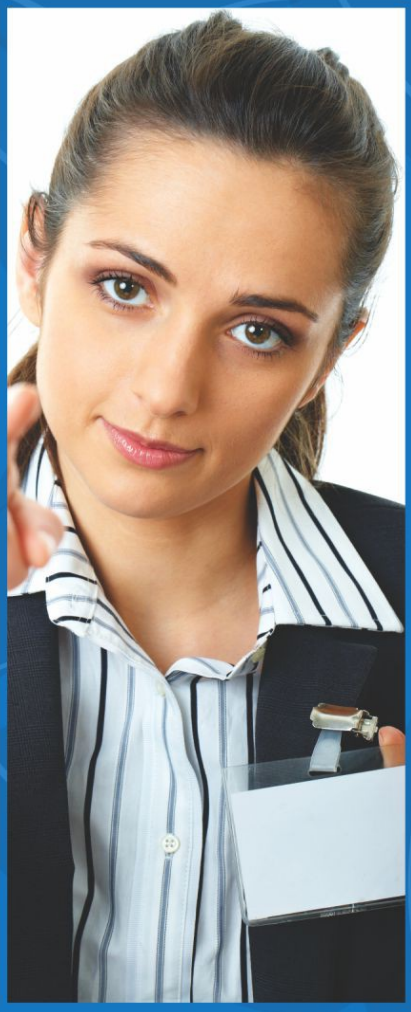
Zig LOCK TCP

Manual de Instalação e Operação



Um produto desenvolvido e fabricado por: Enterplak Produtos Eletrônicos Ltda - CNPJ: 07.013.491/0001-54

Sob licença de

RWTECH

RW Tecnologia Indústria e Comércio Ltda
Centro Empresarial Paulo F. de Toledo, 80
Santa Rita do Sapucaí - MG - CEP: 37540-000
Tel: 35 3471-3172

www.rwtech.com.br

Índice

Antes de Começar

Sr. Usuário:

- Leia atentamente este manual e siga corretamente as instruções de instalação e operação. Assim você estará assegurado de que seu equipamento operará em suas melhores condições de uso.
- Em caso de instalação do equipamento sem as precauções citadas, qualquer troca de peças e manutenção será cobrada.
- A ligação do aparelho à rede elétrica (110/220V) e aos acionamentos externos deve ser efetuada conforme este manual. A ligação errada da rede elétrica ou das demais conexões podem causar danos ao aparelho, não assegurados pela garantia.
- Solicite a instalação a um profissional habilitado.

Antes de instalar seu equipamento, tome as seguintes precauções:

- Verifique se o local é adequado, se o ambiente é coberto, protegido contra água, sol, poeira e outros que podem danificar seu equipamento, pois este equipamento não é adequado para instalação em ambientes externos.
- Evite instalá-lo em ambientes nos quais os usuários possuam, por algum motivo, dedos sujos ou com digitais prejudicadas por produtos químicos, dentre outros.

Observações	*Há um número reduzido de pessoas que não possui digitais com qualidade suficiente para identificação (digitais muito úmidas ou secas, desgastadas, etc.). Assim, para esses casos, o produto oferece a identificação através de cartão de proximidade ou teclado (digitação de matrícula e senha) para o controle de acesso desses usuários.* *Qualquer sistema de identificação biométrica possui taxas de erros FRR (falsa rejeição) e FRA (falso aceite), que devem ser consideradas na aplicação final do produto.*

ATENÇÃO	*Este documento pode conter imprecisões técnicas ou erros tipográficos.* *A RW Tecnologia reserva-se o direito de fazer aprimoramentos e/ou alterações no produto aqui descrito a qualquer momento sem aviso prévio.*

Especificações Técnicas

PEÇAS	ESPECIFICAÇÕES
Processador	ARM7TDMI-S 72MHz
Memória de Sistema	Cartão SD
Display	Alfanumérico de LCD (2 linhas x 16 colunas)
Identificação	1. Matrícula e senha numéricas
	2. Cartão de proximidade RFID 125kHz
	3. Leitura biométrica por digital (modelos BIOCARDs)
Comunicação	Protocolo TCP/IP via *Ethernet* de 100Mbps
Teclado	Numérico com funções de navegação
Portas e Conectores	1 conector USB 2.0
	1 conector contendo*: • 1 saída para acionamento de fechadura • 1 saída para acionamento auxiliar • 1 entrada de alimentação 12V DC • 1 entrada de alimentação de carga • 2 entradas para botoeira e/ou sensor de porta aberta (local e/ou intertravamento), nomeadas Entrada 1 e Entrada 2.
Alimentação	Fonte de 12V 1A (12W)

** Disponível somente nos Controladores ZigLock TCP.*

Introdução

O *Sistema ZigLock TCP* foi concebido para permitir o efetivo controle do acesso de pessoas, a fim de auxiliar a sua proteção física e patrimonial.

Este manual apresenta o *Sistema ZigLock TCP* com seus dois componentes:

1. **Pontos de Acesso *ZigLock TCP*** (*Catraca ZigLock TCP* e *Controlador ZigLock TCP*): atuam como interface de identificação do usuário, controlando os acessos físicos.
2. **Software *ZigLock Web*** (instalado no PC): permite o cadastro dos usuários e o gerenciamento dos eventos de acesso gerados pelos pontos de acesso. Informações a respeito da instalação e utilização estão presentes nos documentos **Guia de Instalação – ZigLock Web** e **Manual do Usuário – ZigLock Web.**

A comunicação entre eles se dá através da *Ethernet* de 100Mbps, utilizando o protocolo TCP (comunicação segura) na camada de transporte do protocolo TCP/IP.

