

Panel 640-zone IP + 4G home security system via radio (Z-wave)



Welcome to the **VESTA Wireless and Hybrid Control Panels Knowledge Base**. Here, you'll find all the essential information for installing, configuring, and maintaining VESTA security control panels that operate via wireless communication and hybrid systems.

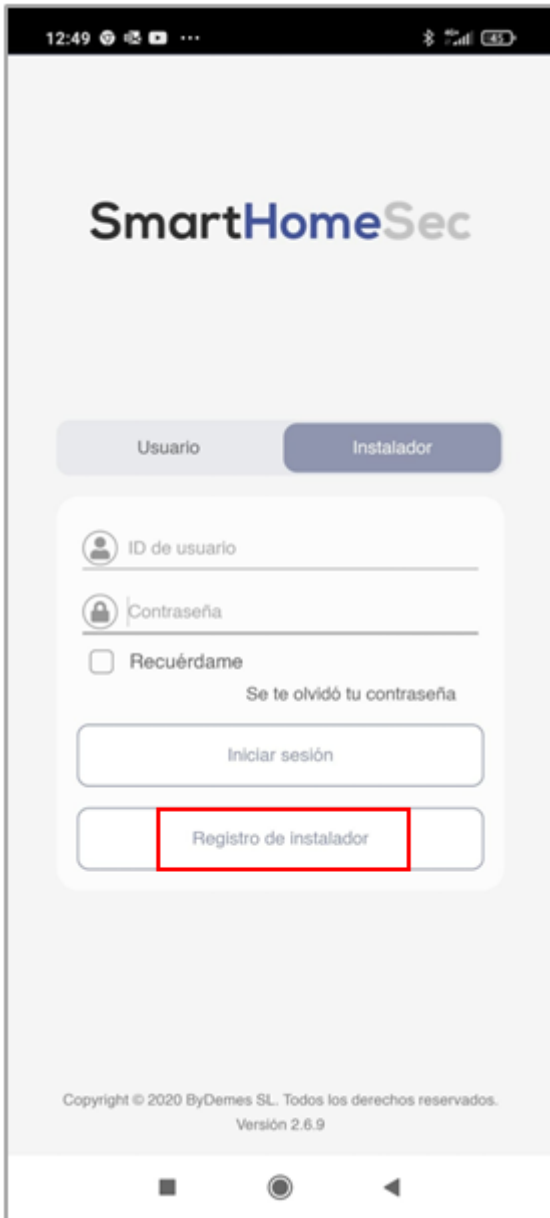
This manual is designed for technicians, integrators, and advanced users who need a detailed understanding of these control panels. It includes step-by-step guides, troubleshooting tips, device compatibility, and best practices to optimize system performance.

QUICK GUIDE

1. Panel Registration as Installer and User

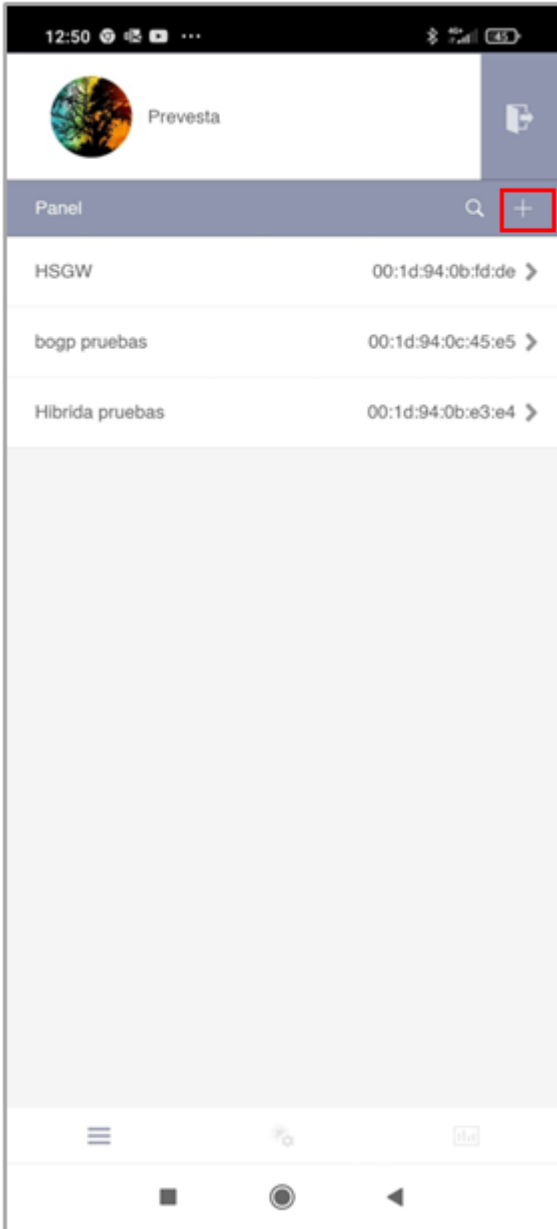
1.1 Installer Registration

Step 1: Log in as an installer in the [SmartHomeSec](#) APP



Step 2: Select the + button

(Add panel)



Step 3: Enter the panel's MAC address found on a label of panel

The screenshot shows a mobile application interface for adding a panel. At the top, the status bar displays the time 12:50, signal strength, and battery level at 43%. The title of the screen is "Agregar panel". Below the title, there are several input fields:

- Dirección MAC:** A field with a red border containing the text "00 1d 94" followed by four empty boxes.
- Nombre del panel:** A text input field with a microphone icon on the left.
- Número de teléfono:** A field with a dropdown menu showing "Argentina - 54" and a telephone icon on the left.
- Ubicación del panel:** A section containing three sub-fields: "Dirección", "Ciudad", and "Provincia" (with "Código postal" next to it).

At the bottom of the form is a blue button labeled "Enviar". The Android navigation bar is visible at the very bottom.

Once the panel is registered as an installer, it is ready ✨ for configuration.

The panel must be on and connected to the internet. We have 15 minutes after powering it up to register the panel.

The MAC of the panel is always on one side of the panel physically. In the NAME field, we should place the subscriber or any identifier of the panel.

2. User Account Registration

The user account is used to control the system and is intended for the end user. From the SmartHomeSec APP, this account allows arming, disarming, and performing any operation. There are two types of user accounts: Master and Slave.

The first account we register is the Master. The main difference between the Master and Slave accounts is that the Master allows creating new users, while the Slave cannot create new accounts.

Step 1: Access the panel as installers, the default code is [7982]

