

intelbras

Manual do usuário

MIP 1000



MIP 1000 (Módulo Inteligente de Portaria) Controlador, cadastrador e configurador de acessos

Parabéns, você acaba de adquirir um produto com a qualidade e a segurança Intelbras.

O MIP 1000 foi desenvolvido para ser o gerenciador de acessos condominial, fazendo o cadastro, registro, gerenciamento de pessoas e veículos nos mais variados modelos de condomínio. Seu papel é fornecer uma interface simples e funcional que permite controlar o horário que cada pessoa ou veículo entrou ou saiu, facilitar a abertura de portas/portões, verificar se portas estão abertas através de sensores e até definir quais usuários terão acesso a cada parte do condomínio.

Seu display exibe, por exemplo, eventos de acesso e notificações de problemas nos dispositivos. O equipamento possui outros serviços como alerta de porteiro, pânico, busca simplificada de eventos, etc.

Estas funções serão demonstradas durante a leitura deste manual.

Obs.: » *A partir da versão 170405 esse equipamento tem o suporte ao funcionamento v2. Permitindo a configuração dos dispositivos (com suporte ao modo autônomo), para que façam a abertura e o registro de eventos sem a necessidade de comunicação com o MIP. Caso o seu equipamento não tenha essa funcionalidade, procure informações para atualização, além das facilidades já encontradas na V2.*

» *A partir da versão 180101 esse equipamento tem suporte para integração de dispositivos biométricos e placas controladoras de antenas TAG, além do funcionamento na v2.*

Cuidados e segurança

- » Não instale em locais úmidos, próximo a fonte de calor ou vibração.
- » Não instale próximo a televisores ou equipamentos que operem em radiofrequência.
- » Evite instalar em locais onde há incidência direta de sol.
- » Não instale em locais onde será necessário o movimento constante do MIP, pois isso evita problemas de quebra da fiação conectada no MIP.

Índice

1. Especificações técnicas	5
2. Características	5
3. Produto	6
3.1. Módulo inteligente de portaria MIP	7
4. Instalação	9
4.1. Barramento de comunicação	9
4.2. Exemplos de instalação	10
4.3. Procedimento de instalação	12
4.4. Conexões do MIP	13
5. Operação/Programação	14
5.1. Descrição de ícones	14
5.2. Inicializando o sistema	15
5.3. Telas de eventos	16
5.4. Teclas de acesso rápido	18
5.5. Níveis de acesso para configuração e consulta de informações	23
5.6. Cadastro	24
5.7. Eventos	71
5.8. Notificações	75
5.9. Configuração de teclas	77
5.10. Configuração do sistema	81
5.11. Sair	105
6. Exceções para dispositivos biométricos	105
6.1. Validação por dispositivo	105
6.2. Validação por usuário	106
Termo de garantia	107

1. Especificações técnicas

Alimentação	5 Vdc / 2 A, acompanha fonte externa
	Tipo A: para conexão de teclado USB
Portas USB	Tipo B: para conexão com um computador através de cabo USB tipo AB (padrão impressoras) com a distância máxima de 1,5 metros.
Saídas de acionamento	Duas saídas de relés (contato seco) padrão NA, 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, sensores de passagem, etc.
Barramento serial RS485	SERIAL_1: utilizado para cadastros dos dispositivos no sistema SERIAL_2: utilizado para comunicação do sistema, permite até 16 (ou 24 na versão 170405 ou superior) dispositivos em rede
Distância máxima dos dispositivos RS485	Até 1.000 metros com cabos de par trançados de boa qualidade ou barramento com impedância máxima de 250 ohms
Display LCD	64 × 128 pontos azul com backlight
Peso	335,0 g
Dimensões (L × A × P)	132 × 109 × 168 mm
Consumo em repouso	1,1 W
Condições ambientais	Temperatura: -10 °C a 60 °C Umidade relativa do ar: 10 a 90% (sem condensação)
Garantia	1 ano

2. Características

- » Cadastro das informações de acesso do morador nos dispositivos para que os mesmos funcionem de forma autônoma.
- » Registro e geração (através do SGA 1000 por exemplo) de relatórios de acessos.
- » Gerenciamento de forma individual dos controles XTR 1000, senhas de usuário, chaveiros RFID (Mifare) de proximidade e digitais (MIP a partir da versão 180101).
- » Porta de comunicação USB (padrão A) para teclado externo (não incluso) facilitando o uso do sistema, principalmente nos cadastros.
- » Comunicação direta com computador através da USB (padrão B) para uso em conjunto com o software.
- » Backup das informações do sistema, no Micro SD do MIP, todos os dias às 03:05 horas. O MIP armazena o backup individual e identificado dos últimos trinta dias, sendo possível recuperá-lo de um dia específico.
- » Backup das configurações do sistema, dos dados cadastrais e dos registros de acesso através do software.
- » Módulo de portaria com identificação do morador quando o mesmo acionar seu elemento (controle, chaveiro, senha ou digitais) de acesso.
- » Cadastro com foto de usuário (foto disponível somente no software SGA 1000).
- » Armazena até cem mil eventos com data e hora.
- » Permite o cadastro de até 4.000 chaveiros RFID (Mifare), 4.000 controles XTR 1000, 4.000 digitais e 4.000 usuários (com uma senha por usuário), totalizando 16.000 elementos de acesso.
- » Indica ao porteiro sobre o status da bateria dos controles remotos.
- » Software para cadastro e gerenciamento das informações de acesso (SGA 1000).
- » Duas saídas relés (contato seco) padrão NA (normalmente aberta) para cargas de até 24 Vdc / 1 A. Podem ser alteradas para funcionarem como NF (normalmente fechada), basta configurar os jumpers *JP3* e *JP4* na placa base do MIP. Estas saídas funcionam de forma diferente, sendo que a *SAIDA_1* é retentiva por tempo configurado, podendo ser utilizada para acionar um portão de garagem, uma zona da central de alarme, entre outras coisas, enquanto a *SAIDA_2* é pulsativa, função esta utilizada para o acionamento de fechaduras eletromecânicas, porém, para isso é necessário utilizar uma fonte externa.

3. Produto

O Módulo Inteligente de Portaria (MIP) será o ponto de interação com o porteiro (vigilante), pois o mesmo ficará sempre ao alcance para liberação de acesso, acionamento das saídas dos dispositivos, programação/bloqueio de novos usuários e visualização dos eventos de entrada/saída. O porteiro irá interagir com esse equipamento através de um display LCD e teclado.

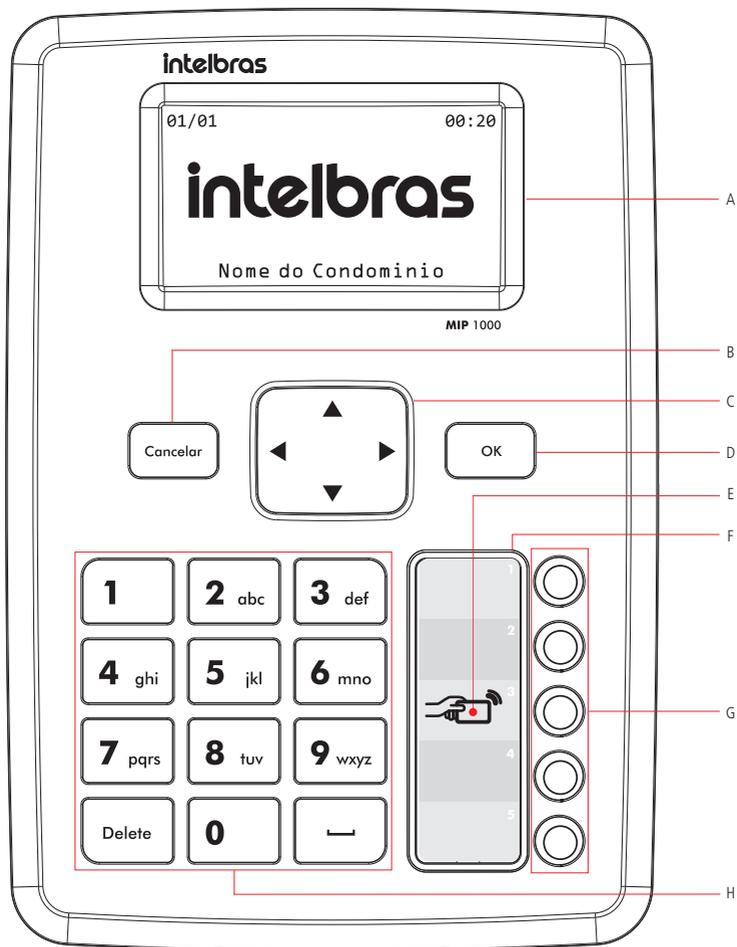
Considerando o MIP o gerenciador do sistema, todos os dados de usuários e dispositivos serão previamente cadastrados nele através de sua interface ou através do software instalado no computador (SGA 1000 por exemplo). Durante o funcionamento do sistema, os eventos serão registrados (armazenados) e ficarão disponíveis para consultas a qualquer momento via produto ou software.

O produto possui duas portas USB, sendo uma para conexão com um teclado USB (padrão ABNT) e outra para comunicação com um computador, entretanto, ao utilizar as duas portas USB ao mesmo tempo, apenas a porta de comunicação com o computador irá funcionar, sendo assim o teclado externo ficará inoperante enquanto o MIP estiver conectado ao computador. Possui duas saídas para acionamentos de cargas (ex.: fechaduras ou portões), duas entradas de sensores (ex.: sensor de porta aberta), dois barramentos seriais para comunicação com os dispositivos do sistema e uma entrada de alimentação externa.

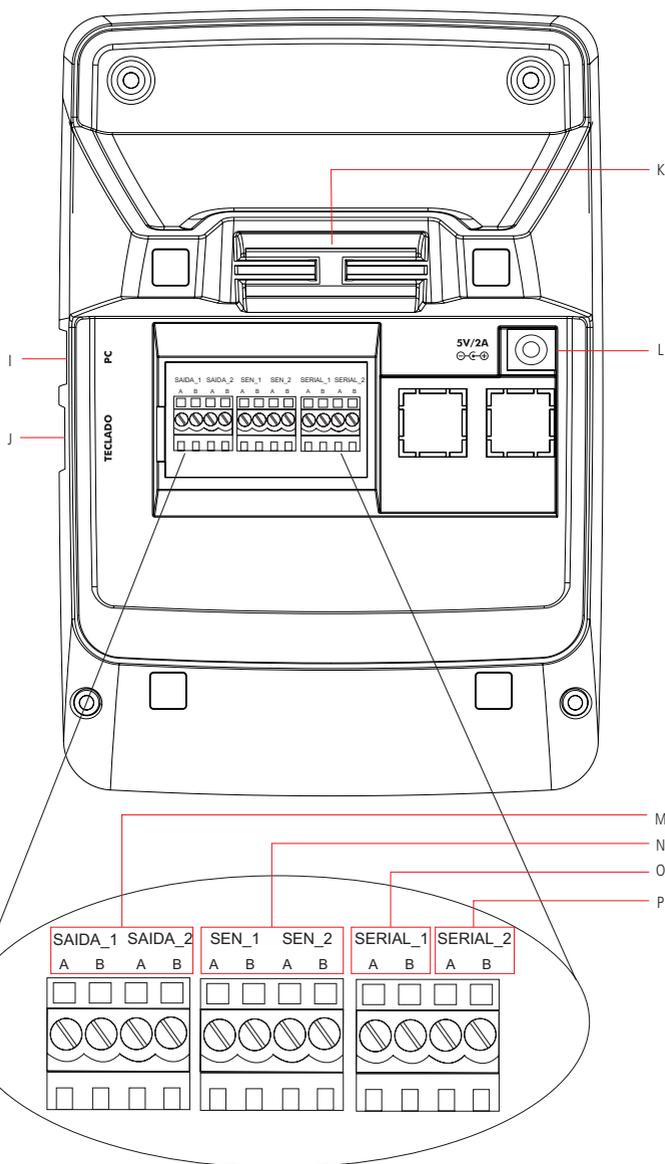
Esse produto, a partir da versão 170405, ganhou a capacidade de configurar seus dispositivos (também atualizados para o suporte autônomo) para que os mesmos possam fazer a abertura de seus acionamentos de forma independente do MIP. Dessa forma, os dispositivos tem a capacidade de identificar e tomar a decisão sozinhos de fazer a abertura. Se o dispositivo autônomo estiver conectado ao MIP através de seu barramento, o evento de abertura será enviado imediatamente para o MIP para que o mesmo possa fazer o registro deste evento na sua base de dados local. Contudo, se o dispositivo estiver impossibilitado de se comunicar com o MIP, o mesmo fará a abertura do acionamento e armazenará o evento dentro do mesmo até que a comunicação com o MIP seja refeita.

A partir da versão 180101, este produto possui suporte a comunicação com os dispositivos Bio Inox Plus SS 311 MF e CT 500 1P através do barramento RS485, possibilitando assim gerenciá-las pelo MIP 1000, além das facilidades já encontradas na V2.

3.1. Módulo inteligente de portaria MIP



- A. Display LCD
- B. Tecla *Cancelar*
- C. Teclas de navegação
- D. Tecla de confirmação: *Ok*
- E. Região de cadastros dos chaveiros RFID (Mifare)
- F. Etiqueta de identificação das teclas de acionamento
- G. Teclas de acionamento (programáveis)
- H. Teclado de 12 teclas para entrada de dados



I. USB para conexão com o PC

J. USB para conexão com o teclado (padrão ABNT)

K. Passagem dos cabos

L. Entrada Fonte de alimentação (5 Vdc / 2 A)

M. Saídas de acionamento contato seco, sendo a SAIDA_1 retentiva e a SAIDA_2 pulsativa. As duas são temporizadas

N. Entradas de sensores

O. SERIAL_1: barramento RS485 para cadastro de dispositivos no sistema

P. SERIAL_2: barramento RS485 para conexão dos dispositivos do sistema durante funcionamento

4. Instalação

4.1. Barramento de comunicação

É muito importante a leitura deste tópico para compreender claramente a forma correta de instalação do sistema de controle de acessos condominial, incluindo o módulo inteligente de portaria (MIP) e os demais dispositivos do sistema que devem ser corretamente instalados no barramento.

O barramento é a conexão física entre o MIP e todos os outros dispositivos através de cabos. Por estes cabos será feita a comunicação dos dispositivos para registro dos acessos. Para ter um barramento com boa qualidade devemos seguir as recomendações abaixo:

1. Cada barramento deverá ter apenas um MIP 1000, sendo este utilizado nas configurações dos usuários, dos elementos de acessos (controles, chaveiros, senhas e digitais) e dos dispositivos, além de realizar o registro dos eventos e informar as notificações do sistema;

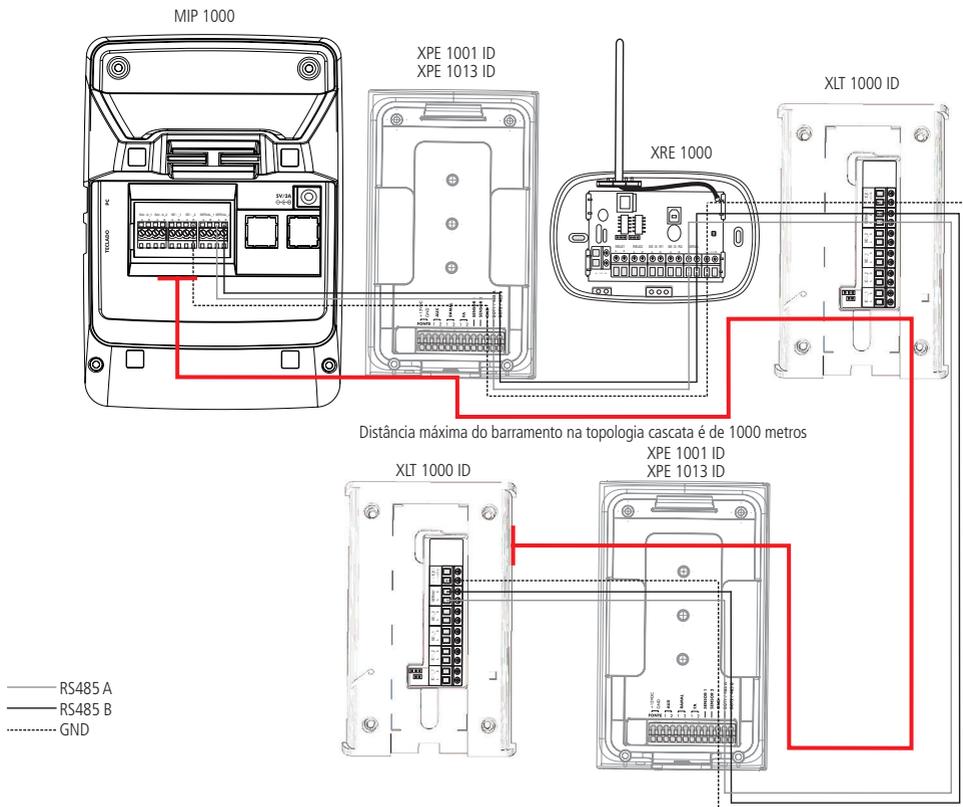
Importante: após as configurações acima, caso o MIP seja desconectado do barramento, os dispositivos continuarão liberando o acesso e armazenando internamente os eventos e, ao retornar o MIP para o barramento, os dispositivos sincronizarão com o mesmo todos os eventos registrados quando estavam em modo *Time Out*.

2. Cada barramento poderá ter de 1 até 24 dispositivos (XRE 1000, XLT 1000 ID, XPE 1013 ID, XPE 1001 ID, etc.) conectados no barramento *SERIAL_2* do MIP 1000, sendo o barramento *SERIAL_1* utilizado apenas no momento de cadastro dos dispositivos;
3. O barramento tem dois fios. Para ambientes com interferência recomenda-se um cabo blindado, com a blindagem ligada no *GND* do MIP e dos dispositivos;
4. No barramento, a referência *SERIAL_A* do MIP deve ser ligada à referência *SERIAL_A* de todos os dispositivos, o mesmo deve ser feito para a referência *SERIAL_B*;
5. Todos os dispositivos devem ser cadastrados no MIP;
6. As ligações devem ser preferencialmente em série (topologia cascata), sempre de um dispositivo para outro;
7. A distância máxima entre o MIP até o último dispositivo deve ser menor que 1.000 metros (verificar os exemplos de instalação) e a impedância total do barramento não deve superar 250 ohms;
8. Deve-se utilizar preferencialmente cabos de pares trançados ou cabos de telefonia para barramentos de pequenas distâncias (até 100 metros);
9. Como referência de instalação, o cabeamento a ser utilizado para conseguir um barramento com distância de até 1.000 metros, deve conter as seguintes especificações:
 - » Cabo de par trançado balanceado e blindado.
 - » Bitola de 22 AWG a 24 AWG.
 - » Resistência do condutor de 14,7 a 17,5 ohm / 304,8 m.
 - » Resistência da blindagem de 2,8 a 2,9 ohm / 304,8 m.
 - » Capacitância diferencial de 11 pF / 30,48 cm.
 - » Comprimento da trança de 6,35 cm.
 - » As conexões (emendas) dos dispositivos com o barramento RS485 devem ser realizadas com solda de boa qualidade.

É aconselhável o uso de nobreaks ou similar para evitar que quedas de energia não paralise o sistema, uma vez que todos os acessos são liberados através do MIP até a versão anterior da 170405. Em versões acima desta, com os dispositivos em modo *Autônomo*, não é necessário a presença do MIP para a abertura/registo dos acionamentos dos dispositivos.

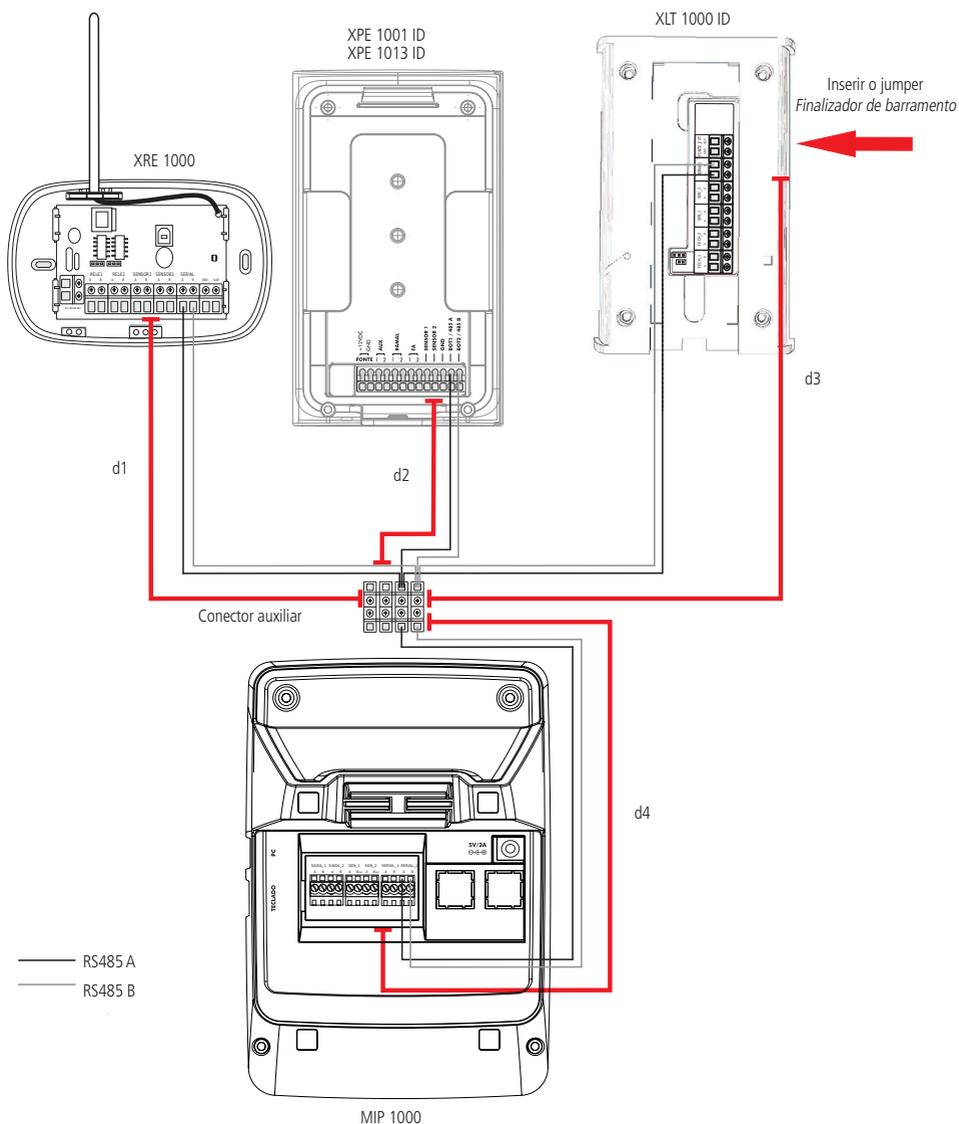
4.2. Exemplos de instalação

Barramento com dois fios e blindagem ligada no GND, utilizando a topologia cascata



Obs.: utilizando a topologia cascata, este dispositivo pode ser ligado a uma distância de até 1.000 metros do MIP ou em cabeamento que não ultrapasse 250 ohms, desde que utilizados cabos de boa qualidade, como informado na recomendação 9 do item 4.1 Barramento de comunicação.

Barramento com dois fios utilizando a topologia estrela

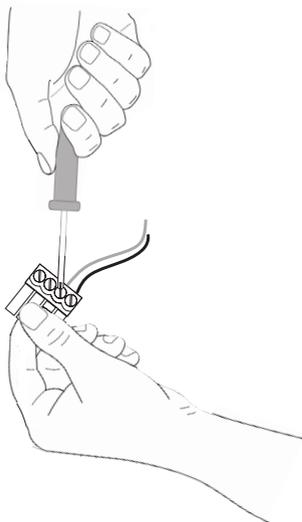


Distância máxima do barramento na topologia estrela é $(d1+d2+d3+d4) = 1000$ metros

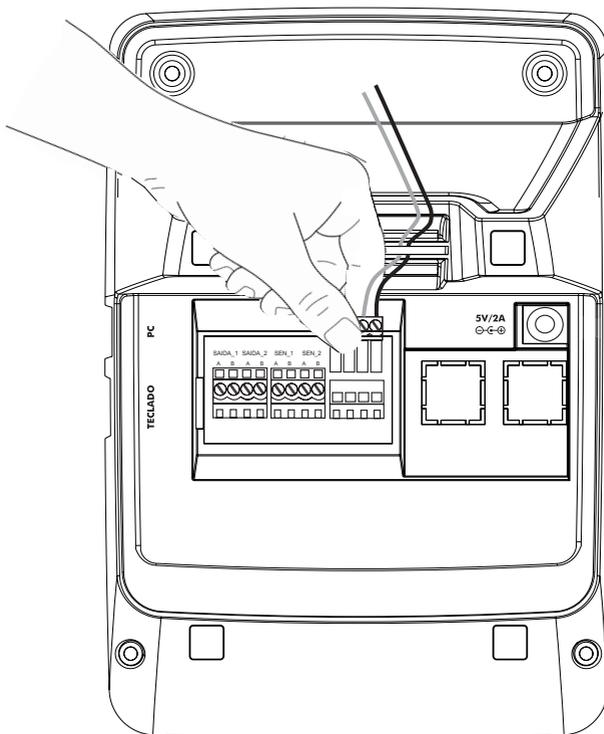
Obs.: recomendado o uso de um conector auxiliar (não incluso) para junção dos fios, evitando que todos os fios cheguem ao conector do MIP. Utilizando a topologia estrela, a soma das distâncias dos dispositivos até o MIP não podem ultrapassar 1.000 metros ou em cabeamento que não ultrapasse 250 ohms, sendo esta distância alcançada desde que utilizados cabos de boa qualidade, como informado na recomendação 9 do item 4.1 Barramento de comunicação.

4.3. Procedimento de instalação

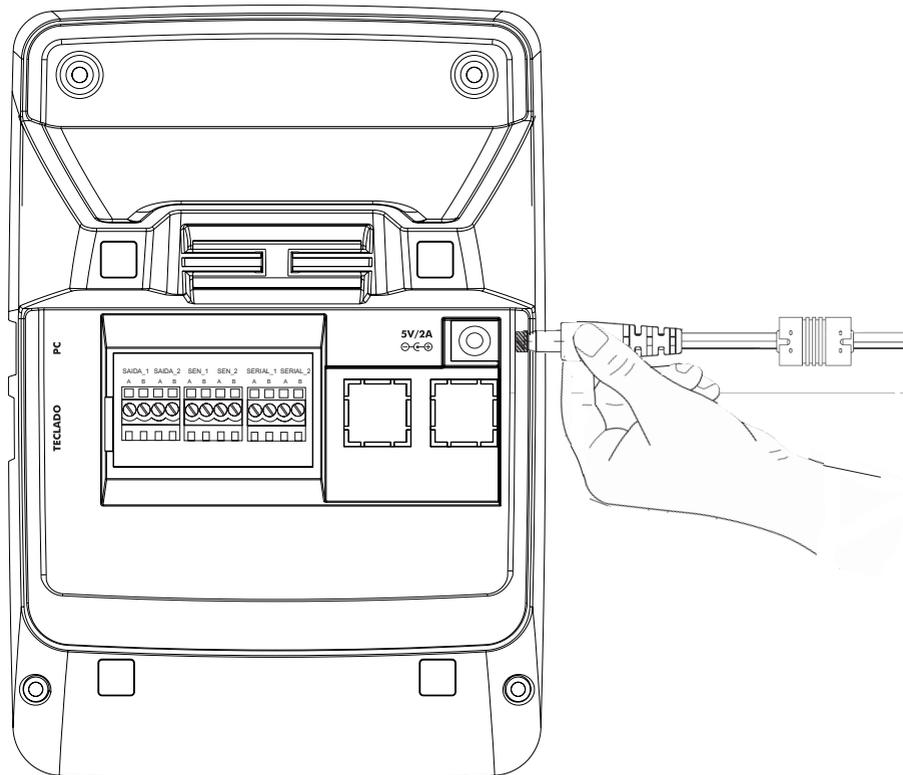
1. Com o auxílio de uma chave de fenda, parafuse os cabos que serão utilizados nos conectores fêmea do MIP;



2. Após parafusar os cabos, encaixe o conector fêmea no conector macho do MIP;



3. Encaixe o conector *Jack* da fonte externa (5 Vdc / 2 A) no local indicado da parte posterior do MIP.



4.4. Conexões do MIP

Saídas de acionamento SAIDA_1 e SAIDA_2

Estas saídas podem ser programadas para:

- » Acionamento de cargas até 24 Vdc / 1 A como fechaduras, placas de comando de motor para portões, etc.
- » Acionamento de sirenes em caso de pânico.
- » Controle de esclusa/gaiola quando sua função de intertravamento estiver habilitada.

Entradas de sensores SEN_1 e SEN_2

Estas entradas podem ser utilizadas como:

- » Sensores de estado de porta aberta, alertando com bips e mensagens na tela do MIP.
- » Sensores no modo de intertravamento.

Teclado USB

O teclado é utilizado para facilitar o cadastro e configuração no MIP. Através dele é possível navegar nos menus e realizar qualquer programação do dispositivo ou sistema, como por exemplo, consultas de eventos, etc.

Cabo USB

Com o cabo USB conectado ao MIP e a um computador (notebook ou desktop) que tenha o software de configuração/cadastro (SGA 1000 por exemplo) instalado, é possível realizar todas as configurações do sistema e fazer consultas de eventos, inclusive gerar relatórios detalhados dos acessos registrados pelos dispositivos.

Obs.: os dois cabos USB podem estar conectados, mas somente uma função está disponível por vez. No MIP, sempre o computador será preferencial.

5. Operação/Programação

O MIP é um equipamento de uso exclusivo do profissional da portaria, em seu modo normal de funcionamento durante o dia a dia. Haverá também modos de acesso destinados a administradores e instaladores do equipamento com níveis de permissões, possibilitando ações/configurações restritas.

A seguir são descritas as possibilidades de uso do MIP a serem realizadas pelo porteiro/instalador:

- » Monitorar todos os eventos de entrada e saída através do display.
- » Liberar acessos aos portões de moradores e automóveis.
- » Incluir, editar e apagar chaveiros RFID (Mifare), senhas de usuários, digitais e controles remotos XTR 1000 de moradores, bem como usuários e dispositivos.
- » Configurar teclas dedicadas para acionamento das suas saídas ou das saídas de qualquer dispositivo configurado.
- » Ajustar hora e data.
- » Configurar função *Desperta porteiro*.
- » Configurar função *Pânico*.
- » Editar rótulos de identificação dos leitores cadastrados no sistema.
- » Configuração do tempo em que os eventos serão exibidos no display.
- » Configurar mensagem de descanso no display.

5.1. Descrição de ícones

Existem situações na qual o MIP irá sinalizar na parte superior de seu display alguns status, sendo estes identificados através dos seguintes ícones:

	Notificações de dispositivos: <i>Time Out</i> (dispositivo desconectado do barramento por mais de trinta segundos) e/ou acionamento de sensores (se ativos) e/ou necessidade de sincronizar o dispositivo.
	Teclado conectado ao MIP para configuração e cadastro.
	MIP conectado ao computador para utilização do software (por exemplo, SGA 1000).
	Notificação de controle(s) remoto com bateria baixa (exibido quando o controle remoto de um usuário estiver com bateria baixa e for acionado). Para maiores informações consulte item 5.8. <i>Notificações</i> .
	Função <i>Alerta porteiro</i> . Para maiores informações consulte item <i>Porteiro alerta</i> .

5.2. Inicializando o sistema

Ao ligar o MIP, após a exibição da versão e a tela de carregamento dos dados contidos internamente, o display exibirá a tela de descanso, que contém as informações de data, hora e nome do condomínio, conforme apresentado nas imagens a seguir.