Por usar TCP/IP via *Ethernet*, todas as vantagens existentes nesse tipo de comunicação se fazem presentes: segurança, agilidade, possibilidade de utilizar a própria rede local (LAN) da empresa, possibilidade de utilizar VPN para comunicação através da internet com outra LAN (alcance global), grande familiaridade de profissionais de TI com a tecnologia (*Ethernet* + TCP/IP), possibilidade de testar se o dispositivo está configurado corretamente na rede utilizando o comando "ping", etc.

Modelos dos Pontos de Acesso *ZigLock TCP*

Os modelos atualmente comercializados dos pontos de acesso *ZigLock TCP* são:

- ***Controlador ZigLock TCP CARD***: modelo do controlador de acesso com identificação por cartão de proximidade (*CARD*).
- ***Controlador ZigLock TCP BIOCARD 480***: modelo do controlador de acesso com identificação por biometria (*BIO*) e cartão de proximidade (*CARD*), possuindo capacidade para armazenar até 480 digitais.
- ***Controlador ZigLock TCP BIOCARD 1500***: modelo do controlador de acesso com identificação por biometria (*BIO*) e cartão de proximidade (*CARD*), possuindo capacidade para armazenar até 1500 digitais.
- ***Catraca ZigLock TCP CARD***: modelo da catraca com identificação por cartão de proximidade (*CARD*).
- ***Catraca ZigLock TCP BIOCARD 480***: modelo da catraca com identificação por biometria (*BIO*) e por cartão de proximidade (*CARD*), possuindo capacidade para armazenar até 480 digitais.
- ***Catraca ZigLock TCP BIOCARD 1500***: modelo da catraca com identificação por biometria (*BIO*) e por cartão de proximidade (*CARD*), possuindo capacidade para armazenar até 1500 digitais.

Observação	*Todos os modelos, tanto do controlador quanto da catraca, permitem identificação também pelo teclado disponível no próprio equipamento.*

Passo a Passo do Conhecimento e Instalação do *Controlador ZigLock TCP*

Passo 1 – Conhecendo o Equipamento

Figura 1

a) Meios de Identificação do Usuário

Os usuários serão identificados pelo *Controlador ZigLock TCP* conforme leitores vistos na **Figura 1** (itens 1, 2 e 3).

Todos os modelos do controlador de acesso *ZigLock TCP* possuem leitor de cartões de proximidade (*RFID*, na forma de chaveiros ou cartões).

Observação	*Dentro destes identificadores, há um chip eletrônico com número único, funcionando como uma identidade digital. Ao ser aproximado à sua leitora, o chip é alimentado e envia, ao aparelho, seu número; por isso, não utiliza pilhas ou baterias.*

Por não haver contato direto (atrito) do cartão com a leitora, o sistema oferece baixo índice de manutenção, bem como maior tecnologia e segurança com relação a sistemas similares de códigos de barras e tarjas magnéticas.

Os cartões podem ser adquiridos diretamente com seu representante e são personalizáveis de acordo com a sua necessidade.

O modelo *ZigLock TCP BIOCARD* trabalha também fazendo a leitura das digitais dos usuários, que não são iguais nem mesmo entre dois dedos de uma mesma pessoa. Para agilizar a identificação, são capturados os pontos únicos em uma digital, chamados minúcias.

O produto torna-se de grande utilidade para o usuário, pois não há o problema do esquecimento de cartões, uma vez que ele pode garantir seu acesso pela identificação da própria impressão digital.

Os benefícios à empresa também são muito interessantes: economia na aquisição e reposição de crachás, bem como a eliminação de fraudes no controle de acesso (garante que o acesso do usuário só será registrado com a presença física do mesmo).

O teclado do equipamento (item 1 da **Figura 1**) possui, também, a função de permitir acesso aos usuários, além de permitir o acesso a funções especiais, conforme ilustra a **Figura 2**.

