

Español

intelbras

Manual del usuario

MIP 1000 IP



MIP 1000 IP (Módulo Inteligente de Portería IP)

Controlador, registrador y configurador de accesos

Felicitaciones, acaba de comprar un producto con la calidad y seguridad de Intelbras.

El MIP 1000 IP fue desarrollado para ser el administrador de acceso a condominios, realizando el registro, gestión de personas y vehículos en los más variados modelos de condominios. Su función es proporcionar una interfaz simple y funcional que le permita controlar el tiempo de entrada o salida de cada persona o vehículo, facilitar la apertura de puertas/portones, verificar si las puertas están abiertas a través de sensores e incluso definir qué usuarios tendrán acceso a cada parte del condominio.

Su pantalla muestra, por ejemplo, eventos de acceso y notificaciones de problemas del dispositivo. El equipo dispone de otros servicios como alerta de portero, pánico, búsqueda simplificada de eventos, etc.

Estas funciones se demostrarán durante la lectura de este manual.



ATENCIÓN: Este producto viene con una contraseña predeterminada de fábrica. Para tu seguridad es imprescindible que la cambies nada más instalar el producto y pregunte a tu técnico sobre las contraseñas configuradas, qué usuarios tienen acceso y los métodos de recuperación.

La contraseña del producto debe tener un mínimo de 8 y un máximo de 20 caracteres. Intente registrar una contraseña segura que contenga al menos una letra mayúscula, una letra minúscula, un número y un carácter especial.



Este es un producto homologado por Anatel, el número de homologación se encuentra en la etiqueta del producto, para consultas acceda al sitio web: <https://www.gov.br/anatel/pt-br>.

Cuidados y seguridad

- » No lo instale en lugares húmedos, cerca de fuentes de calor o vibraciones.
- » No instale cerca de televisores o equipos que funcionen con radiofrecuencia.
- » Evite instalar en lugares donde haya luz solar directa.
- » No instale en lugares donde se requiera el movimiento constante del MIP, ya que esto evita problemas con la ruptura del cableado conectado al MIP.
- » LGPD - Ley General de Protección de Datos Personales: este producto procesa datos personales, sin embargo, Intelbras no tiene acceso a los datos de este producto.

Índice

1. Especificaciones técnicas	6
2. Características	6
3. Producto	7
3.1. Módulo inteligente de portería MIP 1000 IP	8
4. Instalación	10
4.1. Bus de comunicación	10
4.2. Ejemplos de instalación	11
Bus de dos cables y blindaje conectados a GND, utilizando topología en cascada	11
Bus de dos cables con topología en estrella	12
4.3. Procedimiento de instalación	13
4.4. Conexiones del MIP IP	14
Salidas de accionamiento SALIDA_1 y SALIDA_2	14
Entradas de sensores SEN_1 e SEN_2	14
Teclado USB	14
Cable RJ45	14
4.5. Productos integrados con MIP 1000 IP	15
5. Operación/Programación	15
5.1. Descripción de iconos	15
5.2. Inicializando el sistema	16
5.3. Pantallas de eventos	17
5.4. Teclas de acceso rápido	20
5.5. Acceso al MIP 1000 IP	25
5.6. Registro	26
Usuario	26
Registro de residentes	26
Registro de visitantes y proveedores de servicios	35
Dispositivo	36
Incluir dispositivo	36
Resincronizar dispositivo	45
Editar dispositivo	46
Consultar dispositivo	48
Eliminar dispositivo	49
Llaveros	50
Incluir llavero	50
Editar llavero	54
Consultar llavero	54
Eliminar llavero	54

Control	56
Incluir control	56
Editar control	59
Consultar control	59
Eliminar control	59
Digital	61
Incluir huella digital	61
Editar huella digital	65
Consultar huella digital	65
Eliminar huella digital	65
Caras	67
Incluir Caras	67
Editar cara	70
Consultar cara	70
Eliminar cara	70
5.7. Eventos	72
Consultar Eventos	72
5.8. Notificaciones	75
5.9. Configuración de tecla	76
Configurar tecla	77
Volver/Eliminar tecla	78
5.10. Configuración de sistema	78
Fecha y Hora	78
Condominio	80
Cambia la contraseña	81
Buscar usuario	82
Función Pánico	87
Mensaje de descanso	90
Alerta sonora	91
Configurar etiquetas	92
Configurar registro	93
Configuración de temporizaciones	94
Configuración de sobreponer eventos	94
Configuración de red IP	96
Servicios	98
Feriados	101
Configuración de backup y restauración	103
Reset general	105
Salir	106
6. Excepciones para dispositivos biométricos y faciales	106
7. Actualización de firmware	107
Póliza de garantía	108
Términos de garantía	109

1. Especificaciones técnicas

Alimentación	12 Vdc / 1 A, acompanha fonte externa
USB	Tipo A: para conexão de teclado USB ou pendrive
Activar salidas	Duas saídas de relés (contato seco) NA/NF, para cargas de até 24 Vdc / 1 A. Verificar o funcionamento no item 2. <i>Características</i>
Entradas de sensores	Duas entradas de sensores (contato seco), podem ser usadas como sensores de porta aberta, etc.
Bus serie RS485	SERIAL_1: utilizado para cadastros dos dispositivos no sistema SERIAL_2: utilizado para cadastro e comunicação do sistema, permite até 24 dispositivos no barramento 485
La red	10BASE-T Protocolo IPV4
Distancia máxima desde dispositivos RS485	Até 1.000 metros com cabos de par trançados de boa qualidade ou barramento com impedância máxima de 250 ohms
Pantalla LCD	64 × 128 pontos azul com backlight
Peso	335,0 g
Dimensiones (Al. × An. × Pr.)	109 × 132 × 168 mm
Consumo en reposo	1,1 W
Lector RFID	Cartões Mifare (13,56 Mhz)
Lector de control remoto	Controle XTR 1000 (433 Mhz)
Condiciones ambientales	Temperatura: -10 °C a 60 °C Umidade relativa do ar: 10 a 90% (sem condensação)
Garantizar	1 ano

2. Características

- » Registro de la información de acceso del residente en los dispositivos para que funcionen de forma autónoma.
- » Registro de visitantes y prestadores de servicios, con restricciones de acceso por días de la semana y horarios. Para acceder a estos usuarios, el MIP debe estar en el bus.
- » Registro y generación (a través del SGA 1000 IP por ejemplo) de reportes de acceso.
- » Gestión individual de mandos XTR 1000, contraseñas de usuario, llaves de proximidad RFID (Mifare), huellas digitales y caras.
- » Puerto de comunicación USB (estándar A) para teclado externo (no incluido) facilitando el uso del sistema, especialmente en registros.
- » Puerto Ethernet (red) para comunicación con el software SGA 1000 IP y softwares integradores.
- » Respaldo de la información del sistema, en la micro-SD del MIP, todos los días a las 03:04 horas. El MIP almacena el respaldo individual e identificado de los últimos treinta días, pudiendo recuperarlo a partir de un día específico.
- » Backup de configuraciones del sistema, datos de registro y logs de acceso a través del software.
- » Módulo de conserjería con identificación del usuario, cuando activa su elemento de acceso (control, llavero, contraseña, huellas digitales o caras).
- » Registro de foto de usuario (foto disponible solo en el software SGA 1000 IP).
- » Almacena hasta treinta mil eventos con fecha y hora.
- » Permite el registro de hasta 4.000 llaveros, 4.000 controles XTR 1000, 4.000 huellas digitales, 4.000 caras y 4.000 usuarios (con una contraseña por usuario), totalizando 20.000 elementos de acceso.
- » Indica el estado de la batería de los controles remotos al portero.
- » Software de registro y gestión de información de acceso (SGA 1000 IP).
- » Dos salidas de relé (contacto seco) estándar NA (normalmente abierto) para cargas de hasta 24 Vdc / 1 A. Se pueden cambiar para trabajar como NF (normalmente cerrado), solo configure los puentes JP3 y JP4 en la placa base del MIP.
- » Dos entradas de sensor (contacto seco), que se pueden utilizar como sensores de puerta abierta y enclavamiento.

3. Producto

El Módulo Inteligente de Portería 1000 IP (MIP 1000 IP) será el punto de interacción con el portero (guardián), ya que siempre estará al alcance para liberación de acceso, activación de salidas de dispositivos, programación/bloqueo de nuevos usuarios y visualización de eventos de entrada/salida. El portero interactuará con este equipo a través de una pantalla LCD y un teclado.

Considerando al MIP como el administrador del sistema, todos los datos de los usuarios y dispositivos serán previamente registrados en él a través de su interfaz o mediante el software instalado en el equipo (SGA 1000 IP por ejemplo). Durante la operación del sistema, los eventos serán registrados (almacenados) y estarán disponibles para su consulta en cualquier momento a través del producto o software.

El producto tiene un puerto USB (tipo A) para la conexión a un teclado USB (estándar ABNT) o una unidad flash para respaldo, un puerto Ethernet RJ 45 para la comunicación con una computadora. Tiene dos salidas para activación de cargas (por ejemplo, cerraduras o portones), dos entradas de sensor (por ejemplo, sensor de puerta abierta), dos buses seriales para comunicación con los dispositivos del sistema y una entrada de alimentación externa.

Este producto tiene la capacidad de configurar sus dispositivos para que activen sus salidas de bloqueo independientemente del MIP 1000 IP. De esta forma, los dispositivos tienen la capacidad de identificarse y tomar la decisión por sí mismos de realizar la apertura. Si el dispositivo V2 está conectado al MIP 1000 IP, a través de su bus, el evento de apertura será enviado inmediatamente al MIP para que registre este evento en su base de datos local. Sin embargo, si el dispositivo no puede comunicarse con el MIP, abrirá el activador y almacenará el evento dentro de él hasta que se restablezca la comunicación con el MIP.

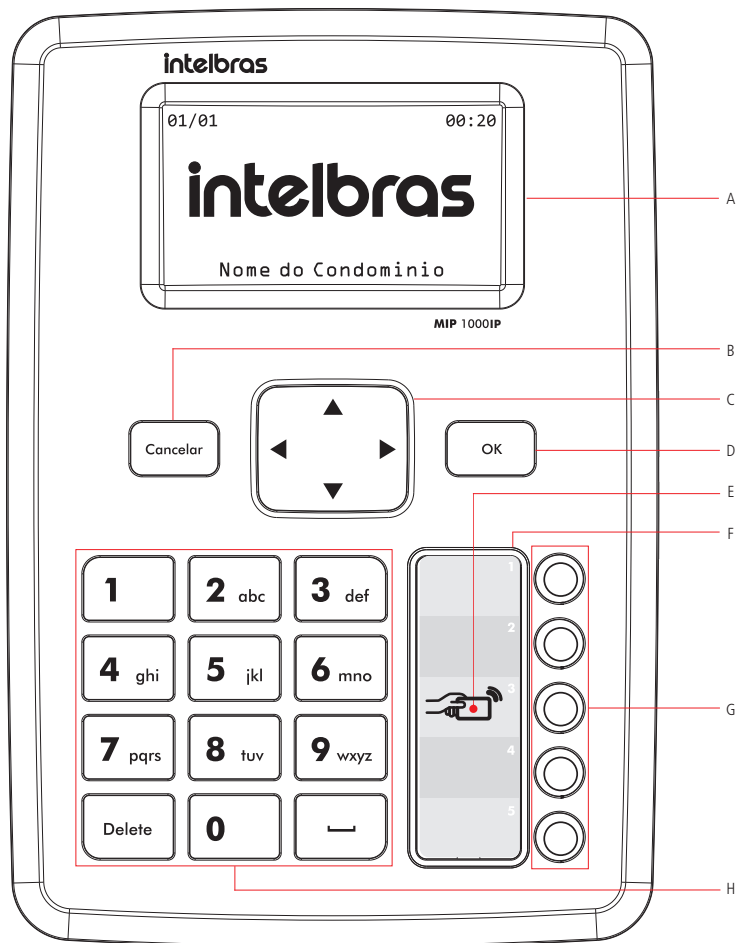
Posibilidad de registro de visitantes y prestadores de servicios, con restricciones de fecha y hora. Para esta función, el dispositivo debe estar actualizado con la versión compatible (consulte el changelog en el sitio web de Intelbras) y conectado al bus RS485 del MIP 1000 IP, ya que el dispositivo no almacena los recursos de los visitantes registrados y los proveedores de servicios.

El MIP 1000 IP soporta la comunicación con los dispositivos Bio Inox Plus SS 311 MF, CT 500 1P y Lector Facial (SS 3530 MF W), a través del bus RS485, siendo posible gestionarlos a través del MIP 1000 IP.

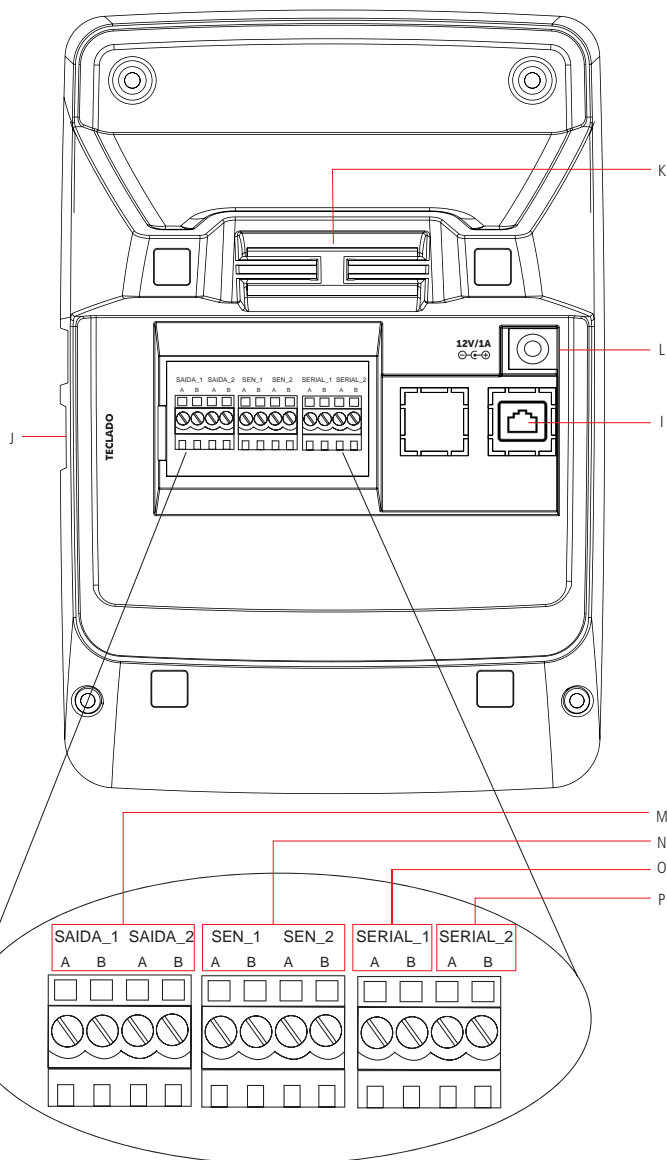


Importante: realizar backup periódico de la tarjeta micro interna del MIP 1000 IP.

3.1. Módulo inteligente de portería MIP 1000 IP



- A. Pantalla LCD
- B. Tecla Cancelar
- C. Teclas de navegación
- D. Tecla de confirmación: Ok
- E. Región de registros de llaveros RFID (Mifare)
- F. Etiqueta de identificación de teclas de accionamiento
- G. Teclas de accionamiento (programables)
- H. Teclado de 12 teclas para ingreso de datos



- I. Conector RJ45 (red)
- J. USB para conexión con el teclado (estándar ABNT)
- K. Paso de cables
- L. Entrada Fuente de alimentación (12 Vdc / 1 A)
- M. Salidas de activación de contacto seco, siendo la SALIDA_1 y la SALIDA_2. Ambas son temporizadas
- N. Entradas de sensores
- O. SERIAL_1: bus RS485 para el registro de dispositivos en el sistema
- P. SERIAL_2: utilizado para registro y comunicación del sistema, permite hasta 24 dispositivos en el bus RS485

4. Instalación

4.1. Bus de comunicación

Es muy importante leer este tema para entender claramente la forma correcta de instalar el sistema de control de acceso del condominio, incluyendo el módulo inteligente de portería (MIP 1000 IP) y los demás dispositivos del sistema que deben instalarse correctamente en el bus.

El bus es la conexión física entre el MIP 1000 IP y todos los demás dispositivos a través de cables. Estos cables comunicarán los dispositivos para registrar los accesos. Para tener un bus con buena calidad, debemos seguir las siguientes recomendaciones:

1. Cada bus debe tener una sola IP MIP 1000, la cual se utiliza en las configuraciones de usuarios, elementos de acceso (controles, llaveros, contraseñas, huellas digitales y cara) y dispositivos, además de registrar eventos y notificar notificaciones del sistema;

Importante: después de las configuraciones anteriores, si el MIP 1000 IP se desconecta del bus, los dispositivos seguirán dando acceso a los residentes y almacenarán internamente los eventos y, al devolver el MIP al bus, los dispositivos sincronizarán con él los eventos registrados cuando estaban en modo *Time Out* (consulte el manual del dispositivo para conocer la capacidad de almacenamiento de eventos en modo *Stand Alone*).

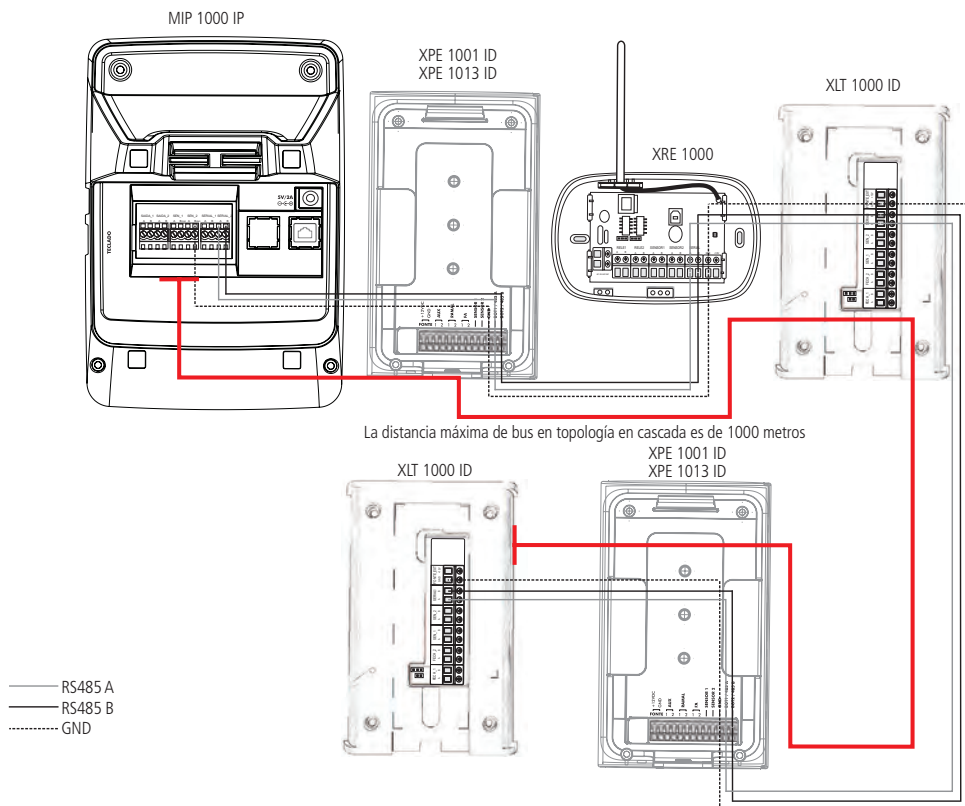
2. Cada bus podrá tener de 1 hasta 24 dispositivos (XRE 1000, XLT 1000 ID, XPE 1013 ID, XPE 1001 ID, etc.) conectados en el bus SERIAL_2 del MIP 1000 IP, siendo el bus SERIAL_1 utilizado solo al momento de registro de los dispositivos;
3. El bus tiene dos cables. Para ambientes con interferencias, se recomienda cable blindado, con el blindaje conectado al GND del MIP IP y de los dispositivos;
4. En el bus se debe vincular la referencia SERIAL_A del MIP IP a la referencia SERIAL_A de todos los dispositivos, lo mismo se debe hacer con la referencia SERIAL_B;
5. Todos los dispositivos deben estar registrados en el MIP 1000 IP;
6. Las conexiones deben ser preferentemente en serie (topología en cascada), siempre de un dispositivo a otro;
7. La distancia máxima de cable entre el MIP 1000 IP y el último dispositivo debe ser inferior a 1000 metros (ver ejemplos de instalación) y la impedancia total del bus no debe exceder los 250 ohmios;
8. Es preferible utilizar cables de par trenzado;
 - » Cable de par trenzado balanceado y blindado.
 - » Calibre de 22 AWG a 24 AWG.
 - » Resistencia del conductor de 14,7 a 17,5 ohm / 304,8 m.
 - » Resistencia de blindaje de 2,8 a 2,9 ohm / 304,8 m.
 - » Capacidad diferencial de 11 pF / 30,48 cm.
 - » Longitud de la trenza de 6,35 cm.
 - » Las conexiones (empalmes) de los dispositivos con el bus RS485 deben realizarse con soldadura de buena calidad.



Importante: se recomienda utilizar un nobreak y/o una fuente nobreak, como la fuente EB 1201, para evitar que los cortes de energía comprometan el sistema de archivos.

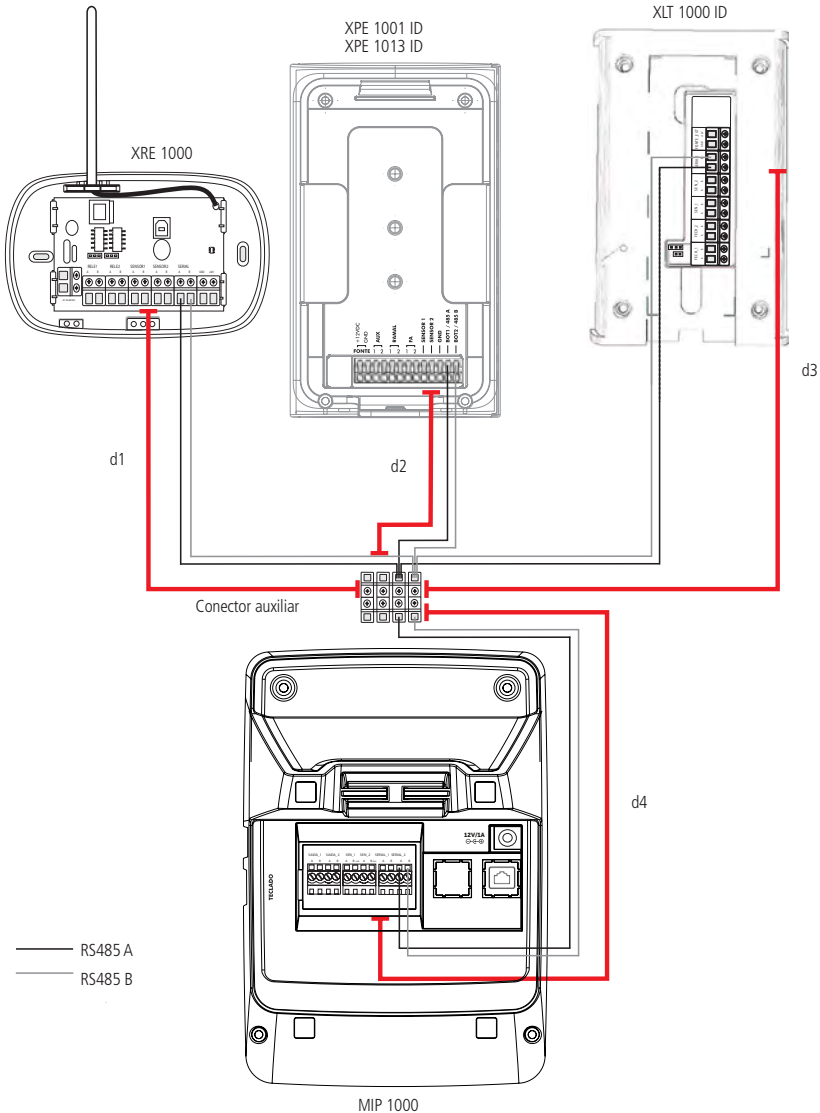
4.2. Ejemplos de instalación

Bus de cables y blindaje conectados a GND, utilizando topología en cascada



Obs.: utilizando la topología en cascada, este dispositivo puede ser conectado a una distancia de hasta 1.000 metros del MIP IP o en cableado que no supere los 250 ohmios, siempre que se utilicen cables de buena calidad, conforme informado en la recomendación 9 del ítem 4.1 Bus de comunicación.