15:18



ab



Equipo



AB1234 - FORMACIÓN SEC
00:1d:94:0d:3c:2a

1 7 >

SHOWROOM BCN ACHRAF
00:1d:94:10:d5:06

0 8 >

HYBRID LITE SICUR
00:1d:94:1b:23:62

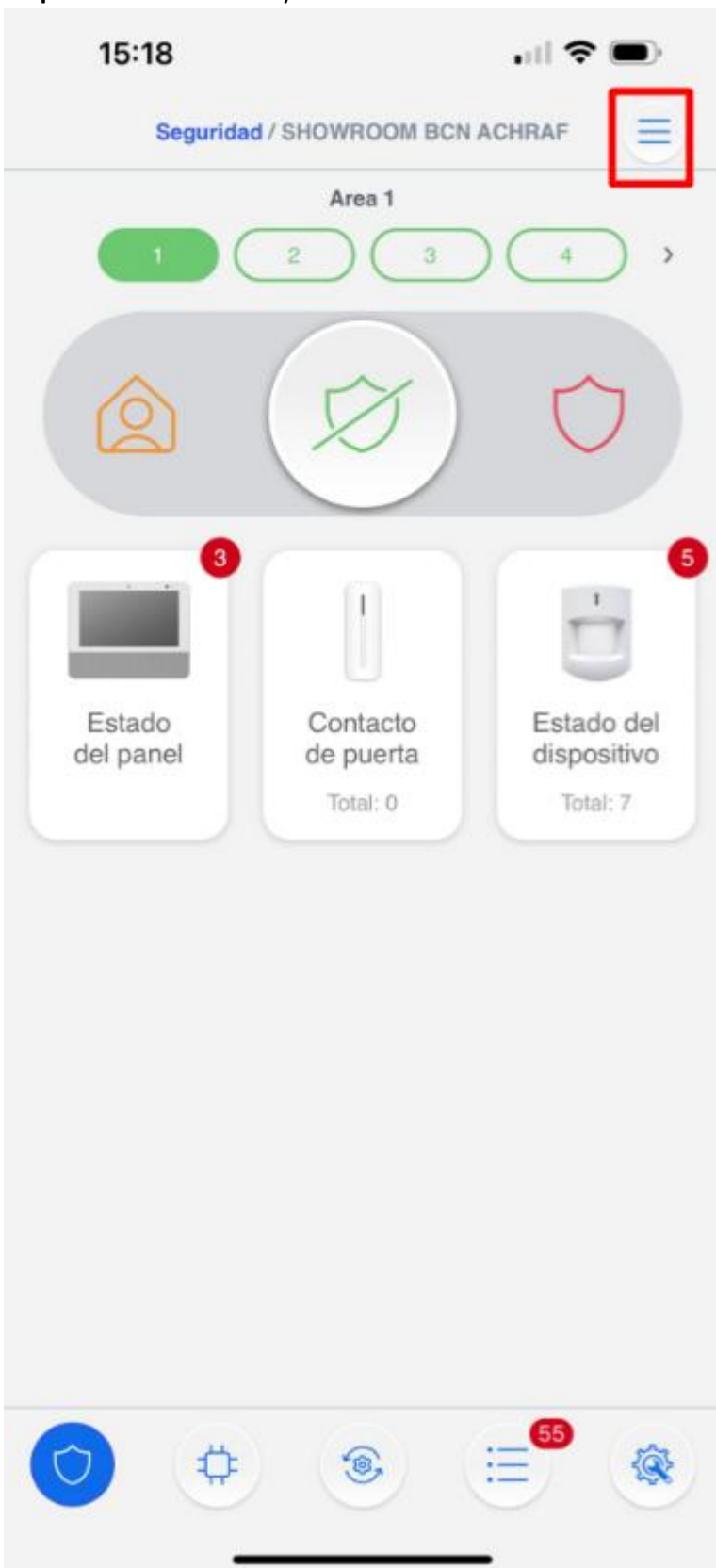
Fuera de línea >

CENTRAL ACHRAF LAB
00:1d:94:1a:93:93

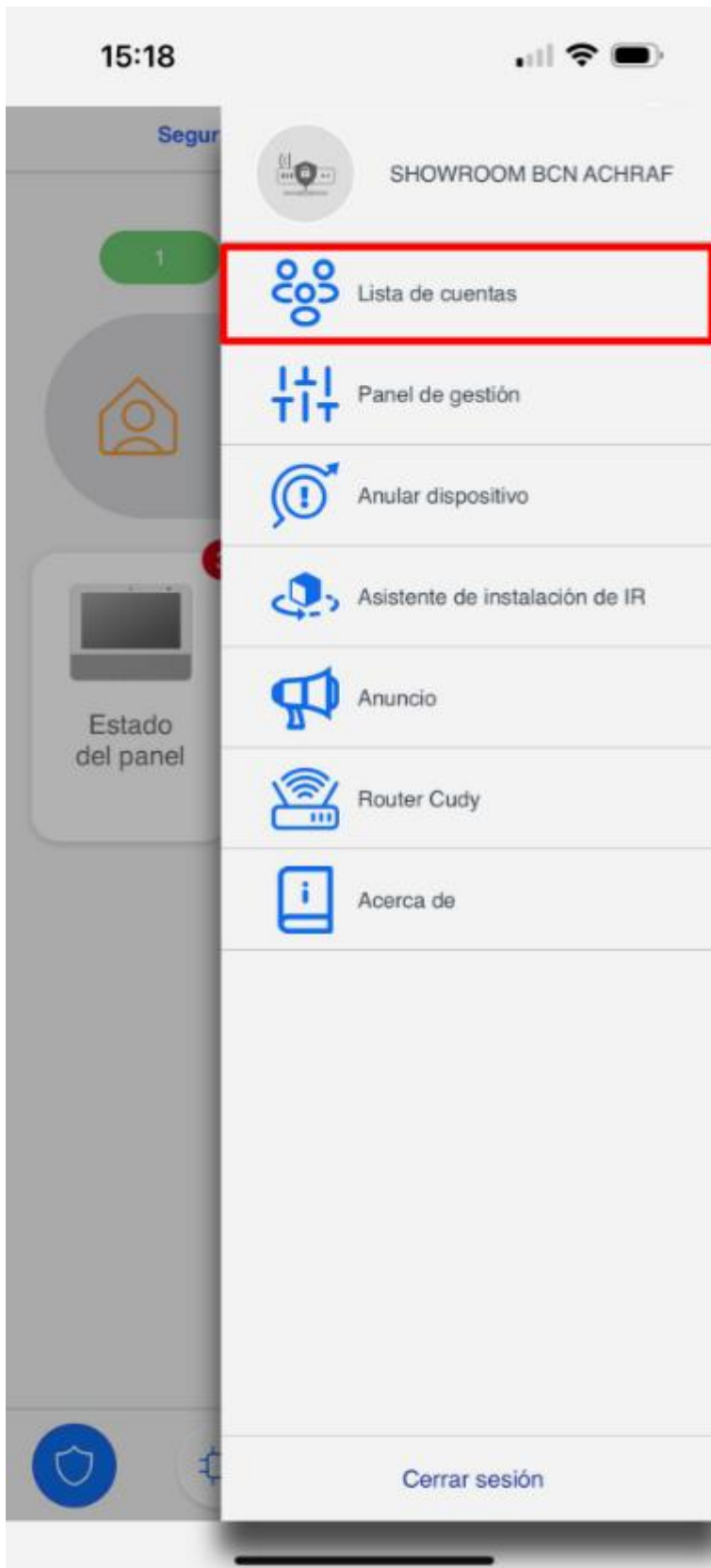
Fuera de línea >



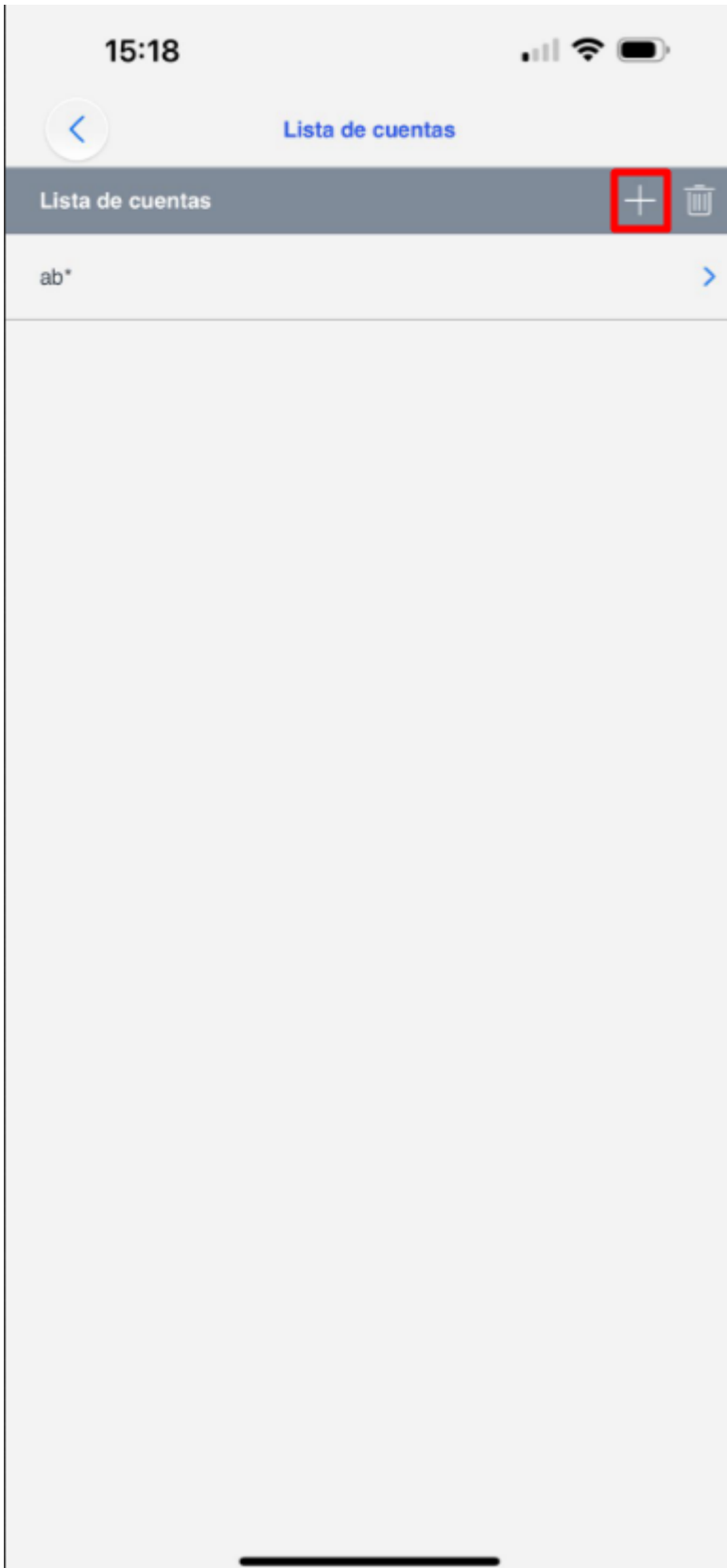
Step 2: Select the Main system menu section



Step 3: Select account list



Step 4: Select add



Step 5: If it's a new user: Select create an account

15:18



Añadir cuenta

¿Desea crear una nueva cuenta u otorgar acceso para una cuenta existente a este panel?

Crear una cuenta

Enlace a cuenta existente

Step 6: Fill in the user data for APP access

15:18 📶 📶 🔋

[←](#) **Crear una cuenta** [📄](#)

ID de usuario

Contraseña

Confirmar contraseña

Email

Derecho de acceso

Características

- Petición multimedia
- Notificación
- Automatización
- Cámaras
- Evento

Area

- Area 1
- Area 2

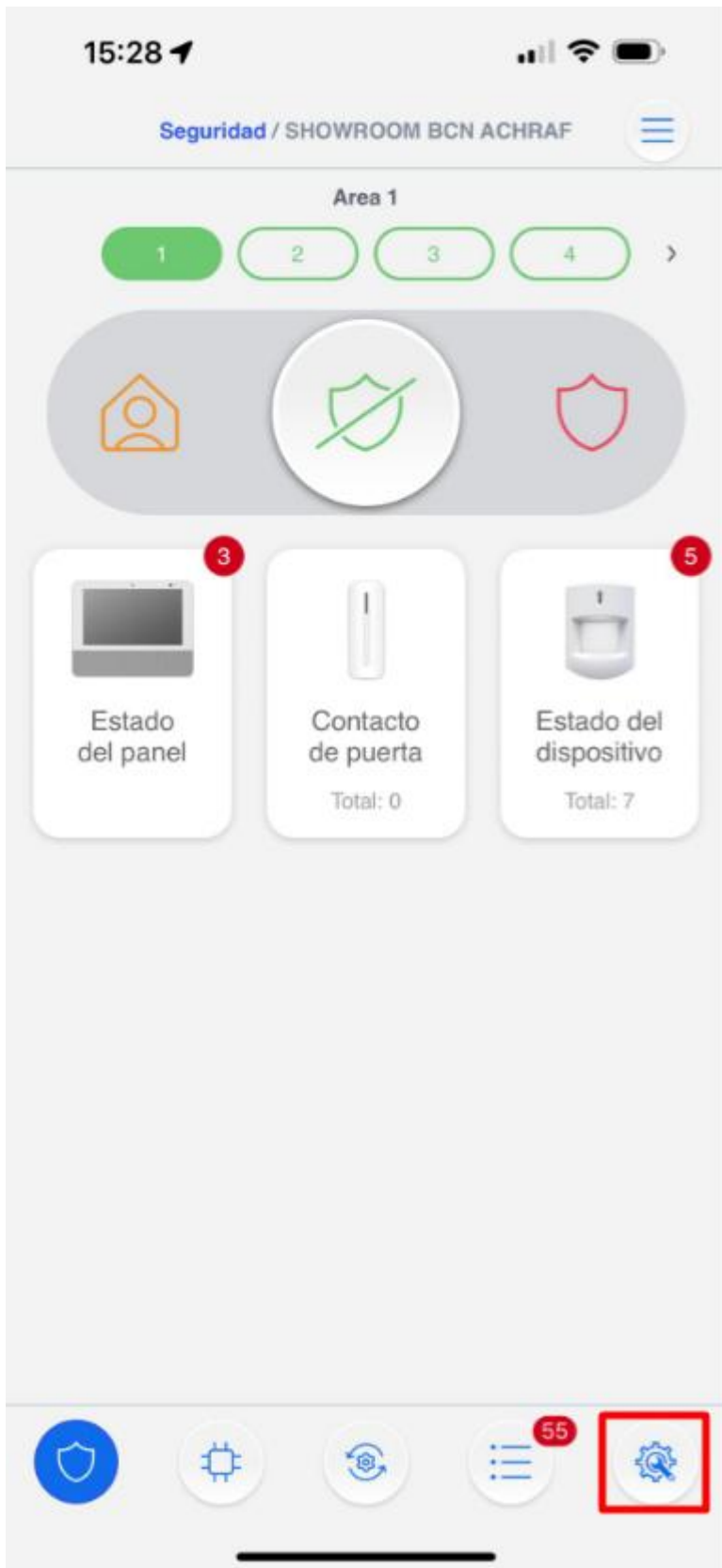
User registration completed! For information on how to operate with the user APP, follow the SmartHomeSec user guide.

