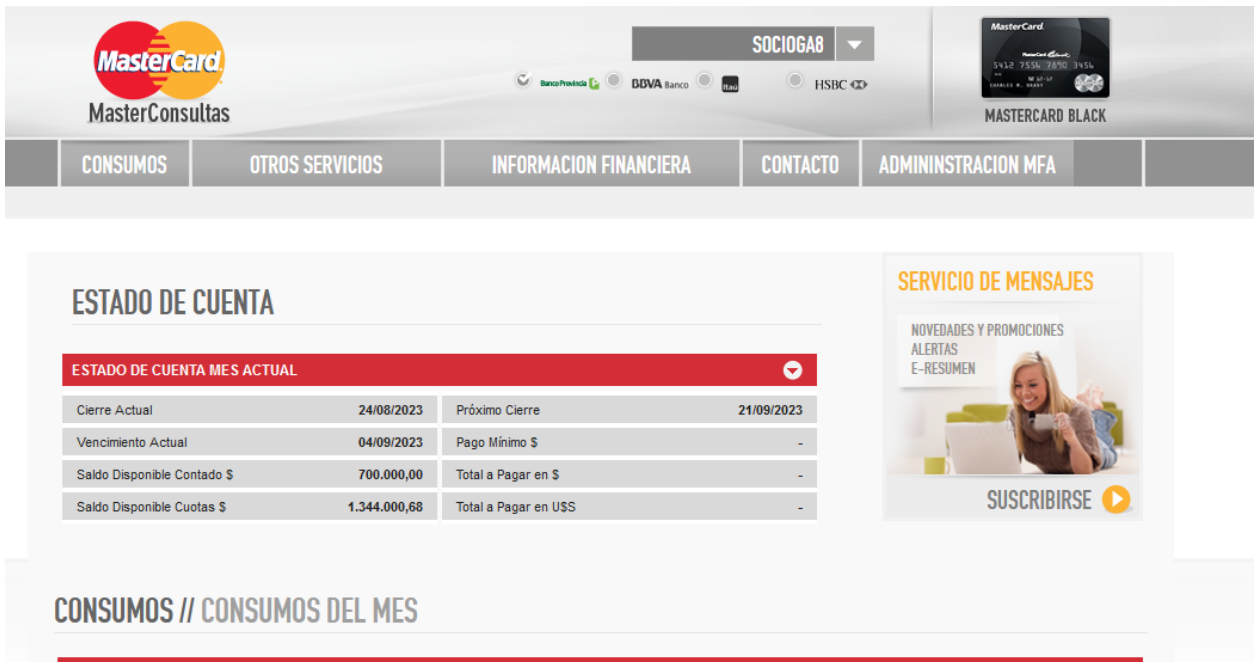
Al seleccionar el dispositivo deseado, Google Authenticator generará un código de 6 dígitos en el dispositivo móvil (imagen 15). El mismo debe ser ingresado en MasterConsultas. Clickear [Continuar](#).

Finalmente se accede a la página principal MasterConsultas.

Administración de dispositivos registrados en la cuenta de MFA

En esta sección se muestran algunas características para el manejo de la cuenta asociada con MFA, y eliminar o agregar un dispositivo con la aplicación Google Authenticator con la cuenta asociada con el portal de MasterConsultas.

Una vez que haya accedido al portal de MasterConsultas, en la página de inicio se muestra la entrada de menú *ADMINISTRAR DISPOSITIVOS*.



The screenshot displays the MasterConsultas portal interface. At the top, there is a navigation bar with the MasterCard logo on the left, a dropdown menu for 'SOCIOGAB' in the center, and a MasterCard Black card image on the right. Below the navigation bar is a horizontal menu with the following items: CONSUMOS, OTROS SERVICIOS, INFORMACION FINANCIERA, CONTACTO, and ADMINISTRACION MFA. The main content area is divided into two sections. The left section is titled 'ESTADO DE CUENTA' and contains a table with account details. The right section is titled 'SERVICIO DE MENSAJES' and features a promotional banner for 'NOVEDADES Y PROMOCIONES', 'ALERTAS', and 'E-RESUMEN' with a 'SUSCRIBIRSE' button. Below the account status section, there is a header for 'CONSUMOS // CONSUMOS DEL MES'.

