WebApp
CITYMESH

Powered by
DEITRES

Manual Cloud Deitres Citymesh

Innovation in Security

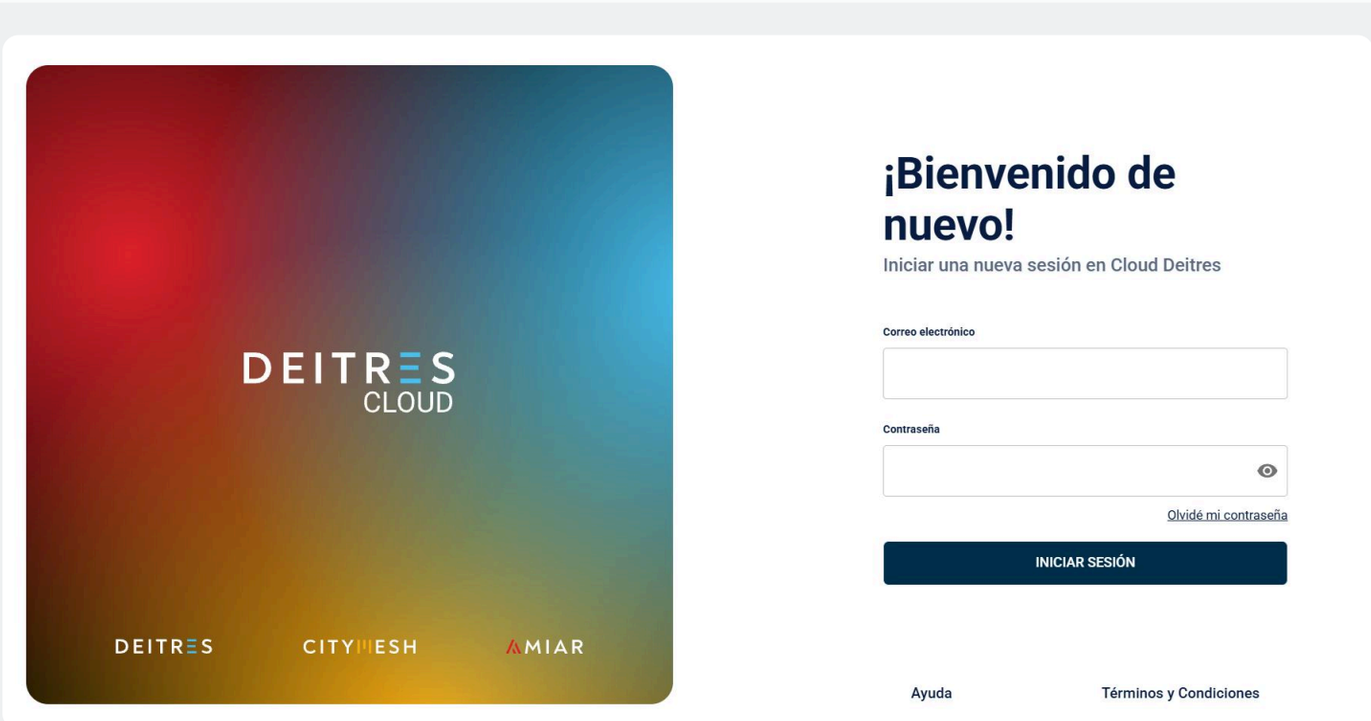
2026

Cloud Deitres Platform Manual – Citymesh

In this user manual, you will find the recommendations and guidance needed to use the Cloud.Deitres Citymesh.

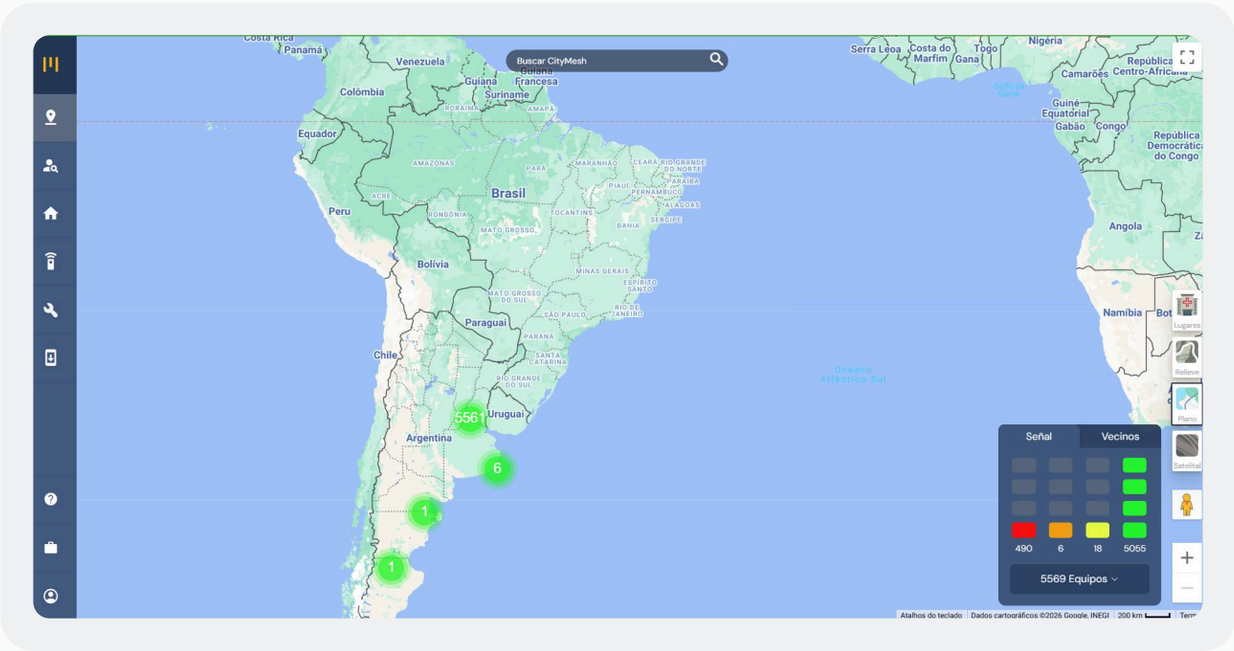
Below, you will see features such as: map, neighbors, user addition, mesh network management, viewing your company information, and much more.

For comments, failures, or questions, please contact our support email: sales@deitres.com where a member of our team will assist you.



Login

To manage users (technicians and end customers), partitions, and CityMesh panels, access cloud.deitres.com using the email address and password provided by Deitres.

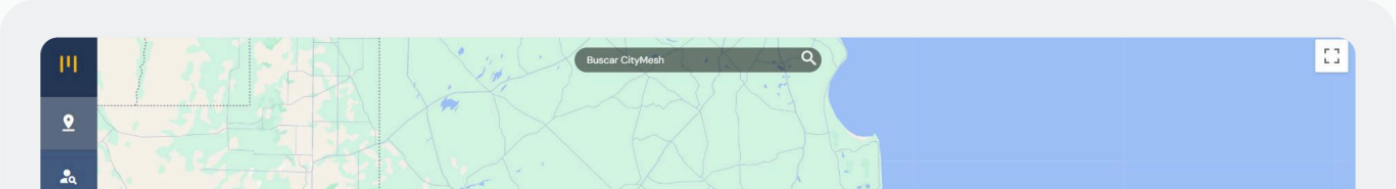


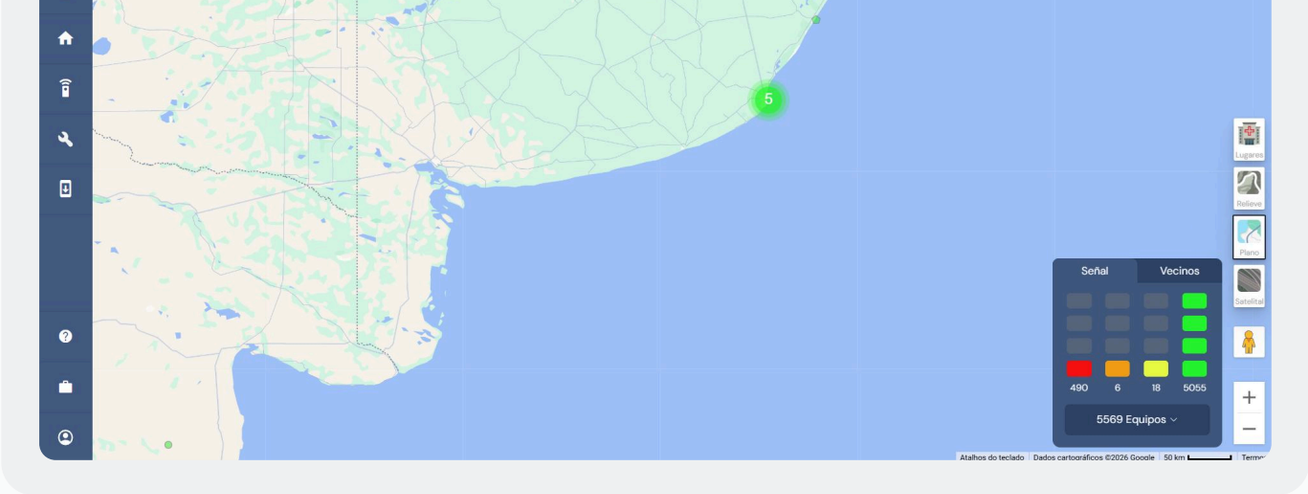
Devise Map

Device aggregation: In this feature, devices are grouped according to a distance range of 3 to 4 km, and the colors are determined by the devices (information from tests performed in the last hour). For example, when there are more green devices, the group will be green. Remember that each color has a weight, with red having the highest weight in the calculation used to choose the group color, because it indicates that the device is disconnected.

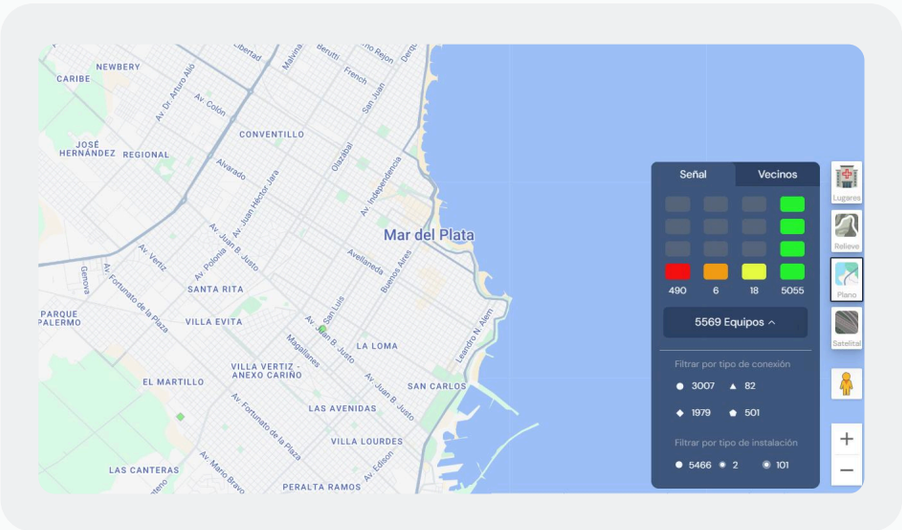
Red **Orange** **Yellow** **Green**

When you zoom in or out on the map, the grouping **is recalculated and updated automatically.**





Connection types:



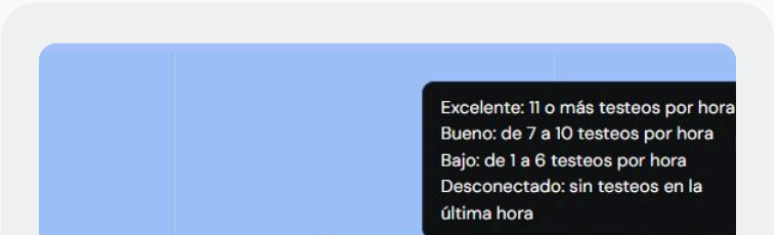
- **Small circle:** devices connected via Mesh.
- **Triangle:** devices connected via Wi-Fi/Ethernet.
- **Diamond:** devices connected via 2G/3G/4G.
- **Pentagon:** devices connected via 2G/3G/4G + Wi-Fi/Ethernet.

Installation types

- **Small circle:** devices located inside a site.
- **Small circle + outline:** devices located outside a site and less than 10 m high.
- **Small circle + 2 outlines:** devices located outside a site and more than 10 m high.

These icons correspond to the type of the device's most recent communication. In other words, if its last communication was through cellular (2G/3G/4G), its icon will be a diamond. However, if the device reports a new latest message through Wi-Fi/Ethernet, the icon will be updated to a triangle.

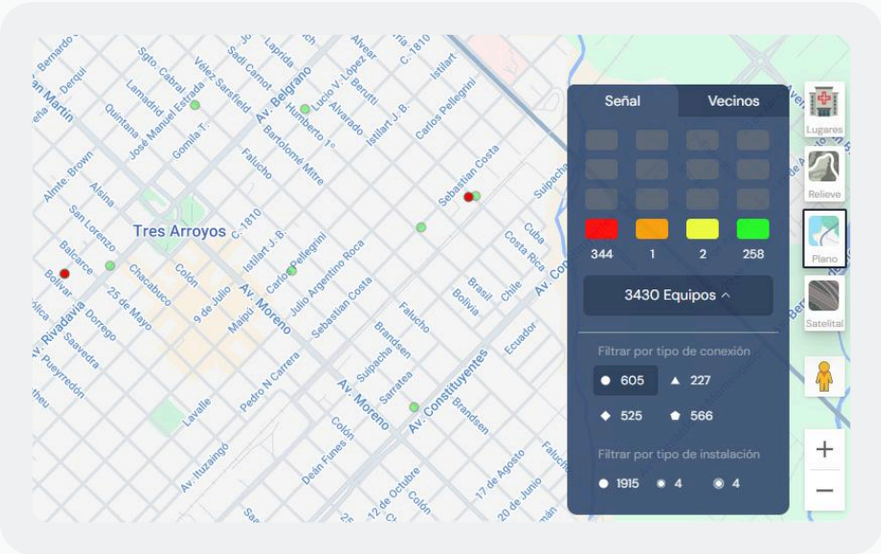
- **Test updates:** The **test legend** displays the **tests performed during the last hour** and is updated every 5 minutes with the status of the equipment visible on screen. As a result, devices are also **automatically updated on the map.**



- **Connection "Type filter":** By clicking on the total number of devices, the legend expands so that you can view the types of links available on the map.

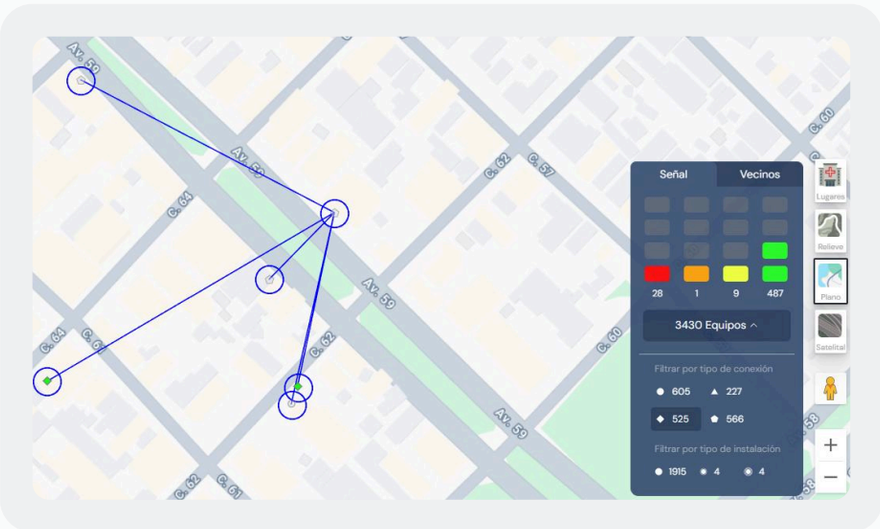
  Each connection-type button is a filter. For example, when you click "Mesh", the map will display only devices using that type of link.