3. Add and Configure Devices

To add and configure VESTA RF devices, follow these steps:

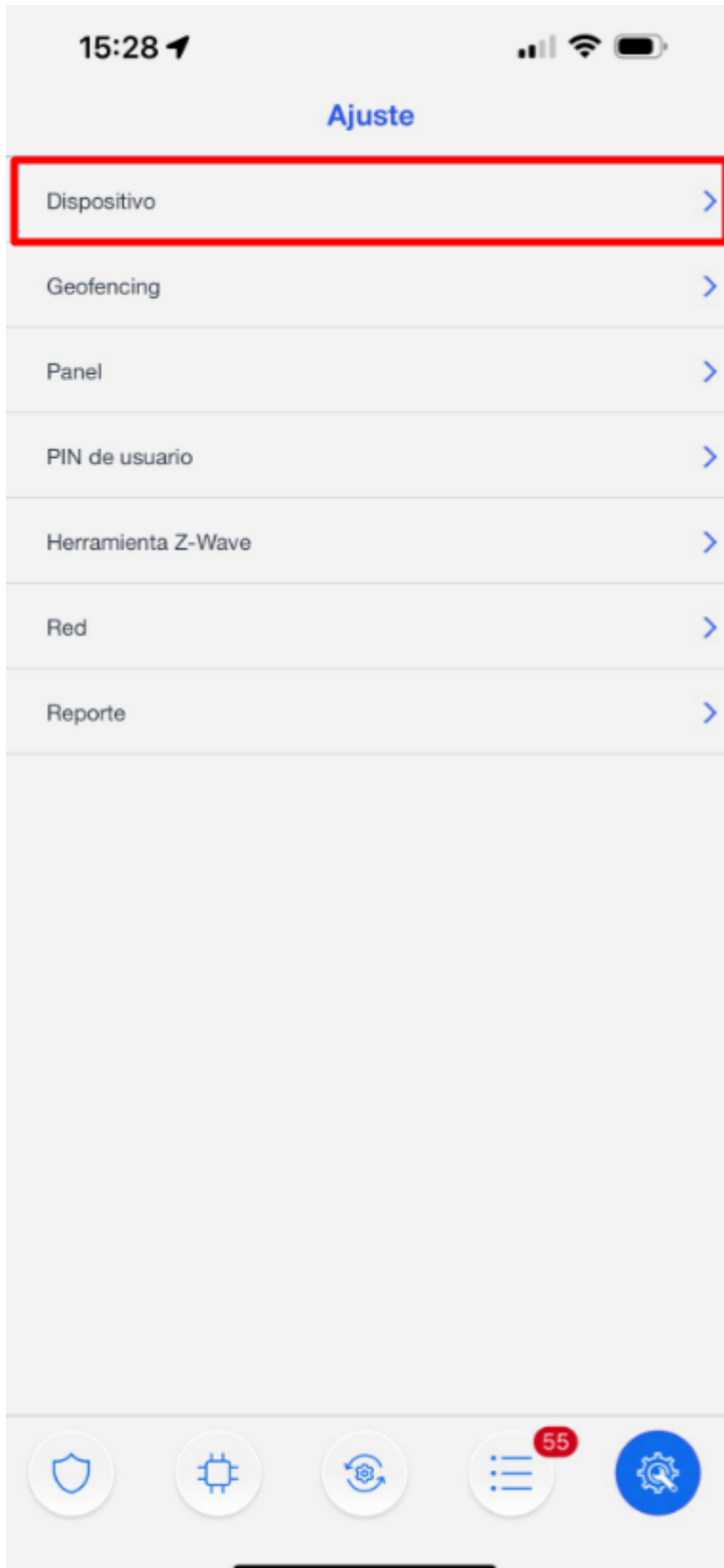
3.1 Add Devices

Step 1: Access the panel configuration from the installer APP:



Installer -> Settings

Step 2: Select "Devices" in the menu.



Installer -> Settings -> Devices

Step 3: In the menu click "Add device".

15:28



< Volver

Dispositivo



TSP-3

Area 1 (Zona 1)



TSP



OPTEX

Area 1 (Zona 2)



Vista exterior



TECLADO

Area 1 (Zona 3)



Teclado



NO USAR

Area 1 (Zona 5)

Inactive >

DIO62 (DI)



PUERTA ENTRADA

Area 1 (Zona 4)

OFF >

DIO52 (DO)



W26 ENTRADA

Area 1 (Zona 6)



Lector de etiquetas



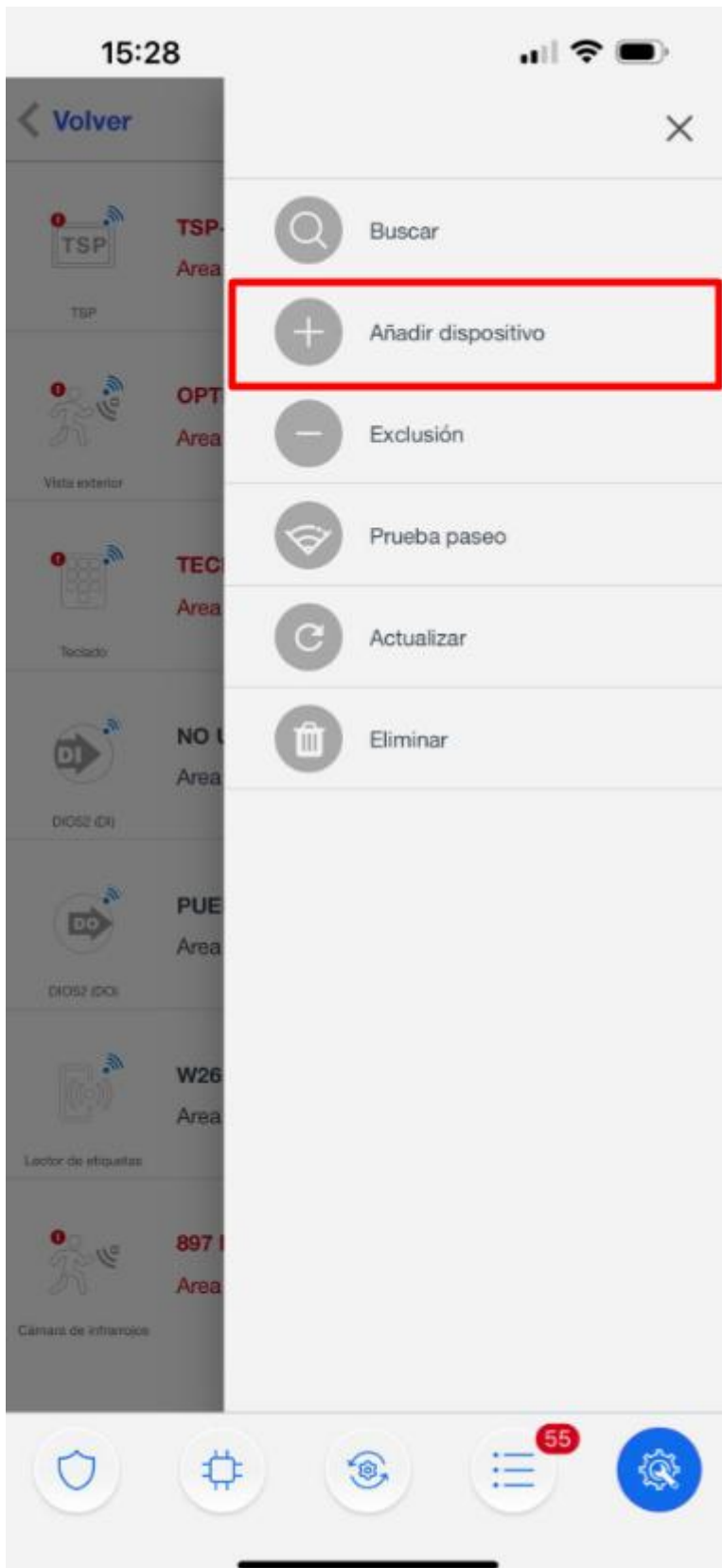
897 MASKING

Area 2 (Zona 1)



Cámara de infrarrojos





Step 4: Select the device type you want to add, e.g., Motion Detector. Press and hold the pairing button on the device until the LED flashes (refer to the device's manual for specific instructions).

Step 5: Follow the on-screen instructions to complete the pairing process. The panel will confirm the successful addition of the device.



Botón learn de los dispositivos VESTA

Important! In case of PIRCAMS and keyboards: The keystroke must be 3 or 4 seconds. While the rest of the devices with a short press is enough to add them.

Once added, the RF devices will be ready for use and can be managed from the same section, here is an example of sensor attribute configuration:

3.2 Zone configuration

15:38



[Volver](#)

Dispositivo



TSP-3

Area 1 (Zona 1)



TSP



OPTEX

Area 1 (Zona 2)



Vista exterior



TECLADO

Area 1 (Zona 3)



Teclado



NO USAR

Area 1 (Zona 5)

Inactive

DIO52 (DI)



PUERTA ENTRADA

Area 1 (Zona 4)

OFF

DIO52 (DO)



W26 ENTRADA

Area 1 (Zona 6)



Lector de etiquetas



897 MASKING

Area 2 (Zona 1)



Cámara de infrarrojos



15:38



[← Volver](#)