Bus de dos cables con topología en estrella

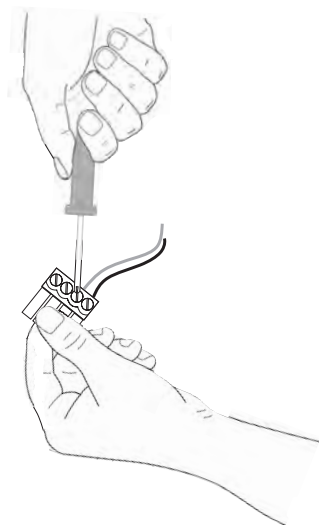


La distancia máxima de bus en topología en estrella es $(d_1+d_2+d_3+d_4) = 1000$ metros

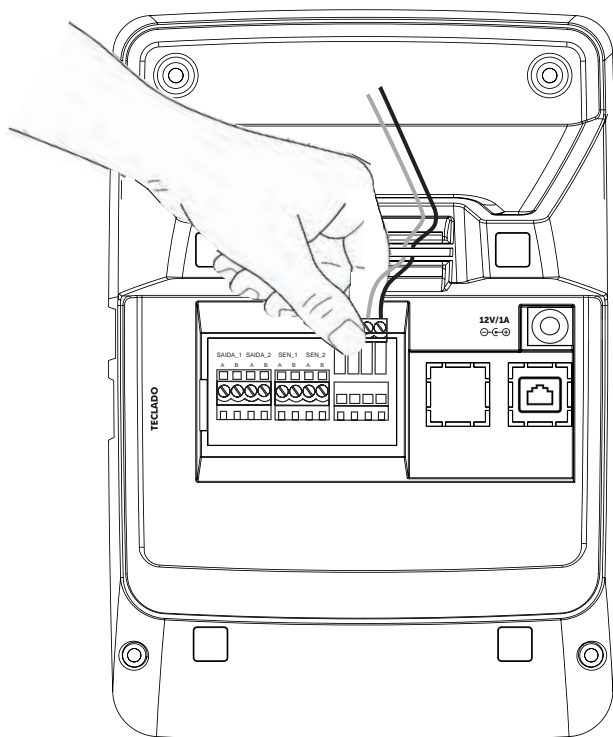
Obs.: se recomienda utilizar un conector auxiliar (no incluido) para unir los cables, evitando que todos los cables lleguen al conector MIP IP. Utilizando la topología en estrella, la suma de las distancias de los dispositivos al MIP IP no puede exceder los 1.000 metros o en cableado que no supere los 250 ohmios, esta distancia se alcanza siempre que se utilicen cables de buena calidad, según se informa en la recomendación 9 de ítem 4.1 Bus de comunicación.

4.3. Procedimiento de instalación

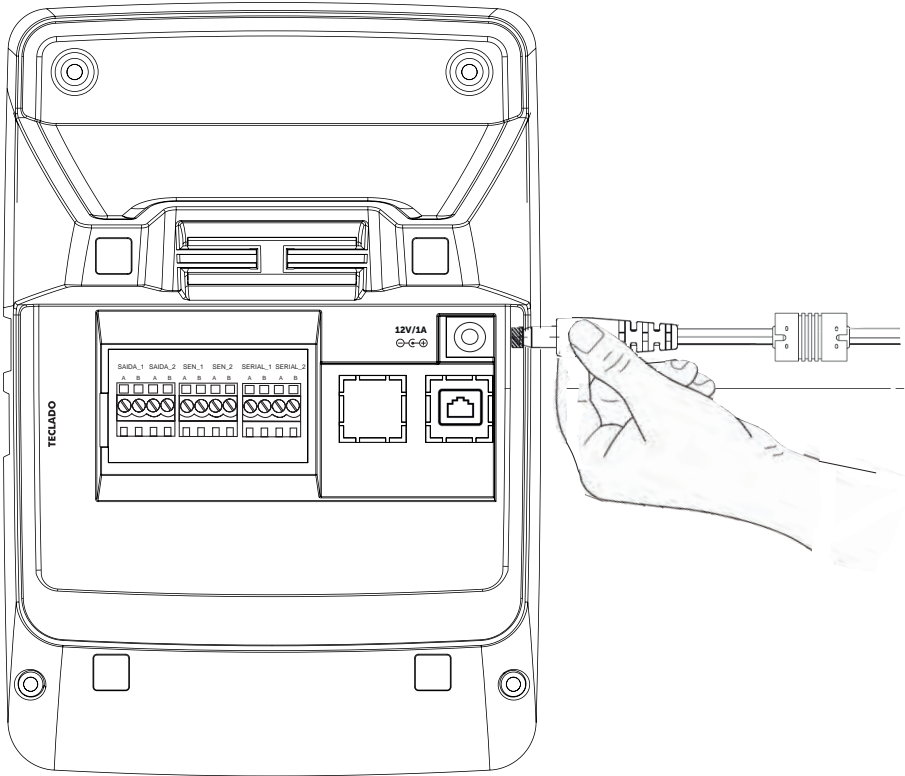
1. Con ayuda de un destornillador, atornillar los cables que se utilizarán en los conectores hembra del MIP IP;



2. Después de atornillar los cables, encajar el conector hembra en el conector macho del MIP IP;



3. Enchufe el conector jack de la fuente de alimentación externa (12 Vdc / 1 A) en la ubicación indicada en la parte posterior del IP MIP.



4.4. Conexiones del MIP IP

Salidas de accionamiento SALIDA_1 y SALIDA_2

Estas salidas se pueden programar para:

- » Activación de cargas hasta 24 Vdc / 1 A como cerraduras, placas de comando de motores para portones, etc.
- » Activación de sirenas en caso de pánico.
- » Control de esclusa/jaula cuando su función de enclavamiento está habilitada.

Entradas de sensores SEN_1 e SEN_2

Estas entradas se pueden utilizar como:

- » Sensores de estado de puerta abierta, alertando con pitidos y mensajes en la pantalla MIP IP.
- » Sensores en modo enclavamiento.

Teclado USB

El teclado se utiliza para facilitar el registro y configuración en el MIP IP. A través de él es posible navegar en los menús y realizar cualquier programación del dispositivo o sistema, como consultas de eventos, etc.

Cable RJ45

Con el cable RJ45 conectado al MIP IP y a un computador (notebook o desktop) o router, permite que un ordenador que tenga el software de configuración/registro (por ejemplo SGA 1000 IP) instalado y conectado a la misma red, pueda realizar todas las configuraciones del sistema y eventos de consulta, incluida la generación de informes detallados de los accesos registrados por los dispositivos.

4.5. Productos integrados con MIP 1000 IP

El MIP 1000 IP admite la comunicación con los dispositivos inferiores a través del bus RS485, por lo que es posible gestionarlos a través del MIP 1000 IP.

- » XRE 1000 PLUS
- » XLT 1000 ID
- » XPE 10xx ID
- » Bio Inox Plus SS 311 MF
- » CT 500 1P
- » SS 3530 MF W
- » SS 3540 MF FACE EX
- » Remote
- » SS 3430 MF BIO
- » SS3420 MF BIO

5. Operación/Programación

El MIP 1000 IP es un equipo para uso del profesional de la conserjería, en su modo de trabajo normal del día a día. También habrá modos de acceso destinados a administradores e instaladores del equipo con niveles de permisos, permitiendo acciones/configuraciones restringidas.

A continuación se describen las posibilidades de uso del MIP IP a realizar por el portero/instalador:

- » Supervise todos los eventos de entrada y salida a través de la pantalla.
- » Liberar el acceso a los portones de peatones y automóviles.
- » Incluya, edite y elimine llaveros RFID (Mifare), contraseñas de usuarios, huellas digitales, caras y controles remotos XTR 1000 para residentes, así como usuarios y dispositivos.
- » Configure teclas dedicadas para activar sus salidas o las salidas de cualquier dispositivo configurado.
- » Ajuste la hora y la fecha.
- » Configurar la función Despierta portero.
- » Configurar la función de pánico.
- » Editar etiquetas de identificación de los lectores registrados en el sistema.
- » Configuración del tiempo en el que se mostrarán los eventos en la pantalla.
- » Configurar el mensaje de descanso en la pantalla.
- » Liberar proveedor de servicios y acceso de visitantes.

5.1. Descripción de iconos

Existen situaciones en las que el MIP señalará algún estado en su pantalla, las cuales se identifican a través de los siguientes iconos agrupados por notificaciones:



Time Out (dispositivo desconectado del bus por más de treinta segundos) y/o activación de sensores (si están activos) y/o necesidad de sincronizar el dispositivo.



Teclado conectado al MIP 1000 IP para configuración y registro.



Cable RJ45 conectado al MIP 1000 IP.



Notificación de control remoto de batería baja (se muestra cuando el control remoto de un usuario tiene poca batería y se activa).



Pen Drive conectado para actualización de firmware y copia de seguridad.

5.2. Inicializando el sistema

Al encender el MIP 1000 IP, luego de mostrar la versión y cargar los datos contenidos internamente, la pantalla mostrará la pantalla de descanso, la cual contiene la información de fecha, hora y nombre del condominio, como se muestra en las siguientes imágenes.



Pantalla de inicio con indicación de versión



Pantalla de inicialización



Pantalla de descanso

5.3. Pantallas de eventos

Durante el funcionamiento normal, cuando ocurre un evento, el MIP IP mostrará la pantalla del evento, informando el número de departamento, nombre y tipo de usuario, dispositivo donde ocurrió el evento, la salida que se activó y el tipo de acceso (Acceso por contraseña, vía departamento, vía llavero, vía control, vía digital y vía cara). También informará los datos de matrícula, modelo y color del vehículo si estos datos están cumplimentados.

01/01/15	00:00:00
Usuario	
Departamento Bloq Tipo do usuario	
Dispositivo - Salida	
Tipo de acceso	
Acceso liberado.	

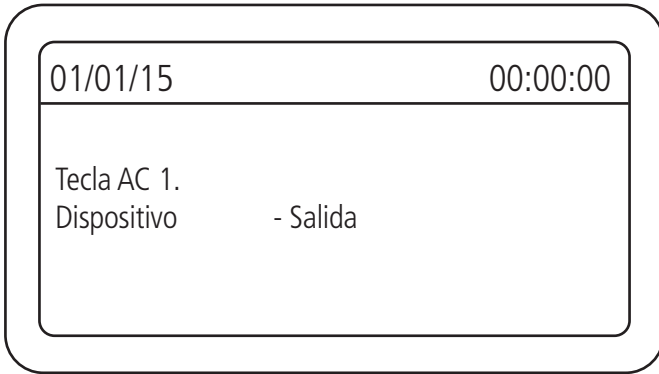
Eventos de acceso en los dispositivos

01/01/15	00:00:00
Usuario	
Departamento Bloq Tipo do usuario	
Dispositivo - Salida	
Modelo de marca	
Placa - Con	
Acceso liberado.	

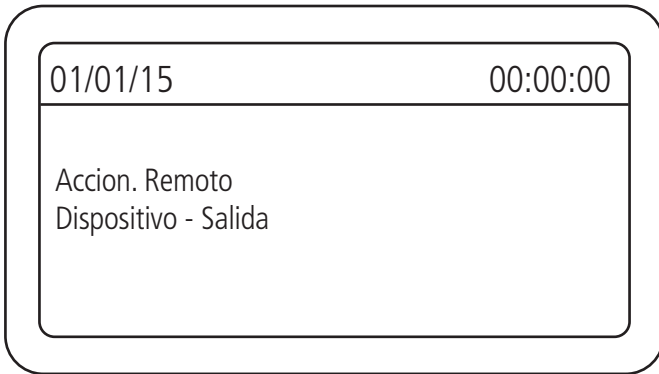
Eventos de acceso con la información del vehículo

01/01/15	00:00:00
Usuario	
Apto:	
Nombre del dispositivo activado	
Acceso por Apto!	

Eventos de acceso a apartamentos en dispositivos XPE



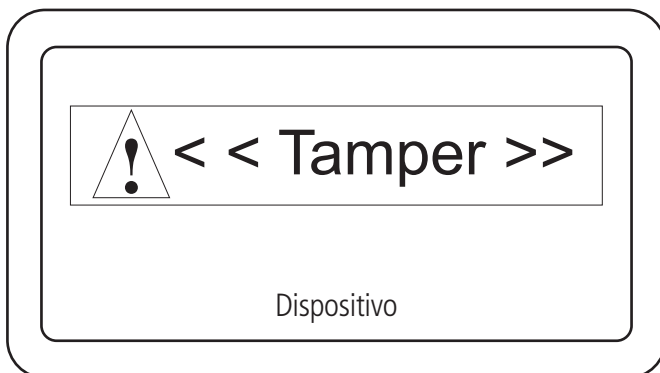
Evento de acceso vía teclas de accionamiento programables del MIP



Evento de acceso remoto en el dispositivo, mediante teclas del SGA 1000 IP o software integrador



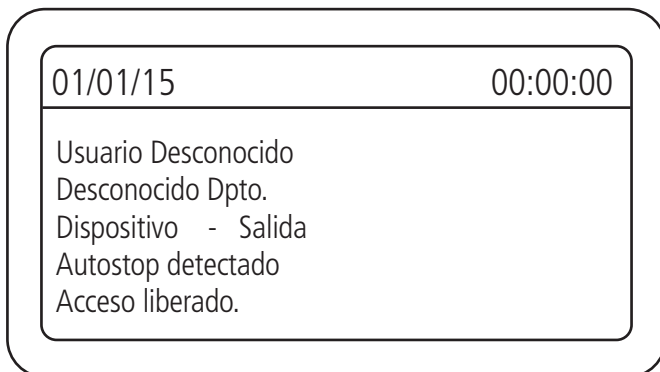
Evento de pánico del sistema que informa al usuario quién activó y en qué dispositivo



Evento de tamper del sistema que indica qué dispositivo fue violado (consulte el manual del dispositivo si tiene esta funcionalidad)

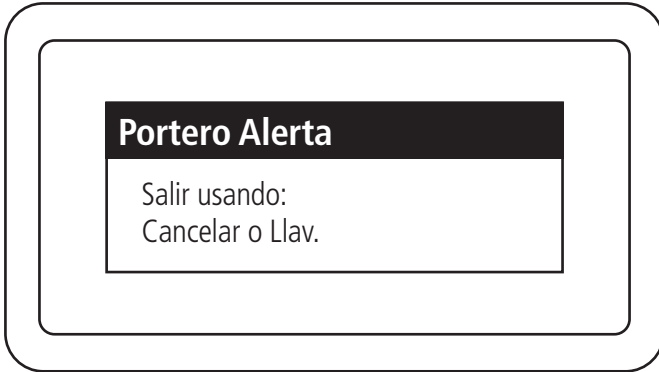


Evento de forzamiento que le dice qué puerta fue violada



Evento señalización a carro en el dispositivo XRE 1000


» **Función de Carro:** cuando la función está habilitada para el XRE, genera un evento informando que un auto pasó por la puerta sin registro en el MIP. El evento se señaliza a través del sensor instalado en el portón.

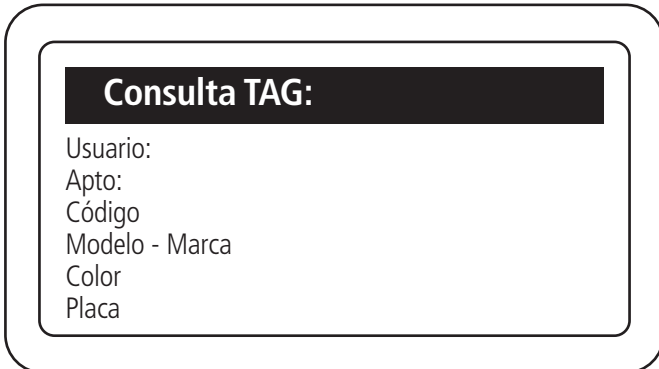
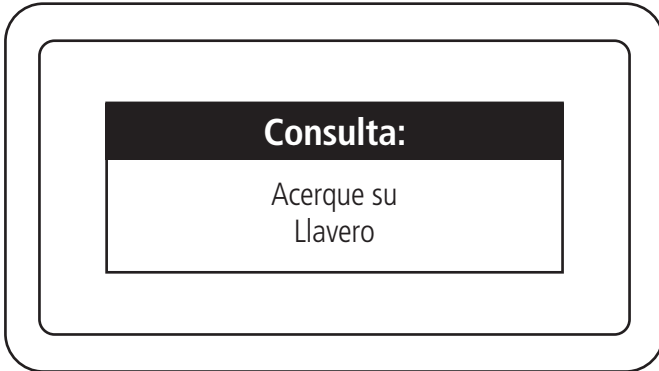



Evento de alerta sonoro para el portero (vigilante) en un rango de horario para mantenerlo atento.

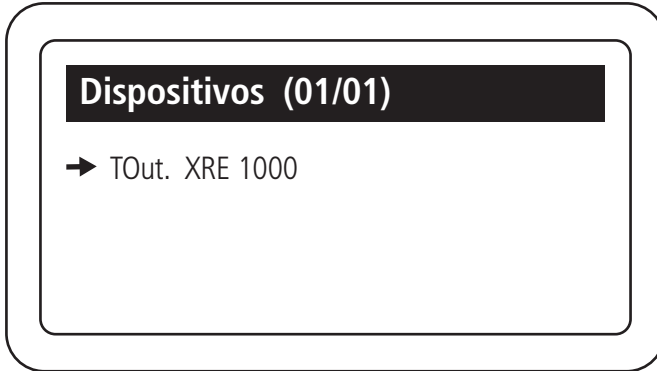
5.4. Teclas de acceso rápido

Con el MIP en la pantalla de descanso o inicial es posible consultar las notificaciones del sistema, consultar llaveros RFID (Mifare) y controles XTR 1000, verificar el estado de la red, realizar la prueba de comunicación en el bus RS485 y verificar la versión del firmware del MIP IP.

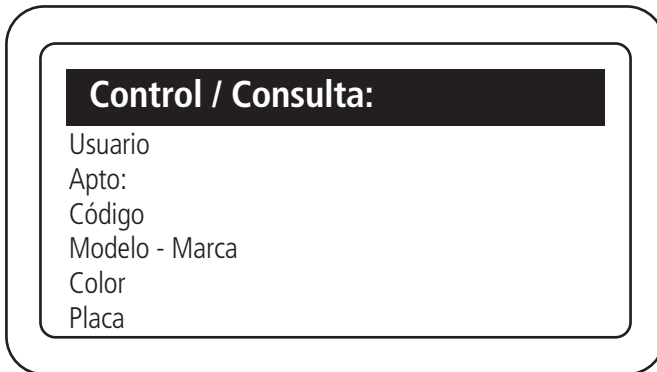
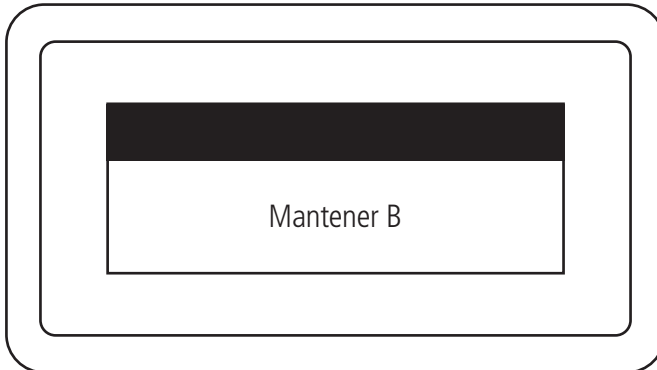
1. Para verificar si un llavero RFID (Mifare) ya está registrado en el sistema, con la MIP IP en la pantalla de inicio o de inicio, presione la tecla 1 y acérquese al llavero RFID en el campo  para su reconocimiento;



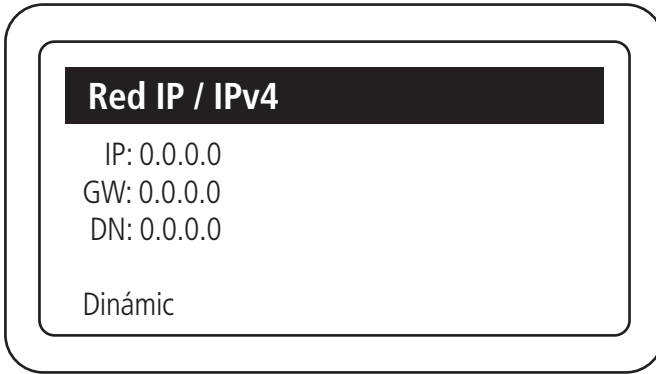
2. Cuando aparece el icono  en la pantalla de descanso o inicial del MIP IP, presione la tecla 2 para ver la notificación del sistema;



3. Para comprobar si un control XTR 1000 ya está dado de alta en el sistema, con el MIP IP en pantalla de reposo o inicial, pulsar la tecla 3 y mantener pulsada la tecla B del control hasta que se reconozca.

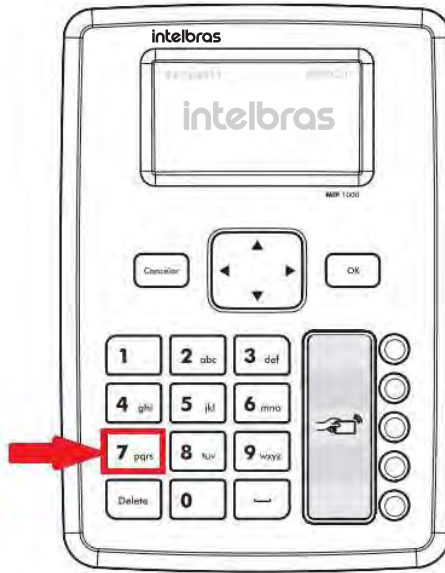


4. Para consultar la información de la red IPv4, con la MIP IP en la pantalla de descanso o inicial, pulsar la tecla 4.

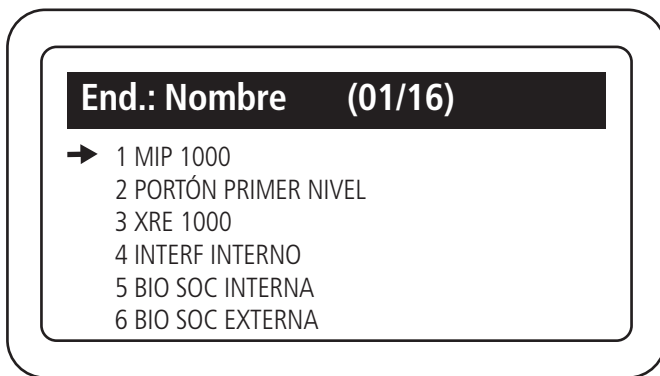


5. Para realizar un análisis de la comunicación entre el MIP IP y los dispositivos en el bus RS485, es necesario seguir los siguientes pasos:

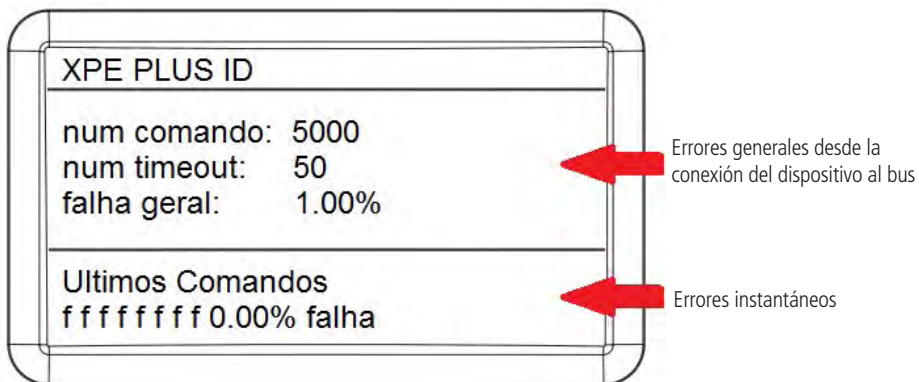
1° Paso: con el MIP en la pantalla de inicio, presione la tecla 7:



2º Paso: seleccione el dispositivo que desea analizar:



3º Paso: verifique el número de errores en la comunicación entre el MIP y el dispositivo seleccionado, de acuerdo con la siguiente información:

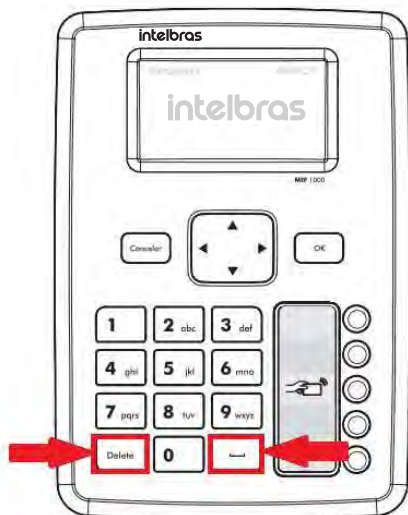


Obs.: el num comando son todos los comandos enviados al dispositivo y el num timeout es cuántos de estos fallaron.