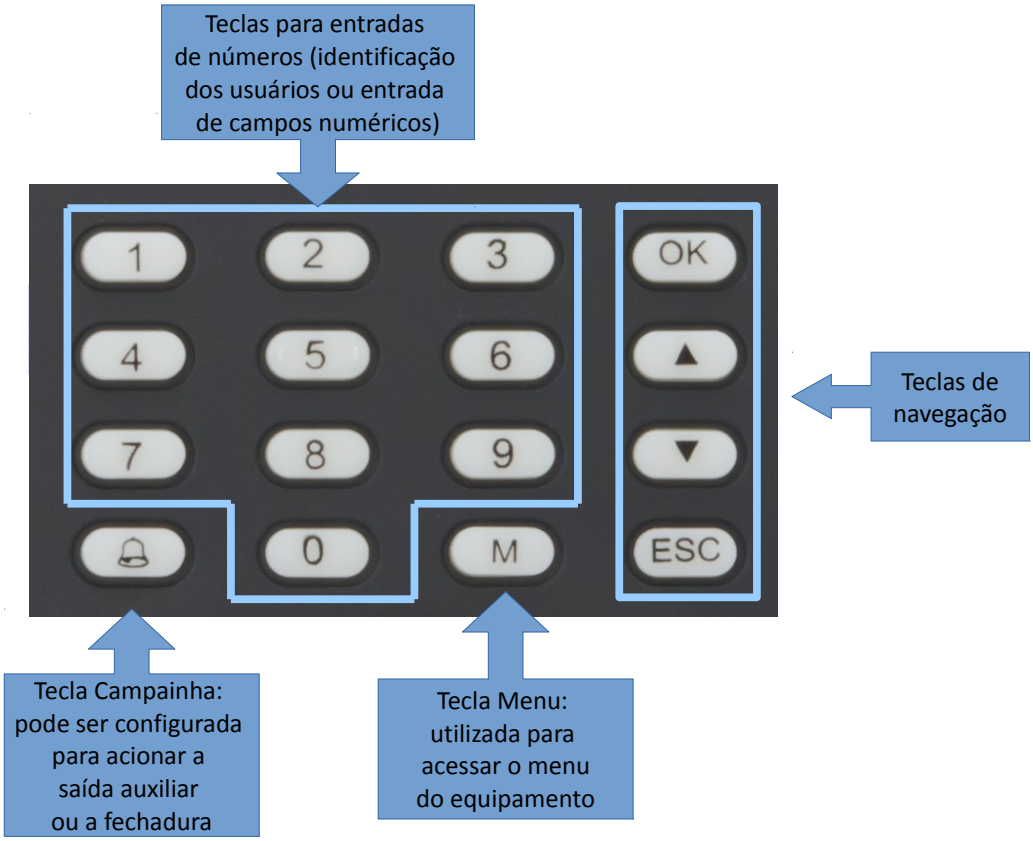


Figura 2

Observação	*Para facilitar a instalação e teste de um equipamento novo, que não tenha nenhum usuário cadastrado, pode-se digitar "123" e a tecla "OK" para liberar o acesso (acionar o fecho ou fechadura). Após o cadastro do primeiro usuário no ponto de acesso, não é mais possível liberar o acesso dessa forma.*

b) Menu do Equipamento

Através do menu do equipamento (**Figura 3**), pode-se: (1) realizar diversas configurações do funcionamento e ajustes do equipamento, (2) visualizar informações a respeito da versão do *firmware* e (3) colocar o equipamento em modo de gravação para ser possível atualizar o *firmware* do equipamento. O menu se encontra organizado da seguinte forma:

1. Configuração do TCP/IP

Menu de leitura e configuração relacionadas à comunicação TCP/IP.

1.1. Endereço IP

Permite ler e atualizar o endereço IP do equipamento da rede. Exemplo: 10.0.0.123 (em rede classe A), 172.16.0.123 (em rede classe B) ou 192.168.0.123 (em rede classe C).

1.2. Máscara de Rede

Permite ler e atualizar a máscara de sub-rede utilizada na rede onde o equipamento está configurado. Exemplo: 255.0.0.0 (padrão da rede classe A), 255.255.0.0 (padrão da rede classe B) ou 255.255.255.0 (padrão da rede classe C).

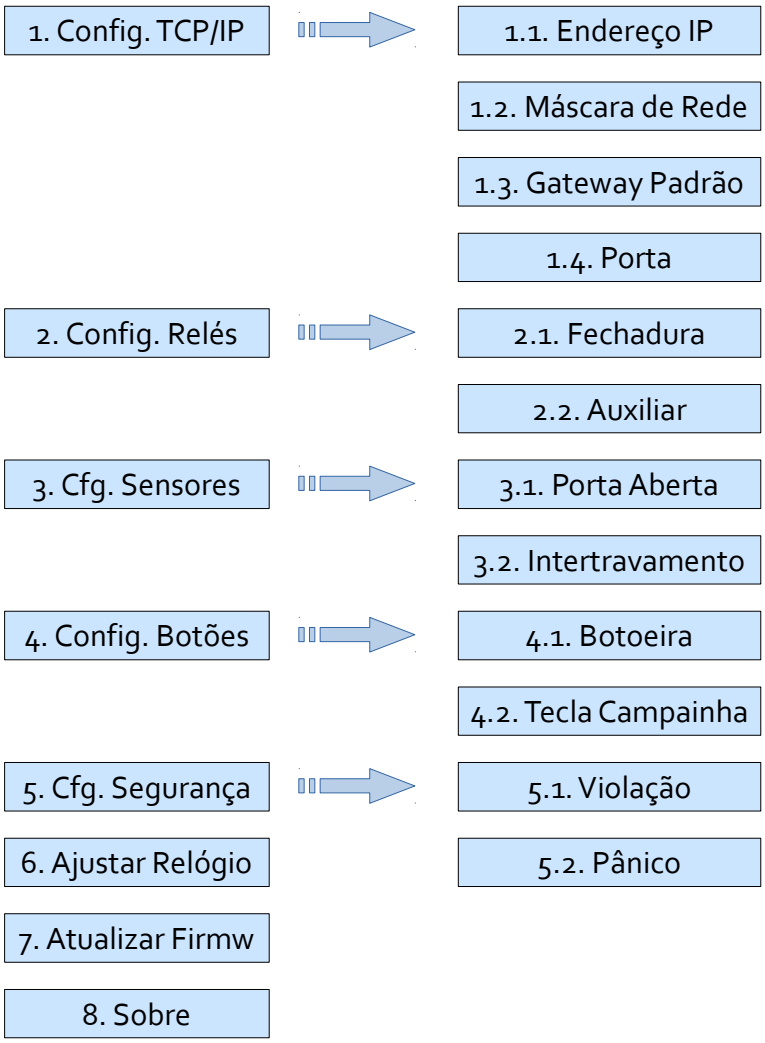


Figura 3

1.3. *Gateway* Padrão

Permite ler e atualizar o *gateway* padrão utilizado na rede, o qual é o *host* destino pra onde o equipamento deve encaminhar os pacotes caso o destinatário não esteja visível na rede local. Uma vez encaminhado um pacote TCP/IP ao *gateway* padrão, ele se encarrega de encaminhá-lo para fora da rede local, buscando entregá-lo ao destinatário.

1.4. Porta

Permite ler e atualizar a porta utilizada para realizar a comunicação com o PC. A porta de rede é muito importante, pois pode ser utilizada para encaminhar pacotes vindos da internet diretamente ao equipamento dentro da rede local (configuração feita no roteador), além de ser utilizado em configurações de segurança e prioridades dentro das redes. É importante verificar que nenhum *firewall*, do PC onde está instalado o aplicativo *ZigLock Web* ou outro equipamento que possa bloquear pacotes em nível de porta, esteja bloqueando a porta utilizada pelo equipamento.