Look at an example:



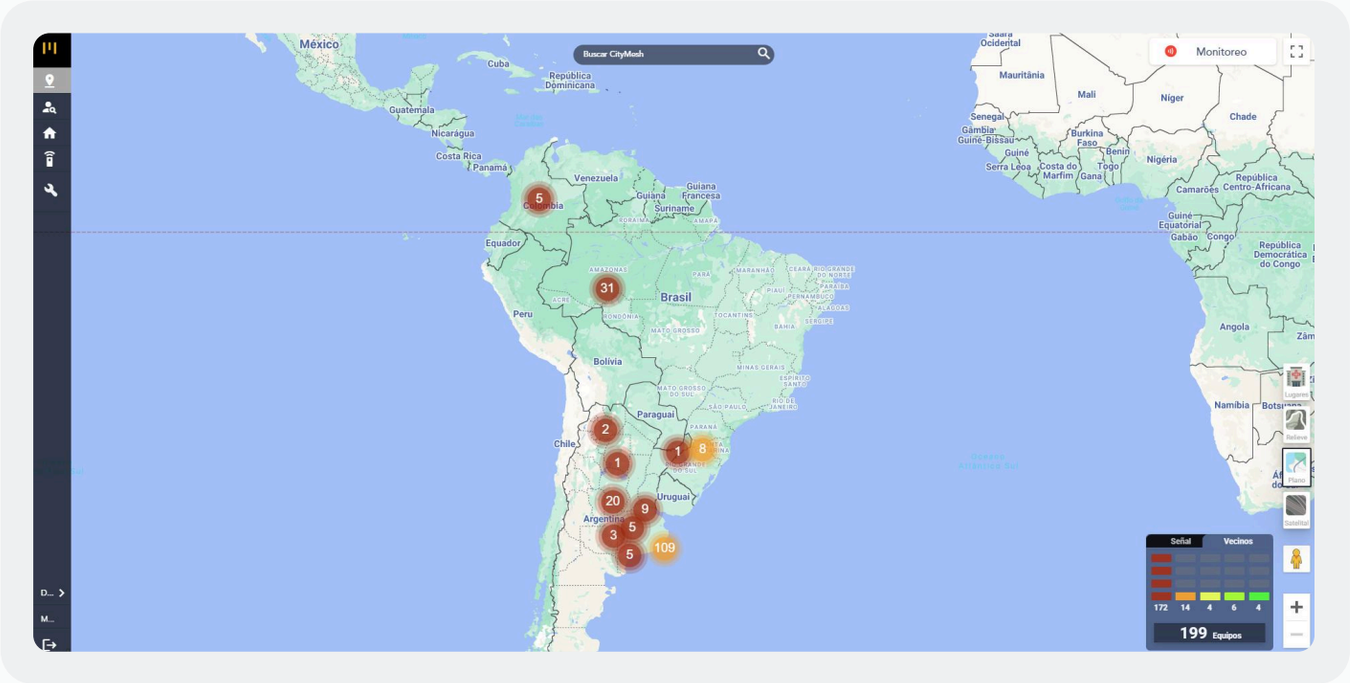
Filters can be combined all at once or incrementally.

You can also apply filters within the neighbors feature. Linked devices of the same type retain their original color, while those with a different connection type are displayed in gray so you can identify them.



- **Neighbors:** When you access the neighbors tab, you can view devices grouped by color on the map. These colors represent the number of links those neighbors have.

Green **Light green** **Yellow** **Orange** **Brown**



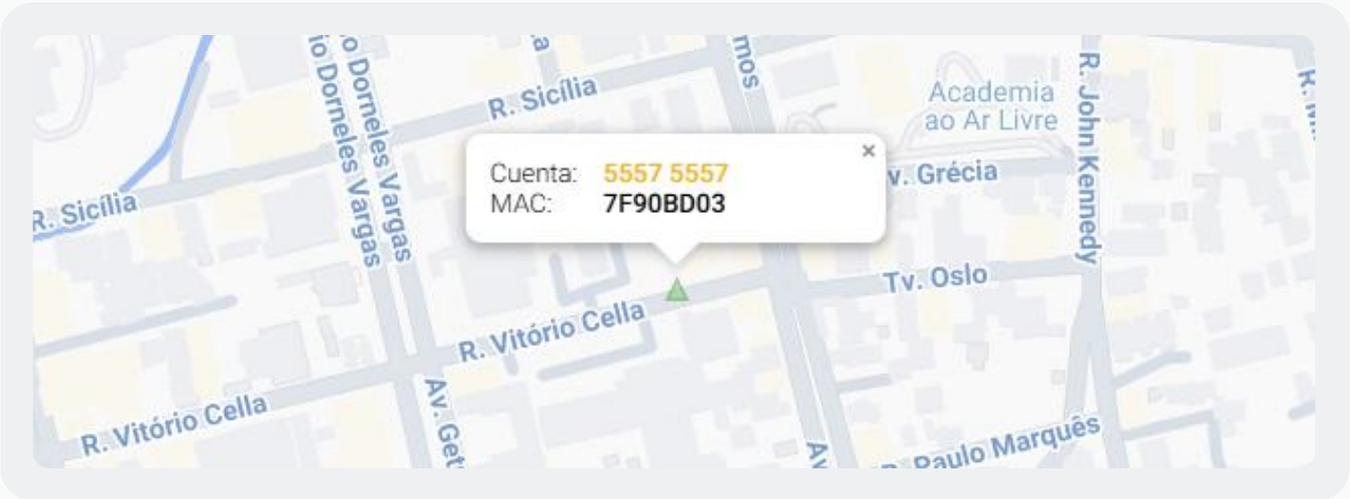
- **Green:** when the device has 3 or more neighbors.
- **Light green:** when the device has 2 neighbors.
- **Yellow:** when the device has only 1 neighbor.
- **Orange:** when the device has no neighbors.
- **Brown:** when the device is disconnected.

The aggregation color on the map is determined by the largest proportion of a device color. For example, if there are more green devices within that radius, the group will be green.

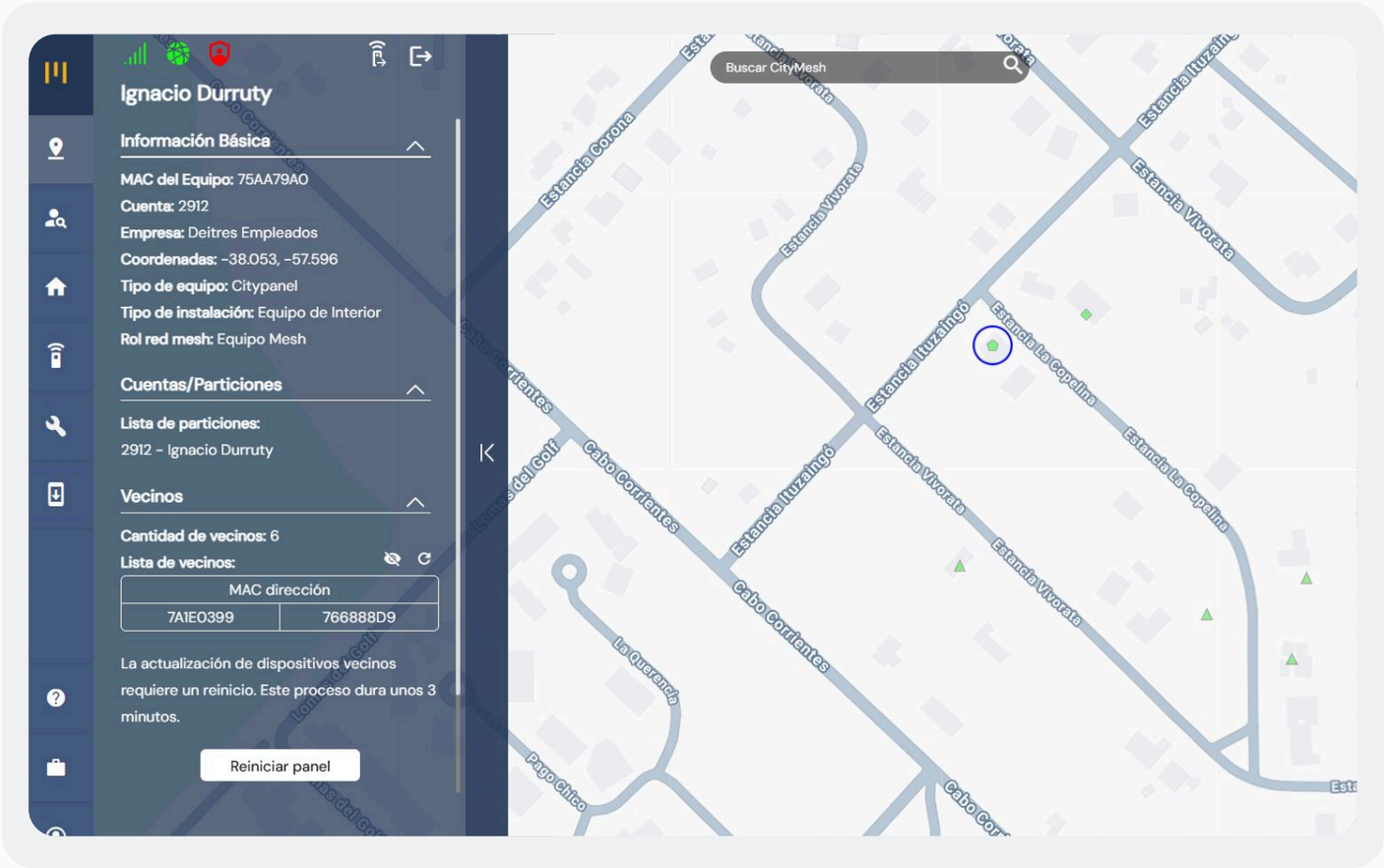
- **Neighbors links:** Here, by **clicking the "eye" icon** in the neighbors section, you can view the devices that are **connected to each other.** You can also **update these links** by restarting the device.

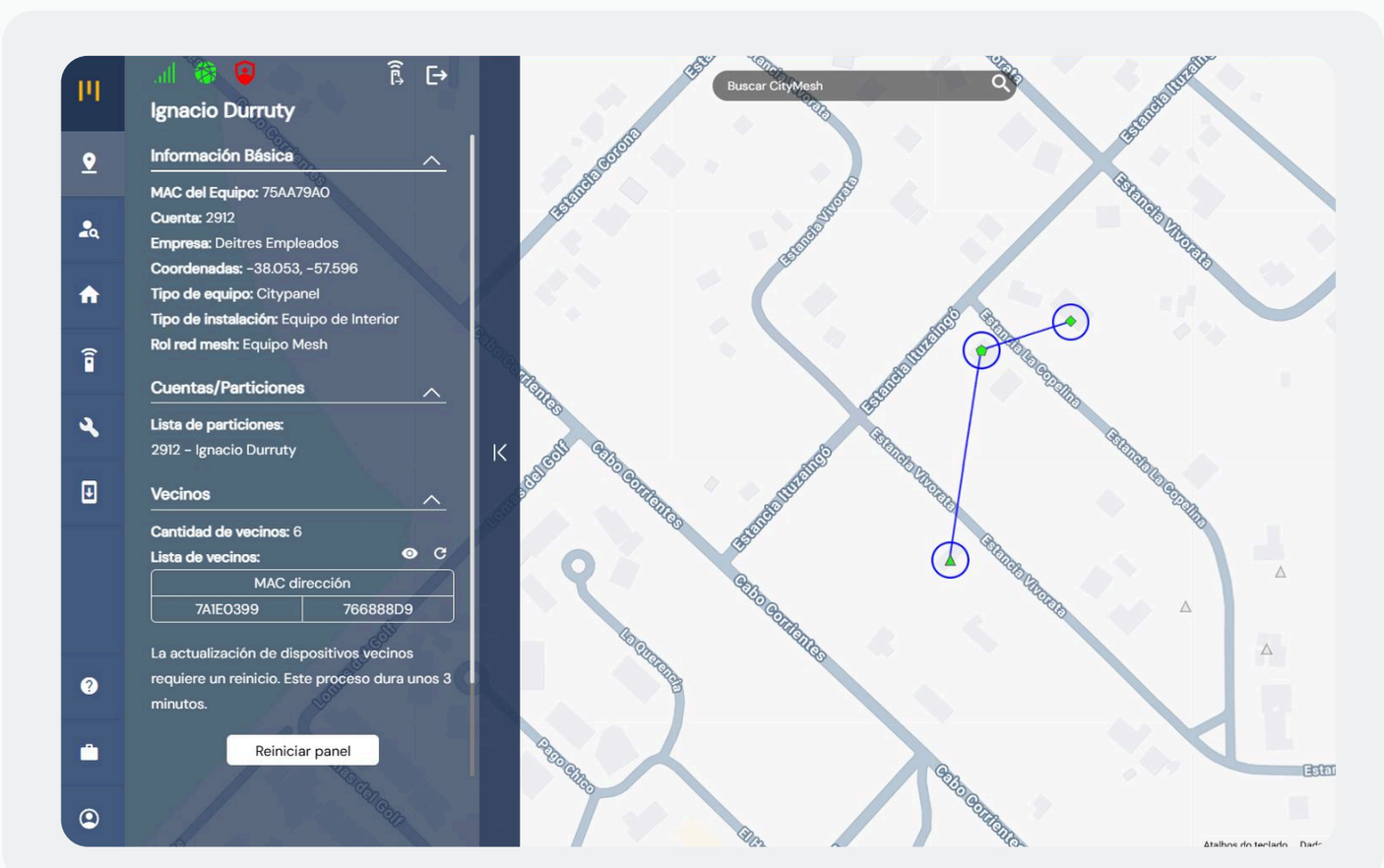
How to view connected neighbors:

1 - **Select a device,** by clicking on it.



2 - In the **sidebar**, select the **"eye"** icon in the neighbors section. **Click once** and wait for it to load. **Click again** to view the linked devices.