Importante: esta prueba le permite analizar si hay algún problema de comunicación en el bus. Como referencia, los errores por debajo del 10% normalmente no causan problemas de comunicación. Si este valor es mucho mayor, es necesario investigar, como se sugiere a continuación:

- » Conecte los dispositivos individualmente al bus y vuelva a realizar el análisis, ya que un dispositivo puede provocar que todos los demás no se comuniquen.

Obs.: es posible restablecer el contador de errores reiniciando el MIP o presionando la tecla Delete, dentro del análisis del dispositivo. La tecla Espacio restablece el contador de todos los dispositivos a la vez.



- » Identificando el dispositivo o el cable de enlace que genera el problema en el bus, realizar algunas comprobaciones, tales como:
 - » Si hay cortocircuitos u otros problemas en el cableado, probar la continuidad e impedancia del cableado;
 - » Si el problema se soluciona conectando los dispositivos a través de un cableado externo;
 - » Si funciona dejando solo la alimentación y el bus encendidos, apagando todo el resto del producto (cerradura, extensión, sensores, etc);
 - » Si hay otros productos conectados a la misma fuente que el dispositivo, causando interferencia;
 - » Si conecta una fuente exclusiva, al lado del dispositivo, si el problema ya no ocurre;
 - » Si ocurre el mismo problema conectando el dispositivo al lado del MIP.
6. Para consultar la versión de firmware de la MIP IP, con ella en la pantalla de descanso o inicio, pulse la tecla de espacio.

Construcción

Versión
Fecha de creación
Hora de creación
Revisión

5.5. Acceso al MIP 1000 IP

Presione *ENTER* o *OK* para comenzar:

Importante: el usuario configurado de fábrica para la autenticación es **admin** y su contraseña es **123456**. Con la autenticación realizada, el usuario tendrá acceso al menú del MIP 1000 IP para realizar la configuración deseada. Durante la configuración, siempre será necesario confirmar o cancelar una opción, para eso, presione *Ok* o *Cancelar* cuando use el teclado MIP y Enter o ESC a través de un teclado USB externo. En el segundo caso, la tecla TAB cambiará las pantallas, aplicándose este rol también a las teclas direccionales del MIP o teclado.

Pulse *ESC* o *Cancelar* para volver al menú anterior.

The image displays three sequential screenshots of the MIP 1000 IP login process, each enclosed in a rounded rectangular frame.

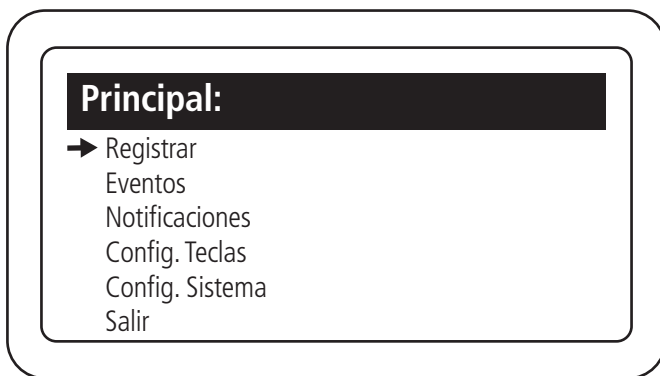
First Screenshot: The title bar reads "Inicio de sesión / Contraseña:". Below it, a field labeled "Inicio de sesión :" contains the text "admin". To the right of the field are up and down arrow icons.

Second Screenshot: The title bar reads "Inicio de sesión / Contraseña:". Below it, a field labeled "Contraseña:" contains the text "123456". To the right of the field are up and down arrow icons.

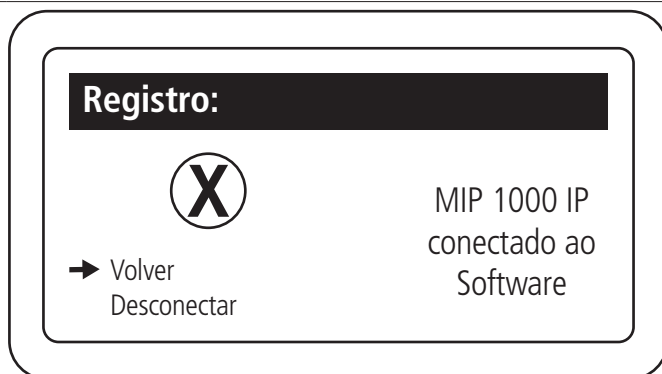
Third Screenshot: The screen displays "OK!" in large bold letters, with "Usuario autenticado como administrador" centered below it.

5.6. Registro

Para dar de alta, editar, consultar o eliminar usuarios, controles remotos, llaveros, huellas digitales, caras y dispositivos, acceda a la opción *Registro del Menú Principal*.



Las operaciones de registro se bloquearán cuando el MIP 1000 IP esté conectado al software.

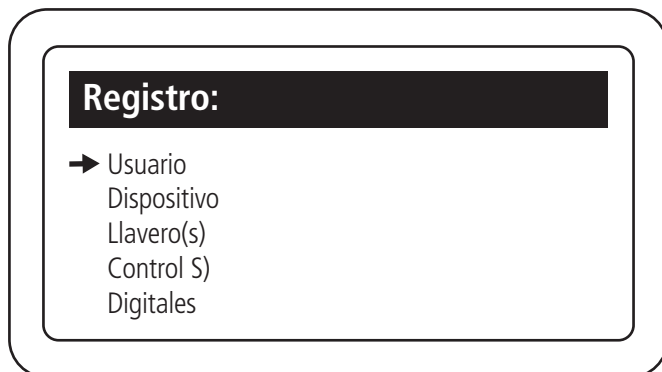


Cuando seleccione Desconectar software, el MIP 1000 IP cerrará las conexiones con el software y permitirá el registro a través del Menú. Después de finalizar las operaciones y regresar a la pantalla de inicio, el MIP 1000 IP le permitirá conectarse nuevamente al software.

Usuario

Registro de residentes

Para registrar un nuevo usuario, realice los siguientes pasos:



Registro:

- Incluir
- Editar
- Consultar
- Excluir

Usuario / Incluir:

Nombre :

↑

↓

Nombrar al usuario que se está registrando (máximo 34 caracteres)

Obs.: con las flechas direccionales en el teclado puede revisar todo el Menú en el teclado.

Usuario / Incluir:

Tipo :

Morador

↑

↓

Establecer el tipo de usuario como residente

The screenshot shows a configuration window with a title bar 'Usuario / Incluir:'. Below the title bar is a text input field labeled 'Dpto:'. To the right of the input field are two arrow buttons, one pointing up and one pointing down, indicating a list or selection menu.

Establecer el número de apartamento del usuario (máximo 5 dígitos)

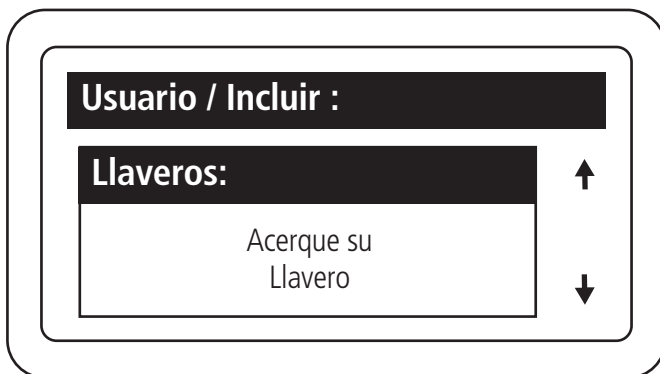
The screenshot shows a configuration window with a title bar 'Usuario / Incluir :'. Below the title bar is a text input field labeled 'Bloque:'. To the right of the input field are two arrow buttons, one pointing up and one pointing down, indicating a list or selection menu.

Definir qual o bloco do morador

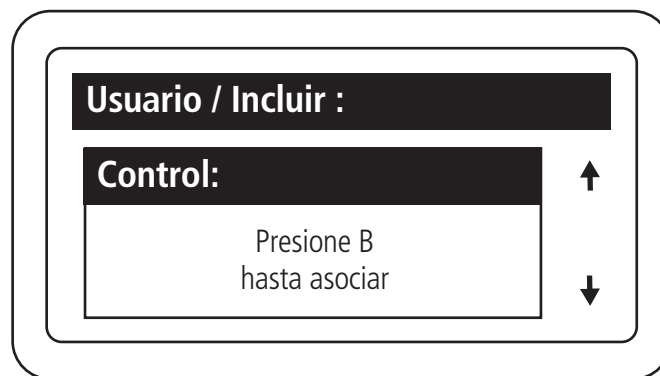
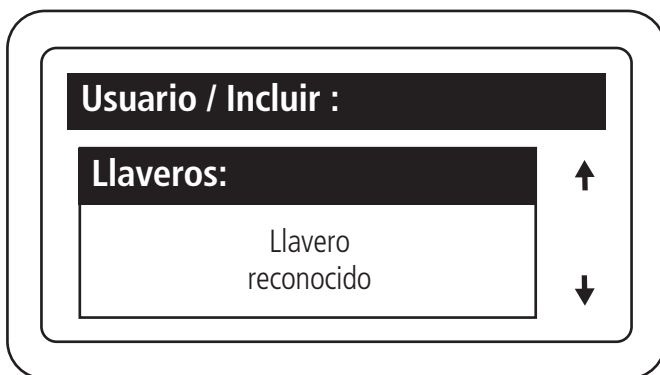
The screenshot shows a configuration window with a title bar 'Usuario / Incluir :'. Below the title bar is a text input field labeled 'Contraseña:'. To the right of the input field are two arrow buttons, one pointing up and one pointing down, indicating a list or selection menu.

Configure la contraseña de usuario para activar las salidas del dispositivo. La contraseña debe ser mayor a 1000 y tener de 4 a 8 dígitos. Para activar, elija salida (1 o 2) + contraseña.

Obs.: las contraseñas no se pueden repetir.



Coloque el llavero RFID Mifare 13,56 MHz que desea registrar en el campo  del MIP



Mantenga presionado el botón B en el control remoto durante aproximadamente cuatro segundos hasta que el MIP confirme la asociación

Usuario / Incluir :

Control: ↑

Control asociado ↓

Usuario / Incluir :

Digital (es): ↑

Bio Inox Porteria
Lector biométrico
Y usa OK/Enter ↓

Seleccione el dispositivo que realizará la captura de huellas digitales y presione OK o Enter para iniciar el registro
Al seleccionar el dispositivo, señalará los pasos de acercamiento a la huella digital. Siga sus instrucciones..

Captura de huella digital:

Bio Inox Porteria : ↑

Esperar 30 s
Paso 01/03 ↓

Inserte la huella digital de acceso 3 veces en el dispositivo según lo solicite el MIP

OK!

¡Éxito en la
captura
Digital!

Usuario / Incluir :

Cara (s):

FACIAL

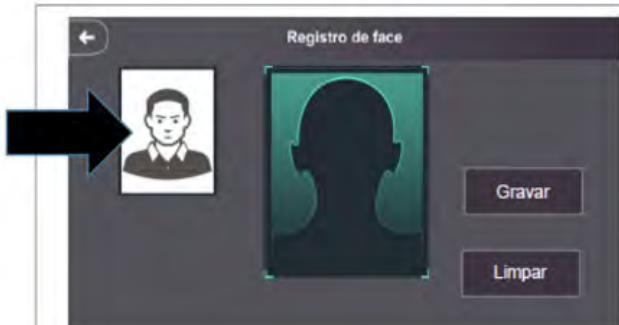
Y use OK/ENTER



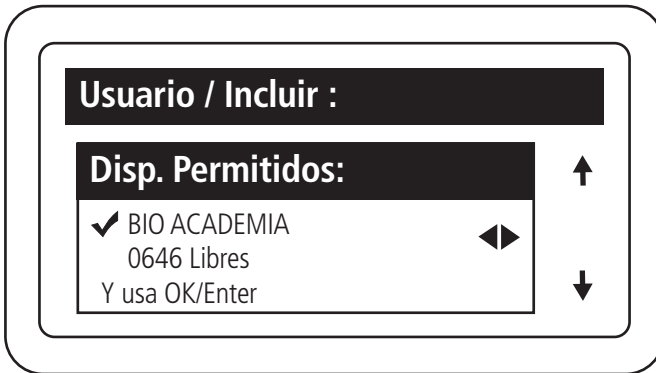
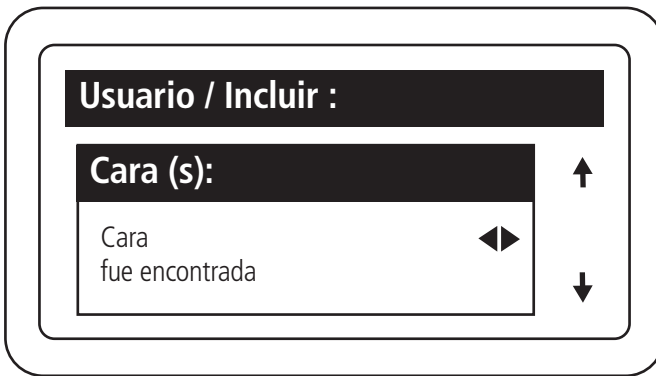
Usuario / Incluir :

Esperar 45s

La persona a registrar debe posicionarse frente al dispositivo facial.



Después de que su foto aparezca clara en el costado, presione Grabar. Si la foto no es buena, presiona borrar y repite el proceso anterior. En la MIP IP, aparecerá el mensaje Se ha encontrado la cara.



Configure a qué dispositivos conectados al bus el usuario tendrá permiso para acceder mediante control remoto, llavero RFID (Mifare), contraseña, huella digital o cara (predeterminado de fábrica: usuarios con permiso en todos los dispositivos registrados)

Atención: si el elemento Modo de registro en Conf. se selecciona la opción Avanzado (predeterminado de fábrica), también se puede configurar la siguiente información en el registro de usuario:

The screenshot shows a configuration window titled "Usuario / Incluir :". Below the title is a field labeled "Cédula de Identidad:" with an empty input area. To the right of the input area are two vertical arrows: an upward-pointing arrow above and a downward-pointing arrow below.

Número de cédula del usuario

The screenshot shows a configuration window titled "Usuario / Incluir :". Below the title is a field labeled "Correo electrónico:" with an empty input area. To the right of the input area are two vertical arrows: an upward-pointing arrow above and a downward-pointing arrow below.

Correo electrónico del usuario (máximo 34 caracteres)

The screenshot shows a configuration window titled "Usuario / Incluir :". Below the title is a field labeled "Tel. Residencial :" with an empty input area. Inside the input area, the characters "()" are visible. To the right of the input area are two vertical arrows: an upward-pointing arrow above and a downward-pointing arrow below.

Número de teléfono residencial del usuario

Usuario / Incluir :

Tel. Celular :

()

↑

↓

This screenshot shows a mobile form with a title bar 'Usuario / Incluir :'. Below it is a label 'Tel. Celular :'. The input field contains the characters '()'. To the right of the input field are two arrow icons, one pointing up and one pointing down, indicating a list or selection menu.

Número de celular del usuario

Usuario / Incluir :

CPF :

↑

↓

This screenshot shows a mobile form with a title bar 'Usuario / Incluir :'. Below it is a label 'CPF :'. The input field is empty. To the right of the input field are two arrow icons, one pointing up and one pointing down, indicating a list or selection menu.

Número de CPF del usuario

Al completar el registro, presione Ok o Enter para confirmar.

Usuario / Incluir :

OK!

Usuario incluido
con éxito

This screenshot shows a mobile form with a title bar 'Usuario / Incluir :'. The main content area displays a success message: 'OK!' followed by 'Usuario incluido con éxito' on two lines.

Registro de visitantes y proveedores de servicios

Si en el Registro de Usuario selecciona su tipo como Visitante o Proveedor de Servicios, algunas opciones cambiarán, como se muestra en las siguientes pantallas:

The screenshot shows a form titled "Usuario / Incluir :". Below the title is a dropdown menu labeled "Tipo :". The selected option is "Prov. Servicio". To the right of the dropdown are two arrows: an upward-pointing arrow above and a downward-pointing arrow below, indicating that the menu can be expanded.

Seleccione el tipo de usuario como proveedor de servicios o visitante

The screenshot shows a form titled "Usuario / Incluir :". Below the title is a text input field labeled "Fecha de inicio :". The field contains the date "01/02/2019". To the right of the field are two arrows: an upward-pointing arrow above and a downward-pointing arrow below, indicating that the field can be expanded for more options.

Informar la fecha inicial de acceso al condominio

The screenshot shows a form titled "Usuario / Incluir :". Below the title is a text input field labeled "Fecha final :". The field contains the date "31/12/99". To the right of the field are two arrows: an upward-pointing arrow above and a downward-pointing arrow below, indicating that the field can be expanded for more options.

Informar la fecha final de acceso al condominio

Usuario / Incluir :

Inicio del Período:

00 : 00

Informar la hora inicial de acceso al condominio

Usuario / Incluir :

Fin del periodo:

23 : 59

Informar la hora inicial de acceso al condominio

Usuario / Incluir :

Días permitidos:

Domingo

Y use OK/Enter

Informar los días de la semana que se permitirá el acceso

Obs.: esta opción solo está disponible cuando MIP IP está configurado con el modo de registro avanzada.

Importante: además de estas funciones, la diferencia entre el registro de visitantes/proveedores de servicios y residentes radica en el tema de las huellas digitales y caras, que solo están disponibles para los residentes.

Dispositivo

Incluir dispositivo

Para registrar un dispositivo, es necesario realizar los siguientes pasos:

El dispositivo a registrar debe estar conectado al serial 1 o serial 2 del MIP IP.

Obs.: después del registro, el dispositivo debe estar en el serial 2 para comunicarse con el MIP IP.



¡Atención!

Los siguientes pasos se refieren a agregar un dispositivo a través del serial 2.

Registro:

- Usuario
- Dispositivo
- Llavero(s)
- Control (es)
- Digitales (es)

Agregar dispositivo conectado al bus

Registro / Dispositivo :

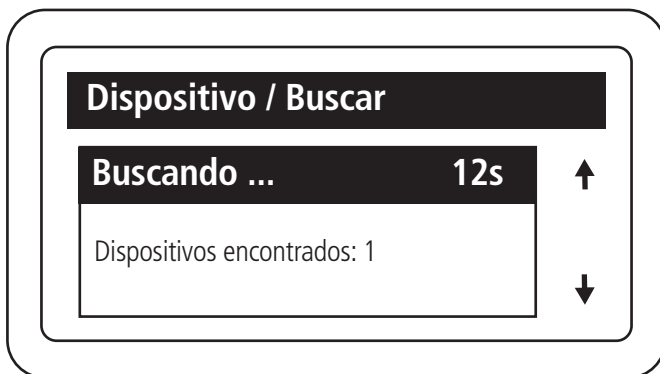
- Agregar nuevo S1
- Agregar nuevo S2
- Resincronizar
- Editar
- Consulta
- Eliminar

Seleccione la inclusión a través del serial 2

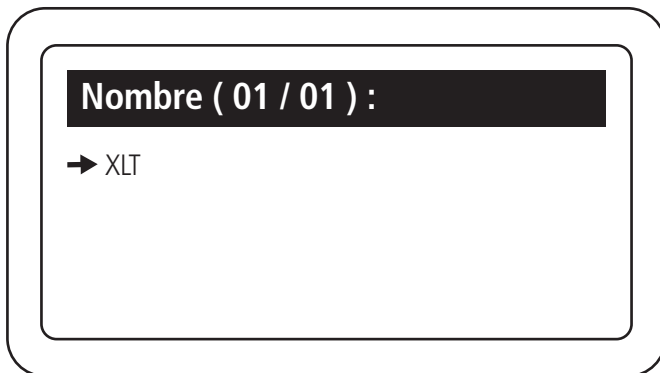
Dispost. / Buscar :

- XRE
- XLT - ID
- XPE - ID
- Biolnox
- CT500 - 1P
- Remote

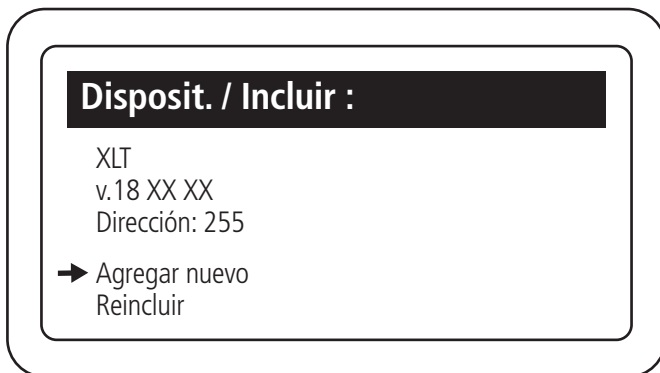
Elegir el dispositivo



El MIP 1000 IP encontrará todos los dispositivos del modelo seleccionado que estén conectados al bus



Obs.: el dispositivo a registrar debe estar alimentado y conectado al bus serial 2, con el MIP IP. Los modelos XPE ID, XPE PLUS ID, XLT 1000 ID y XRE 1000 emiten pitidos de señalización cuando la flecha del menú superior está sobre ellos.



Seleccione la opción incluir como nuevo

Obs.: si elige la opción Reincluir, el MIP reemplazará el nuevo dispositivo con otro que ya existe en el bus con la misma configuración sin necesidad de ingresar la información a continuación.

Dispositivo / Incluir :

Nombre :

↑

↓

Nombrar el dispositivo que se está registrando

Dispositivo / Incluir :

Nombre Accion. 01:

Salida01

↑

↓

Establece el nombre de salida 1 del dispositivo

Dispositivo / Incluir :

Tipo Accion. 01:

Llaveroy Contraseña ◀▶

↑

↓

Seleccione los tipos de accionamientos permitidos en la salida 1 del dispositivo

Importante:

- » **XRE 1000:** configura qué botón del control remoto (Power, A y B) activará la salida.
- » **XLT 1000 ID, XPE ID y XPE PLUS ID:** configura si la salida se puede activar mediante llavero RFID (Mifare) y contraseña, solo llavero RFID (Mifare) o solo contraseña.
- » **SS 311 MF (Bio Inox):** configura si la salida podrá ser accionada a través de biometría y llaveo RFID (Mifare), solo biometría o solo llavero RFID (Mifare).
- » **SS 3530 MF W (facial):** configura si la salida se puede activar a través del cara y llavero RFID (Mifare) o solo a través de cara.
- » **CT 500 1P (controladora):** solo tiene una opción de configuración, que es solo un llavero.

The image shows a configuration screen with a dark header bar containing the text "Dispositivo / Incluir :". Below the header is a white box with a dark bar at the top containing the text "Tiempo Accio. 01". The main area of the white box contains the text "02x0.5s". To the right of the white box are two black arrows, one pointing up and one pointing down, indicating that the value can be adjusted.

Configure el tiempo, múltiplo de 0,5 segundos, para activar la salida 01 del dispositivo. El valor máximo para este campo es 99.