2. Configuração dos Relés

Menu de configuração do funcionamento dos 2 relés (saídas) disponíveis no equipamento.

Através deste menu, é possível: (1) selecionar se o dispositivo é NA (normalmente aberto) ou NF (normalmente fechado), sendo possível configurar a largura de pulso que será dada ao acionar o relé (modo pulsar) ou (2) selecionar se o dispositivo funcionará no modo comutar, onde o relé é invertido (fechado/aberto) a cada acionamento; este modo (comutar) pode ser utilizado para ligar/desligar lâmpadas, por exemplo.

Observação	*O tempo utilizado para configurar o pulso no menu está em milissegundos (ms), ou seja, se for preciso configurar um pulso grande, de 15 segundos, por exemplo, é necessário digitar 15000 (15000 milissegundos = 15 segundos).*

2.1. Fechadura

Permite configurar o relé da fechadura, o qual será utilizado para liberar o acesso do usuário ao local controlado pelo ponto de acesso. Esse relé pode ser acionado através dos seguintes estímulos: (1) identificação de um usuário com acesso liberado (estímulo padrão), (2) pressionamento de uma botoeira (acionada por um porteiro, por exemplo) ou (3) pressionamento da *Tecla Campainha* do próprio equipamento.

Observação	*Os estímulos (2) e (3) devem ser ativados e configurados através do próprio menu para funcionarem.*

2.2. Auxiliar

Permite configurar o relé auxiliar do equipamento. Esse relé auxiliar pode ser utilizado para acionar um dos diversos dispositivos, externos ao equipamento (não inclusos), possíveis; por exemplo: lâmpadas, alarmes e circuitos de segurança [para avisar o dono da empresa ou, diretamente, a polícia da ocorrência de um assalto (pânico), por exemplo].

O relé auxiliar ou **saída auxiliar**, como também é tratado, pode ser acionado através dos seguintes estímulos: (1) pressionamento de uma botoeira, (2) pressionamento da *Tecla Campainha* do próprio equipamento, (3) ocorrência da violação do equipamento (retirada do equipamento de seu suporte), (4) ocorrência de pânico (identificado pela digitação de um dígito qualquer a mais no final da senha durante a identificação do usuário por matrícula e senha ou por um dedo marcado como dedo de pânico) ou (5) estouro do tempo (*timeout*) de espera para que a porta seja fechada.

Observação	*Todos os estímulos devem ser ativados e configurados através do próprio menu para funcionarem.*

3. Configuração dos Sensores

Menu de configuração de possíveis sensores de porta aberta ligados ao equipamento através das 2 entradas disponíveis (*Entrada 1* e *Entrada 2*).

3.1. Porta Aberta

Permite configurar um sensor de porta aberta local ao equipamento com o uso de uma das entradas (*Entrada 1* ou *Entrada 2*), que deve estar disponível para isso. Com esse sensor de porta aberta, é possível acionar o relé auxiliar se a porta não for fechada pelo tempo configurado no menu (identificado como *timeout*), sendo possível soar um alarme ou ligar uma lâmpada de alerta, por exemplo, avisando que a porta foi esquecida aberta e que deve ser fechada.

3.2. Intertravamento

Permite configurar um sensor de porta aberta ligado à porta acionada por outro ponto de acesso. Com esse recurso, é possível bloquear o acesso de um usuário caso ele tenha esquecido de

fechar a outra porta de um corredor, por exemplo, forçando-o a fechar primeiro a outra porta para depois conseguir a liberação do acesso. Esse tipo de bloqueio é conhecido como intertravamento ou gaiola de proteção.

4. Configuração dos Botões

Menu de configuração da botoeira e da *Tecla Campainha* do equipamento.

4.1. Botoeira

Permite configurar o uso de uma botoeira ligada a uma das entradas (*Entrada 1* ou *Entrada 2*) que esteja disponível no equipamento para: (1) acionar a fechadura ou (2) acionar o relé auxiliar.

4.2. Tecla Campainha

Permite configurar o uso da *Tecla Campainha*, do próprio equipamento, para: (1) acionar a fechadura ou (2) acionar o relé auxiliar.

5. Configuração de Segurança

Menu de configuração dos recursos relacionados à segurança disponíveis no equipamento.

5.1. Violação

Permite configurar se o relé auxiliar será ou não acionado durante a ocorrência da violação do equipamento. A violação do equipamento se dá quando ele é retirado de seu suporte enquanto está ligado, momento em que uma pessoa mal-intencionada pode tentar acionar a fechadura ou o relé auxiliar de maneira forçada, pois terá acesso às conexões do equipamento.

5.2. Pânico

Permite configurar se o relé auxiliar será ou não acionado durante a ocorrência de pânico sinalizada pelo usuário. Essa sinalização de pânico é realizada com: (1) a digitação de um dígito qualquer a mais no final da senha durante a identificação do usuário por matrícula e senha ou (2) a identificação do usuário pela digital marcada como digital de pânico.

Esse recurso, conhecido como pânico, é utilizado para sinalizar para o sistema que está ocorrendo algum problema com o usuário (está sendo assaltado, sequestrado, passando mal, quer que alguém do RH lhe procure para uma conversa ou precisou sair às pressas, por exemplo). Ao configurar a saída auxiliar para acionar um circuito externo (não incluso), pessoas ou equipes próprias para resolver os problemas de pânico podem ser avisadas automaticamente pelo próprio sistema.