Dispositivo

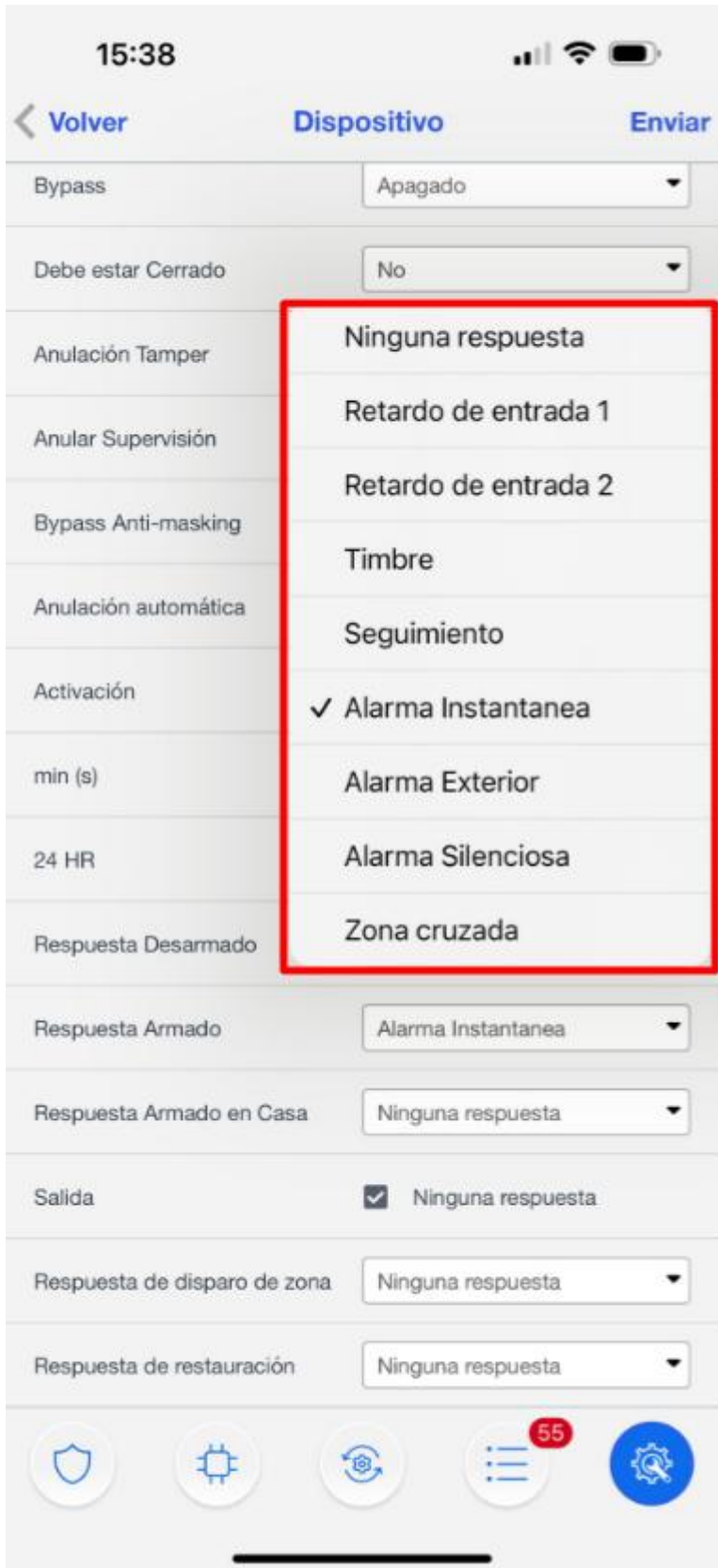
[Enviar](#)

Bypass	Apagado
Debe estar Cerrado	No
Anulación Tamper	Apagado
Anular Supervisión	Apagado
Bypass Anti-masking	Apagado
Anulación automática	Inhabilitar
Activación	1
min (s)	2
24 HR	<input type="checkbox"/> Alarma
Respuesta Desarmado	Ninguna respuesta
Respuesta Armado	Alarma Instantanea
Respuesta Armado en Casa	Ninguna respuesta
Salida	<input checked="" type="checkbox"/> Ninguna respuesta
Respuesta de disparo de zona	Ninguna respuesta
Respuesta de restauración	Ninguna respuesta



55





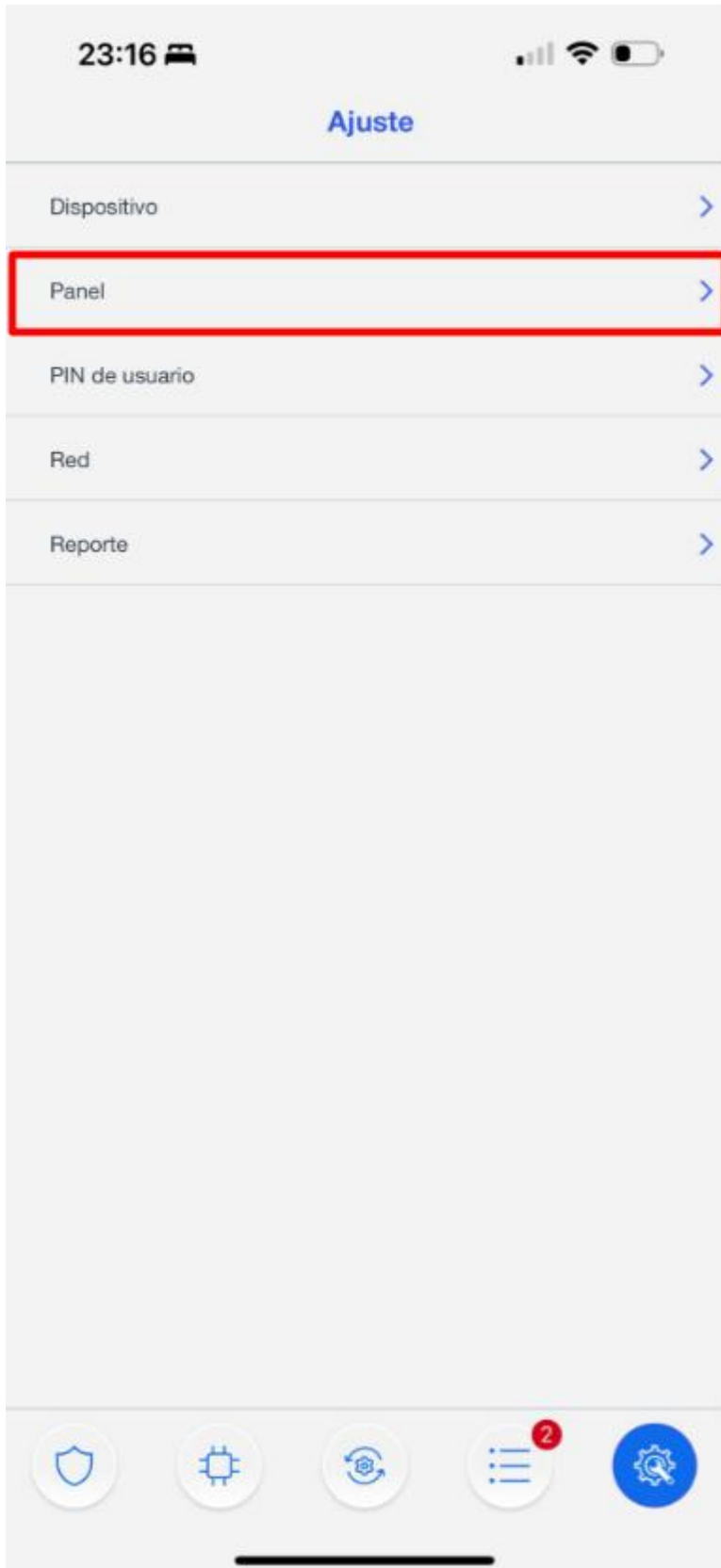
To configure the zones correctly, it is important to be familiar with the available attributes and their impact on the behavior of the alarm system.

For example: Interior is an instant zone and Entry is a delayed zone; we can assign these attributes in the section Response on arming which means "When the system is armed."

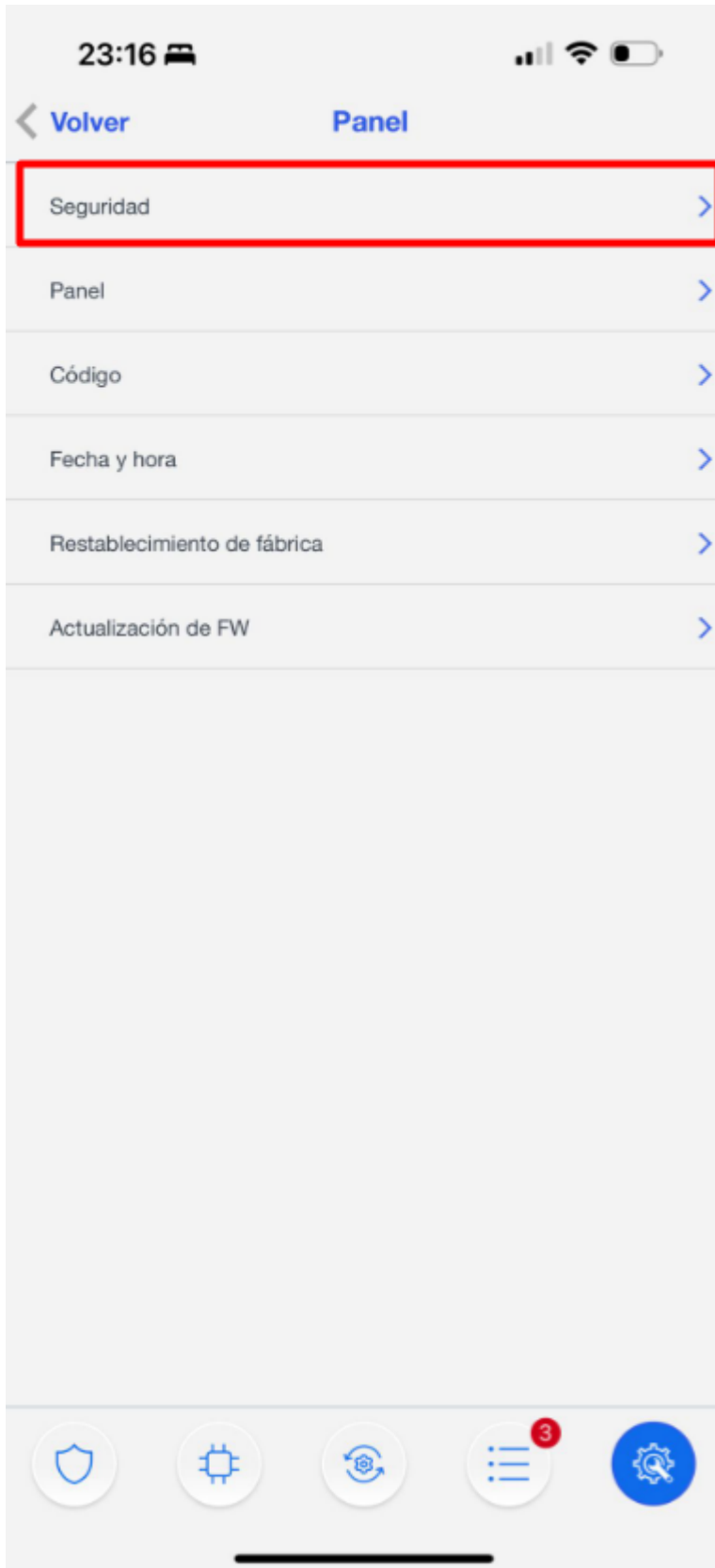
4. Panel configuration and reporting to ARC (Alarm Receiving Central Station)

4.1 Security configuration

This section details how to adjust the **siren duration** during an alarm and set the **input and output delays**. For ease of identification and adjustment, critical options are highlighted in ****color**red**.