Tela inicial com indicação de versão



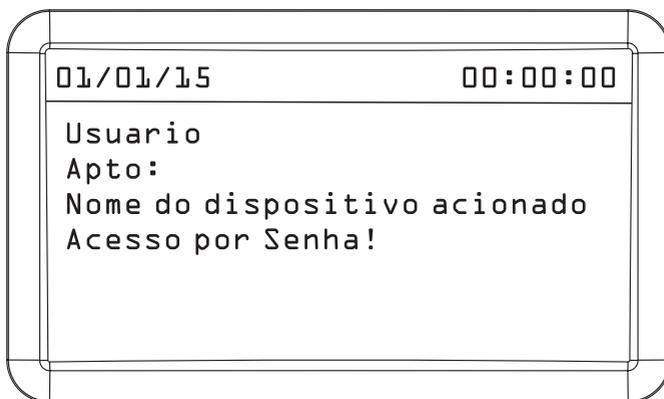
Tela de inicialização



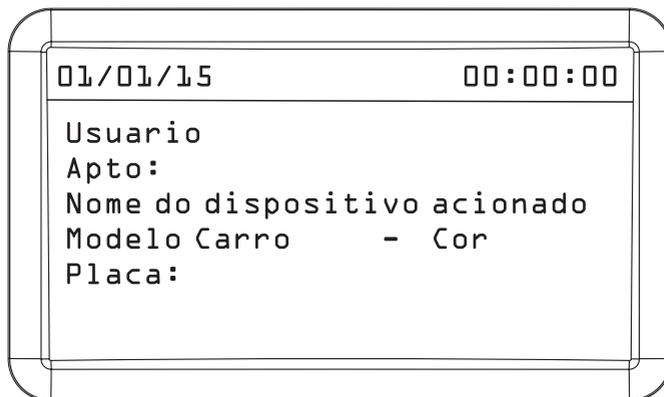
Tela de descanso

5.3. Telas de eventos

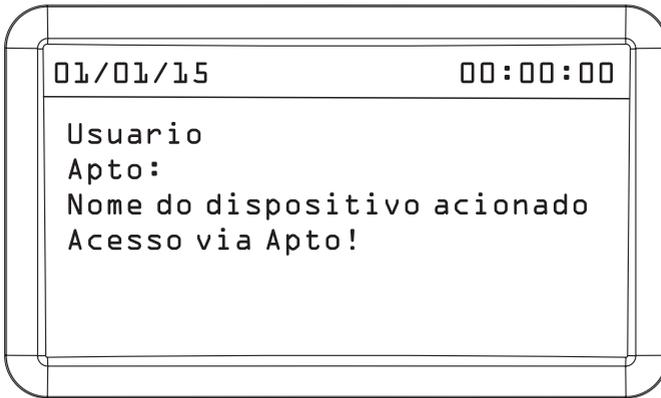
Durante o funcionamento normal, quando ocorrer algum evento, o MIP exibirá a tela de evento, informando o número do apartamento, nome do usuário, dispositivo onde ocorreu o evento e, se o acionamento for via chaveiro RFID (Mifare) ou controle XTR 1000, irá informar também a placa, modelo e cor do veículo se o mesmo estiver com estes dados preenchidos.



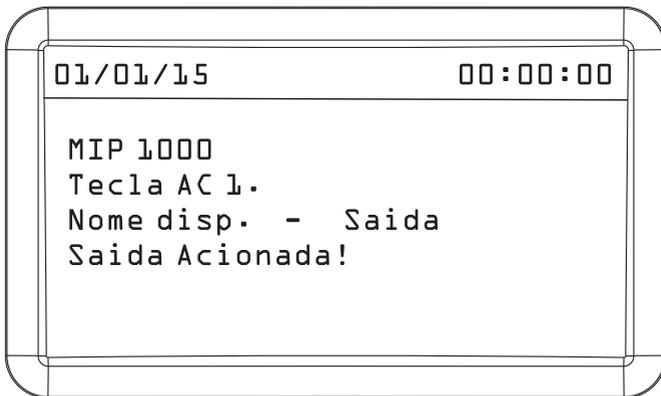
Eventos de acesso via senha nos dispositivos XLT 1000 ID ou XPE 1013 ID



Eventos de acesso via chaveiro RFID (Mifare) nos dispositivos XLT 1000 ID, XPE 1001/1013 ID, Bio Inox Plus SS 311 MF ou CT 500 1P ou eventos de acesso via biometria (digital) nos dispositivos Bio Inox Plus SS 311 MF, eventos de acesso via controle remoto (XTR 1000) no dispositivo XRE 1000



Eventos de acesso via apartamento nos dispositivos XPE 1001 ID ou XPE 1013 ID



Evento de acesso via teclas de acionamento programáveis do MIP



Evento de pânico do sistema que informa o usuário que ativou e em qual dispositivo



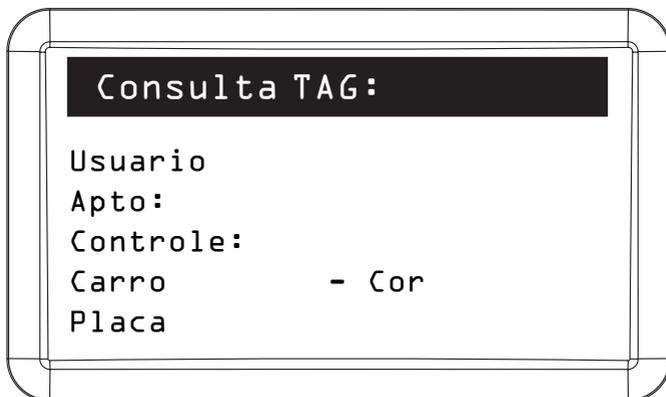
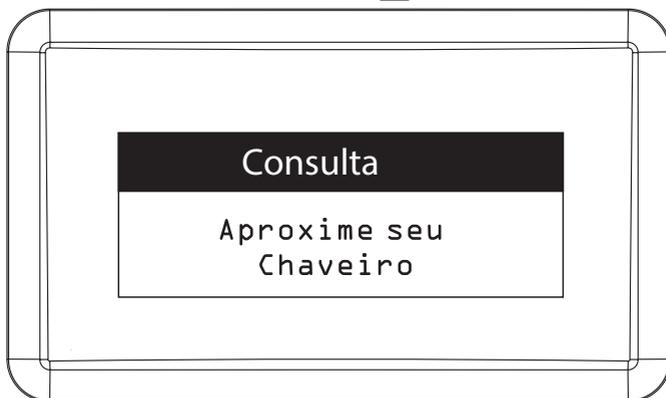
Evento de tamper do sistema indicando qual dispositivo foi violado (verificar no manual do dispositivo se possui esta funcionalidade)

5.4. Teclas de acesso rápido

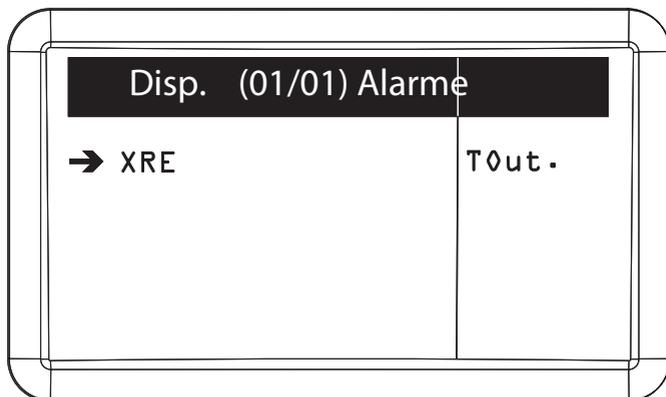
Com o MIP na tela de descanso ou inicial é possível verificar as notificações do sistema, consultar chaveiros RFID(Mifare) e controles XTR 1000, para verificar se já estão cadastrados.

Ainda na tela inicial você consegue consulta a taxa de comunicação dos dispositivos cadastrados no MIP.

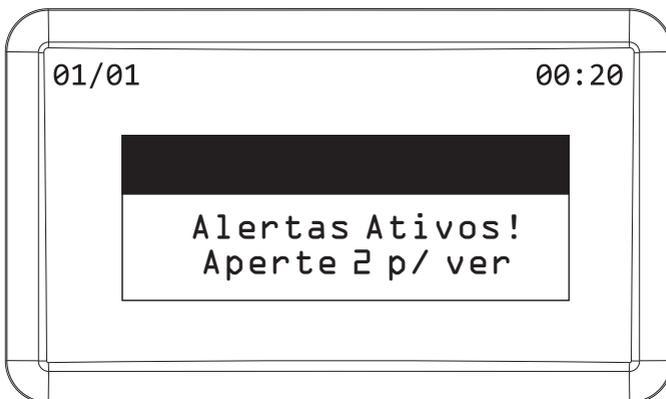
1. Para consultar se um chaveiro RFID (Mifare) já está cadastrado no sistema, com o MIP na tela de descanso ou inicial, pressione a tecla **1** e aproxime o chaveiro RFID no campo  para reconhecimento;



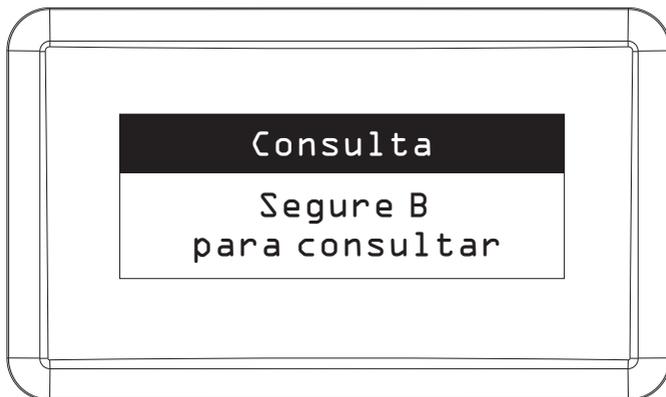
2. Quando aparecer o ícone  na tela de descanso ou inicial do MIP, pressione a tecla 2 para visualizar a notificação do sistema;

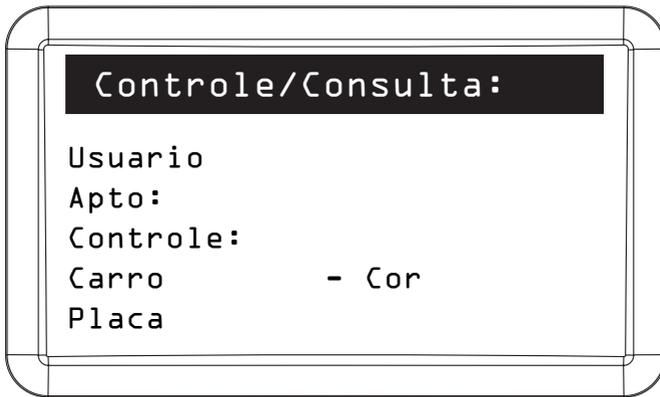


Nas versões de MIP acima de 170405, é exibido além do símbolo de exclamação, um painel na tela de descanso, evidenciando para o operador a ocorrência de um problema para uma ação rápida.



3. Para consultar se um controle XTR 1000 já está cadastrado no sistema, com o MIP na tela de descanso ou inicial, pressione a tecla 3 e segure o botão B do controle até que o mesmo seja reconhecido.

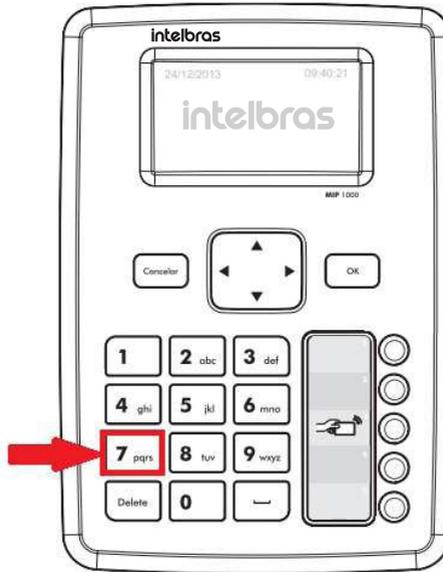




Verificando taxa de comunicação

O MIP 1000, a partir da versão de firmware 20.04.04, possui um menu que possibilita a análise da comunicação entre ele e os dispositivos ligados no barramento. Para utilizar a função, é necessário seguir os seguintes passos:

1º Passo: com o MIP na tela inicial, pressione a tecla 7:



2º Passo: selecione o dispositivo que deseja analisar:

Nome	(01/04)	End.
→ XPE PLUS ID		2
REMOTE		3
BIO INOX		4
XRE 1000		5

3º Passo: verifique a quantidade de erros na comunicação entre o MIP e o dispositivo selecionado, conforme informações abaixo:

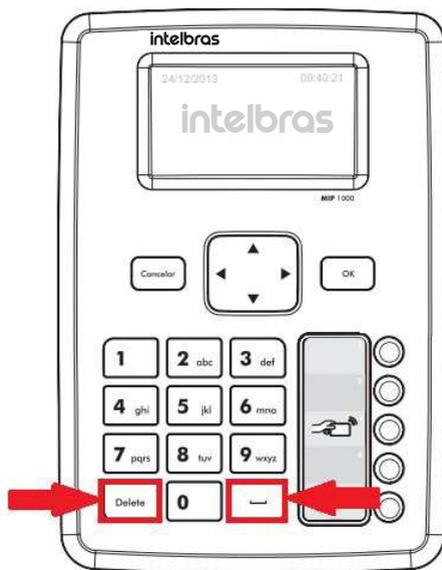
XPE PLUS ID	
num comando: 5000	← Erros geral, desde a conexão do dispositivo no barramento
num timeout: 50	
falha geral: 1.00%	
Ultimos Comandos	
f f f f f f f f 0.00% falha	← Erros instantâneos

Obs.: o num comando são todos os comandos enviados para o dispositivo e o num timeout são quantos destes falharam.

Importante: esse teste permite analisar se existem problemas de comunicação no barramento. Como referência, erros abaixo de 10% normalmente não causam problemas de comunicação. Caso esse valor esteja muito acima, é necessário investigar, conforme sugestões abaixo:

- » Ligue os dispositivos individualmente no barramento e realize a análise novamente, pois um dispositivo pode causar a falha de comunicação de todos os outros.

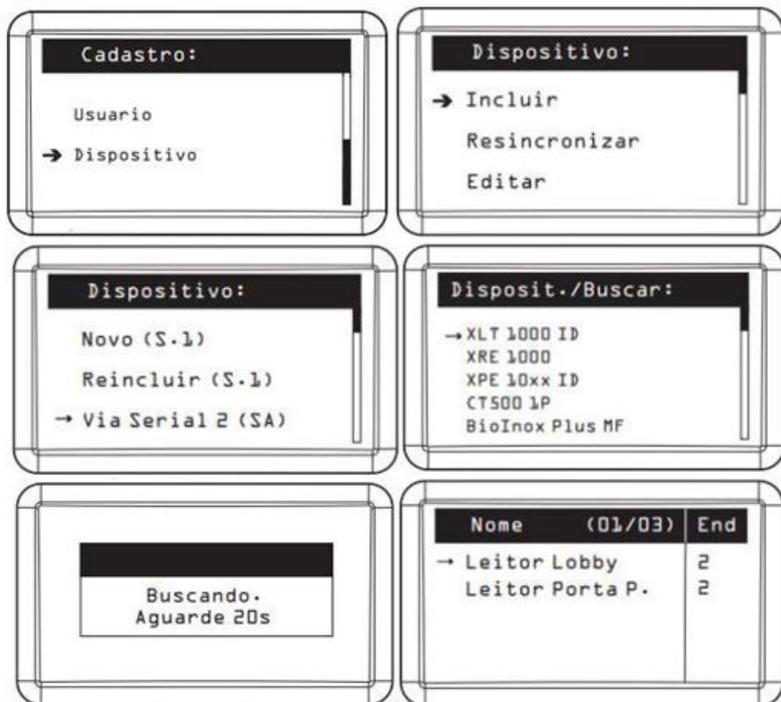
Obs.: é possível zerar o contador de erros reiniciando o MIP ou pressionando a tecla Delete, dentro da análise do dispositivo. A tecla Espaço zera o contador de todos os dispositivos de uma só vez.



- » Identificando o dispositivo ou o enlace de cabos que geram o problema no barramento, realize algumas verificações, tais como:
 - » Se existem curtos ou outros problemas na fiação, testando continuidade e impedância do cabeamento;
 - » Se o problema é solucionado ligando os dispositivos através de uma fiação externa;
- » Se funciona deixando apenas a alimentação e barramento ligados, desligando todo o restante do produto (fechadura, ramal, sensores, etc);
- » Se existem outros produtos ligados na mesma fonte do dispositivo, causando interferências;
- » Se ligar uma fonte exclusiva, ao lado do dispositivo, se o problema deixa de acontecer;
- » Se ocorre o mesmo problema ligando o dispositivo ao lado do MIP;
- » Se existem dispositivos com endereços repetidos no barramento. Para isso, a sugestão é fazer a seguinte análise:
 - » Pressione a tecla 7 do MIP e anote o endereço de cada dispositivo, conforme coluna End.

Nome	(01/04)	End.
→ XPE PLUS ID		2
REMOTE		3
BIO INOX		4
XRE 1000		5

- » Entre no menu *Cadastro / Dispositivo / Incluir / Via Serial 2 (SA)* e selecione o tipo do dispositivo desejado. Faça essa análise para todos os tipos de dispositivos que estejam ligados no barramento (XLT 1000 ID, XRE 1000, XPE 10xx ID, CT500 1P e BiInnox PLUS MF). Anote os endereços encontrados e compare com os informados no menu 7 do MIP. Caso os valores sejam divergentes, será necessário realizar o reset físico no dispositivo e recadastrá-lo novamente no MIP.

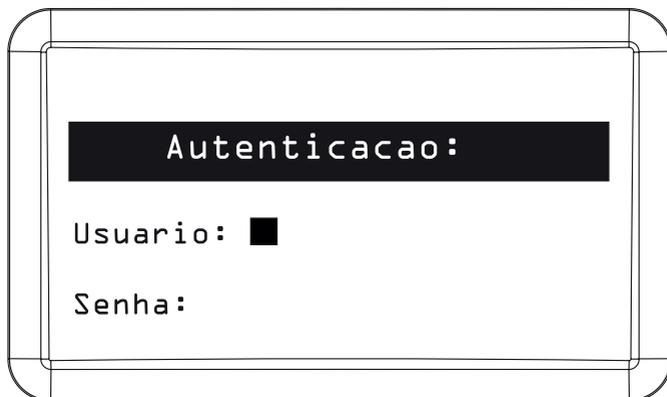


5.5. Níveis de acesso para configuração e consulta de informações

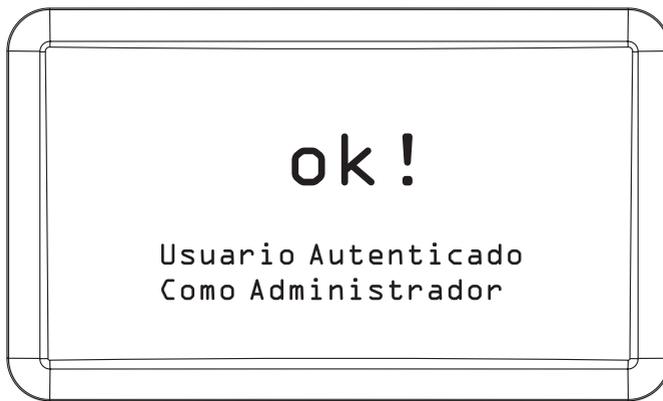
É possível configurar usuários para acessarem o *Menu principal* do MIP e definir níveis de acesso para os mesmos, sendo um total de 4 níveis (ver item *Configuração de login*).

Exemplo: o porteiro (vigilante) poderá ter acesso apenas na tela de eventos do sistema, enquanto o instalador (administrador) tem acesso completo.

Autenticação:



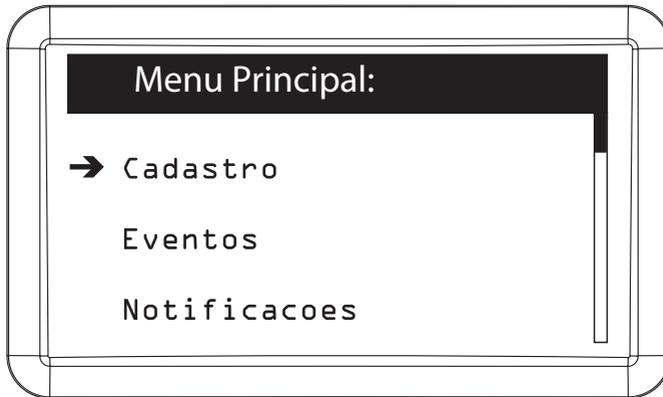
Obs.: o usuário configurado de fábrica para autenticação é o admin e a sua senha é 123456. Com a autenticação realizada o usuário terá acesso ao menu do MIP para realizar as configurações desejadas.



Obs.: durante as configurações, sempre ocorrerá a necessidade de confirmar ou cancelar uma opção, para isso, pressione Ok e Cancelar quando estiver utilizando o teclado do MIP ou Enter e ESC através de um teclado USB externo. No segundo caso, a tecla TAB não alternará as telas, sendo este papel aplicado às teclas direcionais.

5.6. Cadastro

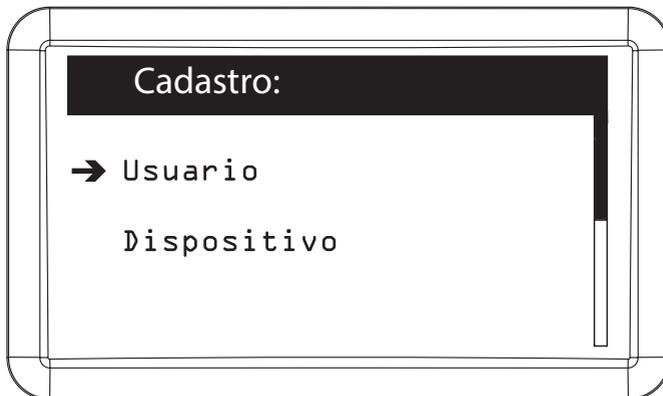
Para cadastrar, editar, consultar ou excluir um usuário ou dispositivo, entre na opção Cadastro do Menu Principal.



Usuário

Incluir usuário

Para cadastrar um novo usuário é necessário realizar os seguintes passos:



Usuario:

→ Incluir

Editar

Consultar

A screen with a title bar 'Usuario:' and three menu items: '→ Incluir', 'Editar', and 'Consultar'. A vertical scrollbar is on the right side.

Usuario/Incluir:

Nome:

■

↑

↓

A screen with a title bar 'Usuario/Incluir:' and a text input field labeled 'Nome:'. The input field contains a cursor '■'. To the right of the input field are up and down arrow icons.

Nomear o usuário que está sendo cadastrado (máximo 34 caracteres)

Usuario/Incluir:

Apto:

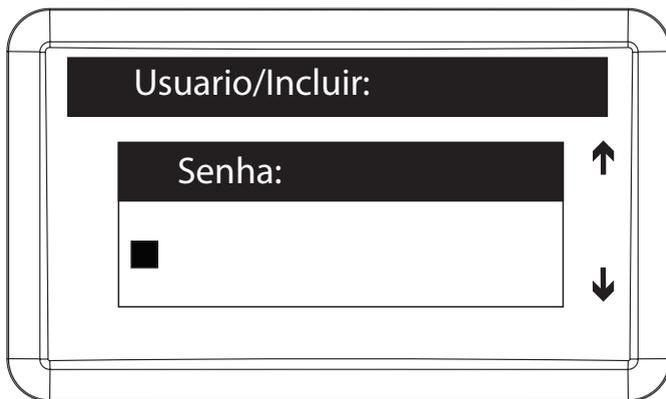
■

↑

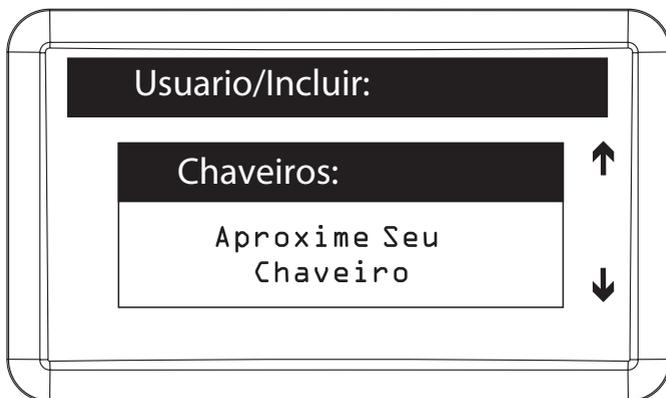
↓

A screen with a title bar 'Usuario/Incluir:' and a text input field labeled 'Apto:'. The input field contains a cursor '■'. To the right of the input field are up and down arrow icons.

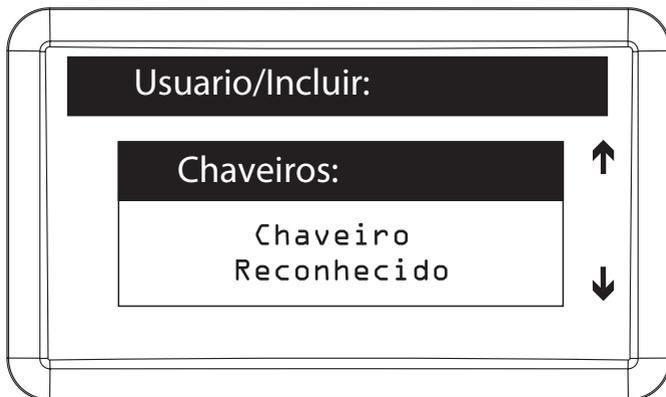
Definir o número do apartamento do usuário (máximo 6 dígitos)

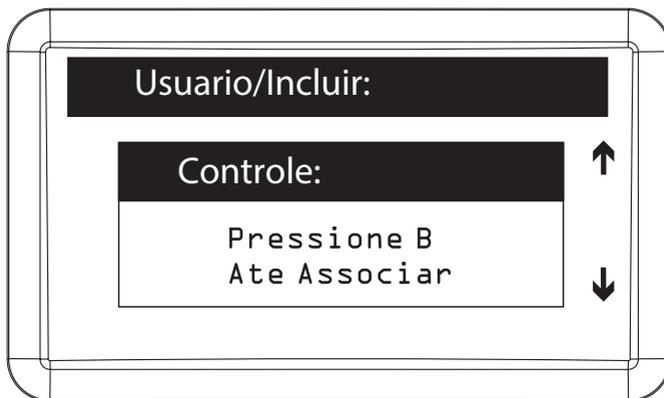


Definir a senha do usuário, entre 100 e 999, para acionamentos das saídas nos dispositivos XLT 1000 ID e XPE 1013 ID. Para o acionamento das saídas no dispositivo, o usuário irá digitar qual saída deseja acionar (1 ou 2), a senha de três dígitos e o número de seu apartamento (consultar o manual do dispositivo)

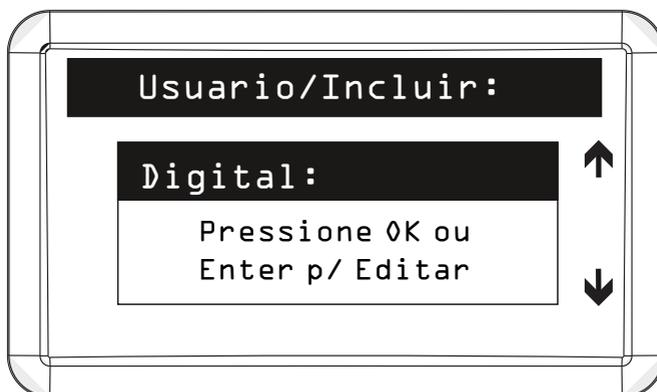
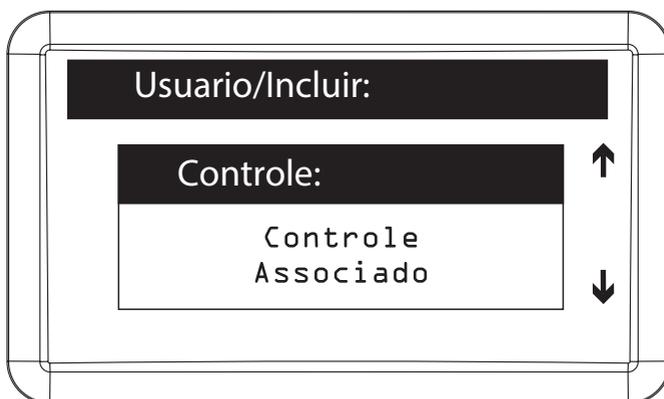


Posicionar o chaveiro RFID Mifare 13,56 MHz que deseja cadastrar no campo  do MIP

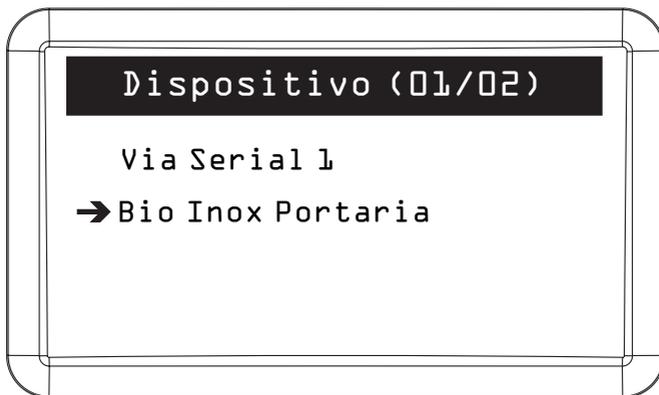




Manter o botão B do controle remoto pressionado, por aproximadamente quatro segundos, até que o MIP confirme a associação



Pressionar OK ou Enter para iniciar o cadastro da digital



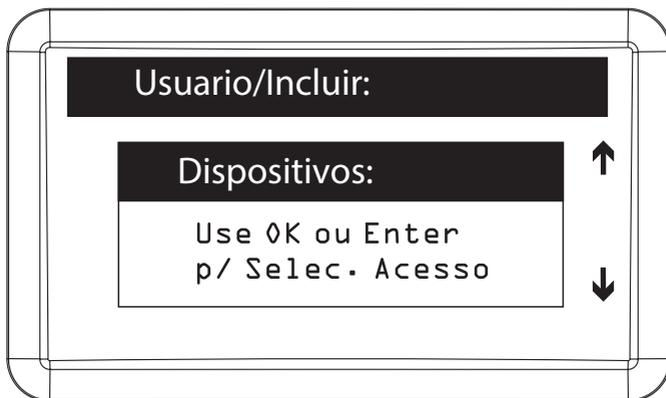
Escolha por qual dispositivo deseja realizar a captura da digital

Via Serial 1, é necessário conectar um dispositivo biométrico na Serial 1 do MIP para realizar o cadastro. Ou através de um dispositivo biométrico cadastrado no sistema. Ao selecionar o Bio Inox SS 311 MF, o processo de cadastro será realizado através do dispositivo *Bio Inox Portaria*, que está em funcionamento no sistema.

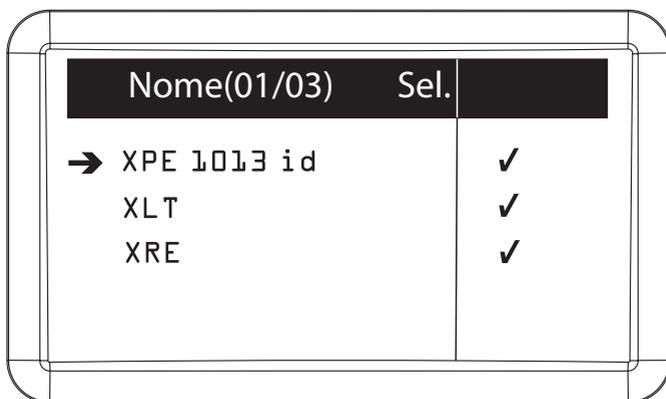


Insira a digital de acesso 3 vezes no dispositivo de acordo com o solicitado pelo MIP





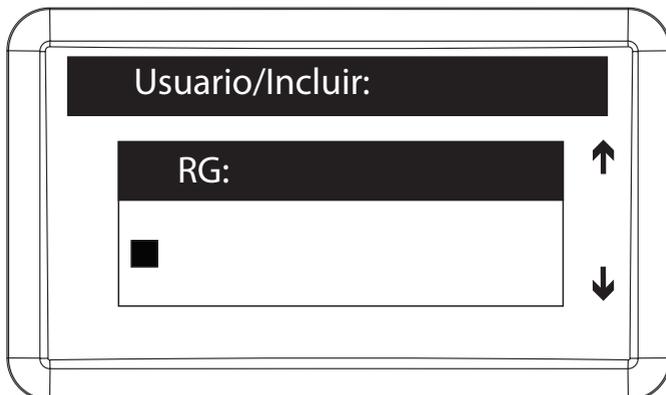
Configurar quais os dispositivos (XRE 1000, XLT 1000 ID, XPE 1001/1013 ID, Bio Inox Plus SS 311 MF, CT 500 1P) conectados ao barramento o usuário terá permissão de acessar através de controle remoto, chaveiro RFID (Mifare), senha ou digital (padrão de fábrica: usuários com permissão em todos os dispositivos cadastrados)



Deixar habilitado apenas os dispositivos que o usuário cadastrado terá permissão de acessar

Pressionar *Cancelar* ou *ESC* para continuar o cadastro de usuário.

Se o item **Modo de cadastro** em **Conf. do sistema** estiver selecionado a opção **Avançado** (padrão de fábrica: *Básico*), no cadastro do usuário também poderão ser configuradas as seguintes informações:



Número do RG do usuário

Usuario/Incluir:

Email:

■

↑

↓

A screenshot of a mobile application form. At the top, there is a dark header bar with the text "Usuario/Incluir:". Below this, there is a white input field with a dark header bar containing the text "Email:". The input field contains a small black square cursor. To the right of the input field, there are two vertical arrows: an upward-pointing arrow above a downward-pointing arrow.