ATENÇÃO	*1. Por motivos de segurança, para que um assaltante não perceba que o usuário está sinalizando pânico, por exemplo, mesmo que a saída auxiliar seja acionada no momento, nada além da mensagem de liberação ou bloqueio de acesso será exibida no display do equipamento.* *2. A sinalização de pânico não altera as prioridades de acesso do usuário, ou seja, o acesso é controlado normalmente, podendo ser liberado ou bloqueado.*

6. Ajustar Relógio

Permite configurar o relógio do equipamento automaticamente (quando o PC está *online*) ou manualmente.

7. Atualizar o *Firmware*

Permite colocar o equipamento em modo de atualização de *firmware*. Para isso, é necessário um cabo USB e o arquivo com o conteúdo do *firmware* a ser atualizado no equipamento.

Após colocar o *firmware* em modo de atualização, quando o *display* fica com o fundo apagado, os seguintes passos devem ser executados para realizar a atualização do equipamento de fato:

1. Retire o equipamento de seu suporte, sem desligá-lo, para ter acesso à porta USB do equipamento.
2. Conecte o cabo USB (macho x macho) no equipamento e no PC.
3. Ao aparecer uma nova unidade USB de armazenamento chamada "RW ZigLock", apague o arquivo "firmware.bin" que estará nela.
4. Copie a versão mais atual do *firmware* (ex.: "CONTROLADOR_ZIGLOCK_TCP-v3.00.bin") para a mesma unidade USB.
5. Mande ejetar a unidade USB ("RW ZigLock") e desconecte o cabo USB logo em seguida.

Observação	*Neste momento, o equipamento será reiniciado e começará a executar o novo firmware.*

6. Recoloque o equipamento em seu suporte o quanto antes, pois o *firmware* novo ficará sinalizando violação enquanto isso não for feito.

7. Sobre

Permite visualizar a identificação do equipamento, incluindo seu nome, versão e momento da compilação do *firmware* (através do código hexadecimal exibido).

Passo 2 – Fixando o Suporte do Equipamento à Parede

O suporte de fixação (acompanha o produto), que pode ser visto na **Figura 4**, é útil para manter o equipamento fixo e travado na parede, além de garantir o seu correto funcionamento.

Os furos do suporte (indicados pelas setas na **Figura 4**) são aqueles que serão fixados na parede através de parafusos. Estes furos "casam" exatamente com o tamanho e localização dos parafusos de caixas padrões 4x2; desta forma, é possível instalar o equipamento sem, ao menos, fazer furos na parede.

Observe a **Figura 4** para a devida posição do suporte. Puxe os fios do conduíte para que passem por dentro da cavidade do suporte antes de fixá-lo à caixa 4x2.

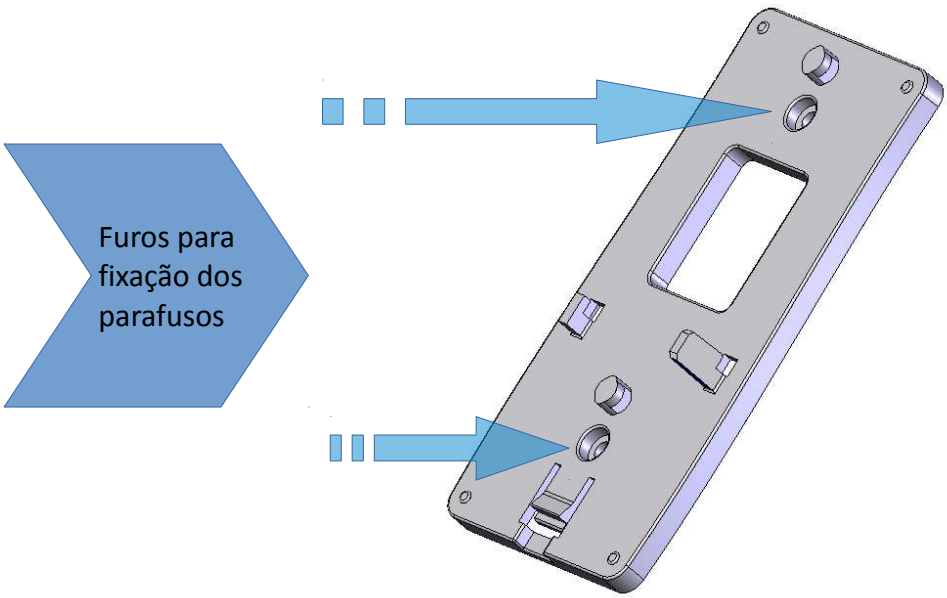


Figura 4

Passo 3 – Fazendo as Ligações Elétricas

Todos os fios de ligação do equipamento são colocados em sua parte traseira, conforme visto na **Figura 5**.