The image shows a configuration screen with a dark header bar containing the text "Dispositivo / Incluir :". Below the header is a white box with a dark bar at the top containing the text "Tiempo Sens. 01". The main area of the white box contains the text "00x1s". To the right of the white box are two black arrows, one pointing up and one pointing down, indicating that the value can be adjusted.

Configure el tiempo, múltiplo de 1 segundo, entre la apertura del sensor 01 y la activación del aviso sonoro. El valor máximo de este campo es 99, que equivale a 99 segundos. Si este campo se establece en 0, deshabilita la función de sensor de puerta abierta para este dispositivo

Dispositivo / Incluir :

Nombre Accion. 02: Salida02

↑

↓

Establece el nombre de salida 2 del dispositivo

Dispositivo / Incluir :

Tipo Accion. 2: Llavero y Contraseña

↑

↓

Seleccione los tipos de accionamientos permitidos en la salida 2 del dispositivo

Importante:

- » **XRE 1000:** configura qué botón del control remoto (Power, A y B) activará la salida.
- » **XLT 1000 ID, XPE ID y XPE PLUS ID:** configura si la salida se puede activar mediante llavero RFID (Mifare) y contraseña, solo llavero RFID (Mifare) o solo contraseña.
- » **SS 311 MF (Bio Inox):** no tiene salida 2.
- » **SS 3530 MF W (facial):** no tiene salida 2.
- » **CT 500 1P (controladora):** no tiene salida 2.

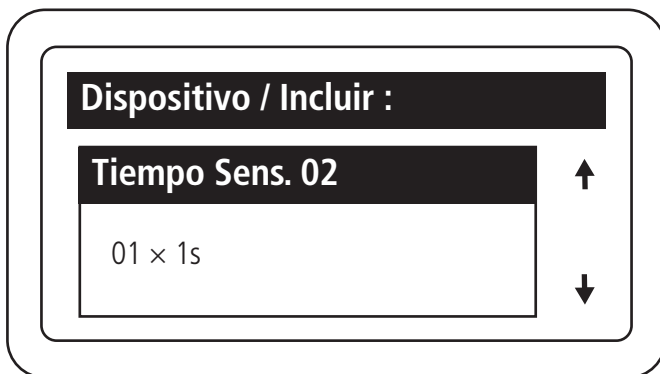
Dispositivo / Incluir :

Tempo Accio. 02 01 x 0,5s

↑

↓

Configure el tiempo, múltiplo de 0,5 segundos, para el disparo de la salida 02 del dispositivo, el valor máximo de este campo es 99.

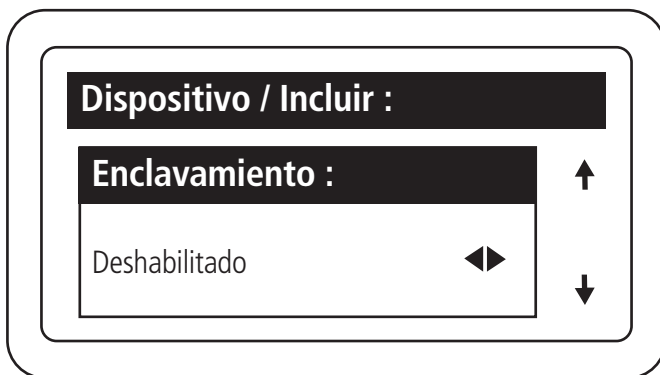


Dispositivo / Incluir :

Tiempo Sens. 02

01 x 1s

Configure el tiempo, múltiplo de 1 segundo, entre la apertura del sensor 02 y la activación del aviso sonoro. El valor máximo de este campo es 99, que equivale a 99 segundos. Si este campo se establece en 0, deshabilita la función de sensor de puerta abierta para este dispositivo.



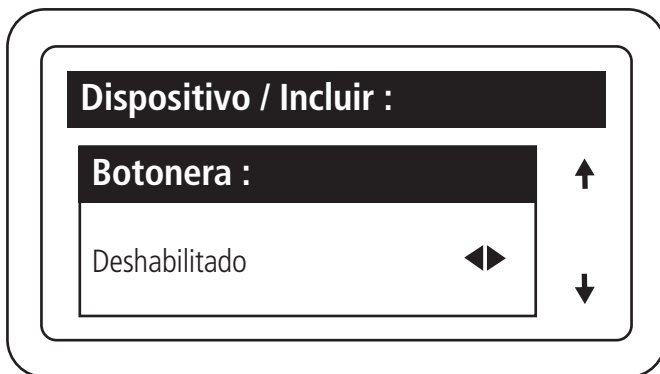
Dispositivo / Incluir :

Enclavamiento :

Deshabilitado

Es posible habilitar la función de enclavamiento en dispositivos con esta funcionalidad (XPE ID, XPE PLUS ID, XLT 1000ID y XRE 1000). Con esta función habilitada, una de las salidas solo se activará si el sensor de la otra salida está cerrado, es decir, una de las puertas/portones solo se abre si el otra está cerrado.

Obs.: consulte ejemplos de instalación con enclavamiento en las guías del dispositivo.



Dispositivo / Incluir :

Botonera :

Deshabilitado

Configure las entradas del sensor del dispositivo como botonera

Hay algunas posibilidades de configuración:

Sen.1&Fech.1

Sen.2&Fech.2

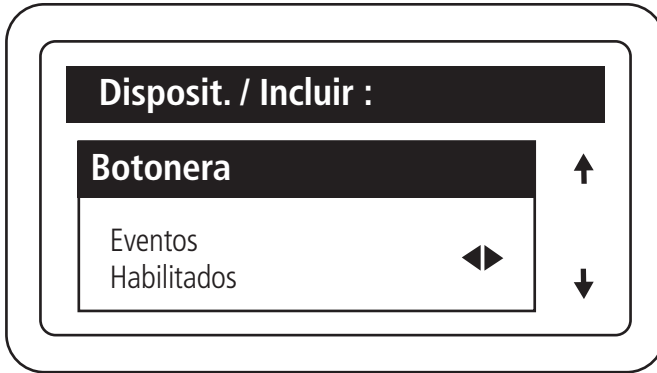
Sen.1&Fech.1 e Sen.2&Fech.2

Sen.1&Fech.2

Sen.2&Fech.1

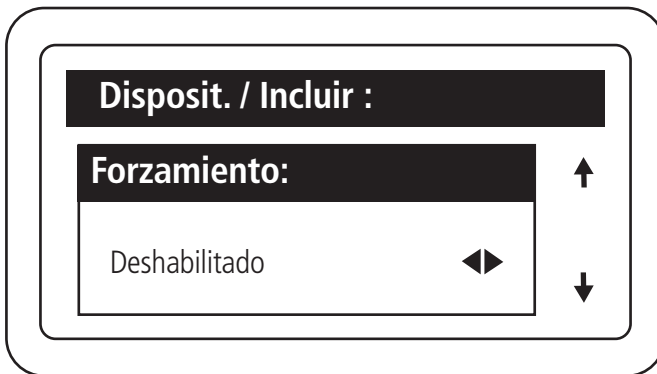
Esto indicará a qué entrada del sensor se conectará a la botonera y qué salida activará.

Obs.: los dispositivos XPE PLUS ID, SS 311 MF (Bio Inox), SS 3530 MF W (facial) y CT 500 1P (controlador) tienen salidas de botoneras independientes, por lo que no utilizan esta configuración.



Habilitación y deshabilitación de eventos de disparo mediante botonera

Obs.: función importante cuando la salida de relé de un dispositivo está conectada a la entrada botonera de otro. Deshabilitarlo evitará que lleguen dos eventos al MIP IP en cada accionamiento.



Esta función le permite señalar cuando una puerta se ha abierto a la fuerza. Esto es posible cuando el sensor conectado a él está abierto y el dispositivo no ha recibido ninguna solicitud de disparo.

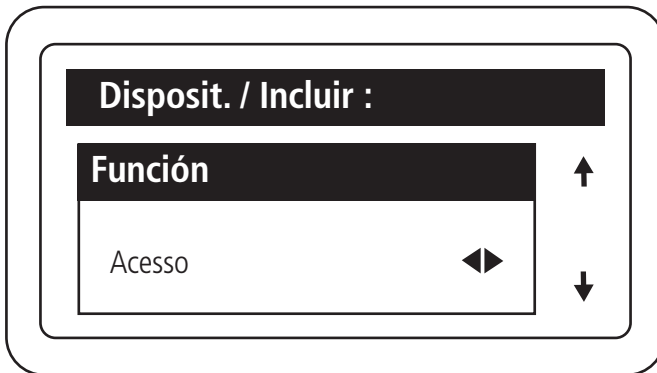
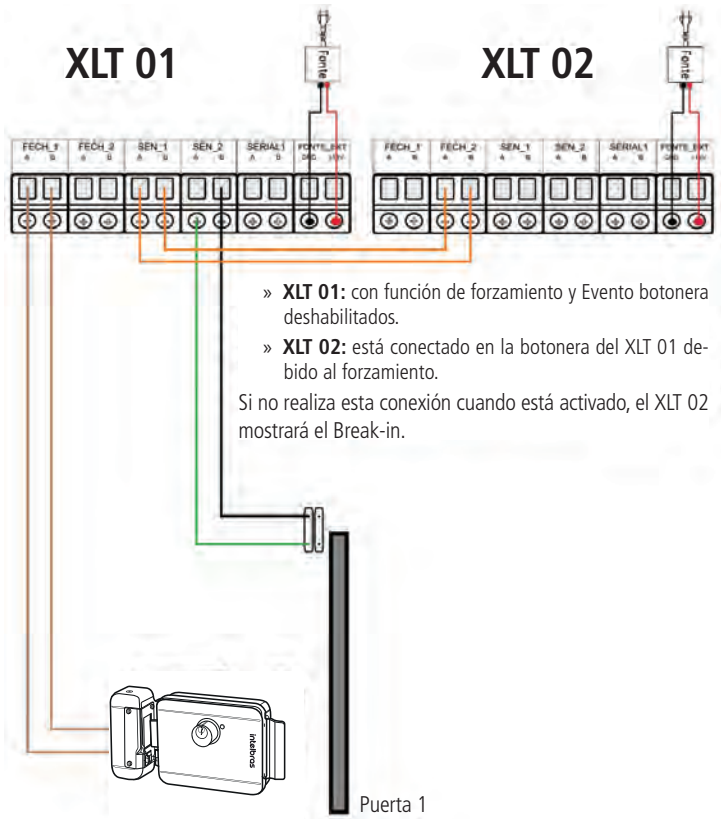
usando las flechas ◀▶ laterales es posible habilitar y elegir qué función desea.

Hay 3 opciones de configuración para el forzamiento:

- » **Sensor 1 para cerradura 1 (Sen.1&Cer.1):** cuando se fuerza la apertura de la puerta donde se encuentra la cerradura 1, el MIP 1000 mostrará la alerta de FORZAMIENTO y el dispositivo emitirá una señal sonora.
- » **Sensor 2 para cerradura 2 (Sen.2&Cer.2):** cuando se fuerza la apertura de la puerta donde se encuentra la cerradura 2, el MIP 1000 mostrará la alerta de FORZAMIENTO y el dispositivo emitirá una señal sonora.
- » **Sensor 1 para cerradura 1 (Sen.1&Cer.2) y Sensor 2 para cerradura 2 (Sen.2&Cer.2):** cuando la puerta donde se encuentra la cerradura 1 o 2 se abre a la fuerza, el MIP 1000 mostrará la alerta FORZAMIENTO y el dispositivo emitirá una señal audible.

Ejemplo de conexión con evento de botón desactivado:

En el diagrama de cableado a continuación, tenemos 2 XLT 1000 id conectados a una sola puerta. El evento botonera del XLT 01 está deshabilitado, su botonera está siendo activado por el XLT 02.



Configuración de la forma en que funcionará el dispositivo

Hay 2 tipos:

- » **Acceso**: función normal para residentes, visitantes y proveedores de servicios.

- » **Colector:** esta función está destinada a dar de baja llaveros RFID (Mifare) de visitantes y proveedores de servicios cuando se utilizan en el dispositivo. No borra los llaveros de los residentes.

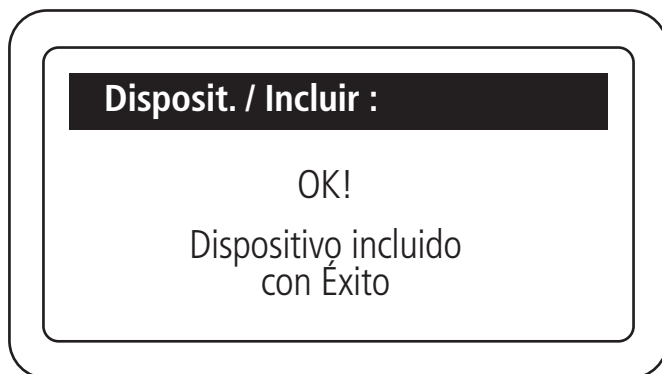
Importante: esta función solo está disponible para el dispositivo XLT 1000 ID.

Después de estos pasos, confirme con Ok o Enter para continuar.

Obs.: para el producto XRE 1000 existe la función Carro. El objetivo de esta función es generar un evento informando que un carro pasó por la puerta sin registro en el MIP 1000.

Ejemplo:

- » El carro 1 arrancó y pasó en el portón.
- » El carro 2 pasó aprovechando la puerta aún abierta (aparecerá Carro detectado en la pantalla MIP IP).



¡Fin del registro del dispositivo!

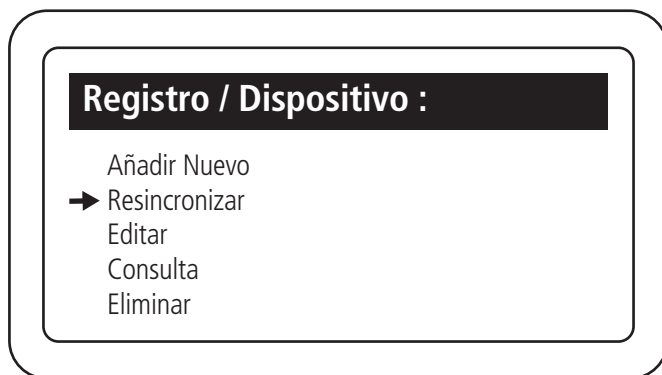
Importante: el registro a través del serial 1 sigue el mismo patrón, sin embargo los dispositivos deben estar conectados al conector Serial1 del MIP IP.



Atención: todos los temas (resincronizar, editar, consultar y eliminar) a continuación están dentro del menú Registro /dispositivo.

Ressincronizar dispositivo

Este comando se utiliza cuando un dispositivo tiene un problema en el bus y tiene información fuera de sincronismo del MIP IP. Esto generará una alerta de falla de sincronización del dispositivo. Para resolver, simplemente siga los pasos a continuación:



Nombre (01 / 06)

- MIP IP
- XRE
- XLT - ID
- XPE - ID
- Biolnox
- CT500 - 1P
- Remote

Seleccione cuál de los dispositivos en su bus le gustaría resincronizar

Disposit. / Ressincronização :

OK!

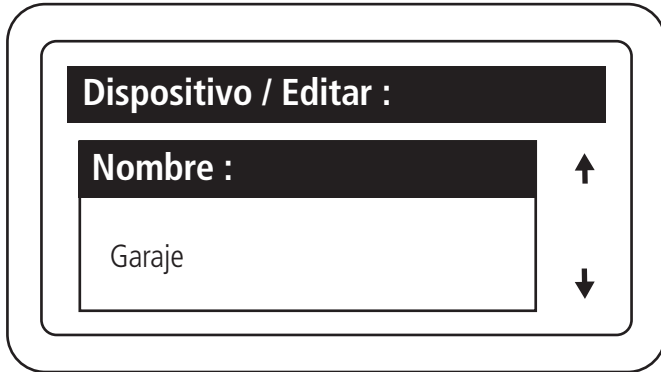
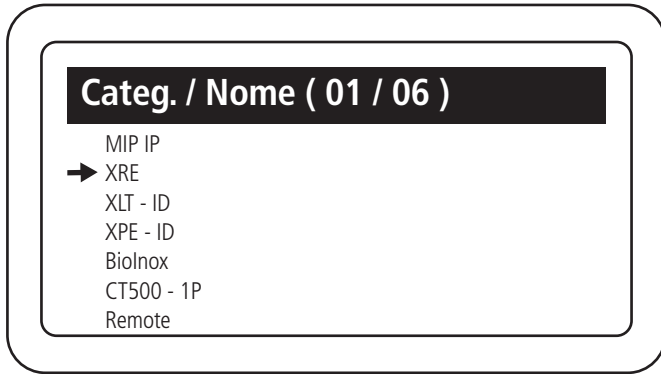
El dispositivo se resincronizó
correctamente

Editar dispositivo

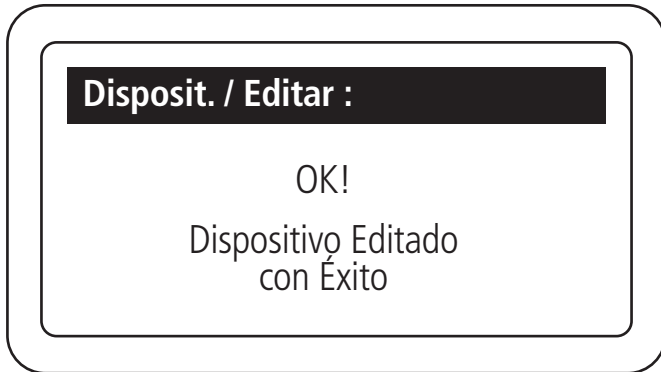
Para editar el registro de un dispositivo, es necesario realizar los siguientes pasos:

Registro / Dispositivo :

- Añadir Nuevo
- Resincronizar
- Editar
- Consulta
- Eliminar



En este menú puede editar toda la información colocada en el momento del registro del dispositivo, al final del cambio presione Entrar o la tecla OK en el MIP.



Consultar dispositivo

Para verificar la información registrada en los dispositivos y la versión de firmware de los dispositivos y el MIP 1000 IP, es necesario utilizar este menú siguiendo los pasos:

Cadastró / Dispositivo :

- Añadir Nuevo
- Resincronizar
- Editar
- Consulta
- Eliminar

Nombre (01 / 07)

- MIP IP
- XRE
- XLT - ID
- XPE - ID
- BioInox
- CT500 - 1P
- Remote

Elige qué dispositivo quiera consultar

Dispositivo / Consultar :

Tipo / Versión / Dir:

XRE
v. 21 xx xx
Dirección: 002



Presione Cancelar o ESC para salir

Eliminar dispositivo

Para eliminar el registro de un dispositivo, es necesario realizar los siguientes pasos:

Cadastre / Dispositivo :

- Añadir Nuevo
- Resincronizar
- Editar
- Consulta
- Eliminar

Nombre (01 / 06)

- MIP IP
- XRE
- XLT - ID
- XPE - ID
- Biolnox
- CT500 - 1P
- Remote

Seleccionar el dispositivo que desea excluir

Dispositivo / Excluir :

Datos del dispositivo:

XRE

↑

↓

Presionar Ok o Enter para continuar

Dispositivo / Eliminar :

¿Eliminar?

(Enter) Confirma
(Escape) Cancela

Disposit. / Eliminar :

OK!

El dispositivo fue
eliminado
con éxito

Obs.: cuando elimine el dispositivo, el MIP ya no podrá acceder a él. Con esto, todos los usuarios tendrán bloqueado su acceso y si está disponible en el bus con el firmware actualizado.

Llaveros

Incluir Llavero

Todavía en el menú de registro del MIP 1000 IP, puede incluir un llavero para el residente/proveedor de servicios o visitante, solo siga los pasos a continuación:

Registro:

Usuario
Dispositivo
→ Llavero(s)
Control (es)
Digital (es)

Registro / Llavero :

- Añadir Nuevo
- Editar
- Consultar
- Eliminar

Usuário / Buscar :

Nombre :



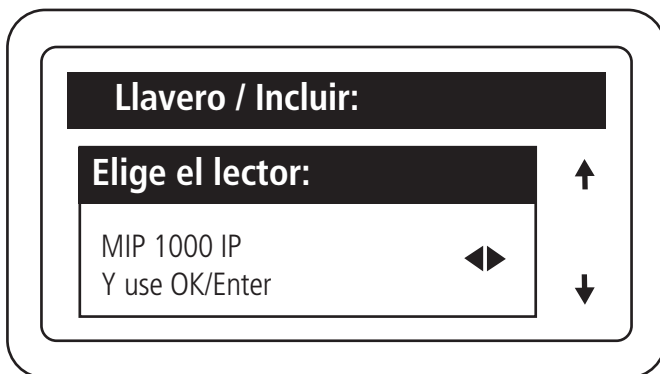
En este campo buscará qué residente/proveedor de servicios o visitante quiere incluir el llavero

Obs.: el usuario ya debe estar registrado en el sistema.

Dpto | Nombre (01/01)

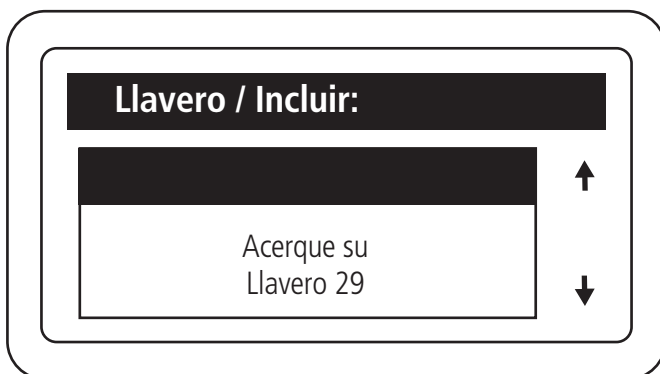
- 102 - Residente

Seleccione el residente para registrar el llavero

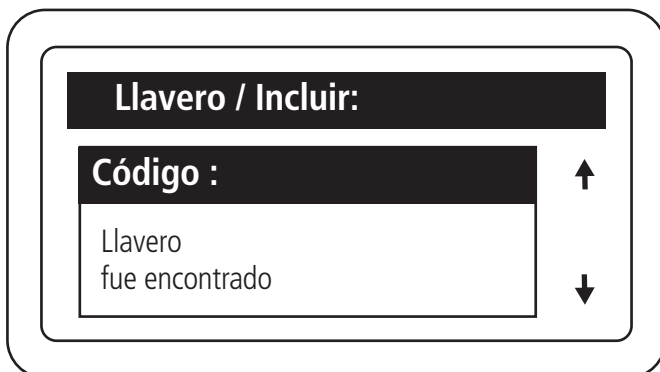


Seleccione en qué dispositivo se leerá el llavero o seleccione Enter si el código se ingresa manualmente en hexadecimal

Obs.: los dispositivos que permiten la lectura son: MIP 1000 IP, XPE PLUS ID, XLT 1000 ID y CT 500 1P.



Seleccione en qué dispositivo se leerá el llavero o seleccione Enter si el código se ingresa manualmente en hexadecimal



Al presionar la flecha en el teclado, puede ingresar la información de registro opcional que se detalla a continuación:

Llavero / Incluir:

Carro (Modelo) : ↑

↓

Llavero / Incluir:

Carro (Marca) : ↑

↓

Llavero / Incluir:

Carro (Color) : ↑

↓

Llavero / Incluir:

Carro (Matrícula) :

↑

↓

OK!

Llavero añadido
con éxito

Presione Entrar o la tecla OK para agregar llavero

Obs.: no es necesario rellenar todos los campos, pero si tiene más de un llavero registrado, le facilitará su identificación.

Editar llavero

En este menú puede cambiar toda la información completada durante el registro mencionado anteriormente.

Consultar llavero

En este menú podrá consultar toda la información cumplimentada durante el registro mencionado anteriormente.

Eliminar llavero

Registro / Llavero :

Añadir Nuevo

Editar

Consultar

→ Eliminar

Llavero (s) (01 / 02)

→ 0xe9b1df1d
0xd9x1bf1e

Escolher qual chaveiro deseja excluir

Llavero / Eliminar:

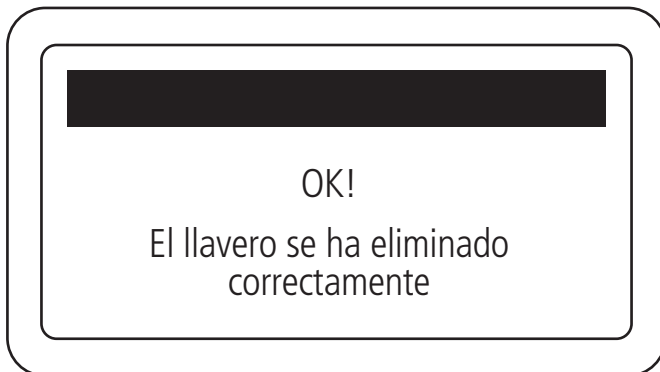
¿Está seguro?