Ajustes -> Panel



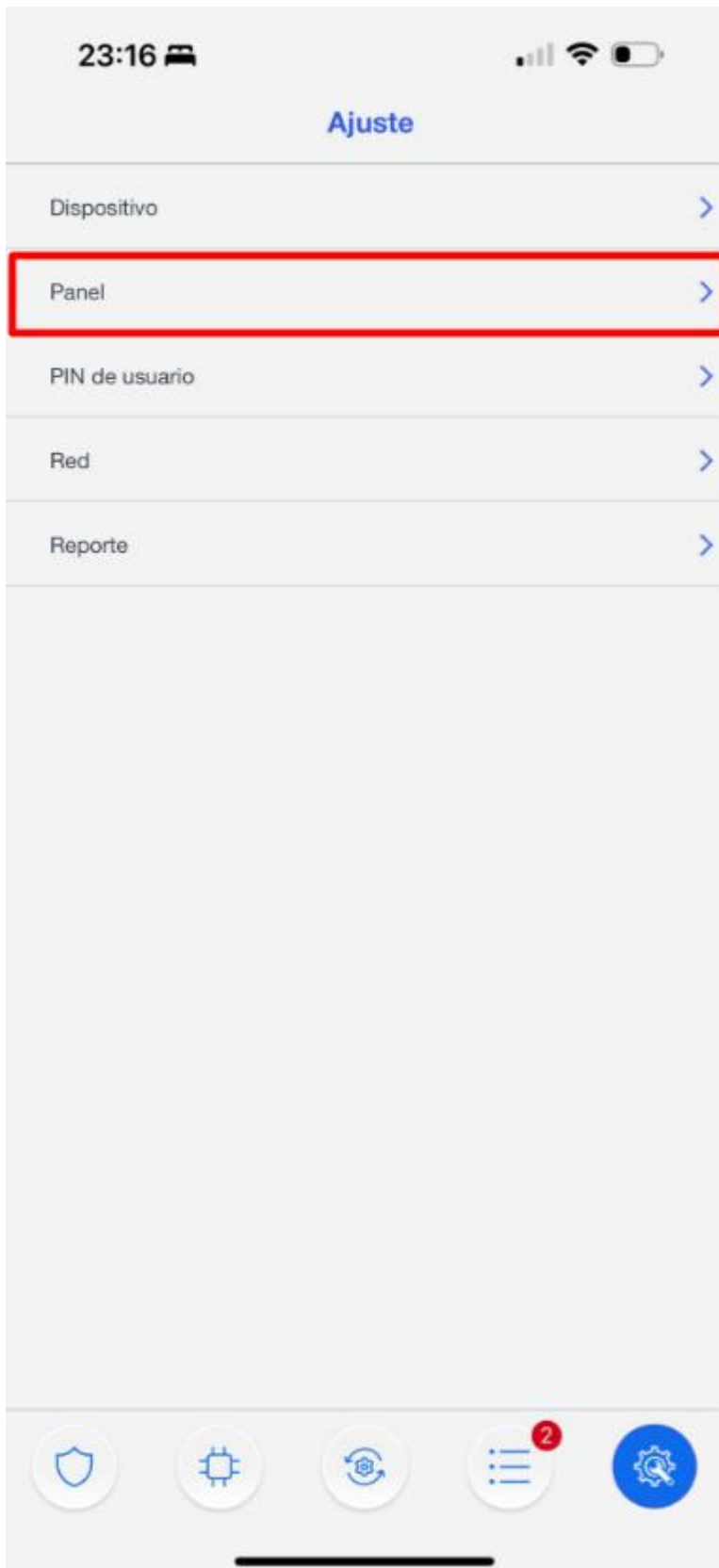
Ajustes -> Panel -> Seguridad



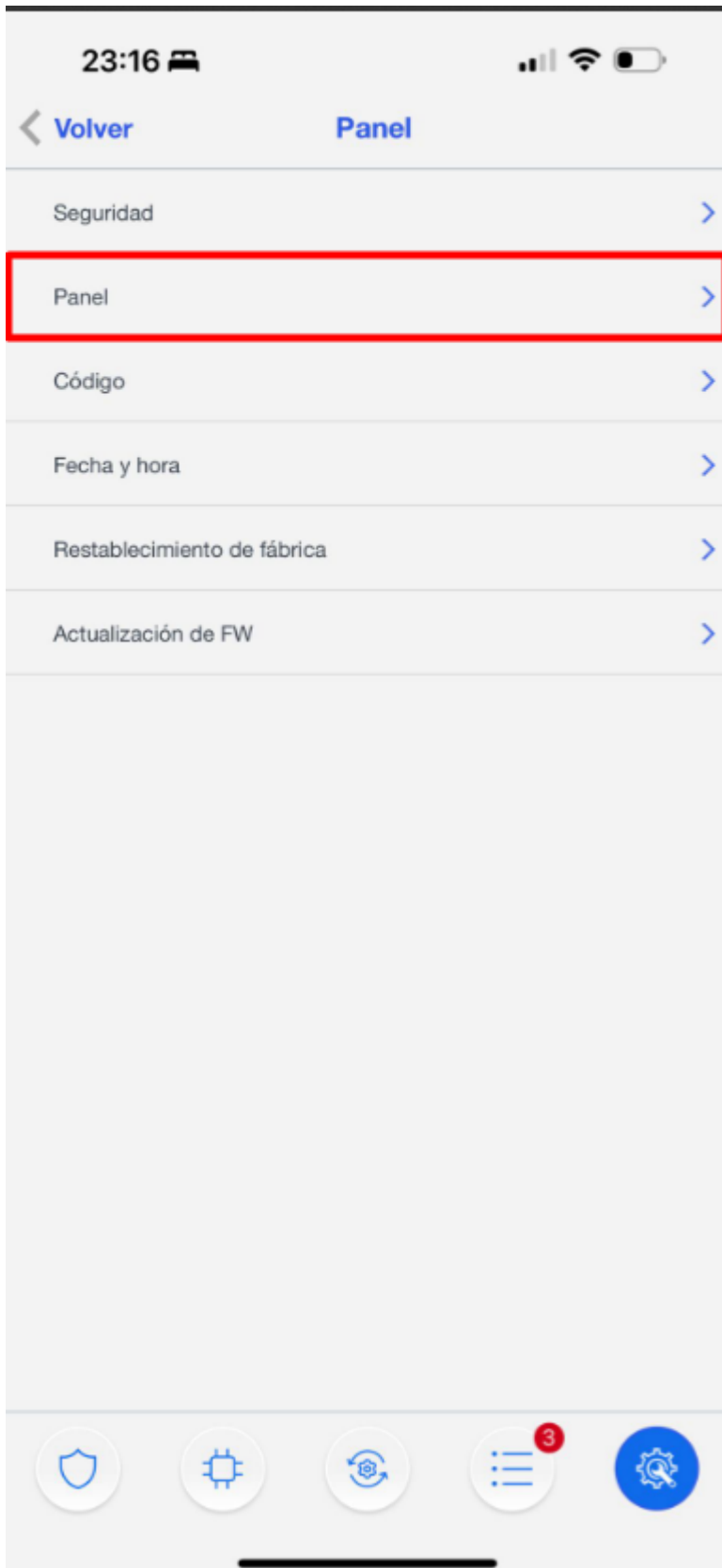
1. La **siren duration** en in case of alarm
2. Enabling this option delays the alarm reporting by 30 seconds. (**Recommended to leave OFF**)