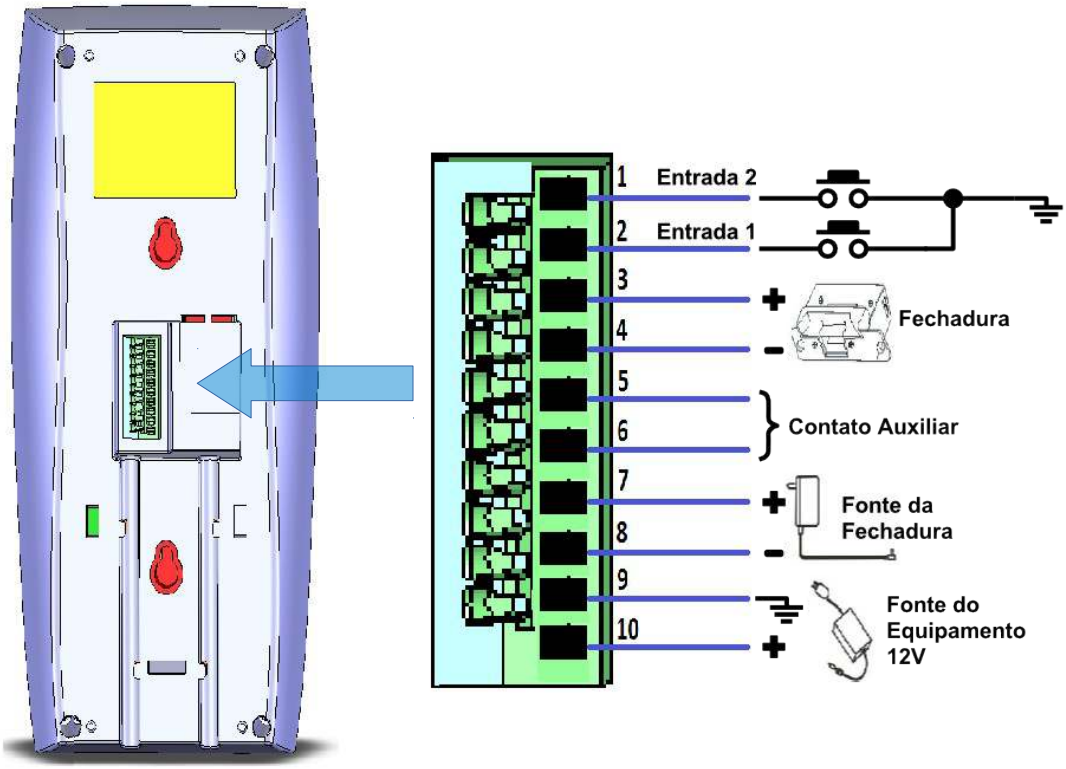


Figura 5

– Pino 1: destinado à ligação de (1) uma botoeira, possibilitando a abertura da fechadura sem que haja uma identificação (isso também pode ser feito utilizando a *Tecla Campainha*,

do teclado do próprio equipamento), (2) um sensor de porta aberta local, possibilitando acionar um alarme ou acender uma luz se a porta ficar aberta após o tempo de espera configurado ou (3) um sensor de porta aberta remoto, possibilitando bloquear o acesso a um determinado controlador se a porta controlada por outro controlador ainda estiver aberta (intertravamento). Todos esses recursos devem ser NA (normalmente abertos).

Observação	*Considere estas mesmas características e possibilidades para a "Entrada 1" (pino 2); com estas 2 entradas (Entrada 1 e Entrada 2), pode-se ligar uma botoeira e um sensor de porta aberta, ao mesmo tempo, no equipamento, por exemplo.*

- Pinos 3 e 4: destinados à ligação de um fecho ou fechadura (não inclusos), configuráveis em NA (normalmente abertos) ou NF (normalmente fechados) pelo menu do próprio equipamento. Dependendo da configuração, realizada no menu do próprio equipamento, e do acionamento realizado, as seguintes conexões são estabelecidas:
  - Pino 7 ligado ao Pino 3.
  - Pino 8 ligado ao Pino 4.

ATENÇÃO	*Este contato suporta fechaduras de até 1,5 A. Não exceda este valor!*

Caso a fechadura seja do tipo de alimentação contínua (DC), recomenda-se a utilização de um diodo *FR107* (incluso) para evitar danos ao sistema. Para este caso, siga o esquema da **Figura 6.**

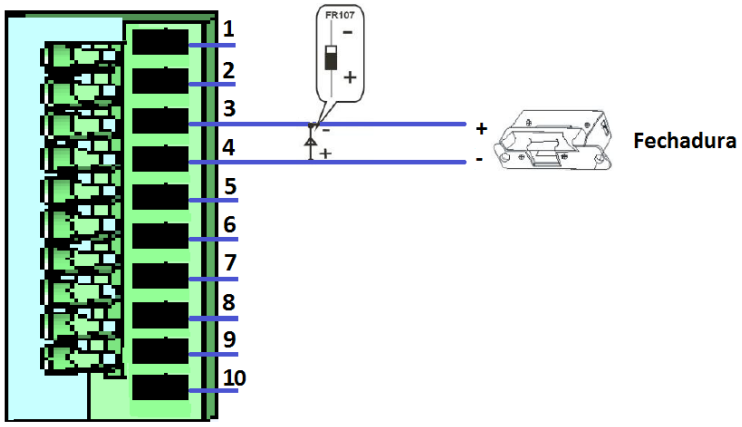


Figura 6

- Pinos 5 e 6: estes são pinos do relé auxiliar, o qual pode ser utilizado para ligar uma lâmpada, acionar uma campainha, ativar um alarme, acionar um determinado circuito externo (todos não inclusos), dentre outros. De acordo com a configuração feita pelo menu do próprio equipamento, esta saída auxiliar (relé) pode ser configurada (1) como NA ou NF, com largura de pulso configurável ou (2) em modo comutar, onde cada acionamento faz com que o contato seja invertido (para ligar e desligar uma lâmpada, por exemplo). A funcionalidade de ligar ou desligar uma lâmpada pode ser útil nos casos onde o equipamento é instalado exatamente no lugar do interruptor da lâmpada, já que o equipamento possui um suporte para fixação em caixas elétricas 4x2. Vide o **Passo 2 – Fixando o Suporte do Equipamento à Parede** para mais detalhes neste sentido.
- Pinos 7 e 8: destinados à ligação da fonte de alimentação compatível com o fecho ou fechadura instalado. Consulte o fabricante desses dispositivos para escolher corretamente uma fonte compatível.

ATENÇÃO	***Não** utilize a fonte do equipamento (pinos 9 e 10) para alimentar estes pinos.*

- Pinos 9 e 10: nestes pinos, é ligada a fonte de alimentação do equipamento.

Passo 4 – Fixando o Equipamento ao Suporte de Fixação

Uma vez com o suporte fixado e os fios conectados ao aparelho, siga a **Figura 7** para o devido encaixe do equipamento ao suporte.