Ignacio Durruty
Información Básica
MAC del Equipo: 75AA79A0
Cuenta: 2912
Empresa: Deitres Empleados
Coordenadas: -38.053, -57.596
Tipo de equipo: Citypanel
Tipo de instalación: Equipo de Interior
Rol red mesh: Equipo Mesh
Cuentas/Particiones
Lista de particiones:
2912 - Ignacio Durruty
Vecinos
Cantidad de vecinos: 6
Lista de vecinos:
MAC dirección
7A1E0399
766888D9
La actualización de dispositivos vecinos requiere un reinicio. Este proceso dura unos 3 minutos.
Reiniciar panel
Buscar CityMesh
Estancia Corona
Estancia Vivorata
Estancia Ituzaingó
Estancia La Copelina
Cabo Corrientes
La Quarenó
Pago Chico

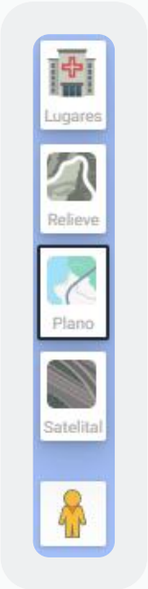

Ignacio Durruty
Información Básica
MAC del Equipo: 75AA79A0
Cuenta: 2912
Empresa: Deitres Empleados
Coordenadas: -38.053, -57.596
Tipo de equipo: Citypanel
Tipo de instalación: Equipo de Interior
Rol red mesh: Equipo Mesh
Cuentas/Particiones
Lista de particiones:
2912 - Ignacio Durruty
Vecinos
Cantidad de vecinos: 6
Lista de vecinos:
MAC dirección
7A1E0399
766888D9
La actualización de dispositivos vecinos requiere un reinicio. Este proceso dura unos 3 minutos.
Reiniciar panel
Buscar CityMesh
Estancia Corona
Estancia Vivorata
Estancia Ituzaingó
Estancia La Copelina
Cabo Corrientes
La Quarenó
Pago Chico

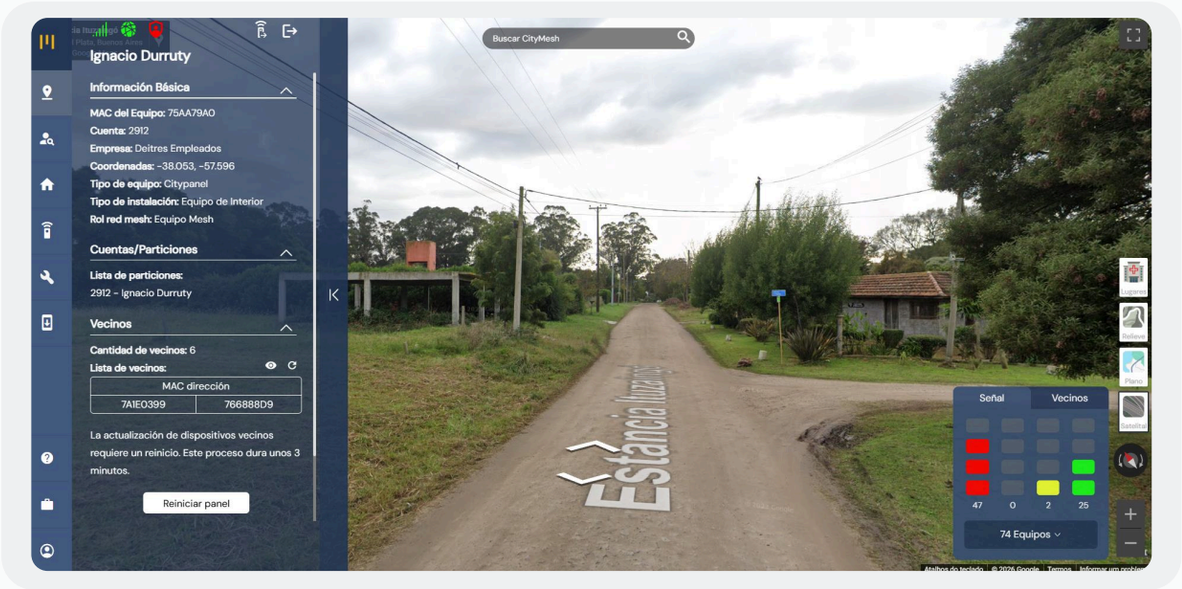
- **View types:** You can select or deselect multiple views on the map. Customize the map view according to your needs.

Available options:

- **Standard mode:** Clean display without location or road markings.
- **Terrain mode:** Ideal for monitoring devices installed at height.
- **Flat mode:** Traditional view for clear monitoring.
- **Street View:** Locates the exact street where the device is installed.

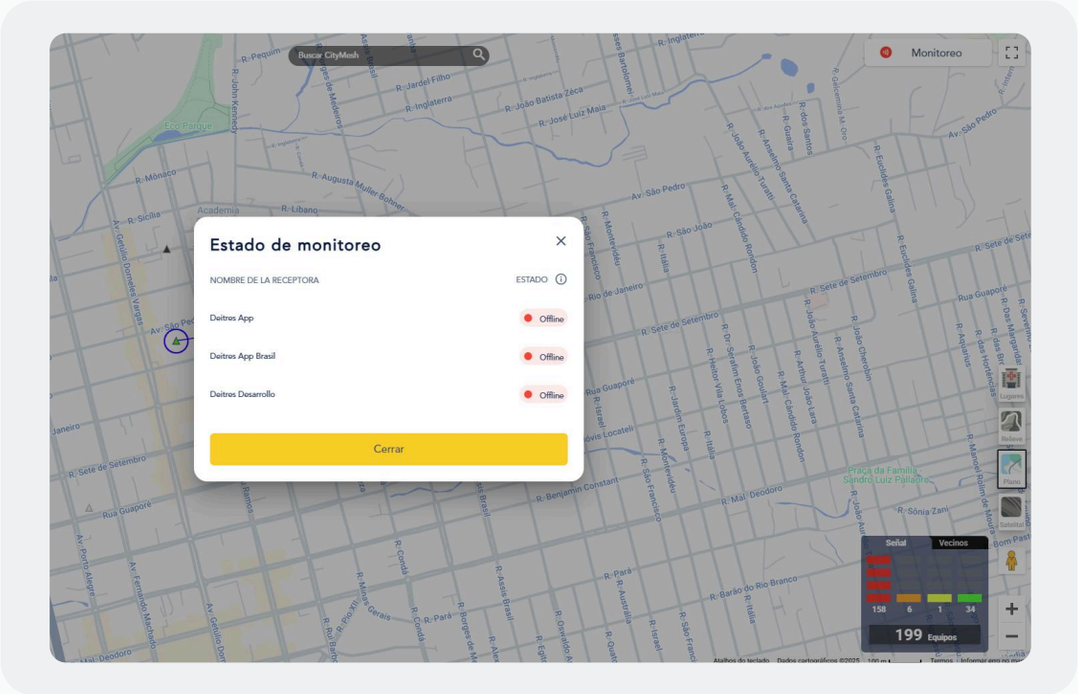
Adjust the view according to what you need at each moment.



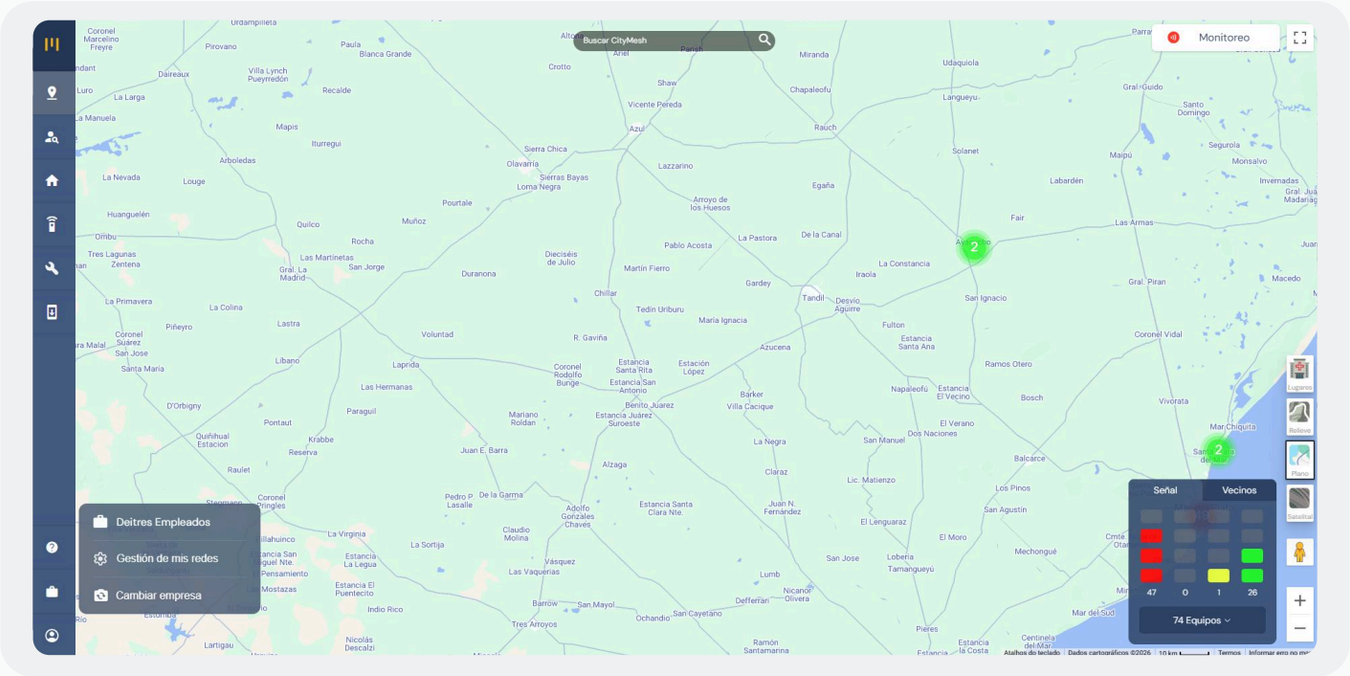


- **Receiver monitoring:** This function displays the **monitoring status** of the receivers, indicating on the screen which **ones require attention** and which have active or inactive monitoring. It always appears **in the top-right corner.** Clicking on it allows you to view the names of the **receivers** currently being monitored.

- **Active:** Approximately every 5 minutes, the receiver sends a message to our services indicating the connection status with the monitoring system, i.e., whether it is transmitting information to monitoring software. If it is, it will be active.
- **Inactive:** Cases in which the receiver is not transmitting messages to the monitoring software. In other words, the monitoring software is not connected to the Citymesh receiver.
- **Receiver Offline:** In this scenario, the receiver has not sent a message in the last 5 minutes. The Citymesh receiver is not available for use.

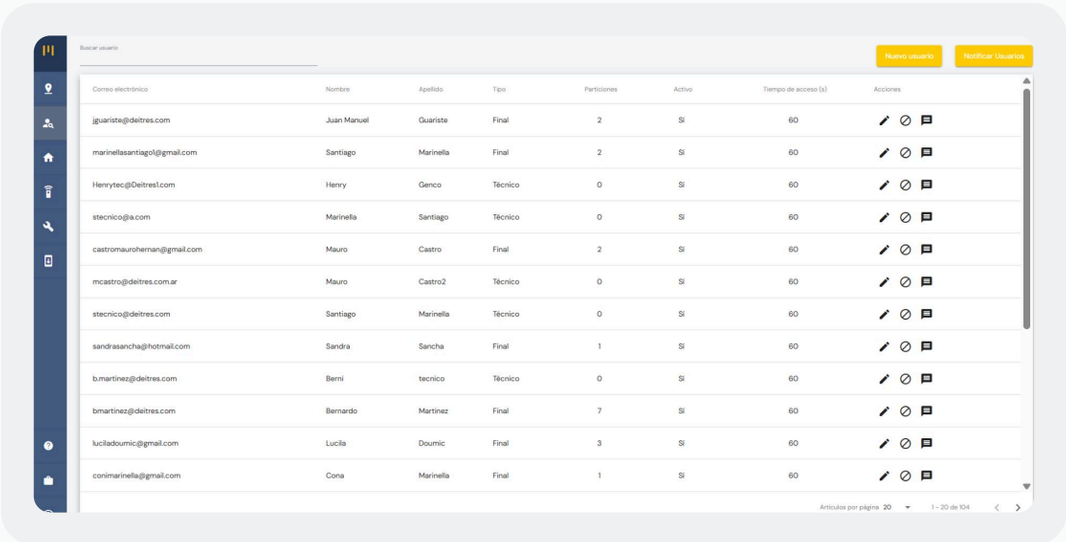


- **Company filter:** Here you can **view and filter** the companies you have access to. With this **menu filter,** you can view and select **each company and receiver** according to the options available to your user. If you are a **distributor** and have **administrator access,** you will have an additional access level.



Users

In the Users tab, you will find options for creating a new user, editing, deactivating, and viewing information, as described below.



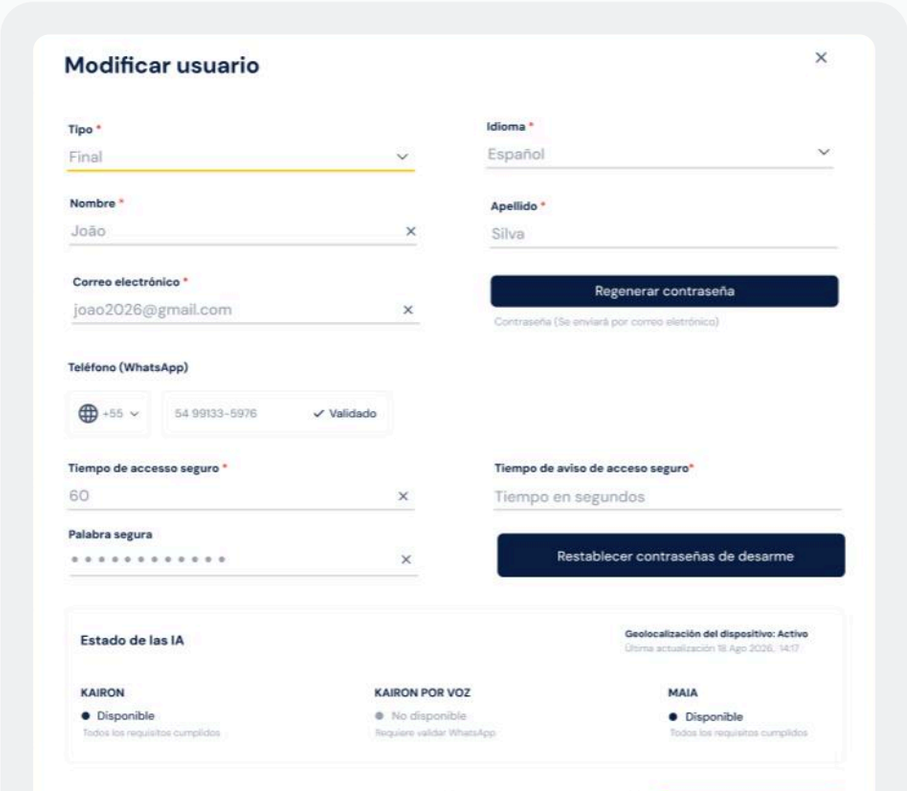
- **New Users:** Can be end customers, who will later be assigned partitions associated with panels, or technicians, who will perform installations, partition additions, and technical services. You must have the email address, first name, and last name ready to create the user. The password is created automatically by pressing “Regenerate password”. The customer logs in for the first time using this generated password, and the CityMesh App asks them to change it to a personal password. Finally, on this screen you can edit the secure access time, which is set to 60 seconds by default, as well as define the security word that the user will use with the Kairon voice feature.

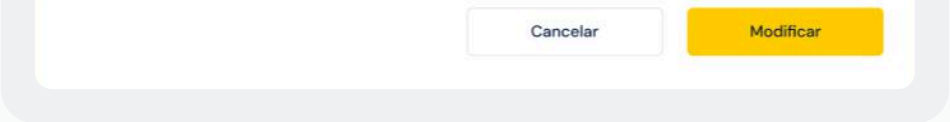
- **End customers:** users who will be assigned partitions associated with panels.
- **Technicians:** users who perform installations, partition additions, and technical services.

Important!