3. Ajustar los entry and exit delays

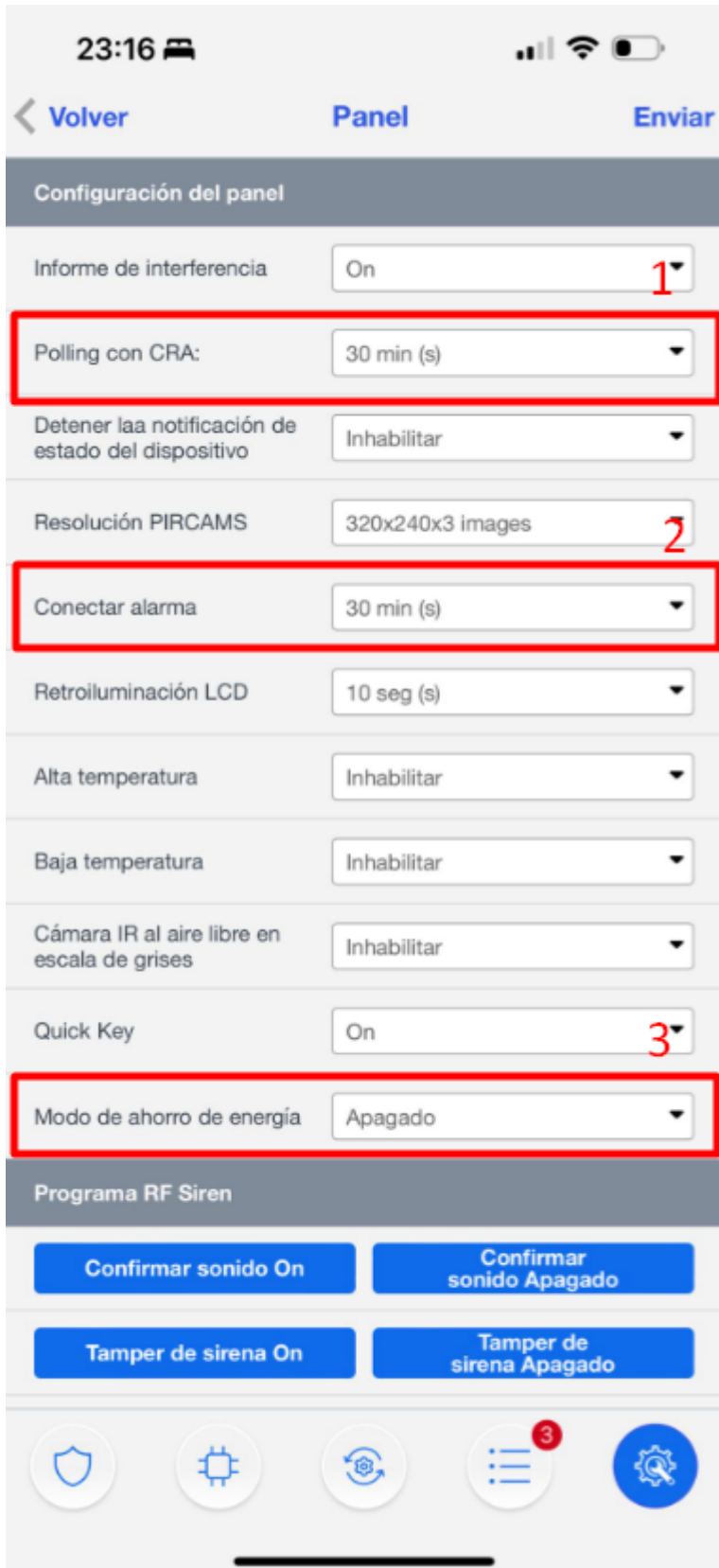
4.2 Panel configuration



Settings -> Panel



Settings-> Panel -> Panel

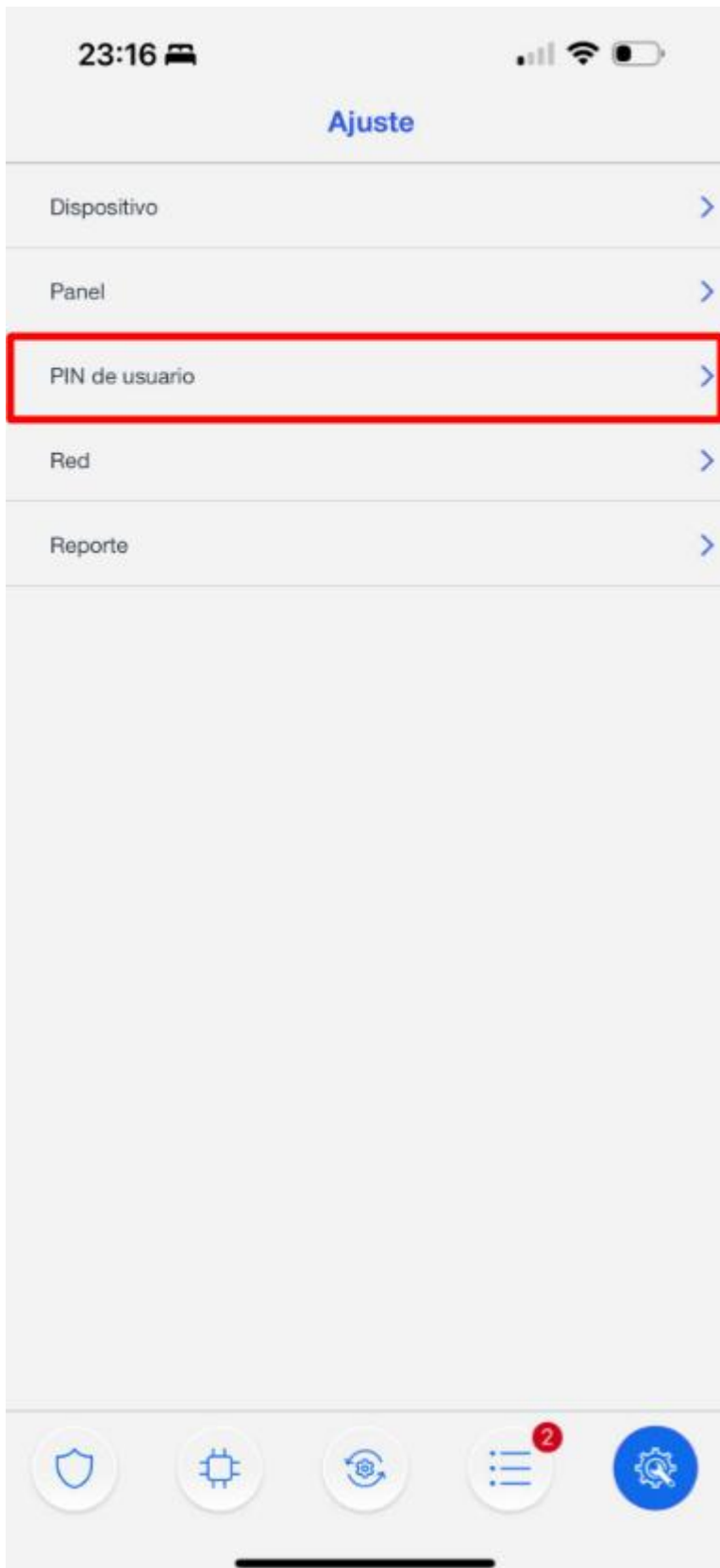


Polling --> test time to ARC





4.3 Configure user codes




Inslogging -> Settings








Settings -> User PIN

23:17    

[← Volver](#) **PIN de usuario** [Enviar](#)

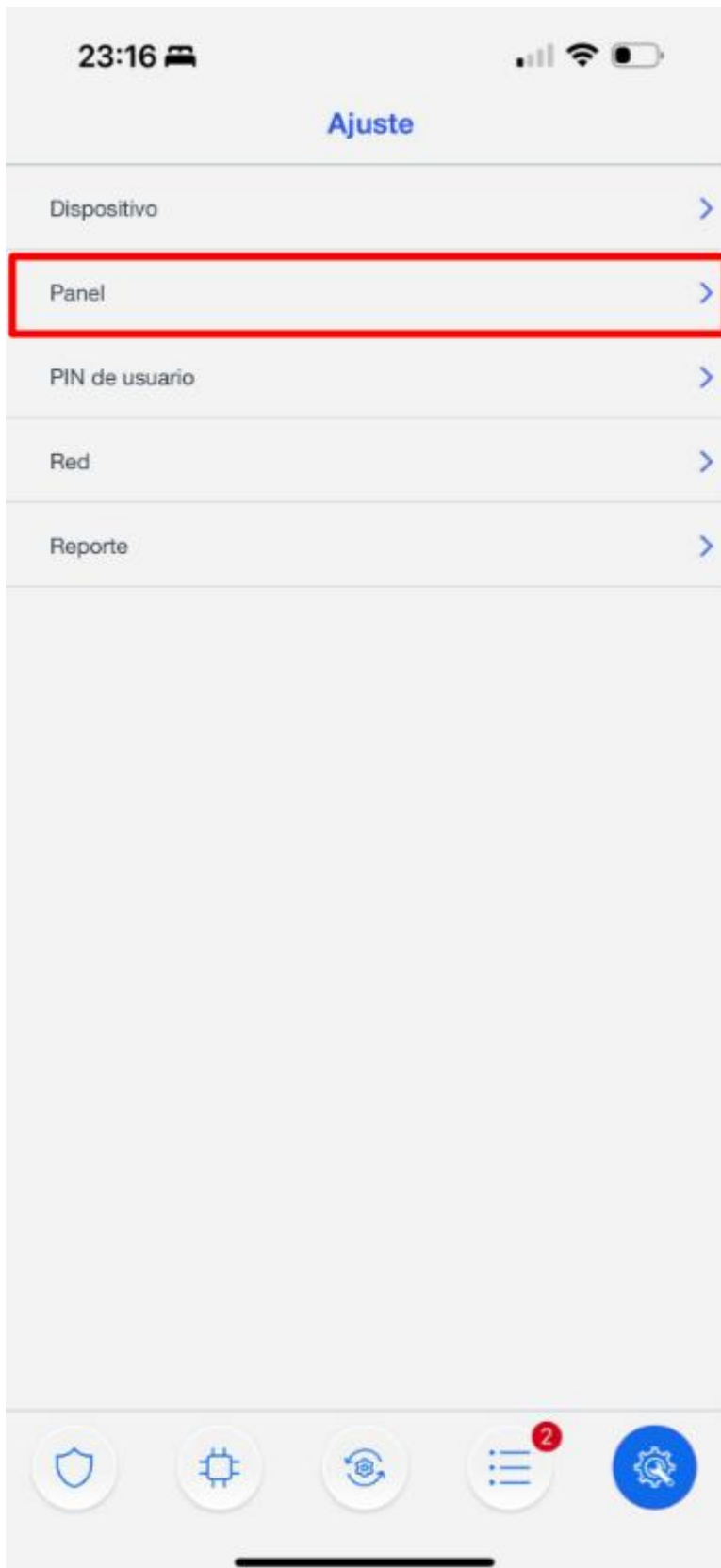
	Nombre de usuario	Código PIN	
1	user	••••••	
2			
3			
4			
5			
6			
7			
8			
9			
10			

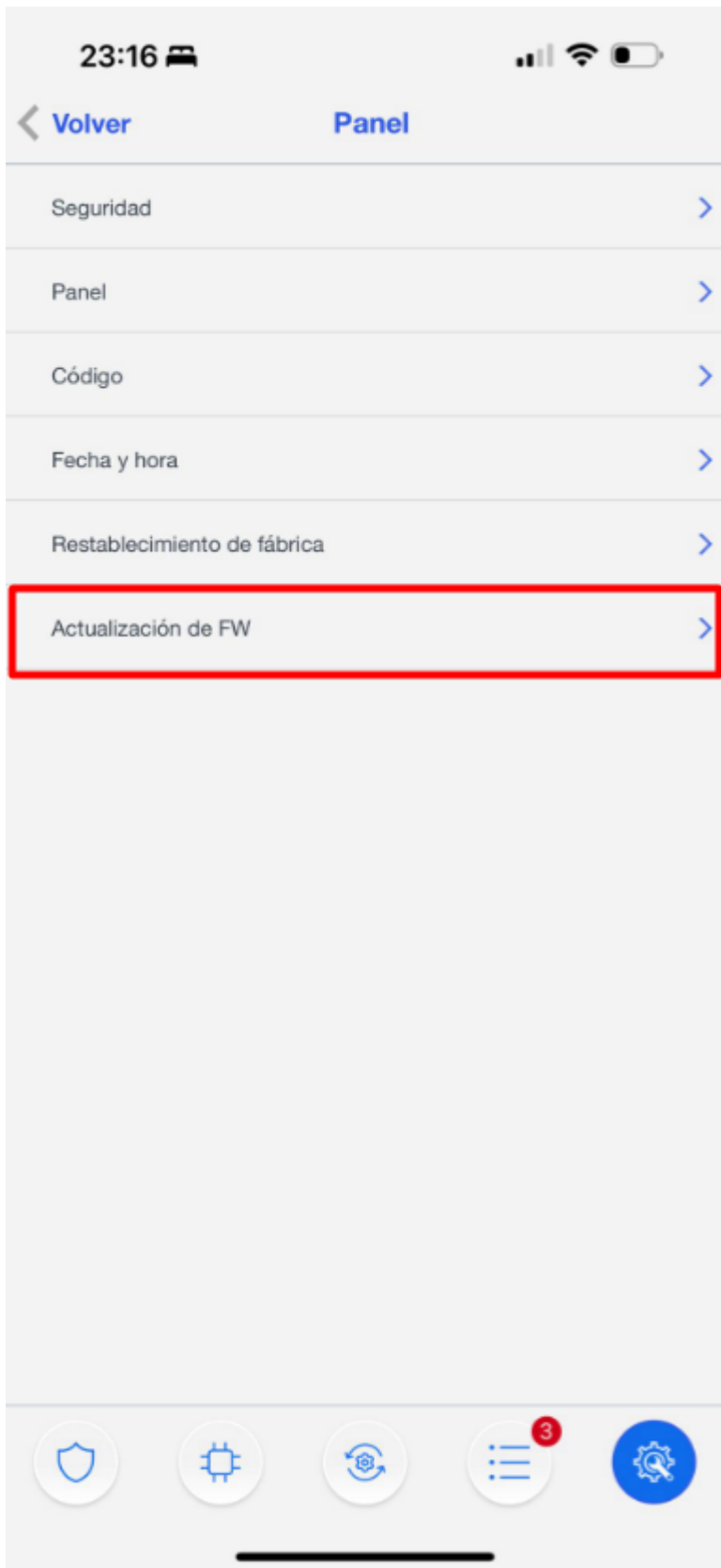
Add the Name and code for each user, this code will allow the user to switch modes from the APP or keyboards see User Manual for more information.