E-mail do usuário (máximo 34 caracteres)

Usuario/Incluir:

Tel. Residencial

(■)

↑

↓

A screenshot of a mobile application form. At the top, there is a dark header bar with the text "Usuario/Incluir:". Below this, there is a white input field with a dark header bar containing the text "Tel. Residencial". The input field contains the text "(■)". To the right of the input field, there are two vertical arrows: an upward-pointing arrow above a downward-pointing arrow.

Número do telefone residencial do usuário

Usuario/Incluir:

Tel. Celular:

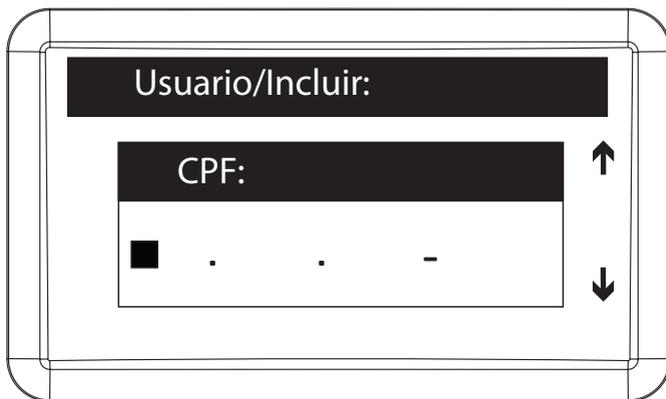
(■)

↑

↓

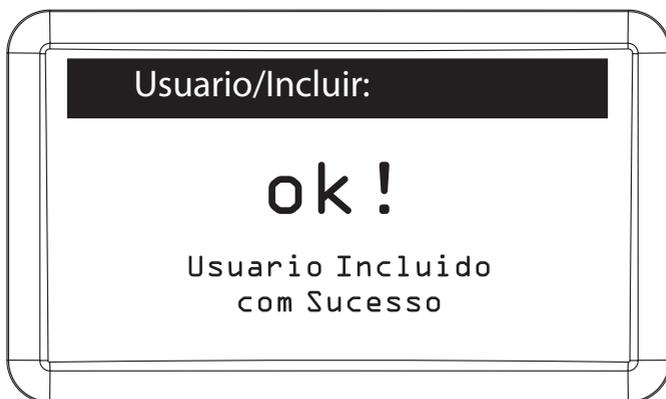
A screenshot of a mobile application form. At the top, there is a dark header bar with the text "Usuario/Incluir:". Below this, there is a white input field with a dark header bar containing the text "Tel. Celular:". The input field contains the text "(■)". To the right of the input field, there are two vertical arrows: an upward-pointing arrow above a downward-pointing arrow.

Número do telefone celular do usuário



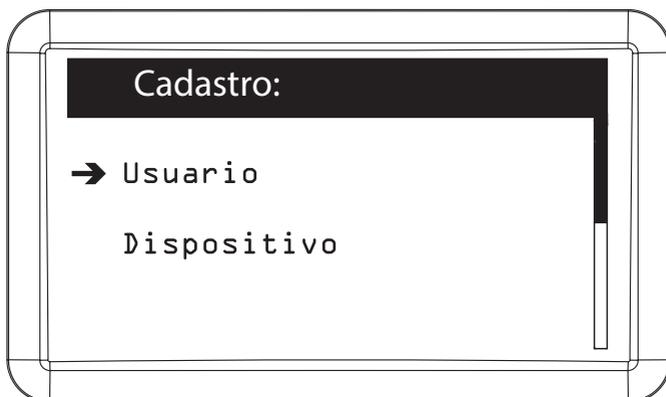
Número do CPF do usuário

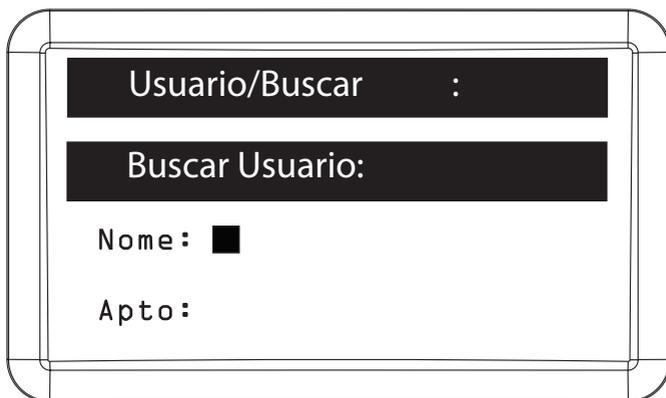
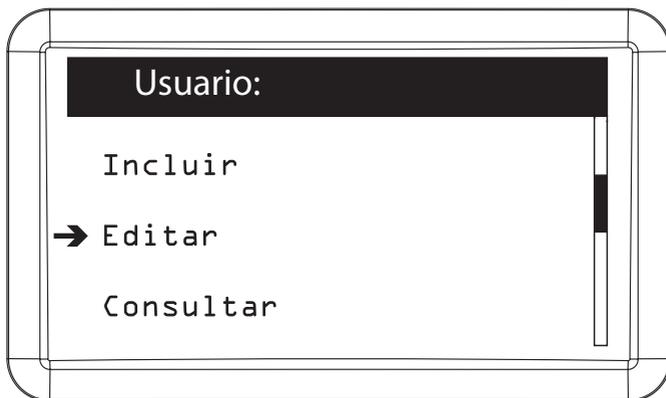
Ao finalizar o cadastro, pressionar *Ok* ou *Enter* para confirmar.



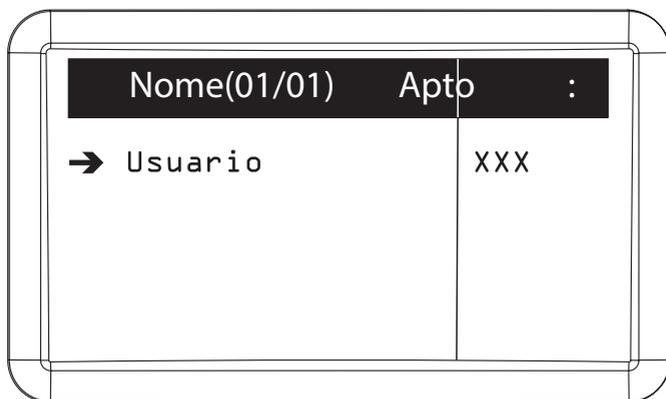
Editar usuário

Para editar o cadastro de um usuário é necessário realizar os seguintes passos:





O usuário pode ser encontrado através de seu nome ou do número do apartamento



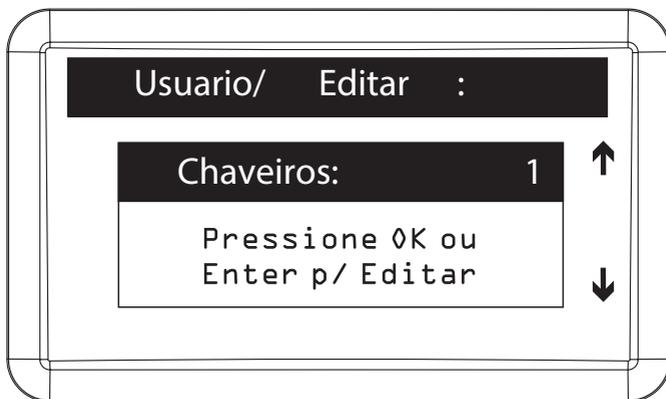
Selecionar o usuário para realizar as alterações necessárias

Além de alterar os dados do usuário (dados informados na opção *Incluir usuário*) é através da edição que podemos cadastrar novos chavesiros RFID (Mifare), controles remotos (XTR 1000) e digitais para este usuário em edição, bem como editá-los, colocando informações como: modelo do carro, cor e placa.

Para realizar as programações de *Chaveiros, Controles e Digitais* os passos a seguir devem ser feitos.

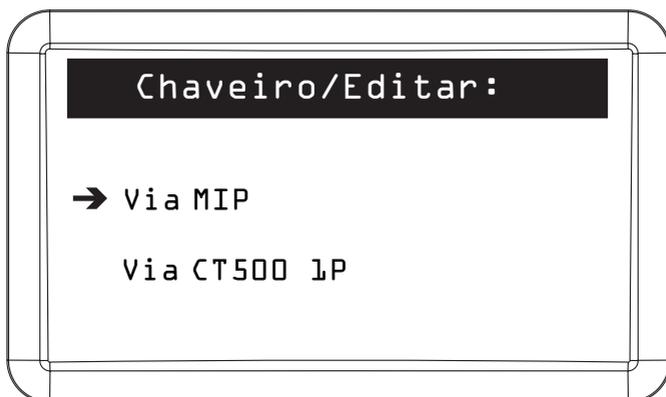
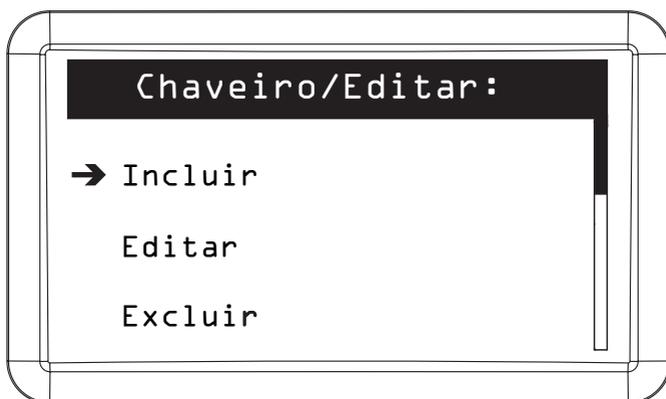
Chaveiro

Após selecionar o usuário que deseja editar, uma das opções que pode ser editada é o chaveiro. Realize os seguintes passos para incluir, editar ou excluir um chaveiro.

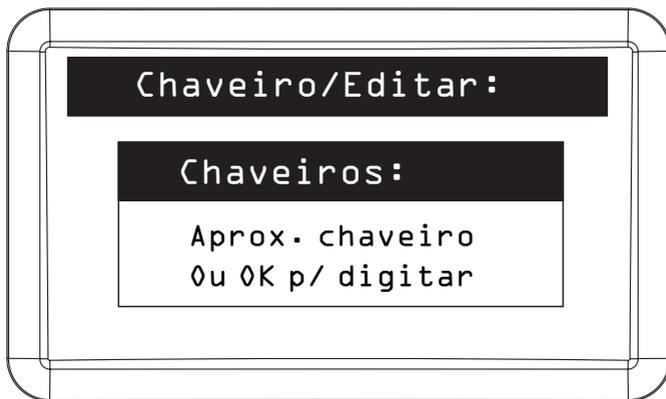


Incluir novo chaveiro RFID Mifare 13,56 MHz

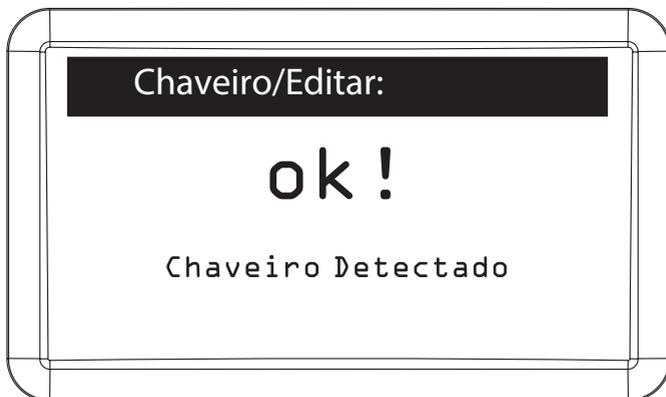
Para incluir um novo chaveiro RFID (Mifare) para o usuário é necessário realizar os seguintes passos:



Selecionar opção Via MIP

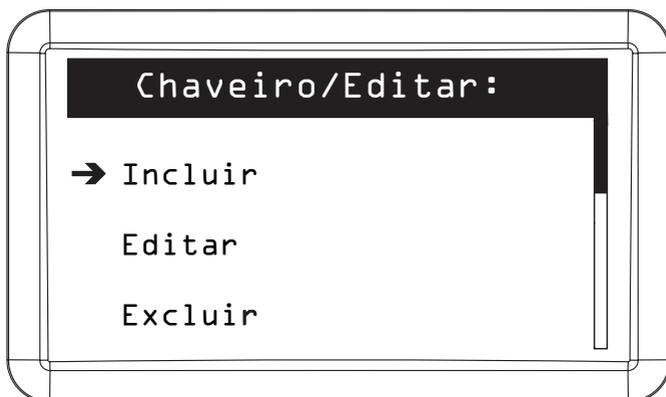


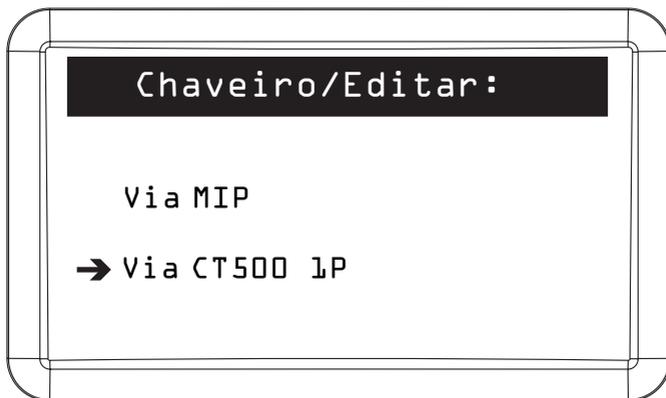
Posicionar o chaveiro RFID Mifare 13,56 MHz que deseja cadastrar abaixo do campo  do MIP ou pressionar OK ou Enter para digitar o código do chaveiro a ser cadastrado



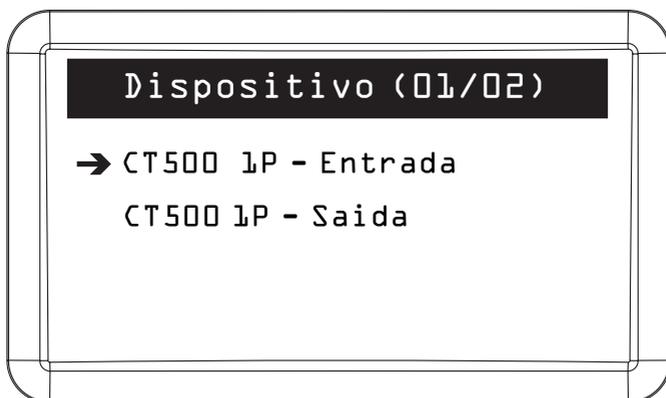
Incluir TAG veicular UHF

Para incluir uma TAG veicular (UHF) para o usuário é necessário realizar os seguintes passos:

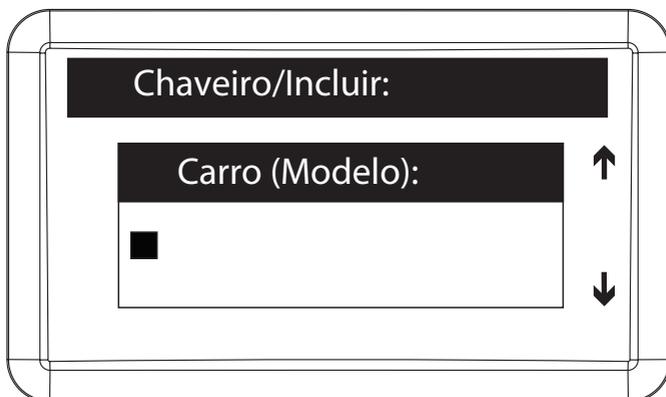




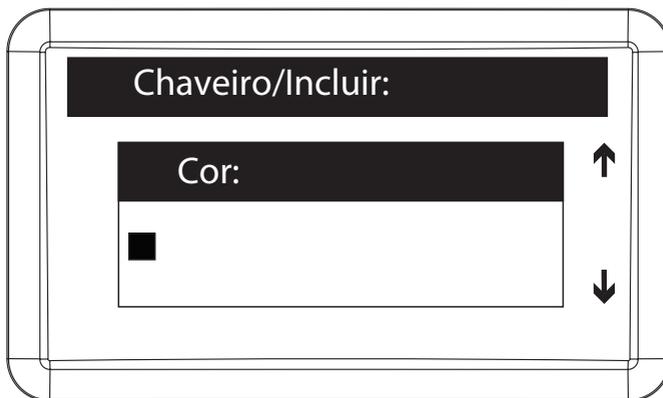
Selecionar opção Via CT 500 1P



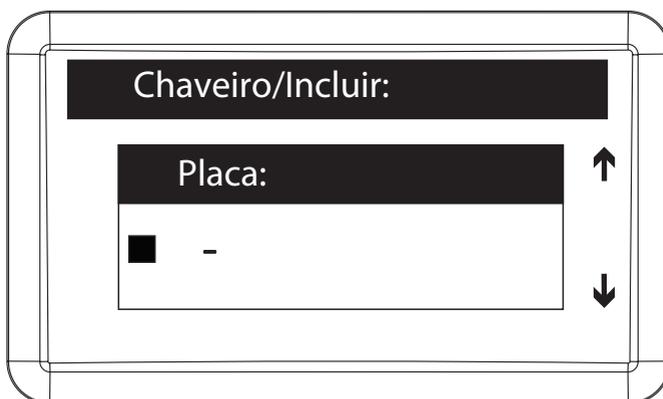
Escolher um dispositivo (de categoria CT 500 1P) e posicionar a TAG veicular (UHF) que deseja cadastrar a frente da antena instalada neste dispositivo



Informar o modelo do carro do usuário (máximo 17 caracteres). O nome informado neste campo aparecerá na listagem dos chaveiros cadastrados, facilitando a identificação do mesmo para edição ou exclusão



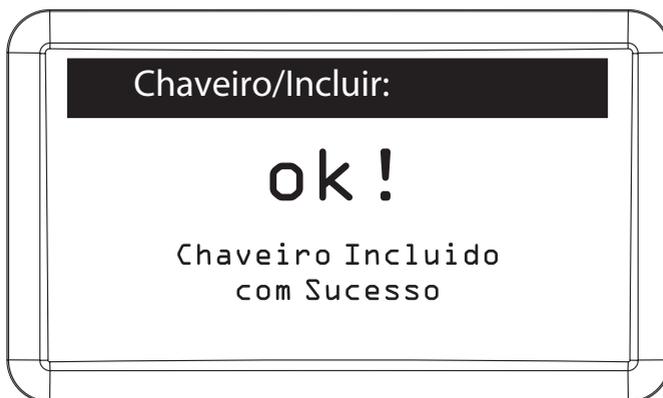
Informar a cor do carro do usuário (máximo 17 caracteres)



Informar a placa do carro do usuário

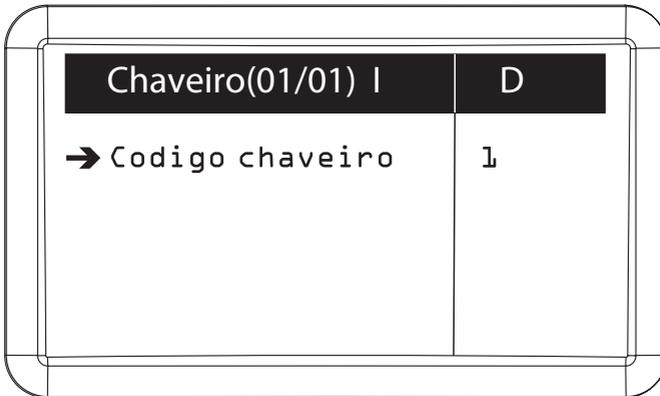
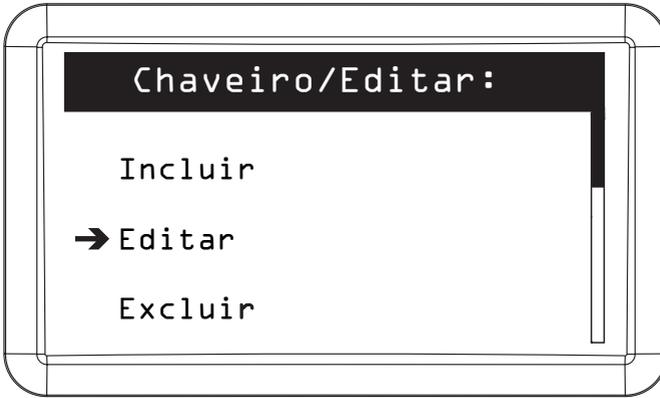
Obs.: as informações de modelo, cor e placa do carro não são obrigatórias, mas se incluídas, facilitam a identificação do chaveiro RFID (Mifare) em possíveis processos de edição, exclusão ou verificação de relatórios.

Ao finalizar o cadastro, pressionar *Ok* ou *Enter* para confirmar.



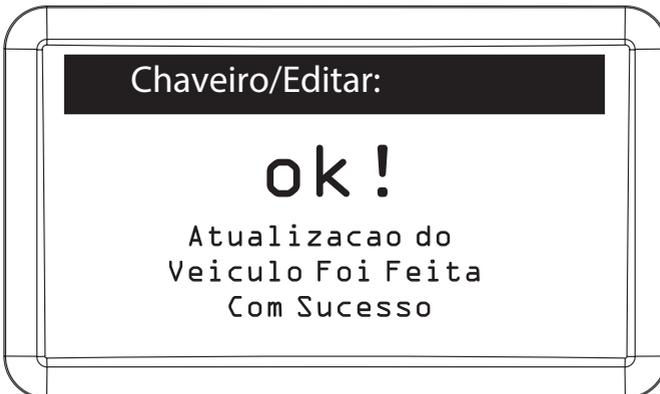
Editar chaveiro RFID Mifare 13,56 MHz ou TAG veicular UHF

Para editar o cadastro de um chaveiro RFID Mifare 13,56 MHz ou uma TAG veicular UHF é necessário realizar os seguintes passos:



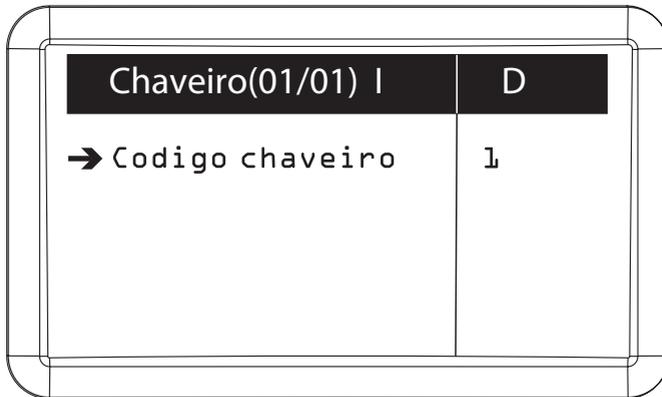
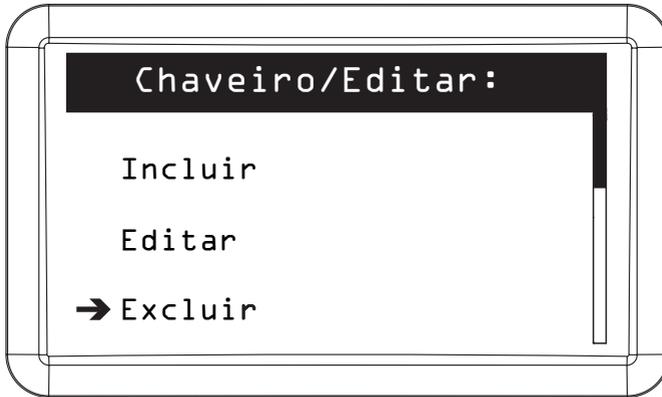
Selecionar o chaveiro para realizar as alterações necessárias. Se o campo Carro (modelo) estiver preenchido, ao invés de mostrar o código do controle, na tela acima, será exibido o nome deste campo

Ao finalizar as alterações, pressionar OK ou Enter para salvá-las.

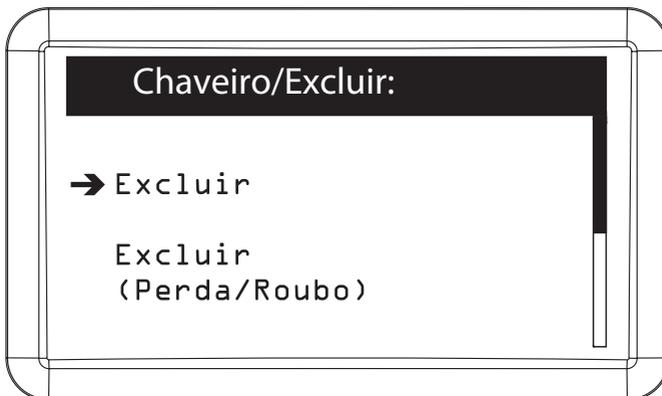


Excluir chaveiro RFID Mifare 13,56 MHz ou TAG veicular UHF

Para excluir o cadastro de um chaveiro RFID Mifare 13,56 MHz ou TAG veicular UHF é necessário realizar os seguintes passos:

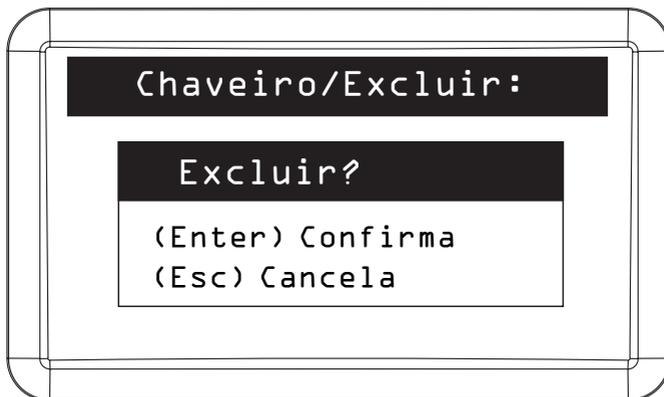


Selecionar o chaveiro que deseja excluir. Se o campo Carro (modelo) estiver preenchido, ao invés de mostrar o código do controle, na tela acima, será exibido o nome deste campo

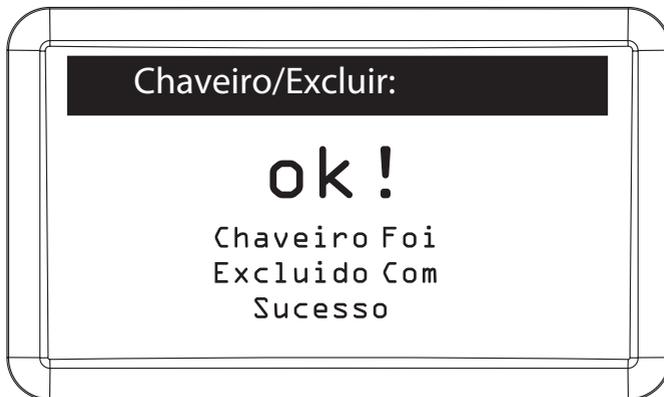


Informar se o chaveiro RFID (Mifare) está sendo excluído por motivo de perda/roubo ou por outro motivo. Caso escolha o motivo Perda/Roubo, quando alguém tentar utilizar este chaveiro será exibido um evento no MIP bloqueando o acesso, mas sinalizando o uso do mesmo

Pressionar *Ok* ou *Enter* para continuar;

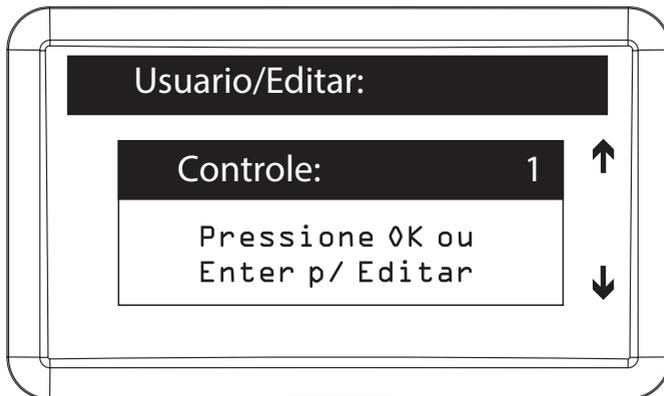


Pressionar OK ou Enter para confirmar. Para cancelar exclusão pressionar Cancelar ou Esc



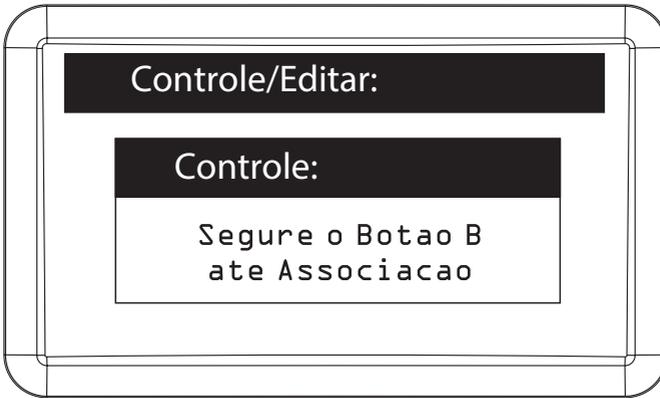
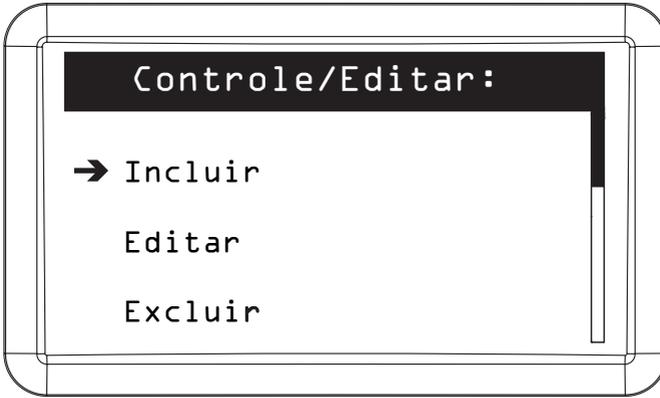
Controle

Após selecionar o usuário que deseja editar, uma das opções que pode ser editada é o controle. Realize os seguintes passos para incluir, editar ou excluir um controle remoto.

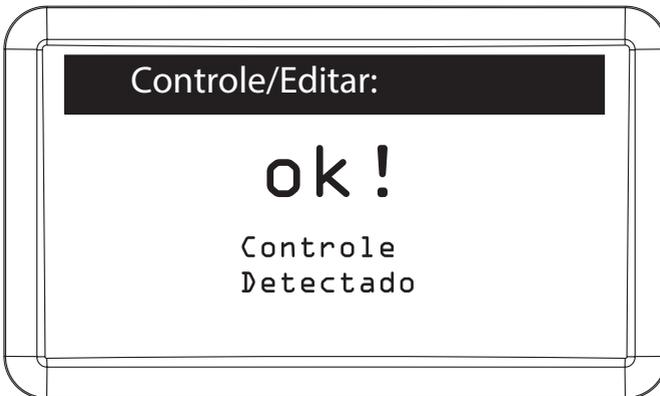


Incluir novo controle

Para incluir um novo controle remoto para o usuário é necessário realizar os seguintes passos:



Manter o botão B do controle remoto pressionado, por aproximadamente quatro segundos, até que o MIP o detecte



A screenshot of a control panel. At the top, a dark header bar contains the text 'Controle/Incluir:'. Below this, a white rectangular area is titled 'Carro (Modelo):'. Inside this area, there is a small black square on the left side. To the right of the white area, there are two vertical arrows: an upward-pointing arrow above a downward-pointing arrow.

Informar o modelo do carro do usuário (máximo 17 caracteres)

A screenshot of a control panel. At the top, a dark header bar contains the text 'Controle/Incluir:'. Below this, a white rectangular area is titled 'Cor:'. Inside this area, there is a small black square on the left side. To the right of the white area, there are two vertical arrows: an upward-pointing arrow above a downward-pointing arrow.

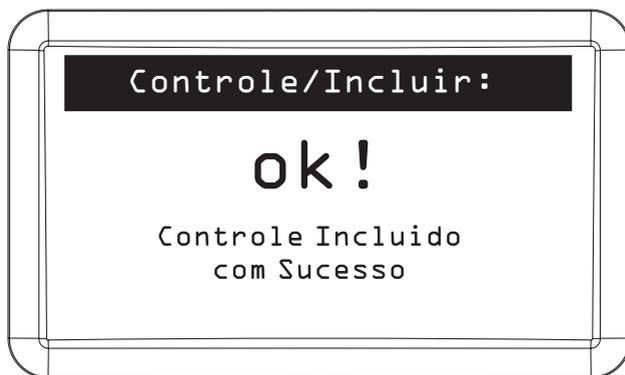
Informar a cor do carro do usuário (máximo 17 caracteres)

A screenshot of a control panel. At the top, a dark header bar contains the text 'Controle/Incluir:'. Below this, a white rectangular area is titled 'Placa:'. Inside this area, there is a small black square on the left side, followed by a hyphen '-' character. To the right of the white area, there are two vertical arrows: an upward-pointing arrow above a downward-pointing arrow.

Informar a placa do carro do usuário

Obs.: as informações de modelo, cor e placa do carro não são obrigatórias, mas se incluídas, facilitam a identificação do controle em possíveis processos de edição, exclusão ou verificação de relatórios.

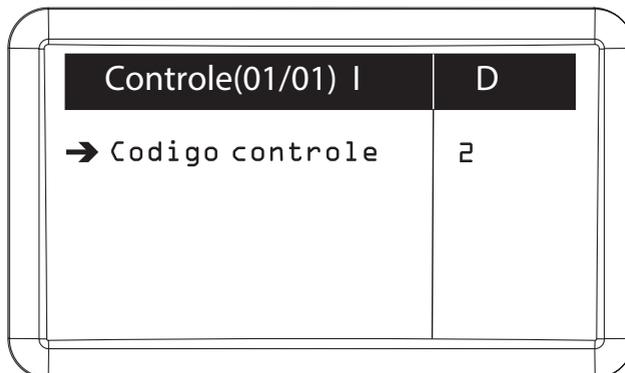
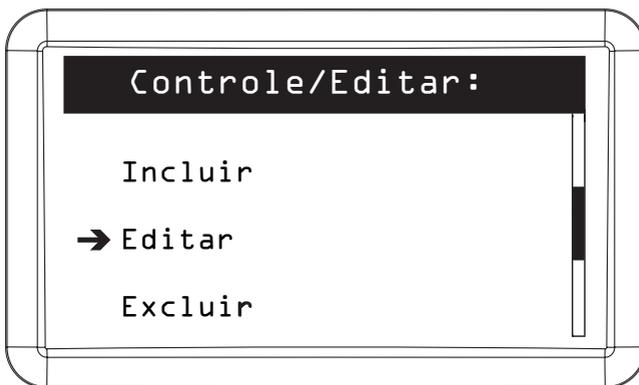
Ao finalizar o cadastro pressionar *Ok* ou *Enter* para confirmar.



Obs.: este controle possui um sistema anti-clonagem baseado em tempo, portanto se desejar manter o funcionamento do mesmo após um problema que seja necessário restaurar as informações do MIP, é **NECESSÁRIO** que esta restauração seja executada de um backup do sistema com menos de um mês. Esse backup é feito através do software SGA 1000 no momento que for finalizado o sincronismo.

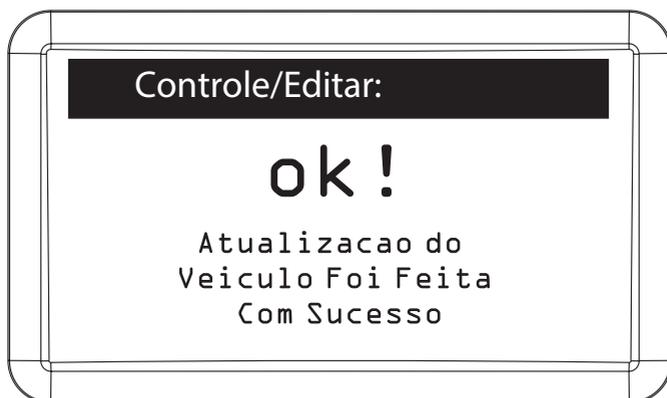
Editar controle

Para editar o cadastro de um controle é necessário realizar os seguintes passos:



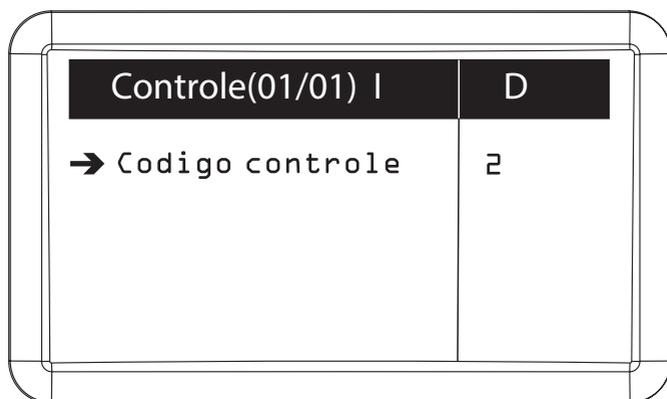
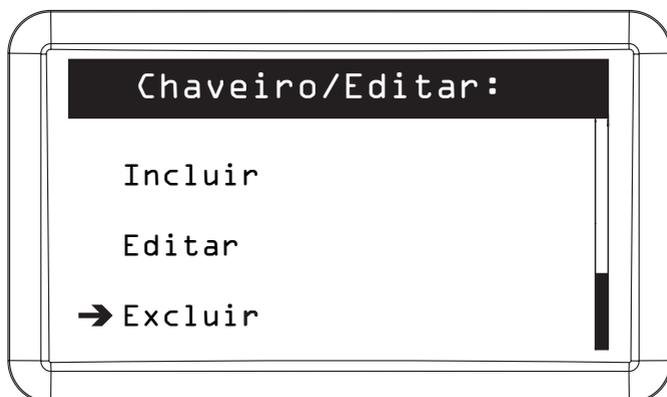
Selecionar o controle remoto para realizar as alterações necessárias. Se o campo Carro (modelo) estiver preenchido, ao invés de mostrar o código do controle, na tela acima, será exibido o nome deste campo

Ao finalizar as alterações, pressionar *OK* ou *Enter* para salvá-las.

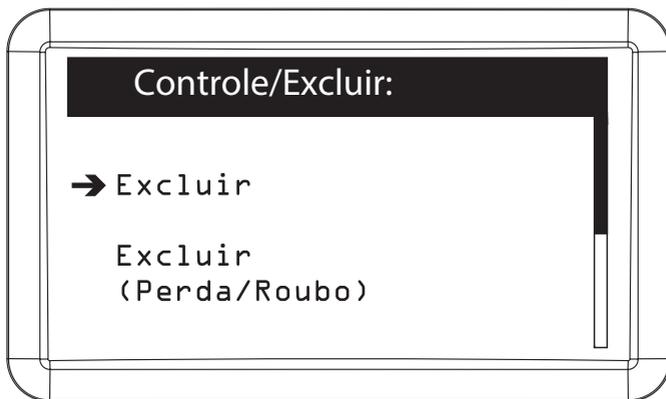


Excluir controle

Para excluir o cadastro de um controle remoto é necessário realizar os seguintes passos:

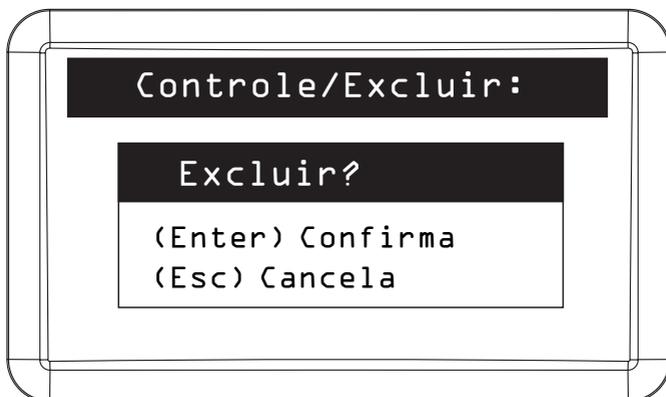


Selecionar o controle remoto que deseja excluir. Se o campo Carro (modelo) estiver preenchido, ao invés de mostrar o código do controle, na tela acima, será exibido o nome deste campo

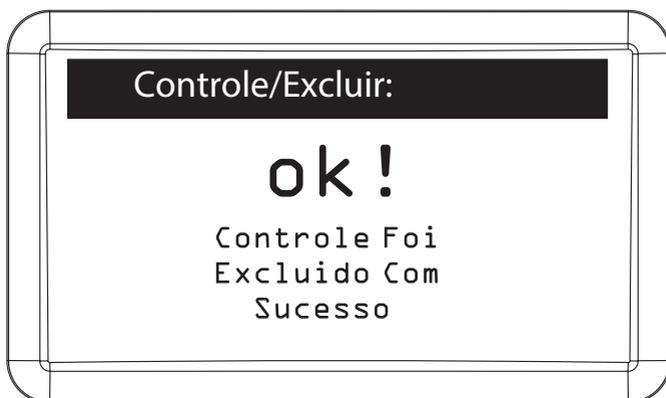


Informar se o controle remoto está sendo excluído por motivo de perda/roubo ou por outro motivo. Caso escolha o motivo Perda/Roubo, quando alguém tentar utilizar este controle remoto será exibido um evento no MIP, bloqueando o acesso, mas sinalizando o uso do mesmo

Pressionar Ok ou Enter para continuar.

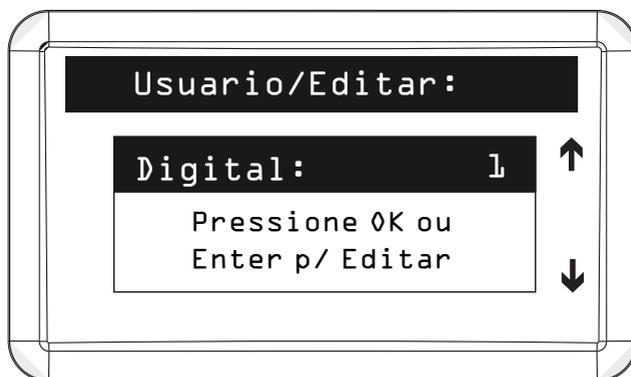


Pressionar OK ou Enter para confirmar. Para cancelar exclusão pressionar Cancelar ou Esc

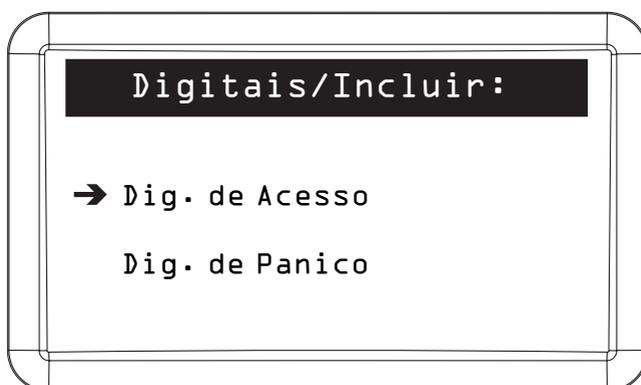
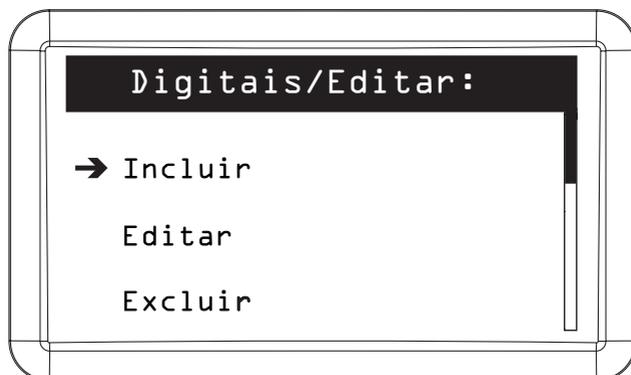


Digital

Após selecionar o usuário que deseja editar, uma das opções que pode ser editada é a digital. Realize os seguintes passos para incluir, editar ou excluir uma digital.



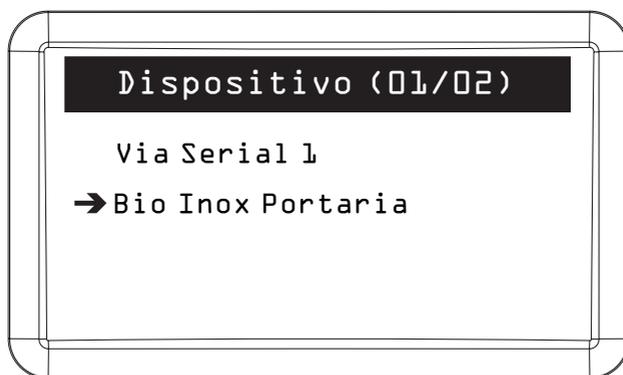
Incluir nova digital



Selecionar o tipo de digital a inserida

Obs.: as digitais podem ser:

- » **Digital de acesso:** gera um evento comum quando o usuário utiliza esta digital.
- » **Digital de pânico:** gera evento de pânico para o porteiro no momento da utilização desta digital.



Escolha por qual dispositivo deseja realizar a captura da digital

Via Serial 1, é necessário conectar um dispositivo biométrico na Serial 1 do MIP para realizar o cadastro. Ou através de um dispositivo biométrico cadastrado no sistema. Ao selecionar o *Bio Inox Portaria*, o processo de cadastro será realizado através do dispositivo com este nome, que está em funcionamento no sistema.



Insera a digital 3 vezes de acordo com o solicitado pelo MIP



Digital/Incluir:

Carro (Modelo):

■

↑

↓

Informar o modelo do carro do usuário

Digital/Incluir:

Cor:

■

↑

↓

Informar a cor do carro do usuário

Digital/Incluir:

Placa:

■ -

↑

↓

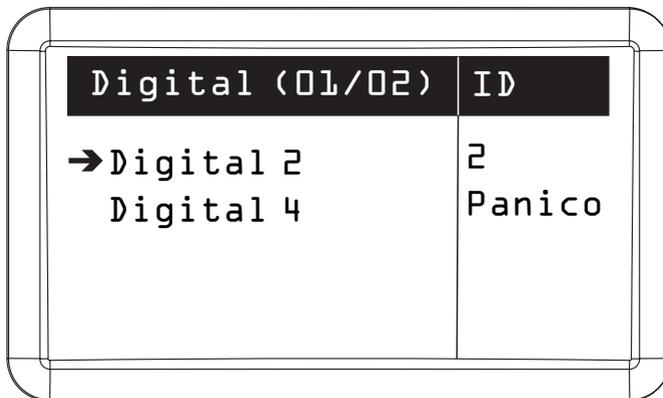
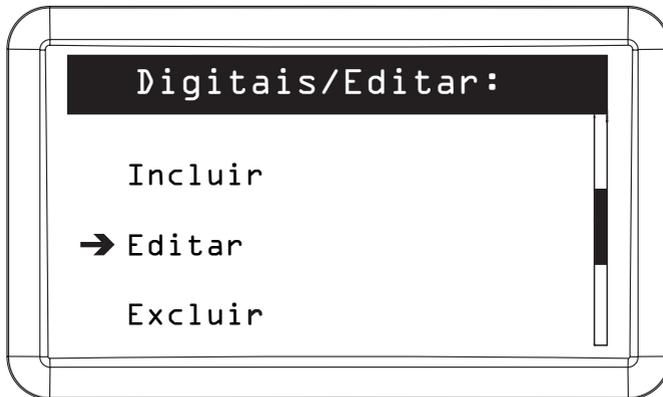
Informar a placa do carro do usuário

Obs.: as informações de modelo, cor e placa do carro não são obrigatórias, mas se incluídas, facilitam a identificação da digital em possíveis processos de edição ou exclusão.

Ao finalizar o cadastro pressionar Ok ou Enter para confirmar.

Editar digital

Para editar o cadastro de uma digital é necessário realizar os seguintes passos:



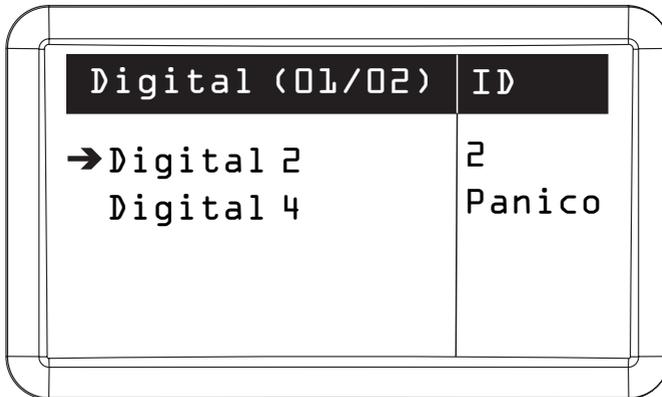
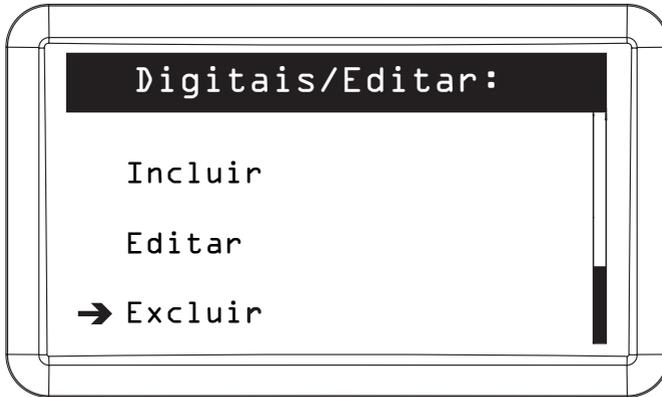
Selecionar a digital para realizar as alterações necessárias. Se o campo Carro (modelo) estiver preenchido, ao invés de mostrar Digital ID, na tela acima, será exibido o nome deste campo

Pressionar *Ok* ou *Enter* para salvar as alterações.



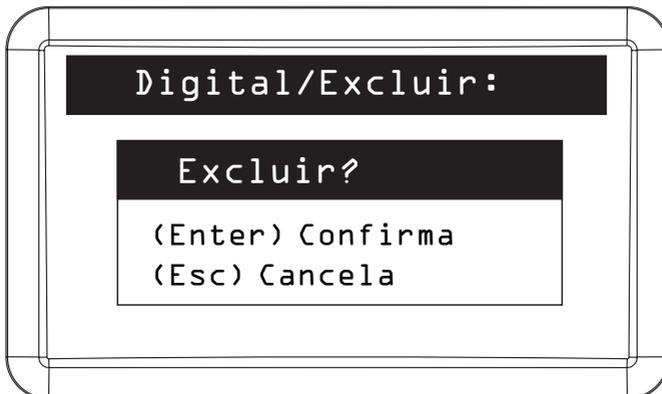
Excluir digital

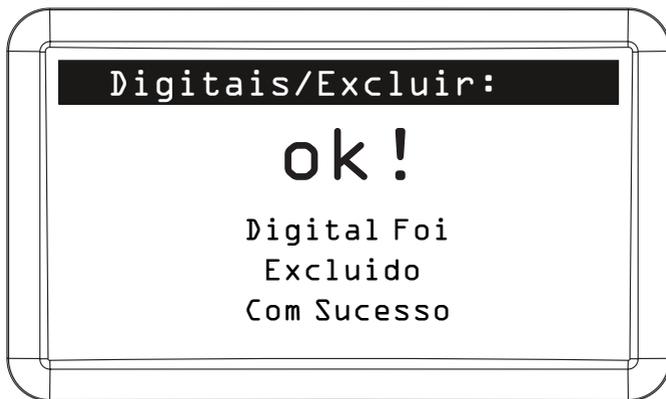
Para excluir o cadastro de uma digital é necessário realizar os seguintes passos:



Selecionar a digital que deseja excluir. Se o campo Carro (modelo) estiver preenchido, ao invés de mostrar Digital Código, na tela acima, será exibido o nome deste campo

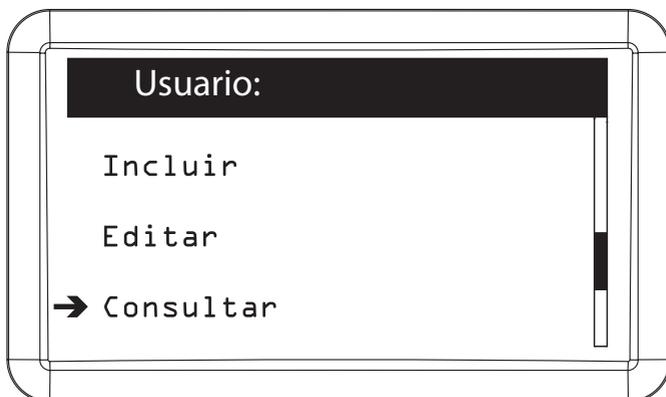
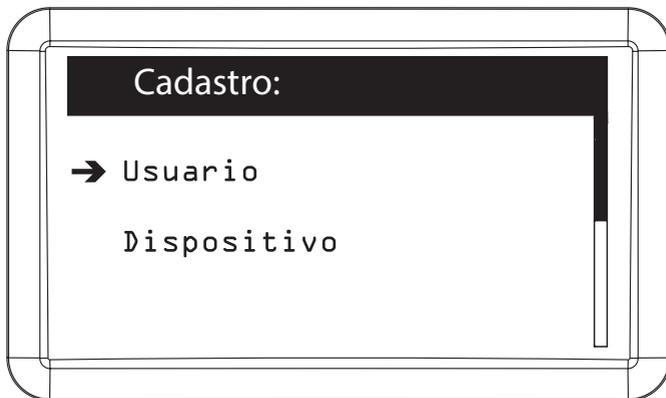
2. Pressionar *OK* ou *Enter* para confirmar. Para cancelar exclusão pressionar *Cancelar* ou *Esc*.





Consultar usuário

Para consultar o cadastro de um usuário é necessário realizar os seguintes passos:



Usuario/Buscar :
 Buscar Usuario:
 Nome: ■
 Apto:

O usuário pode ser encontrado através de seu nome ou do número do apartamento

Nome(01/01)	Apto	:
→ Usuario	XXX	

Selecionar o usuário para consultar as suas configurações

Pressionar *Cancelar* ou *ESC* para sair.

Excluir usuário

Para excluir o cadastro de um usuário é necessário realizar os seguintes passos:

Cadastro:
 → Usuario
 Dispositivo

Usuario:

Editar

Consultar

→ Excluir

Usuario/Buscar :

Buscar Usuario:

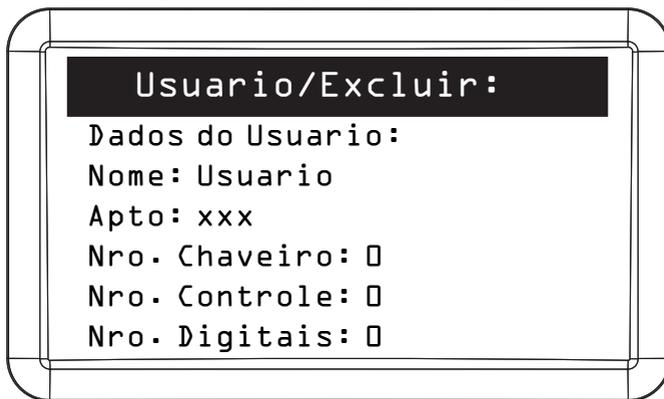
Nome: ■

Apto:

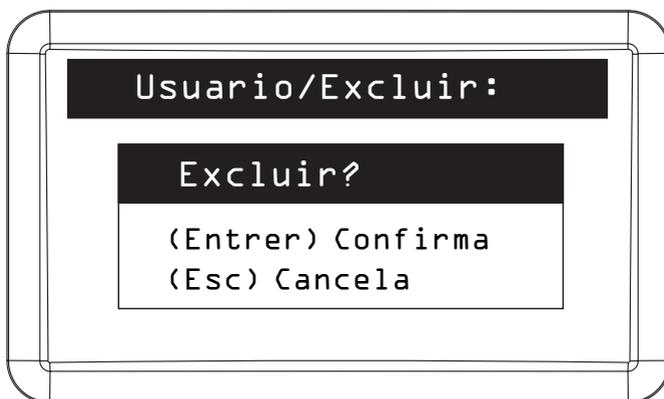
O usuário pode ser encontrado através de seu nome ou do número do apartamento

Nome(01/01) Apto :	
→ Usuario	XXX

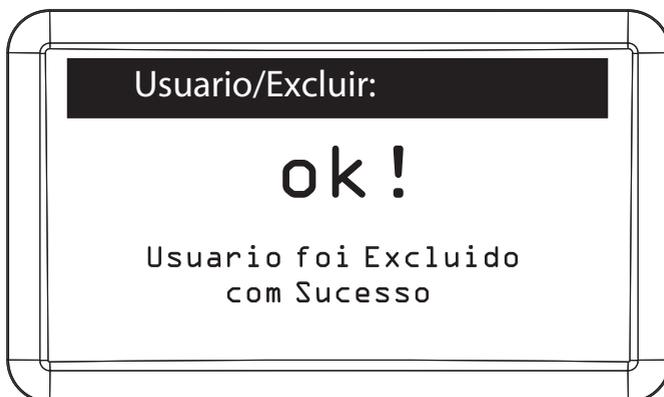
Selecionar o usuário que deseja excluir



Pressionar *Ok* ou *Enter* para continuar;



Pressionar *OK* ou *Enter* para confirmar. Para cancelar exclusão pressionar *Cancelar* ou *Esc*.



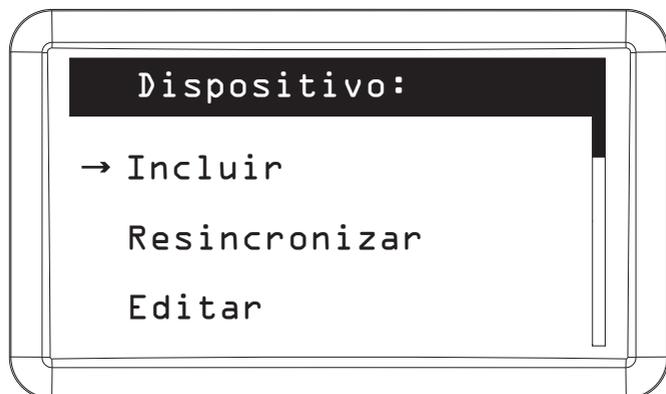
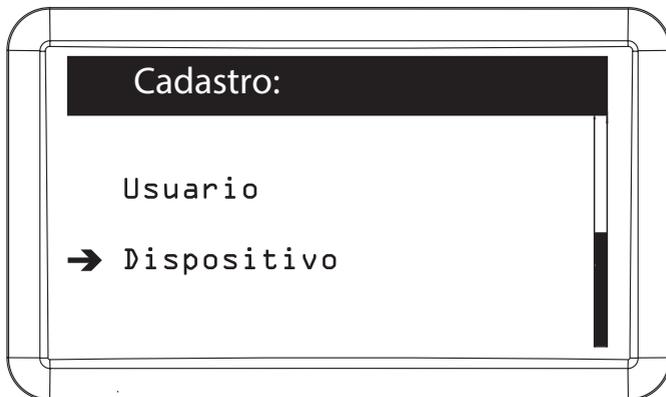
Obs.: com a exclusão do usuário todos os chaveiros RFID Mifare, TAG veicular, controles remotos e digitais dele serão excluídos, portanto esta operação deve ser feita com cautela.

Atenção: caso algum dispositivo esteja desconectado do MIP durante esse processo o morador pode não ter seu acesso bloqueado. Fica a cargo do usuário garantir que todos os dispositivos estejam em comunicação com o MIP.

Dispositivo

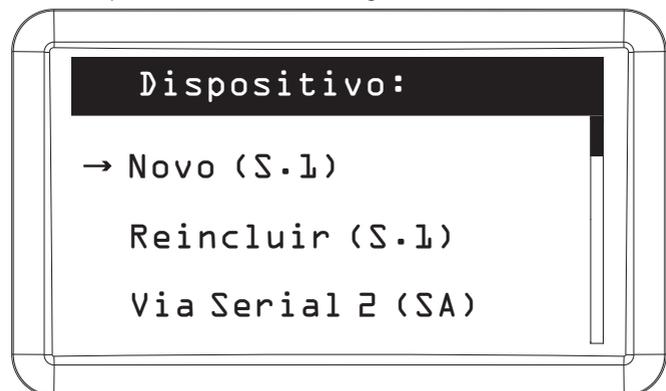
Incluir dispositivo

Para cadastrar um dispositivo é necessário realizar os seguintes passos:



A partir da versão 170405, o MIP conta com mais um processo de inclusão de dispositivos que não exige a troca do dispositivo do barramento *SERIAL_1* para a *SERIAL_2*, permitindo que o dispositivo seja instalado no seu local e depois cadastrado pelo MIP.

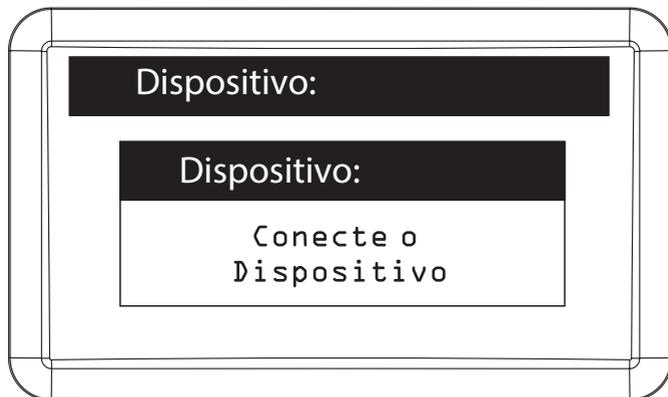
Dessa forma, a tela de *Inclusão* para versões mais novas é da seguinte forma:



Aqui temos três formas de adicionar um dispositivo:

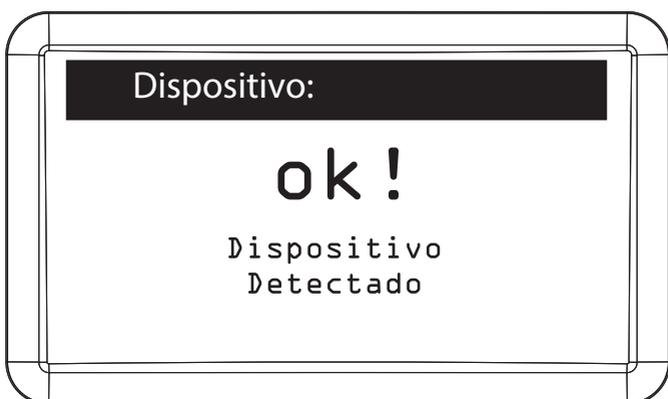
- » **Novo (S.1):** adiciona um novo dispositivo ao sistema utilizando a *SERIAL_1* para cadastro.
 - » **Reincluir (S.1):** reinclui um dispositivo já cadastrado. Uso para quando se deseja substituir um dispositivo defeituoso e não se quer perder as configurações.
 - » **Via SERIAL_2 (SA):** procedimento novo, que combina o melhor das duas opções acima, sendo este item descrito de forma melhor a seguir.
- » **Novo (S.1)**

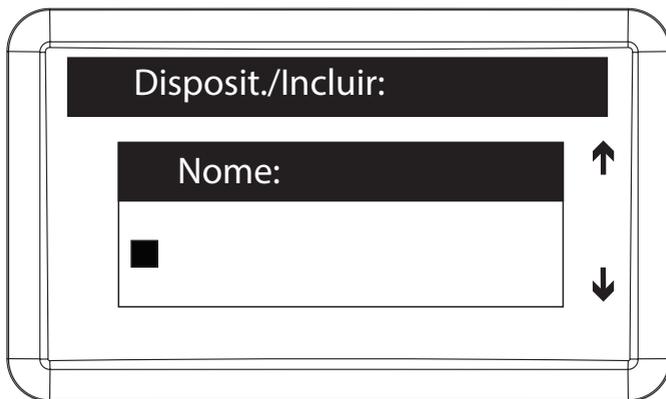
Assim, esta primeira opção para cadastro permite adicionar um novo dispositivo ao sistema utilizando a *SERIAL_1* do MIP e para isso temos que seguir o procedimento:



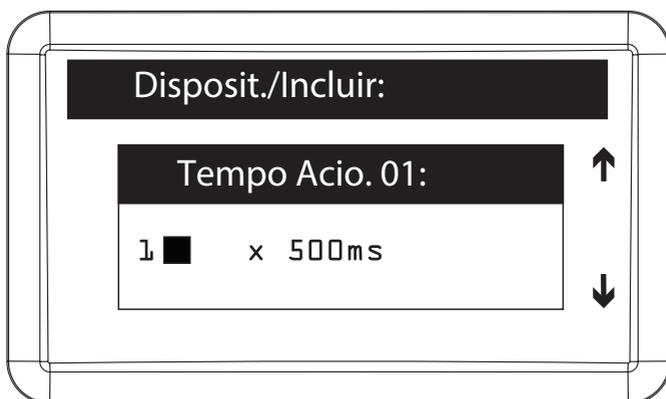
Obs.: o dispositivo que será cadastrado precisa estar alimentado e ligado individualmente, via barramento serial 1, via barramento serial, com o MIP.

Utilizar o conector *SERIAL_1* para o cadastro do dispositivo.

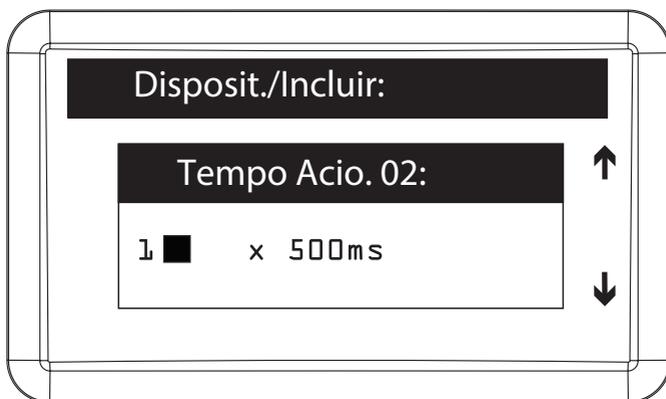




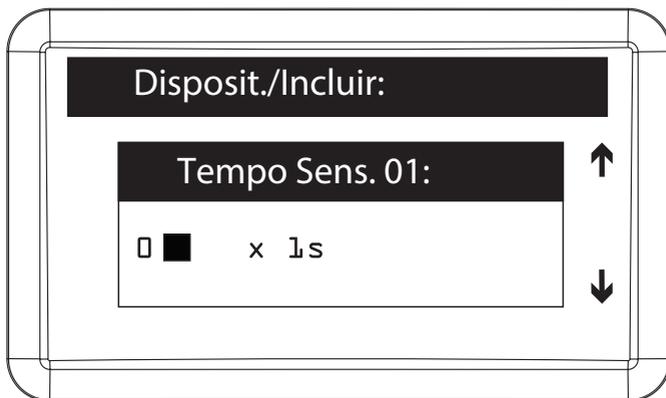
Nomear o dispositivo que está sendo cadastrado



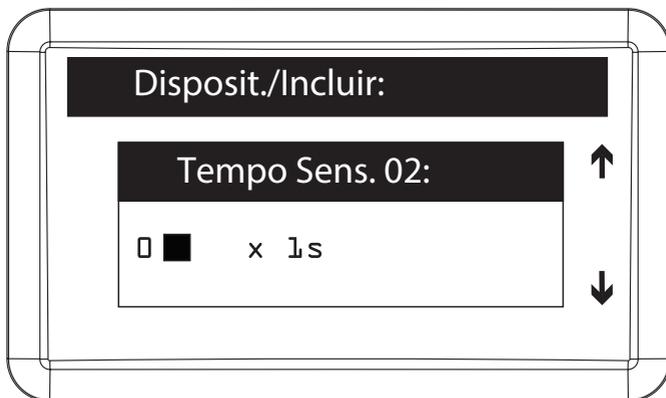
Configurar o tempo, múltiplo de 0,5 segundo, de acionamento da saída 01 do dispositivo. O valor máximo deste campo é 99, sendo equivalente a 49,5 segundos



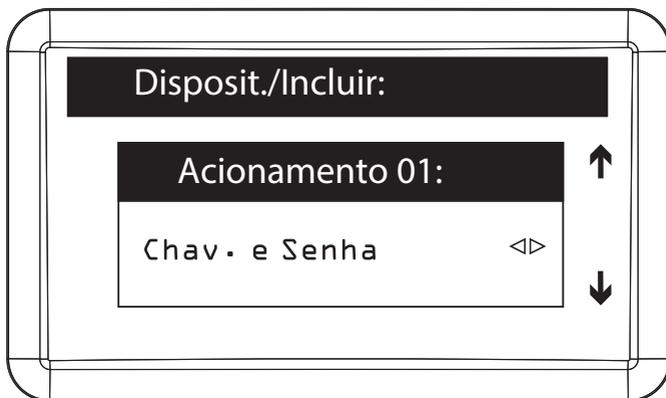
Configurar o tempo, múltiplo de 0,5 segundo, de acionamento da saída 02 do dispositivo. O valor máximo deste campo é 99, sendo equivalente a 49,5 segundos



Configurar o tempo, múltiplo de 1 segundo, entre a abertura do sensor 01 e o disparo do aviso sonoro. O valor máximo deste campo é 99, sendo equivalente a 99 segundos. Caso este campo seja configurado com 0, desabilita a função de sensor de porta aberta para este dispositivo



Configurar o tempo, múltiplo de 1 segundo, entre a abertura do sensor 02 e o disparo do aviso sonoro. O valor máximo deste campo é 99, sendo equivalente a 99 segundos. Caso este campo seja configurado com 0, desabilita a função de sensor de porta aberta para este dispositivo



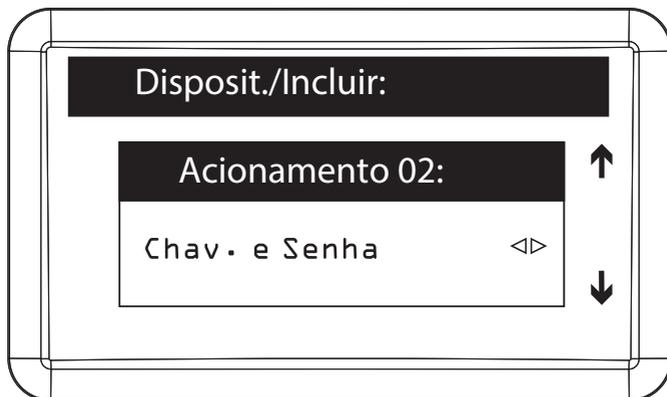
Importante:

Se o dispositivo cadastrado for o XRE 1000, configurar qual botão do controle remoto (*Power, A, B*) acionará a sua saída 01.

Se o dispositivo cadastrado for o XLT 1000 ID ou XPE 1001/1013 ID (imagem acima), configurar se a sua saída 01 poderá ser acionada através de chaveiro RFID (Mifare) e senha (padrão de fábrica), somente chaveiro RFID (Mifare) (disponível somente em versões 170405 ou superior) ou somente senha.

Se o dispositivo cadastrado for biométrico, possui somente a saída 01 e esta poderá ser configurada para digital e chaveiro ou somente digital.

Controladora de antena veicular, possui somente a saída 01 e permite configurar como somente chaveiro.

**Importante:**

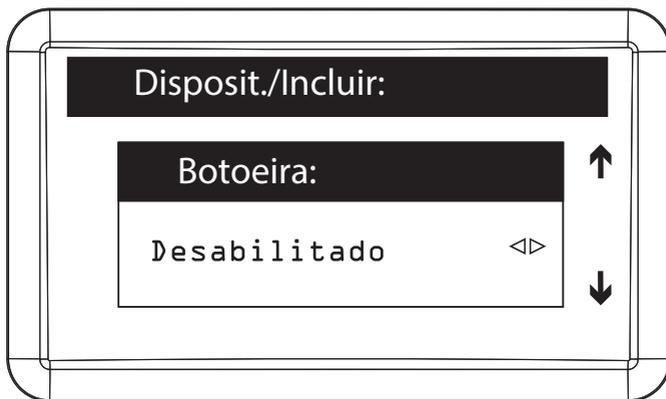
Se o dispositivo cadastrado for o XRE 1000, configurar qual botão do controle remoto (*Power, A, B*) acionará a sua saída 02.

Se o dispositivo cadastrado for o XLT 1000 ID ou XPE 1001/1013 ID, configurar se a sua saída 02 poderá ser acionada através de chaveiro RFID (Mifare) e senha (padrão de fábrica) somente chaveiro RFID (Mifare) (disponível somente em versões 170405 ou superior) ou somente senha.



É possível habilitar a função de Intertravamento nos dispositivos com esta funcionalidade (XPE 1001/1013 ID, XLT 1000ID e XRE 1000). Com esta função habilitada, uma das saídas só será acionada se o sensor da outra saída estiver fechado, ou seja, uma das portas/portões só abre se a outra estiver fechada.

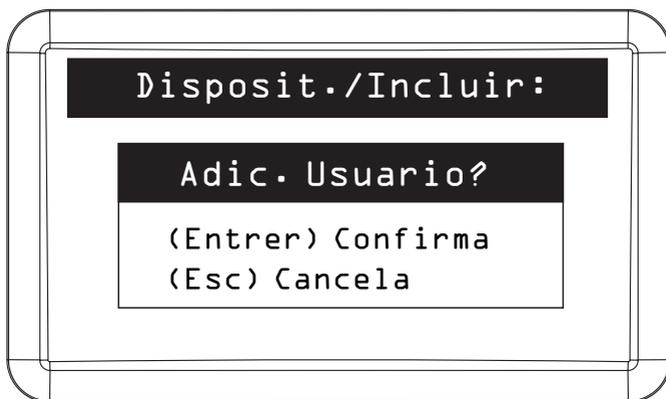
Obs.: verificar exemplos de instalação com intertravamento nos guias dos dispositivos.



É possível habilitar uma das entradas de sensor do dispositivo para utilizar uma botoeira. Para os dispositivos biométricos e controladoras, a botoeira está sempre habilitada.

Se a botoeira for configurada como *Sen.1&Fech.1*, quando a mesma for pressionada, acionará a saída 1 do dispositivo cadastrado. O mesmo irá ocorrer se for configurada como *Sen.2&Fech.2*, ela acionará a saída 2 do dispositivo.

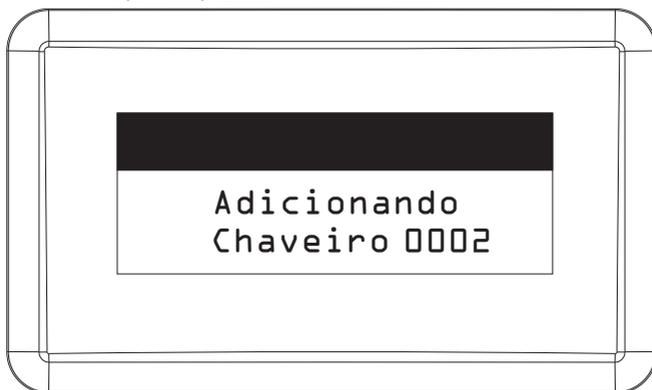
Confirmar com *Ok* ou *Enter* para continuar.



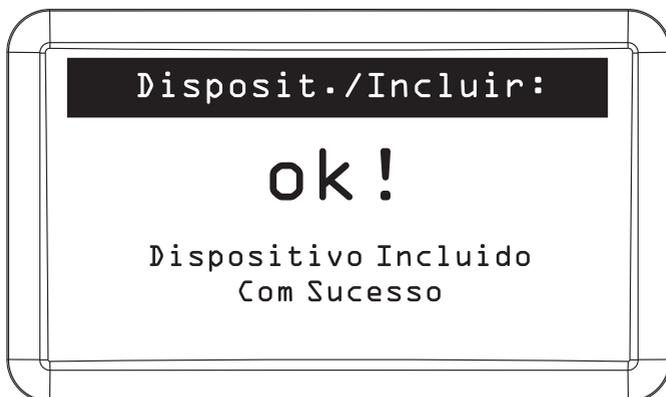
Pressionar *Ok* ou *Enter* para adicionar todos os usuários do sistema para terem acesso ao dispositivo cadastrado. Caso pressione *Cancelar* ou *ESC*, o dispositivo será incluso mas nenhum usuário terá acesso a ele;

- Obs.:** » Para as versões de MIP acima de 170405, podemos ter dois processos diferentes na adição de um novo dispositivo.
- » Para dispositivos com firmware anteriores a versão autônoma, o MIP somente adicionará internamente a permissão para que os usuários cadastrados possam usar o dispositivo.
 - » Para dispositivos com firmware na versão autônoma, se foi escolhido o processo de adição dos usuários, o MIP enviará todos os elementos de acesso dos usuários para o dispositivo recém adicionado. Essa adição obedece a capacidade de tipo de elemento para cada dispositivo.

Esse processo, para o XLT 1000 ID por exemplo, será sinalizado com uma tela semelhante a exibida a seguir:



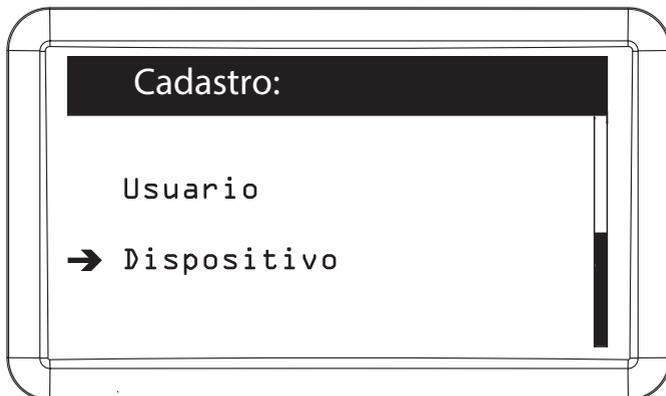
Se o processo for feito corretamente, teremos a indicação da tela abaixo:

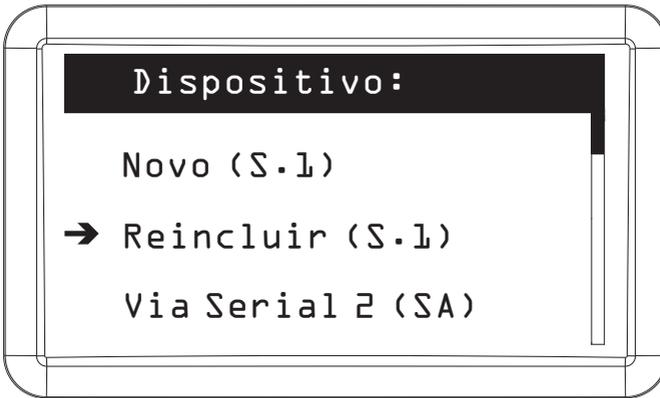
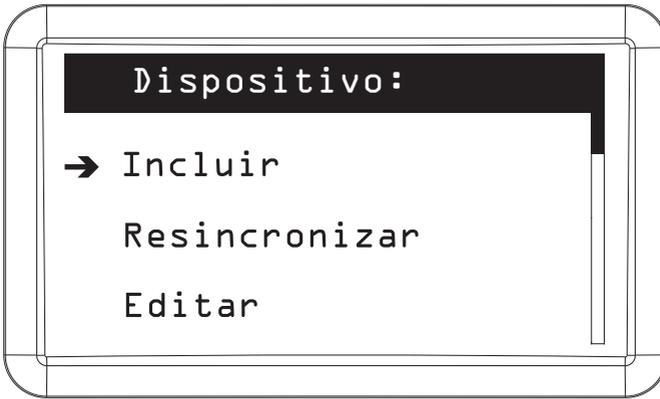


Reincluir (S.1)

Este comando é utilizado quando um dispositivo apresentar problema e precisar ser trocado por outro do mesmo modelo. O novo dispositivo será cadastrado no sistema com as configurações do anterior. Para substituir o anterior é necessário realizar os seguintes passos:

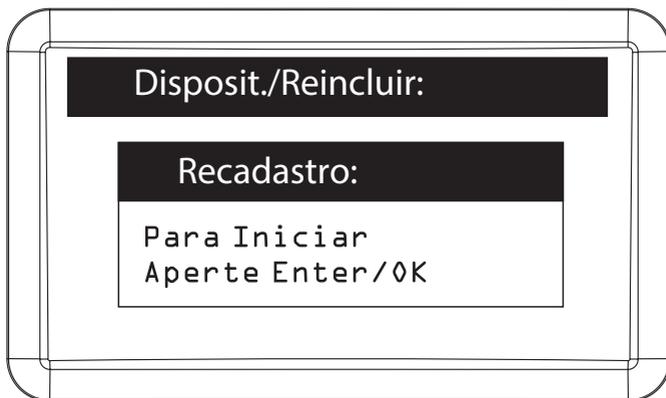
Importante: antes de executar as funções abaixo, o dispositivo deve estar ligado no conector *SERIAL_1* do MIP, respeitando as polaridades *A* e *B*.





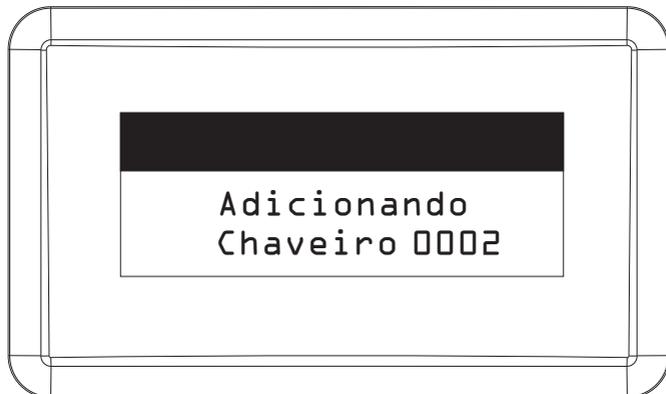
Nome	(01/03)	End
→ XPE 1013 id		2
XLT		3
XRE		4

Selecionar o dispositivo que será substituído

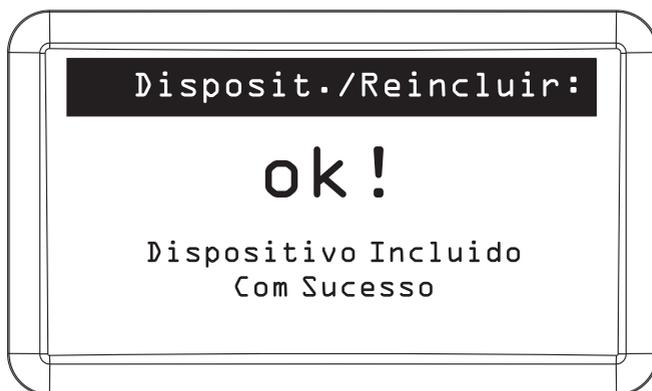


- Obs.:** » Para as versões de MIP acima de 170405, podemos ter dois processos diferentes na reinclusão de um novo dispositivo.
- » Para dispositivos com firmware anteriores a versão autônoma, o MIP somente adicionará os dados de cadastro do dispositivo existentes no MIP.
 - » Para dispositivos com firmware na versão autônoma, o MIP enviará todas as configurações deste dispositivo e os elementos de acesso dos usuários liberados para uso do dispositivo configurado anteriormente. Essa adição obedece a capacidade de tipo de elemento para cada dispositivo. Assim, para o XLT 1000 ID e os XPE 10xx ID serão enviados os códigos dos chaveiros RFID (Mifare) e das senhas de cada usuário, já para o XRE 1000 será enviado os códigos de cada controle cadastrado atualmente no MIP. Para o Bio Inox Plus SS 311 MF serão enviados os templates das digitais e os códigos dos chaveiros RFID (Mifare). Para a CT 500 1P serão enviados os códigos dos chaveiros RFID (Mifare e UHF).

Esse processo, para o XLT 1000 ID por exemplo, será sinalizado com uma tela semelhante a vista a seguir:



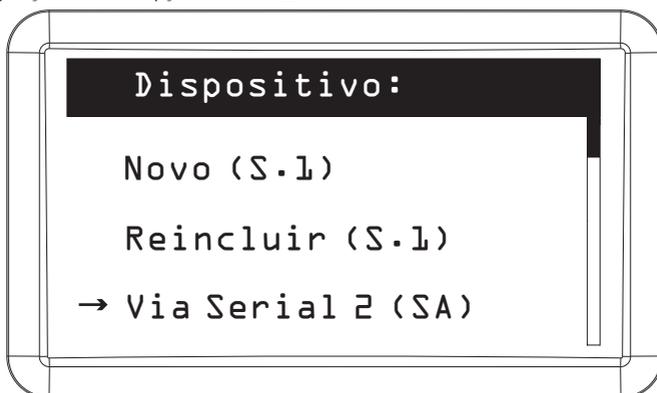
Se o processo for feito corretamente, teremos a indicação da tela abaixo:



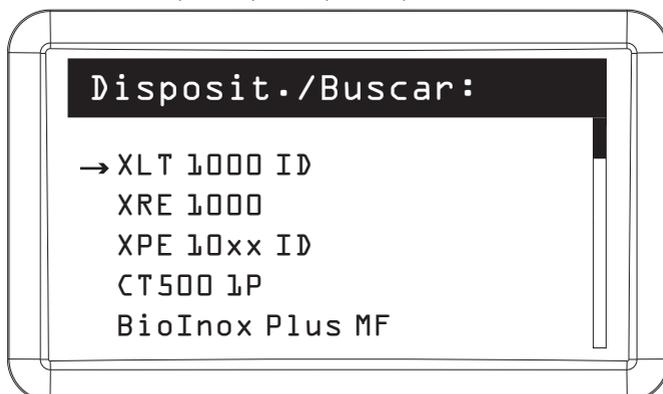
O dispositivo foi substituído

» **Via SERIAL_2 (SA)**

Este tipo de cadastro só é encontrado em versões do MIP acima da versão 170405 e só permite a busca de dispositivos que estão com o firmware atualizado para funcionamento em modo *Autônomo*. Esse item permite a busca dos dispositivos de cada tipo que estão conectados no barramento *SERIAL_2* e a posterior inclusão ou reinclusão destes dispositivos. Para acessar essa configuração escolha a opção *Via SERIAL_2*:



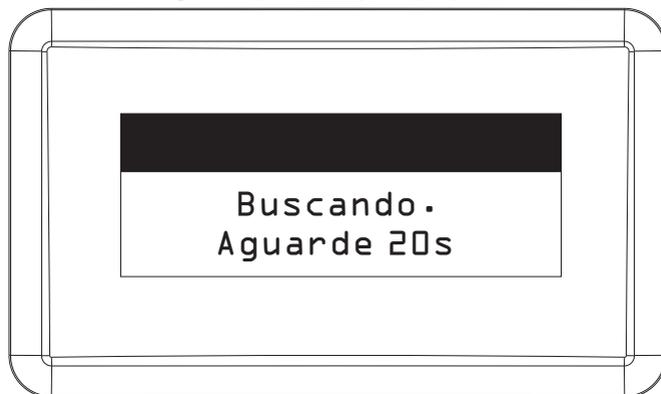
Após a escolha deste item, selecione o tipo de dispositivo que você quer adicionar (ou reincluir):



Após a escolha do tipo de dispositivo, o MIP iniciará um processo de busca no barramento SERIAL_2 destes dispositivos durante trinta segundos.

Obs.: neste processo é necessário que o barramento esteja sem problemas de cabeamento ou de comunicação, respeitando os parâmetros que foram estabelecidos anteriormente.

Durante a busca, será exibida a tela a seguir, informando o tempo faltante para o encerramento da busca:



Depois de passado o tempo de busca, se algum dispositivo do tipo escolhido for encontrado, ele será listado conforme a tela a seguir. Nesta tela temos o resultado de uma busca do tipo de dispositivo XLT 1000 ID.

Ilustração de uma tela de resultados de busca. A tela exibe uma tabela com o seguinte conteúdo:

Nome	(01/03)	End
→ XLT 1000 ID		255
Leitor Lobby		2
Leitor Porta P.		4

Na tela acima podemos tirar as seguintes informações:

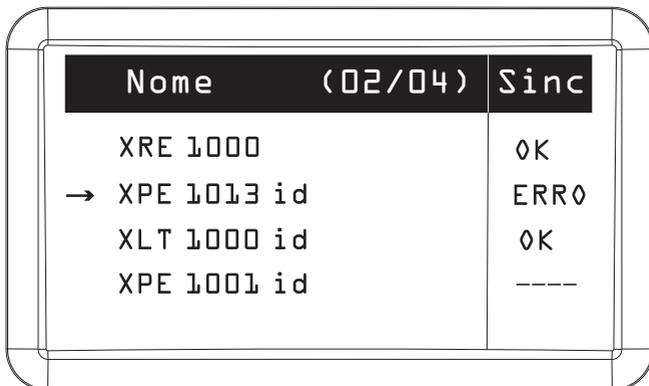
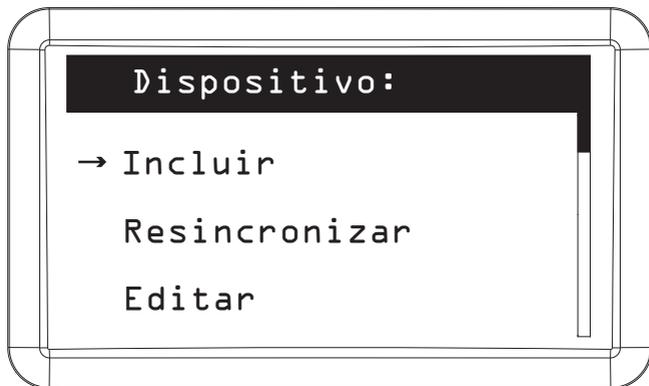
- » O primeiro dispositivo está indicado pelo nome do produto do dispositivo com o endereço 255, indicando que o mesmo está resetado e não cadastrado no MIP.
- » O segundo dispositivo, está com um endereço que já está cadastrado no MIP. Mas isso não significa que o mesmo está plenamente funcional, significa somente que o dispositivo foi encontrado e já tem um endereço. Então se selecionarmos este equipamento ele será atualizado com todas as informações do dispositivo cadastrado no MIP, suas permissões e suas configurações, apagando todas as informações que ele tinha anteriormente.

Obs.: » Há casos que nenhum dispositivo pode ser encontrado no barramento, mesmo que tudo esteja correto. Isso se deve a possíveis interferências de dispositivos que não estejam atualizados para a versão autônoma e por isso os mesmos devem ser retirados do barramento durante o processo de busca. Para evitar esse problema, encorajamos que todos os dispositivos sejam atualizados pois há um ganho enorme de funcionalidade.

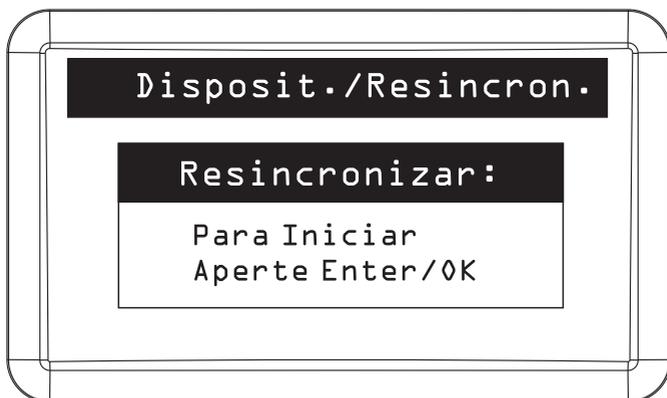
- » É importante que dispositivos que já tenham sido utilizados em outro MIP sejam resetados antes de serem incluídos no MIP, evitando conflito de endereços.

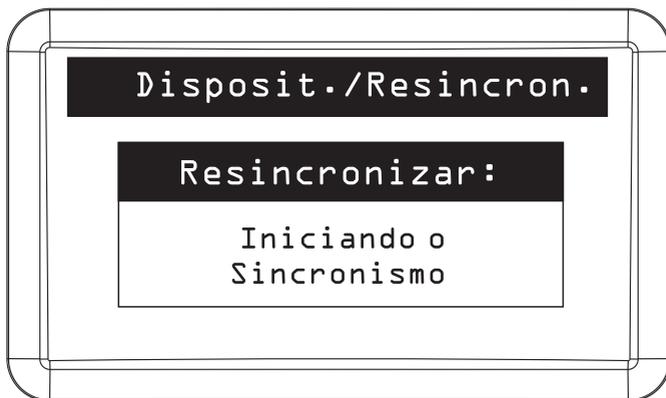
Resincronizar

Ao realizar configurações no MIP o mesmo automaticamente irá sincronizar as modificações com os dispositivos, porém se algum dispositivo estiver sem comunicação com o barramento durante um período maior que cinco minutos, este sincronismo pode não acontecer, sendo necessário realizar a resincronização manualmente. O ícone *Notificação* irá sinalizar caso exista esta necessidade. Para resincronizar o dispositivo é necessário realizar os seguintes passos:

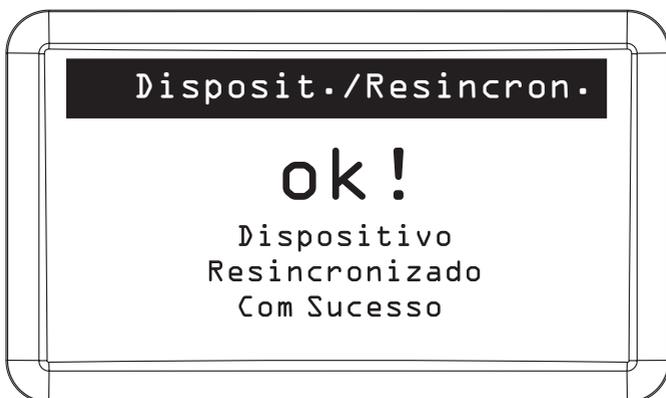


Selecione o dispositivo com sinalização de *Erro* para realizar o resincronismo. Lembrando que esta função só está presente nos dispositivos com a versão de firmware com a função *Autônoma*. Para versões de firmware anteriores, o dispositivo necessita do MIP para liberar os acessos e por isso será exibido ---- na coluna de *Sinc*, sinalizando que essa função está indisponível.



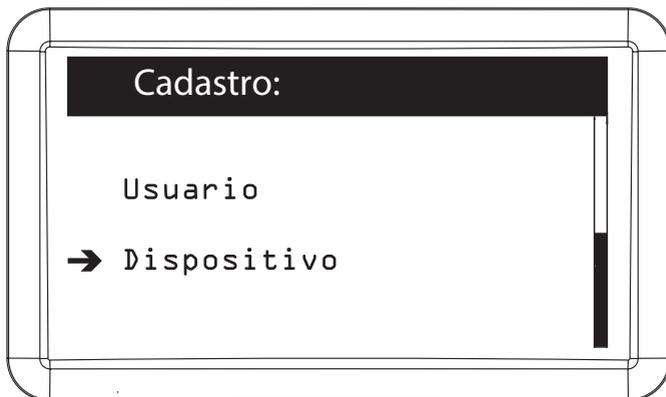


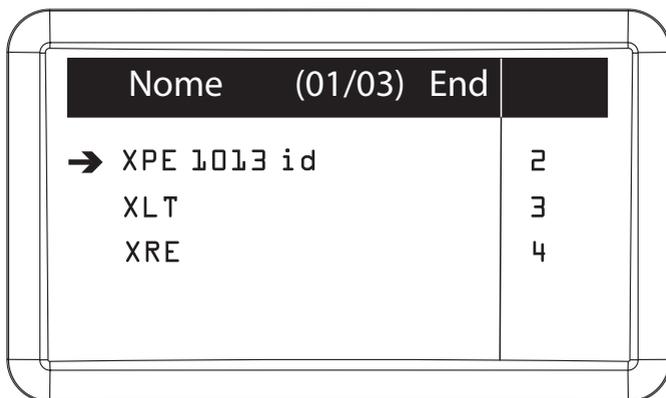
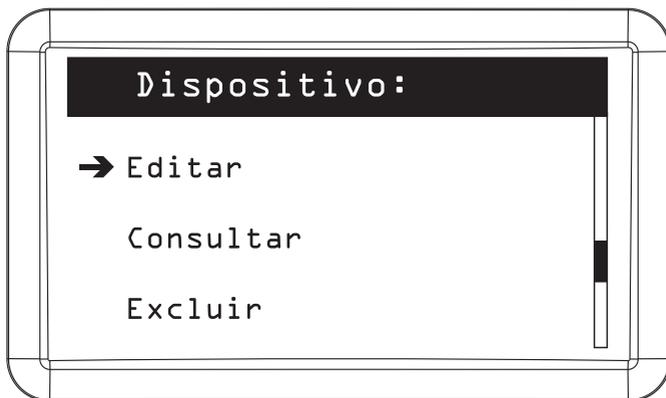
Nesta etapa, serão enviados os dados de cadastro para os dispositivos que possuem as versões *Não autônoma*. Para versões *Autônomas*, além das informações de cadastro também serão enviados os elementos de acesso compatíveis com o tipo de dispositivo a ser resincronizado.



Editar dispositivo

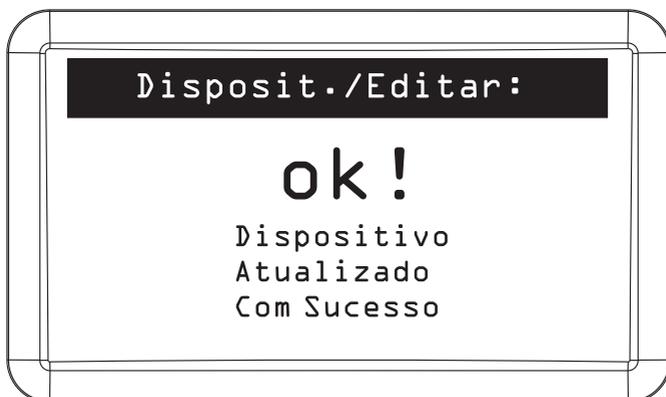
Para editar o cadastro de um dispositivo é necessário realizar os seguintes passos:





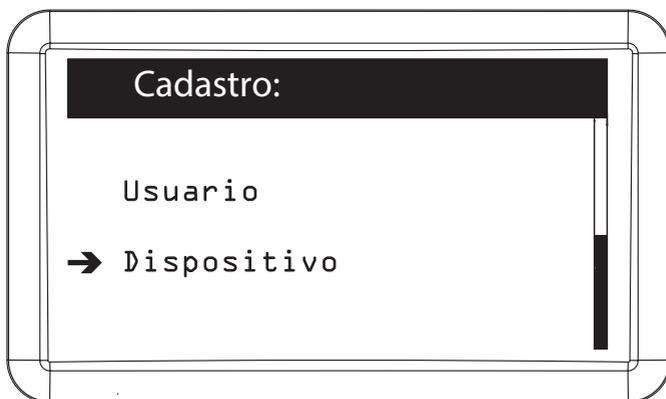
Selecionar o dispositivo para realizar as alterações necessárias

Confirmar com *Ok* ou *Enter* para salvar as alterações realizadas.



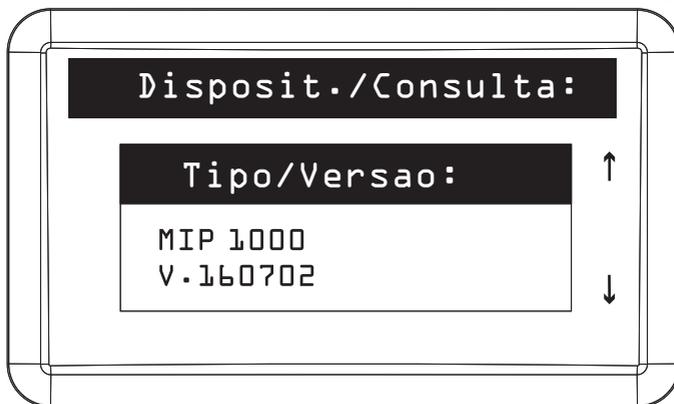
Consultar dispositivo

Para verificar as informações cadastradas nos dispositivos e a versão de firmware destes e do MIP 1000, é necessário utilizar este menu. Para realizar a consulta é necessário realizar os seguintes passos:



Nome	(01/05)	End.
→ MIP 1000		1
XRE 1000		2
XPE 1013 id		3
XLT 1000 id		4
XPE 1001 id		5

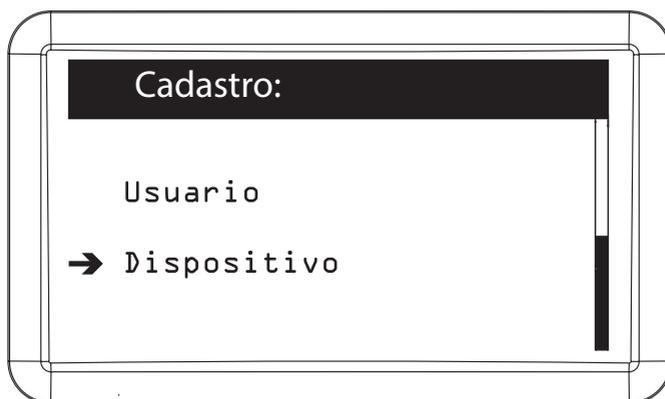
Selecionar o dispositivo para consultar as suas configurações. Nas versões de MIP igual ou superior a 170405, um dos itens adicionais que poderão ser consultados é a versão do firmware dos dispositivos já cadastrados e se eles são autônomos ou não (indicado pelo texto *S. Alone* após a versão). Um exemplo de exibição da versão pode ser visto a seguir:



Pressionar *Cancelar* ou *ESC* para sair.

Excluir dispositivo

Para excluir o cadastro de um dispositivo é necessário realizar os seguintes passos:



Nome	(01/03)	End
→ XPE 1013 id		2
XLT		3
XRE		4

Selecionar o dispositivo que deseja excluir

Disposit./Excluir :

Dados do Disposit.:

Nome:

ID:

Tipo:

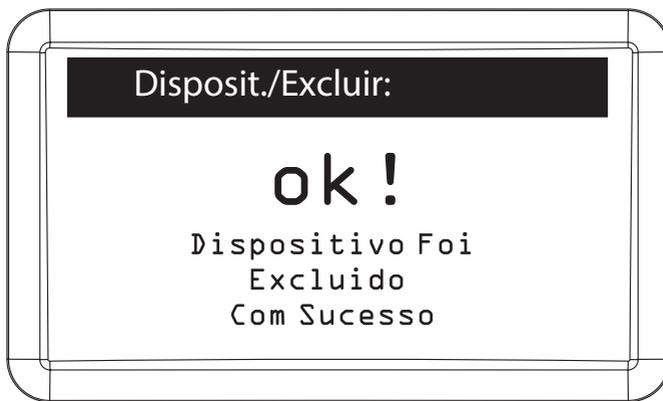
Pressionar *Ok* ou *Enter* para continuar.

Disposit./Excluir:

Excluir?

(Enter) Confirma

(Esc) Cancela

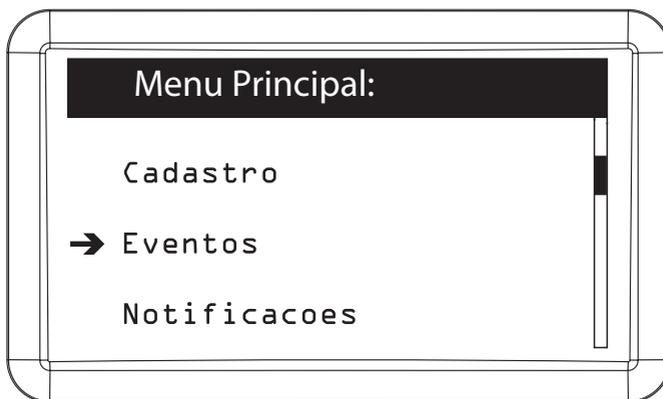


Obs.: ao excluir o dispositivo, ele não será mais acessado pelo MIP. Com isso, todos os usuários terão seu acesso bloqueado e se o mesmo estiver disponível no barramento com o firmware atualizado para o modo Autônomo, o mesmo será resetado, voltando às configurações de fábrica.

5.7. Eventos

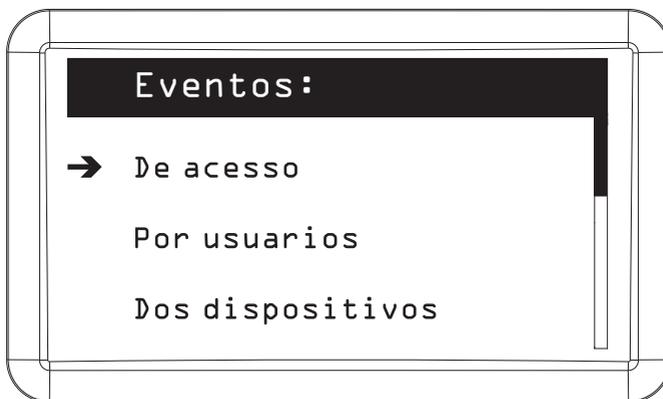
Para consultar todos os eventos de acesso registrados e/ou os últimos cinco eventos por usuário e/ou os últimos cinco eventos de dispositivo, entrar na opção *Eventos* do Menu Principal.

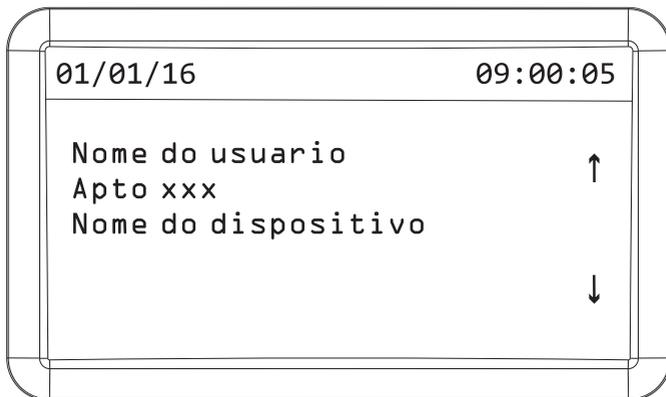
Obs.: é possível gerar relatórios detalhados de todos os eventos registrados através do software SGA.



De acesso

Para consultar todos os eventos de acesso registrados no sistema é necessário realizar os seguintes passos:



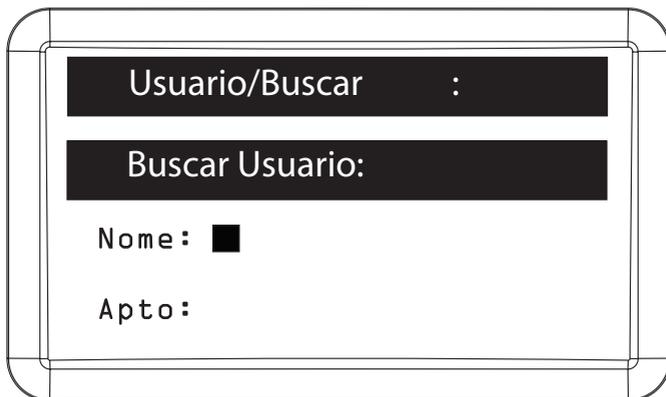
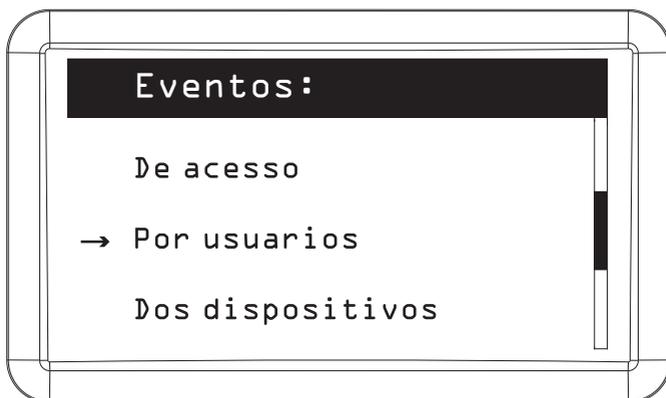


Pressionar *Cancelar* ou *ESC* para sair.

Obs.: caso na tela de eventos apareça a mensagem Registro pelo disp., significa que este evento ocorreu quando o dispositivo, em modo Autônomo, fez o registro quando estava sem comunicação com o MIP. Outra mensagem que pode aparecer é Pânico acionado, indicando o acionamento das saídas através de coação.

Por usuário

Para consultar os últimos cinco eventos registrados por um usuário específico é necessário realizar os seguintes passos:



O usuário pode ser encontrado através de seu nome ou do número do apartamento

Nome (01/01) Apto :	
→ Usuario	XXX

Selecionar o usuário no qual deseja consultar os últimos cinco eventos

Eventos		(01/05)
→ 02/01	11:43	XRE 1000
02/01	11:41	XRE 1000
01/01	20:16	XLT 1000 id
01/01	16:29	XPE 1001 id
01/01	16:28	XPE 1013 id

Selecionar o evento que deseja consultar

02/01/16	11:43:21
Nome do usuario	
Apto xx	
XRE 1000	

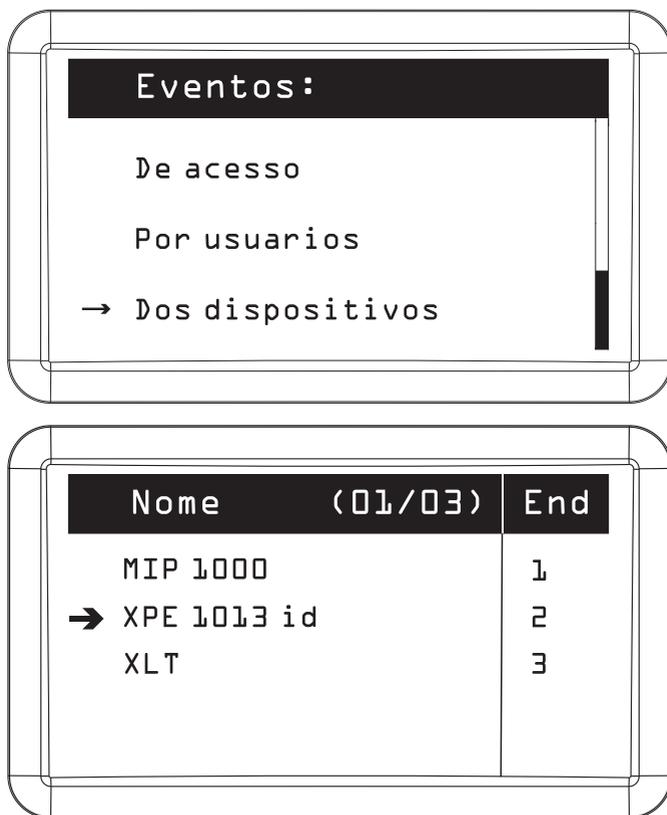
Pressionar *Ok* ou *Enter* para sair.

Por dispositivo

Os eventos por dispositivo podem sinalizar:

- » **Tout.ON:** evento que indica o dispositivo que ficou fora da rede por mais de cinco segundos.
- » **Tout.OFF:** evento que indica a volta do dispositivo ao barramento.
- » **Sen1.ON:** evento que indica a ativação do sensor 01 do dispositivo.
- » **Sen1.OFF:** evento que indica a desativação do sensor 01 do dispositivo.
- » **Sen2.ON:** evento que indica a ativação do sensor 02 do dispositivo.
- » **Sen2.OFF:** evento que indica a desativação do sensor 02 do dispositivo.
- » **TAC1.ON:** evento que indica o acionamento da tecla 01 de acesso rápido.
- » **TAC2.ON:** evento que indica o acionamento da tecla 02 de acesso rápido.
- » **TAC3.ON:** evento que indica o acionamento da tecla 03 de acesso rápido.
- » **TAC4.ON:** evento que indica o acionamento da tecla 04 de acesso rápido.
- » **TAC5.ON:** evento que indica o acionamento da tecla 05 de acesso rápido.
- » **TAMP.ON:** evento que indica o disparo do tamper (violação) do equipamento.

Para consultar os últimos cinco eventos registrados por dispositivo é necessário realizar os seguintes passos:



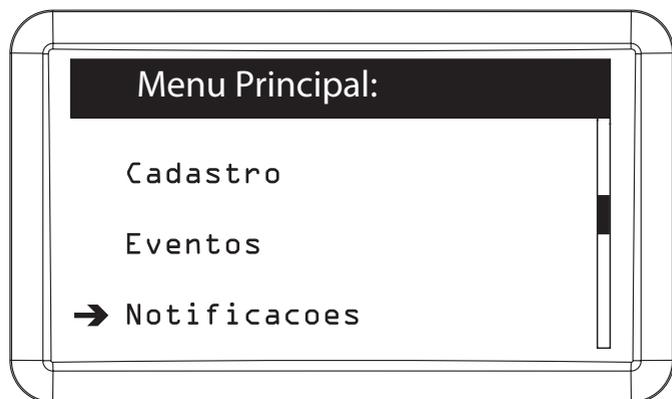
Selecionar o dispositivo no qual deseja consultar os últimos cinco eventos

Eventos		(02/05)
05/01	11:41	TAMP.0N
→ 04/01	10:30	TOUT.0FF
04/01	10:27	TOUT.0N
02/01	20:16	TAMP.0N
02/01	16:28	SEN1.0FF

Pressionar *Ok* ou *Enter* para sair.

5.8. Notificações

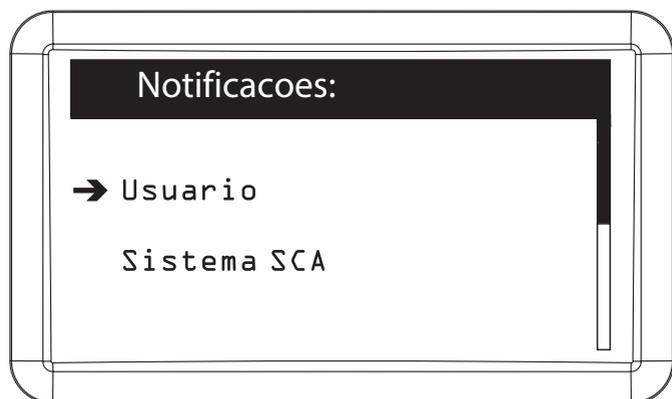
Para consultar as notificações de usuário ou do sistema SCA, entrar na opção *Notificações* do Menu Principal.

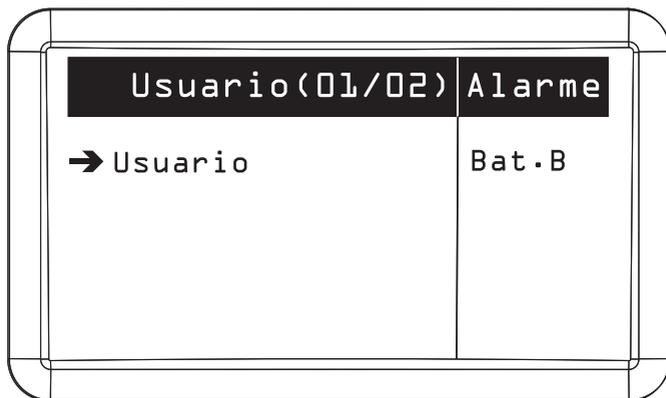


Usuário

As notificações de usuário sinalizam quando o controle remoto do usuário estiver com a bateria baixa.

Para consultar as notificações do usuário é necessário realizar os seguintes passos:



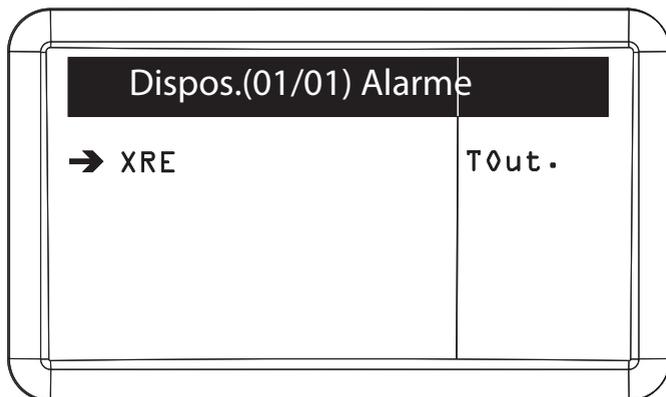
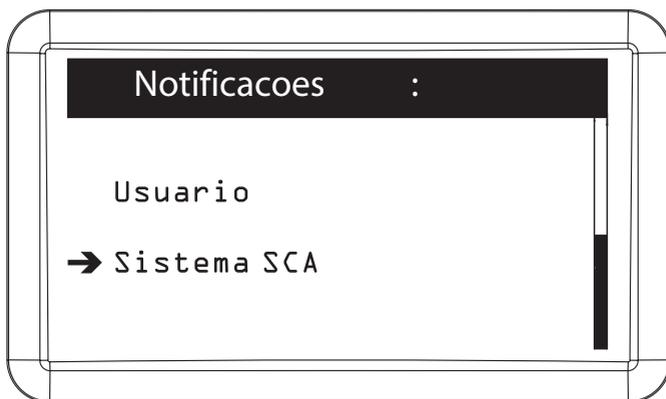


Pressionar *Cancelar* ou *ESC* para sair.

Sistema SCA

As notificações do sistema SCA podem sinalizar se algum dispositivo está fora do barramento (após trinta segundos desconectado), tamper acionado ou se o sensor de porta aberta de algum dispositivo está acionado. Este menu também pode ser acessado através da tecla 2 do teclado, quando o *MIP* estiver na tela de descanso ou inicial.

Para consultar as notificações do sistema SCA é necessário realizar os seguintes passos:

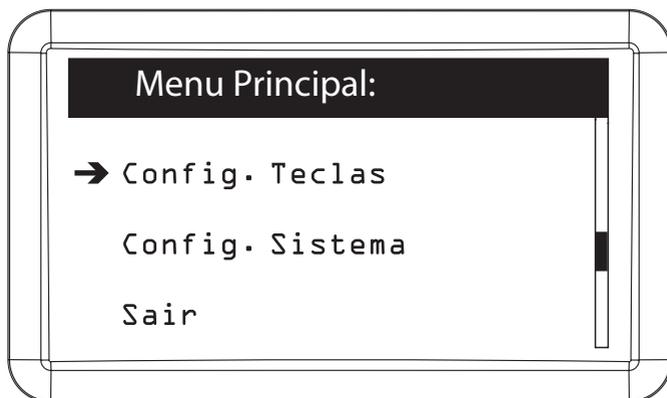


Pressionar *Cancelar* ou *ESC* para sair.

5.9. Configuração de teclas

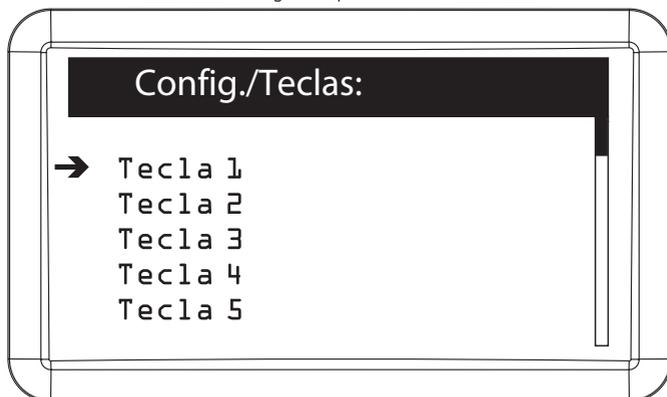
O MIP possui cinco teclas que podem ser configuradas para acionamento de saídas. Estas saídas podem ser de um dispositivo ou do próprio MIP. Quando uma tecla for configurada, ela ficará acesa indicando o funcionamento. Esta tecla também indica, através de piscadas, quando o dispositivo associado a ela está com o sensor disparado, tamper acionado ou em *Time Out*.

Para configurar as teclas de acionamento, entrar na opção *Config. Teclas* do Menu Principal.



Configurar tecla

Para configurar uma tecla é necessário realizar os seguintes passos:



Nome	(01/04)	End
→ MIP 1000		1
XRE		2
XLT		3
XPE 1013		4

Selecionar o dispositivo que terá a saída acionada através de uma tecla do MIP

Config./Teclas:

MIP 1000.:

Acionamento 1 <>

Informar qual das saídas do dispositivo selecionado será acionada pela tecla

Pressionar *Ok* ou *Enter* para confirmar.

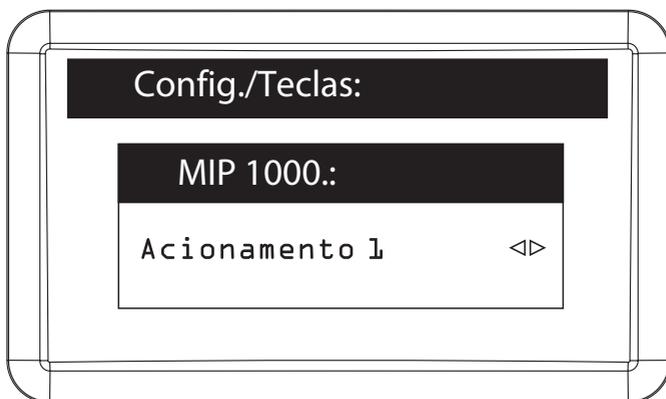
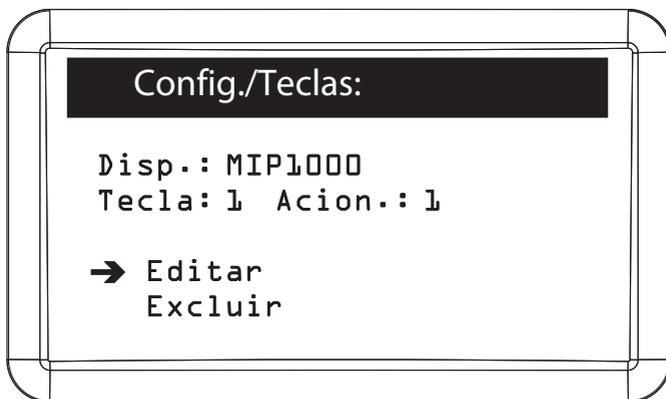
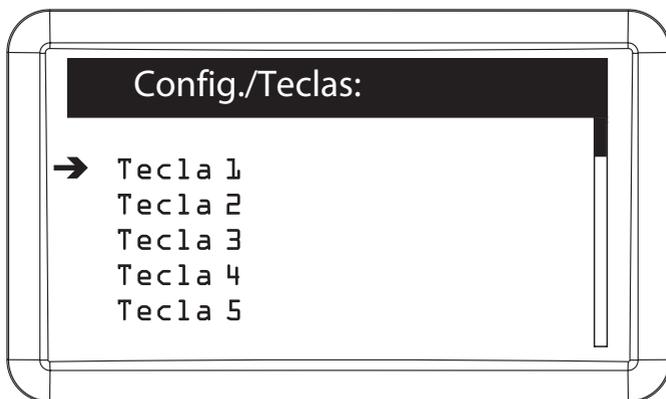
Config./Teclas:

ok !

Tecla
Atualizada
Com Sucesso

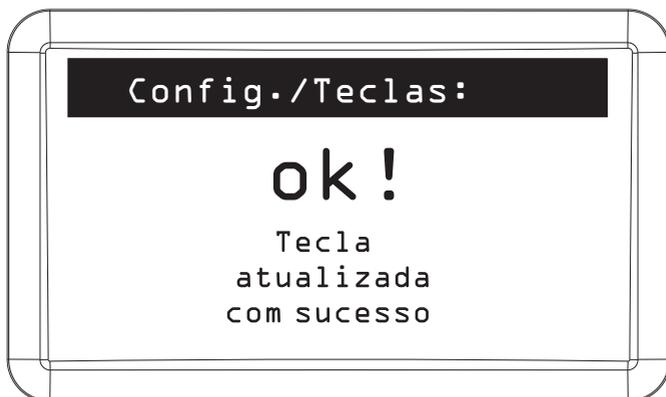
Editar tecla

Para editar uma tecla é necessário realizar os seguintes passos:



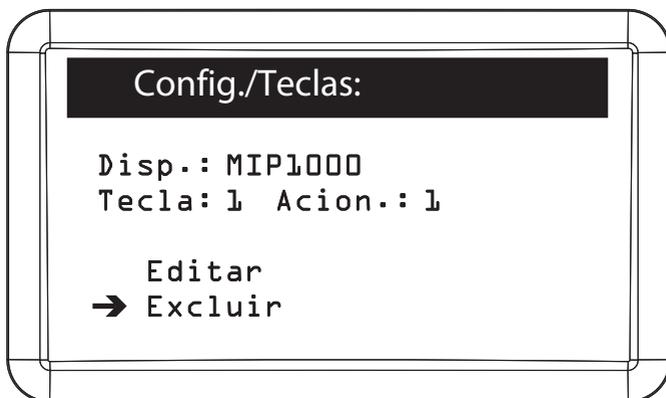
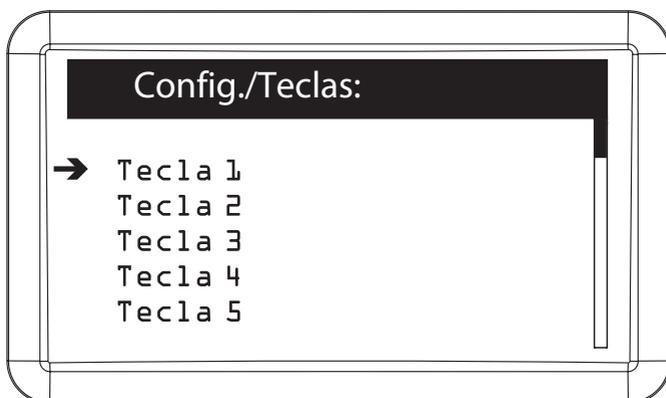
Informar qual das saídas do dispositivo selecionado será acionada pela tecla

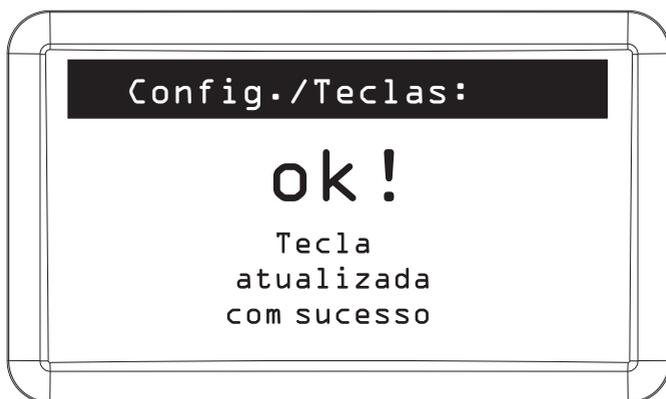
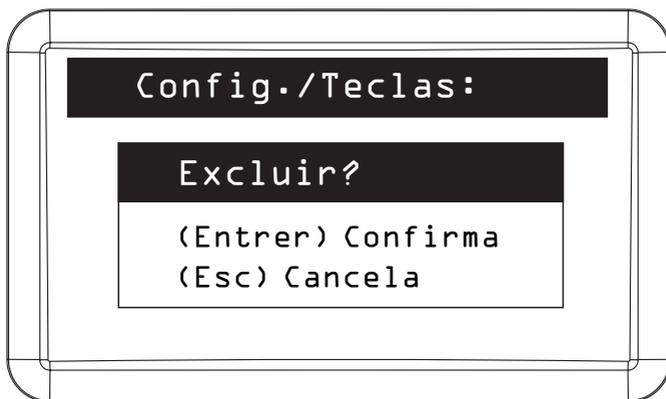
Pressionar *Ok* ou *Enter* para confirmar.



Excluir tecla

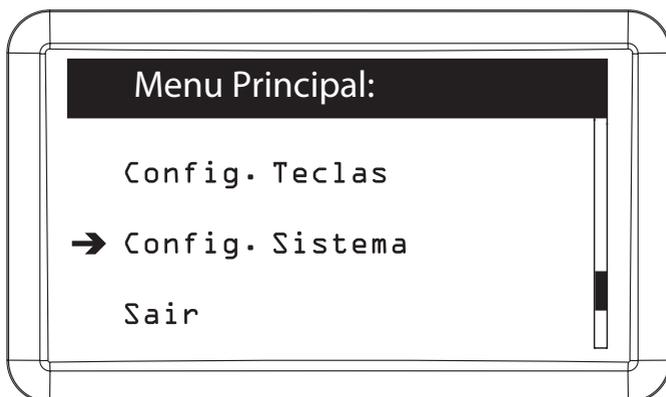
Para excluir uma tecla de acionamento é necessário realizar os seguintes passos:





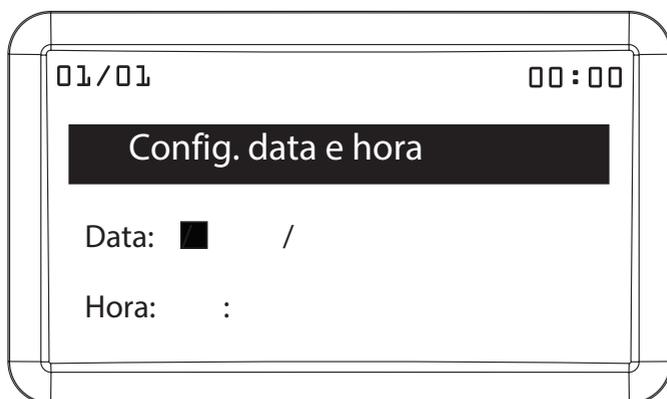
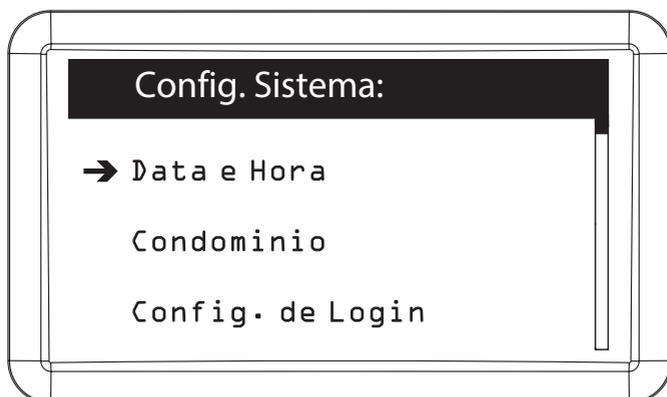
5.10. Configuração do sistema

Para configurar data/hora, informações sobre o condomínio, usuário e senha de autenticação no MIP, desperta porteiro, função pânico, mensagem de descanso, alertas sonoros nos dispositivos e MIP, rótulos, modo de cadastro, temporização, intertravamento, sobreposição de eventos, verificar os status do sistema ou realizar o reset geral no MIP 1000, entre na opção *Config. sistema* do Menu Principal.

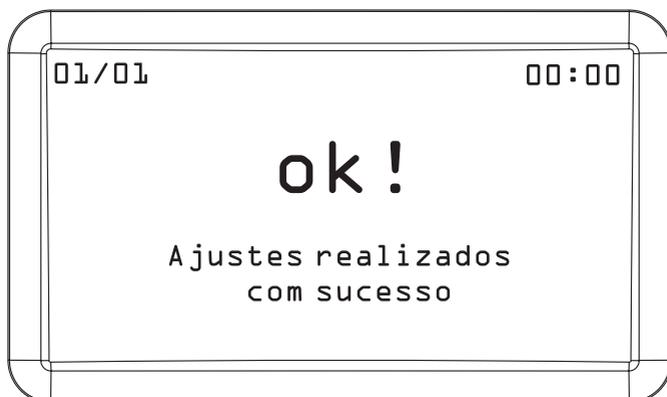


Data e hora

Para configurar ou editar data e hora do sistema é necessário realizar os seguintes passos:

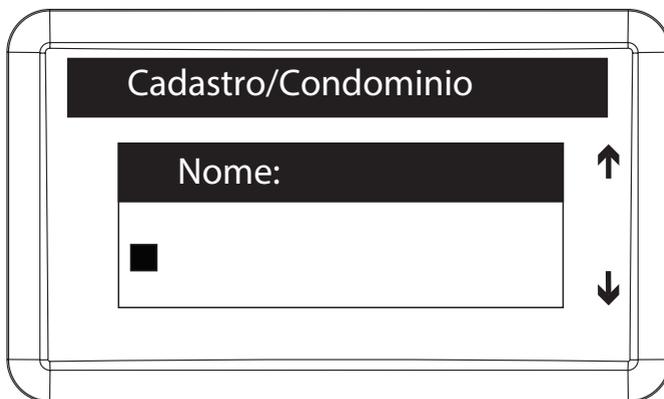
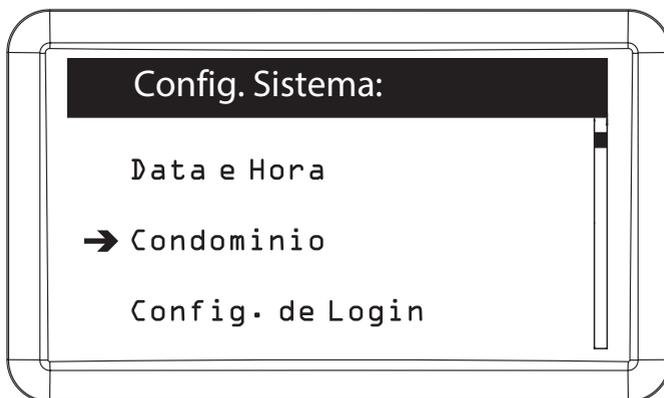


Pressionar *Ok* ou *Enter* para confirmar.



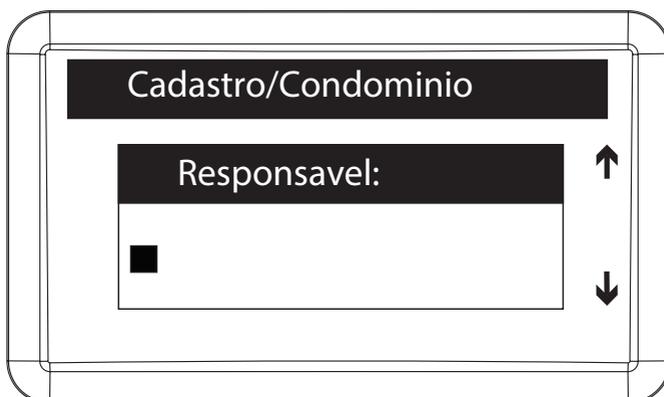
Condomínio

Para configurar ou editar os dados do condomínio é necessário realizar os seguintes passos:



Nomear o condomínio

Obs.: o nome do condomínio ficará visível no display do MIP quando o mesmo estiver na tela inicial.



Identificar o responsável pelo condomínio

Se no item *Modo de cadastro* em *Conf. do sistema* estiver selecionada a opção *Avançado* (padrão de fábrica: *Básico*), no cadastro do condomínio também poderão ser inseridas as seguintes informações:

The screenshot shows a mobile application interface with a title bar 'Cadastro/Condominio'. Below the title bar is a dark header with the text 'E-mail:'. Underneath is a white text input field with a black cursor. To the right of the input field are two vertical arrows: an upward-pointing arrow above and a downward-pointing arrow below.

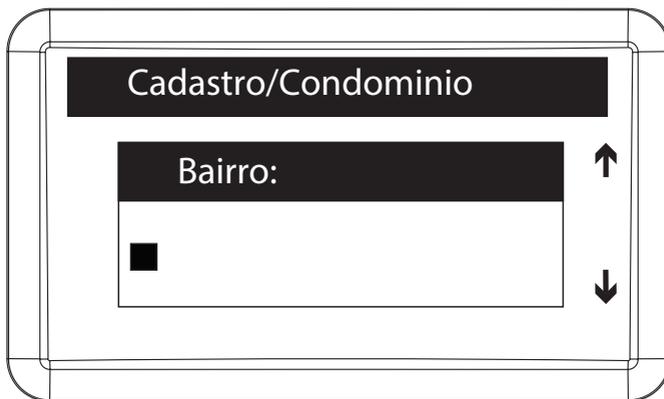
E-mail do condomínio

The screenshot shows a mobile application interface with a title bar 'Cadastro/Condominio'. Below the title bar is a dark header with the text 'Telefone:'. Underneath is a white text input field with a black cursor and a pair of parentheses '()' on the left side. To the right of the input field are two vertical arrows: an upward-pointing arrow above and a downward-pointing arrow below.

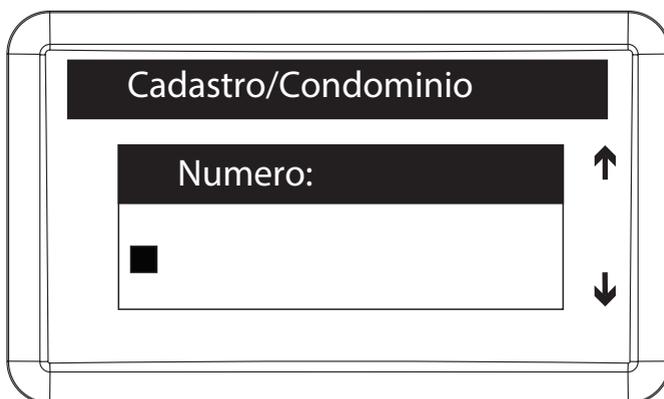
Número do telefone do condomínio

The screenshot shows a mobile application interface with a title bar 'Cadastro/Condominio'. Below the title bar is a dark header with the text 'Rua:'. Underneath is a white text input field with a black cursor. To the right of the input field are two vertical arrows: an upward-pointing arrow above and a downward-pointing arrow below.

Nome da rua do condomínio



Bairro do condomínio



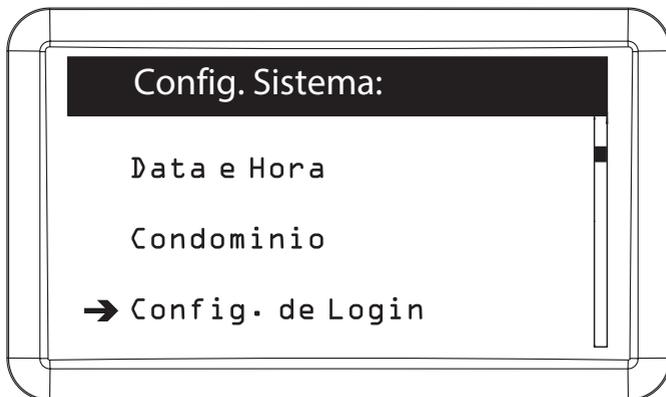
Número do condomínio

Ao finalizar o cadastro ou edição, pressionar *Ok* ou *Enter* para confirmar.



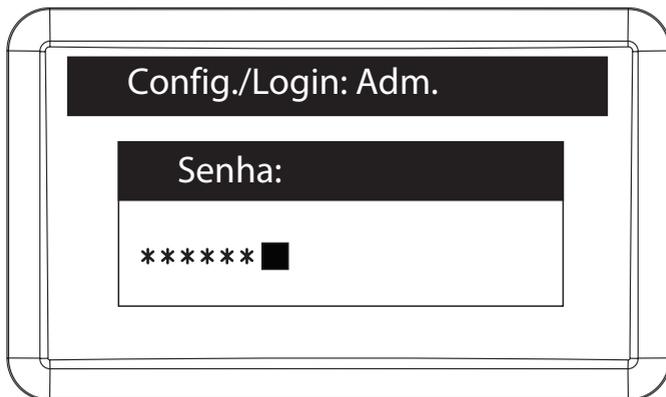
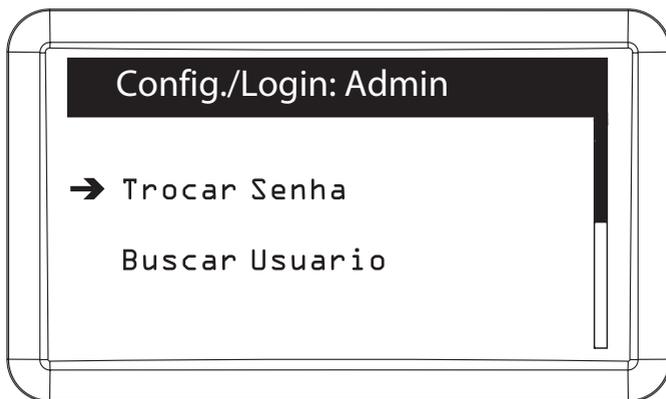
Configuração de login

Para alterar a senha do administrador ou alterar o nível de permissão dos usuários ao sistema, é necessário realizar os seguintes passos:

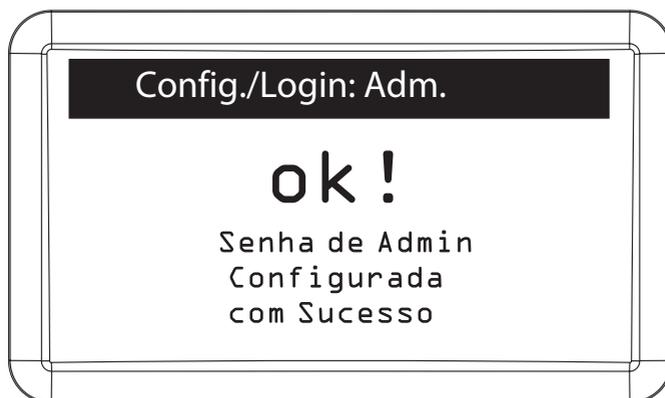


Trocar senha

Para alterar a senha do administrador (senha utilizada para autenticação como *admin*) é necessário realizar os seguintes passos:



Pressionar *Ok* ou *Enter* para confirmar.

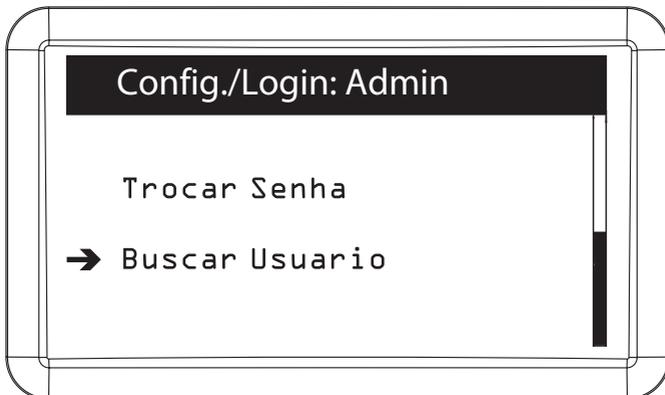


Buscar usuário

É possível configurar novos usuários para acessarem o *Menu Principal* do MIP e definir níveis de acesso para os mesmos, sendo um total de 4 níveis.

- » **Nível 1:** usuário com permissão completa ao menu do sistema.
- » **Nível 2:** usuário com permissão nas configurações de usuários e para visualizar eventos e notificações.
- » **Nível 3:** usuário com permissão para visualizar eventos e notificações.
- » **Nível 4:** usuário com permissão apenas para visualizar eventos.

Para configurar o login dos usuários e definir/alterar o nível de permissão do mesmo ao menu do sistema, é necessário realizar os seguintes passos:



Usuario/Buscar :

Buscar Usuario:

Nome: ■

Apto:

O usuário pode ser encontrado através de seu nome ou do número do apartamento

Nome (01/01)	Apto :
→ Usuario	XXX

Selecionar o usuário para realizar as alterações

Config./Login:

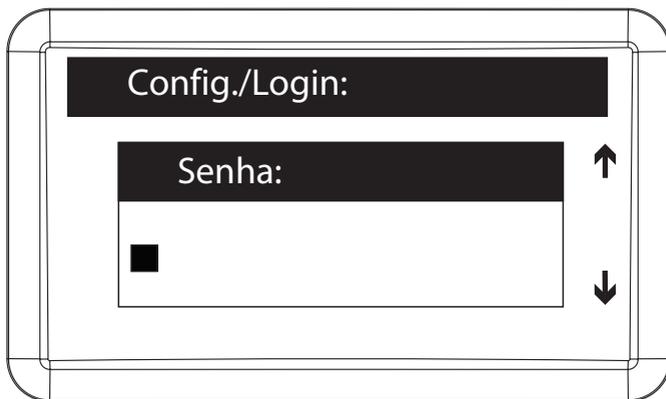
Usuario:

■

↑

↓

Definir o nome do usuário para realizar a autenticação no sistema

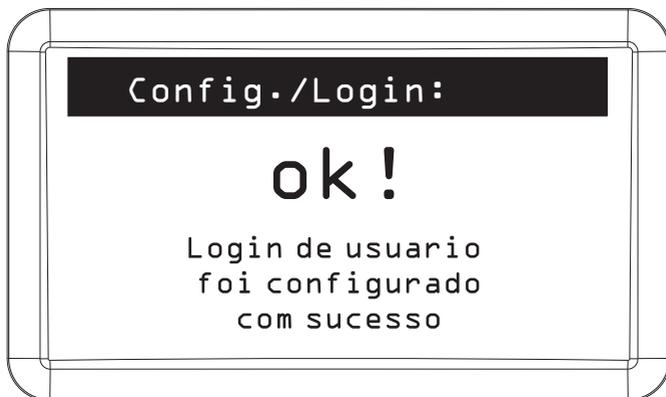


Definir a senha do usuário para realizar a autenticação no sistema



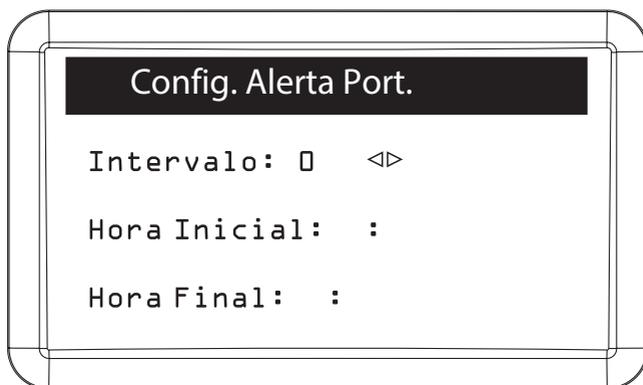
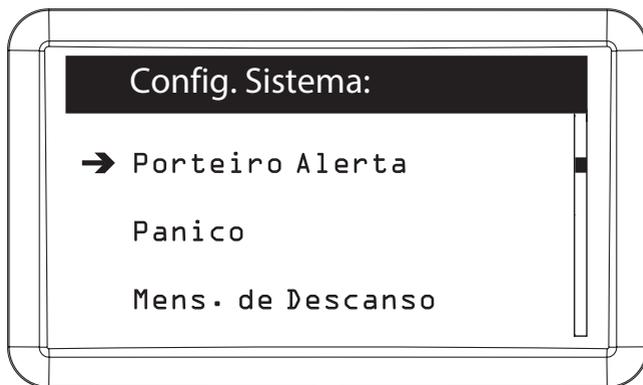
Definir o nível de permissão do usuário

Pressionar *Ok* ou *Enter* para confirmar.



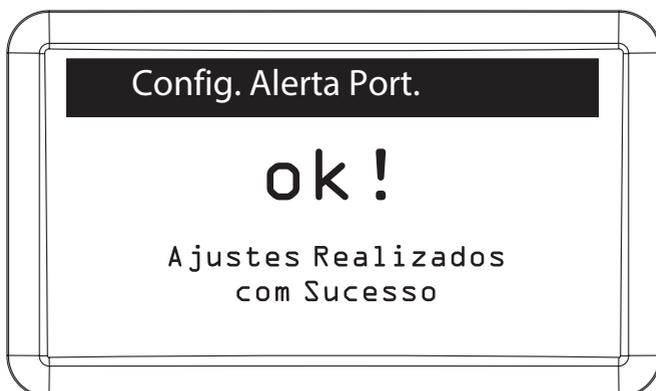
Porteiro alerta

O objetivo do porteiro alerta é enviar alertas sonoros para o porteiro (vigilante) em uma faixa de horário para mantê-lo atento. Os alertas são feitos em intervalos regulares dentro da faixa de horário configurada. Esses intervalos podem ser de 15 minutos até 120 minutos e são configurados pelo usuário, sendo que a ativação e desativação deste alerta gera evento de dispositivo para que possa ser acompanhado pelo administrador do condomínio. Para configurar alertas sonoros em um período de tempo no MIP é necessário realizar os seguintes passos:



Definir o intervalo de alertas sonoros dentro de um período determinado de tempo. Para desativar esse alarme é só definir o intervalo de tempo igual a Zero

Pressionar *Ok* ou *Enter* para confirmar.



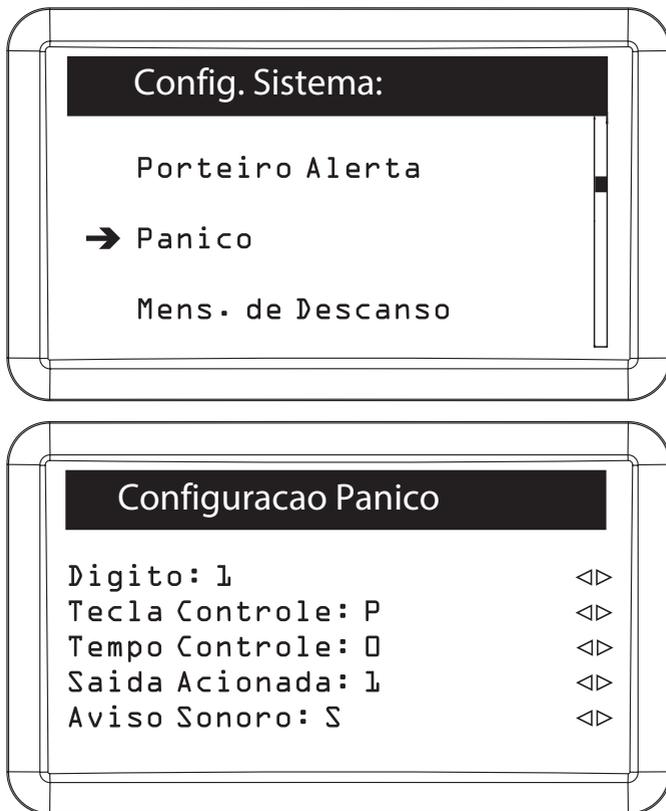
Pânico

A função *Pânico* é utilizada para alertar o porteiro (vigilante) de algum perigo no condomínio. O alerta pode ser apenas visual (indica no display *Pânico*, qual usuário fez o acionamento e qual dispositivo acionou) ou também sonoro. Esta função é registrada pelo MIP como evento de pânico e será visível no relatório deste usuário como acionamento por coação (ou pânico).

O pânico pode ser acionado das seguintes maneiras:

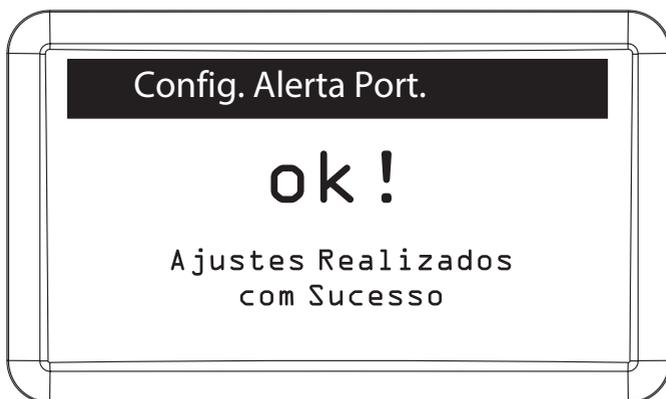
1. Configurando um dígito de pânico, sendo ele colocado entre a senha do usuário e o número de seu apartamento no momento da abertura de fechadura através de senha (ex.: *senha do usuário + dígito de pânico + apto de usuário*);
2. Configurando uma tecla do controle remoto para ser pressionada por um determinado tempo configurando abaixo;
3. Segurando o dígito de pânico no teclado do MIP 1000.

Para configurar a função *Pânico* no sistema é necessário realizar os seguintes passos:



Definir o dígito de acionamento por senha, a tecla do controle remoto e o tempo, em segundos, que esta tecla deve ser pressionada (máximo 10s), qual saída do MIP será acionada quando o pânico for acionado e se terá aviso sonoro

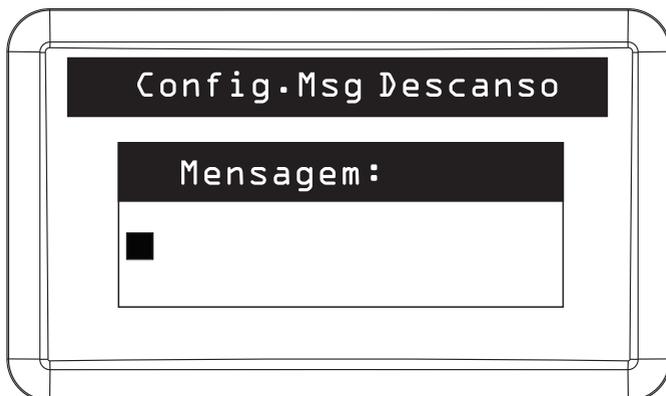
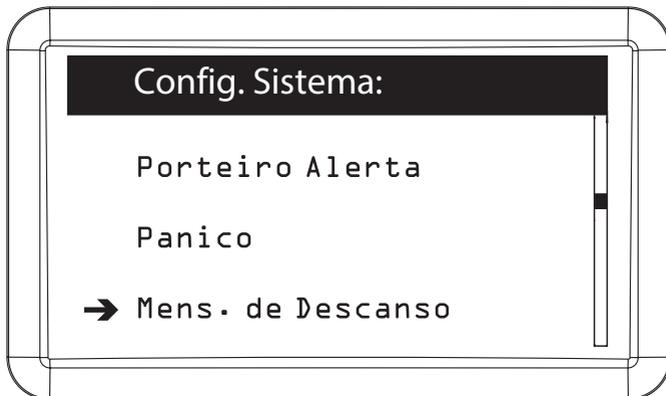
Pressionar *Ok* ou *Enter* para confirmar.



Mensagem de descanso

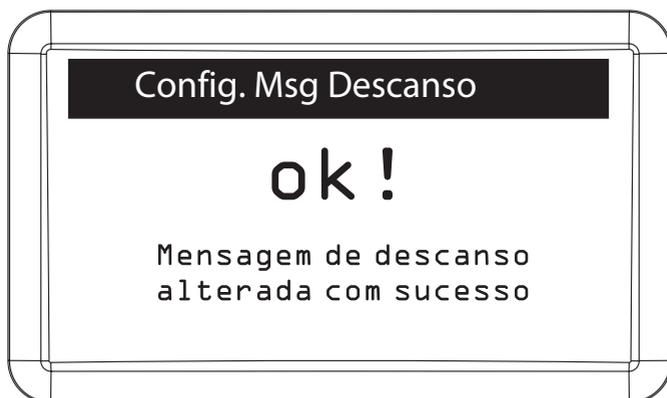
Esta mensagem ficará visível no display do MIP, acima do nome do condomínio, quando o mesmo estiver na tela inicial.

Para configurar a mensagem de descanso na tela do MIP é necessário realizar os seguintes passos:



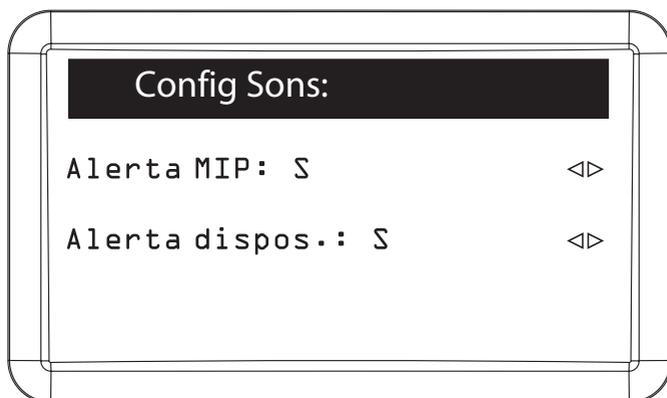
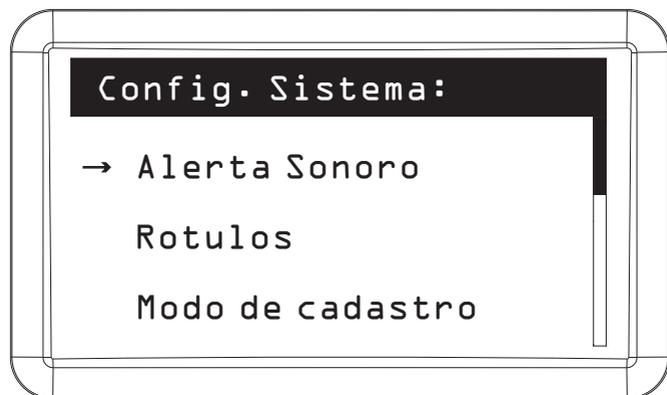
Definir a mensagem de descanso

Pressionar *Ok* ou *Enter* para confirmar.



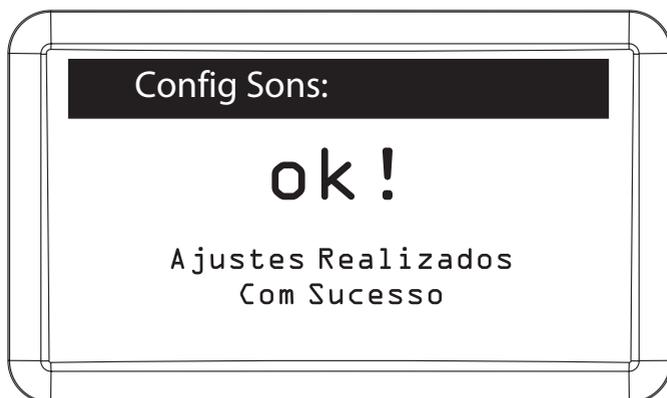
Alerta sonoro

Para configurar o alerta sonoro no MIP e nos dispositivos (sons de confirmação/negação) é necessário realizar os seguintes passos:



Habilitar/desabilitar o MIP e os dispositivos para terem alertas sonoros

Pressionar *Ok* ou *Enter* para confirmar.



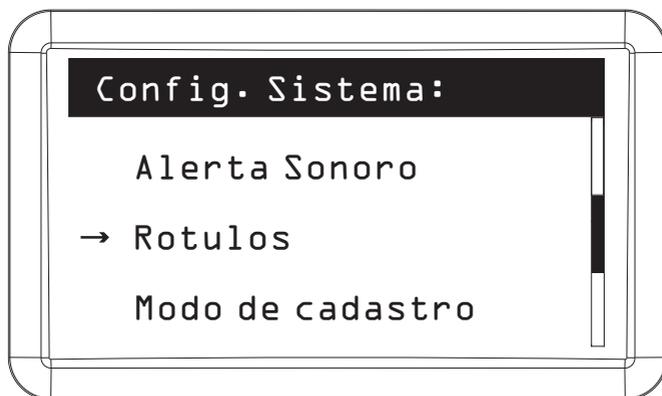
Rótulos

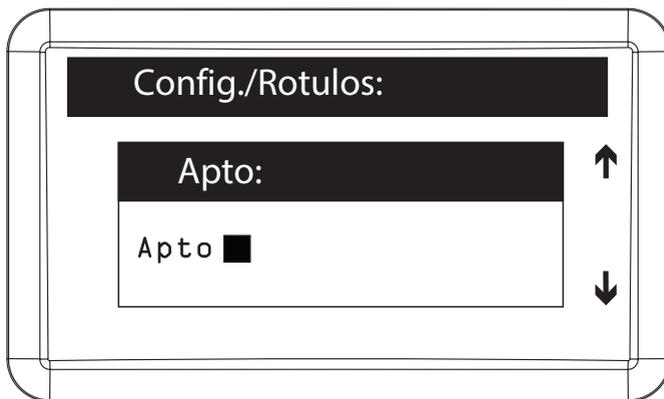
É possível renomear alguns rótulos do MIP.

Exemplos de utilização:

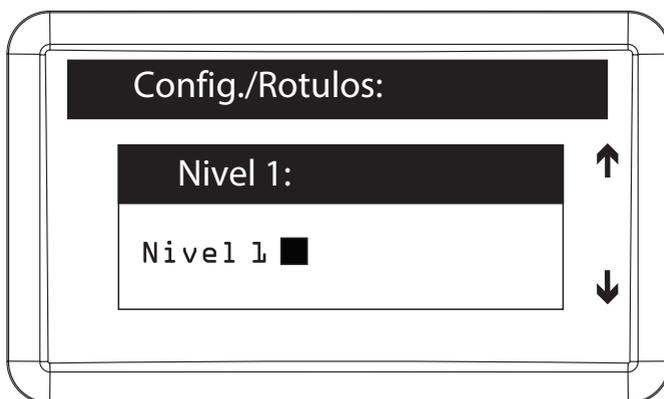
- » Em um condomínio de casas, o rótulo apto que é encontrado, por exemplo, na inclusão de um usuário é possível ser alterado para qualquer texto de quatro caracteres (ex.: casa).
- » Os rótulos níveis de permissão podem ser renomeados da mesma forma que o rótulo apto (ex.: porteiro, síndico, instalador).

Para renomear os rótulos é necessário realizar os seguintes passos:

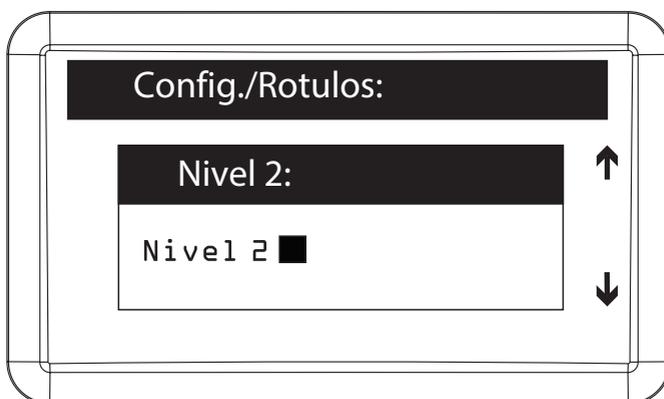




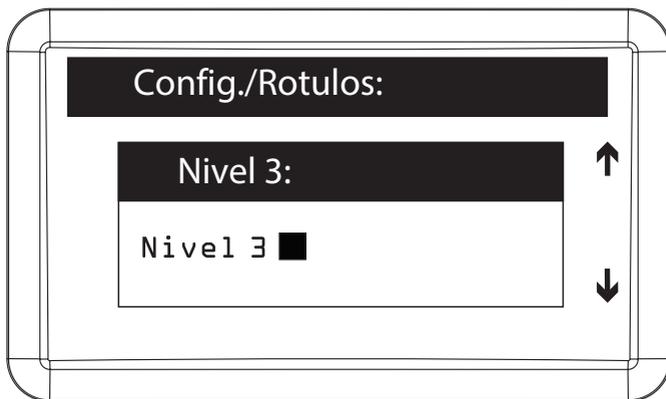
Renomear o rótulo Apto



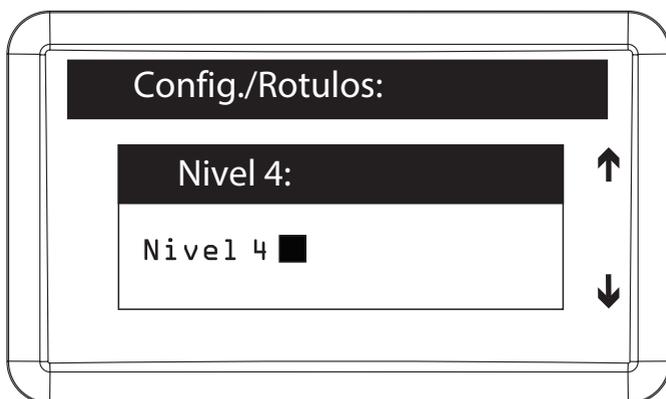
Renomear o rótulo Nivel 1



Renomear o rótulo Nivel 2

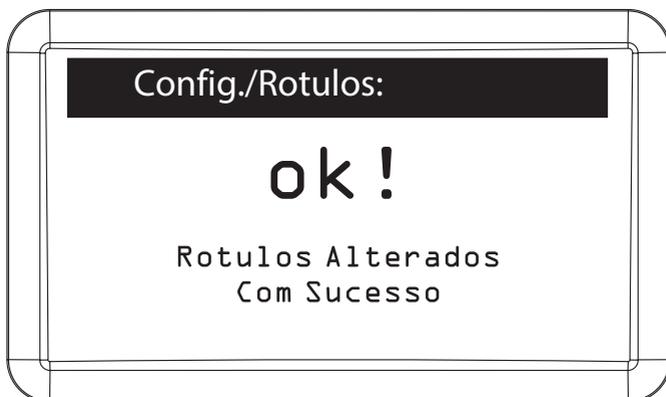


Renomear o rótulo Nível 3



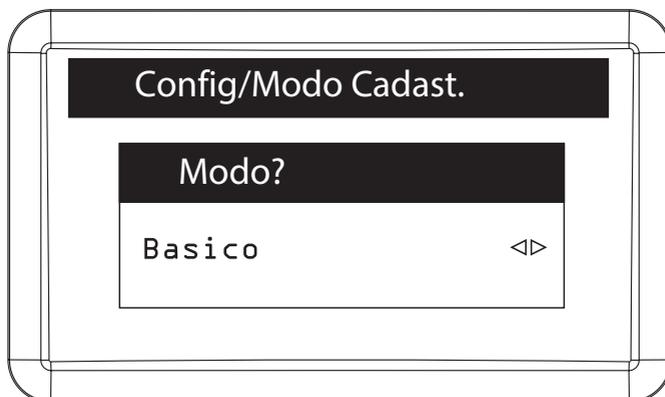
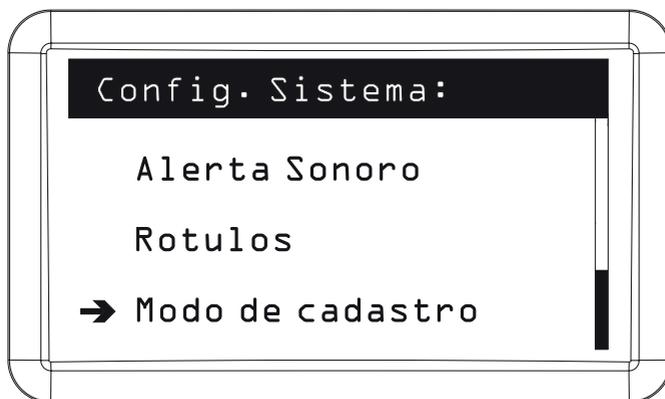
Renomear o rótulo Nível 4

Pressionar *Ok* ou *Enter* para confirmar.



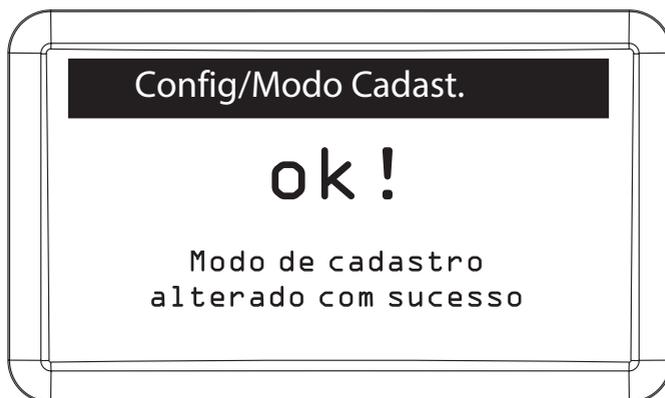
Modo cadastro

Para alterar o modo cadastro do sistema de Básico para Avançado (maior número de informações no cadastro de usuário e do condomínio) é necessário realizar os seguintes passos:



Definir se o modo cadastro será básico ou avançado

Pressionar *Ok* ou *Enter* para confirmar.



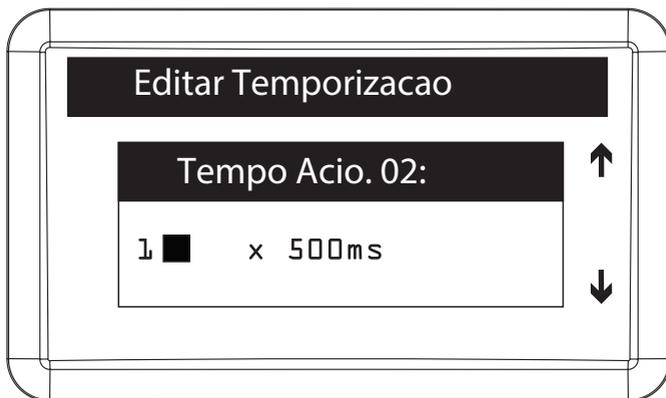
Temporização

É possível alterar o tempo de acionamento das saídas do MIP, sendo este o tempo que as saídas ficarão acionadas. Pode-se configurar o tempo entre a abertura dos sensores e o acionamento do aviso sonoro, o intervalo entre chaveiros RFID (Mifare) em qualquer dispositivo e o tempo que um evento do sistema ficará visível no display do MIP. Parte destas modificações também estão disponíveis no menu de *Editar dispositivo* quando selecionado o *MIP* (disponível somente para versão igual ou superior a 170405).

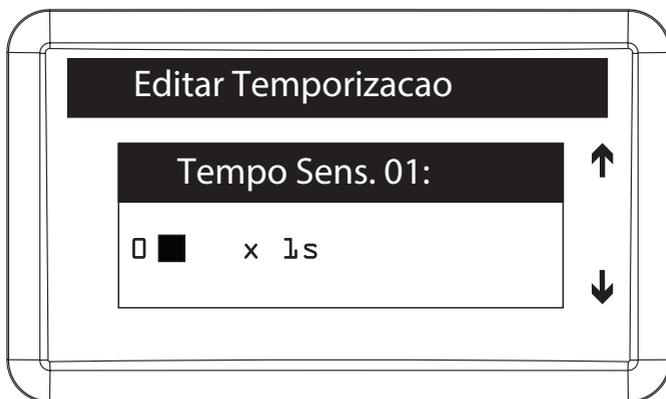
Para efetuar essas alterações é necessário realizar os seguintes passos:



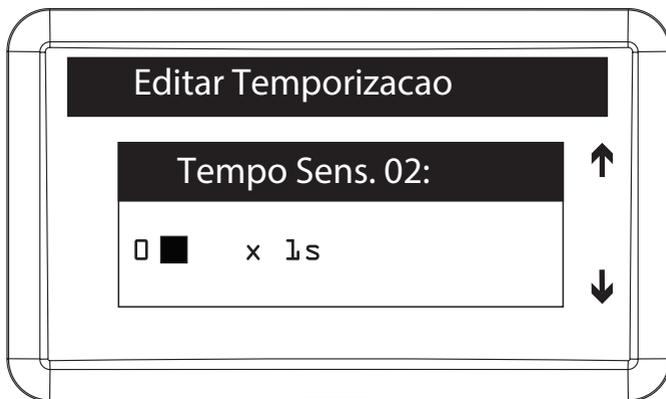
Configurar o tempo, múltiplo de 0,5 segundo, de acionamento da saída 01 do MIP. O valor máximo deste campo é 99, sendo equivalente a 49,5 segundos



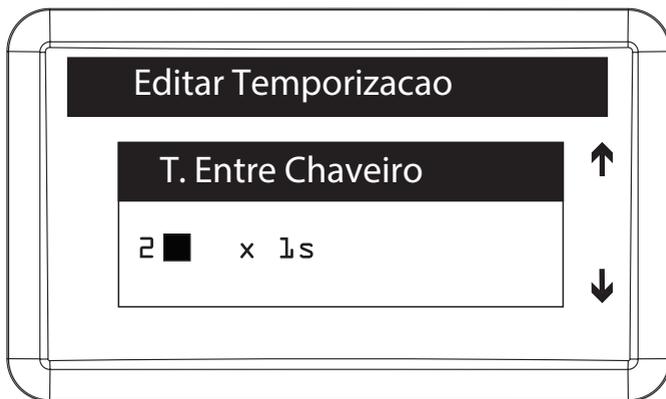
Configurar o tempo, múltiplo de 0,5 segundo, de acionamento da saída 02 do MIP. O valor máximo deste campo é 99, sendo equivalente a 49,5 segundos



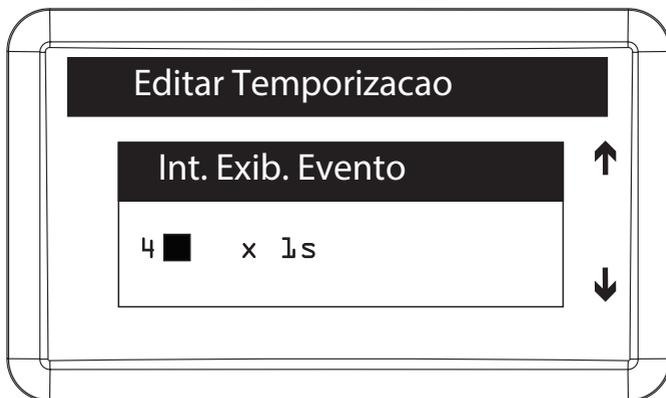
Configurar o tempo, múltiplo de 1 segundo, entre a abertura do sensor 01 do MIP e o disparo do aviso sonoro. O valor máximo deste campo é 99, sendo equivalente a 99 segundos. No caso do valor inserido ser igual a 0, o sensor será desativado



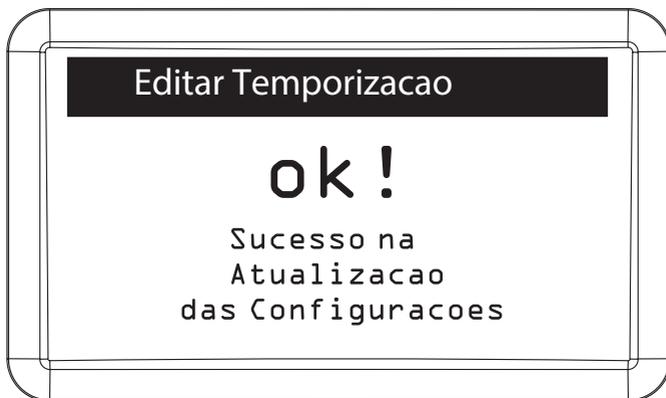
Configurar o tempo, múltiplo de 1 segundo, entre a abertura do sensor 02 do MIP e o disparo do aviso sonoro. O valor máximo deste campo é 99, sendo equivalente a 99 segundos. No caso do valor inserido ser igual a 0, o sensor será desativado



Configurar o tempo, múltiplo de 1 segundo, entre a detecção de chaveiros RFID (Mifare) nos dispositivos do sistema. O valor máximo deste campo é 99, sendo equivalente a 99 segundos



Configurar o tempo, múltiplo de 1 segundo, entre a exibição dos eventos ocorridos no sistema através display do MIP. O valor máximo deste campo é 99, sendo equivalente a 99 segundos



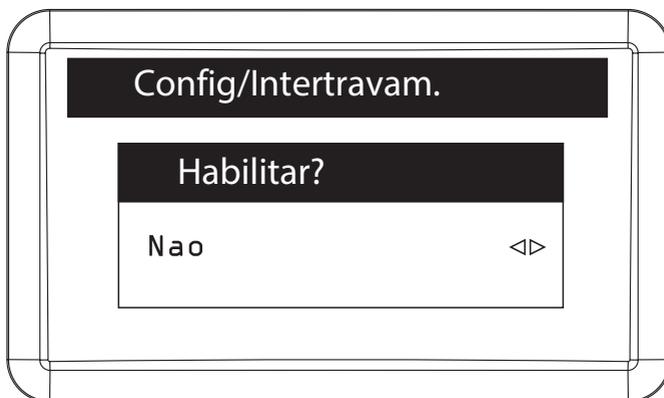
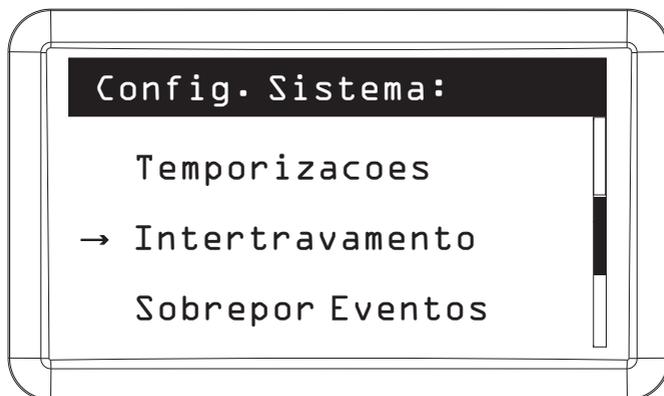
Intertravamento

Controle de intertravamento para entrada de pedestres (eclusa ou gaiola).

É utilizado para garantir que um segundo portão/porta somente será aberto quando o primeiro estiver fechado. Esta condição é indicada para condomínios que desejam maior segurança e utilizam eclusas, por exemplo, durante o acesso de entrada em um condomínio, o segundo portão/porta só abrirá se fecharmos o primeiro portão/porta.

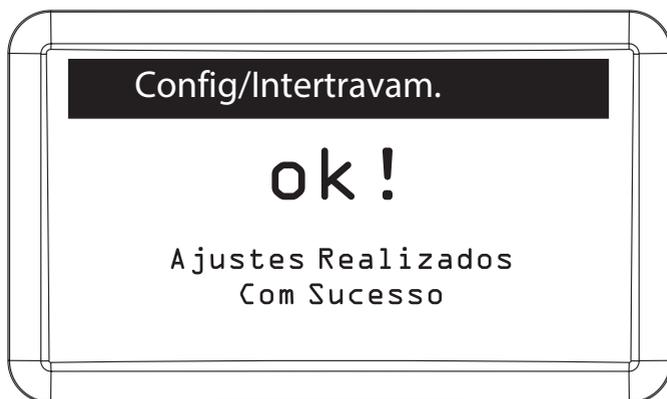
Importante dizer que neste caso, o intertravamento será aplicado aos sensores e acionamentos presentes no MIP e não aos dispositivos. Para implementar essa função nos dispositivos, acesse o menu de *Edição* dos mesmos, lembrando que essa modificação também está disponível no menu de *Editar dispositivo* quando selecionado o MIP (disponível somente para versão igual ou superior a 170405).

Então para habilitar/desabilitar o intertravamento do MIP é necessário realizar os seguintes passos:



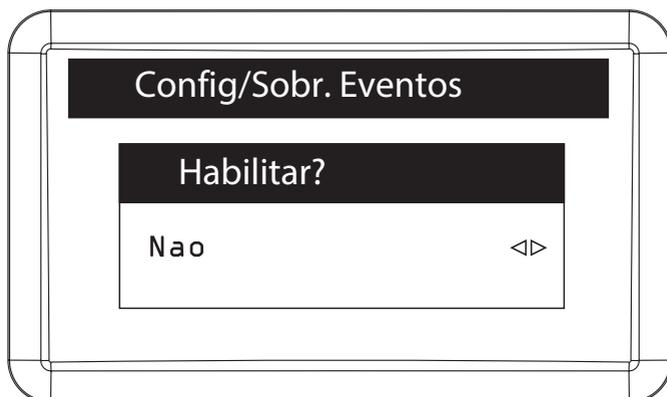
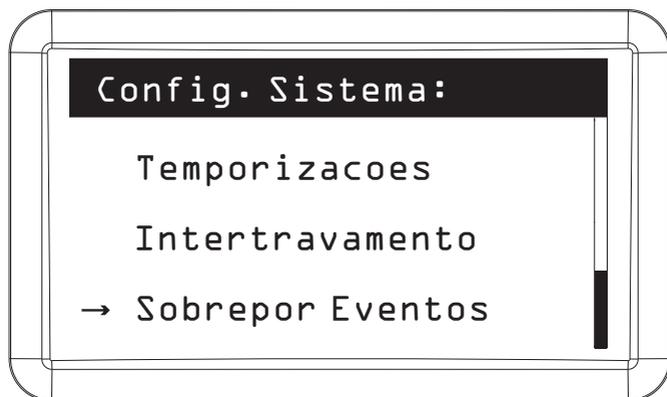
Habilitar/desabilitar o intertravamento

Pressionar *Ok* ou *Enter* para confirmar.



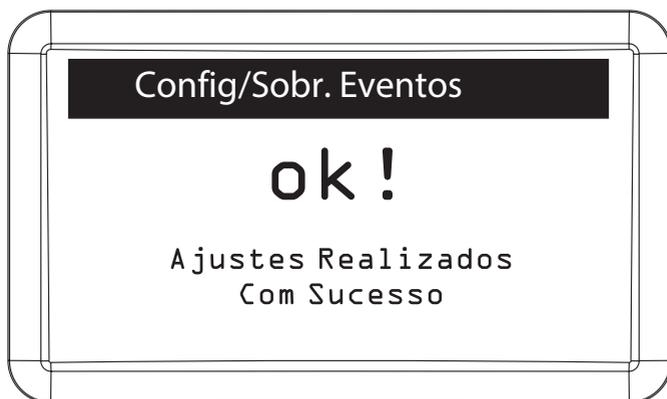
Sobrepor eventos

Para habilitar/desabilitar a função sobrepor eventos (se acontecer um evento em seguida de outro, o sistema não irá aguardar o tempo entre eventos para exibir o novo e sim sobrepor o atual sobre o anterior) é necessário realizar os seguintes passos:



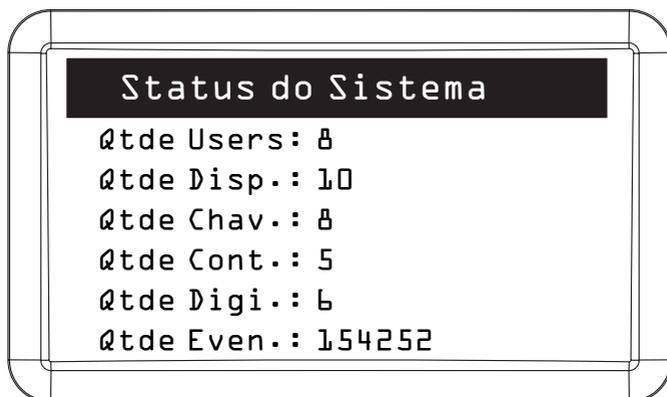
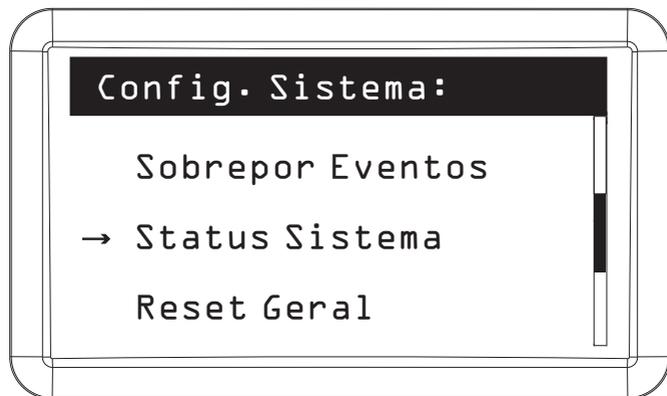
Habilitar/desabilitar a função sobrepor eventos

Pressionar *Ok* ou *Enter* para confirmar.



Status do sistema

Para verificar a quantidade de usuários, dispositivos, chaveiros, controles e eventos que já foram registrados no sistema é necessário realizar os seguintes passos:

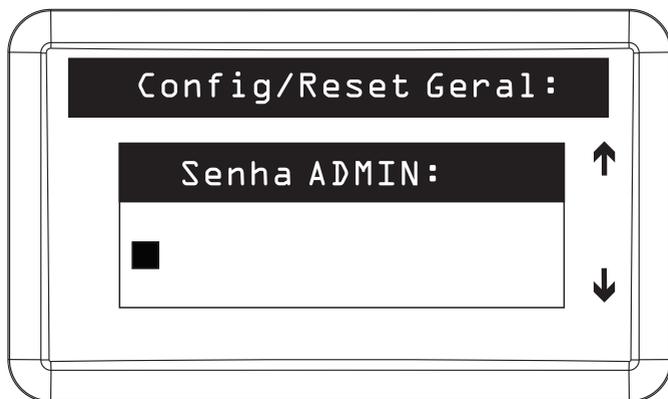
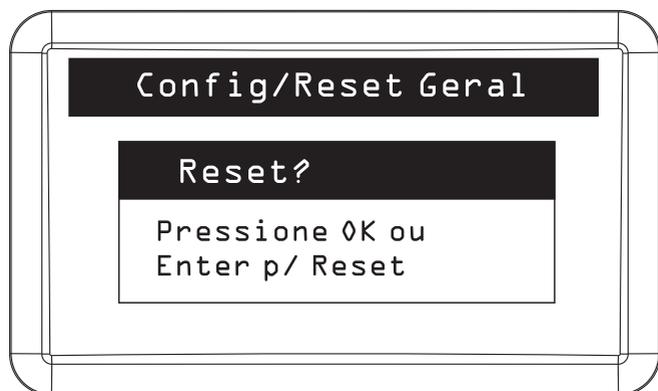
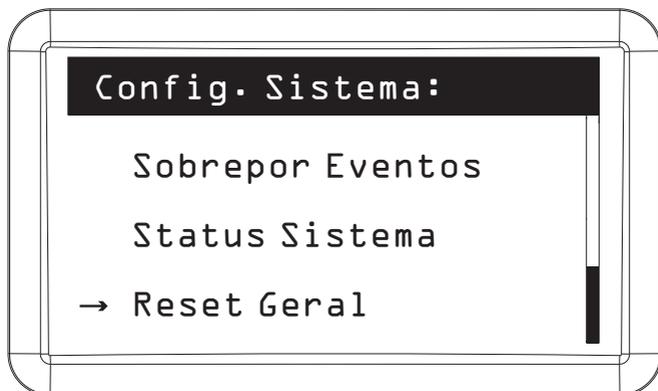


Pressionar *Cancelar* ou *ESC* para sair da consulta.

Reset geral

Este comando é responsável por apagar todas as informações cadastradas no MIP, retornando todas as configurações para o padrão de fábrica.

Para realizar o reset geral é necessário realizar os seguintes passos:



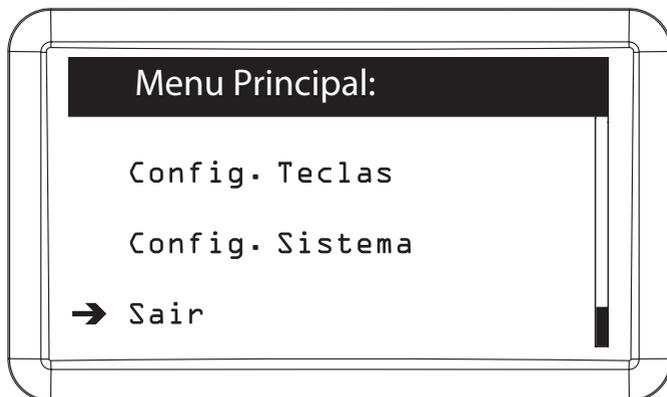
Digitar a senha do administrador para realizar o reset geral

Pressionar Ok ou Enter para confirmar.

Obs.: após o reset geral o MIP irá retornar para a tela inicial com todas as configurações padrão de fábrica.

5.11. Sair

Para retornar a tela inicial do MIP clicar na opção *Sair* do Menu Principal.



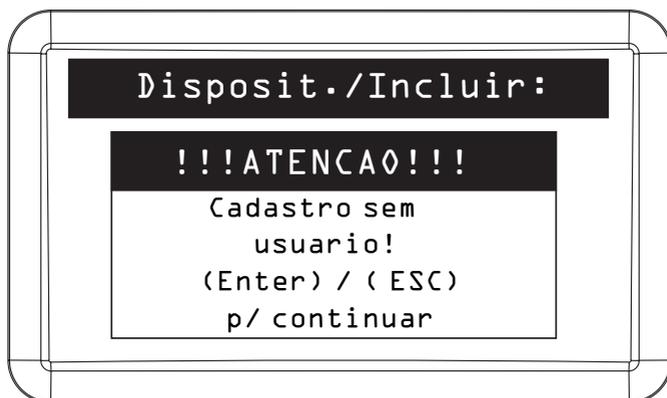
6. Exceções para dispositivos biométricos

O MIP 1000 possui capacidade de armazenamento para 4000 Digitais e os dispositivos biométricos integrados ao SCA 1000 tem capacidades diferentes de digitais, por exemplo o *Bio Inox Plus SS 311 MF*, quando utilizado com o SCA 1000 possui capacidade para 1499 digitais e para garantir a integridade dos dados existentes o MIP 1000 faz dois tipos de validação.

6.1. Validação por dispositivo

É a validação que o MIP 1000 faz para verificar se um dispositivo pode receber ou não usuários no momento do cadastro de um novo dispositivo.

Exemplo: temos cadastrado no MIP mais de 1499 digitais e estamos inserindo um Bio Inox Plus SS 311 MF. Ao finalizar o cadastro aparecerá na tela do MIP a seguinte mensagem:



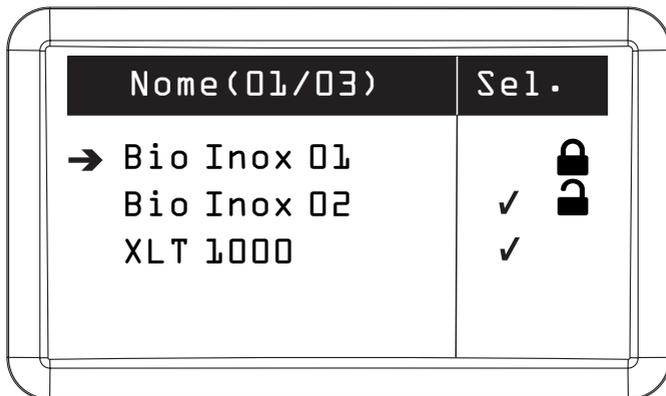
Isso significa que o Bio Inox Plus SS 311 MF foi inserido, mas nenhum usuário terá acesso ao mesmo devido a quantidade de digitais no MIP ser superior a sua capacidade.

Através do menu de edição do usuário é possível adicionar usuários, individualmente, para o dispositivo inserido.

6.2. Validação por usuário

É a validação que o MIP 1000 faz para verificar se um usuário possui permissão ou não para inserir uma nova digital ou ter acesso a um dispositivo biométrico, no momento do cadastro ou edição de usuário.

Exemplo: o MIP 1000 não permitirá adicionar uma nova digital a um usuário quando este usuário possuir acesso a um dispositivo que atingiu o limite da capacidade de digitais permitidas. Para incluir uma digital para este usuário é preciso entrar no menu *Dispositivo* e remover o dispositivo que está bloqueando, indicado pelo cadeado.



Nome (01/03)	Sel.
→ Bio Inox 01	
Bio Inox 02	✓ 
XLT 1000	✓

Ao realizar seleção dos dispositivos permitidos para o usuário podemos ter 2 tipos de restrição:

-  O dispositivo não tem capacidade para receber as digitais do usuário que está sendo editado.
-  O dispositivo com capacidade máxima de digitais, porém, o usuário que está sendo editado possui acesso ao dispositivo.

Termo de garantia

Fica expresso que esta garantia contratual é conferida mediante as seguintes condições:

Nome do cliente:

Assinatura do cliente:

Nº da nota fiscal:

Data da compra:

Modelo:

Nº de série:

Revendedor:

1. Todas as partes, peças e componentes do produto são garantidos contra eventuais vícios de fabricação, que porventura venham a apresentar, pelo prazo de 1 (um) ano – sendo este de 90 (noventa) dias de garantia legal e 9 (nove) meses de garantia contratual –, contado a partir da data da compra do produto pelo Senhor Consumidor, conforme consta na nota fiscal de compra do produto, que é parte integrante deste Termo em todo o território nacional. Esta garantia contratual compreende a troca gratuita de partes, peças e componentes que apresentarem vício de fabricação, incluindo as despesas com a mão de obra utilizada nesse reparo. Caso não seja constatado vício de fabricação, e sim vício(s) proveniente(s) de uso inadequado, o Senhor Consumidor arcará com essas despesas.
2. A instalação do produto deve ser feita de acordo com o Manual do Produto e/ou Guia de Instalação. Caso seu produto necessite a instalação e configuração por um técnico capacitado, procure um profissional idôneo e especializado, sendo que os custos desses serviços não estão incluídos no valor do produto.
3. Constatado o vício, o Senhor Consumidor deverá imediatamente comunicar-se com o Serviço Autorizado mais próximo que conste na relação oferecida pelo fabricante – somente estes estão autorizados a examinar e sanar o defeito durante o prazo de garantia aqui previsto. Se isso não for respeitado, esta garantia perderá sua validade, pois estará caracterizada a violação do produto.
4. Na eventualidade de o Senhor Consumidor solicitar atendimento domiciliar, deverá encaminhar-se ao Serviço Autorizado mais próximo para consulta da taxa de visita técnica. Caso seja constatada a necessidade da retirada do produto, as despesas decorrentes, como as de transporte e segurança de ida e volta do produto, ficam sob a responsabilidade do Senhor Consumidor.
5. A garantia perderá totalmente sua validade na ocorrência de quaisquer das hipóteses a seguir: a) se o vício não for de fabricação, mas sim causado pelo Senhor Consumidor ou por terceiros estranhos ao fabricante; b) se os danos ao produto forem oriundos de acidentes, sinistros, agentes da natureza (raios, inundações, desabamentos, etc.), umidade, tensão na rede elétrica (sobretensão provocada por acidentes ou flutuações excessivas na rede), instalação/uso em desacordo com o manual do usuário ou decorrentes do desgaste natural das partes, peças e componentes; c) se o produto tiver sofrido influência de natureza química, eletromagnética, elétrica ou animal (insetos, etc.); d) se o número de série do produto tiver sido adulterado ou rasurado; e) se o aparelho tiver sido violado. A Intelbras não se responsabiliza pela contratação e eventuais custos de terceiros para suprir a ausência do produto que estiver em processo de conserto ou troca.
6. Esta garantia não cobre perda de dados, portanto, recomenda-se, se for o caso do produto, que o Consumidor faça uma cópia de segurança regularmente dos dados que constam no produto.
7. A Intelbras não se responsabiliza pela instalação deste produto, e também por eventuais tentativas de fraudes e/ou sabotagens em seus produtos. Mantenha as atualizações do software e aplicativos utilizados em dia, se for o caso, assim como as proteções de rede necessárias para proteção contra invasões (hackers). O equipamento é garantido contra vícios dentro das suas condições normais de uso, sendo importante que se tenha ciência de que, por ser um equipamento eletrônico, não está livre de fraudes e burlas que possam interferir no seu correto funcionamento. A Intelbras não se responsabiliza pela contratação e eventuais custos de terceiros para suprir a ausência do produto que estiver em processo de conserto ou troca.
8. Após sua vida útil, o produto deve ser entregue a uma assistência técnica autorizada da Intelbras ou realizar diretamente a destinação final ambientalmente adequada evitando impactos ambientais e a saúde. Caso prefira, a pilha/bateria assim como demais eletrônicos da marca Intelbras sem uso, pode ser descartado em qualquer ponto de coleta da Green Eletron (gestora de resíduos eletroeletrônicos a qual somos associados). Em caso de dúvida sobre o processo de logística reversa, entre em contato conosco pelos telefones (48) 2106-0006 ou 0800 704 2767 (de segunda a sexta-feira das 08 às 20h e aos sábados das 08 às 18h) ou através do e-mail suporte@intelbras.com.br.

Sendo estas as condições deste Termo de Garantia complementar, a Intelbras S/A se reserva o direito de alterar as características gerais, técnicas e estéticas de seus produtos sem aviso prévio.

O processo de fabricação deste produto não é coberto pelos requisitos da ISO 14001.

Todas as imagens deste manual são ilustrativas.

Produto beneficiado pela Legislação de Informática.

intelbras



fale com a gente

Suporte a clientes: (48) 2106 0006

Fórum: forum.intelbras.com.br

Suporte via chat: intelbras.com.br/suporte-tecnico

Suporte via e-mail: suporte@intelbras.com.br

SAC: 0800 7042767

Onde comprar? Quem instala?: 0800 7245115

Produzido por: Intelbras S/A – Indústria de Telecomunicação Eletrônica Brasileira
Rodovia BR 459, km 124, nº 1325 – Distrito Industrial – Santa Rita do Sapucaí/MG – 37540-000
CNPJ 82.901.000/0016-03 – www.intelbras.com.br

01.20
Indústria brasileira