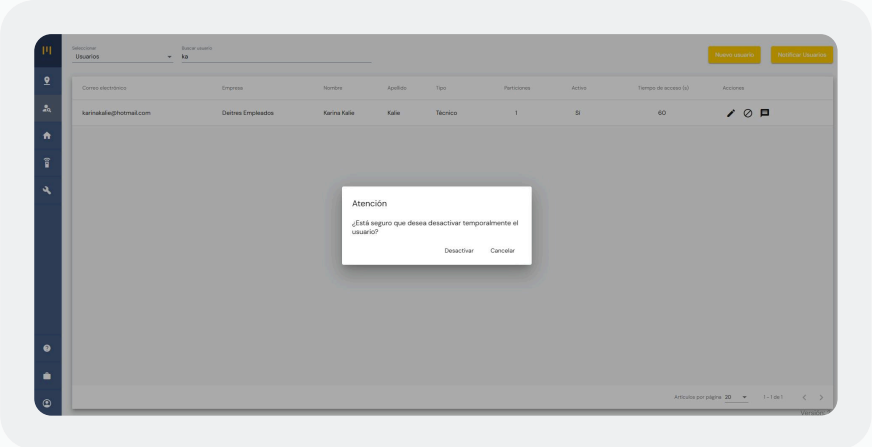
- Once you click “**Add User**”, an **automatic email** will be sent to the registered email address containing the application **access password.**

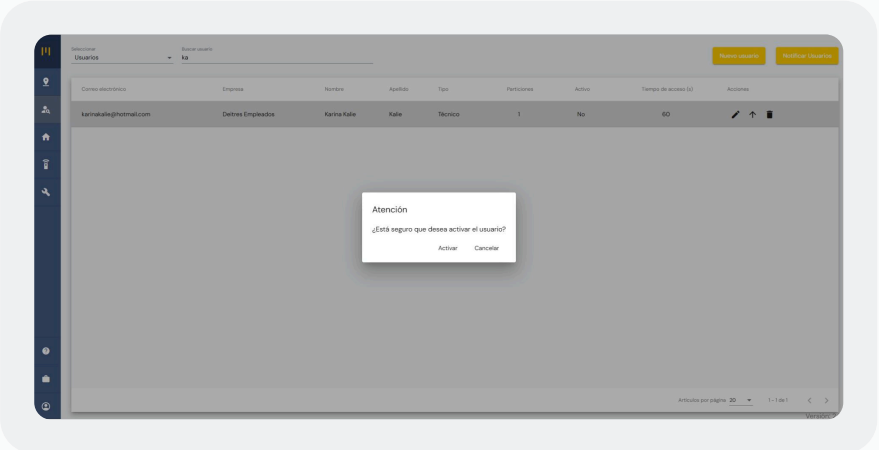
- **Edit User:** Once a user has been created, it can be edited to change any of the fields configured previously. This means that if a user was mistakenly defined as a technician when they are actually an end customer, or if there is an error in the first or last name, it can be corrected. You can also regenerate the user's passwords and clear both disarm PINs. When the password is regenerated, it must be sent to the user, who must change it to a personal password. If the disarm PINs are cleared, the user can define them again as desired. On this screen, the technician can also verify whether the user's WhatsApp number has already been validated. Finally, in the "**AI Status"** section, you can check whether the artificial intelligences are active/available for that user or review which requirements are missing for activation (for example, WhatsApp validation).



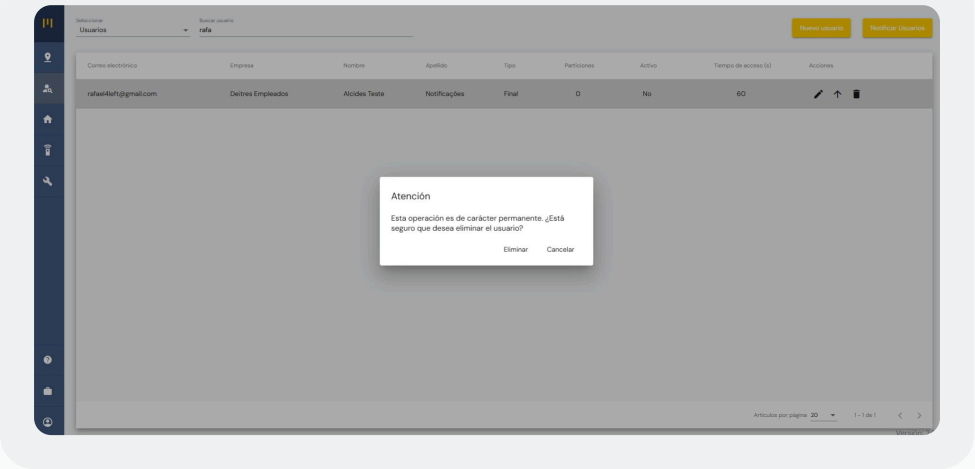


- **Temporarily deactivate user:** this prevents the user, whether a technician or end customer, from using the CityMesh App. The action is reversible and can be reactivated without losing the user's information.





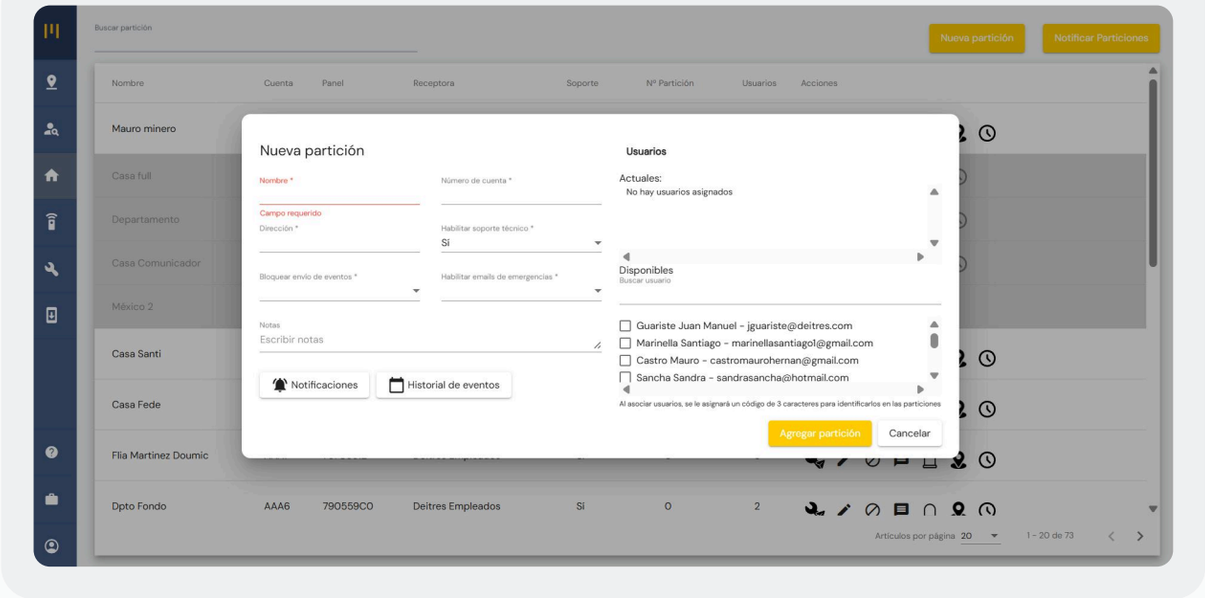
- **Delete user:** after temporarily deactivating a user, you can permanently delete them. This will cause the information associated with the user to be lost, and to have the user in the system again, you must create a new user.



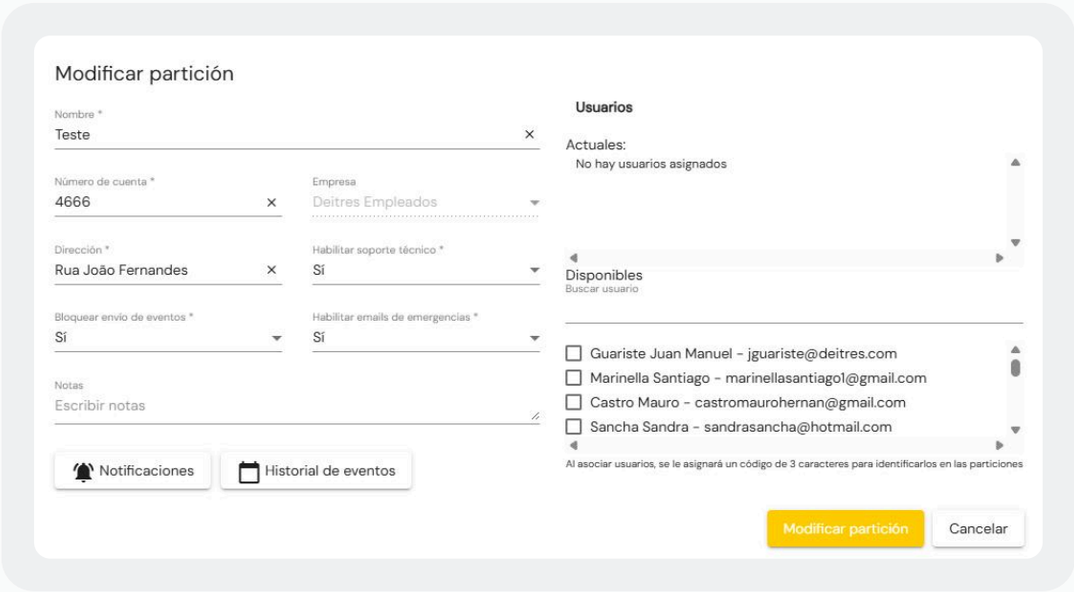
Particões

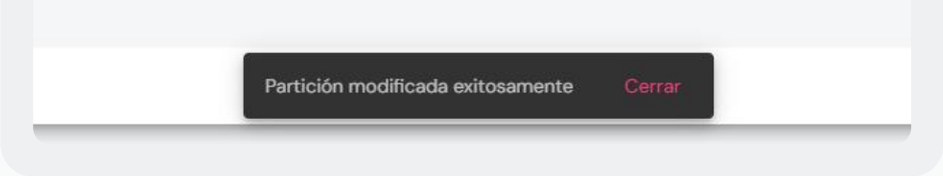
You can access the partitions view, where actions similar to those available in the users view can be performed, but with other types of fields. Specifically, this screen allows you to send a partition to the technical support screen, edit the partition, delete it, send notifications, trigger the siren, view its location on the map, and configure Kairon schedules.

- **New partition:** to do this, you need the name, address, account number, and the users to be assigned to the partition. It is extremely important to associate all end users who will use this partition; they must have been created previously. You can also define whether technical support will be enabled for this partition. Optionally, you can add a note with any additional relevant information.

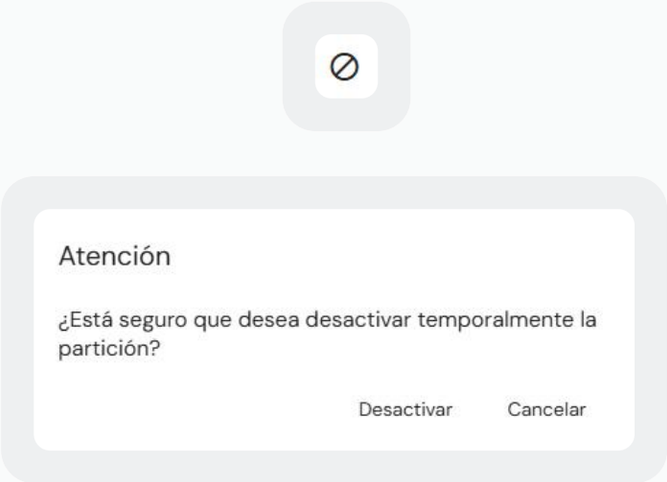


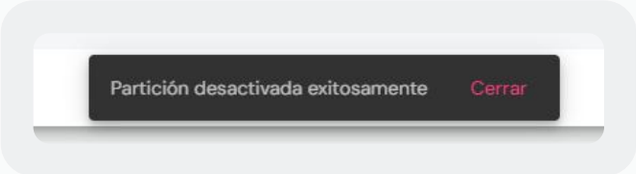
- **Edit Partition:** once the partition has been created, it can be edited to change any of the previously configured fields. If the partition is already associated with a MAC number, its partition account number cannot be edited.



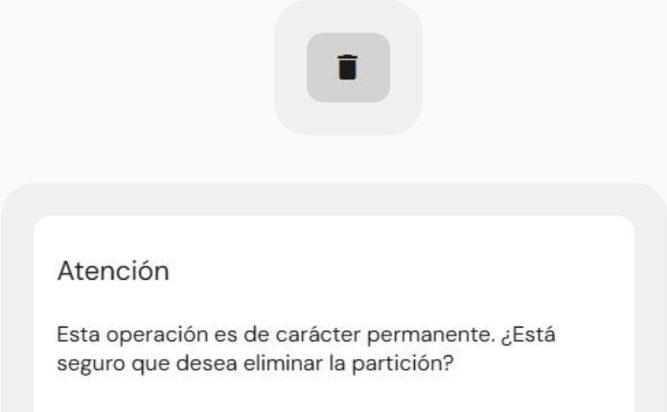


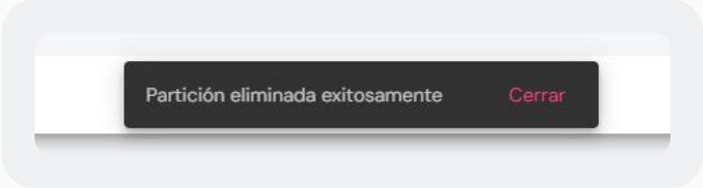
- **Temporarily Deactivate Partition:** this causes the partition to stop reporting. The action is reversible and can be reactivated without losing the partition information.





- **Delete Partition:** after temporarily deactivating a partition, it can be permanently deleted. This will cause the information associated with it to be lost, and to have it in the system again, you must create a new partition.





- **Send to technical support:** sends the partition directly to the technical support screen.
- **Notify:** sends notifications to linked users.
- **Trigger siren:** activates the siren remotely.
- **View on map:** displays the geographic location of the partition.
- **Configure Kairon schedules:** defines the operating schedules or time schemes for the Kairon AI.

Panels

You can access the panels view, where some of the same actions available for users and partitions can be performed. There is no “New Panel” feature because a panel is created automatically when the installed panel reports for the first time. There is also no “Deactivate Panel” feature. Panels cannot be deleted either. The only available action is:

- **Edit Panel:** although most fields cannot be changed, you can add a note. You can also verify link status.
- **Panel Installation Process:** to install a new alarm panel, follow a series of steps. First, create a technician user who will install the alarm panel through the CityMesh App, and create all end users who will use the equipment. Then create the partition and assign the corresponding end users to it. Everything will then be ready for a successful installation.

- **Panel Uninstallation Process:** before uninstalling equipment, it is recommended to deactivate and delete all associated partitions from the WebApp. At this point, partitions associated with the MAC number being uninstalled will move to the "deprecated" state. Once the partitions have been deactivated and deleted, you can proceed with uninstalling CityMesh from the corresponding subscriber.
  The equipment can be reused with new customers by following the normal panel installation steps. When installing this new equipment, partitions that were previously associated will appear as deprecated. The system will ask whether you want to delete them, and you can remove them.