Código de llavero

Llavero / Eliminar:

Eliminar ?

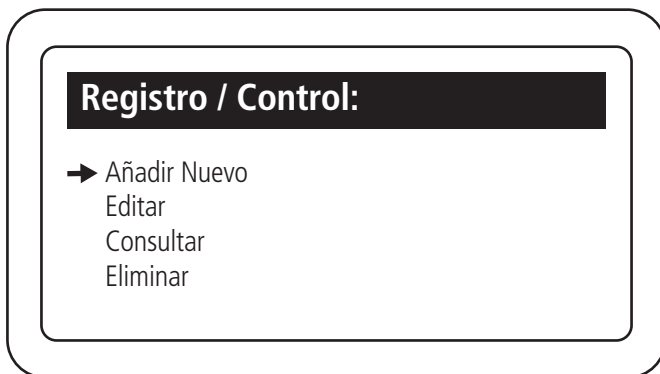
(Enter) Confirma
(Escape) Cancela



Control

Incluir control

En el menú de registro añadiremos un nuevo control para el usuario ya registrado. Siga los pasos a continuación:



Usuário / Buscar :

Nombre : ↑

Residente ↓

Digitar o nome de qual usuário você deseja incluir

Control / Incluir :

Código : ↑

Mantener B ↓
hasta asociar

Después de agregar el control, aparecerá el mensaje el Control fue encontrado con la flecha hacia abajo para completar los datos opcionales.

Control / Incluir :

Carro (Modelo) : ↑

↓

Control / Incluir :

Carro (Marca) : ↑

↓

Control / Incluir :

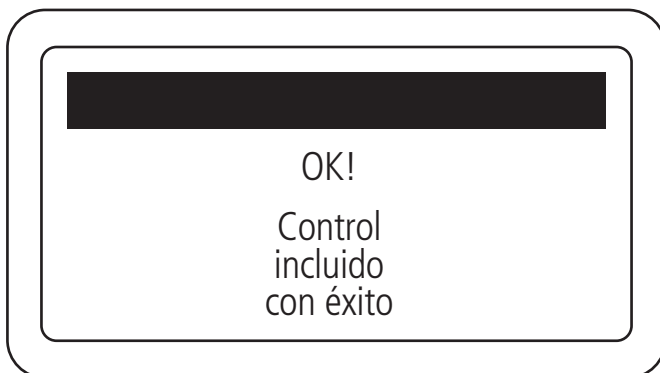
Carro (Color) : ↑

↓

Control / Incluir :

Carro (Matrícula) : ↑

↓



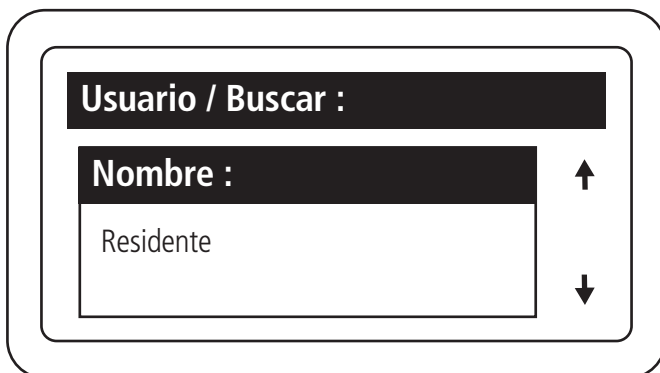
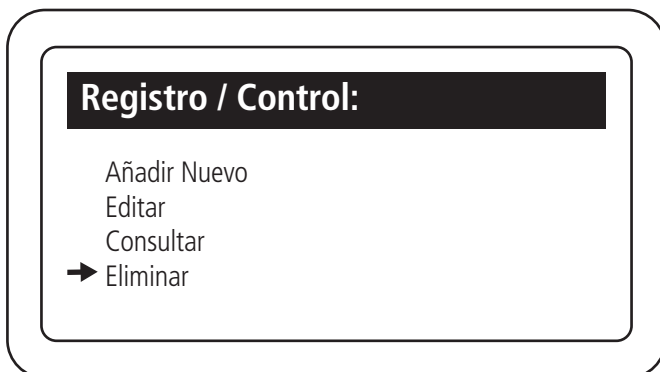
Editar control

En este menú puede cambiar toda la información completada durante el registro mencionado anteriormente.

Consultar control

En este menú podrá consultar toda la información cumplimentada durante el registro mencionado anteriormente.

Eliminar control



Control (s) (01 / 01):

→ 1256074242

Control / Eliminar :

¿Está seguro?

1256074242

Presione Enter para eliminar el control o ESC para cancelar

OK!

Control
eliminado
con éxito

Digital

Incluir huella digital

Dentro del menú de registro puede Incluir/Editar/Consultar y Eliminar huella digital, solo siga los siguientes pasos:

Registro:

- Usuario
- Dispositivo
- Llavero(s)
- Control (es)
- digital (es)

Registro / Huella digital:

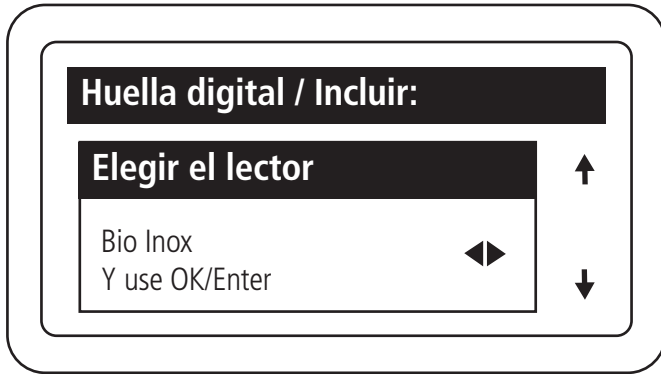
- Añadir Nuevo
- Editar
- Consultar
- Eliminar

Usuario / Buscar :

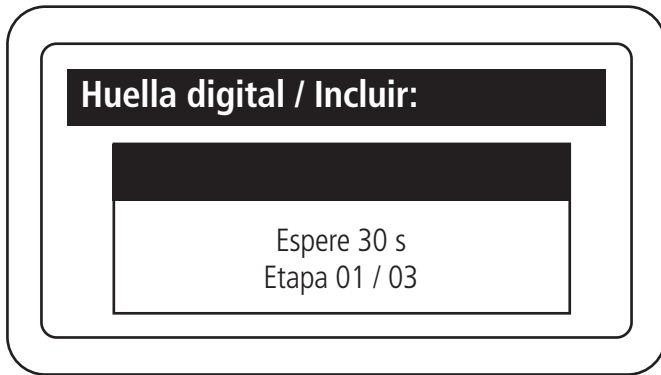
Nombre : ↑

Residente ↓

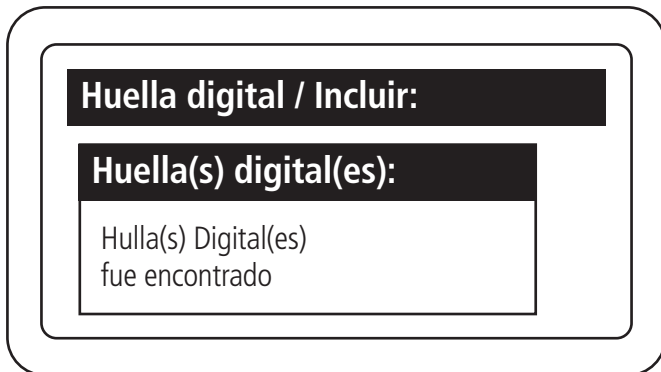
Busca qué residente incluirá la nueva huella digital



Elija en qué lector de huellas dactilares registrar la huella digital



La huella digital debe insertarse en el Bio Inox 3 veces, como se indica en el producto



Huella digital / Incluir:

Tipo: ↑

Normal ◀▶ ↓

Huella digital / Incluir:

Carro (Modelo): ↑

↓

Huella digital / Incluir:

Carro (Marca): ↑

↓

Huella digital / Incluir:

Carro (Color): ↑

↓

Huella digital / Incluir:

Carro (Matrícula): ↑

↓

OK!
Huella digital añadida
con éxito

Presiona Enter para terminar de agregar la huella digital

Editar huella digital

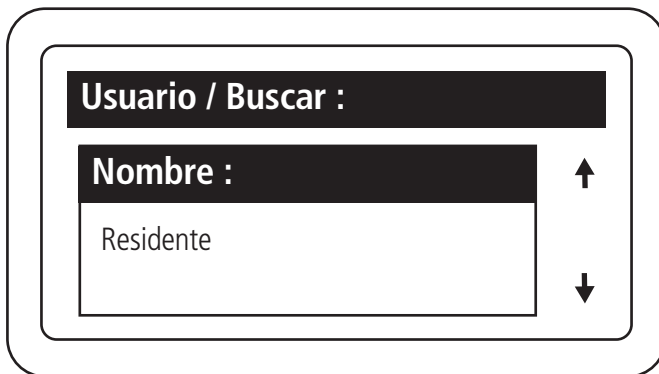
En este menú puede cambiar toda la información completada durante el registro mencionado anteriormente.

Consultar huella digital

En este menú podrá consultar toda la información cumplimentada durante el registro mencionado anteriormente.

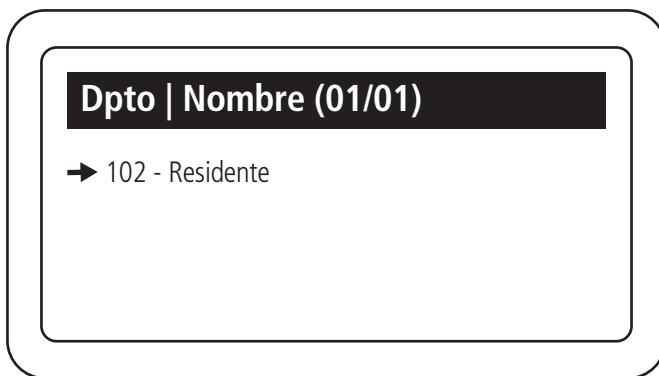
Eliminar huella digital

Si desea eliminar una huella digital de un residente que no tendrá acceso con la huella digital, debe seguir estos pasos:



The screenshot shows a search interface with a dark header bar containing the text "Usuario / Buscar :". Below this is a search input field with the text "Nombre :". The input field contains the text "Residente". To the right of the input field are two arrows: an upward-pointing arrow above a downward-pointing arrow, indicating a search or list navigation function.

Buscar al residente para eliminar la huella digital



The screenshot shows a search result interface with a dark header bar containing the text "Dpto | Nombre (01/01)". Below this is a search result entry: "→ 102 - Residente".

Después de seleccionar el residente presione Entrar

Huella(s) Digital(es) (01/ 01)

→ 00002

Normal

Selecione qué huella dactilar del residente eliminar

Huella digital / Eliminar:

¿Está seguro?

00002

Presione Enter para eliminar la huella digital o ESC para cancelar

Huella digital/Editar:

OK!

La huella digital se eliminó
con éxito

Caras

Incluir Caras

Dentro del Menú Registrar/Cara puede incluir, editar, consultar y borrar caras, solo siga los siguientes pasos:

Registro:

- Usuario Dispositivo
- Llavero(s)
- Control(es)
- Huella(s)
- Digital(es)
- Cara(s)

Registro / Cara:

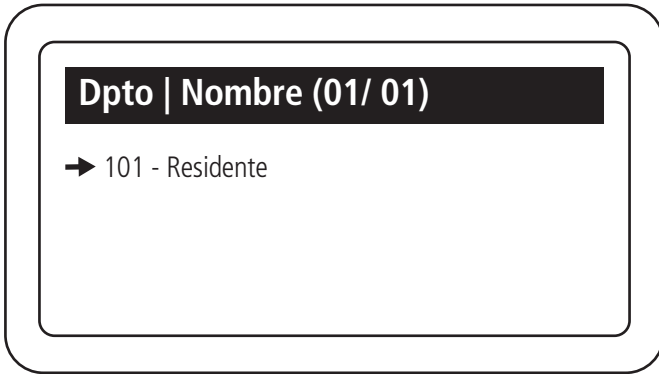
- Añadir Nuevo
- Editar
- Consultar
- Eliminar

Usuario / Buscar :

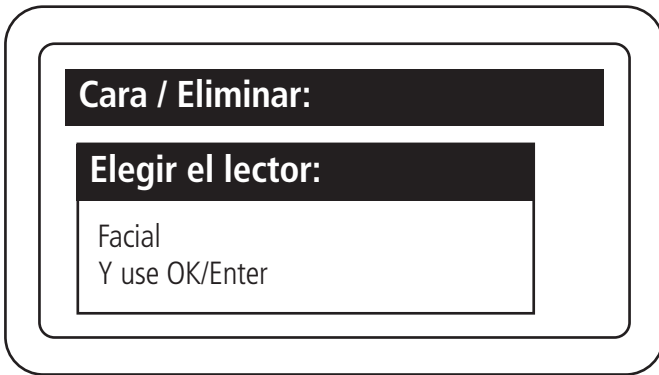
Nombre : ↑

Residente ↓

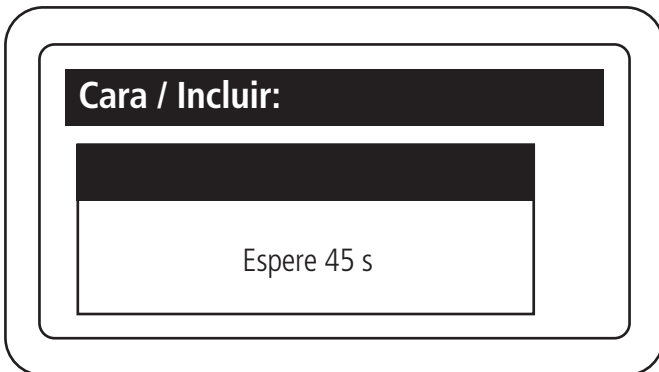
Buscar qué residente incluirá la cara



Selecionar o morador e pressionar Enter ou Ok



Escolher em qual leitor de Face irá cadastrar



Durante los 45 segundos, el MIP espera una respuesta del Facial.

La persona a registrar debe posicionarse frente al dispositivo Facial y seguir los siguientes pasos:

Atención antes del registro

- » Las gafas, los sombreros y la barba pueden influir en el rendimiento del reconocimiento facial. No cubra sus cejas cuando use sombreros.
- » Actualice el registro si hay un cambio visual importante, como quitarse la barba, si el acceso es difícil.
- » Mantenga su cara visible.

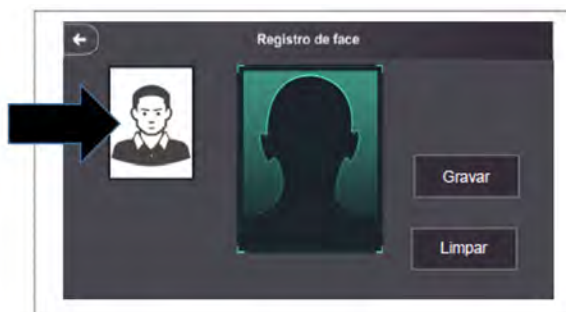
- » Mantenga el dispositivo al menos a dos metros de la fuente de luz y al menos a tres metros de ventanas o puertas; de lo contrario, la luz solar directa puede influir en el rendimiento del reconocimiento facial del dispositivo.

Coloque su cabeza en el marco de captura de fotos. Una foto de su cara será capturada automáticamente.

- » Quédese quieto, no sacuda la cabeza o el cuerpo, ya que el registro puede fallar.
- » Encadre todo el rostro, vista frontal y ojos abiertos;
- » Dar preferencia a un fondo neutro;
- » Solo debe aparecer una cara en la foto;
- » Evite las sombras en la cara o el fondo;
- » Hacer una expresión neutra y natural;



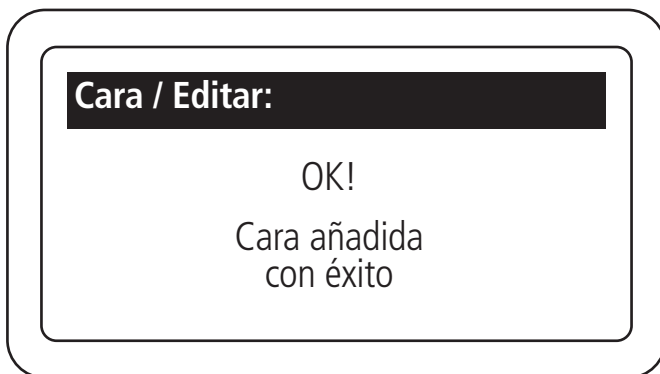
Dispositivo Facial



Después de que su foto aparezca clara en el costado, presione Grabar. Si la foto no es buena, presiona Limpiar y repita el proceso anterior. En la MIP IP, aparecerá el mensaje Se ha encontrado la cara.

Obs.: si es necesario puede rellenar los siguientes datos.

Presione Enter en el teclado o OK en MIP IP.



Editar cara

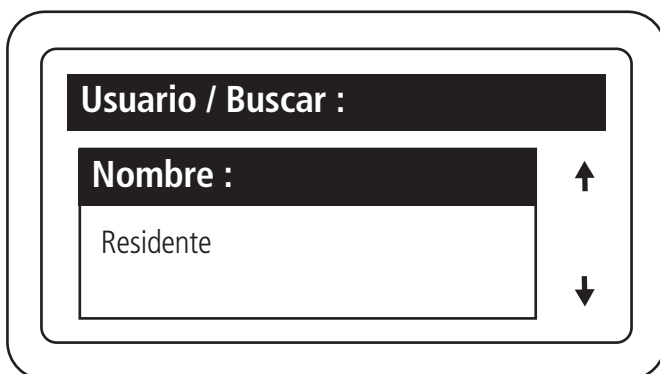
En este menú puede cambiar toda la información completada durante el registro mencionado anteriormente.

Consultar cara

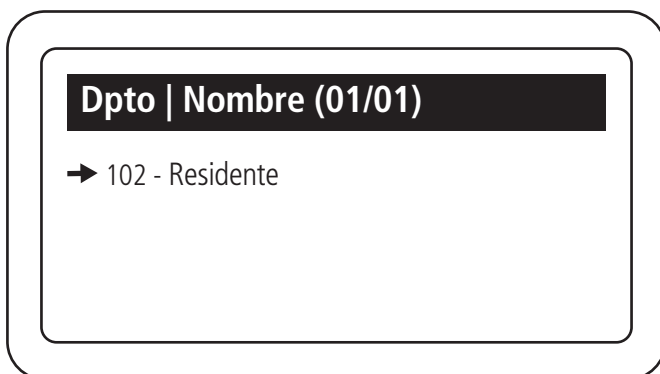
En este menú podrá consultar toda la información cumplimentada durante el registro mencionado anteriormente.

Eliminar cara

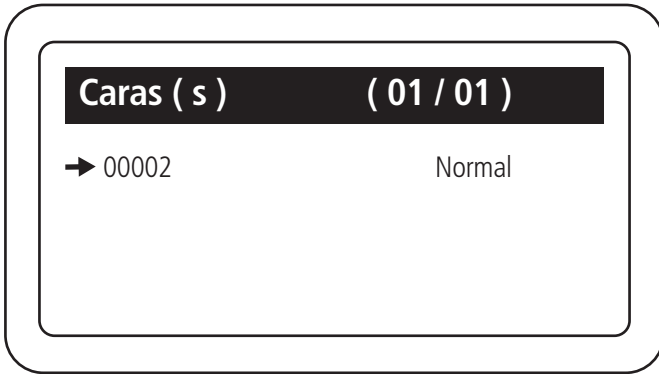
Si desea eliminar una cara de un residente que no tendrá acceso, debe seguir los siguientes pasos:



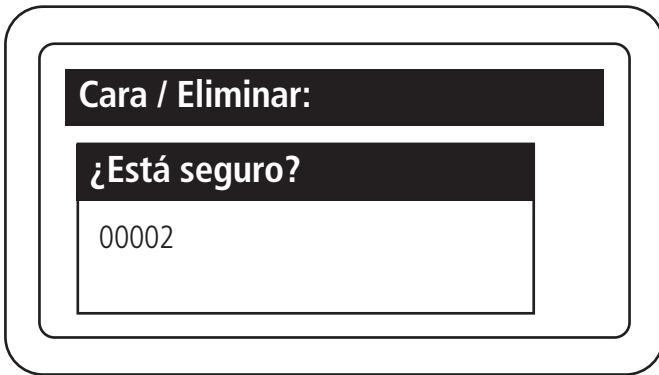
Buscar al residente para eliminar la cara



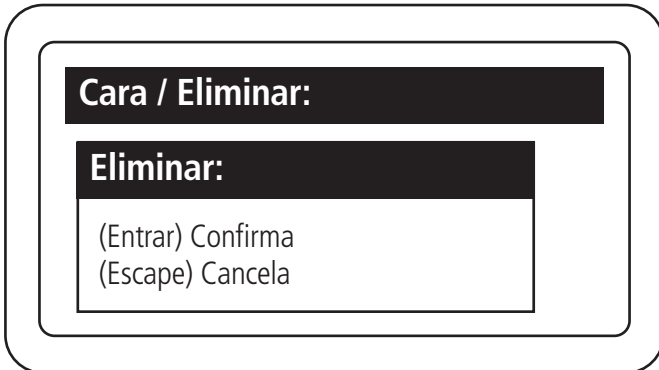
Después de seleccionar el residente presione Entrar

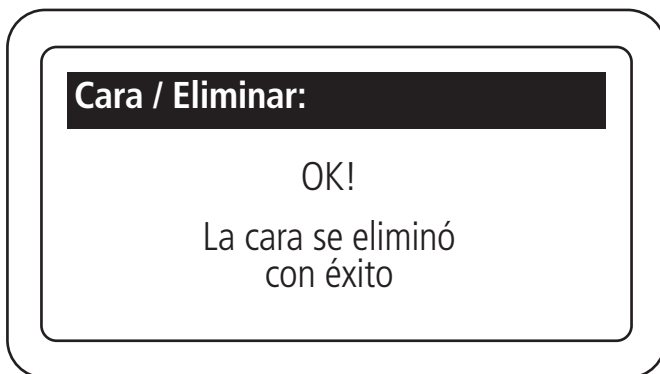


Seleccione qué cara del residente eliminar



Presione Enter para eliminar la huella digital o ESC para cancelar



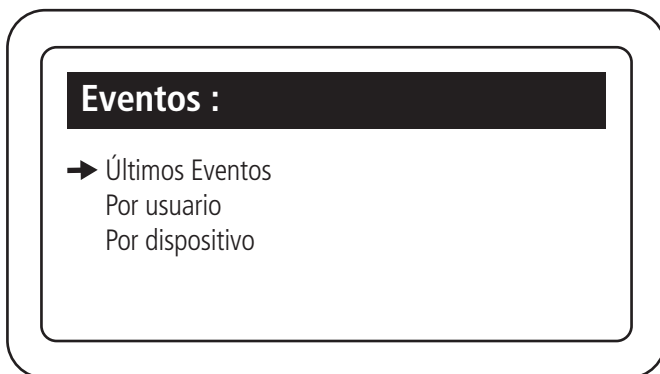


5.7. Eventos

Consultar Eventos

En este menú hay 3 tipos de consulta de eventos: (Últimos eventos, Por usuario, Por dispositivo), a continuación se muestra una descripción de cada consulta:

1. Últimos eventos



04/02/2019	13:22:14
Nombre del residente	↑
Departamento	
Dispositivo de acceso	
Acceso liberado.	↓

2. Por usuario

Usuário / Buscar :	
Nombre :	↑
Residente	
	↓

Dpto Nombre (01/01)
→ 102 - Maria

Presiona Enter para ver los eventos del usuario

04/02/2019	13:22:14
María	↑
Departamento 102	
Portaria	
Acceso liberado.	↓

Pressionando a tecla para baixo você consegue visualizar os 26 últimos acessos do usuário