Encaixe os pinos do suporte às cavidades da parte posterior do equipamento, conforme a **Figura 7**, e empurre o equipamento para baixo; isso fará com que ele fique travado ao suporte, segurando-o à parede. Isto se dá por um sistema de "click" que trava uma lingueta do suporte a um orifício do equipamento.

Quando for necessário retirar o equipamento da parede: (1) insira uma chave de fenda entre o equipamento e o suporte para liberar o "click", (2) empurre o equipamento para cima e (3) puxe o equipamento para frente.

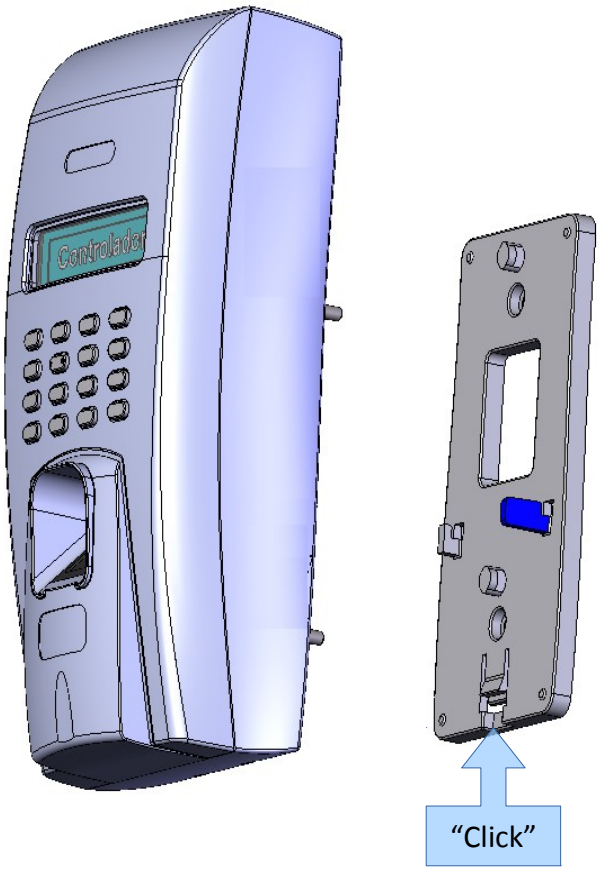


Figura 7

Conhecimento da *Catraca ZigLock TCP*

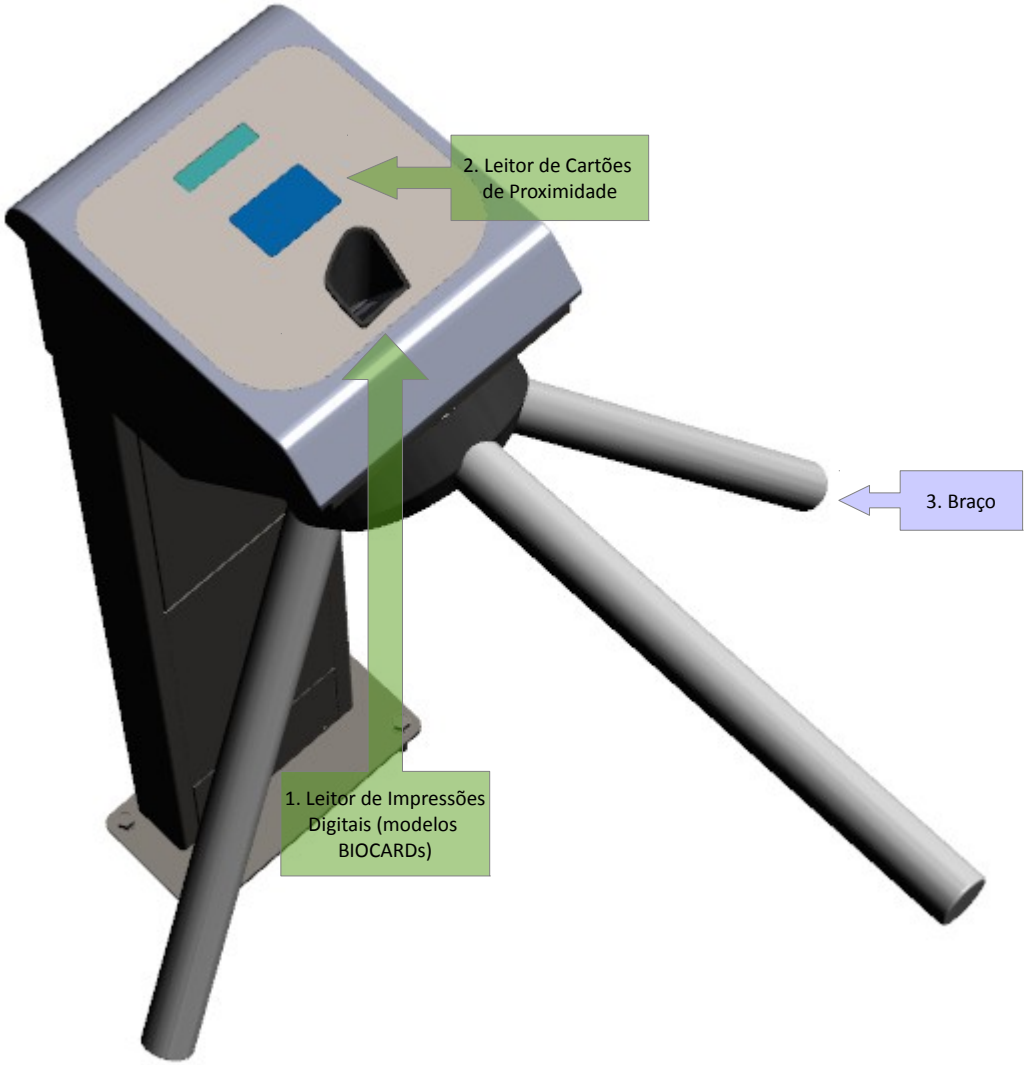


Figura 8

a) Meios de Identificação do Usuário

Os usuários serão identificados pela *Catraca ZigLock TCP* conforme leitores vistos na **Figura 8** (itens 1 e 2).