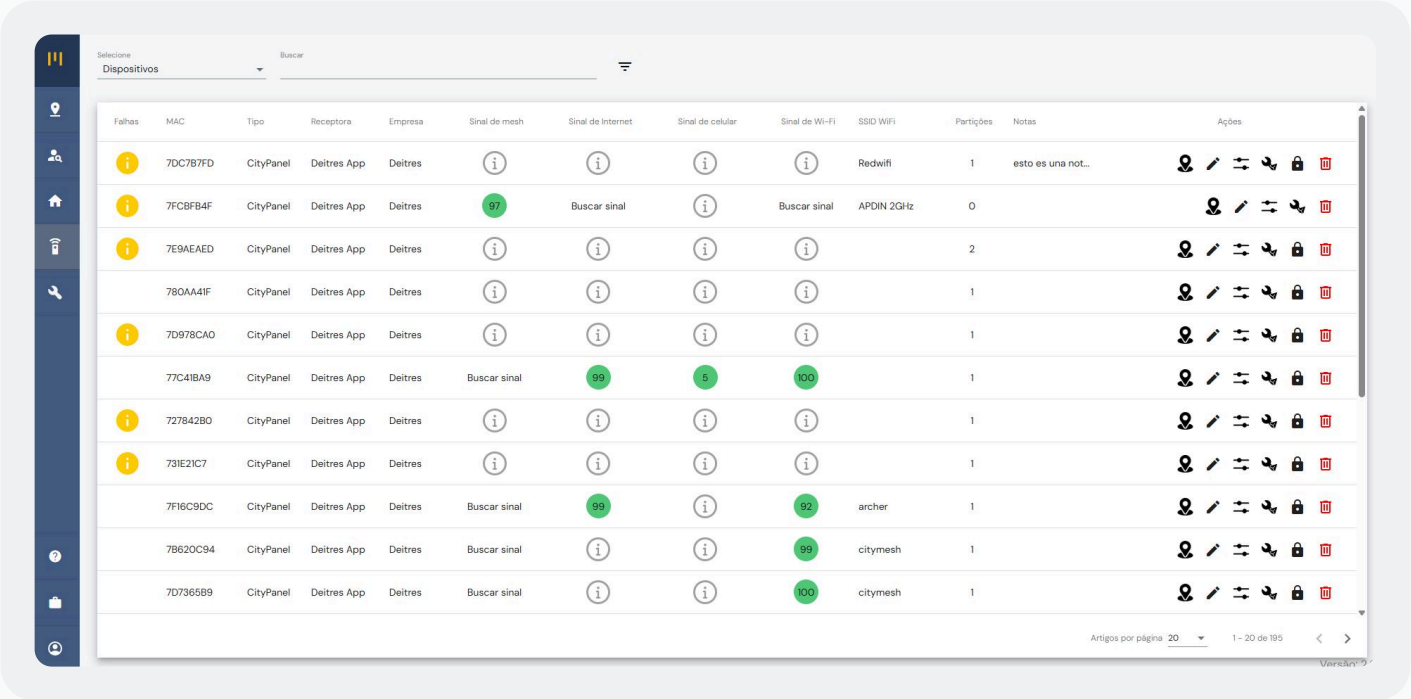
CityMesh Management

In this tab, you can manage your devices, which are the same devices shown on the map.

Main features:

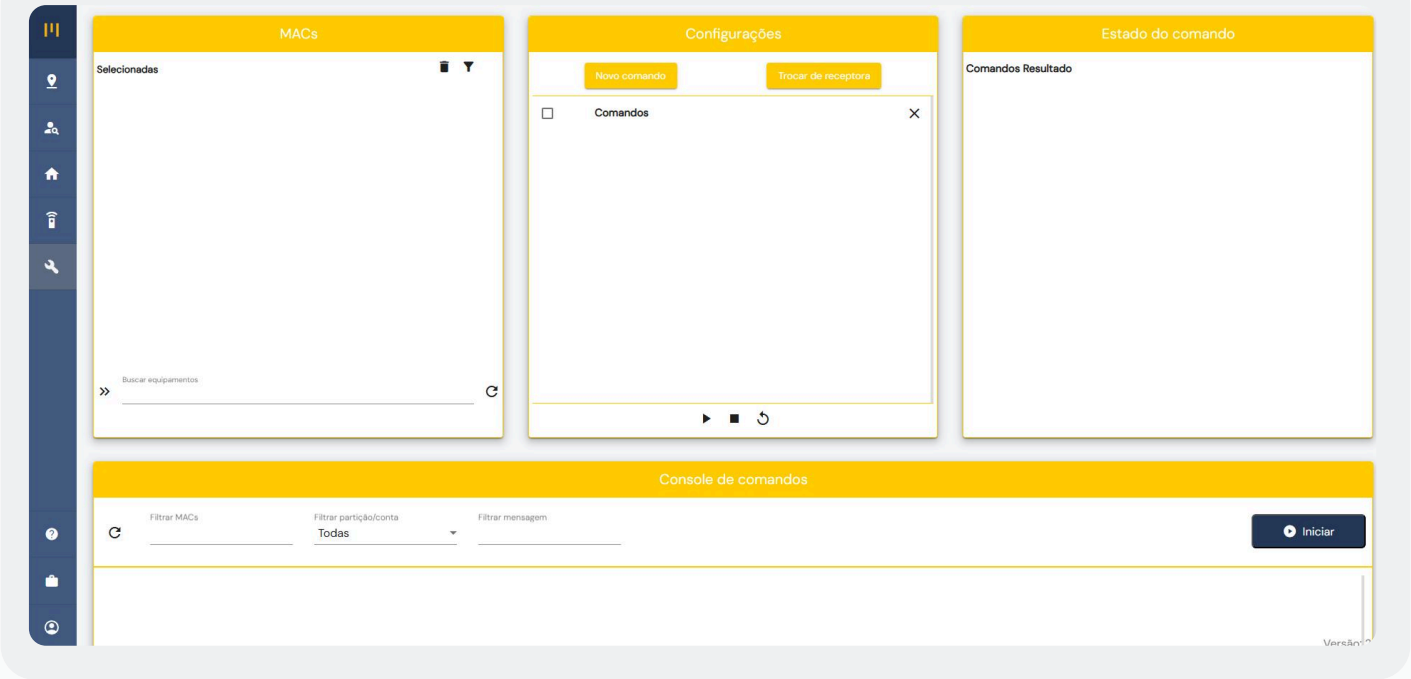
- **List view with the most relevant information.**
- **Send a device to the support tab.**
- **Modify panel information.**
- **Access the map directly by clicking the device location icon.**
- **Other actions such as the virtual keyboard and installation mode.**

Manage your devices quickly and efficiently from this section.



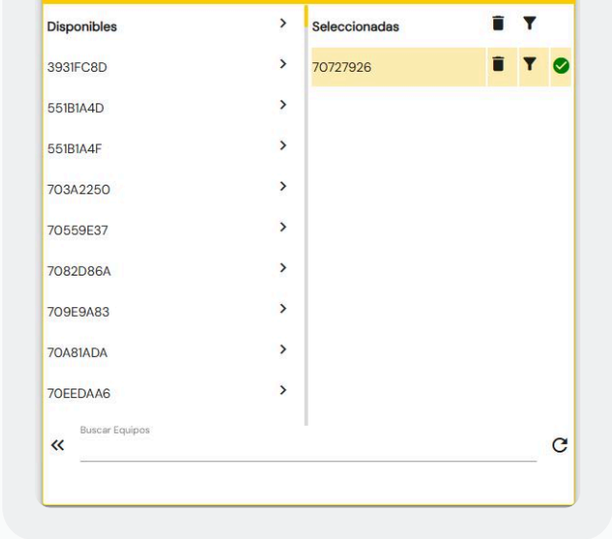
Technical support

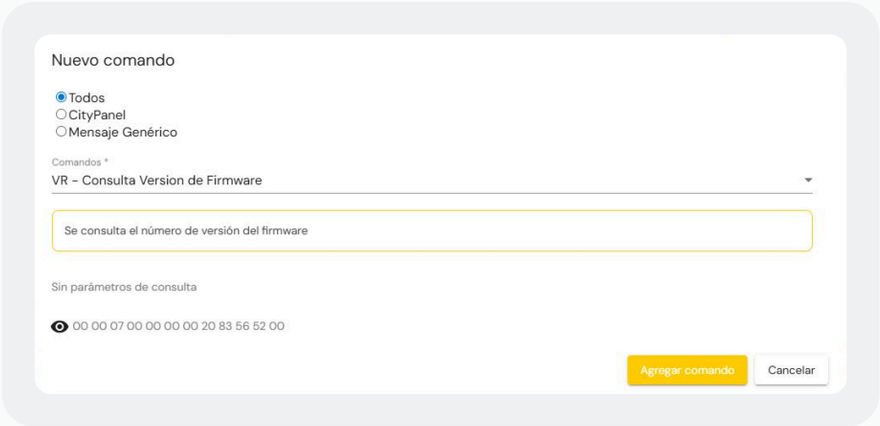
In the **technical support** tab, you can **send commands** to a device, **track feedback** from the sent command, and **analyze the information on screen**. These actions can be **performed on more than one device at the same time**. You can then **filter** devices by **MAC** for a more specific search.



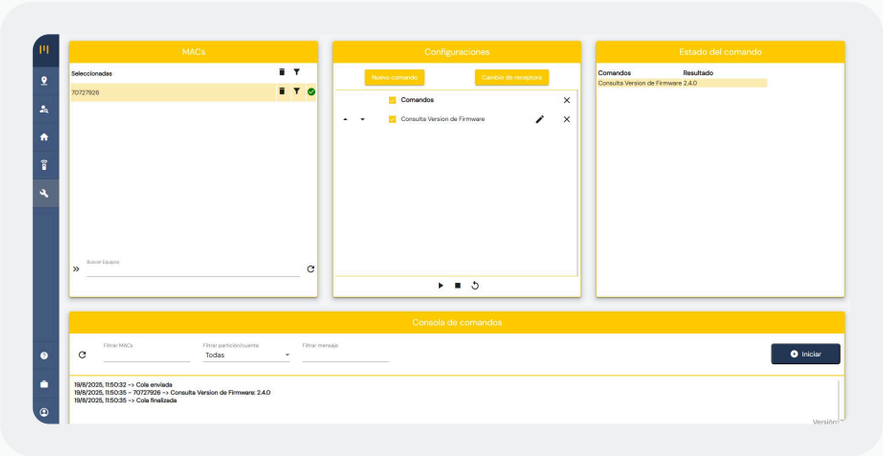
- **Sending commands:** On this screen, you can choose which device(s) to send commands to. There is a search equipment option, where all equipment in your account will be listed. After selecting them, they will be shown in the “Selected” item.

  In the settings section, you can select which commands to send, customizing them according to the standard through the “eye” icon.

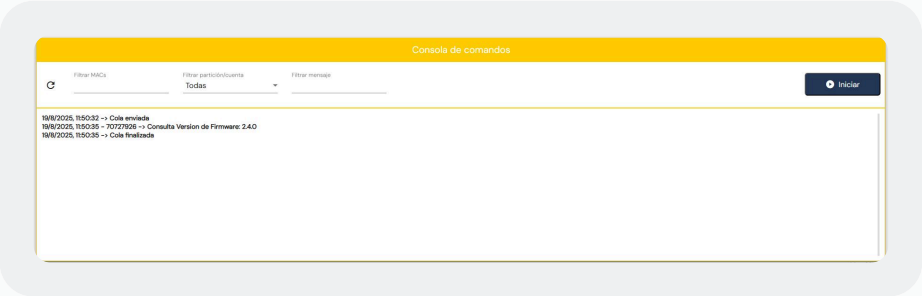




After choosing the command, click the “Start” button so the system executes the send operation, and monitor its status in the “Command status” section.

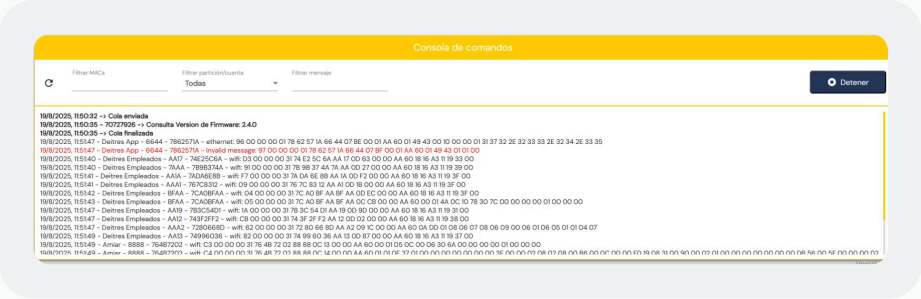


You can also view the results in the command console, located below the sections mentioned above. If you are sending commands to more than one device, you can use filters by MAC, partitions, or even message.



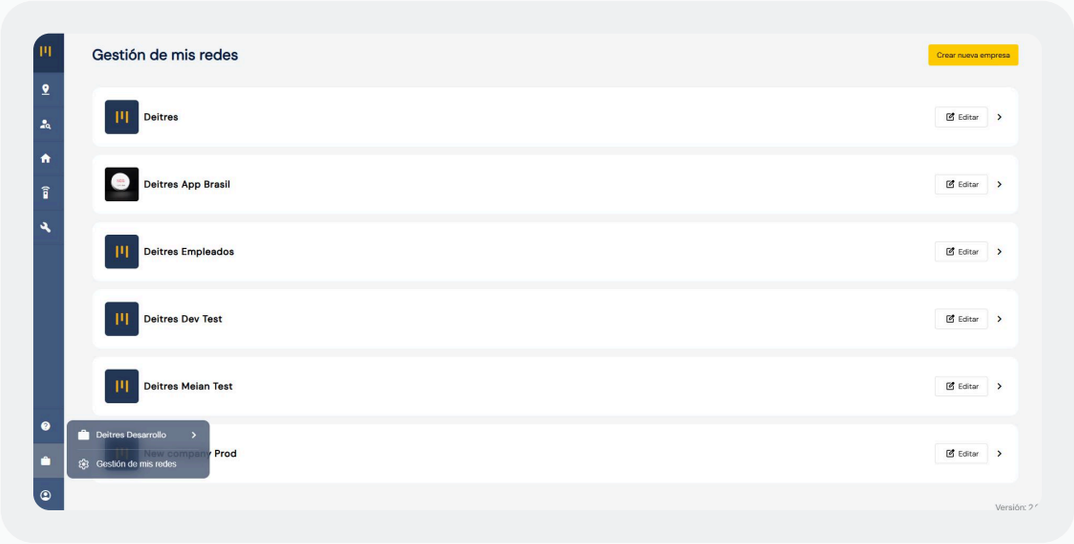
- **Command Console:** In this section, you can click “Start” directly, and the console will display the messages traveling through all devices in your account.

  This feature provides an overview of your network, helping identify possible failures, as in the example shown. Remember that you can also apply filters by MAC, partition, or specific message. When you click “Stop”, the console stops displaying messages in real time.

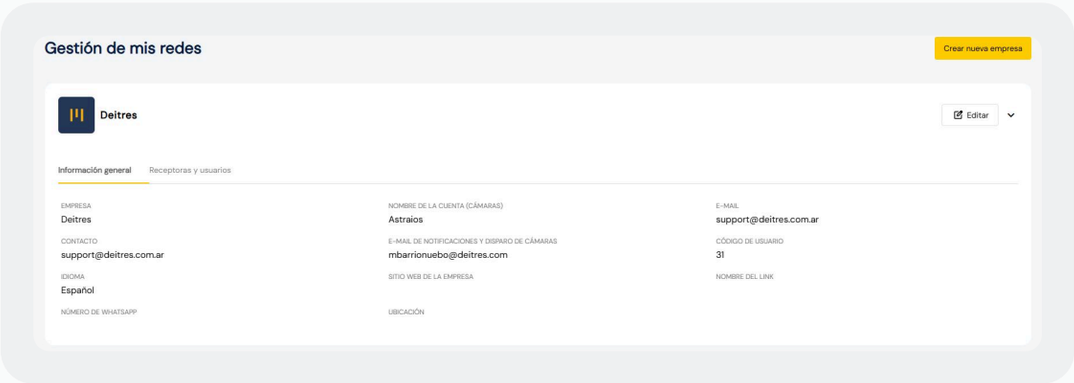


Manage my network

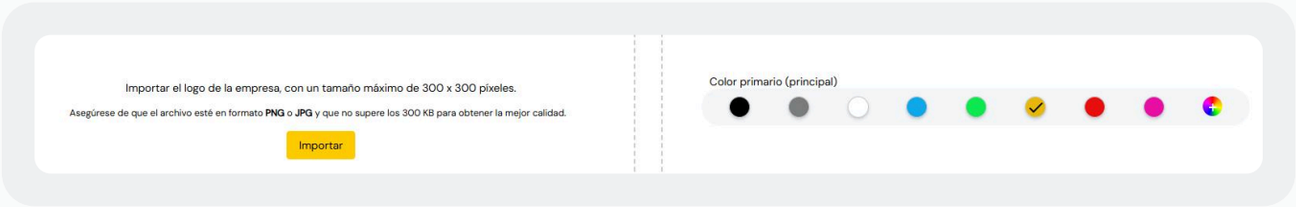
This feature allows users with administrator profiles to adjust their company and receiver registration information, as well as manage the users who access the platform and view company information (network, equipment, failures, and command sending).