3. Por dispositivo

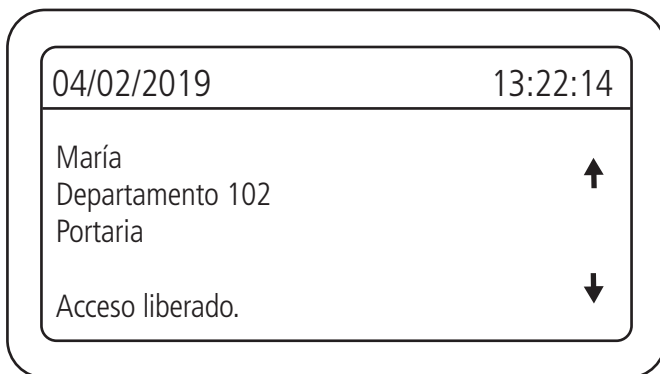
Eventos :

Últimos Eventos
 Por usuario
 → Por dispositivo

Nombre (01 / 06)

MIP 1000 IP
 XRE
 XLT 1000 ID
 → XPE 1013 ID
 Bio Inox plus SS 311
 CT 500 1 P

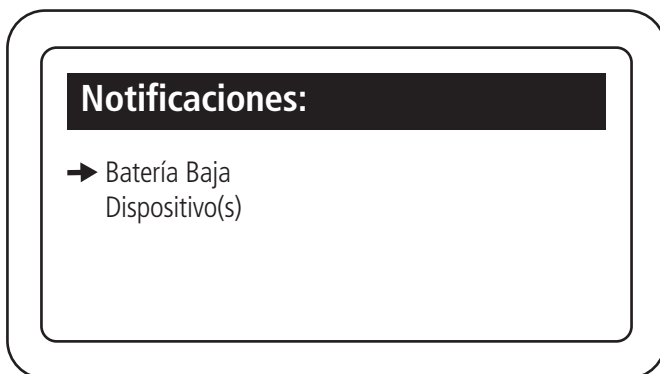
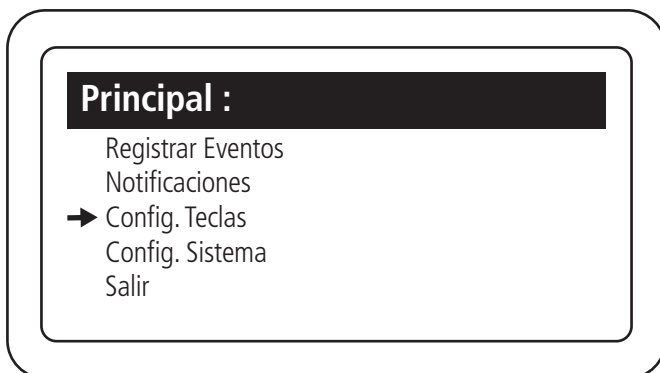
Selecione qué dispositivo para obtener los eventos



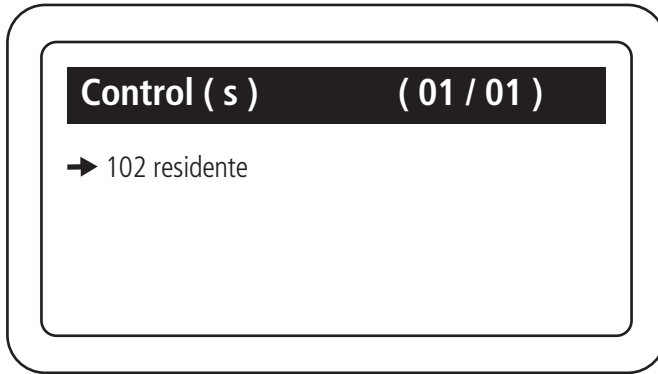
Al presionar la tecla hacia abajo, puede ver los últimos 26 eventos en ese dispositivo

5.8. Notificaciones

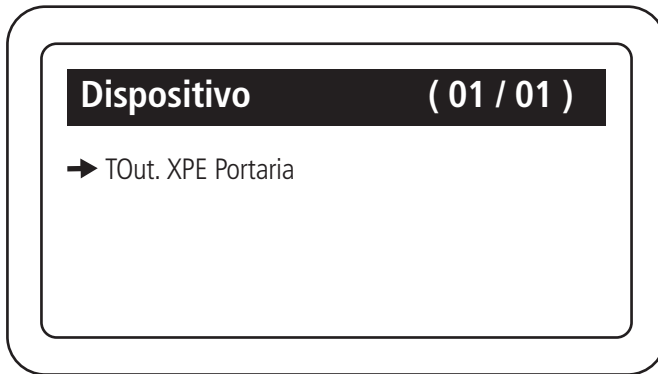
Para consultar las notificaciones del usuario o del sistema SCA, ingrese a la opción Notificaciones en el menú principal, tendrá 2 opciones de notificación (batería baja y Dispositivos).



Seleccione qué tipo de notificación le gustaría consultar



Mostrará qué residente tiene el control con batería baja

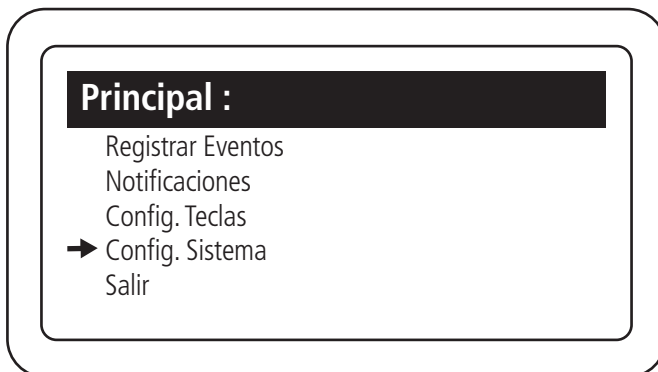


En la notificación del dispositivo, se mostrará qué dispositivo tiene un problema (consulte el ítem 5.3.Pantallas de eventos)

5.9. Configuración de tecla

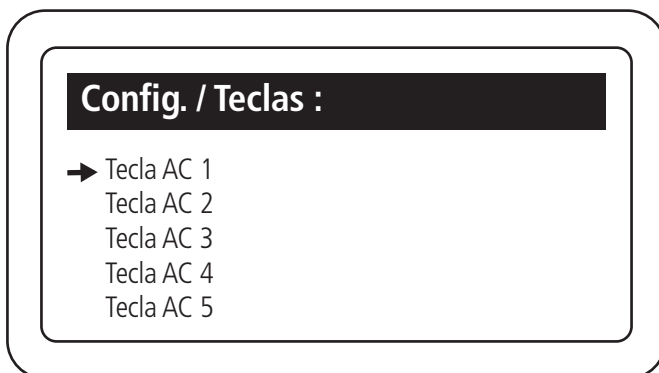
El MIP IP tiene cinco teclas que se pueden configurar para activar salidas desde un dispositivo o desde el mismo MIP IP. Cuando se configura una tecla, se encenderá indicando su funcionamiento. Esta tecla también indica, mediante parpadeo, cuando el dispositivo asociado está en Time Out.

Para configurar las claves de activación, ingrese a la opción Config. Teclas del menú principal.



Configurar tecla

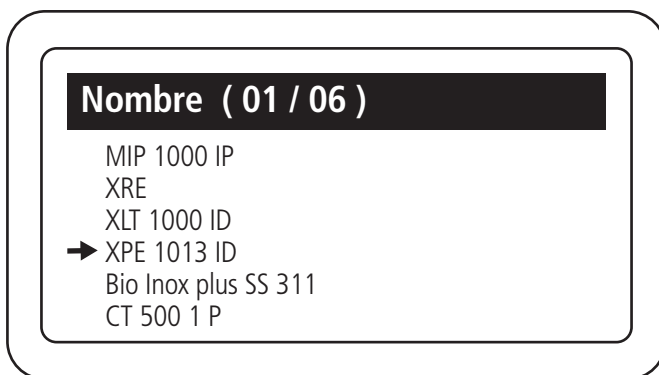
Para configurar una tecla é necessário realizar os seguintes passos:



Config. / Teclas :

- Tecla AC 1
- Tecla AC 2
- Tecla AC 3
- Tecla AC 4
- Tecla AC 5

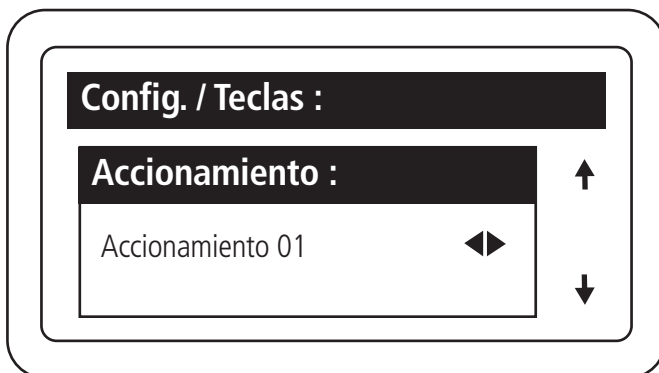
Selecciona qué tecla desea utilizar



Nombre (01 / 06)

- MIP 1000 IP
- XRE
- XLT 1000 ID
- XPE 1013 ID
- Bio Inox plus SS 311
- CT 500 1 P

Seleccione qué dispositivo se activará al presionar la tecla



Config. / Teclas :

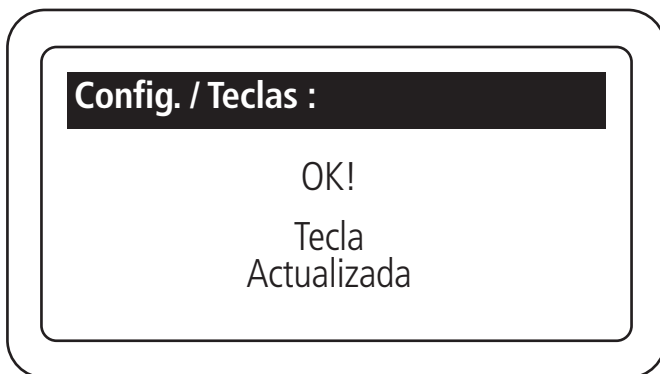
Accionamiento :

Accionamiento 01

↑

↓

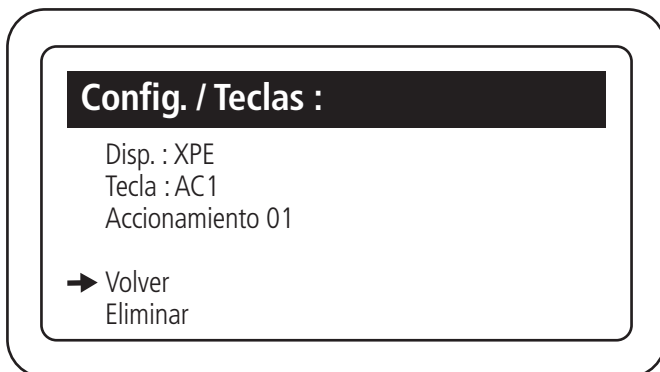
Seleccione con la flecha derecha cuál de las salidas del dispositivo se activará y presione Enter



Después de seleccionar la tecla deseada, se encenderá en el teclado del MIP 1000 IP

Volver/Eliminar tecla

Cuando seleccione una tecla ya registrada, aparecerá la opción de Volver o Eliminar, como se muestra en la siguiente pantalla:

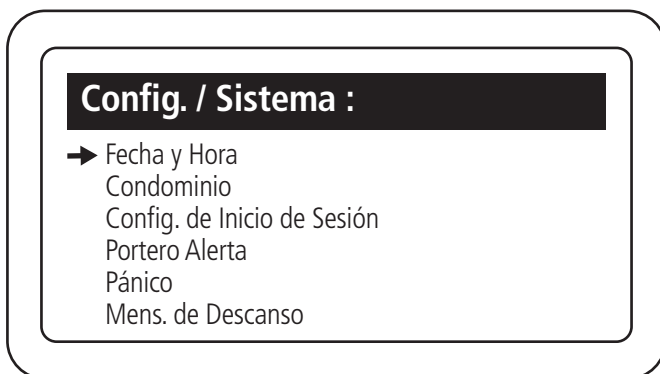


No es posible editar una tecla ya registrada, por lo que es necesario borrar la actual y dar de alta la nueva configuración. Si no desea editar, simplemente seleccione la opción Volver.

5.10. Configuración de sistema

En el menú Configuración del sistema puede cambiar las funciones de MIP IP.

Fecha y Hora



Config. / Fecha :

Fecha : ↑

07/02/19 ↓

Config. / Fecha :

Fecha : ↑

08:40 ↓

Obs.: después de configurar la fecha y la hora, presione Enter, la pantalla MIP mostrará la frase OK, la fecha y la hora se cambiaron correctamente.

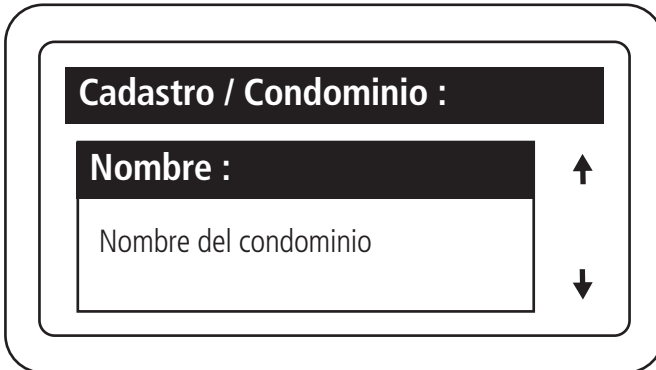
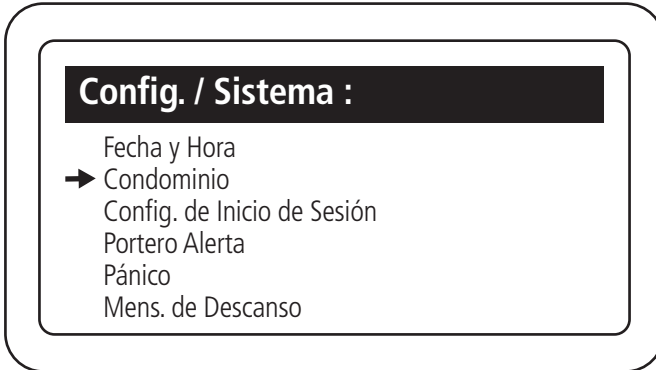
Config. / Fecha :

OK!

Fecha y hora cambiadas
con éxito

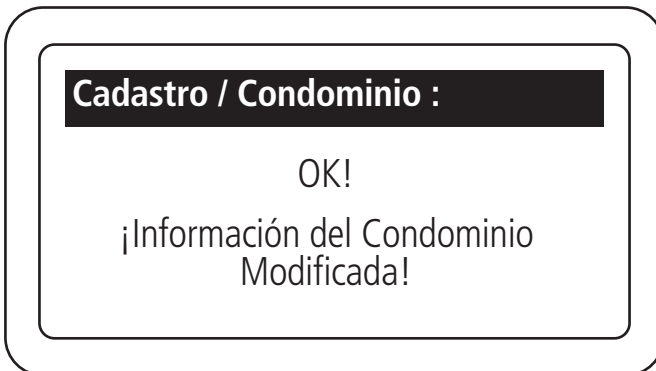
Condominio

Dentro del menú de Config. /Sistema puede agregar información sobre su condominio como se muestra:



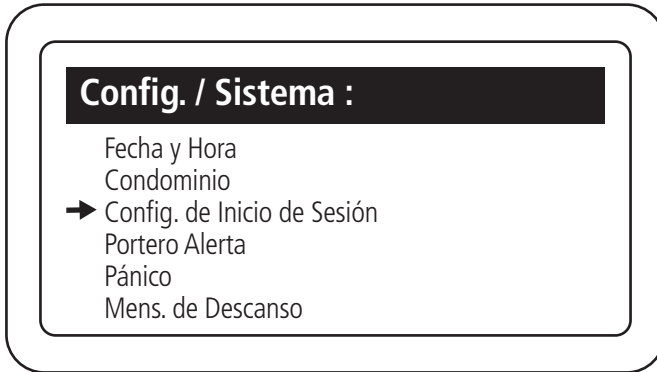
Preencher todos os dados do condominio (Responsável/Email, telefone, rua) e pressionar OK ou Enter

Obs.: os dados inseridos no campo nome do condomínio serão exibidos no display do MIP IP, quando ele estiver na tela inicial / repouso. O campo aceita 34 caracteres, porém apenas os 21 primeiros serão exibidos no display.

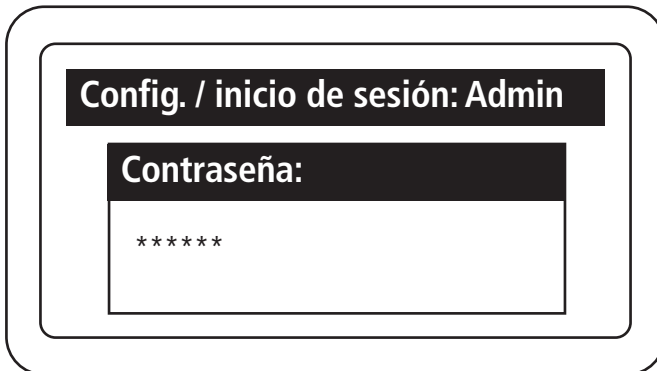
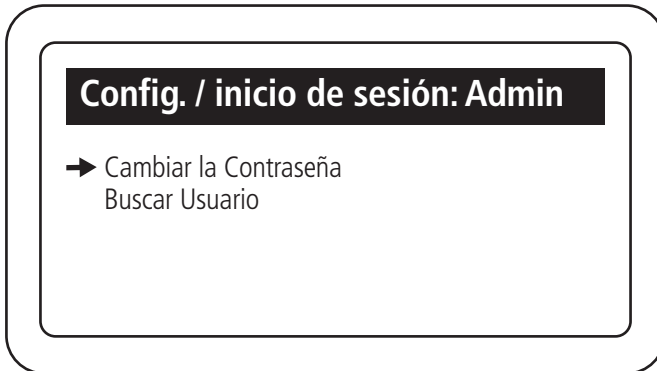


Configuración de inicio de sesión

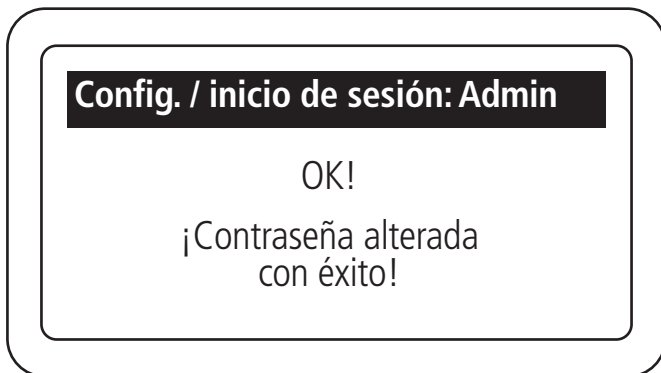
Para cambiar la contraseña de administrador o cambiar el nivel de permisos de los usuarios al sistema, es necesario realizar los siguientes pasos:



Cambia la contraseña



La contraseña predeterminada de fábrica es 123456 para cambiar, simplemente borre y escriba la nueva contraseña deseada y presione Enter (use un mínimo de 1 a 6 caracteres).

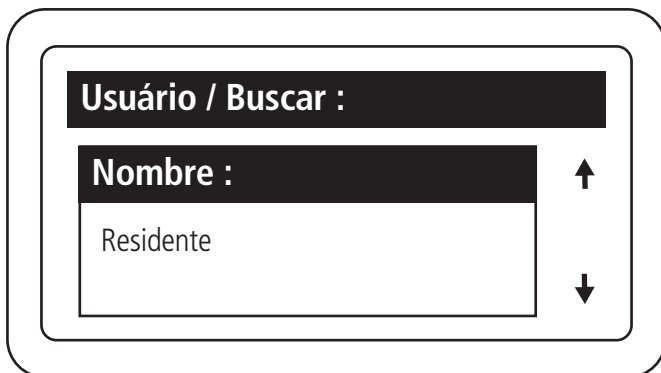
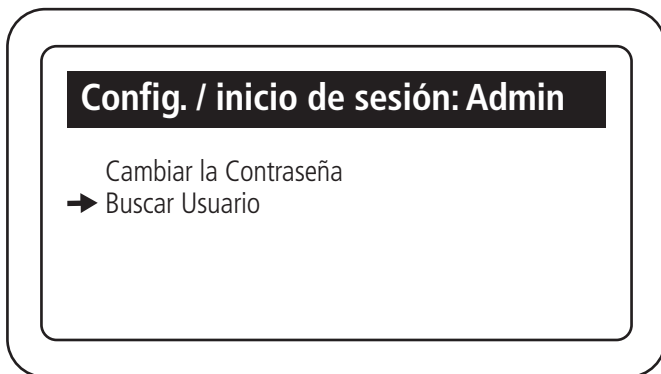


Buscar usuario

Es posible configurar usuarios ya registrados para acceder al menú principal de MIP y definir niveles de acceso para ellos, con un total de 4 niveles.

- » **Nivel 1:** usuario con permiso completo para el menú del sistema.
- » **Nivel 2:** usuario con permiso en la configuración de usuario y para ver eventos y notificaciones.
- » **Nivel 3:** usuario con permiso para ver eventos y notificaciones.
- » **Nivel 4:** usuario con permiso para ver eventos solamente.

Para configurar el inicio de sesión del usuario y definir/cambiar el nivel de permiso del usuario al menú del sistema, es necesario realizar los siguientes pasos:



Buscar cual residente tendrá acceso

Dpto | Nombre (01/01)

→ 102 - Residente

Config. / inicio de sesión:

Inicio de sesión:

Configurar el Inicio de Sesión de acceso al menú del MIP IP

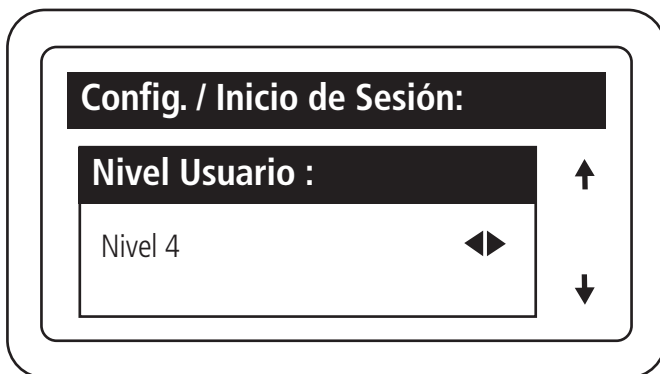
Config. / inicio de sesión:

Contraseña:

↑

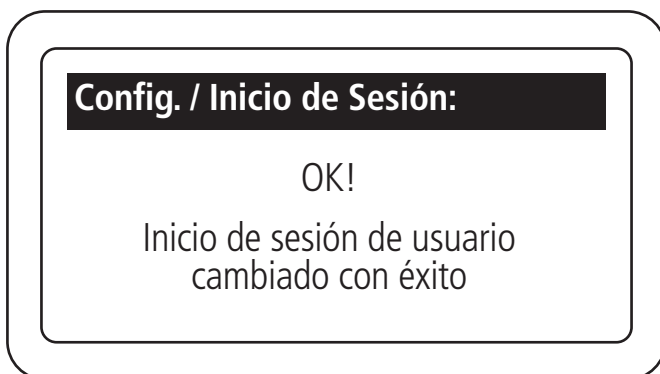
↓

Configurar la contraseña de acceso al menú del MIP IP



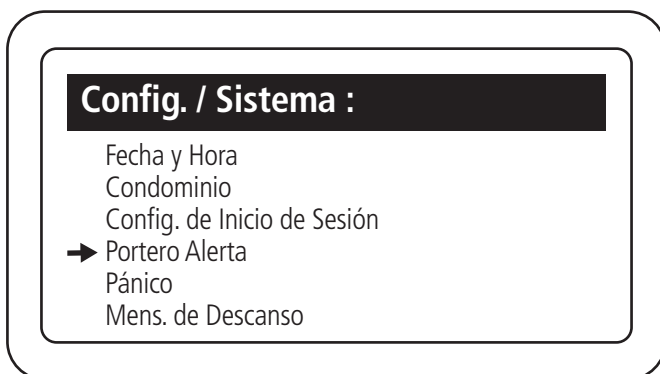
Establezca el nivel de acceso del usuario en el menú MIP IP y presione Enter para confirmar

Importante: si el usuario registrado es Nivel 1, será posible acceder al menú del MIP IP utilizando su llavero RFID (Mifare).