4.4 Updating the panel

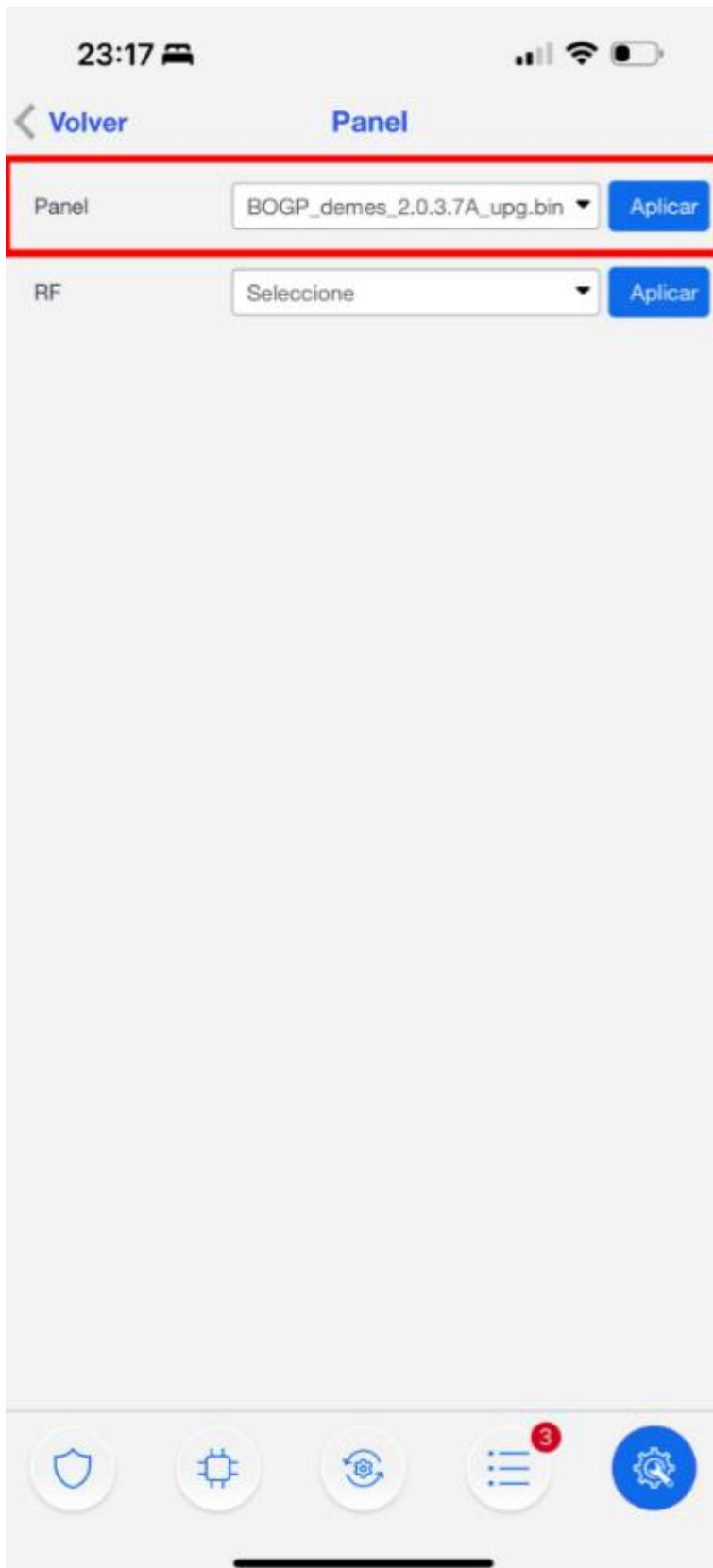
It is crucial to keep the control panel up to date to ensure optimal system performance and security. Updates may contain essential enhancements, bug fixes and security patches that protect against known vulnerabilities.



Ajustes -> Panel



Panel -> Actualización de FW



Select from the list the firmware with the highest version (Highest number and highest letter).

NOTE: The panel by 2G or low coverage may take 8 minutes to update.

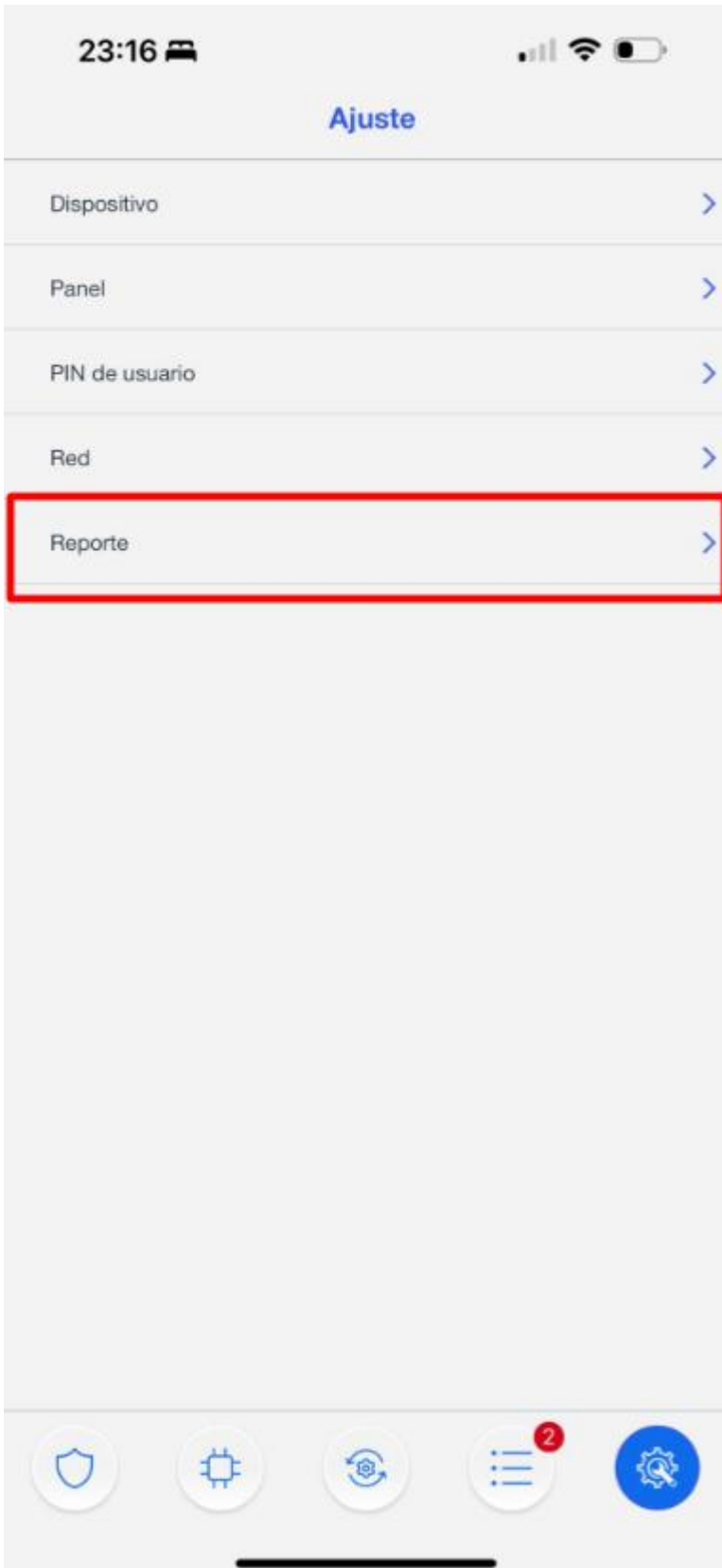
If the panel communicates over 4G/LTE with good coverage the update may take 3-5 minutes

Once the panel is in upgrade mode **Do NOT turn off** or disconnect under any circumstances. The panel will restart automatically.

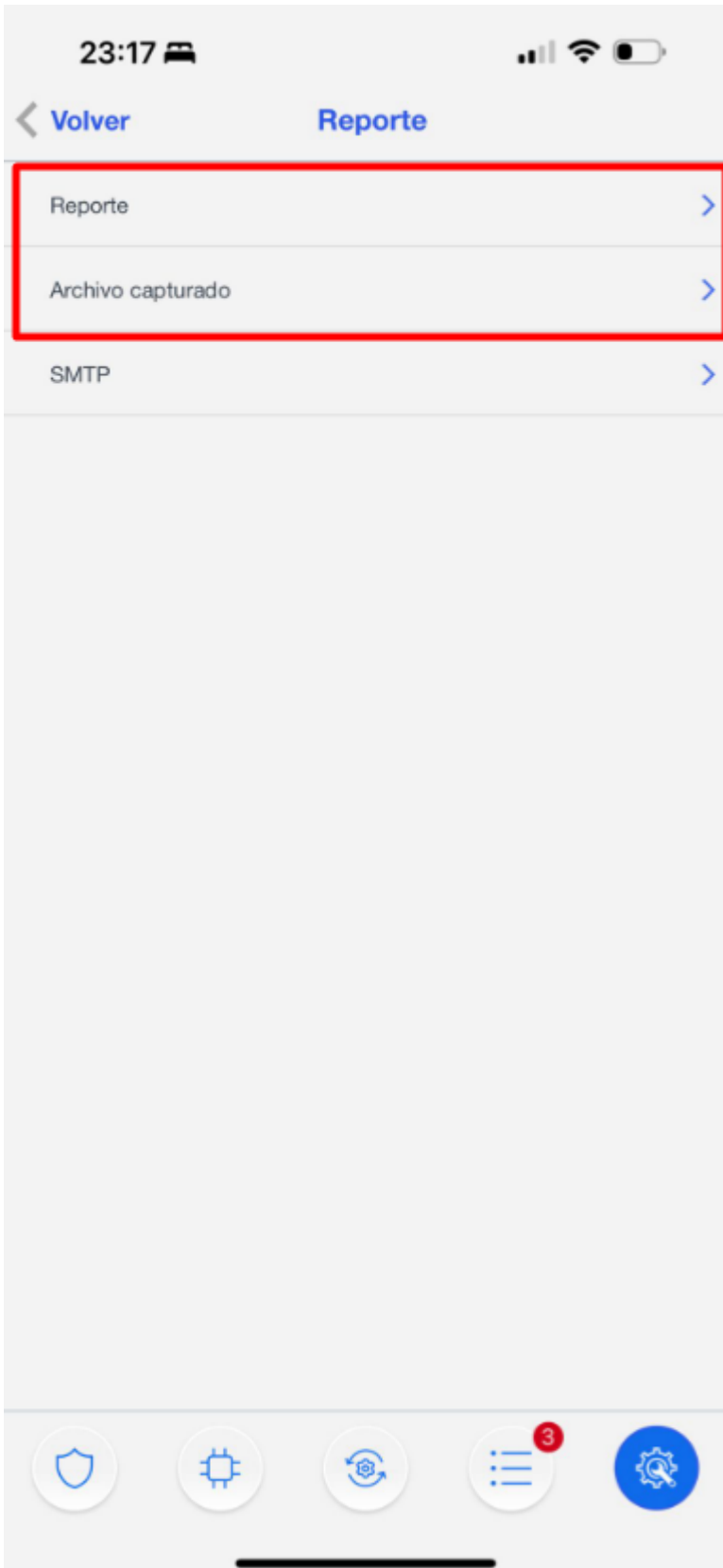
SWITCHING OFF THE PANEL DURING AN UPGRADE MAY RENDER IT COMPLETELY INOPERATIVE.