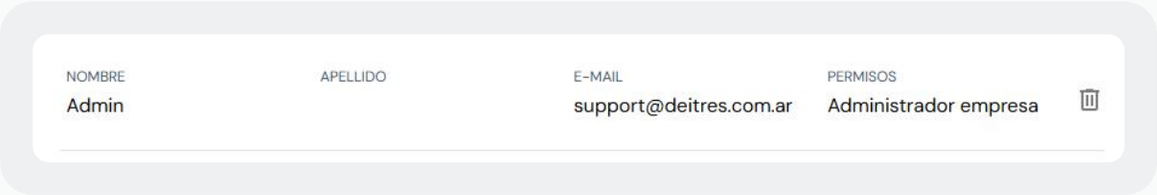
As shown in the example, you can view and edit (according to your permissions) the company's main registered information by clicking the "Edit" button in the upper-right corner of the screen. Remember that some data is mandatory and must be kept up to date.



- On this page, you can also change the logo displayed in the application, together with its colors.
- Remember to follow the instructions regarding the file format and size shown on screen.
- After saving the changes, they will be reflected in your application. If they are not updated, we recommend logging out and logging in again to renew your session and load the new information.

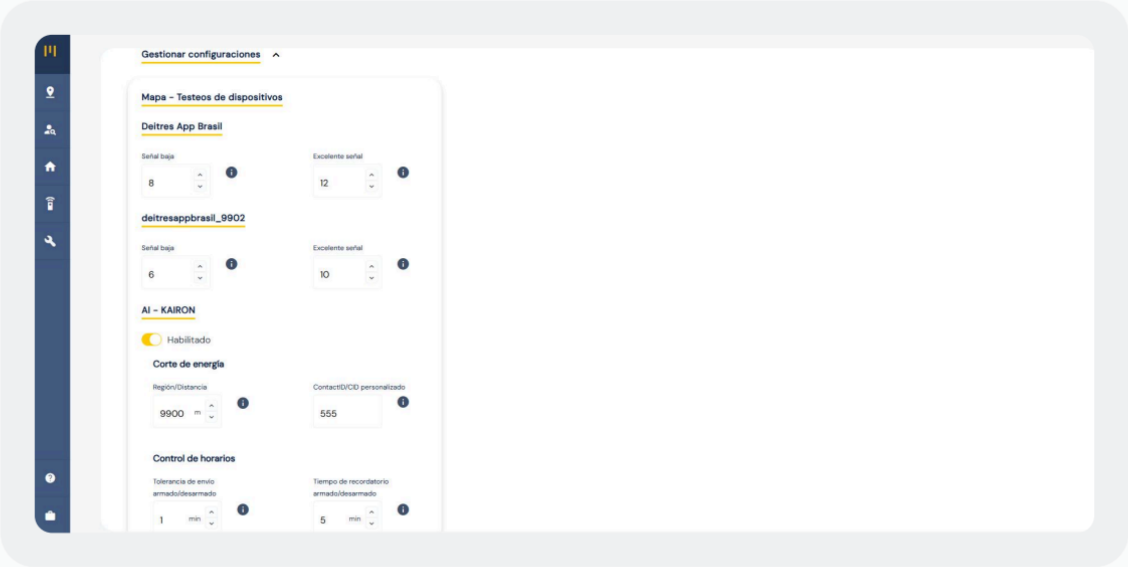


When creating a company, the email address entered as administrator on the first screen will receive the platform access password information. Attention: you do not need to create a user using that same email address again.



IA – Kairon

In the Settings tab, you will find the “Kairon AI” option. When enabled, you can use the “**Power outage**” and “**Schedule control**” features. When a user has a permission level lower than Administrator, no editing is allowed in these settings. In that case, they must contact the company’s direct administrator.



When the user is an administrator, the Edit button is available. Clicking it takes the user to the feature configuration modification screen.

- **Power outage:** This feature is designed to manage mass power failures in a region, where the monitoring software will receive the automatically handled Contact ID or CID event, preventing the monitoring center operator from spending time checking an event that does not require human action.

Important!

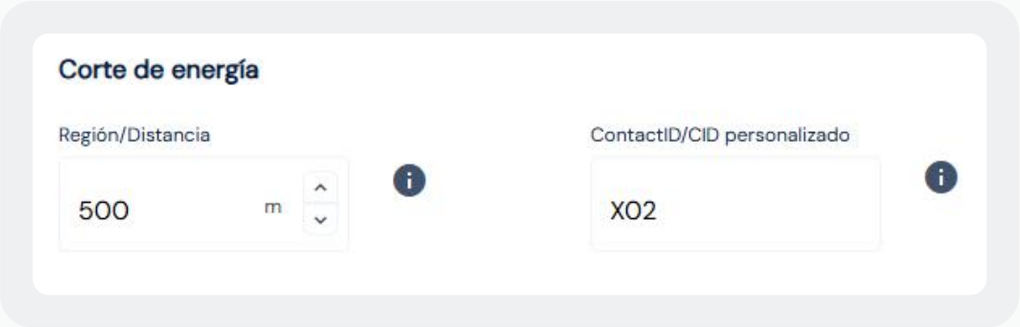
Key points:

- Use of Contact ID (CID), the standard for alarms.
- Events marked as automatically handled (without manual intervention).

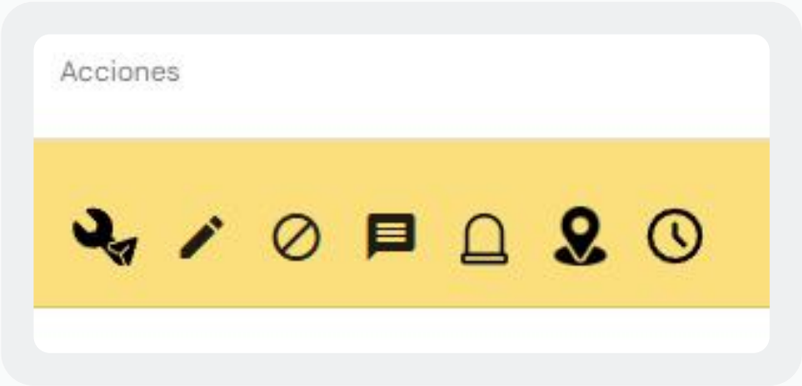
To configure this feature, complete the fields:

- **Region/Distance:** The area the system will consider when determining whether a mass failure has occurred. Example: equipment within a 500-meter radius that reported event E301 (power failure), where the report arrived within a 60-second interval, with more than 2 events, is considered a mass power failure.
- **Custom ContactID/CID:** Code used in your company's monitoring software to represent an automatically handled event (without human action). Completing this field tells the system that when a power failure meeting the mass-failure criteria occurs, your monitoring software will automatically receive this information, integrating the workflow configured by the company.

These fields are configured by default, but the user can modify them. The region field is entered in meters and can be increased in 100-meter increments. The ContactID field accepts up to 5 characters, using letters and numbers.



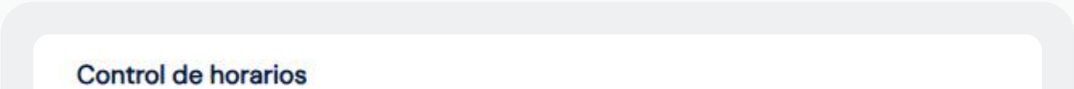
- **Schedule monitoring:** This function allows for logging the sending of reminders to the end user via WhatsApp, notifying them of the alarm panel's arming or disarming times. Upon activating the Kairon AI feature, the system displays a clock icon next to the existing settings in the “Partitions” tab.

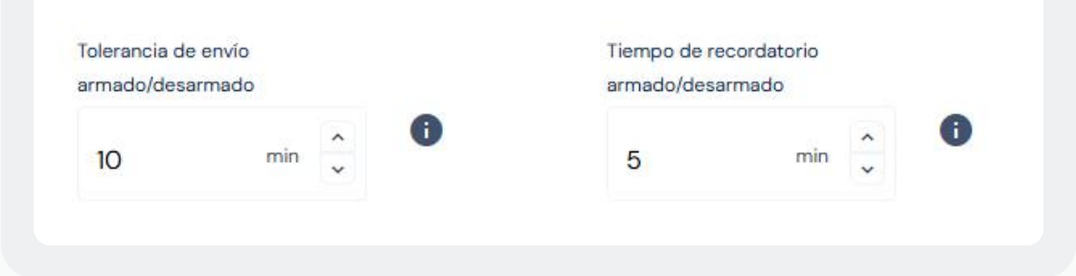


This is where the operator configures schedules. Before that, some settings can be modified:

- **Arming/disarming reminder tolerance:** this time can be configured according to need. By default, there is a 10-minute tolerance. If the end user arms or disarms within the configured tolerance period, they will not receive the WhatsApp reminder.

- **Arming/disarming reminder time:** this is the interval at which Kairon sends reminders to the end user. Remember that reminders are sent a maximum of 2 additional times, for a total of 3 messages including the first message. The default interval is 5 minutes, but it can be changed as needed.



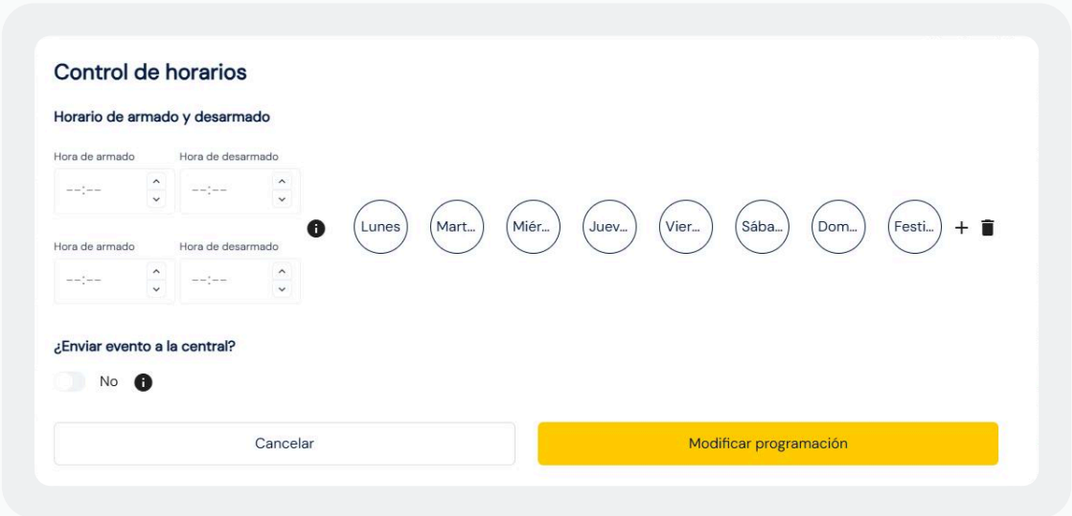


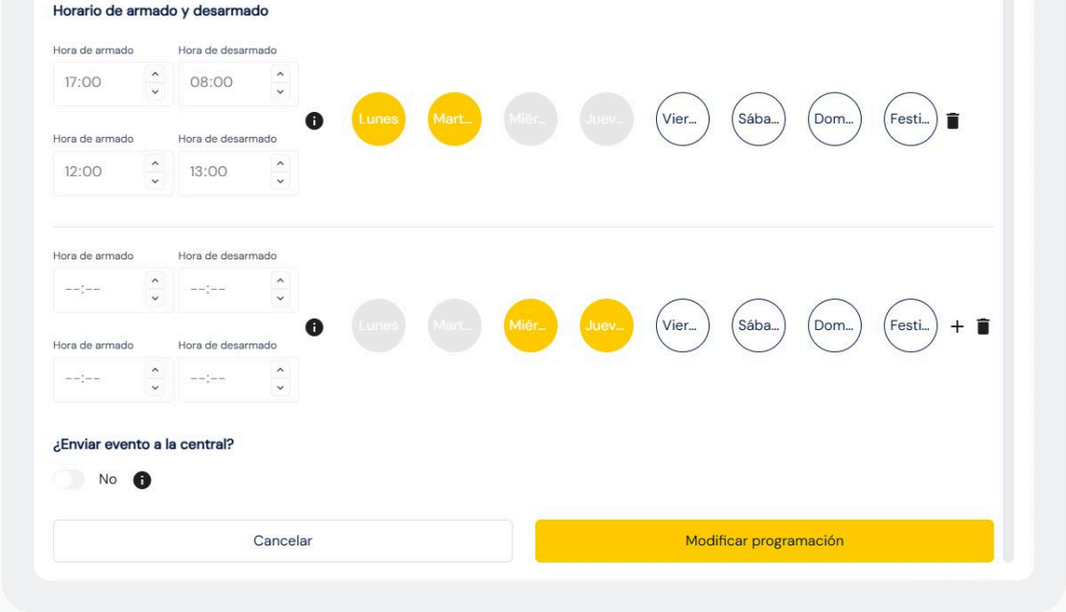
After completing the previous settings, return to the partitions screen. By clicking the clock icon, the user will see a pop-up to configure the times and days of the week when reminders should be sent to the end user.

This feature allows a maximum of 4 schedules for arming and disarming actions per day of the week.

Fill in the times in the available fields, **paying attention** to which field is for arming and which is for disarming. Then select the day of the week that should follow that schedule; you can select one day or all days.

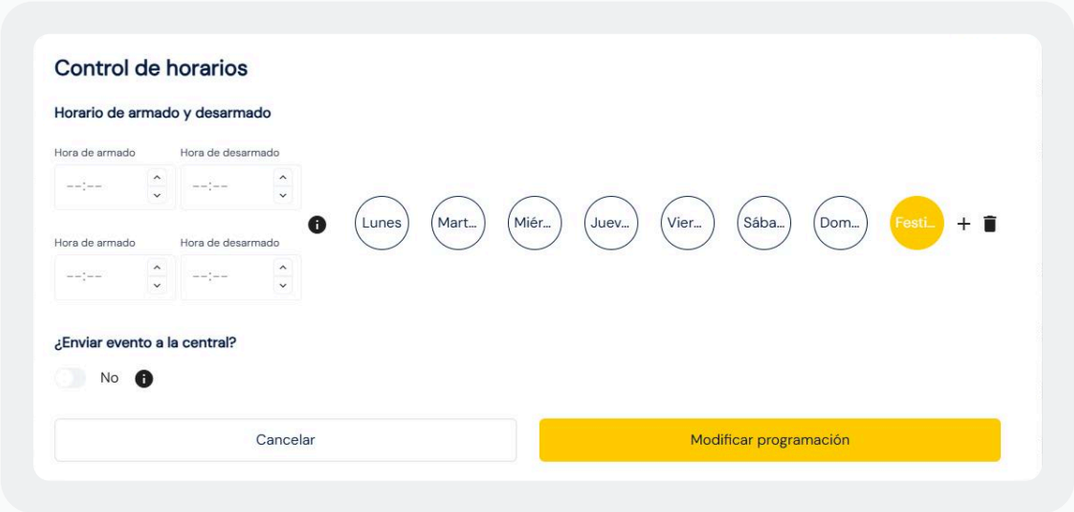
For different schedules, click the “+” icon to display the next available row for days.





The trash can icon allows you to delete the schedule set for that row. When you are on the first schedule row and use the trash can icon, all day settings will be cleared, leaving the fields empty.