Portero Alerta

El portero alerta tiene como finalidad enviar alertas sonoras al portero (vigilante) en una franja horaria para mantenerlo alerta. Las alertas se realizan a intervalos regulares dentro del rango de tiempo configurado. Estos intervalos pueden ser de 15 minutos a 120 minutos y son configurados por el usuario, y la activación y desactivación de esta alerta genera un evento de dispositivo para que pueda ser monitoreado por el administrador del condominio. Para configurar alertas sonoras en un periodo de tiempo en el MIP, es necesario realizar los siguientes pasos:



Config. / Alerta Port.

Hora Inicial : ↑

22:00 ↓

Seleccionar la hora iniciar del portero alerta

Config. / Alerta Port.

Hora Final : ↑

06:00 ↓

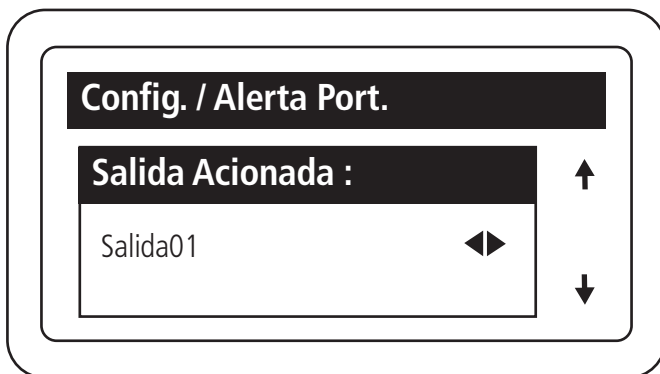
Seleccionar la hora final del portero alerta

Config. / Alerta Port.

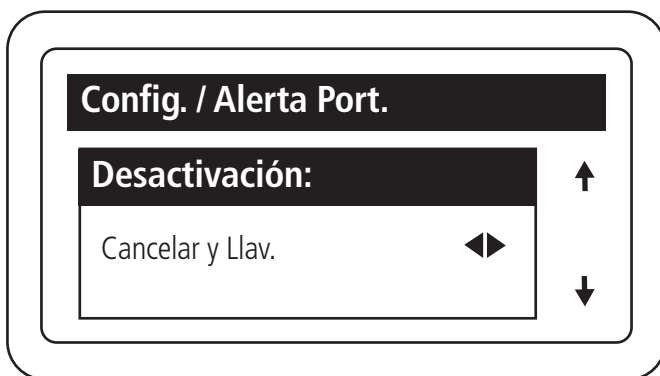
Intervalo : ↑

0 ◀▶ ↓

Establezca el intervalo de alerta audible dentro de un período de tiempo específico. Para deshabilitar esta alarma, simplemente configure el intervalo de tiempo igual a cero

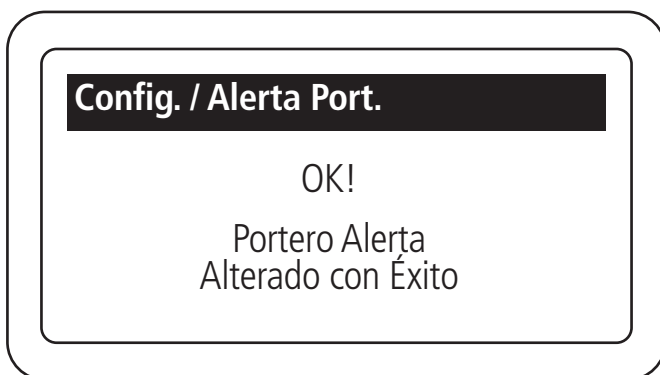


Seleccione qué salida debe activarse cuando el portero de alerta está activo



Seleccione si la alerta de portero se puede desactivar mediante cancelar y llavero, solo llavero o simplemente cancelar.

Presiona Enter para terminar



Función Pánico

La función Pánico se utiliza para alertar al portero (vigilante) de cualquier peligro en el condominio. La alerta solo puede ser visual (indica en la pantalla de Pánico, qué usuario la activó y qué dispositivo la activó) o también audible. El MIP registra esta función como un evento de pánico y será visible en el informe de este usuario como un disparador de coacción (o pánico).

El pánico se puede desencadenar de las siguientes maneras:

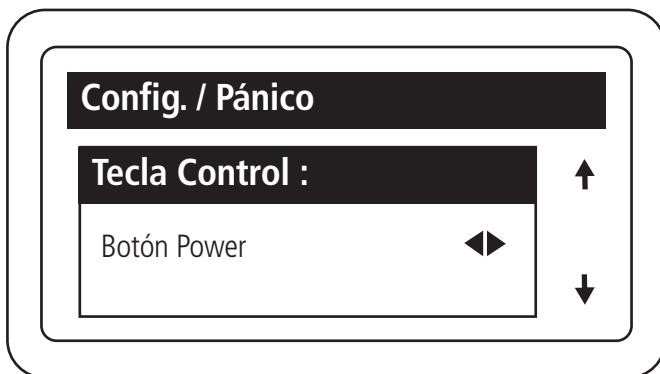
1. Configurando un dígito de pánico, situándose entre el tercer y cuarto dígito de la contraseña de apertura de la cerradura. Disponible en dispositivos XPE PLUS ID, XPE ID y XLT 1000 ID;
2. Configurar una tecla del control remoto para que se pulse durante un tiempo determinado configurado a continuación. Disponible en el dispositivo XRE 1000;
3. Establecer un tiempo para mantener el llavero RFID (Mifare) sobre el área de lectura del dispositivo. Disponible en dispositivos XPE PLUS ID y XLT 1000 ID.

Obs.: la función de pánico solo está disponible para usuarios de tipo residente. Los proveedores de servicios y los visitantes no pueden desencadenar el pánico.

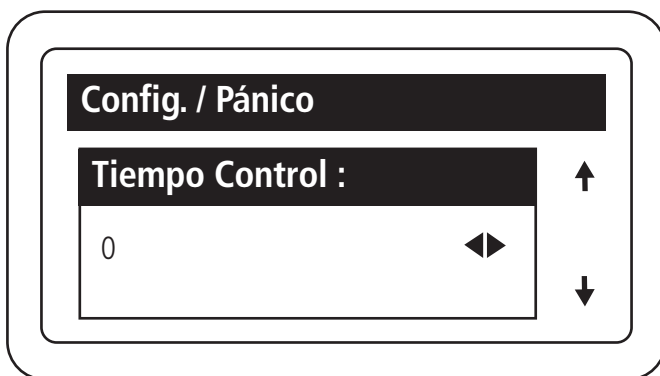
Para configurar la función Pánico en el sistema, es necesario realizar los siguientes pasos:



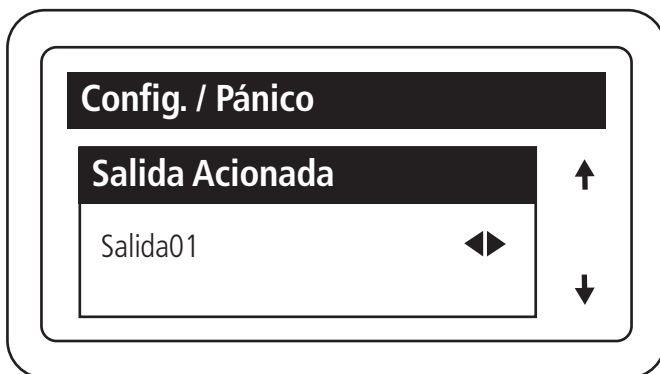
Establecer dígito de activación por contraseña



Configuración de la tecla de control remoto (Power/A/B)



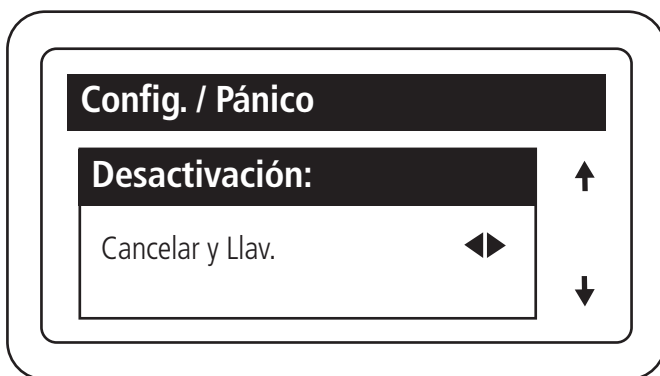
Define el tiempo que se necesita presionar el botón de control para que se active el pánico, siendo que Cero es deshabilitado.



Define qué salida MIP se activará cuando se active el pánico



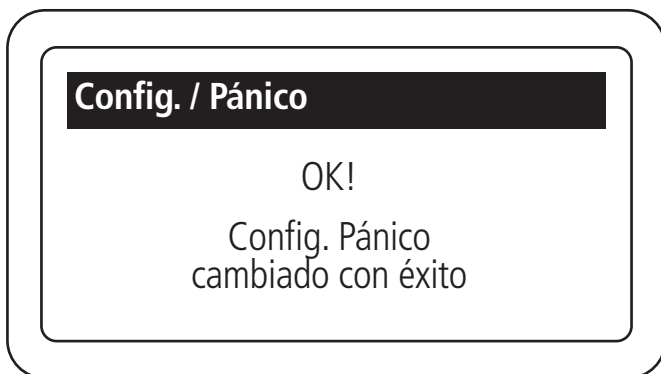
Defina si el pánico emitirá un pitido en el MIP IP o será silencioso.



Seleccione si el pánico se puede desactivar mediante cancelar y llavero, solo llavero o simplemente cancelar.

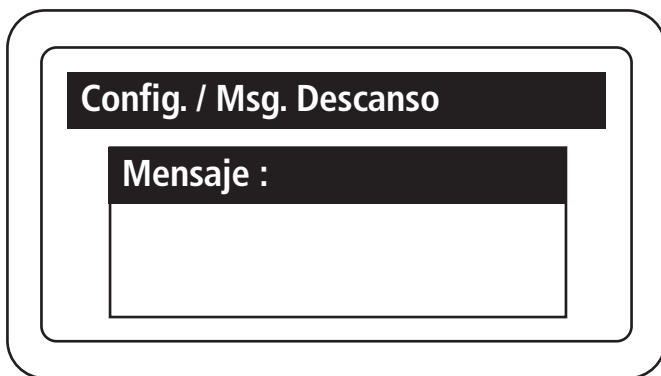
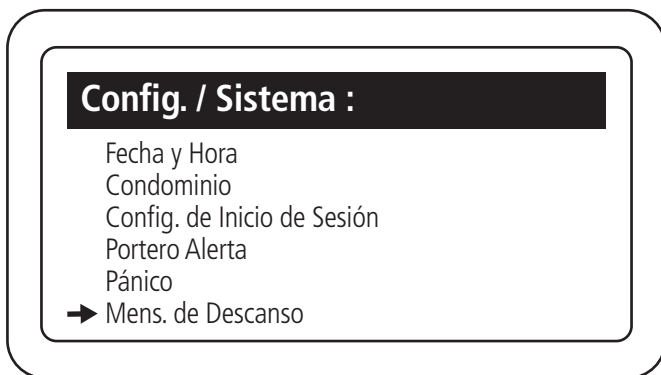


Informe el tiempo que el llavero RFID (Mifare) necesitará estar en el área de lectura del llavero para activar el pánico y presione Entrar para terminar.

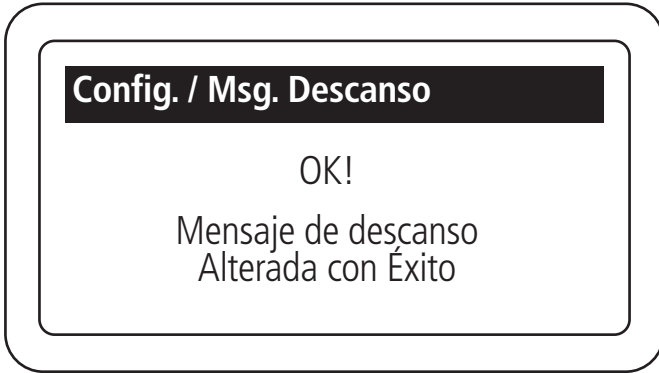


Mensaje de descanso

Este mensaje será visible en la pantalla del MIP, arriba del nombre del condominio, cuando este se encuentre en la pantalla inicial. Para configurar el mensaje de suspensión en la pantalla MIP, es necesario realizar los siguientes pasos::

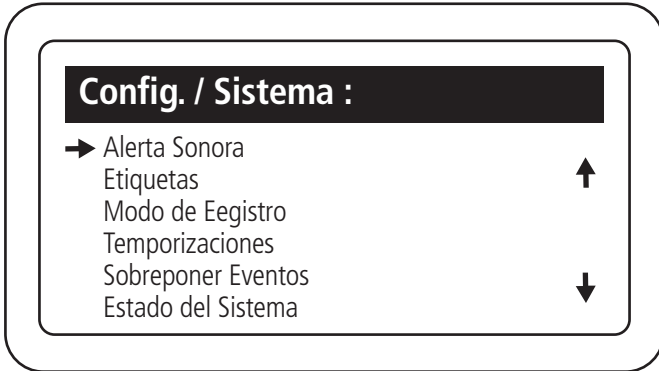


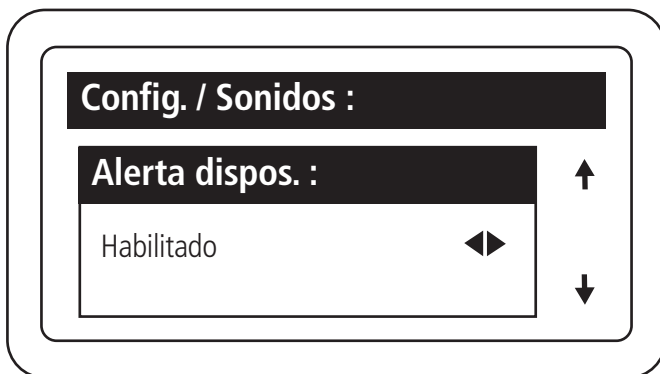
Defina qué mensaje aparecerá en la pantalla de inicio de MIP 1000 IP, luego de escribir el mensaje presione Enter (máximo 20 caracteres).



Alerta sonora

Para configurar la alerta sonora en el MIP IP y en los dispositivos (sonidos de confirmación/negación) es necesario realizar los siguientes pasos:





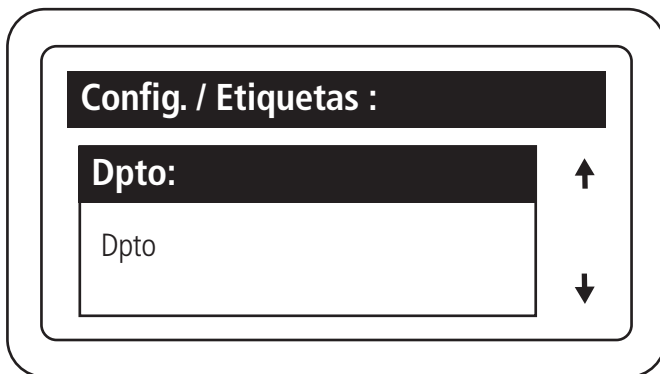
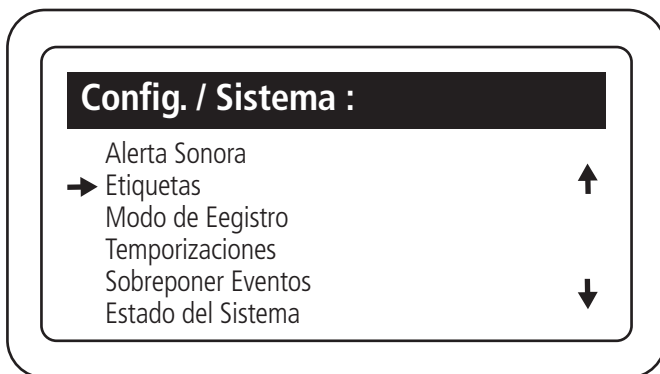
Presione Enter para actualizar la información definida

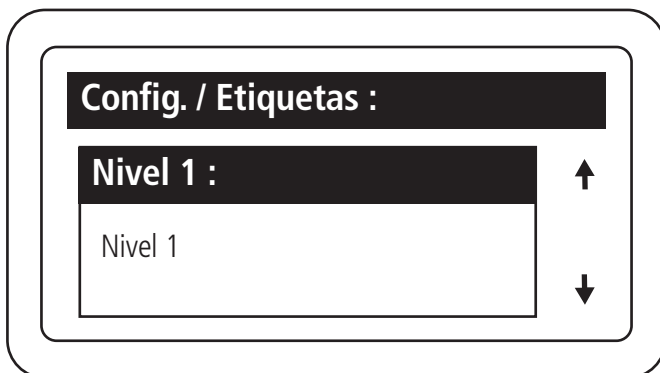
Configurar etiquetas

Es posible cambiar el nombre de algunas etiquetas del MIP IP. Ejemplos de utilización:

- » En un condominio de casas, la etiqueta dpto que se encuentra, por ejemplo, en la inclusión de un usuario se puede cambiar a cualquier texto de cuatro caracteres (ej.: casa).
- » Las etiquetas de nivel de permiso se pueden renombrar de la misma manera que la etiqueta dpto (por ejemplo, portero, síndico, instalador) y pueden tener hasta diez caracteres.

Para cambiar el nombre de las etiquetas, realice los siguientes pasos:

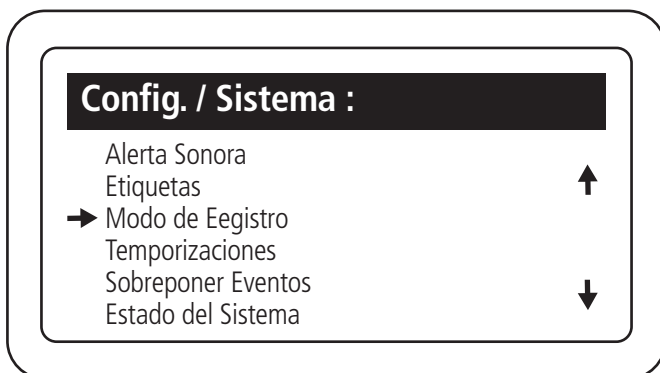




Obs.: con la flecha hacia abajo puede definir el nombre de todos los niveles del 1 al 4, luego de definir presione Enter para actualizar la información.

Configurar registro

Para cambiar el modo de registro del sistema de avanzado a básico (menos información en el registro de usuario y condominio) es necesario realizar los siguientes pasos.



Defina en qué modo registrará al usuario (básico o avanzado predeterminado de fábrica), luego de elegir presione Enter.

Configuración de temporizaciones

Es posible definir el tiempo, en segundos, que el evento se mostrará en la pantalla del MIP 1000 IP.

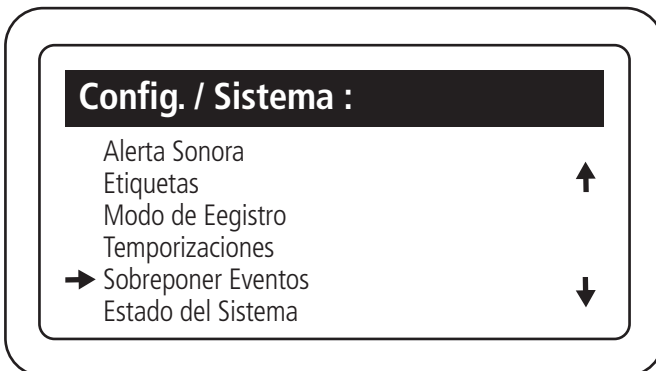


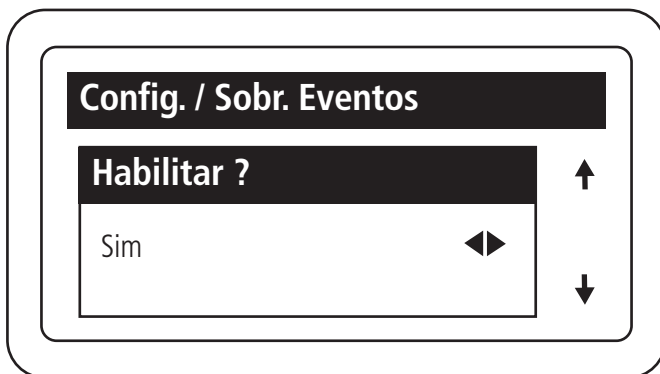
Configure el tiempo, en segundos, para que el evento se muestre en la pantalla del MIP

Obs.: presione Enter para finalizar los cambios.

Configuración de sobreponer eventos

Para habilitar/deshabilitar la función de superponer eventos (si ocurre un evento tras otro, el sistema no esperará el tiempo entre eventos para mostrar el nuevo, sino que superpondrá el actual sobre el anterior) es necesario realizar los siguientes pasos:

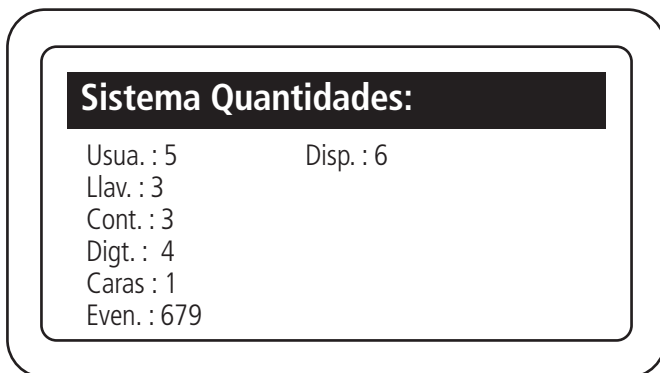
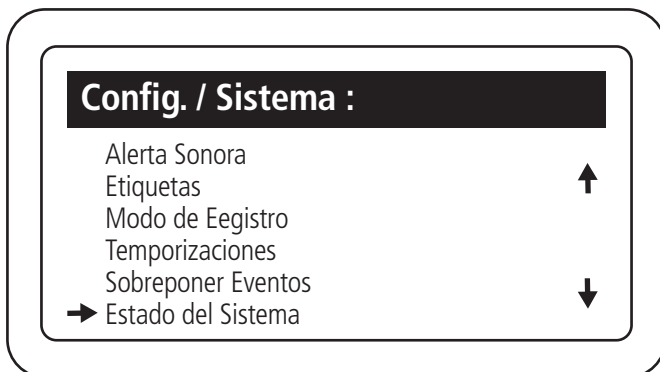




Después de seleccionar sí o no, presione Entrar para finalizar el proceso

Configuración del estado del sistema

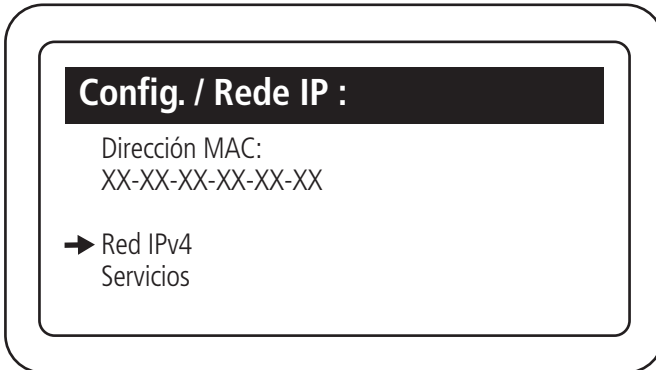
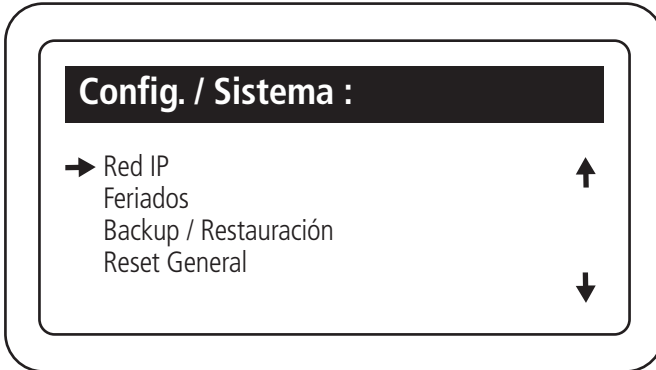
Para verificar la cantidad de usuarios, dispositivos, llaveros, controles, huellas digitales, caras y eventos que ya han sido registrados en el sistema, es necesario realizar los siguientes pasos:



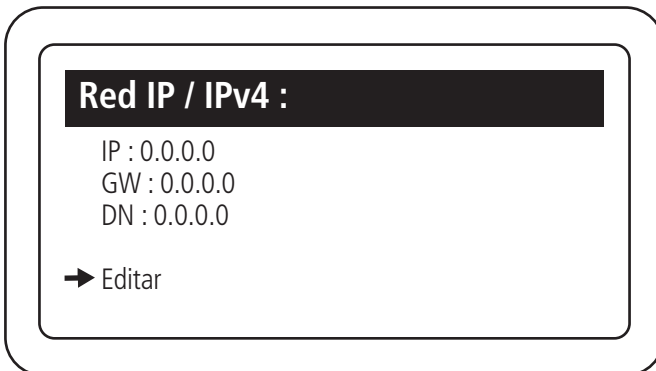
Presione ESC en el teclado USB o Cancelar en el teclado del MIP

Configuración de red IP

En el menú Red IP, es posible configurar y ver el estado actual del direccionamiento IP.



Seleccione IPv4 para configurar



Red IP / IPv4 :

Endereçamento : ↑

Dinámico: ◀▶ ↓

Configurar: dinámico, estático o deshabilitado

Cuando conecta el MIP 1000 IP a la red configura una IP automática.

Si ingresa IP estática, debe definirla de acuerdo con los siguientes pasos (configuración estática de IPV4):

Red IP / IPv4 :

Dirección IP: ↑

192.168.000.000 ↓

Red IP / IPv4 :

Máscara IP: ↑

255.255.255.0 ↓

Red IP / IPv4 :

Gateway IP : ↑

192.168.000.1 ↓

Red IP / IPv4 :

Servidor DNS : ↑

8.8.8.8 ↓

Servicios

En el menú Servicios, usted define cómo funciona la MIP IP en términos de comunicación con algún Software.

- » **SCA Server** : el MIP IP funciona como servidor y el software se encarga de realizar la conexión con el MIP IP (modo utilizado por el SGA IP).
- » **SCA Cliente**: MIP IP opera como un cliente y es responsable de realizar la conexión con el Software.

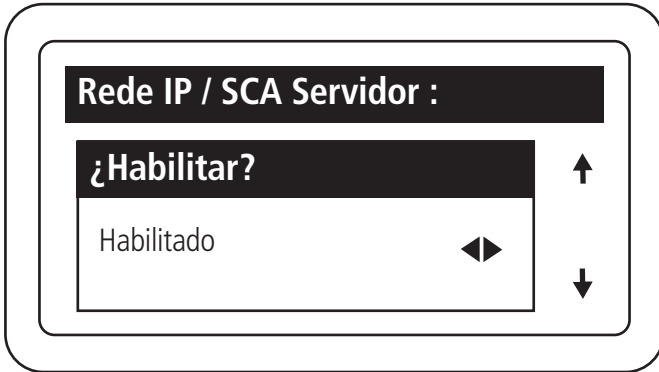
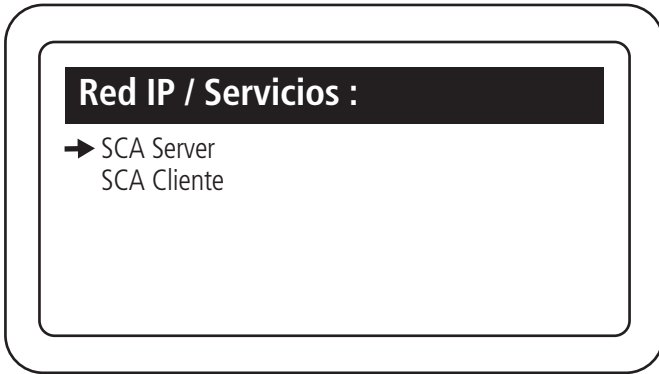
Obs.: como el MIP 1000 IP tiene dos conexiones, es posible dejar ambas opciones activas.

Config. / Red IP :

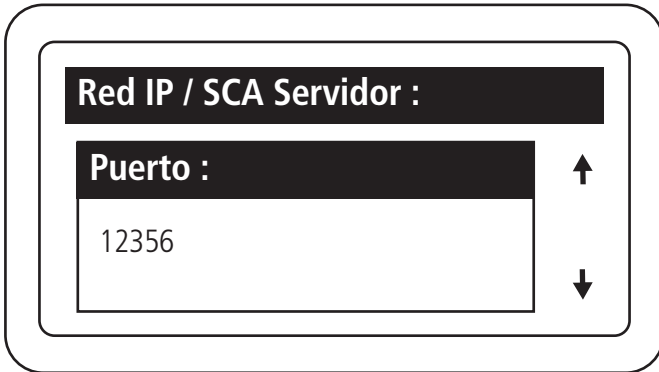
Dirección MAC:
XX-XX-XX-XX-XX-XX

Red IPv4
→ Servicios

Coloque la pantalla de SCA server y SCA cliente



Habilitar o deshabilitar la función



Puerto de comunicación estándar del MIP 1000 IP

Red IP / Servicios :

SCA Server
→ SCA Cliente

Red IP / SCA Cliente :

¿Habilitar?

Deshabilitado



Red IP / SCA Cliente :

Host

192.168.1.2



Configurar la IP de la red

Red IP / SCA Cliente :

Puerto :

09000

Feridos

El MIP sale con unos feriados configurados por defecto, si quiere cambiar, borrar o añadir nuevas fechas, debe seguir los siguientes pasos:

Config. / Sistema :

- Red IP
- Feriados
- Backup / Restauración
- Reset General

Nombre (01 / 12)

- 01/01 Confraternización Universal
- 21/04 Tiradentes
- 01/05 Día del Trabajo
- 07/09 Independencia
- 12/10 N Sra Aparecida
- 02/11 Finados

Para agregar/editar un feriado, siga los pasos a continuación:

Nombre (01 / 12)

15/11 Proclamación de la República

25/12 Navidad

00/00 Carnaval

00/00 Viernes Santo

00/00 Corpus Christi

→ -- / -- Añadir

Editar Feriados

Fecha :

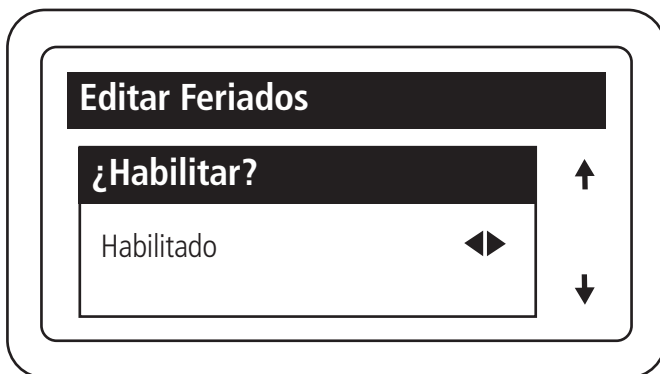
00 / 00



Editar Feriados

Nombre :

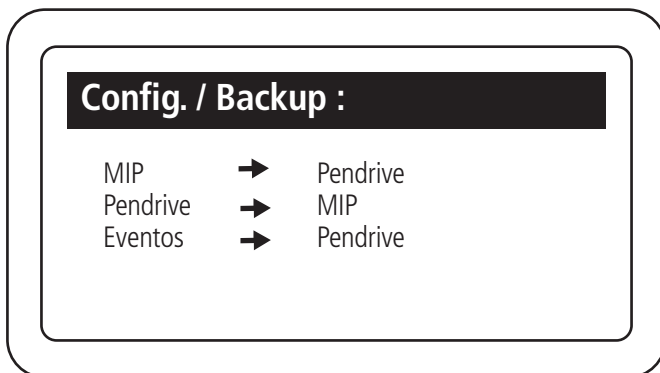
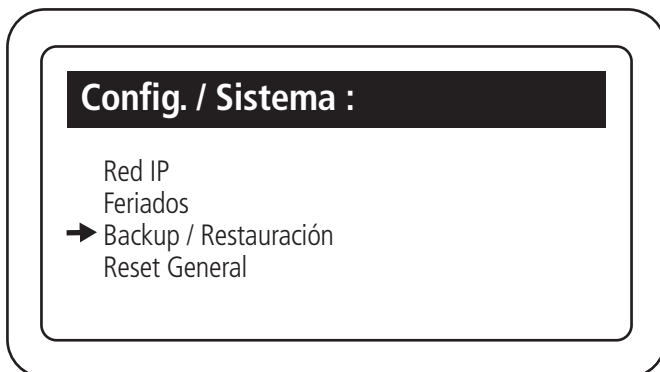




Presione Enter para finalizar el proceso

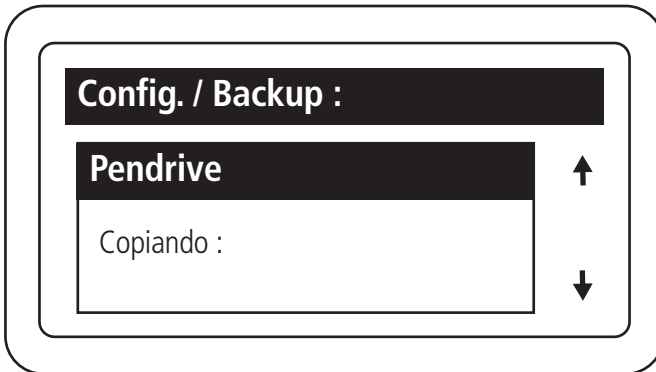
Configuración de backup y restauración

Este comando es el encargado de realizar el proceso de backup y restauración de los archivos del MIP 1000 IP. A continuación se muestra el detalle de cada una de las tres opciones:



1. MIP para Pendrive (presione Enter para seleccionar)

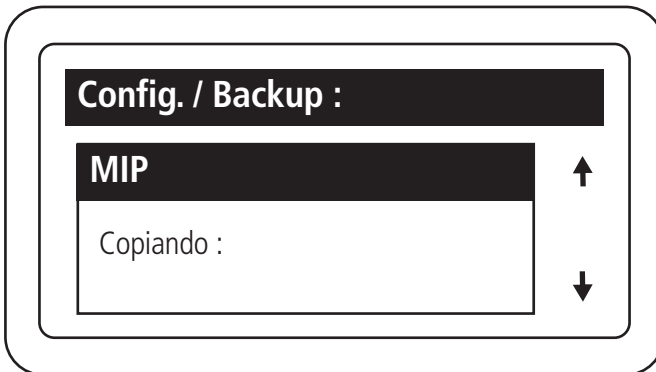
Realiza un backup de todas las configuraciones y los últimos 30.000 eventos registrados en el MIP 1000 IP en el Pendrive.



Obs.: se creará una carpeta MIPIP en la raíz del pendrive, con todos los archivos del MIP 1000 IP.

2. Pendrive a Mip (pulsa Enter para seleccionar)

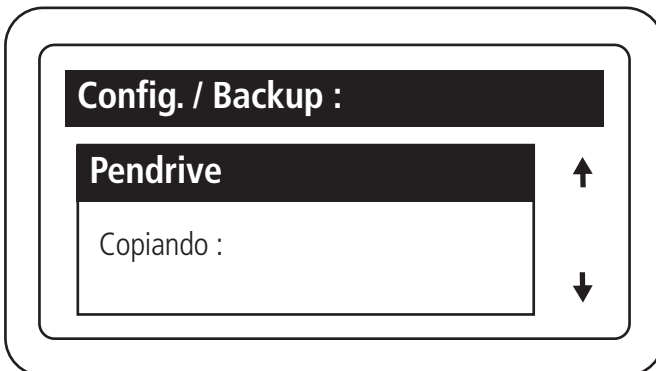
Restaura los archivos que se encuentran en el Pendrive al MIP 1000 IP.



Obs.: es necesario que todos los archivos del MIP 1000 IP estén en una carpeta, llamada MIPIP, en la raíz del pendrive.

3. Eventos para Pendrive (presione Enter para seleccionar)

Realiza un backup de todos los eventos registrados en el MIP 1000 IP en el Pendrive.



Obs.: se creará una carpeta de Eventos en la raíz del pendrive, con todos los archivos de eventos del MIP 1000 IP.



Importante: realiza copias de seguridad recurrentes para evitar que se pierdan datos en posibles cortes de energía.



Atención: antes de realizar el backup, verifique si el Pen drive está en la configuración a continuación:

Volume	Layout	Tipo	Sistema de ...	Status
— PEN DRIVE (F:)	Simple	Básico	FAT32	Íntegro (Ativo, Partição primária)

Reset general

Este comando se encarga de borrar toda la información registrada en el MIP, devolviendo todas las configuraciones a los valores predeterminados de fábrica.

Para realizar el reset general es necesario realizar los siguientes pasos:

Config. / Backup :

Red IP
Feriados
Backup / Restauración
→ Reset General

Config. / Backup :

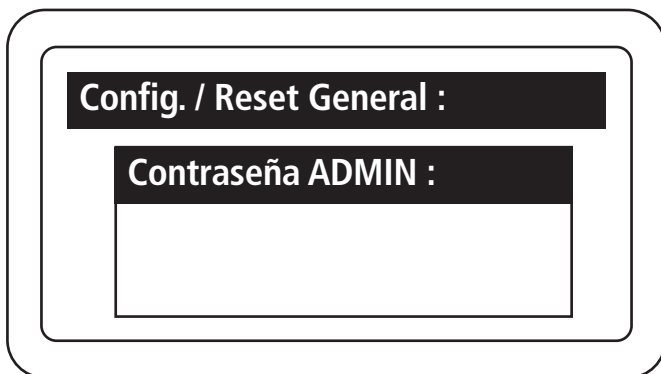
¿Reset?

Presione OK o Enter
para continuar

Config. / Reset General :

¿Está seguro?

Presione OK o Enter
para continuar



Después de ingresar la contraseña de administrador, el MIP volverá a la configuración de fábrica.

Salir

Presione Ok o Enter para volver a la pantalla de inicio del MIP IP.

6. Excepciones para dispositivos biométricos y faciales

El MIP 1000 tiene capacidad de almacenamiento para 4000 Huellas digitales y 4000 Caras, sin embargo los dispositivos integrados tienen diferentes limitaciones de capacidad, por lo que el registro en el MIP IP dependerá de la cantidad que soporten los dispositivos.

Ejemplo: Bio Inox SS 311 MF tiene una capacidad de 1499 huellas digitales y el lector de caras SS 3530 MF W tiene una capacidad de 1500 caras.

Para garantizar la integridad de los datos existentes en el MIP 1000 IP, realiza dos tipos de validación:

1. **Validación por dispositivo:** es la validación que realiza el MIP 1000 para verificar si un dispositivo puede o no recibir usuarios al dar de alta un nuevo dispositivo.

Ejemplo: hemos registrado más de 1499 huellas digitales en el MIP y estamos insertando un Bio Inox Plus SS 311 MF. Al finalizar el registro, aparecerá un mensaje en la pantalla del MIP advirtiéndole de esta situación.

Esto significa que se ha insertado el Bio Inox Plus SS 311 MF, pero ningún usuario tendrá acceso a él porque el número de huellas digitales en el MIP es mayor que su capacidad.

A través del menú de edición de usuarios es posible agregar usuarios individualmente para el dispositivo insertado.

2. **Validación por usuario:** es la validación que hace el MIP 1000 IP para verificar si un usuario tiene o no permiso para insertar una nueva huella digital o tener acceso a un dispositivo biométrico, al momento del registro o edición del usuario.

El MIP 1000 IP no permitirá que se agregue una nueva huella digital a un usuario cuando ese usuario tenga acceso a un dispositivo que haya alcanzado el límite de la capacidad de huellas digitales permitida.

7. Actualización de firmware

Para actualizar el firmware de su módulo inteligente de portería MIP 1000 IP, realice los siguientes pasos:

- 1° Paso:** retire la fuente de alimentación y con la ayuda de un destornillador Philips retire los cuatro tornillos en la parte posterior del MIP1000 IP para tener acceso a la placa del equipo;
- 2° Paso:** cierre el jumper JP1 en la placa base MIP 1000 IP;
- 3° Paso:** coloque la versión de firmware en un pendrive;
- 4° Paso:** encienda nuevamente la fuente de alimentación (aparecerá el mensaje indicándole que coloque el pendrive);
- 5° Paso:** coloque el pendrive en el conector lateral del MIP 1000 IP y espere el mensaje MIP 1000 OK! ¡Reiniciar!
- 6° Paso:** retire la fuente de alimentación, saque la unidad flash y el jumper JP1 y vuelva a colocar los tornillos en la parte posterior.
- 7° Paso:** encienda la fuente de alimentación y verifique, usando la barra espaciadora, si la versión de firmware se ha actualizado correctamente.

Atención: la versión debe llamarse mip-ip.bin, si es diferente no se realizará la actualización. Este archivo debe estar en la raíz del pendrive y debe estar formateado en fat32.

Póliza de garantía

Producido por:

Intelbras S/A - Industria de Telecomunicación Electrónica Brasileña

Rodovia BR 459, km 126, nº 1325 – Distrito Industrial – Santa Rita do Sapucaí/MG – 37538-400 – CNPJ 82.901.000/0016-03
soporte@intelbras.com | www.intelbras.com.br | www.intelbras.com/es

Industria de Telecomunicación Electrónica Brasileña S/A, se compromete a reparar o cambiar las piezas y componentes defectuosos del producto, incluyendo la mano de obra, o bien, el producto entero por un período de 1 año (3 meses por norma y 9 meses adicionales otorgados por el fabricante) a partir de la fecha de compra. Para hacer efectiva esta garantía, solamente deberá presentarse el producto en el Centro de Servicio, acompañado por: esta póliza debidamente sellada por el establecimiento en donde fue adquirido, o la factura, o el recibo, o el comprobante de compra, en donde consten los datos específicos del producto. Para las ciudades en donde no hay un centro de servicio, deberá solicitarse una recolección mediante el servicio de paquetería asignado por Intelbras, sin ningún costo adicional para el consumidor. El aparato defectuoso debe ser revisado en nuestro Centro de Servicio para evaluación y eventual cambio o reparación. Para instrucciones del envío o recolección favor comunicarse al Centro de Servicio:

El tiempo de reparación en ningún caso será mayor de 30 días naturales contados a partir de la fecha de recepción del producto en el Centro de Servicio.

ESTA GARANTÍA NO ES VÁLIDA EN LOS SIGUIENTES CASOS:

- a. Cuando el producto ha sido utilizado en condiciones distintas a las normales.
- b. Cuando el producto no ha sido instalado o utilizado de acuerdo con el Manual de Usuario proporcionado junto con el mismo.
- c. Cuando el producto ha sido alterado o reparado por personas no autorizadas por Industria de Telecomunicación Electrónica Brasileña.
- d. Cuando el producto ha sufrido algún daño causado por: accidentes, siniestros, fenómenos naturales (rayos, inundaciones, derrumbes, etc.), humedad, variaciones de voltaje en la red eléctrica, influencia de naturaleza química, electromagnética, eléctrica o animal (insectos, etc.).
- e. Cuando el número de serie ha sido alterado.

Con cualquier Distribuidor Autorizado, o en el Centro de Servicio podrá adquirir las partes, componentes, consumibles y accesorios.

Datos del producto y distribuidor.

Producto:

Colonia:

Marca:

C.P.:

Modelo:

Estado:

Número de serie:

Tipo y número de comprobante de compra:

Distribuidor:

Fecha de compra:

Calle y número:

Sello:

Términos de garantía

Se expresa que esta garantía contractual se otorga bajo las siguientes condiciones:

Nombre del cliente:

Firma del cliente:

Número de factura:

Fecha de compra:

Modelo:

Número de serie:

Revendedor:

1. Todas las partes, piezas y componentes del producto están garantizados contra cualquier defecto de fabricación, que pueda presentar, por un período de 1 (un) año, siendo 90 (noventa) días de garantía legal y 9 (nueve) meses de garantía contractual, contado desde la fecha de compra del producto por parte del Consumidor, según consta en la factura de compra del producto, la cual es parte integrante de estos Términos en todo el territorio nacional. Esta garantía contractual incluye el intercambio gratuito de partes, piezas y componentes que presenten un defecto de fabricación, incluyendo los gastos con la mano de obra empleada en esta reparación. Si no se encuentra ningún defecto de fabricación, pero vicios que surgen de un uso inadecuado, el Consumidor correrá con estos gastos.
2. La instalación del producto debe realizarse de acuerdo con el Manual del Producto y/o la Guía de Instalación. Si tu producto requiere instalación y configuración por parte de un técnico calificado, busca un profesional adecuado y especializado, y los costos de estos servicios no están incluidos en el valor del producto.
3. Una vez que se encuentre el defecto, el Consumidor deberá comunicarse inmediatamente con el Servicio Autorizado más cercano en la lista proporcionada por el fabricante; solo estos están autorizados a examinar y remediar el defecto durante el período de garantía aquí estipulado. Si esto no se respeta, esta garantía perderá su vigencia, ya que se caracterizará como una violación del producto.
4. En el caso de que el Consumidor solicite atención domiciliaria, deberá acudir al Servicio Autorizado más cercano para consultar el costo de la visita técnica. Si se encuentra la necesidad de retirar el producto, los gastos resultantes, como el transporte y la seguridad de ida y vuelta del producto, quedan a cargo del Consumidor.
5. La garantía perderá totalmente su vigencia en el caso de cualquiera de las siguientes hipótesis: a) si el defecto no es un defecto de fabricación, sino causado por el Consumidor o por terceros ajenos al fabricante; b) si el daño al producto proviene de accidentes, agentes de la naturaleza (rayos, inundaciones, deslizamientos de tierra, etc.), humedad, tensión en la red eléctrica (sobretensión provocada por accidentes o fluctuaciones excesivas en la red), instalación/uso en desacuerdo con el manual del usuario o debido al desgaste natural de partes, piezas y componentes; c) si el producto ha sido influenciado por una naturaleza química, electromagnética, eléctrica o animal (insectos, etc.); d) si el número de serie del producto ha sido alterado o borrado; e) si el dispositivo ha sido manipulado.
6. Esta garantía no cubre la pérdida de datos, por lo tanto, se recomienda que el Consumidor realice regularmente copias de seguridad de los datos contenidos en el producto, en su caso.
7. Intelbras no es responsable de la instalación de este producto, y también de cualquier intento de fraude y/o sabotaje de sus productos. Mantén actualizadas las actualizaciones de software y aplicaciones utilizadas, si corresponde, así como las protecciones de red necesarias para protegerse contra intrusiones (hackers). El equipo está garantizado contra adiciones dentro de sus condiciones normales de uso, y es importante tener en cuenta que, por ser un equipo electrónico, no está libre de fraudes y estafas que puedan interferir en su correcto funcionamiento.
8. Deseche adecuadamente su producto después de su vida útil: entréguelo en los puntos de recolección de productos eléctricos y electrónicos, en un centro de asistencia técnica autorizado Intelbras o consulte nuestro sitio web www.intelbras.com.br y support@intelbras.com.br o (48) 2106-0006 o 0800 7042767 para más información.

Siendo estas las condiciones de estos Términos de Garantía complementario, Intelbras S/A se reserva el derecho a modificar las características generales, técnicas y estéticas de sus productos sin previo aviso.

Todas las imágenes de este manual son ilustrativas.

Producto beneficiado por la Legislación Informática.

intelbras



hable con nosotros

Atención al cliente:  +55 (48) 2106 0006

Soporte vía e-mail: soporte@intelbras.com

Producido por:

Intelbras S/A – Indústria de Telecomunicação Eletrônica Brasileira

Rodovia BR 459, km 126, nº 1325 – Distrito Industrial – Santa Rita do Sapucaí/MG – 37538-400

CNPJ 82.901.000/0016-03 – www.intelbras.com.br | www.intelbras.com/es

02.25

Fabricado en Brasil