ESTADO DE CUENTA MES ACTUAL			
Cierre Actual	24/08/2023	Próximo Cierre	21/09/2023
Vencimiento Actual	04/09/2023	Pago Mínimo \$	-
Saldo Disponible Contado \$	700.000,00	Total a Pagar en \$	-
Saldo Disponible Cuotas \$	1.344.000,68	Total a Pagar en US\$	-

Imagen 19

Cuando se ingresa en la opción de *ADMINISTRAR DISPOSITIVOS* se muestra un listado de los nombres de los dispositivos MFA asociados con el portal de MasterConsultas.



Es posible realizar las siguientes gestiones:

1. Al seleccionar el nombre de un dispositivo del listado mostrado de los dispositivos registrados, el mismo será eliminado.
2. Se puede agregar un nuevo dispositivo haciendo click en **AGREGAR DISPOSITIVO**.

Para agregar un dispositivo por primera vez se deberán seguir los pasos de la sección *Acceder a MasterConsultas y registrar el dispositivo móvil*.

Apéndice A, Cambiar los nombres de los dispositivos asociados en la aplicación Google Authenticator.

Se puede renombrar el nombre del dispositivo en la aplicación Google Authenticator con el nombre registrado en la aplicación Master Consultas Socios, con los siguientes pasos:

Paso 1. En la aplicación Google Authenticator seleccionar el dispositivo a renombrar, por ejemplo, el dispositivo que dice MASTERCONSULTAS-SITIO-SOCIOS, que es el nombre por default de cuando se agrega un dispositivo en Master Consultas Empresas MCS, con MFA. Pulsar el ícono que representa un lápiz.

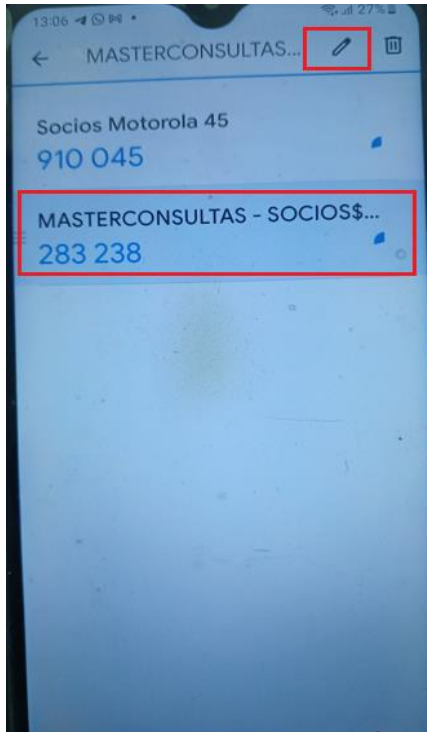


Imagen 20

Paso 2. Editar el nombre en el campo que dice Nombre de la Cuenta a elección, por ejemplo, se escribe Samsung A24. Para guardar los cambios, pulsar el botón Guardar.

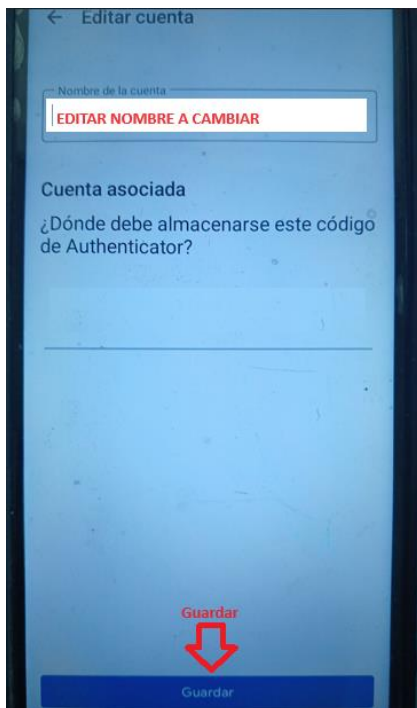


imagen 21

Paso 3. Los cambios quedan realizados.

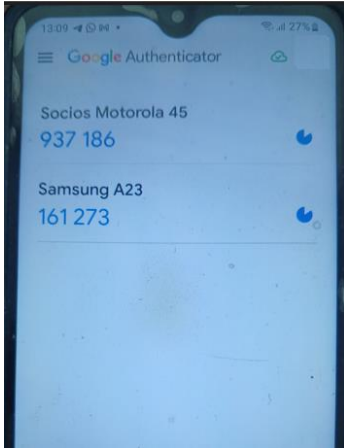


imagen 22