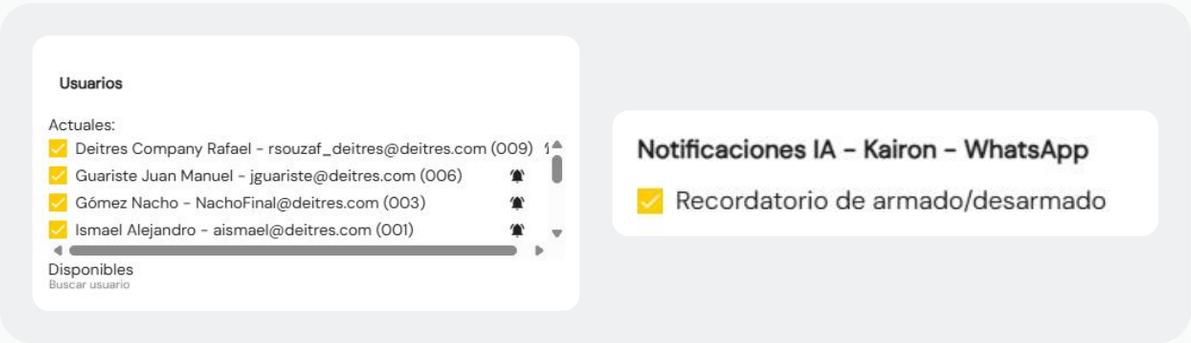
To deselect a chosen day, simply click on it again. Holidays follow your region's standard calendar. Therefore, you may need to use different schedules on these days; these can be configured by creating a row with only that option selected.



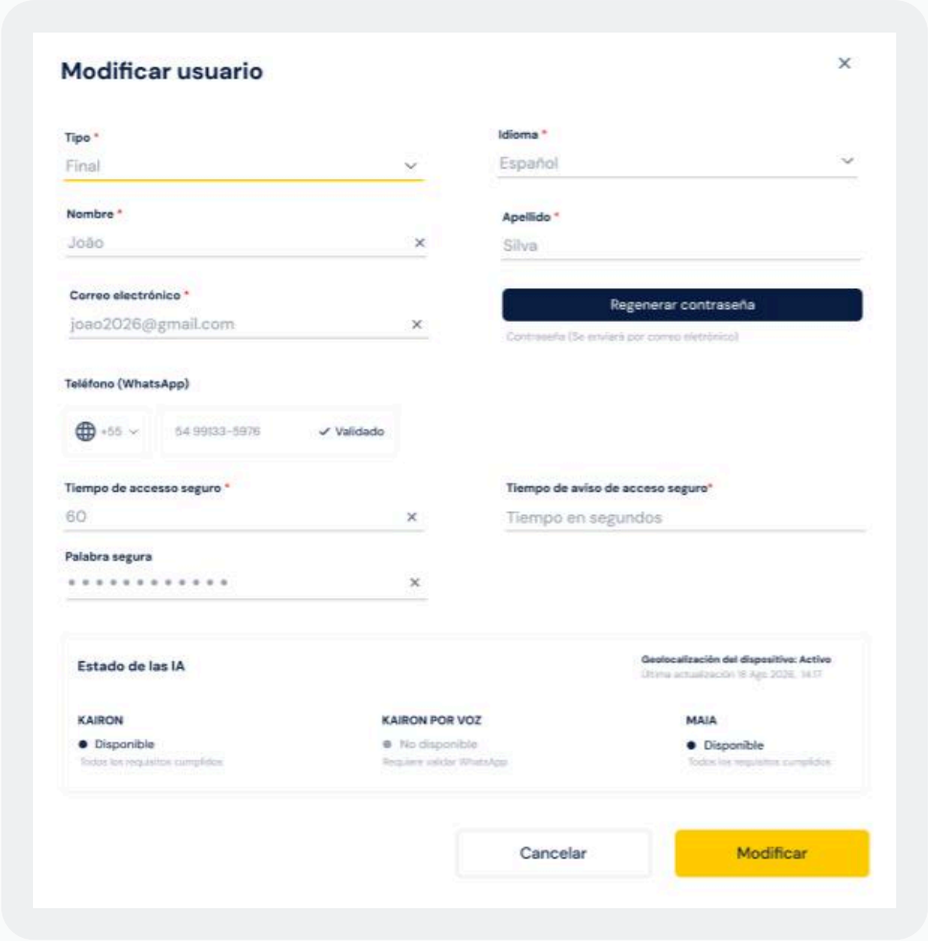
After completing the schedule and day configuration, do not forget to save the action using the “Modify schedule” button.

After the change is saved, the end user of that partition will start receiving Kairon reminders via WhatsApp.

To choose which user or users can receive the notification, access the partition tab, open Edit, and click the end-user notification setting (bell icon next to the user’s name). Then select the “Arming/disarming reminder” option and save the configuration.



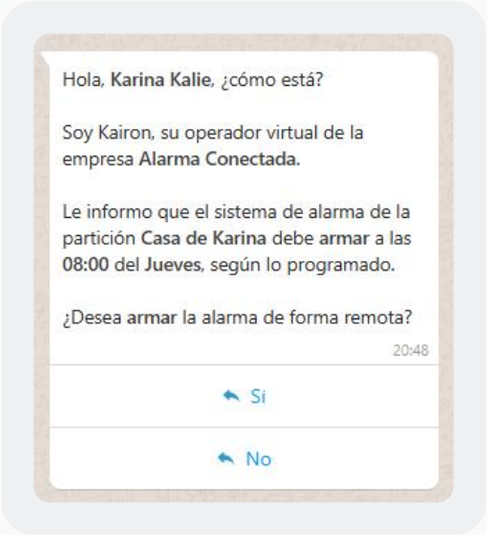
The user must always have a phone number entered so Kairon can communicate with them via WhatsApp. This can be configured in the user creation or editing tab.



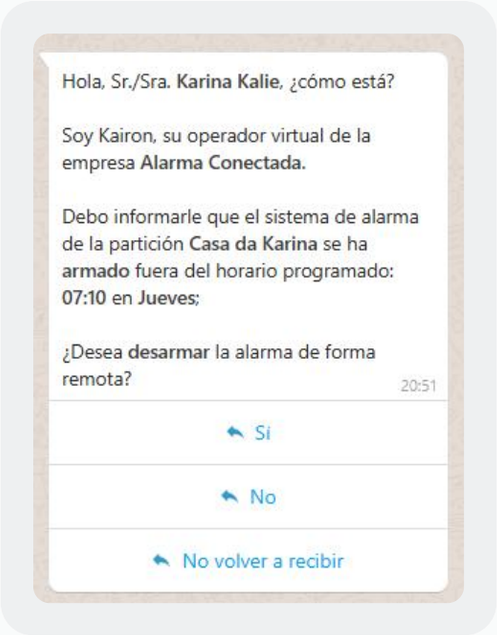
Based on the previous settings, the user will begin receiving reminders according to the scheduled times. In the event of a power outage, they will receive an alert message stating that the company is already aware of the situation and is continuing to monitor it.

Examples of messages sent:

1. Alarm panel arming or disarming reminder.

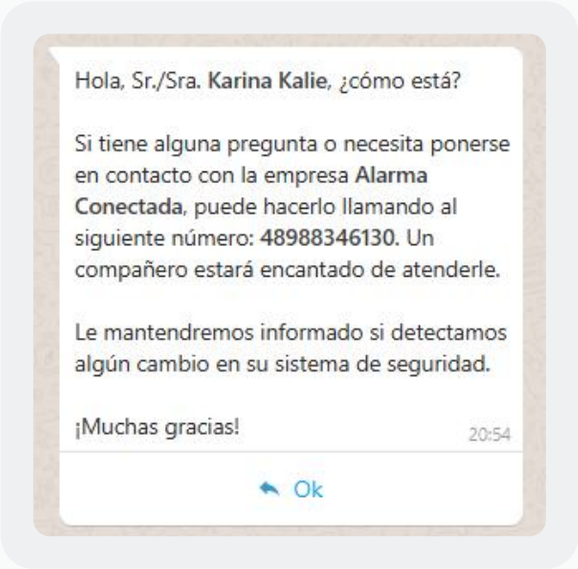


2. Reminder sent when the user arms or disarms outside the scheduled time and also outside the configured tolerance.

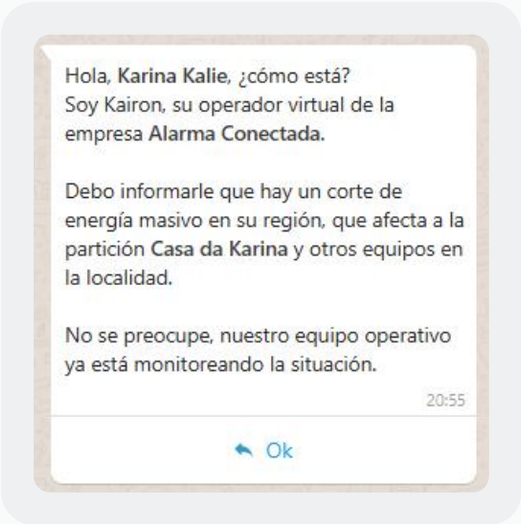


When the user activates “Do not receive again”, they will not receive new arming or disarming reminders outside the scheduled time for 24 hours. After 24 hours, they will resume receiving this type of reminder normally.

3. Reminder sent when the user sends a message outside the contact flow.



4. Reminder sent when a mass power failure occurs.



Always remember to check the previous settings:

- Kairon AI feature enabled on your company settings screen;
- Fields configured according to your operation;
- End user phone number registered;
- Notification enabled for that specific user.

- **Send event to monitoring center:** when this option is enabled, it means that the end customer wants human contact after the 3 communication attempts made by Kairon through WhatsApp.

  In this scenario, after the attempts are exhausted, the monitoring software receives a Contact ID or CID event: E616, meaning "Service request", so the monitoring center operator can contact the end user.

When this option is disabled, the 3 reminders are sent by Kairon through WhatsApp and no other action is taken.

KAIRON por Voz

Kairon by Voice is an Artificial Intelligence assistant that communicates with the end user by telephone at the exact moment an alarm is triggered. Its goal is to automatically filter false alarms and detect real-risk situations (coercion or panic) safely and discreetly, reducing the monitoring center's operational workload.

1. For the Monitoring Center (configuration in Cloud Deitres)

For the service to work, the administrator must enable and configure it from the cloud platform.

How to cnfigure?

1. Log in to Cloud Deitres.
2. Go to the **Manage my network menu > Configuration tab.**
3. Select the desired company, click Edit, and find the **"AI KAIRON BY VOICE"** block.

Configurable parameters:

- **Enabled (Switch):** Switch to turn Kairon's voice flow on or off for the entire company.
- **Call retry limit:** Maximum number of times Kairon will attempt to call users (minimum 1, maximum 5; default: 3).
- **CID (Contact ID) code mapping:** Fields used to customize event codes sent to your monitoring software.

Notification note: *When a call classified as risk (Event B) or communication failure (Event D) ends, Kairon will automatically send an email to the monitoring center with the call audio and/or the complete conversation transcript attached.*

How does Kairon logic work?

- **Geofencing (200 meters):** Kairon will only start the call if the system detects at least one user within a 200-meter radius of the panel. If nobody is nearby, Kairon does not intervene and the alarm goes directly to the monitoring center.

- **Contact priority:** if several people are within the geofence, Kairon will call the **last user who armed the panel**, if that person is within the radius. If they are not, it will call the oldest user.
- **Security and discreet closure:** to protect the user's integrity, **the bot will never indicate an error** (for exemple, incorrect word or alert sent). If the user says the keyword incorrectly (coercion), or if there is noise and Kairon cannot understand after 4 attempts (or 10 seconds of silence), the bot will end the call politely and naturally, without alerting possible criminals at the location, and will silently send the alert event to the monitoring center.

2. For the End User (Mobile App Activation)

For Kairon to assist the end user through calls, it is essential that the **MAIA** assistant be enabled in the application, since they share the same technical requirements.

Essential prerequisites: As with MAIA, the user must have:

1. **A linked WhatsApp** number.
2. **Geolocation permissions configured as "Always"** (required to detect whether the user is within the alarm's 200-meter radius).
3. **Physical supervision** enabled.

Keyword Configuration (City Alarme App): The user has full autonomy to manage the security password that Kairon will request by phone to cancel a false alarm.

1. Open the **City Alarme** application and go to the **"AI"** (Artificial Intelligence) screen.
2. Find the **Kairon** section.
3. On this screen, you can manage your **keyword**. It is essential to choose a word that is easy to remember because you will need to dictate it to the voice assistant. If an incorrect word is repeatedly provided, the system will silently alert the monitoring center.

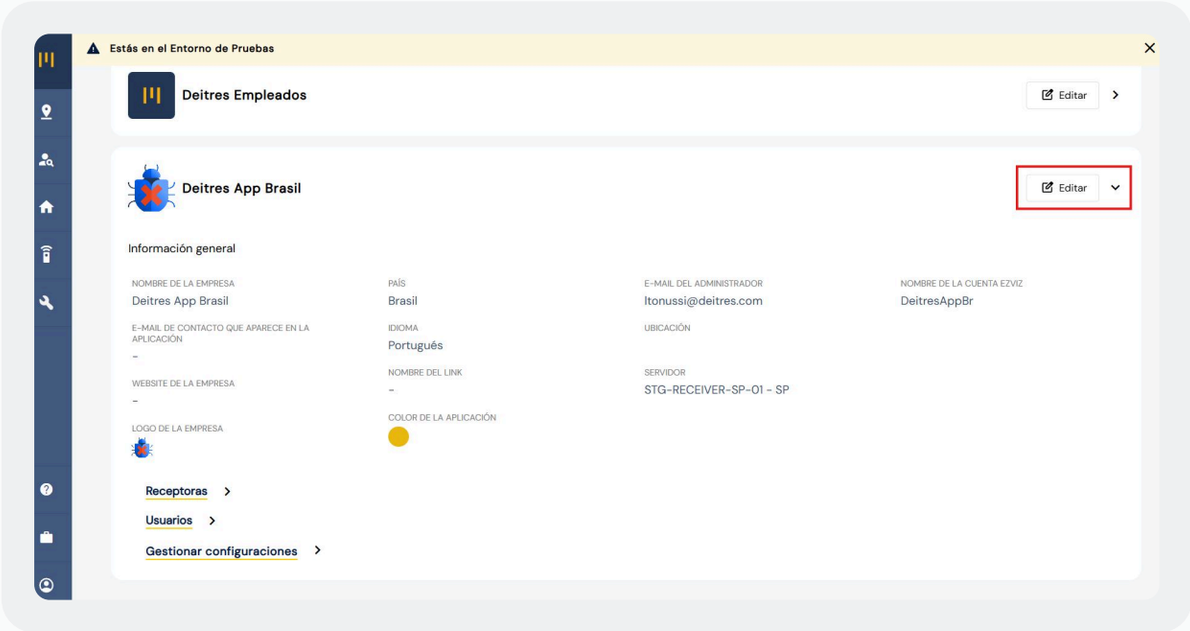
IA – Maia

MAIA is an AI-based assistant that uses user location to suggest perimeter arming and full arming.

1. **Administrator configuration (Cloud Deitres)**

Step 1: Global MAIA activation

1. Log in to Cloud Deitres.
2. Go to the Manage my network menu > Configuration tab.
3. Select the desired company and click Edit.



4. Locate the MAIA selector (flag) and enable it.
5. Required field: complete the “Perimeter arming from” and “to” fields (for example, 10:00 PM to 4:00 AM).