4.5 Reporting configuration to ARC (Alarm Receiving Center)

Reporte Eventos



Settings -> Report



In the report section we have report configuration for events and captured files for PIRCAMS photos.

< Volver
Reporte
Enviar

Reporte
+ 🗑️

URL 1:
Grupo 1 ▼
Todos los eventos ▼

URL 2:
Grupo 2 ▼
Todos los eventos ▼
⋮

URL 3:
Grupo 2 ▼
Todos los eventos ▼
⋮

Note:

1. Report via IP (Ethernet or GPRS) in CID format, ex: ip://ACCT@server:port/CID
2. Report via IP (Ethernet or GPRS) in SIA format, ex: ip://ACCT@server:port/SIA
3. Report via E-mail, ex: mailto: user@example.com

Configuración de reporte

Polling SIA:

🛡️
🔧
🔄
☰ ³
⚙️

In this section we configure the repote URL of our ARC, and very important the GROUP 2 or higher since group 1 is used for the APP. APPENDIX 2 for examples

APPENDIX 2

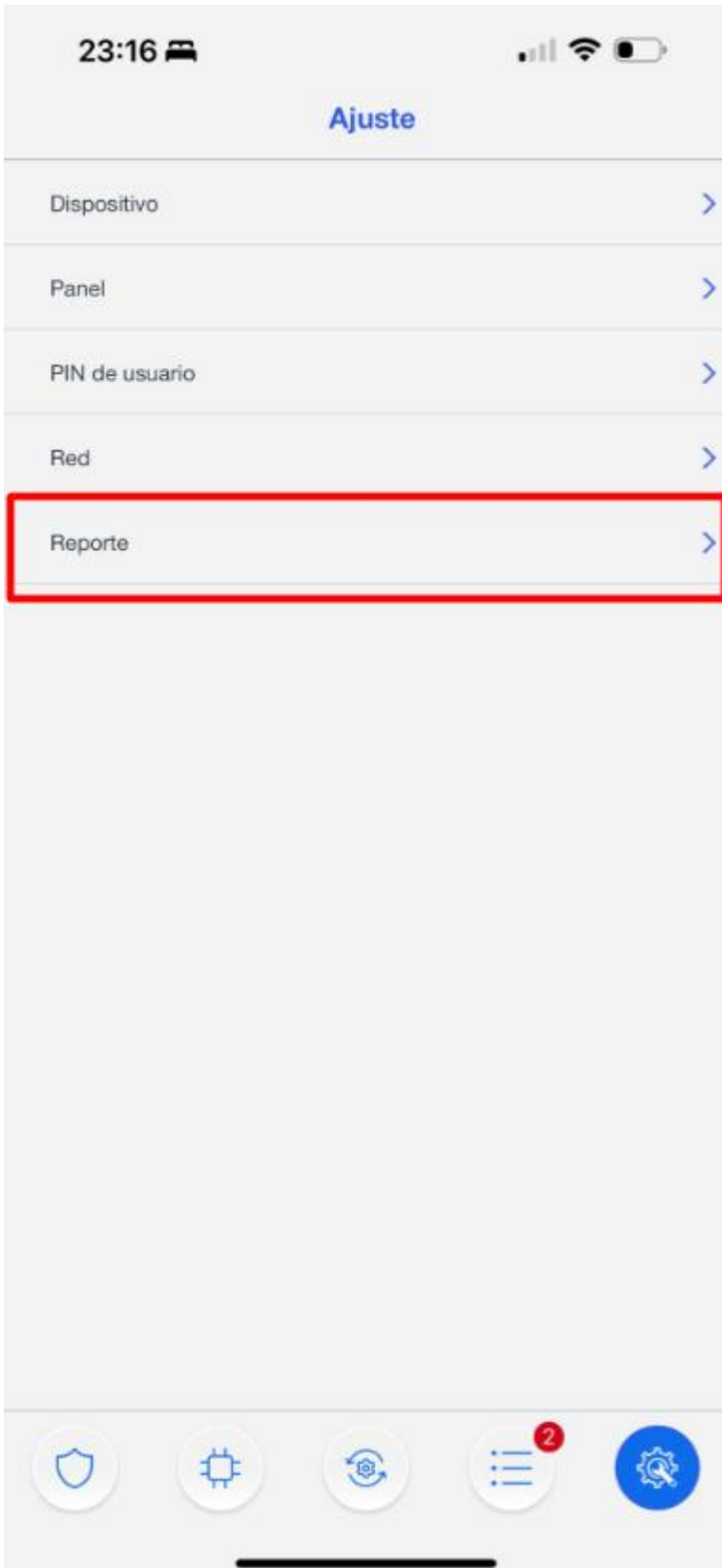
Examples of **EVENTS** reporting in different protocols:

🔥 **MANITOU (most used in Spain): ip://ACCT@IP:PORT/MAN**

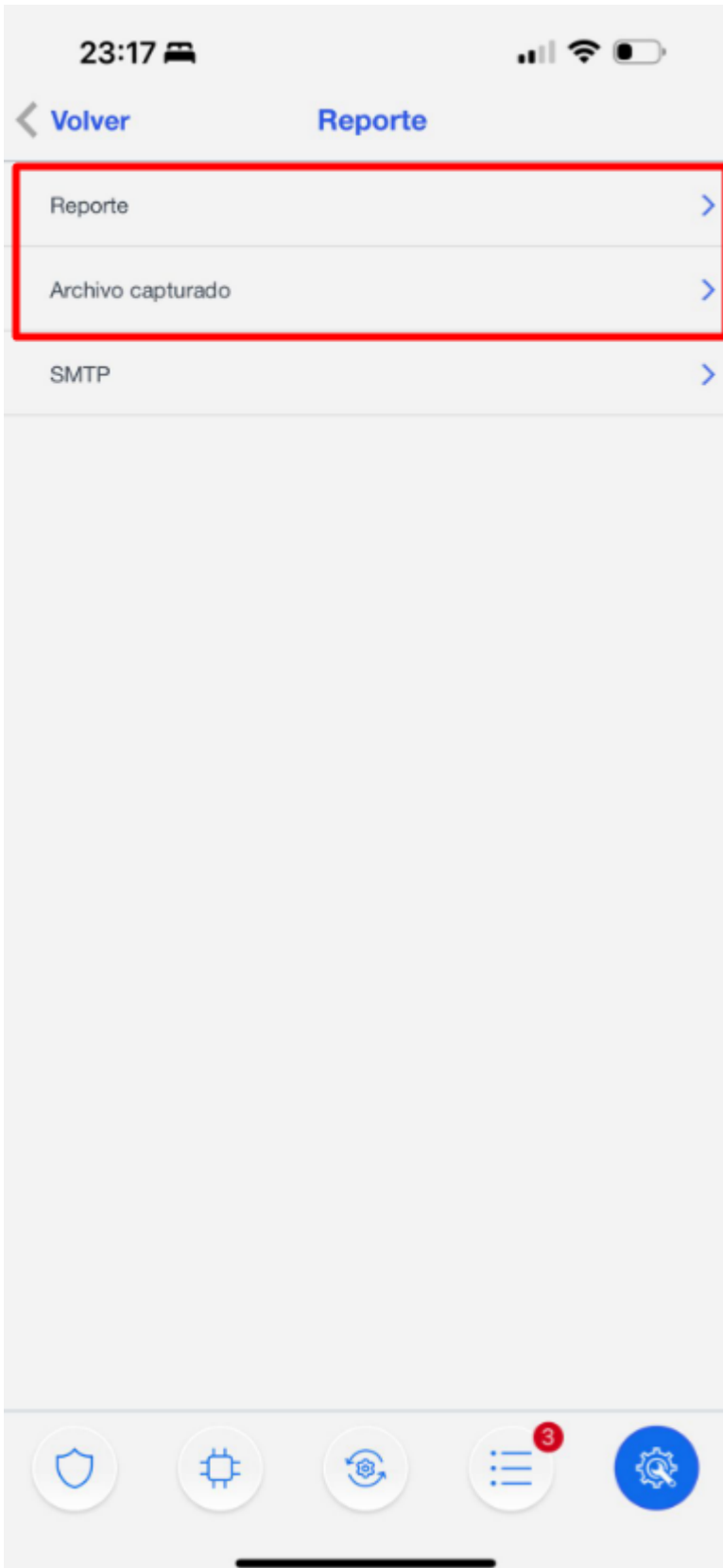
SIA: **ip://ACCT@IP:PORT/SIA2**

CID: **ip://ACCT@IP:PORT/CID**

Photo report.



Settings -> Report



In the report section we have report configuration for events and captured files for PIRCAMS photos.



In this section we configure the repote URL of our CRA for sending photos. APPENDIX 3 for examples

Examples of **PHOTOS** reporting in different protocols:

🔥 **MANITOU: ACCT@IP:PORT**

Photo report for SENTINEL software

Step 1: Program SMTP information in settings -> Report

Ajuste - Reporte

Reporte SMS Archivo capturado SMTP Voz

SMTP

Servidor:

Puerto: Utilizar canales encriptados TLS/SSL (SMTP seguro))

Nombre de usuario: Contraseña:

Desde:

Example

Step 2: Program the email provided by central monitoring station in "Captured files"

Ajuste - Reporte

Reporte SMS Archivo capturado SMTP Voz

Archivo capturado +

URL 1:

IP de BACKUP:

URL 2:

IP de BACKUP:

Note:

1. Upload via IP (Ethernet or GPRS) in FTP protocol, e.g.: ftp://user:password@server/path
2. Upload via IP (Ethernet or GPRS) in HTTP protocol, e.g.: http://server/path
3. Mail via IP (Ethernet or GPRS), e.g.: mailto: user@server
4. Manitou via IP (Ethernet or GPRS), e.g.: manitou://user@server:port

Email Setting

Sólo alarma SMTP: