Controle de Acesso

ID-3K

Manual do Usuário

Uma marca do Grupo legrand

ÍNDICE

CAPÍTULO I – INTRODUÇÃO

A Família de Controle de Acesso HDL são equipamentos microprocessados que permite a abertura de fechaduras e/ou dispositivos através de métodos como: Senha, TAG/Cartão RFID, Biometria, Controle RF e Bluetooth (Via Aplicativo) - de acordo com o seu modelo. O controle de acesso, pode operar no modo STAND ALONE (onde toda a informação e processamento são realizados localmente), no modo REDE (SISTEMA/GATEWAY) no qual o equipamento valida os dados e envia ao Software Acessos ID-3K e ainda o modo Reader para leitura do meio de autenticação e envio da informação à uma controladora ou Software Acessos ID-3K para cadastro.

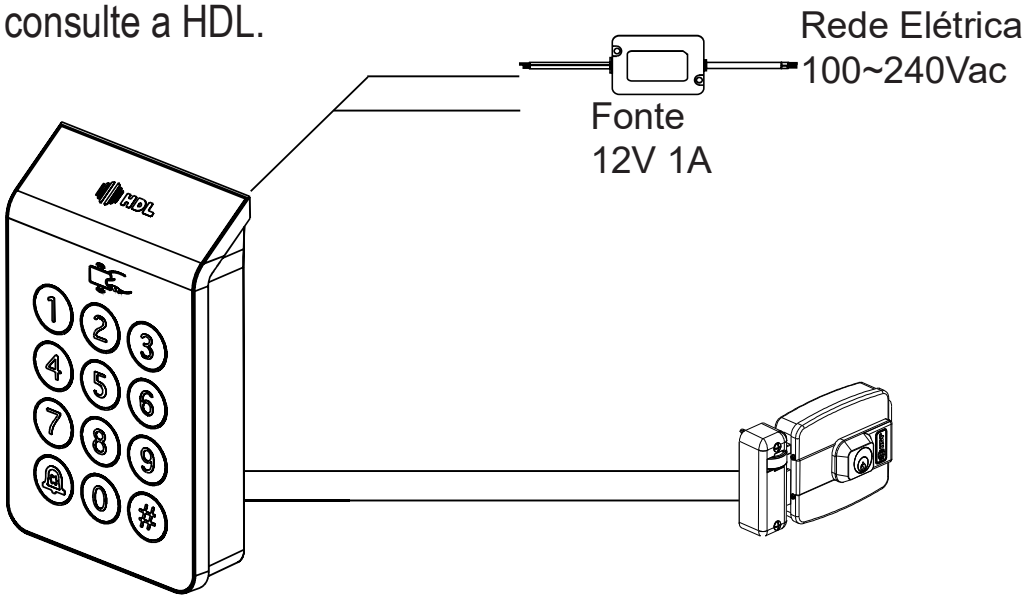
O Software Acessos ID-3K e seu manual de configurações, está disponível no site HDL na secção de downloads (www.hdl.com.br).

Identifique a seguir qual o modo de funcionamento que se melhor adequa a sua necessidade.

Modo Stand Alone:

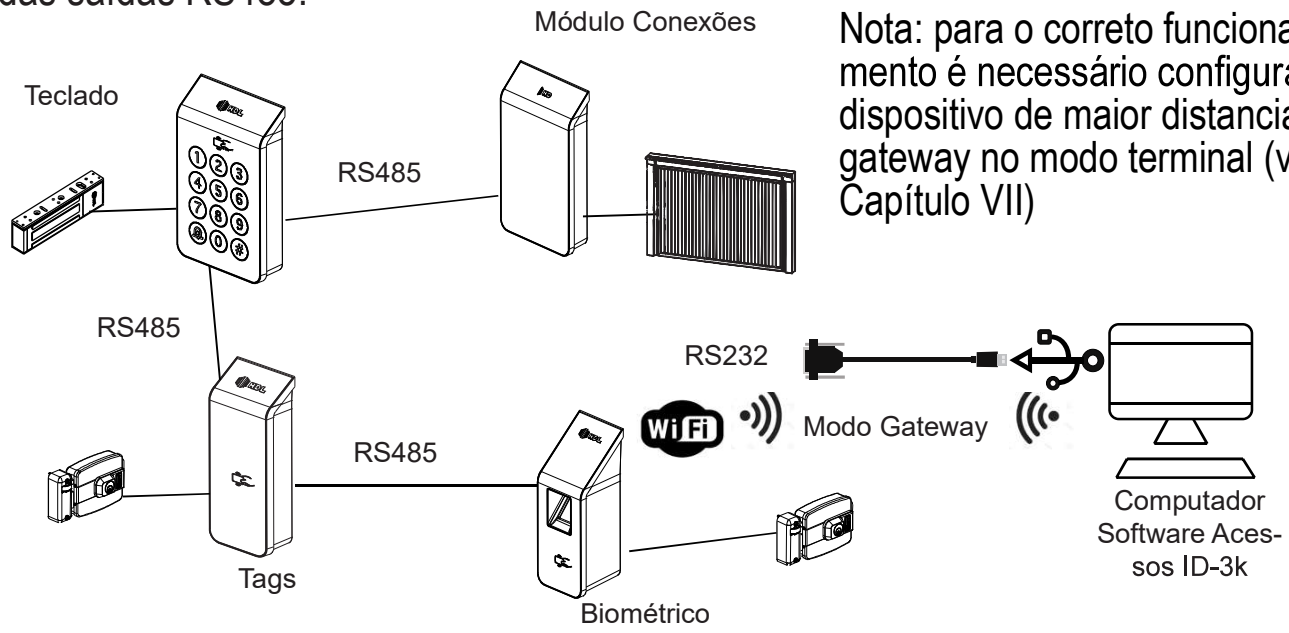
Caracteriza-se pela forma de trabalho autônoma, onde os usuários e registros são armazenados no próprio aparelho e os comandos disponíveis executados pelo mesmo.

Sendo assim possuindo uma instalação simples e sem a necessidade de outros módulos ou computadores. Limitando-se a 3000 usuários, para uma quantidade maior, consulte a HDL.



Modo Rede (Sistema / Gateway):

Caracteriza-se pela conexão entre os equipamentos da família Controle de Acesso através de RS485, é possível criar uma rede entre todos os dispositivos e gerencia-los através de Software. Para isso conecte todos os aparelhos em paralelo através das saídas RS485.



Nota: para o correto funcionamento é necessário configurar o dispositivo de maior distancia do gateway no modo terminal (vide Capítulo VII)

Nota: Recomenda-se a Utilização do Módulo Biométrico como Gateway, quando houver a utilização de acesso por biometria no sistema.

Toda a comunicação será transmitida por Wi-fi para o Software Acessos ID-3K através do dispositivo GATEWAY, o qual é o gerenciador da comunicação entre os dispositivos em rede e o Software Acessos ID-3K, os demais dispositivos devem estar configurados no modo SISTEMA

Modo Reader (Leitor):

O modo READER oferece ao usuário duas maneiras de utilização, combinando ou interligando com o controladoras Weigand ou como um dispositivo para cadastro de usuários no Software Acessos ID-3K conectado a rede e com sua comunicação através do Wi-fi.

1.1– Cuidados e Orientações

1.1.1 - Cuidados com a Segurança

a) É obrigatório o uso de fontes de alimentação estabilizadas ou lineares que protejam o equipamento;

b) Recomendamos a utilização das fontes HDL.(90.02.92.001 90.01.90.000, 90.01.03.024);

c) Execute toda a instalação com o equipamento desligado da rede elétrica com o intuito de prevenir danos causados pela energia estática;

d) Utilize os cabos indicados para a instalação e em ambientes que possuam interferências eletromagnéticas, utilize cabos com blindagem;

e) Não compartilhe a tubulação elétrica com o cabos de dados;

f) Não faça derivação dos terminais de alimentação do equipamento para conectar outro dispositivo, as conexões elétricas devem ser individuais;

1.1.2 - Cuidados com Limpeza

O Controle de Acesso HDL não pode ser limpo com derivados etílicos ou solventes, como, por exemplo: Álcool, Thinner, Benzina e Benzeno.

O frontal do aparelho é composto de uma peça em policarbonato. Ao se fazer a limpeza com derivados iguais ou da mesma família acima, irá causar aspecto esbranquiçado instantaneamente e também rachaduras.

Para limpeza se deve utilizar água e sabão neutro ou detergente, evitando usar esponja ou pano áspero. Após isto, fazer o polimento com flanela macia.

Importante: não dirigir jatos de água (mangueira) sobre o produto.

O policarbonato frontal pode sofrer danos. Evite qualquer contato com objetos rígidos e abrasivos;

CAPÍTULO II – SOBRE O MANUAL

Este Manual do Usuário busca informar as configurações básicas e avançadas da linha de Controle de Acesso HDL, Software Acessos ID-3K e Aplicativo Home + Security. Sendo composta por:

1) Controle de Acesso por Teclado;
2) Controle de Acesso Biométrico;
3) Controle de Acesso por Leitor (TAGs/ Cartões);
4) Controle de Acesso Módulo Conexões RF;

CAPÍTULO III – ESPECIFICAÇÕES TÉCNICAS

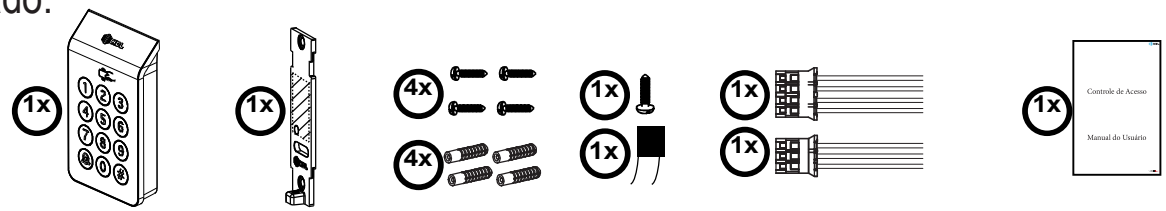
A seguir as especificações técnicas de cada equipamento da linha de Controle de Acesso HDL.

Produto / Especificação	90.02.25.002	90.02.25.003	90.02.25.001	90.02.26.000
	Teclado	Biométrico	Leitor	Módulo Conexões
Registros	3000			
Alcance RFID	15mm			-
Autenticação	Senha / TAG / APP	Biometria/ TAG / APP	TAG / APP	Controle Remoto/ TAG Veícular /APP*
Tipo Antena	Interna (RFID 125KHz)			Interna (RF433 MHz)
Nº de Usuários	3000			
Freq do TAG	RFID 125KHz			UHF RFID (900MHz)
Temp de Operação	0º ~ 40º C			
Tensão	12V			
Consumo	300 mA (Controle de Acesso)			
Dimensão (mm)	125,6x74,9x22,1	126,5x46,7x45,2	125,6x46,7x22,1	125,6x74,9x22,1
Índice de Proteção	IP66	IP44	IP66	IP66
Bluetooth	Sim			
Interface Com.	RS485 (máx 32 dispositivos - 300 mts)			
Wiegand	Sim (1 Saída 26 bits)			Sim (2 Entradas 26/34 Bits)
Wi-Fi*	Sim			
RF 433 MHz Receptor	-			Sim
Aplicativo Móvel	Sim			

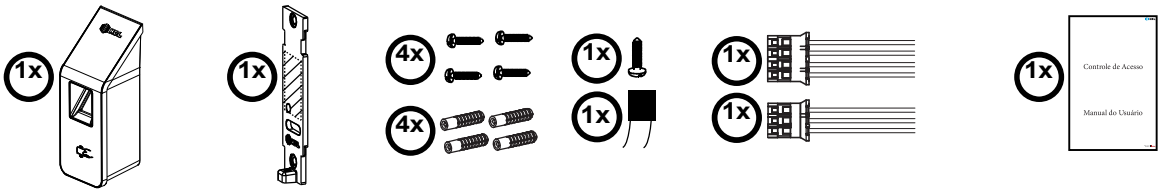
CAPÍTULO IV – CONTEÚDO

Esta embalagem contém:

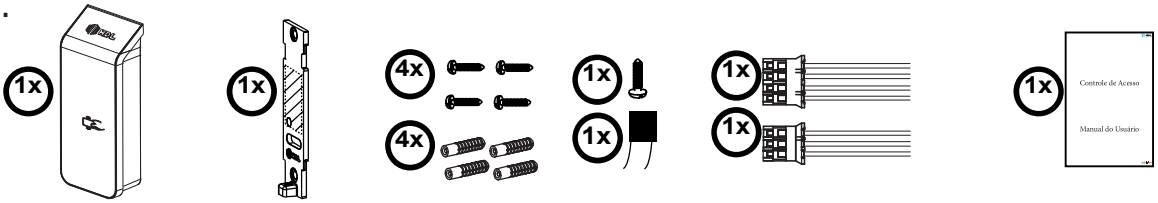
Teclado:



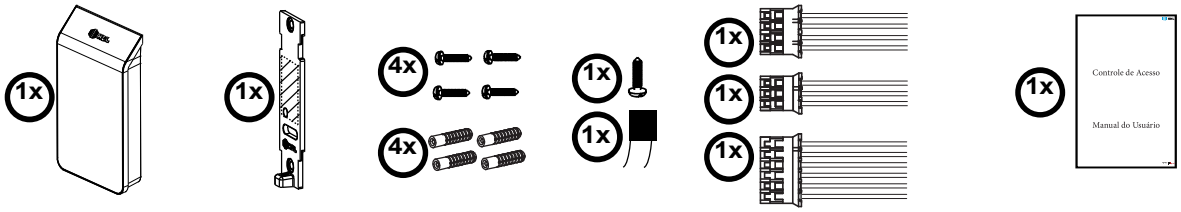
Biométrico:



Leitor:



Módulo Conexões:



CAPÍTULO V – ACESSÓRIOS

Esses equipamentos necessitam de alguns acessórios para o completo funcionamento, antes de iniciar a instalação certifique-se que possua todos os itens essenciais. Utilize os acessórios HDL para um melhor desempenho e vida útil dos equipamentos

Esses acessórios são facilmente encontrados no mercado dessa forma o sistema de Controle de Acesso HDL é compatível com tecnologia já disponíveis. (cartões, TAGs).

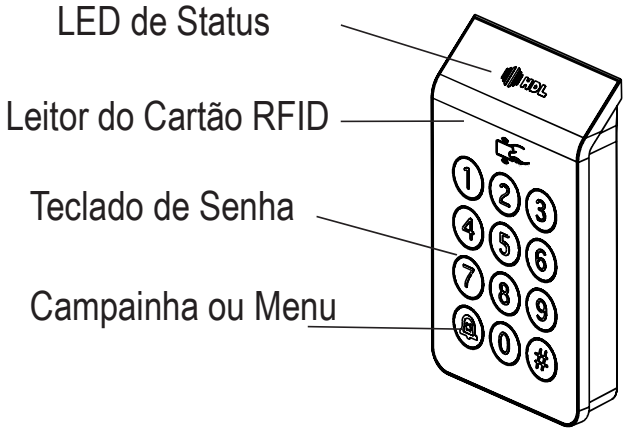
Nota: Utilize apenas fontes de alimentação certificadas para garantir o correto funcionamento e evitar danos aos equipamentos.

Acessório HDL	Código do Produto
Fonte 1A	90.02.92.001
Fonte 3A Light	90.01.90.000
Fonte 3A	90.01.03.024
Controle Remoto (433 MHz)	90.02.02.135
Chaveiro TAG 125KHz	90.02.25.008
Cartão RFID 125KHz	90.02.25.009
Botoeira	90.02.92.003
Aplicativo Movel	HOME + SECURITY

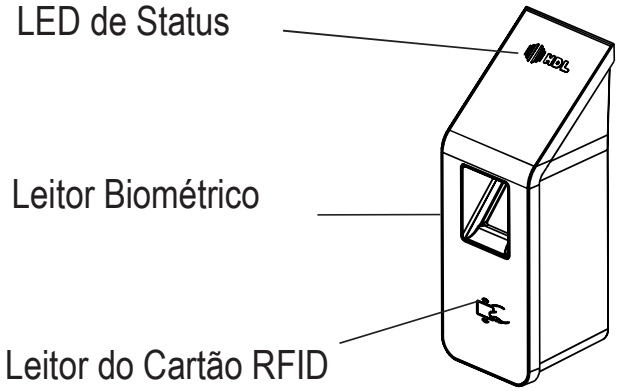
CAPÍTULO VI – APRESENTAÇÃO DO PRODUTO

Este Manual contempla toda a linha de Controle de Acesso da HDL, a seguir será possível conhecer cada equipamento e suas diferenças:

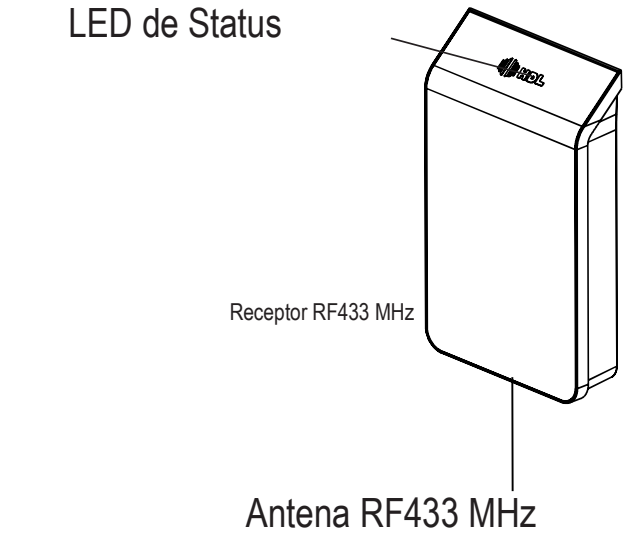
Teclado



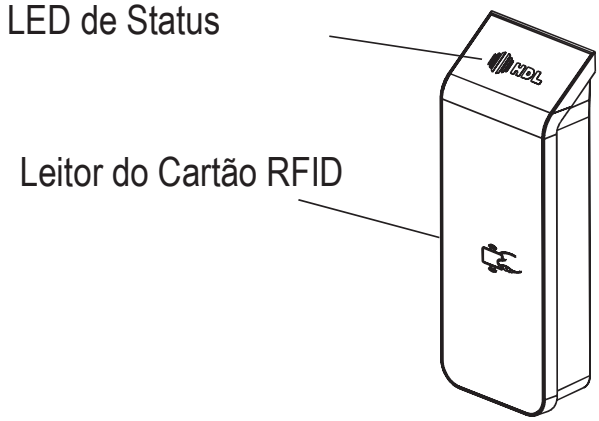
Biometria



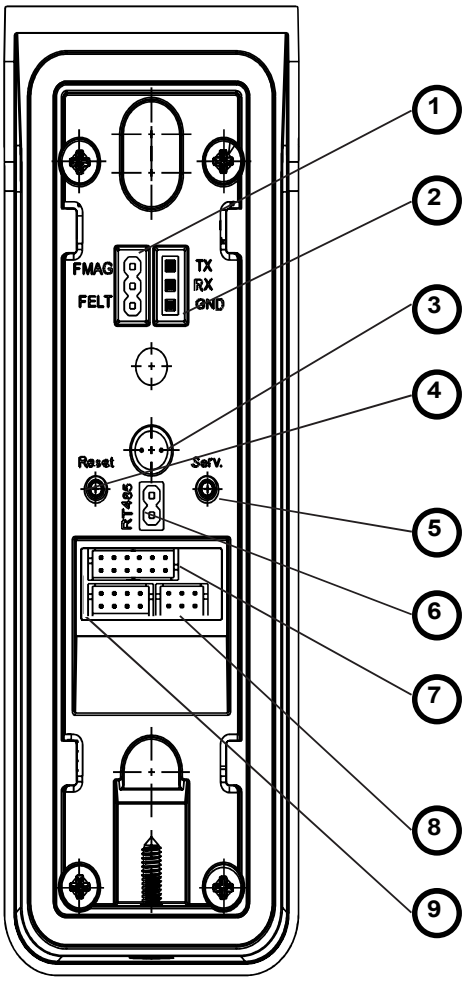
Terminal de Conexões



Leitor



CAPÍTULO VII – IDENTIFICANDO AS CONEXÕES



1

Ao instalar uma fechadura, é necessário posicionar o Jumper de acordo com o tipo utilizado.

 F MAG  F ELT

2

TX/RX- Comunicação Serial RS232

3

Sensor de Violação, após instalado e configurado, esse sensor se torna ativo, quando acionado, todo o sistema é bloqueado.

4

Reset - Reinicia o Aparelho. Vide 8.4 - Essa função não apaga nenhuma informação do equipamento

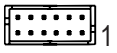
5

Serviço (SERV) - Botão para cadastro dos Cartões/ TAGs ou Controle Remoto Master, Reset de Configurações, usuários e Reset geral.

6

RT485 - Resistor Terminal - Para a instalação no Modo Sistema, É necessário adicionar o jumper em alguns casos de instalações, quando há perdas nas transmissões de dados no barramento RS-485.

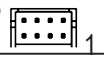
7

Conector 3 (exclusivo para o Módulo de Conexões (RF) 

8

Conector 1 (Comunicação e Alimentação) 

9

Conector 2 (Comandos) 

Conector 1					
1	2	3	4	5	6
Comunicação				Alimentação	
Verde Escuro	Amarelo	Branco	Laranja	Preto	Vermelho
Wiegand D0	RS485_N	Wiegand D1	RS485_P	GND	12V

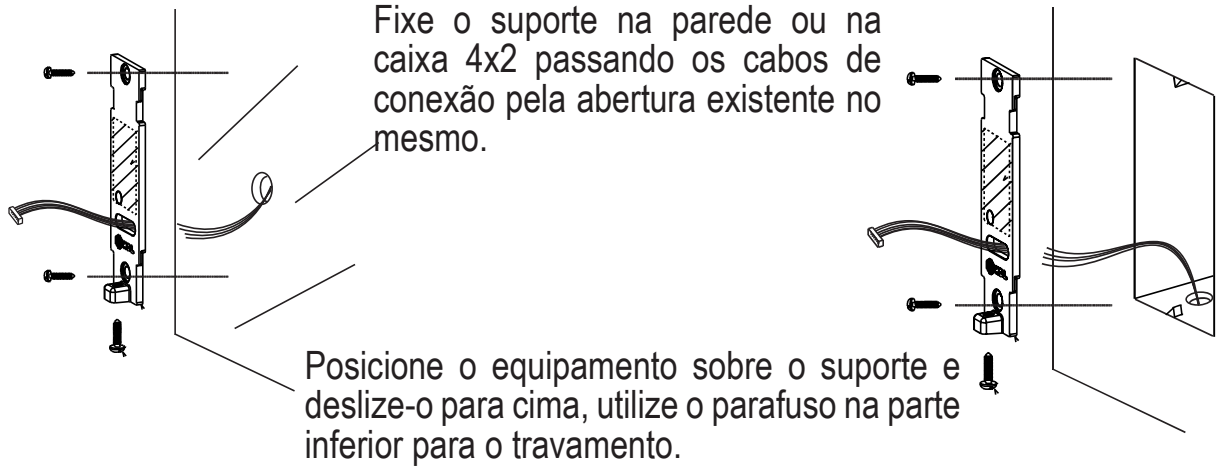
Conector 2							
1	2	3	4	5	6	7	8
Marron	Azul	Preto	Roxo	Cinza	Verde C.	Preto	Preto
Comandos							
F. Elet. Mec	F. Comum	GND	F. Mag	Bot	Camp	GND	GND

Conector 3											
1	2	3	4	5	6	7	8	9	10	11	12
Verde Esc.	Branco	Amarelo	Laranja	Azul	Preto	Cinza	Preto	Amarelo	Laranja	Azul	Preto
Comunicação		Comandos									
Wiegand 2_D0	Wiegand 2_D1	Contato Seco_1	Contato Seco_1	Sensor 1	GND	Bot_2	GND	Contato Seco_2	Contato Seco_2	Sensor 2	GND

CAPÍTULO VIII – INSTALAÇÃO

8.1 - Fixando o equipamento

Desenvolvido com o objetivo de tornar a instalação simples e prática, o suporte de fixação dos controles de acesso HDL possui o mesmo design e fixação, podendo a mesma ser alternada entre os dispositivos.



Fixe o suporte na parede ou na caixa 4x2 passando os cabos de conexão pela abertura existente no mesmo.

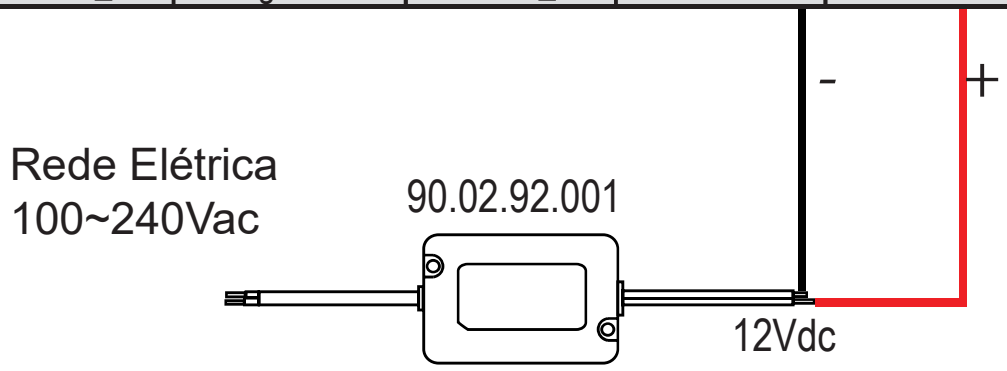
Posicione o equipamento sobre o suporte e deslize-o para cima, utilize o parafuso na parte inferior para o travamento.

8.2 - Conectando a Fonte de Alimentação

A seguir poderá identificar a conexão elétrica do controle de acesso de acordo com a fonte de alimentação, recomendamos a utilização de fontes HDL.

8.2.1 - Utilizando a Fonte de Alimentação Controle de Acesso

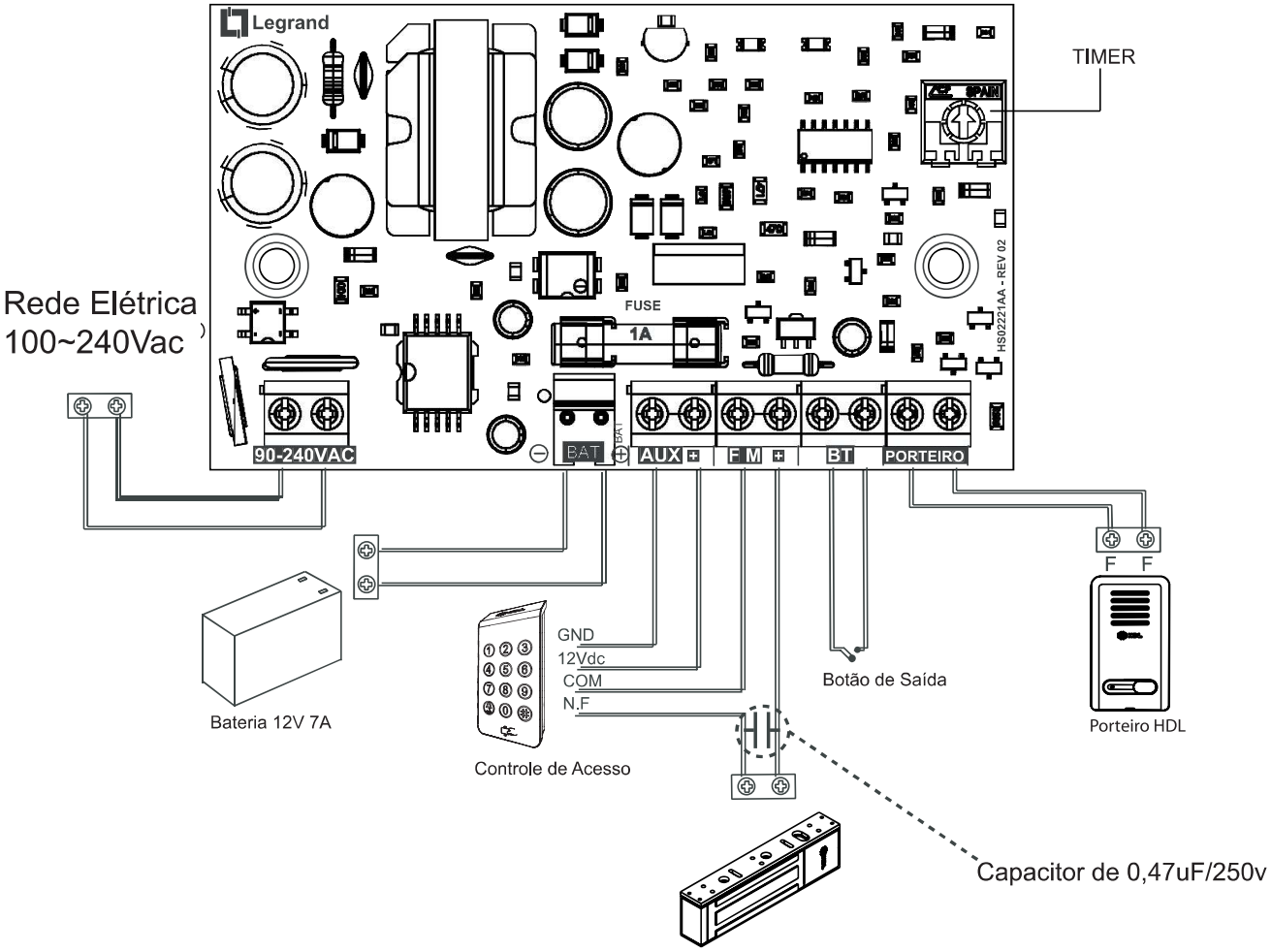
Conector 1					
1	2	3	4	5	6
Comunicação				Alimentação	
Verde Escuro	Amarelo	Branco	Laranja	Preto	Vermelho
Wiegand D0	RS485_N	Wiegand D1	RS485_P	GND	12V



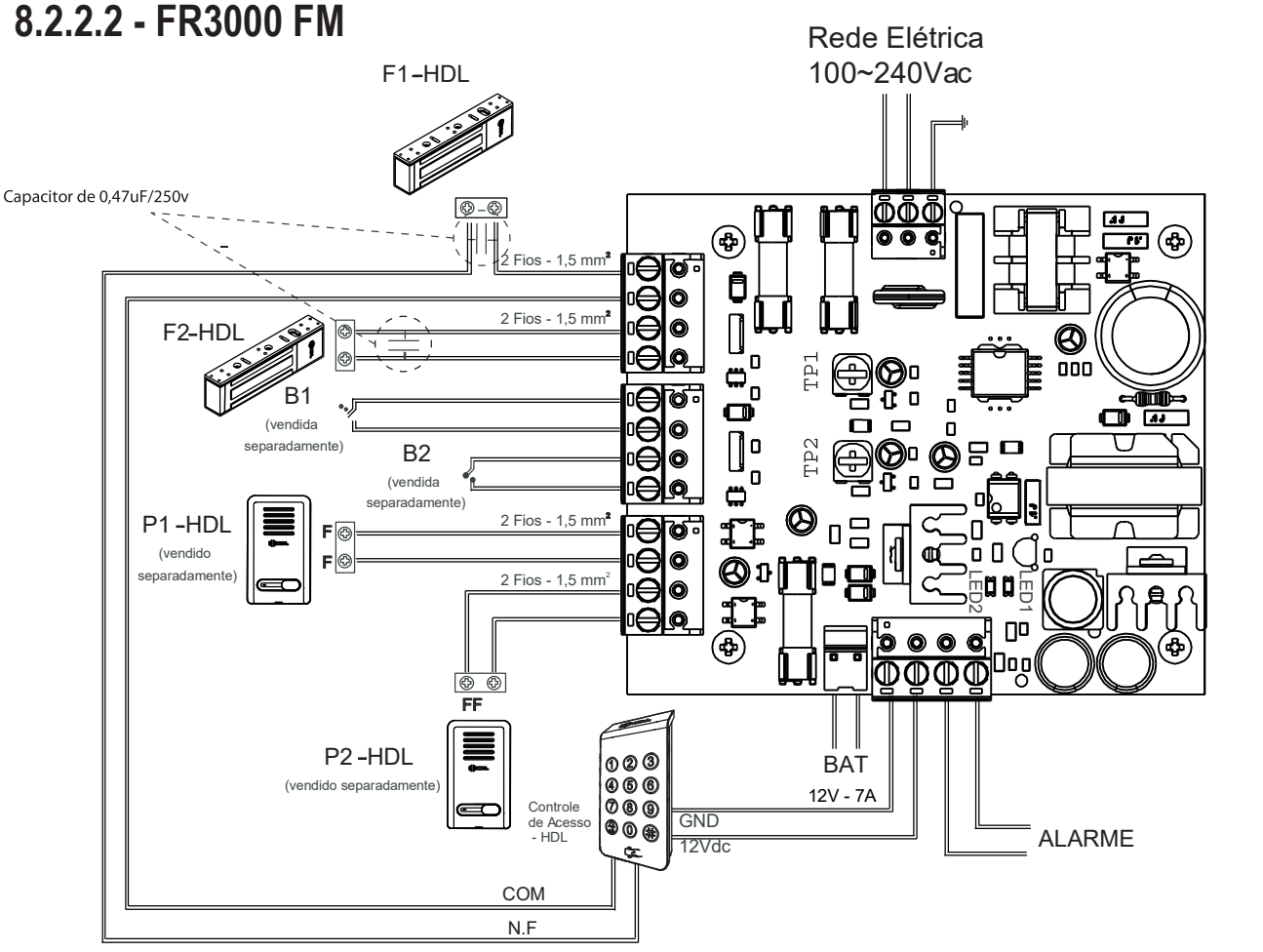
8.2.2 - Utilizando a Fonte de Alimentação FR3000 Light ou FR3000FM

As fontes FR3000 FM ou FR3000 Light, são desenvolvidas para reduzir a quantidade de dispositivos necessários para a instalação, possuindo saídas e entradas para diversos dispositivos que possam compor o sistema de controle de acesso, veja a seguir as formas de Conexão. Para maiores informações sobre as fontes, consulte o manual do modelo escolhido.

8.2.2.1 - FR3000 LIGHT



8.2.2.2 - FR3000 FM

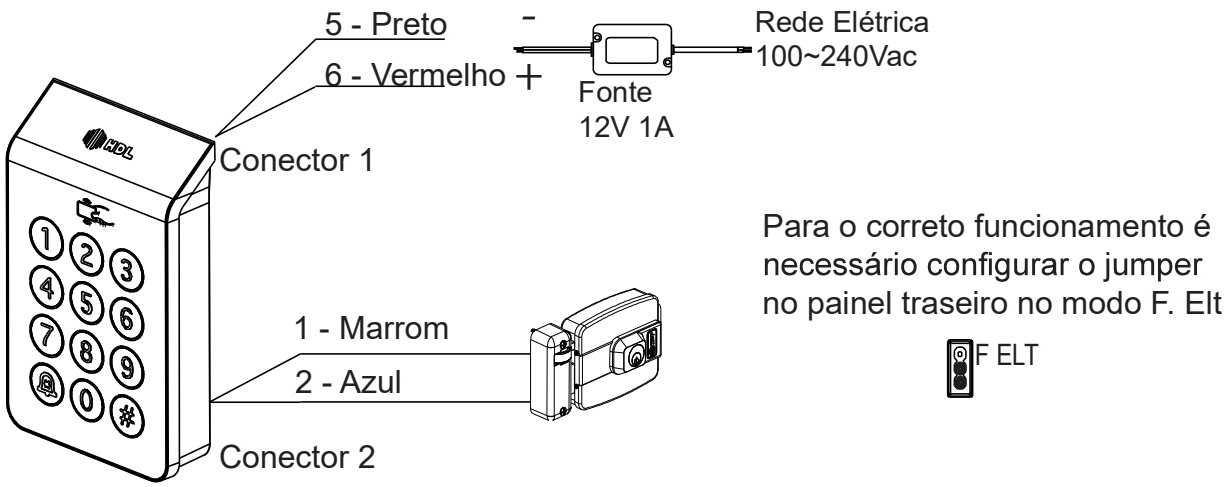


Nota: Na fonte FR3000 FM, Não oferece compatibilidade de abertura independente das fechaduras através do Controle de Acesso.

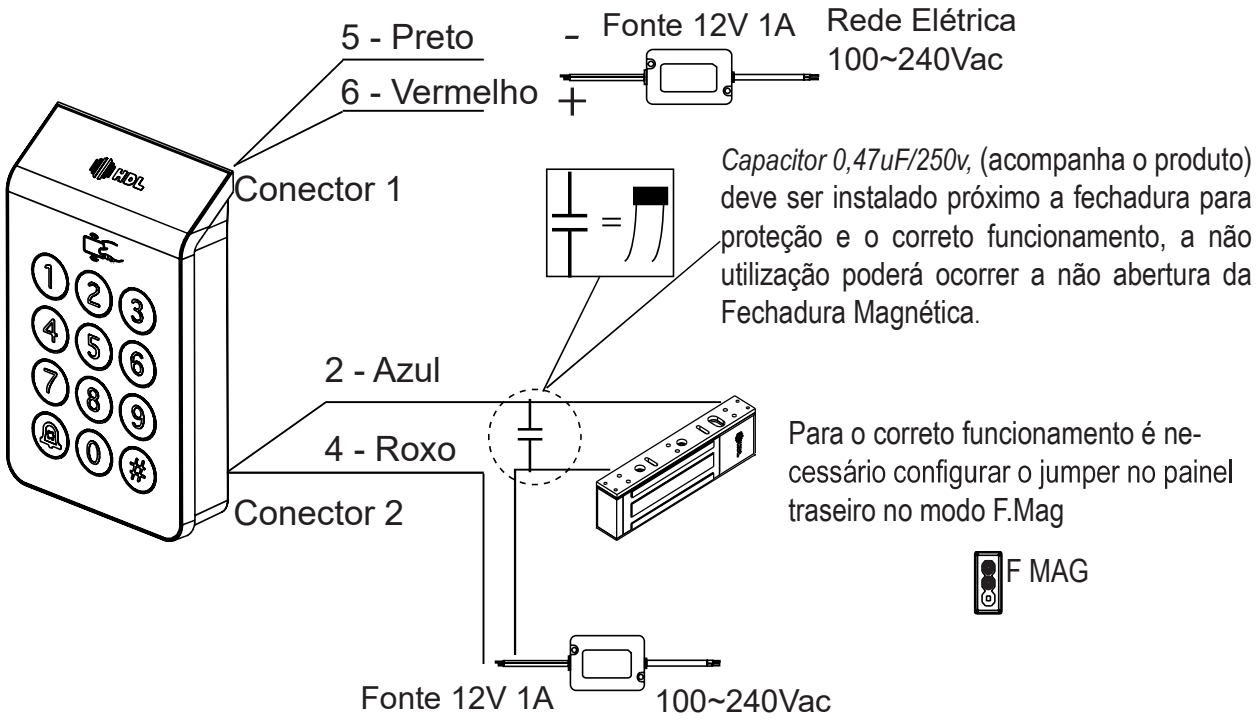
8.3 - Conectar uma Fechadura

Selecione o Jumper, conforme mostrado no CAPÍTULO VII, de acordo com o tipo de fechadura utilizada. (Fechadura Eletro-Mecânica ou Fechadura Magnética), essa configuração aplica-se a todos os equipamentos da linha de Controle de Acesso.

8.3.1 - Fechadura Elétrica



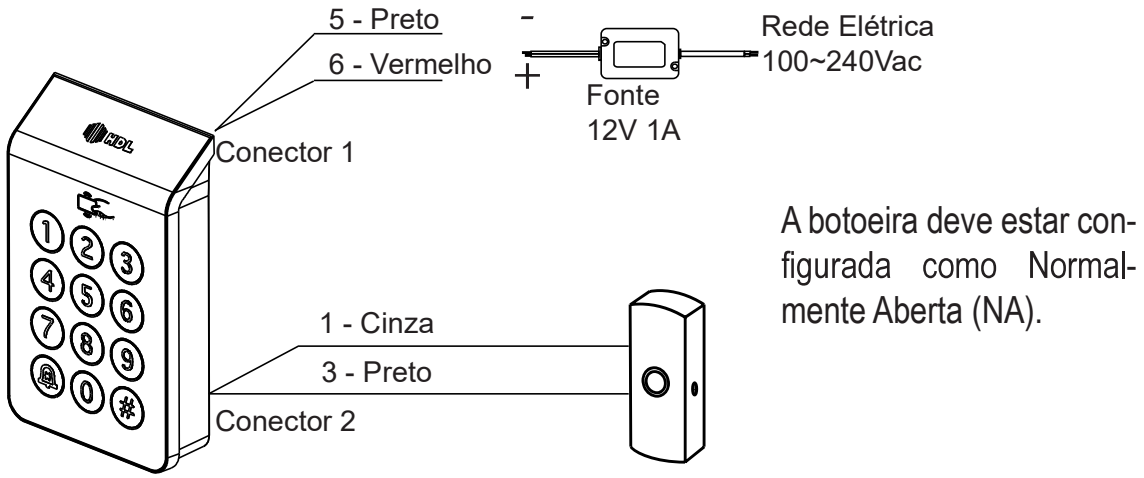
8.3.2 - Fechadura Magnética



8.4 - Conectar uma Botoeira / Sensor de Porta

Para a abertura da porta ou portão pelo interior do ambiente, é possível instalar uma botoeira ao sistema. Toda abertura por comando de botoeira é registrada em memória como um evento de botoeira para monitoramento ou posterior adoção de medidas de controle. Recomendamos a utilização da Botoeira HDL. A entrada de botoeira compartilha também a função de sensor de porta o que permite monitorar o estado da porta. Ao identificar em estado aberto emite um alerta de forma a informar sua abertura. Permite configurar para receber sensor NA ou NF além da configuração de retardo para informar a abertura.

Gera eventos de porta Aberta e fechada para monitoramento.

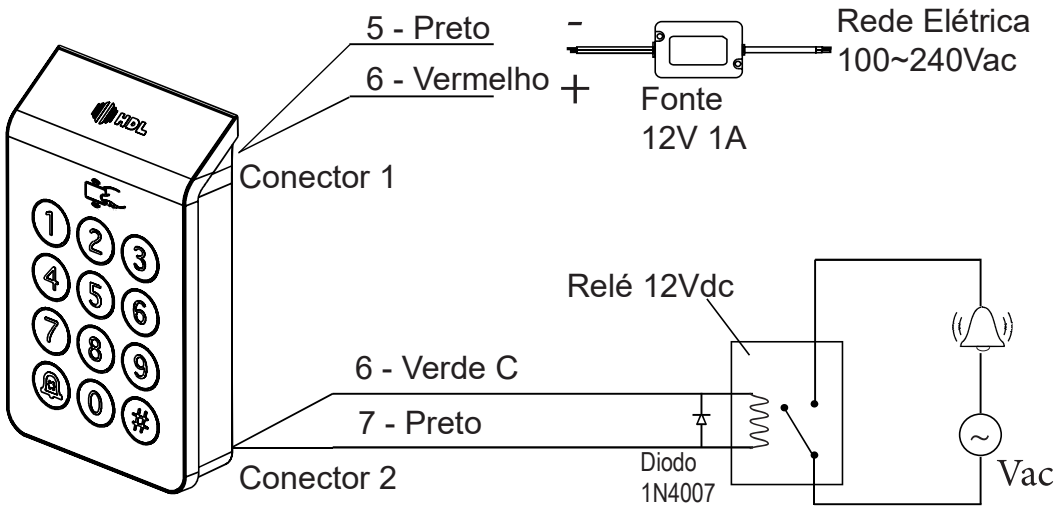


A botoeira deve estar configurada como Normalmente Aberta (NA).

Nota: É possível através do Software Acessos ID-3k, desativar a botoeira e utilizar a conexão para entrada de sensor de porta, dessa forma, quando a porta permanecer aberta mais que o tempo determinado. (sinalização sonora + evento de Software).

8.5 - Conectar uma Campainha

No Controle de Acesso por teclado, existe a opção de campainha, no qual é possível conectar um modulo sonoro para acionamento. (pressione por 3 seg)

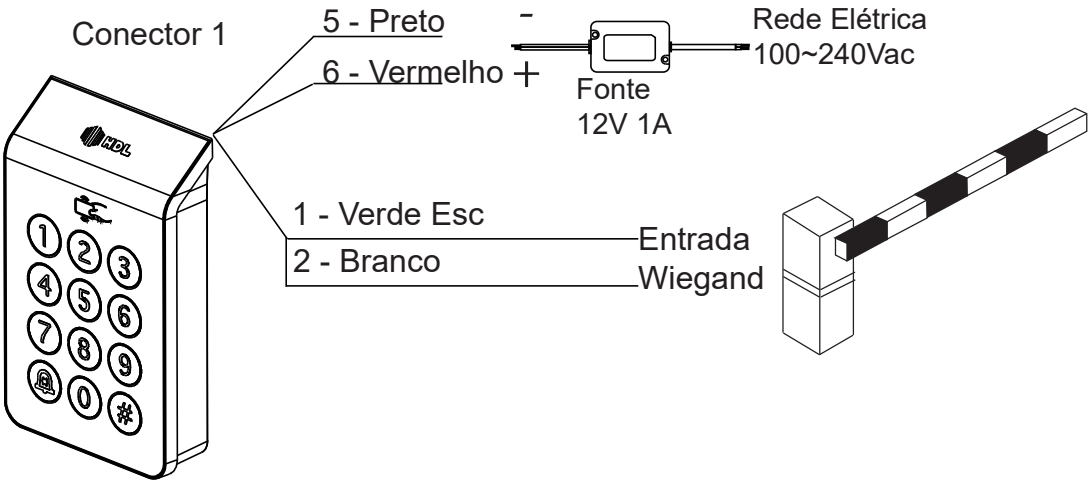


NOTA: Função disponível apenas para o modelo com teclado Numérico. Relé, diodo e campainha não acompanham o produto. Pressione por 3 seg ou mais.

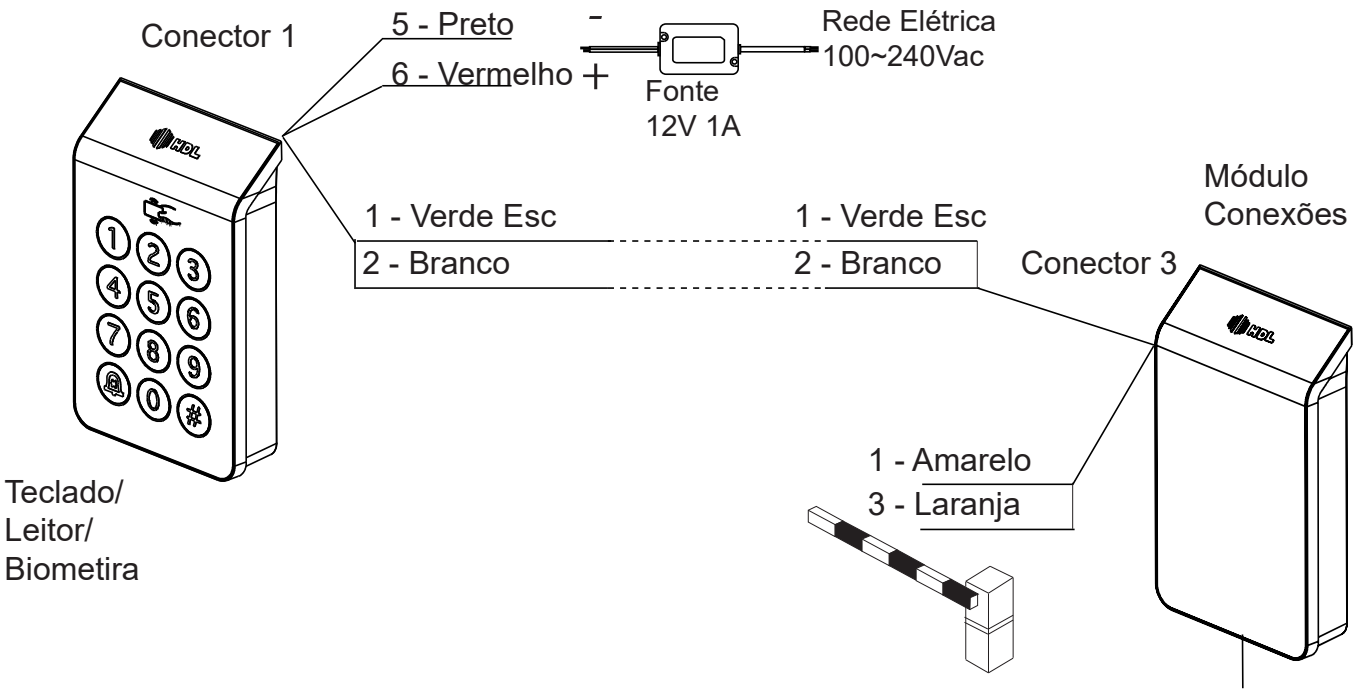
8.6 - Adicionando uma catraca ou cancela Wiegand

Os equipamentos da linha de Controle de Acesso HDL, possuem o protocolo Wiegand para integração de outros dispositivos de controle permitindo assim a utilização dos equipamentos em locais com equipamentos já existentes (catracas, cancelas e etc...).

Nota: Disponível para modelos Leitor, Biométrico e Teclado quando em modo Reader ou Stand Alone, dessa forma, é necessário uma controladora na Cancela.



Instalando Cancela com o Módulo de Conexões:



Dessa forma, na figura acima o Módulo de Conexões HDL assume a função de Controladora, recebendo as informações dos dispositivos, verificando e acionando cancelas ou portões. A credencial BIOMETRIA não é enviada através do Weigand devido ao tamanho da informação. Nesse cenário, TAGs lidas no módulo Teclado serão enviadas para o módulo Conexões e validadas nas credenciais registradas no campo Tag Wiegand.

8.7 - Módulo de Conexões

O Módulo de Conexões pode ser acionado por controle remoto, por TAGs veículares (utilizando antena UHF RFID via Protocolo Wiegand) ou Aplicativo através do Bluetooth.

8.7.1 - Acionamento por Controle Remoto

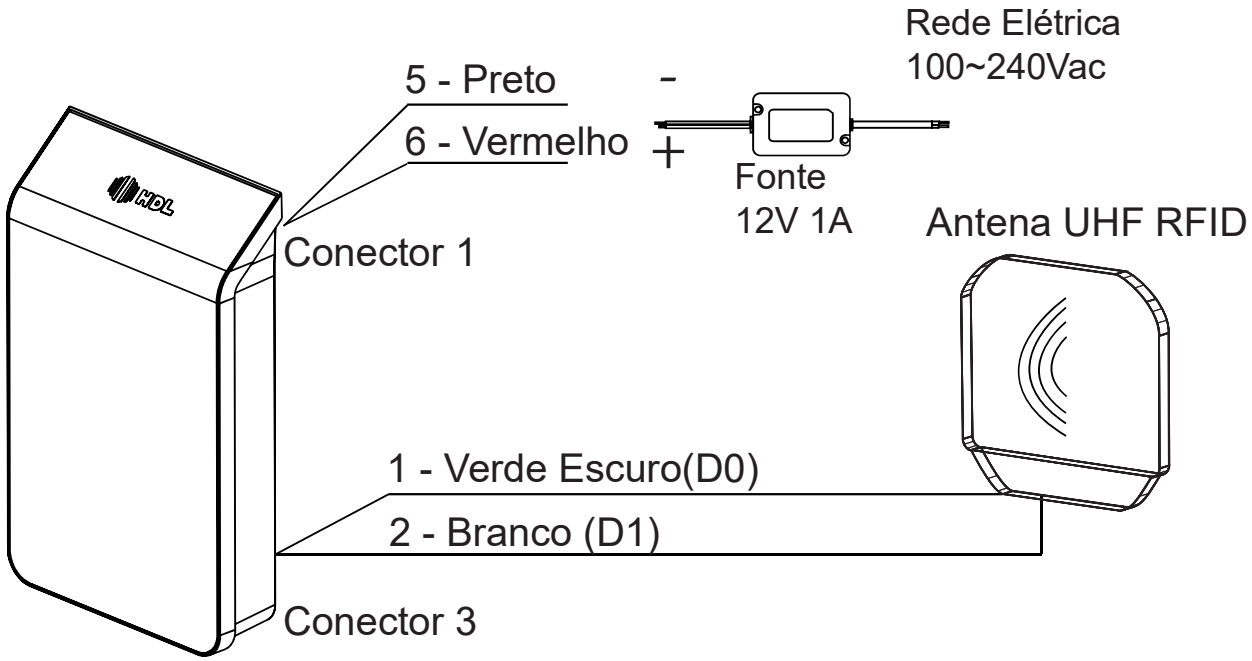
Para funcionamento por Controle Remoto do Módulo de Conexões, faça o cadastramento do controle remoto, veja no Capítulo XI - Cadastro de Controle Remoto

.

8.7.2 - Acionamento por TAGs Veículares

Para o funcionamento por TAGs Veículares (adesivo fixado no vidro dos veículos) deve-se instalar a antena de recepção e em seguida realizar o cadastro das TAGs localmente ou através do Software de forma manual.

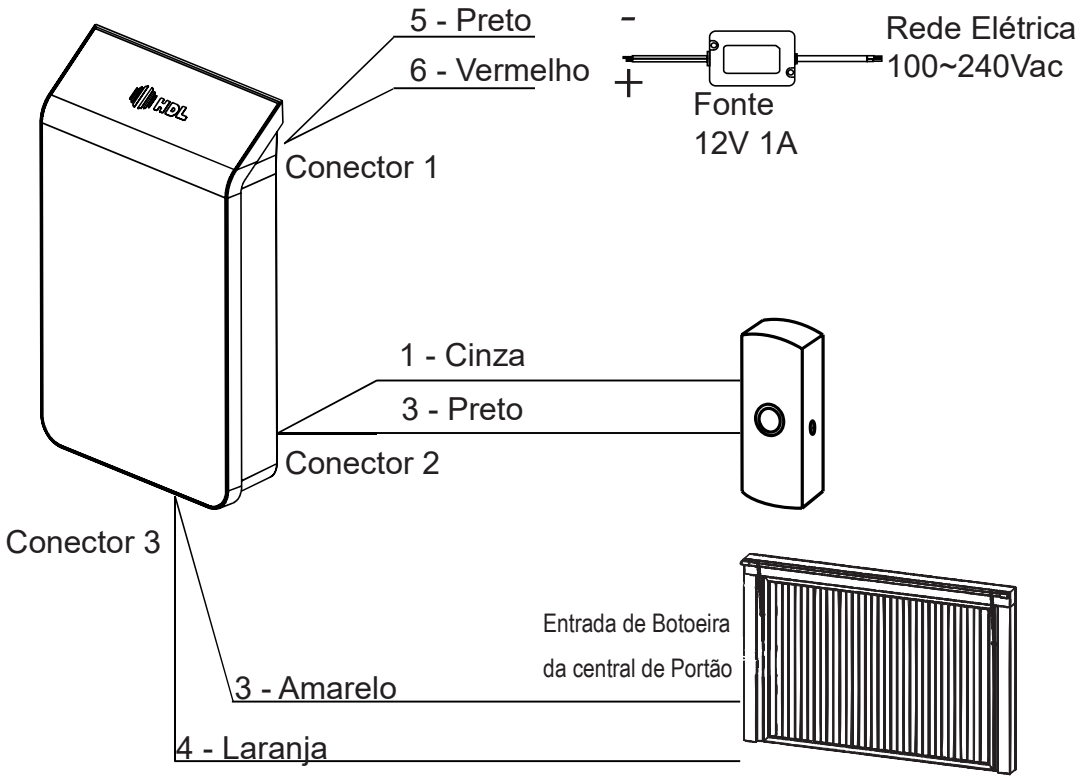
8.7.3 - Conectando uma Antena Externa



Nota: Verifique a forma de alimentação da Antena UHF RFID de acordo com o modelo utilizado. A alimentação da Antena e do Módulo de Conexões devem estar balanceadas.

Nota: A antena deve possuir comunicação pelo protocolo Wiegand, sendo ela responsável pelo reconhecimento e envio do comando para o Módulo de Conexões. deve ser conectado através do Conector 3 (Wiegand In - pode ser configurado como 26 ou 34 bits).

8.7.4 - Conectando Portões e Botoeiras



O Módulo de Conexões, possui 2 saídas de contatos secos, nas quais estão relacionadas com os botões do controle remoto, ou seja, botão 1 controle remoto aciona Saída Contato_Seco 1 e botão 2 controle remoto aciona saída Contato Seco 2 do equipamento.

O Módulo de Conexões, também possui saída de acionamento para fechadura eletromecânia ou fechadura eletro magnética, entretanto essa saída é sempre acionada através do botão 1 ou botão 2 do controle remoto ou por Bluetooth (exceto o contato seco).

Obs: Conecte o contato seco do Modulo de Conexões a entrada de pulso do portão, para maiores informações consulte o manual do portão.

Nota: É altamente recomendado a utilização de sensores de barreira para acionamento do portão a fim de evitar acidentes com o fechamento do portão na presença

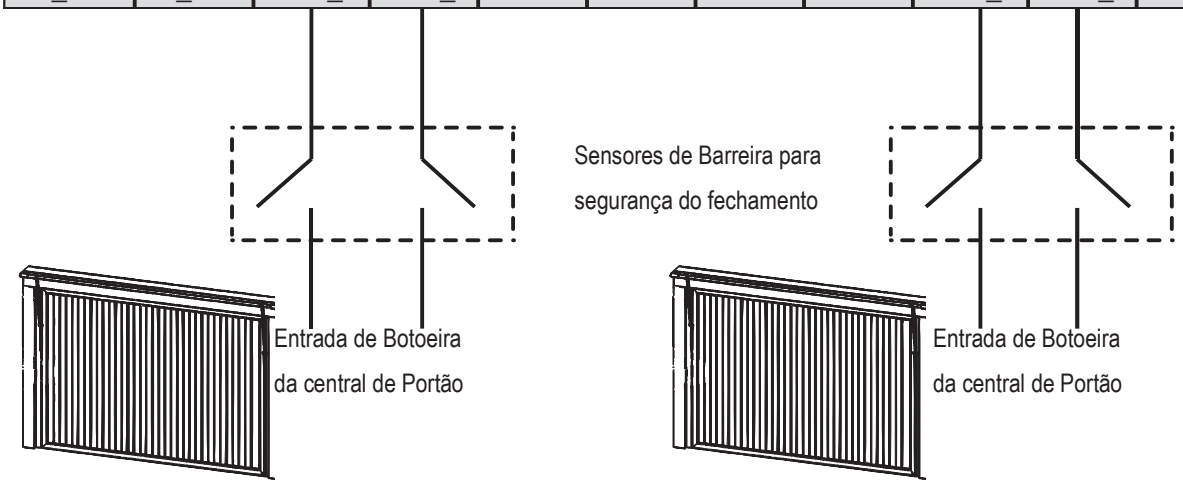
de veículos.

Evite a transição de pedestres através do portão, mesmo possuindo os sensores de bloqueio o mesmo poderá ser acionado.

8.8 - Modos de acionamento de Portões

O modulo de Conexões permite a instalação do sistema de eclusa ou gaiola para utilização em condomínios, podendo ser aplicado em portões de pedestre ou de veículos, a seguir os possíveis modos de instalação.

Conector 3											
1	2	3	4	5	6	7	8	9	10	11	12
Verde Esc.	Branco	Amarelo	Laranja	Azul	Preto	Cinza	Preto	Amarelo	Laranja	Azul	Preto
Comunicação		Comandos									
Wiegand 2_D0	Wiegand 2_D1	Contato Seco_1	Contato Seco_1	Sensor 1	GND	Bot_2	GND	Contato Seco_2	Contato Seco_2	Sensor 2	GND

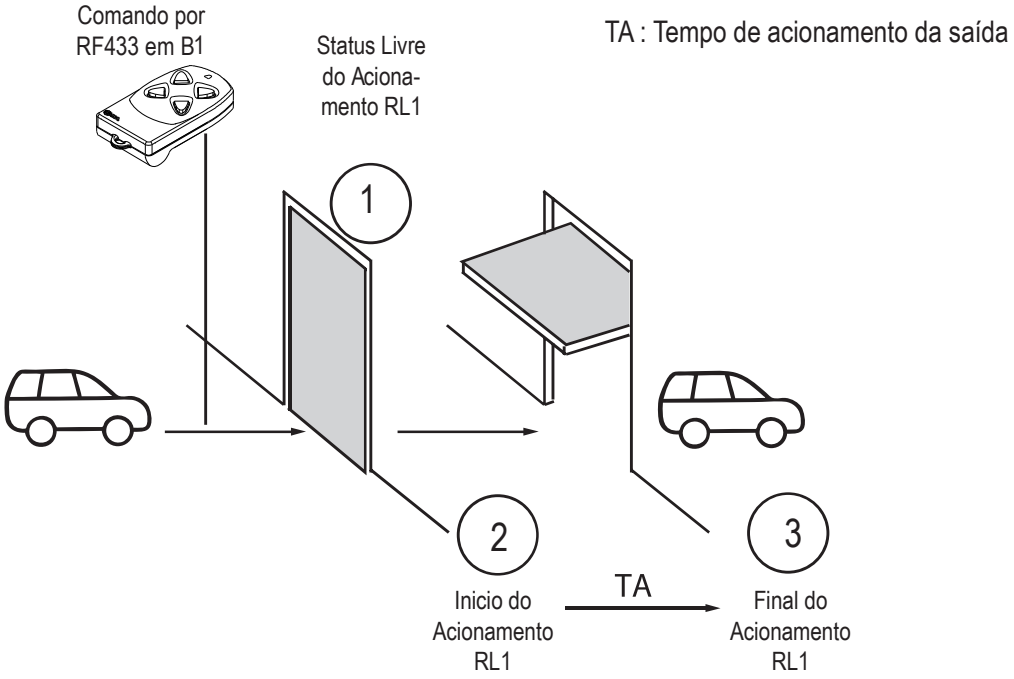


Os modos de operação do módulo conexões se divide em dois grupos, modo independente e modo de intertravamento. Os modos independentes são indicados a aplicações nas quais as duas saídas RL1 e RL2 precisam ser ativadas simultaneamente e de forma independente. Os modos com intertravamento, utilizam-se dos estados indicados pelos sensores S1 e S2 para não permitir que as duas saídas sejam ativadas simultaneamente.

8.1 - Independente Simples

O Acionamento de cada Relé (RL1, RL2) é feita individualmente, ou seja, ambos podem serem acionados ao mesmo tempo através do comando de acionamento de

Controle Remoto, Conexão wiegand ou Botoeiras.

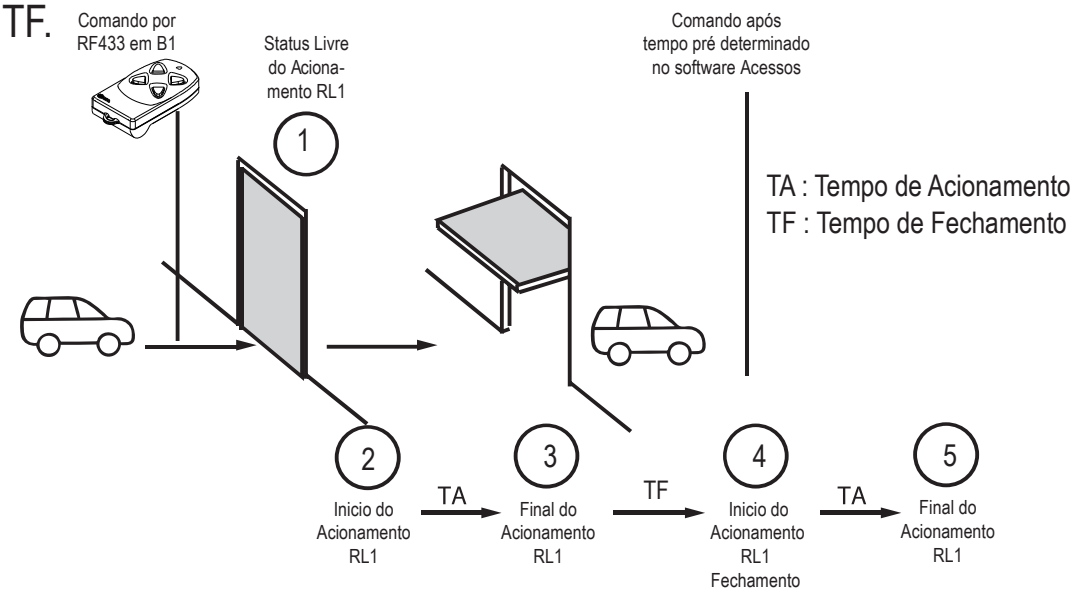


Nota: O diagrama acima é válido também para B2 e RL2.

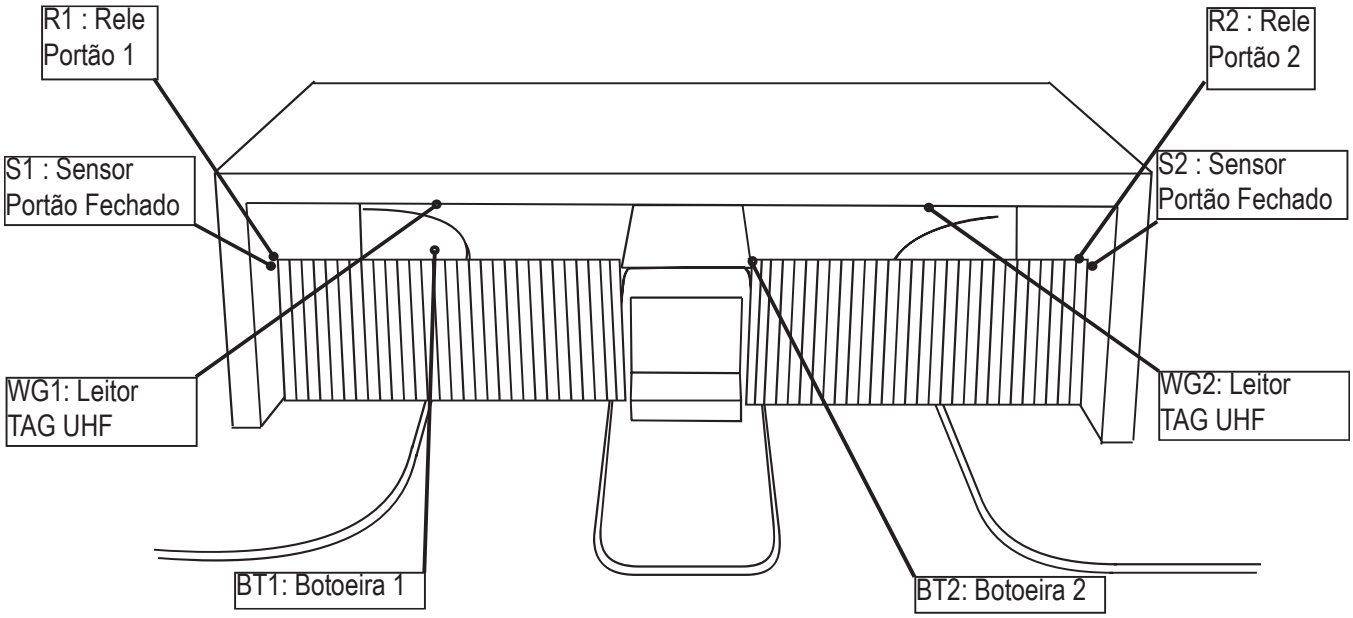
8.2 - Independente Temporizado

O Acionamento de cada Relé (RL1, RL2) é feita individual (ambas podem serem acionadas ao mesmo tempo) e há um segundo pulso para fechamento de forma temporizada (2s, 5s, 10s, 20s,30s, 1min, 2min).

O Diagrama abaixo exibe o fluxo de acionamento iniciado com um comando por controle remoto RF433. O tempo TA corresponde ao tempo de acionamento da saída a relé, configurado pelo Software Acessos ID-3K. Após o término do acionamento é iniciado a contagem do tempo de Temporização, intervalo de tempo configurado após o acionamento para gerar um segundo pulso, da mesma saída, para fechamento TF.



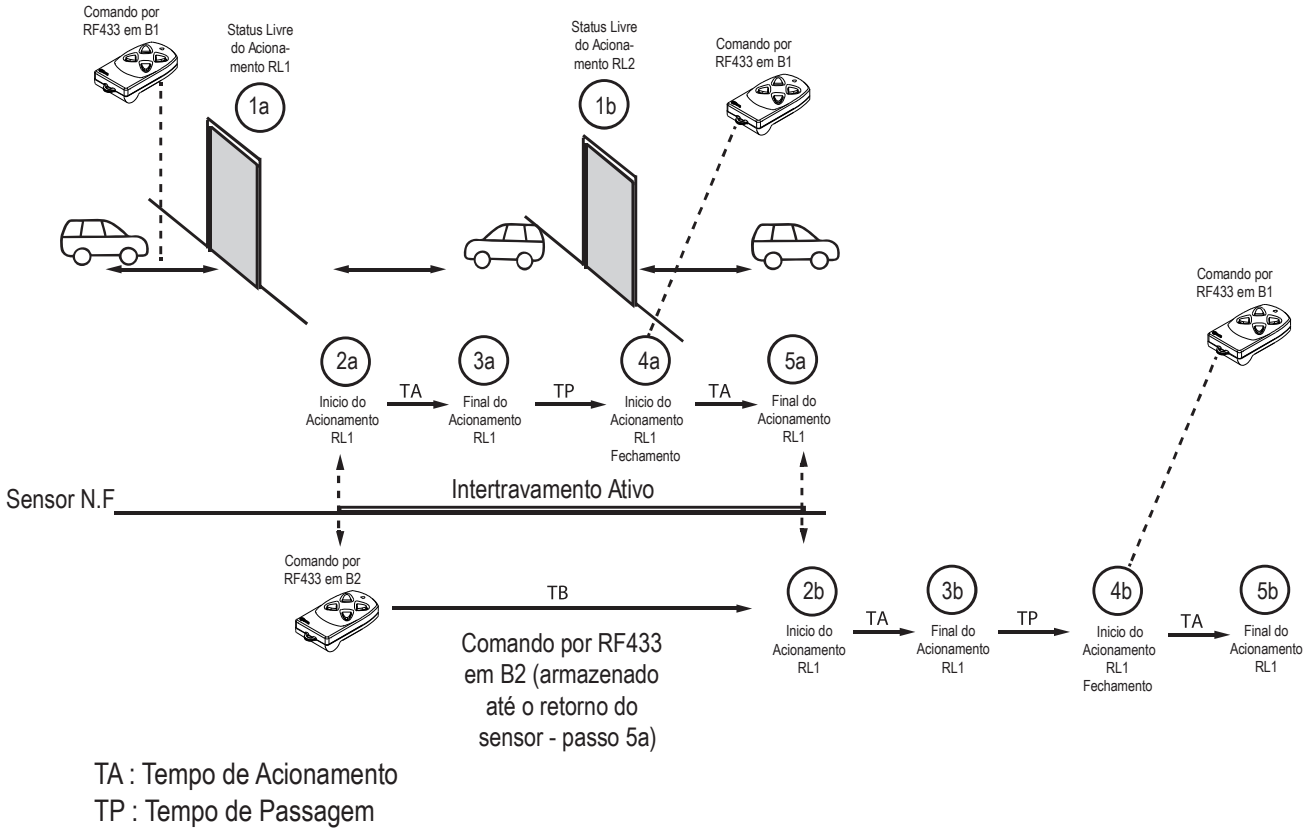
Nota: O diagrama acima é válido também para B2 e RL2.



8.3 - Intertravamento Simples

Neste modo de operação o acionamento de cada uma das saídas a Relé (RL1 e RL2) são intertravados, logo somente uma das saídas poderá ser acionada por vez.

O Acionamento de cada Relé (RL1, RL2) são intertravados, possibilitando somente a ativação de um por vez. Quando ocorre a ativação de um acionamento e o seu sensor passa para estado ativo (porta aberta) o outro acionamento é possível somente quando o sensor do acionamento anterior retorne para estado desativado (porta fechada). Caso ocorra uma tentativa do acionamento que não possa atuar naquele momento, o comando é memorizado esperando o retorno do sensor do acionamento anterior para o estado desativado.



Nota: O intertravamento, visualizado no diagrama acima, ocorre nos 2 sentidos, tanto da Entrada (RL1 e depois RL2) quanto na saída (RL2 e depois RL1).

8.4 - Intertravamento Temporizado

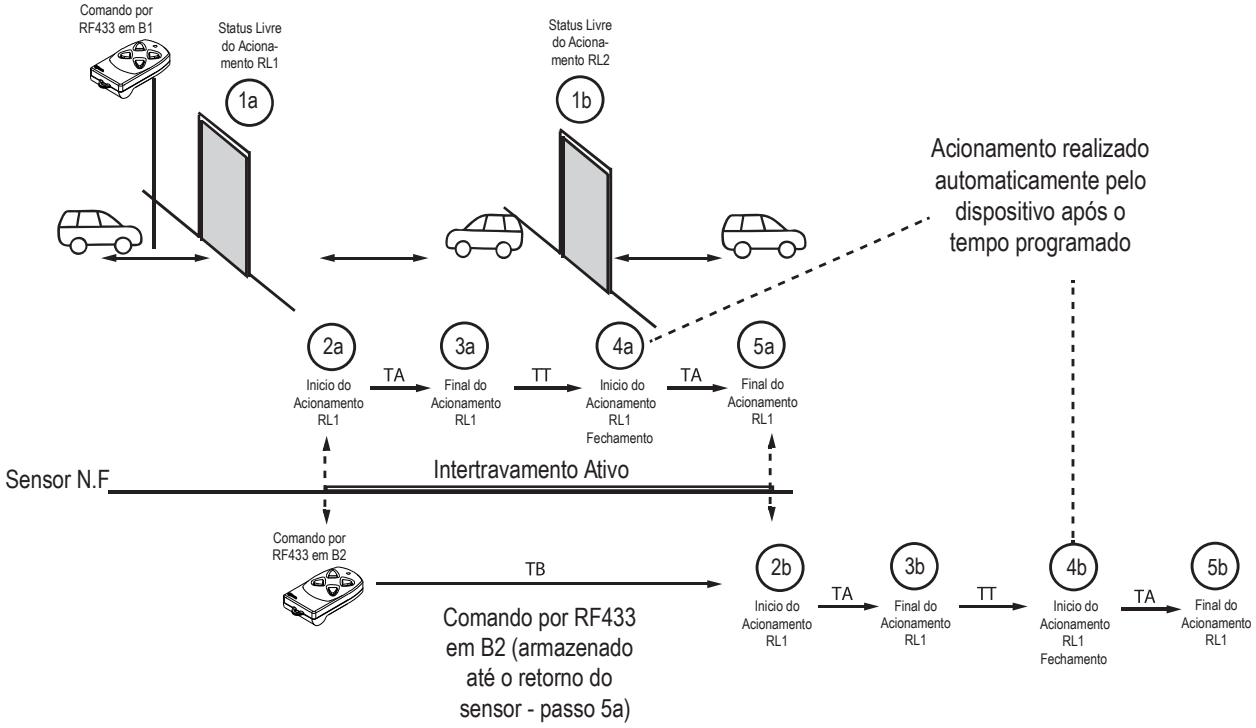
O Acionamento de cada Relé (RL1, RL2) são intertravados, possibilitando somente a ativação de um por vez. Quando ocorre a ativação de um acionamento e o seu sensor passa para estado Ativo (Porta aberta) o outro acionamento é possível somente quando o sensor do acionamento anterior retorne estado desativado (Porta Fechada). É dado um segundo pulso para fechamento de forma temporizada (2s, 5s, 10s, 20s,30s, 1min, 2min).

Caso ocorra uma tentativa do acionamento que não possa atuar naquele momento, o comando é memorizado esperando o retorno do sensor do acionamento anterior para ABERTO.

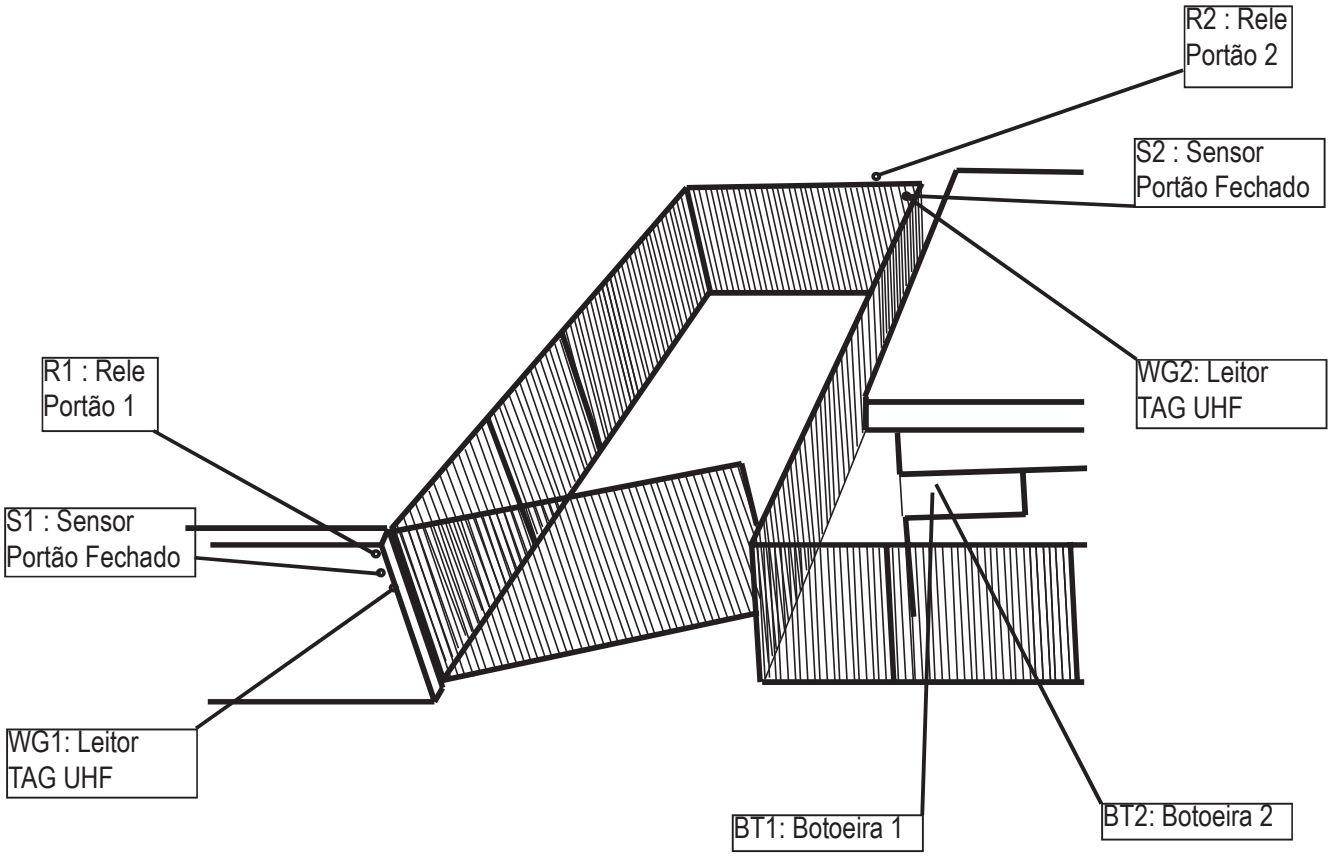
Neste modo se os sensores não forem conectados, ou seja, sempre em Aberto, funcionará como o modo independente temporizado.

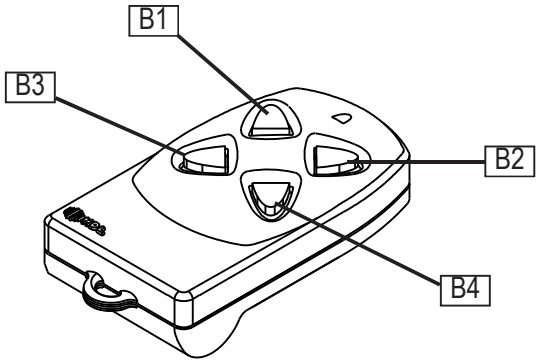
Importante ressaltar que a temporização de fechamento é independente do estado do sensor. Após o término do acionamento se inicia a contagem do tempo de abertura do portão que quando finalizado gera um novo acionamento para fecha-

mento do portão



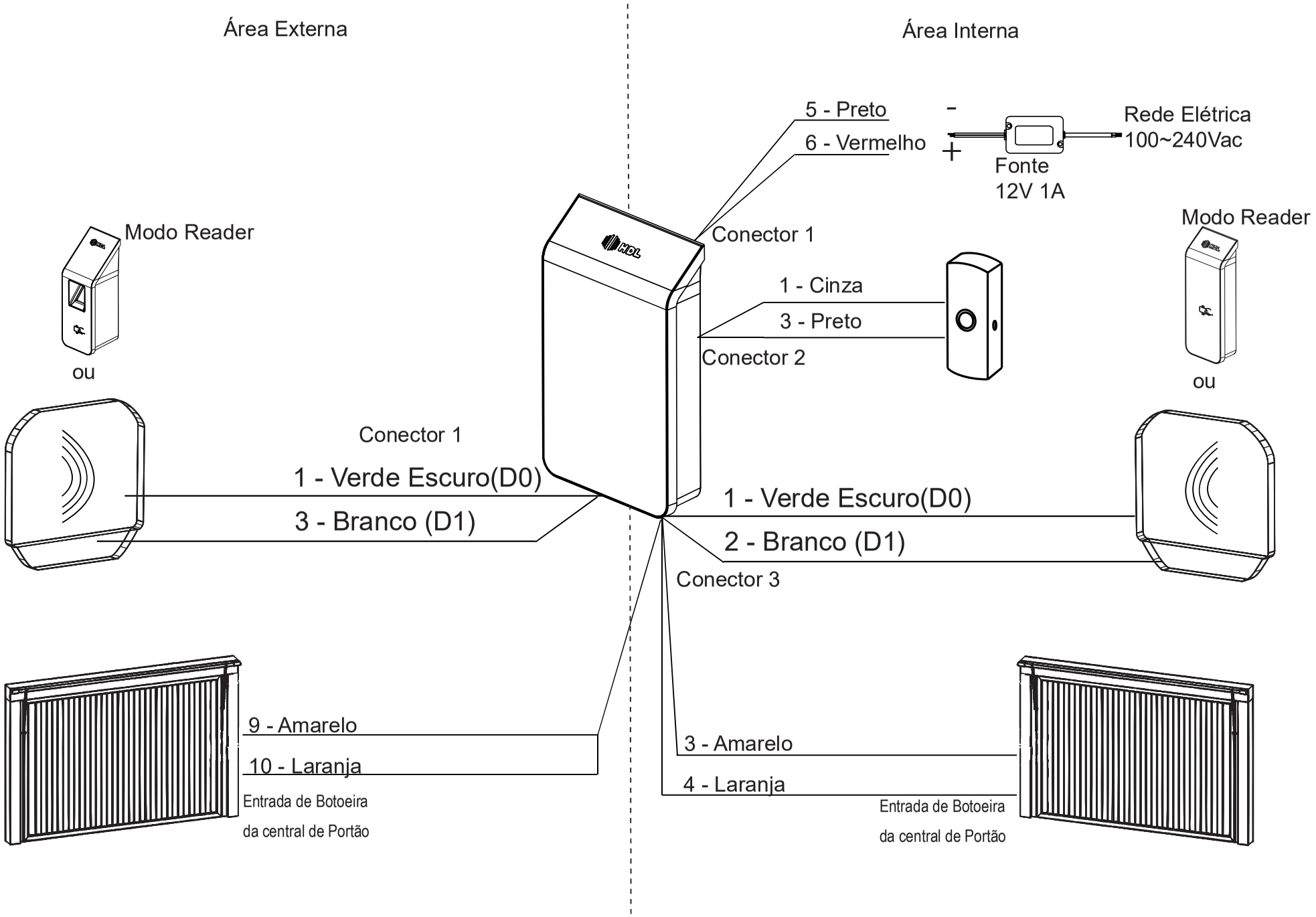
TA : Tempo de Acionamento
TT : Tempo do Temporizador





8.5 - Tabela Comando x Saída

Comando de Acionamento		Saídas Acionadas			
		Relés		Fechos	
		RL1 - Portão 1	RL2 - Portão 2	Comum	Magnético
Controle Remoto	B1	X		X	X
	B2		X	X	X
	B3	X		X	X
	B4		X	X	X
TAG Veicular (Wiegand)	WG1	X		X	X
	WG2		X	X	X
Botoeiras	BT1	X		X	X
	BT2		X	X	X


Área Externa
Área Interna
5 - Preto
6 - Vermelho
-
+
Fonte
12V 1A
Rede Elétrica
100~240Vac
Modo Reader
Conector 1
1 - Cinza
3 - Preto
Conector 2
Modo Reader
ou
ou
Conector 1
1 - Verde Escuro(D0)
3 - Branco (D1)
1 - Verde Escuro(D0)
2 - Branco (D1)
Conector 3
9 - Amarelo
10 - Laranja
Entrada de Botoeira
da central de Portão
3 - Amarelo
4 - Laranja
Entrada de Botoeira
da central de Portão

CAPITULO IX – INFORMAÇÕES SOBRE PRODUTO

9.1 - Padrões de Fábrica

Função	Descrição	Valor	Padrão
Sistema	Senha de Admin	1234	Cadastrada
	Modo Simplificado	-	Ativado
Cadastro	TAGs Master	-	Não Cadastrada
	N° Max TAGs Master	2	-
	TAGs de Acesso	-	Não Cadastrada
Sinalização	Sinalização Sonora	-	Ativado
Fechadura/Botoeira	Modo Botoeira	1	Ativado
	Modo de Acionamento	0	Modo Pulsado
	Tempo de Acionamento	50	0,5 seg
	Tempo pulso ON	02	02 ms
	Tempo pulso OFF	06	06 ms

9.2 - Sinalização Visual

Status do Aparelho	Identificação de Cor
Estado Normal	Azul
Modo de Programação	Amarelo
Acesso Negado	Vermelho
Acesso Liberado	Verde
Confirmação de Programação	Verde
Rejeição de Programação	Vermelho
Estado de Violação	Vermelho Piscando
Modo de Descadastro	Amarelo Piscando
Modo de Edição (Cadastro simples)	Amarelo e Piscando Verde

9.3 - Sinalização Sonora

Status do Aparelho	Identificação de Bips
Confirmação	3 Bips Curtos
Modo de Programação	5 Bips Curtos
Acesso Negado	1 Bip Longo
Acesso Liberado	3 Bips Curtos
Final de Operação(timeout)	1 Bip longo
Alerta de Reset (Exclusão de Dados)	3 bips longos + Led em vermelho
Memória de Usuários Cheia	2 bips longos + 2x vermelho piscando
Estado de Violação	Bips longos continuamente

9.4 - Botão Serv (Serviço)

Permite que o Administrador do Sistema realize algumas ações nos equipamentos.

1- Pressione o botão **SERV** por 3 Segundos.
Acessa o Modo Cadastro Mestre.
2- Pressione o botão **SERV** por 5 Segundos .
Apaga os Registros e Usuários (Cartões, Biometria, Cartões Mestre)
3- Pressione o botão **SERV** por 8 Segundos.
Apaga todas as programações (Exceto registros e usuários)
4- Pressione o botão **SERV** por 10 Segundos.
Reset Geral do equipamento

Nota: Veja a posição do botão **SERV** no Capítulo VII.
Ao pressionar o Botão soará um BIP a cada segundo, para auxílio do usuário.
É possível habitar para que as funções de Resets sejam confirmadas através da TAG Mestre (Via Software Acessos ID-3K).

9.5 - Sensor de Violação

Os equipamentos de Controle de Acesso HDL possuem um sistema de antiviolação, como um sistema de proteção para o sistema, caso o aparelho seja aberto durante o funcionamento. Irá soar um sinal de Alerta e o status do LED ficará piscando vermelho.

Nota: Caso o equipamento não tenha uma TAG/ Celular Mestre cadastrado, o sensor de Violação não é ativado. Assim o equipamento permite o cadastro da TAG Mestre sem o disparo da função.

9.6 - Acionamento da Campainha

Para acionar a saída da campainha deve-se manter pressionado o botão de campainha por no mínimo 3 segundo. A configura do tipo de toque (cadência, da saída da campainha) pode ser realizada através do Menu Sistema ->Toque Campainha. Disponível apenas no módulo Teclado.

9.7 - Acionamento por Botoeira

Permite a ativação da saída de fechadura configurada de forma manual. O acionamento da fechadura por Botoeira pode ser desativado por configuração.

Para realizar a abertura através da botoeira realize os passos abaixo:

1. Realize um curto circuito entre os fios “BOT1” e o fio “GND” .

Nota: Para Conexão Vide CONECTOR 2 no Capítulo VII.

9.8 - Sensor de Porta Aberta

A entrada de botoeira também pode ser configurada como entrada para Sensor de Porta Aberta. Neste caso a função botoeira é desativada.

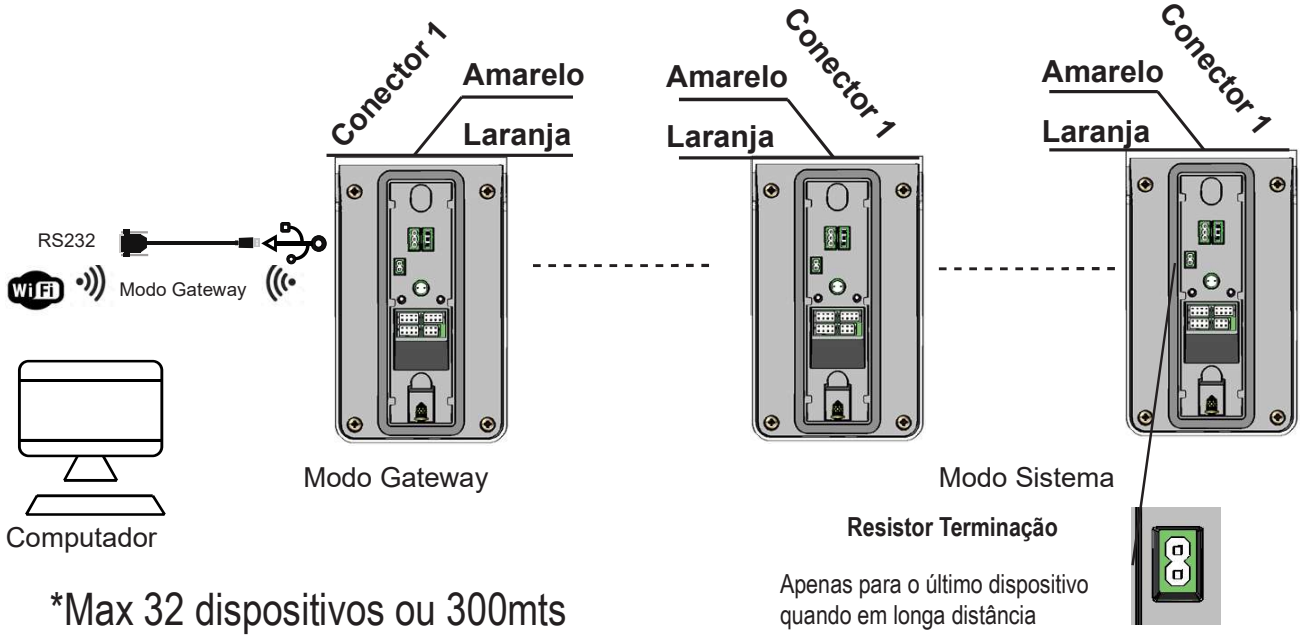
CAPÍTULO X - CONFIGURANDO O MODO DE OPERAÇÃO

A seguir será exibido os modos de operação dos dispositivos, no qual oferecerá ao usuário uma enorme variedade de aplicações, monitoramento e gestão. Para maiores detalhes sobre como configurar, veja o Manual do Software Acessos ID-3K.

10.1 - Modo Sistema e Gateway

O funcionamento dos equipamentos de controle de acesso definidos como Sistema e Gateway (1 unidade) oferece ao usuário a possibilidade de realizar o gerenciamento de todos os dispositivos através do software de comunicação instalado em seu computador. (Sendo o Dispositivo Gateway responsável pela comunicação Software - Dispositivos).

O Modo Sistema se conecta entre os dispositivos através de um barramento RS485, tornando a instalação mais simples e prática, não necessitando de conhecimentos de Rede de Computador. Dessa forma, basta fazer um circuito com fios paralelos conectando os dispositivos a essa rede. (Em longas distâncias pode ser necessario o Resistor de Terminação no último dispositivo.



*Max 32 dispositivos ou 300mts

Na ilustração acima, o dispositivo 01, deve ser configurado como Gateway, permitindo comunicar-se com o Software Acessos ID-3K via Wi-Fi (Cliente ou Ponto de Acesso), e comunica-se com os outros dispositivos da rede através de conexão RS485. Essa funcionalidade só se aplica a equipamentos HDL, dispositivos de outros fabricantes não funcionaram nesse modo.

10.1.1 Criando uma Rede de dispositivos

Para se instalar os dispositivos em rede, utilizando os modos Sistema e Gateway, deve-se primeiramente definir os seguintes parametros nos equipamentos.

1- Definir qual equipamento funcionará como Gateway, esse equipamento será o responsável pela comunicação entre os dispositivos e o computador de gerenciamento através do Wi-fi ou RS232. Para isso utilize um equipamento com fácil acesso físico ou a rede Wireless do local e ao mesmo tempo um equipamento com maior restrição de acesso por usuários.

2- Conecte individualmente os dispositivos ao Software Acessos ID-3K para a sua configuração “inicial” (pode-se utilizar um conversor USB para RS232. (Consulte o Anexo 1 para a conexão).

3- Após Conectar no Software Acessos ID-3K realize as configurações mínimas descritas abaixo em cada um dos dispositivos (Consulte o Manual do Software Acessos ID-3K o Menu de Comunicação)

3.1 Equipamento Gateway:

a) Defina o Modo como gateway

b) Defina o ID como 01 e um nome para o dispositivo

c) Insira as informações do Wifi como SSID (nome da rede) e senha do Wi-fi, conexão de Acess Point ou via RS232.

d) Reinicie o equipamento e verifique no menu Conexões o status da mesma.

3.2 Equipamentos Sistemas:

a) Defina o Modo como SISTEMA

b) Defina o ID como 02~32 e um nome para o dispositivo

d) Reinicie o equipamento

4- Interligue todos os equipamentos conforme exibido no item 10.1, energize os equipamentos;

5- Altere o Modo de Comunicação para Rede no Software Acessos ID-3K,e realize a conexão no dispositivo Gateway, em seguida a busca da rede no Software Acessos ID-3K, o mesmo deve identificar todos os dispositivos a ele conectado.

Nota: 1- Para a conexão RS485, é recomendado a utilização de cabo UTP CAT 5 100% cobre (Máx de 32 dispositivos ou 300 mts);

2- Não deve haver endereços de ID repetidos e os mesmos devem ser seqüênciais, sem intervalos entre eles;

3- Os controles de Acesso HDL podem funcionar como um ponto de Acesso Wifi, dessa maneira é possível conectar o Software Acessos ID-3K aos dispositivo via Wifi, sem a necessidade de um Roteador, consulte o Manual do Software Acessos ID-3K no Site HDL para maiores Informações.

4- Caso a comunicação com o Software Acessos ID-3K esteja lenta ou com frequentes falhas de transmissão, é recomendado a utilização de comunicação via Serial com o Gateway que é a prova de falhas a curtas distâncias.

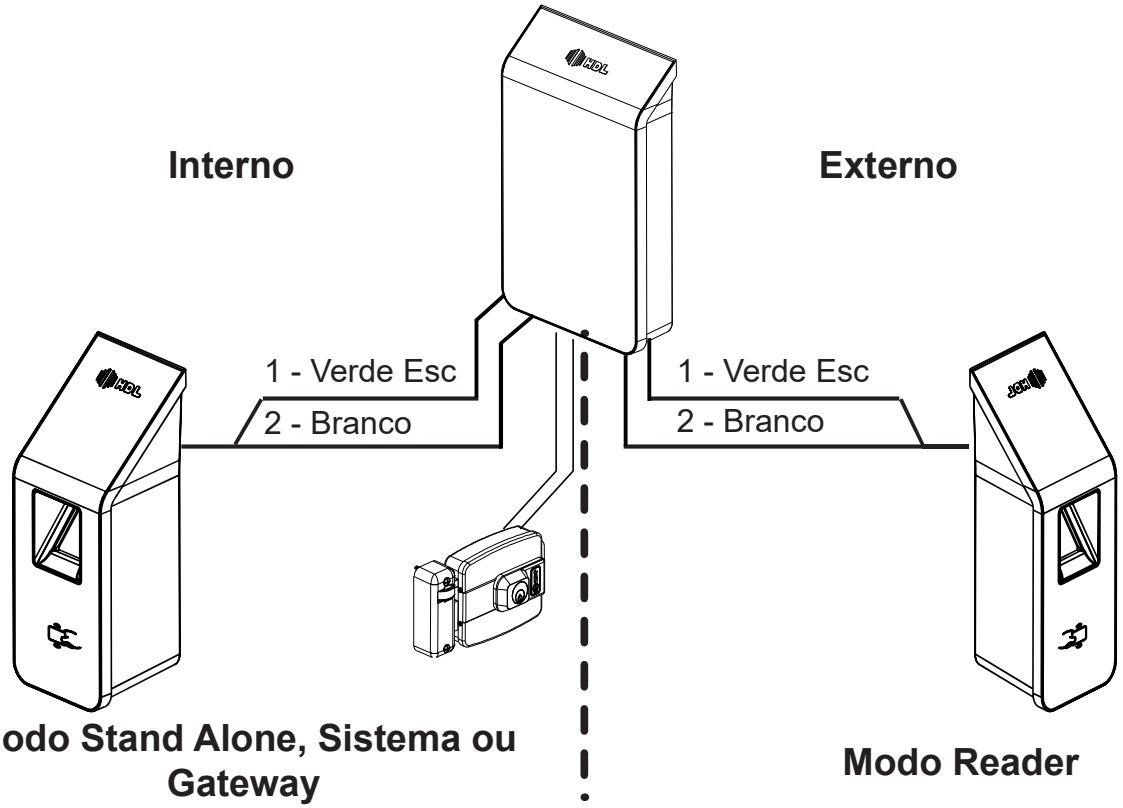
10.2 - Modo Stand Alone

Utilizado para aplicações onde não há necessidade de conectividade ou gestão através de software, sendo este configurado através das credenciais Masters,(TAG, CARTÃO, SENHA, Biometria ou Celular.) Para o dispositivo de Teclado, permite-se realizar algumas configurações via teclado, vide anexo 2 deste manual.

10.3 - Modo Reader

10.3.1 - Função Escravo

Quando em modo Reader, o dispositivo apenas realizará a leitura da TAG, Controle Remoto e Teclas enviando a informação para outros dispositivos realizarem a autenticação e acionamento da porta ou portão. Essa informação é enviada através do protocolo Wiegand. Utilizado para integração do dispositivo a outros sistemas.



10.3.1.1 - Conectando um Dispositivo como Reader ao Módulo de Conexão

O módulo de conexão será o responsável por verificar, validar e dar ação a solicitação (TAG, Controle Remoto) enviada pelo dispositivo Reader.

1- Conecte aos dispositivos pelo Software Acessos ID-3K utilizando conexão RS232 (pode-se utilizar um conversor USB para RS232. (Consulte o Anexo 1 para a conexão).

2- Após Conectar no Software Acessos ID-3K é necessários realizar configurações em cada dispositivos, (Consulte o Manual do Software Acessos ID-3K o Menu de Comunicação)

2.1 Equipamento Reader:

a) Defina o Modo como Reader

b) Reinicie o equipamento

3- Interligue os equipamentos conforme exibido no item 10.3, energize os equipamentos.

10.3.2 - Função Cadastrador de Mesa

O dispositivo quando selecionado para operar no modo Reader, o mesmo pode ser utilizado para a realização do cadastro do usuário (Biometria / Cartão ou TAG).

2.1 Equipamento Reader:

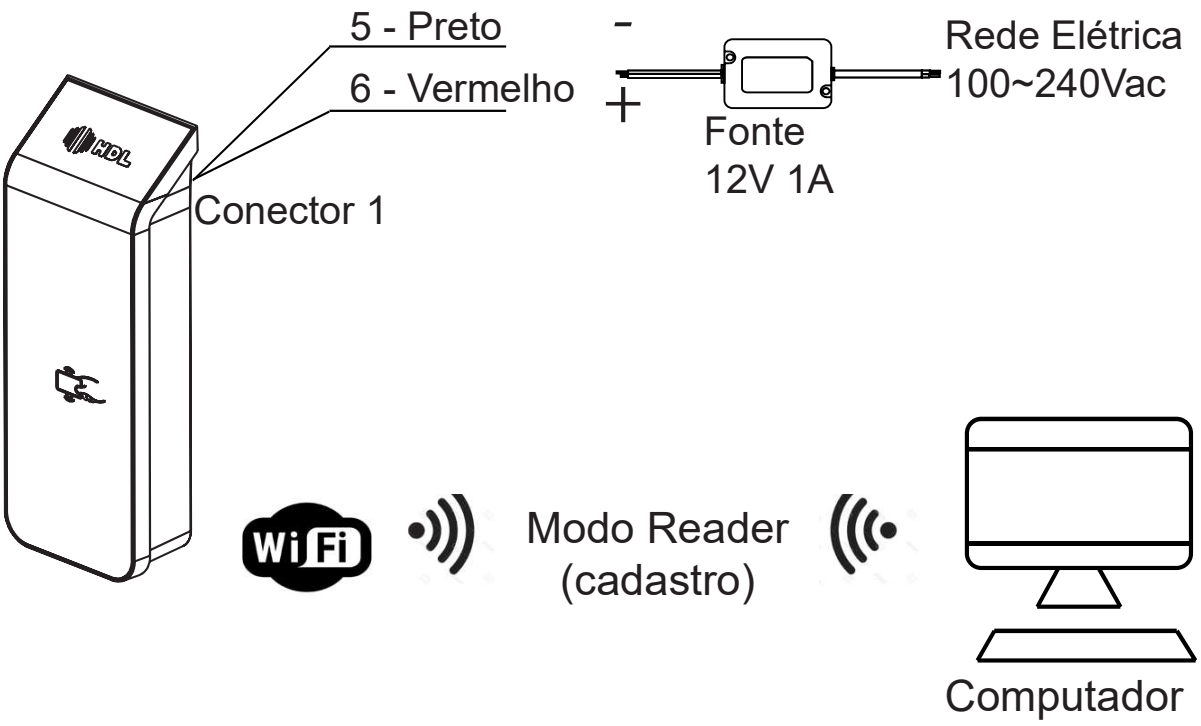
a) Defina o Modo como Reader

b) Reinicie o equipamento

c) Rede Wifi do dispositivo,

d) Na tela de cadastro do usuário, pressione o botão ATIVAR READER para realizar a leitura do CARTÃO, BIOMETRIA ou SENHA.

Essa configuração pode ser realizada através do APP. Veja no Capítulo XIV.



NOTA: Todos os dispositivos da linha controle de acesso podem ser utilizados como Reader. (Exceto o Módulo de Conexões)

O Reader deve estar configurado no mesmo WiFi do Gateway.

CAPÍTULO XI - PROGRAMAÇÕES NO DISPOSITIVO

11.1 - Cadastrar uma TAG Mestre ou Controle Remoto Mestre

Permite que o Administrador do Sistema Cadastre uma TAG Mestre ou Controle Remoto Mestre (Veicular).

1- Pressione o Botão **SERV** por 3 Segundos.
2- O dispositivo gera um bip auxiliar a cada segundo que o botão esteja pressionado.
3- Ao soltar o Botão **SERV** após 3 segundos, serão emitidos **5 bips** de indicação do modo de programação e o LED de status ficará Amarelo.
4- Passe a TAG no local indicado ou pressione o botão do Controle Remoto para a captura. Em seguida soará **3 Bips** de confirmação.
5- Aproxime novamente a TAG/Controle Mestre para sair do menu de programação ou aguardar 30 segundos para que o dispositivo retorne ao estado normal de operação (LED azul).

11.2 - Cadastrar lote de TAGs, Controles Remotos

Permite o cadastrar um lote de TAGs/ Controles Remotos para o acesso.

1- O Administrador. irá passar o TAG MESTRE/ pressionar o botão do CONTROLE REMOTO MESTRE. O dispositivo irá emitir **5 bips curtos** e o LED de status ficará em amarelo (Modo de Programação- Operação de Cadastro).
2- O Usuário irá passar a TAG /pressionar o botão do controle remoto a ser cadastrado. Serão emitidos **3 bips curtos** (confirmação).
3- Após a confirmação pode-se passar para o próximo cadastro de forma seqüêncial.
4- Para sair do modo de cadastro pode-se passar a TAG Mestre novamente ou aguardar 30 segundos para que o dispositivo retorne ao estado normal de operação (LED azul).

Nota: O cadastro em Lote não esta disponível para o cadastro de biometria, o cadastro será realizado de até 3 biometrias por usuário, sendo a 3ª biometria cadastrada definido como PÂNICO. Ao cadastrar as 3 biometrias, poderá relacionar as biometrias a um usuário ja existente aproximando o cartão, TAG ou celular ja cadastrado ou saia do modo de programação aproximando a TAG Mestre ou aguarde 30 segundos.

11.3 - Cadastrar Acesso por Senha (Teclado) - Simplificado

Permite que o administrador do sistema cadastre senhas de usuários para acesso.

1- O Administrador. irá passar o TAG MESTRE. Serão emitidos **5 bips curtos** e o LED de status ficará em Amarelo (Modo de Programação).

2- O Usuário irá digitar a senha de acesso com 4 dígitos (modo simplificado) a ser cadastrada seguida da tecla  .

3- Serão emitidos **3 bips curtos** de confirmação.

4- Para finalizar o cadastro pode-se passar a TAG Mestre novamente, ou aguardar 30 segundos para que o dispositivo retorne ao estado normal de operação (LED azul).

Nota: No modo **SIMPLIFICADO** é permitido à diferentes usuários possuírem a mesma senha de acesso, dessa forma impossibilitando a identificação no Software Acessos ID-3K. Utilize essa função apenas quando não houver uma gestão continua dos acessos.

Quando houver a necessidade da gestão recomenda-se desativar o modo simplificado através do Software Acessos ID-3K, consulte o manual do Software para mais detalhes.

O Modo Apt/ID + Senha, permite ao Gestor identificar os horários e locais que um determinado usuário realizou o acesso. Neste modo o sistema não permite o cadastro de dois ou mais usuários com o mesmo conjunto ID + Senha, logo, o usuário após um acesso pode ser identificado.

No dispositivo, com teclado, é possível realizar algumas configurações através de códigos utilizando o teclado numérico. Veja no Anexo 1 a tabela de programação via códigos.

OBS: Caso o cadastro seja realizado com Apt/ID + SENHA, em uma segunda entrada de cadastro, o usuário será reconhecido e o sistema entra em modo de UPDATE de registro.

11.4 - Dígito Falso

Nesta configuração,durante um acesso por senha(Teclado), antes da senha de acesso o usuário necessita digitar a quantidade de dígitos falsos configurados. Este recurso solicita ao usuário a digitação de 1 a 9 dígitos numéricos falsos, de acordo com a configuração realizada pelo administrador do sistema, antes da digitação da senha de acesso.

Os dígitos falsos são dígitos numéricos que serão ignorados pelo sistema de controle de acesso durante o acesso por senha. Estes dígitos tem a função de aumentar a segurança durante o acesso por senha ou ID + senha evitando que observadores identifiquem a senha de acesso do usuário.

Por padrão, a configuração de dígitos falsos é desativada, e realizada através do Software Acessos ID-3K

Nota: O cadastro do usuário pode conter Apt/ID + Senha e o modo de acesso ser configurado em MODO SIMPLIFICADO OU MODO ID + SENHA

11.5 - Apagando um usuário cadastrado

Permite que o Administrador do Sistema Apague um cadastro existente via terminal.

1- Aproxime o Cartão MASTER já cadastrado.
2- Aproxime novamente o cartão MASTER
3- O LED amarelo do status de programação ira piscar.
4- Aproxime o Cartão/Tag ou posicione a biometria ou pressione o controle remoto ou Celular para para excluir o registro do usuário cadastrado..

Nota: No Controle de acesso por teclado, quando utilizado no modo simplificado caso haja mais de um usuário com a mesma senha, todos os usuários perderão o acesso,

Quando no modo avançado, insira o Apt/ID+SENHA do usuário para descadastro.

11.6 - Atualizar cadastro com TAG cadastrada

Permite ao Administrador adicionar diretamente no controle de acesso outra forma de autenticação (associadas ao dispositivo já cadastrados).

1- Aproxime o cartão MASTER já cadastrado.
2- Insira Biometria/Senha/Celular (é permitido até 3 biometrias, sendo a ultima com a função de Pânico) vinculado ao mesmo usuário.
3- Aproxime uma TAG/Celular/Biometria cadastrada anteriormente.
4- Led de status começa a piscar verde entre a cor Amarela
5- Aproxime a TAG MASTER ou aguarde para sair do menu de programação.

Nota:
1- Para o controle de acesso por teclado, é possível programa-lo através das teclas, veja o Anexo 1 para os códigos de programação.
2- É recomendado sempre inserir a biometria cadastrada primeiramente, sempre

que já houver para que o registro do usuário seja identificado.

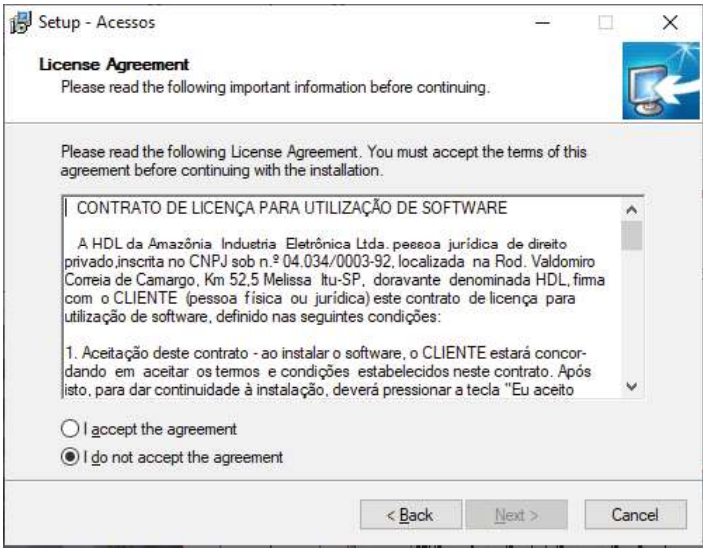
3- A biometria de Pânico funciona de forma a liberar o acesso normalmente, mais gerando um Evento de Pânico para o Software Acessos ou PSIM

CAPÍTULO XII - INSTALANDO O SOFTWARE ACESSO

Com um duplo clique no arquivo .exe a instalação será iniciada, veja a seguir o passo a passo:

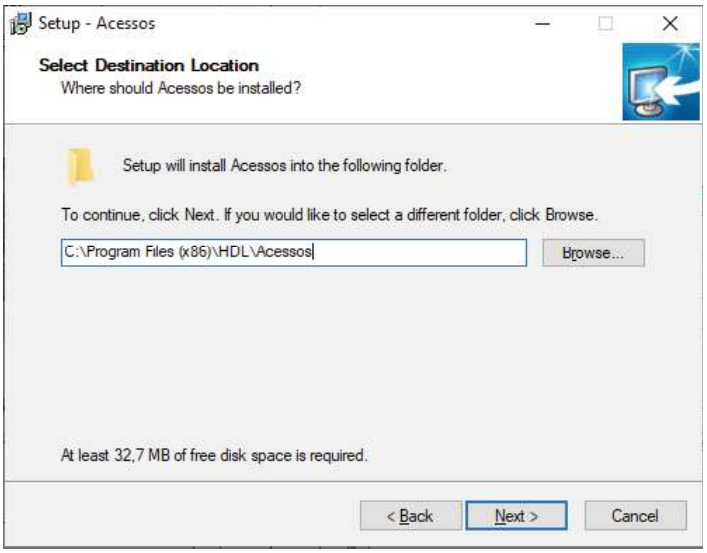
1) Clique em Next para iniciar a instalação.

2) Leia o contrato de licença de utilização do software e selecione a opção " I Accept the agreement" e clique em Next.

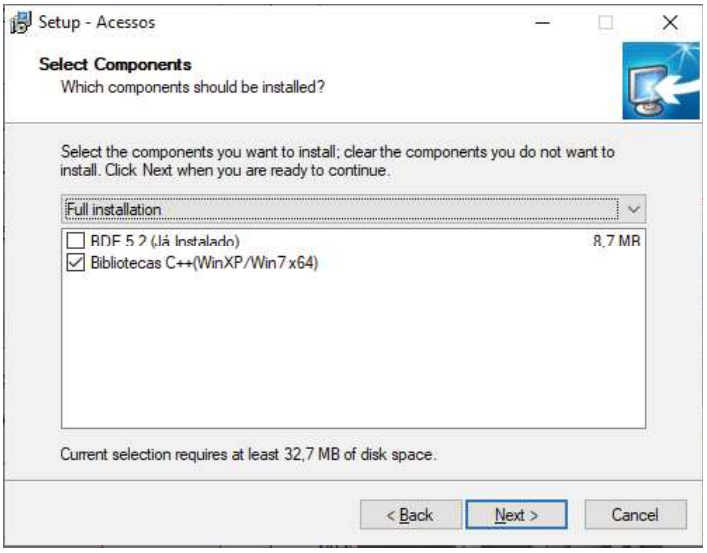


3) Selecione a pasta de destino da instalação do Software Acessos ID-3K e clique em Next.

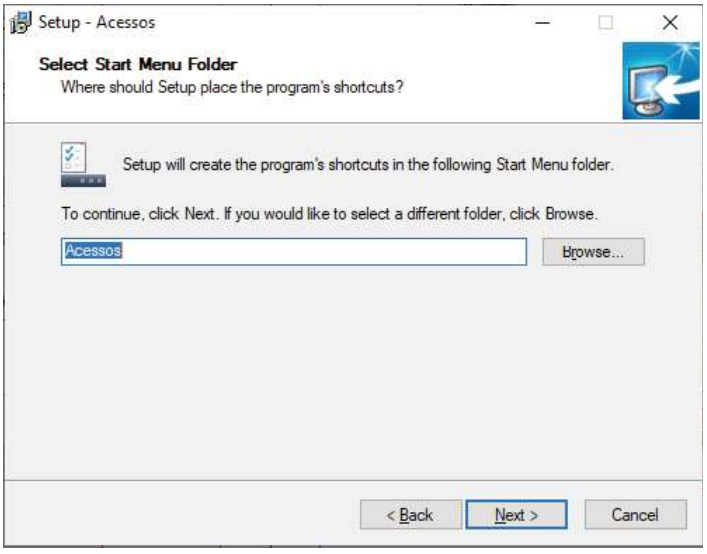
Pasta padrão de instalação: C:\Program Files (x86)\HDL\Acessos



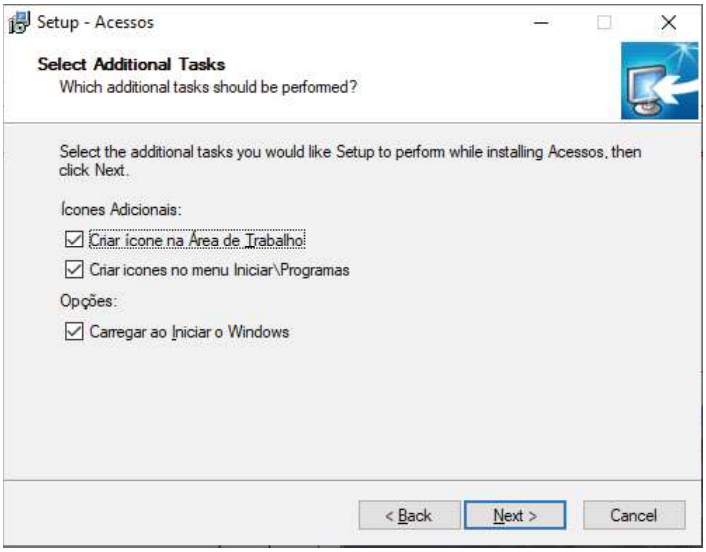
4) Selecione os componentes a serem instalados. Em uma instalação nova, selecione a opção “Full Instalation”e clique em Next.



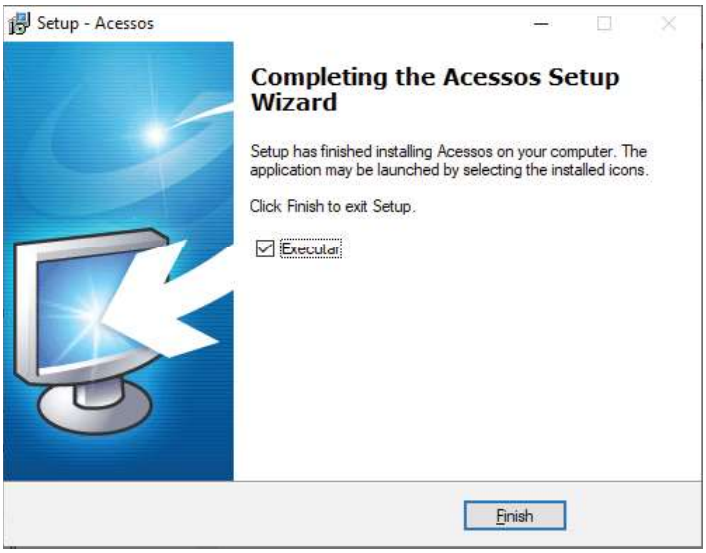
5) Caso desejado pode-se alterar o nome da pasta criada no menu iniciar,. A pasta padrão é “ ACESSOS”.



6) Selecione os atalhos desejados e clique em Next.



7) Veja o resumo das opções selecionadas e clique em INSTALL para iniciar a instalação do Software Acessos ID-3K, aguarde até ser concluído, a seguinte tela será exibida.



Clique em FINISH para iniciar o Software Acessos ID-3K

12.1 - Funções via software Acessos ID-3K

Algumas funções presentes nos equipamentos só são acessíveis para configuração através do Software Acessos ID-3K.

12.1.1 - Controle de Turnos

Se pode controlar o acesso a um local mediante o dia e faixa de horários.
Então pode-se bloquear o acesso de um prestador de serviço, exemplo zelador,

nos fins de semana

12.1.2 - Controle de Zonas

Com as Zonas se pode determinar quem tem permissão de acesso a uma determinado local controlado. Por exemplo, uma sala de academia, depósito ou sala de jogos, que não pode entrar crianças ou pessoas não autorizadas.

No registro do usuário, pertencente a criança, não se dá permissão as zonas x,y,z.

12.1.3 - Expiração do Usuário

Permite criar um período de validade da credencial de um visitante, se auto excluindo dos dispositivos após período de validade expirado..

12.1.4 - Modo da Botoeira

Definir o modo de operação da botoeira Ativada ou Desativada.

12.1.5 - Sensor de Porta Aberta

Habilitado após a botoeira for selecionada como Desativada, permitindo configurar como sensor de porta aberta.

12.1.6 - Tempos de Acionamento das Saídas

Permite determinar o tempo de acionamento das fechaduras, de acordo com a necessidade do local

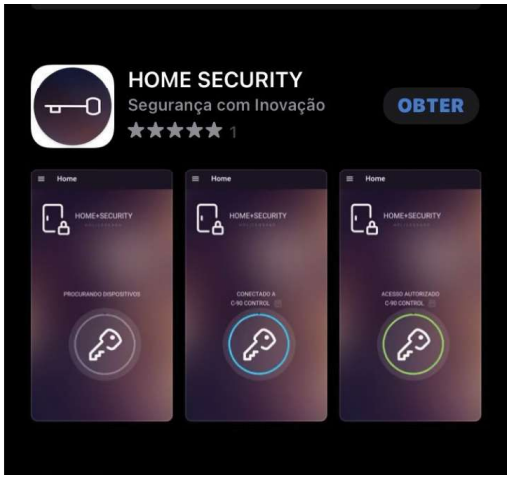
12.1.7 - Modos de Acionamento das Saídas

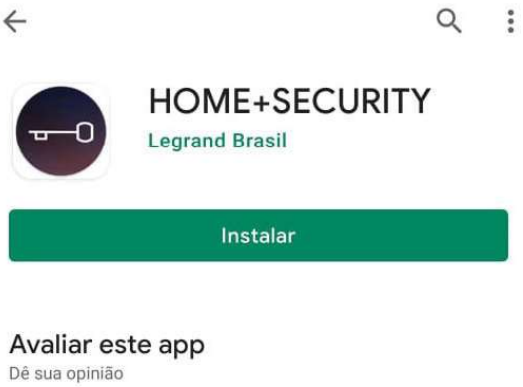
Permite determinar a forma de acionamento, continuo, pulsado, pulso unico.

Nota: para maiores detalhes consulte o Manual do Software Acessos disponível em nosso site, http://www.hdl.com.br

CAPITULO XIII - INSTALANDO O APP

Em sua loja de aplicativos busque o aplicativo HOME+SECURITY e clique em OBTER ou INSTALAR, aguarde o download, a instalação deve ocorrer de forma automática.





Clique no ícone  para iniciar o aplicativo, siga os procedimentos do tutorial para os primeiros passos com o APP.

Nota: Para que o APP funcione corretamente os serviços de BLUETOOTH E LOCALIZAÇÃO do celular devem estar ativos.

CAPÍTULO XIV - PROGRAMAÇÕES ATRAVÉS DO APP

14.1 - Cadastrar um Celular como Mestre

É permitido ao administrador habilitar o celular como Mestre para que possa ser utilizado para configurações locais dos equipamentos de controle de acesso.

Para isso é necessário no primeiro momento que realize o processo similar ao cadastro dos outros modos mestres.

1 - Pressione o botão SERV por 3 seg, irá soar 5 bips de confirmação e o LED de status ficará amarelo.

2 - Com o Aplicativo Home + Security aberto, abra a lista de opções no canto superior esquedo.

3 - Clique em Configurações

4 - Clique em MODO MESTRE

5 - Siga as instruções na Tela.

14.2 - Cadastrar um Celular

O cadastro de Celular para acesso, é permitido através de credenciais Mestre (TAGs, Controle Remoto, Senha ou Celular)

15.2.1 Utilizando TAG, Controle Remoto, Senha

1 - Acesse o modo cadastro utilizando o dispositivo Mestre.

2 - Com o Aplicativo aberto, pressione o botão de abertura para captura do ID

3 - Saia do menu aproximando novamente o dispositivo Mestre ou aguarde 30 segundos para que o dispositivo saia do menu automaticamente.

14.2.2 - Cadastro de usuário através do Celular Mestre

1 - Acesse o modo cadastro utilizando o celular Mestre através do Menu Configurações, Modo Mestre, Ativar Modo Cadastro.

2 - Com o Aplicativo aberto, pressione o botão de abertura para captura do ID ou insira a senha de acesso, biometria ou aproxime a TAG/Cartão de Acesso para cadastro.

3 - No Dispositivo Mestre finalize o cadastro entrando em Menu Configurações, Modo Mestre, Finalizar Operação ou aguarde 30 segundos.

Nota: É possível utilizar um Celular Mestre como Usuário.

14.3 - Funções

As funções no aplicativo, oferece ao administrador a possibilidade de configurar todos os equipamentos nos modos de utilização já vistos nesse manual. Sendo assim possível configurar um projeto simples com 1 ou dois dispositivos assim como um sistema complexo de controle de acesso.

14.3.1 - Definindo modo de Operação

Defina o modo de Operação do equipamento:

1 - Reader

2 - Stand Alone

3 - Sistema

4 - Gateway

14.3.2 - Nome do Dispositivo

Defina um nome para o dispositivo, facilitando assim a identificação do mesmo pelos usuários de aplicativo ou através do Software Acessos ID-3K..

14.3.3 - ID do Dispositivo

Defina o ID do dispositivo, esse ID é utilizado quando operando no modo Rede, onde tem-se 1 dispositivo configurado como Gateway (ID 01) e Sistemas (2~32)

14.3.4 - Configurando o Wi-Fi

Quando em modo Gateway, é possível ativar a função Wifi do controle de acesso. Dessa forma, a comunicação dos dispositivos e do Software Acessos ID-3K se dá através do Wifi, tornando o sistema mais escalonável e prático.

14.3.5 - Registros

Permite ao usuário o acesso aos registros de uso do aplicativo, informando os ultimos registros de atividade

14.3.6 - Modo Mestre

Permite cadastrar o celular como dispositivo Mestre, dessa forma, sendo possível cadastrar outros celulares, TAGs, Biometria ou Controles Remotos através do celular.

CAPÍTULO XV - REALIZANDO ACESSO

15.1 - Acesso por TAG/ Controle Remoto

A funcionalidade de acesso por TAG/ Controle Remoto permite que um usuário cadastrado no sistema, após a apresentação da credencial (TAG) ao leitor realize a abertura da fechadura mediante sua validação.

Para abrir a fechadura:

1- Aproxime a TAG () no Painel do controle de acesso ou pressione o botão de Controle Remoto (Módulo de Conexões)

2- Caso a TAG seja cadastrada ocorrerá o retorno sonoro de aprovação da credencial com 3 bips curtos, o LED de status ficará na cor verde e a abertura da fechadura ocorrerá.

3- Caso a TAG não seja cadastrada ocorrerá o retorno sonoro de rejeição da credencial com 1 bip longo e LED de status na cor vermelha

15.2 - Acesso por Senha (Teclado)

O acesso por senha permite que um usuário mediante a apresentação de sua senha, quando em modo simplificado, ou código de usuário + senha, quando em modo normal, possa acionar a fechadura.

Como acessar:

1- O usuário deve se aproximar do produto pressionar a tecla “  ” seguida da senha de acesso cadastradas, quando em modo simplificado, ou Apto/ID + senha, quando em modo normal.

2- Caso a validação seja positiva ocorrerá o retorno sonoro de aprovação da credencial com **3 bips curtos** e o LED de status ficará na cor verde. Ocorrerá a a abertura da fechadura.

3- Caso a validação seja negativa ocorrerá o retorno sonoro de rejeição da credencial. Será gerado **1 bip longo** e o LED de status mudará para a cor vermelha.

15.3 - Acesso por Biometria

Permite que o usuário realize um acesso através de sua biometria cadastrada.

Como acessar:

1- O usuário deve se aproximar do dispositivo e deve pressionar o dedo contra a leitora.

2- Caso a validação seja positiva ocorrerá o retorno sonoro de aprovação da credencial com **3 bips curtos** e o LED de status ficará na cor verde. Ocorrerá a a abertura da fechadura.

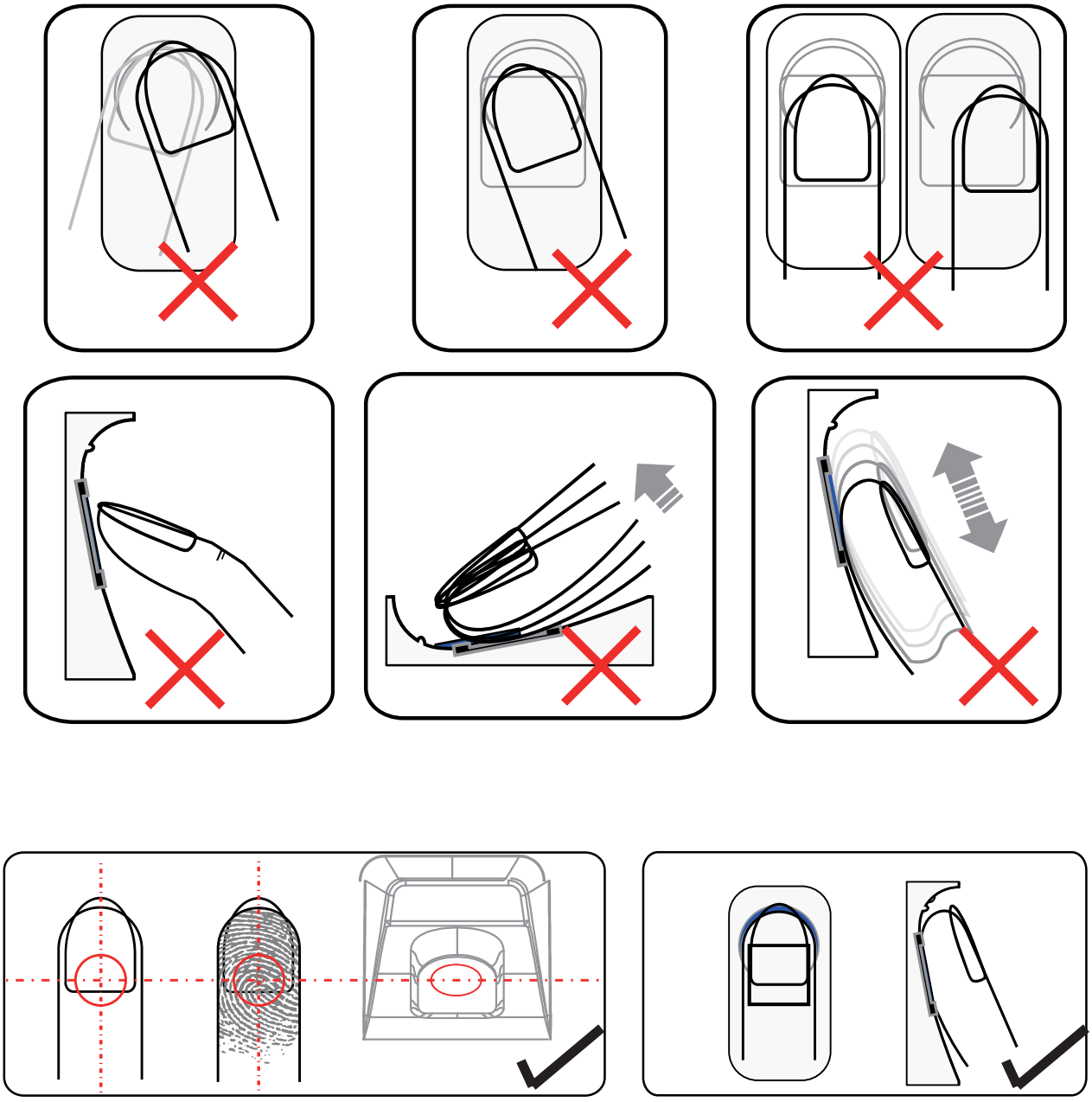
3- Caso a validação seja negativa ocorrerá o retorno sonoro de rejeição da credencial. Será gerado **1 bip longo** e o LED de status mudará para a cor vermelha.

Nota:

1- Caso o dedo seja posicionado sem pressionamento pode não ocorrer a leitura ou invalidar a credencial.

2- Dedos muito pequenos, como o de crianças de menos de 4 anos, podem não ser detectados caso não consigam preencher o leitor ou pressionar corretamente.

3- Dedos com sujeita/cicatrizes ou desgaste nas digitais como idosos e trabalhadores manuais também podem ter dificuldades no cadastro de digitais. Deve nestes casos cadastrar 2 digitais e pressionar o dedo com mais força no cadastro.



15.4 - Acesso por Aplicativo Móvel (APP)

Com o Aplicativo já instalado e configurado, ative o bluetooth e a localização, o controle de acesso mais próximo deve ser identificado e exibido o nome na tela do celular.

1 - Pressione o botão “CHAVE” por 1 segundo para acionar o dispositivo.

2- Caso a validação seja positiva ocorrerá o retorno sonoro de aprovação da credencial com 3 bips curtos e o LED de status ficará na cor verde. Ocorrerá a abertura da fechadura.

3- Caso a validação seja negativa ocorrerá o retorno sonoro de rejeição da credencial.

Será gerado 1 bip longo e o LED de status mudará para a cor vermelha.

Para o acesso via smartphone, realize o download gratuitamente do aplicativo “HOME + SECURITY” em sua loja de aplicativos Google Play ou Apple Store.

Nota: para o cadastro do celular com o dispositivo, deve-se ter uma distância de aproximadamente 30cm.

15.5 - Autenticação

15.5.1 - Dois Fatores

Através do Software Acessos Acessos ID-3K, é possível ativar a autenticação de dois fatores, sendo assim necessário a confirmação de dois modos de autenticidade do usuário
(SENHA + CARTÂO, BIOMETRIA + CARTÂO, CARTÂO + CELULAR)

Para realizar o acesso, faça a autenticação de modo sequencial, não havendo uma seqüência exata (BIOMETRIA + CARTÃO ou CARTÃO + BIOMETRIA).

Nota: Para usuários com 3 formas de autenticação, apenas duas autenticações será o suficiente para liberação e abertura da porta.

Se o dispositivo Teclado estiver com o modo Simplificado utilize (SENHA + TAG) se no modo Avançado ((ID+SENHA)+ TAG).

Se os dígitos falsos ativos, Dígitos Falsos + SENHA ou DF + ID + SENHA e na sequencia a próxima credencial .

15.5.2 - Simples

Por padrão todos os dispositivos estão configurados para o modo de autenticação simples, ou seja, apenas uma das formas de autenticação validada (TAG / Senha / Biometria / Celular / Controle Remoto) é o suficiente para que o usuário possua acesso.

ANEXO I

Categoria	Programação de Fábrica			
Sistema	Modo de Operação			Standalone
	Endereço Dispositivo			0
	Zona do Dispositivo			Nenhuma
	MASTER		TAG 1	Nenhuma
			TAG 2	Nenhuma
			Controle RF433 1	Nenhuma
			Controle RF433 2	Nenhuma
			Mobile 1	Nenhuma
			Mobile 2	Nenhuma
	Acesso	Modo de Autenticação		Autenticação Simples
		Teclado	Modo Simplificado	Ativado
			Dígitos falsos	Desativado
	Biometria		Modo Biometria (LUZ de detecção)	Desativado (Auto)
	Teclado		Tipo de Toque Externo Campainha	6 - Toque Triplo
			Senha de Programação	1234
Conectividade	WiFi		Modo	Desativado
			SSID	Nenhum
			Password	Nenhum
			DHCP	Ativo
			IP	192.168.0.160
			Máscara de Rede	255.255.255.0
			IP Gateway	192.168.0.1
			DNS	8.8.8.8
	Portas		UDP	15377
			Log	514
			HTTP	8080
	Integração		Chave API	Nenhum
			IP Server	0.0.0.0
			Porta TCP	8080
			Token	Nenhum
			Conta	Nenhum
			Zona	Nenhum

Wiegand	Protocolo		Wiegand 26/34 bits
Sensor de Porta	Tipo Sensor		Desativado
	Tempo de Retardo		10 segundos
Botoeira	Modo Botoeira		Ativado
Fechadura 1	Modo de acionamento		Modo Pulsado
	Tempo de Acionamento		0,5 segundos
	Tempo pulso ON		02 ms
	Tempo pulso OFF		06 ms
Fechadura 2	Modo de Acionamento		Pulso Único
	Tempo de Acionamento		2s
	Tempo Pulso ON		-
	Tempo Pulso Off		-
Terminal de Conexões	Modo Acionamento Veicular		Independente simples
	Padrão Wiegand - Leitura		26/34 bits
	Padrão Wiegand - Envio		26 ou 34 bits
	Grupo 1	Botoeira 1	Ativada Saída 1
		Modo de Acionamento	Pulso Único
		Tempo de Acionamento	2 segundos
		Sensor 1	Desativado
		Temporarização	5 segundos
	Grupo 2	Botoeira 2	Desativada
		Modo de Acionamento	Pulso Único
		Tempo de Acionamento	2 segundos
		Sensor 2	Desativado
		Temporização	5 segundos
Permissões	Turnos		Desativado
	Zonas		Desativado

ANEXO II

Menu	Código Programação	Opção	Parâmetro	Dados	Descrição
Sistema	0	0	-	*	Reset Geral
		2	-	M + *	Acesso modo simplificado (somente por senha) M=0 (desativado) /1 (Ativado)
		4	-	D + *	Acesso com Digitos Falsos D=0 (Desativado) /1~9 (Qtd de dígitos)
		5	-	M + *	Tons de Teclado M = 0 (Desativado) /1 (Ativado)
		7	-	SSSS + * (3Bips)	Senha de Programação
Cadastro	5	0	-	TAG ou (Apt + *) (3Bips)	Exclui TAG/Apt
		1	-	Apt + * (opcional) + TAG(3Bips)	Cadastro TAG
		2	-	Apt + SSSS + * (3Bips)	Exclui Apt + Senha +TAG (Específico)
		3	-	TAG + TAG + ... + * (3Bips)	Cadastro TAG seriada
		4	-	Apt + SSSS + * (3Bips)	Cadastro APT + Senha
		5	-	Apt + Senha + * (3Bips) TAG(3Bips)	Cadastro APT + Senha + TAG
		6	-	OP + Tabela1 + TAG ou (Apt + *) (3Bips)	Altera turno por TAG OP=0 Desativado / 1(Ativado)
		8	-	TAG (3Bips)	Cadastro TAG Mestre
		9	-	*	Exclui todos os Registros

Fechadura/ Botoeira	6	0	-	Modo + * 0- Desativada / 1- Ativada (Fech 1)	Modo Botoeira
		Fecho 1 ou 2	1	[0....4] + *	Modo de Acionamento
			2	[0....99] + * (2 digitos)	Tempo de Acionamento
			3	[1....99] + * (2 digitos)	Tempo Pulso ON
			4	[1....99] + * (2 digitos)	Tempo Pulso Off
Turnos	7	1	-	1 -ON / 0 - OFF + *	Modo Permissôes (Turnos)
		2	-	T + S + HHi + MMi + HHf + MMf + *	Configura Turno
		3	-	T + S + *	Apaga Turno
		4	-	T + *	Apaga todos Turnos

Ajustes de turnos

1	2	3	4	5	6	7
Dom	Seg	Ter	Qua	Qui	Sex	Sab

CAPÍTULO XVI - CERTIFICADO DE GARANTIA

Esse produto passou por todos os testes de resistência exigidos pelo nosso Controle de Qualidade e encontra-se apto para servi-lo durante muitos anos.

A HDL DA AMAZÔNIA INDÚSTRIA ELETRÔNICA LTDA. assegura ao adquirente deste equipamento, garantia contra defeitos de matéria-prima e de fabricação, por 01 (um) ano, a contar da data de sua aquisição, comprovada mediante apresentação da respectiva Nota Fiscal do revendedor ao consumidor, observando o que segue:

• A garantia acima supra é a única garantia quer expressa, quer implícita, ficando excluídos quaisquer danos ou prejuízos indiretos, tais como (de forma meramente explicativa e não taxativa) lucros cessantes, interrupção de negócios e outros prejuízos pecuniários decorrentes de uso, ou da possibilidade de usar esse aparelho.

• A HDL declara a garantia nula e sem efeito se for constatado por ela, ou pela Assistência Técnica Credenciada que o equipamento sofreu dano causado por uso em desacordo com o manual de instruções, ligação à tensão de rede errada, acidentes (quedas, batidas, etc.), má utilização, instalação inadequada, defeitos decorrentes de influências climáticas (raios, inundações, etc.), sobrecargas na rede elétrica, danos ou prejuízos causados por furto ou vandalismo, e ainda sinais de haver sido violado, ajustado ou consertado por terceiros não autorizados.

• Equipamentos com número de série adulterado ou ilegível também não serão cobertos pela presente garantia.

• Os danos ou defeitos causados por agentes externos e demais peças que se desgastam naturalmente com o uso, ou por outras condições anormais de utilização, em hipótese alguma serão de responsabilidade do fabricante.

• Todos os equipamentos fabricados pela HDL possuem um selo de garantia que não poderá ser violado. A não observância deste item acarretará na perda da garantia do equipamento.

• Os consertos e manutenção do equipamento, dentro da garantia, serão de competência exclusiva da rede de Assistência Técnica Credenciada pela HDL.

• A Garantia somente terá validade quando o equipamento for apresentado juntamente com a Nota Fiscal de venda ao consumidor.

• As despesas do frete não estão cobertas por esta garantia, sendo de responsabilidade exclusiva do proprietário.

• O proprietário que desejar atendimento domiciliar deverá consultar antecipadamente a rede de Assistência Técnica Credenciada sobre a disponibilidade deste serviço e a taxa de visita cobrada.

Recomendamos que a instalação do equipamento seja efetuada por um profissional qualificado.

Para obter informações referentes à nossa rede de Assistência Técnica Credenciada, entre em contato com um dos nossos atendentes pelo telefone 0800 11 8008 ou acesse nosso site: www.hdl.com.br.

90.02.25.001
90.02.25.003

ANATEL

Agência Nacional de Telecomunicações

05446-20-01968

Resolução 680/2017: " Este equipamento não tem direito à proteção contra interferência prejudicial e não pode causar interferência em sistemas devidamente autorizados"

90.02.25.002

ANATEL

Agência Nacional de Telecomunicações

05447-20-01968

Resolução 680/2017: " Este equipamento não tem direito à proteção contra interferência prejudicial e não pode causar interferência em sistemas devidamente autorizados"

90.02.26.000

ANATEL

Agência Nacional de Telecomunicações

05445-20-01968

Resolução 680/2017: " Este equipamento não tem direito à proteção contra interferência prejudicial e não pode causar interferência em sistemas devidamente autorizados"

"Este equipamento carrega internamente o módulo Modelo ESP32-S código de homologado sob n° 04262-20-10018"

LE12706AA_R1- 12/2020

PRODUZIDO NO PÓLO INDUSTRIAL DE MANAUS

CONHEÇA A AMAZÔNIA

HDL da Amazônia Indústria Eletrônica Ltda.
Avenida Abiurana, 1.150 - Distrito Industrial
Manaus - AM - Cep 69075-010
Tel: 0800 11 8008
CNPJ: 04.034.304/0001-20
e-mail: sac@legrand.com.br
http://www.hdl.com.br