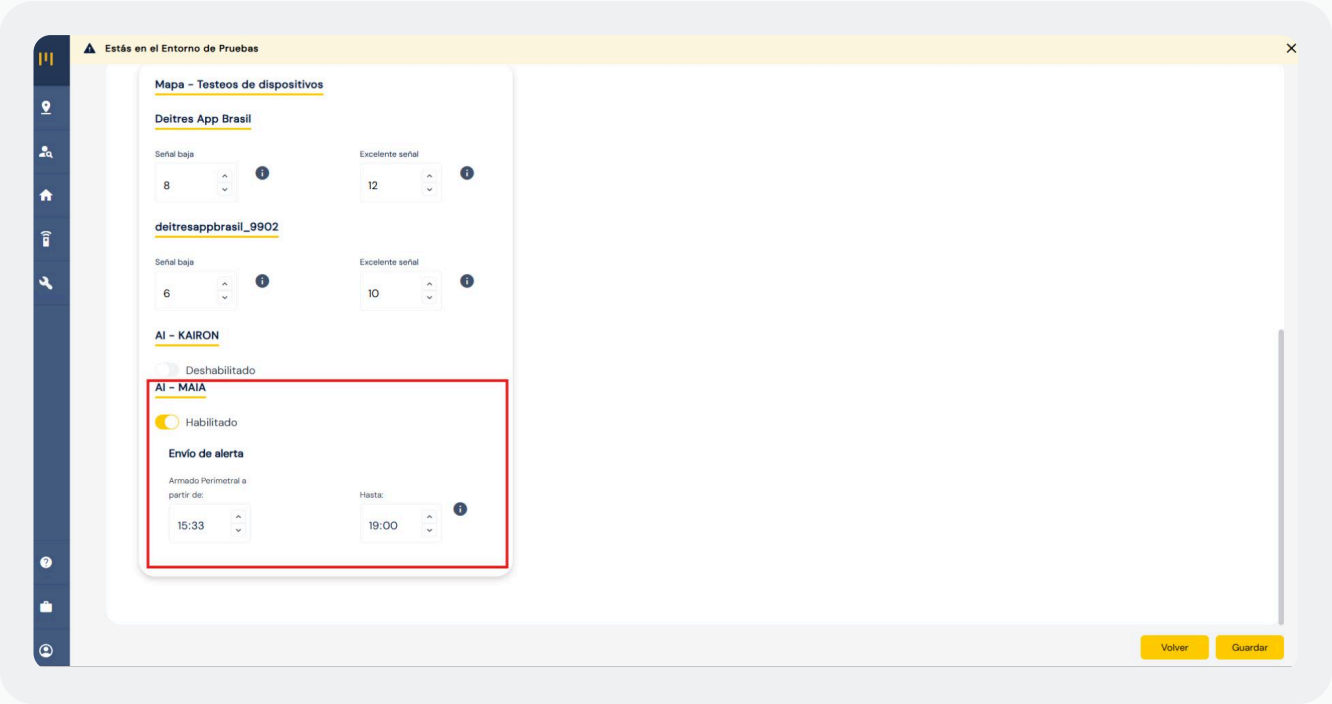
Important!

- The system will not allow the configuration to be saved if this field is empty.
- This perimeter arming configuration will apply globally to all users linked to the company; it is not an individual setting.

General Rules

- For perimeter arming, MAIA will always send the suggestion to the last person who approached the panel perimeter.

- In the case of **perimeter activation**, MAIA will always send the suggestion to the **last person who approached the panel's perimeter.**
- The system will only suggest perimeter activation again the **following day,** thereby avoiding repetitive notifications, since human interaction has already taken place.



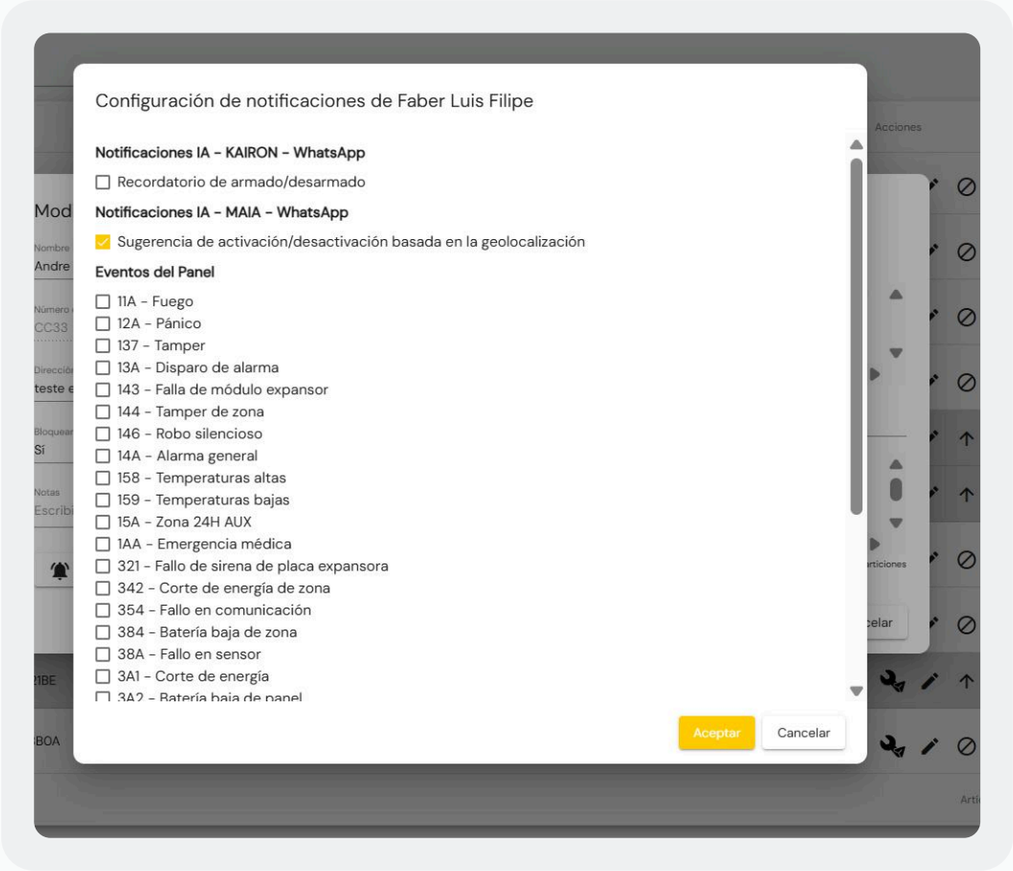
Step 2: Configuration by Partition

1. Go to the Partitions tab.
2. Select a partition and click Edit.
3. In the User Notifications section, you will see the new area:

   "AI Notifications - MAIA - WhatsApp".
4. Enable the "Arming/disarming suggestion" switch.

Important!

- By default, this option is enabled for all users. It is important to note that this is a **user-level setting, not a partition-level one.**



2. End-user configuration (App Mobile)

For MAIA to work, the user must authorize tracking on their device. The following step-by-step instructions show how customers can complete the configuration.

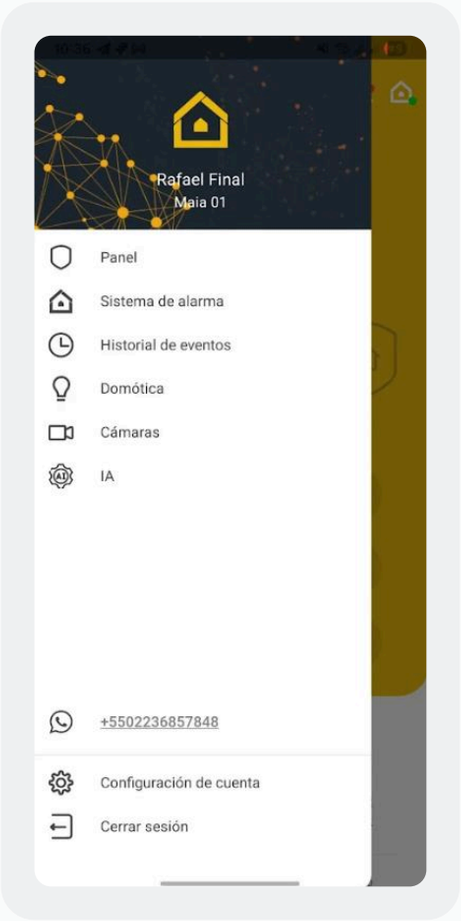
Prerequisites for MAIA assistance

To ensure MAIA alerts and suggestions work correctly, the app will indicate three essential requirements. You will know they are configured correctly when **a green check icon appears** next to each one:

1. Linked WhatsApp number.
2. Background geolocation access (“Always”).
3. Physical supervision enabled..

Activation steps

1. Open the **City Alarme** application and go to the **“AI”** (Artificial Intelligence) screen.



2. Locate the **MAIA** section. There you will see a switch that is **OFF by default.**

3. Tap the switch to change it to ON.

Automatic validation flow: When you try to activate the switch, the system will guide you step by step if any configuration is missing.

- **Step 1:** WhatsApp linking. If your number has not yet been registered, the app will pause MAIA activation and redirect you to the WhatsApp linking screen. Once the number has been successfully registered, the flow will continue automatically.

- **Step 2:** Location and supervision permissions. If you have not granted the required permissions, a phone pop-up will appear requesting access to your location.

What happens if I deny a permission?

If you choose not to grant geolocation permissions or cancel WhatsApp linking, the switch will automatically return to **OFF** and you will see an alert explaining that MAIA cannot work without these accesses.

Done! Once the steps are completed and all indicators are green, the switch will remain ON and MAIA will be ready to interact with you.

Important!

- The customer must keep their WhatsApp number updated in their WebApp profile to receive alerts.

3. General Rules

1. Schedule priority (Kairon)

MAIA is intelligent and respects previous configurations:

- If Kairon Schedule Control is active, MAIA will remain paused and will not send suggestions to avoid duplication.
  - Without Schedule Control, MAIA takes over arming suggestions.

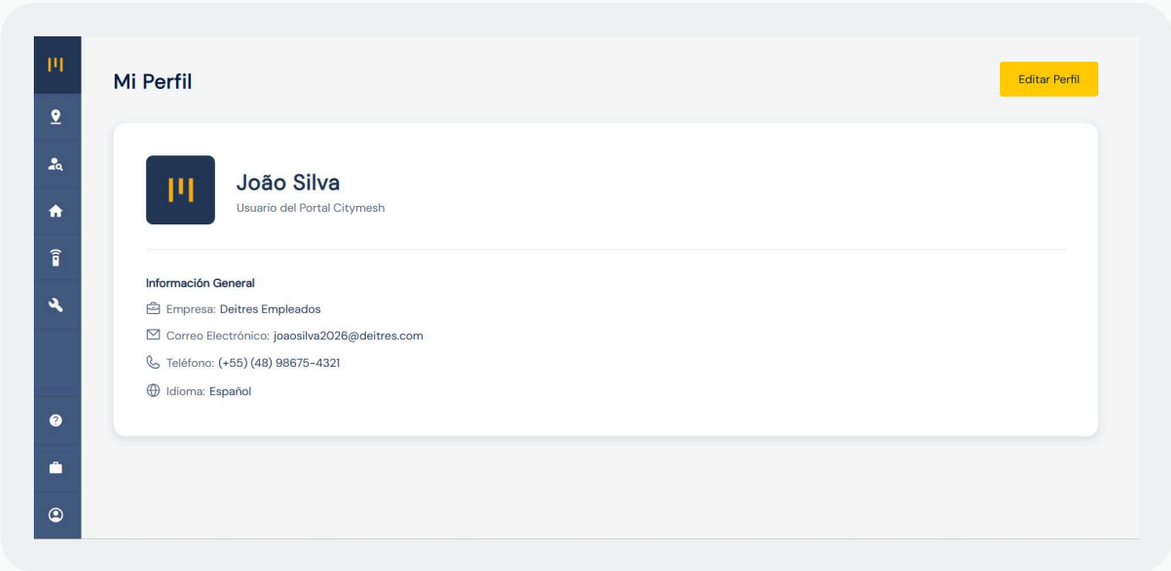
2. Proximity radii (Geofencing)

The system uses a default comparison radius of 200 meters from the panel location.

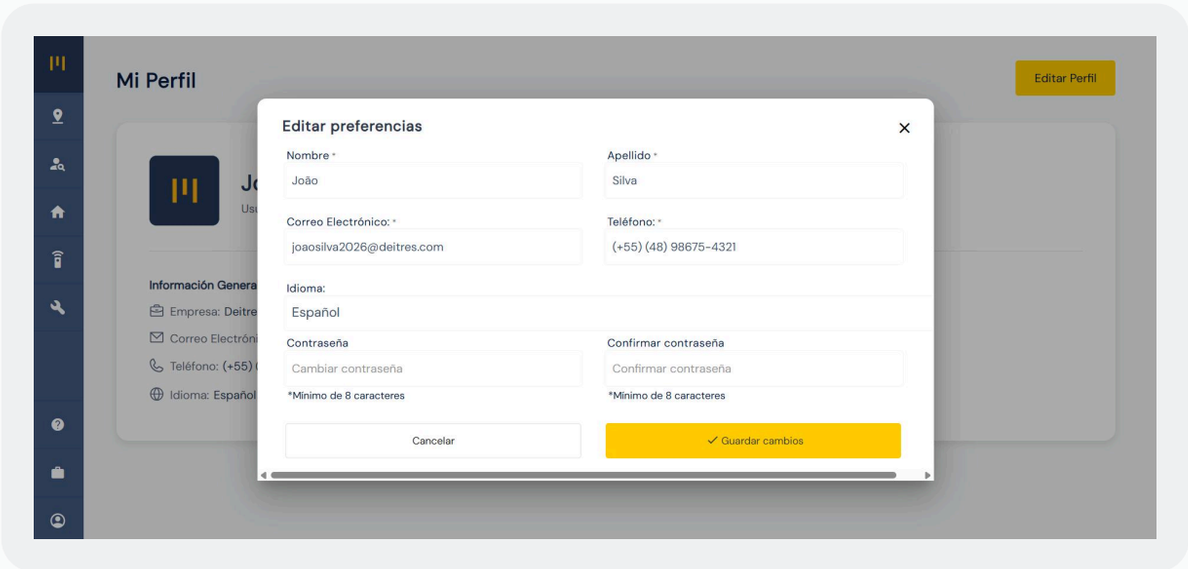
- **Arming suggestion (leaving):** When the system detects that the user has left the perimeter, the location is updated every 15 minutes to confirm the departure.
- **Perimeter Arming suggestion:** When users who have geolocation enabled in the application and have their phone number (WhatsApp) filled in are at the **SAME** coordinates as the panel installed at the property, and the panel is **DISARMED**, if the time is within the sending schedule configured in the company management screen, one of them (the last person to arrive at the perimeter) will receive a perimeter arming suggestion through WhatsApp and can perform the action directly through WhatsApp.

3. A WhatsApp message is sent to the user closest to the panel.
4. If that user does not respond within 5 minutes, the alert moves to the second-closest user.
5. This process continues until someone responds or the users are exhausted.
6. Once a user makes a decision (Arm/Ignore), the system notifies the other users involved about the action taken.

When you access the side menu, in the lower corner you will find an icon representing your user, with your name registered on the platform. When you click it, two options appear: My Profile and Log out. Select the first option and you will be redirected to a page containing personal information such as name, email, language, phone, and more.



This page provides an “Edit profile” button that allows you to edit your personal information. You can also update your platform access password. After completing the process, do not forget to save the change.



Seguimos Mejorando 🚀

Si tienes alguna duda, **estamos a tu disposición.**

Nuestro objetivo es **centralizar todas las acciones**, que actualmente están distribuidas en varios entornos.

✨ **Muy pronto habrá nuevas funcionalidades. ¡Estate atento!**

2026 © Deitres Group – All Rights Reserved

San Luis 4580
B7602 Mar del Plata,
Buenos Aires, Argentina

Powered by
DEITRES