Todos os modelos da *Catraca ZigLock TCP* possuem leitor de cartões de proximidade (*RFID*, na forma de chaveiros ou cartões) .

Observação	*Dentro destes identificadores, há um chip eletrônico com número único, funcionando como uma identidade digital. Ao ser aproximado à sua leitora, o chip é alimentado e envia, ao aparelho, seu número; por isso, não utiliza pilhas ou baterias.*

Por não haver contato direto (atrito) do cartão com a leitora, o sistema oferece baixo índice de manutenção, bem como maior tecnologia e segurança com relação a sistemas similares de códigos de barras e tarjas magnéticas.

Os cartões podem ser adquiridos diretamente com seu representante e são

personalizáveis de acordo com a sua necessidade.

Os modelos *ZigLock TCP BIOCARD 480* e *ZigLock TCP BIOCARD 1500* trabalham também fazendo a leitura das digitais dos usuários, que não são iguais nem mesmo entre dois dedos de uma mesma pessoa. Para agilizar a identificação, são capturados os pontos únicos em uma digital, chamados minúcias.

O produto torna-se de grande utilidade para o usuário, pois não há o problema do esquecimento de cartões, uma vez que ele pode garantir seu acesso pela identificação da própria impressão digital.

Os benefícios à empresa também são muito interessantes: economia na aquisição e reposição de crachás, bem como a eliminação de fraudes no controle de acesso (garante que o acesso do usuário só será registrado com a presença física do mesmo).

O equipamento possui um teclado externo, qua para ser utilizado deve ser conectado a placa principal no interior do painel da Catraca. Este teclado possui a função de permitir acesso aos usuários, além de permitir também o acesso a funções especiais, conforme ilustra a **Figura 10**.

Figura 9

Observação	*Para facilitar a instalação e teste de um equipamento novo, que não tenha nenhum usuário cadastrado, pode-se digitar "123" e a tecla "OK" para liberar o acesso. Após o cadastro do primeiro usuário no ponto de acesso, não é mais possível liberar o acesso dessa forma.*

b) Menu do Equipamento

Através do menu do equipamento (**Figura 10**), pode-se: (1) realizar alguns ajustes do equipamento, (2) visualizar informações a respeito da versão do *firmware* e (3) colocar o equipamento em modo de gravação para ser possível atualizar o seu *firmware*.

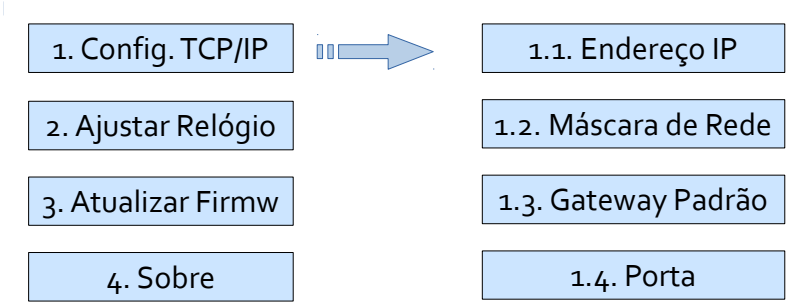


Figura 10

1. Configuração do TCP/IP

Menu de leitura e configuração relacionadas à comunicação TCP/IP.

1.1. Endereço IP

Permite ler e atualizar o endereço IP do equipamento da rede. Exemplo: 10.0.0.123 (em rede classe A), 172.16.0.123 (em rede classe B) ou 192.168.0.123 (em rede classe C).

1.2. Máscara de Rede

Permite ler e atualizar a máscara de sub-rede utilizada na rede onde o equipamento está configurado. Exemplo: 255.0.0.0 (padrão da rede classe A), 255.255.0.0 (padrão da rede classe B) ou 255.255.255.0 (padrão da rede classe C).

1.3. *Gateway* Padrão

Permite ler e atualizar o *gateway* padrão utilizado na rede, o qual é o *host* destino pra onde o equipamento deve encaminhar os pacotes caso o destinatário não esteja visível na rede local. Uma vez encaminhado um pacote TCP/IP ao *gateway* padrão, ele se encarrega de encaminhá-lo para fora da rede local, buscando entregá-lo ao destinatário.

1.4. Porta

Permite ler e atualizar a porta utilizada para realizar a comunicação com o PC. A porta de rede é muito importante, pois pode ser utilizada para encaminhar pacotes vindos da internet diretamente ao equipamento dentro da rede local (configuração feita no roteador), além de ser utilizado em configurações de segurança e prioridades dentro das redes. É importante verificar que nenhum *firewall*, do PC onde está instalado o aplicativo *ZigLock Web* ou outro equipamento que possa bloquear pacotes em nível de porta, esteja bloqueando a porta utilizada pelo equipamento.

2. Ajustar Relógio

Permite configurar o relógio do equipamento automaticamente (quando o PC está *online*) ou manualmente.

3. Atualizar o *Firmware*

Permite colocar o equipamento em modo de atualização de *firmware*. Para isso, é necessário um cabo USB e o arquivo com o conteúdo do *firmware* a ser atualizado no equipamento.

Após colocar o *firmware* em modo de atualização, quando o *display* fica com o fundo apagado, os seguintes passos devem ser executados para realizar a atualização do equipamento de fato:

1. Conecte o cabo USB (macho x macho), ligado à placa do equipamento, no PC.
2. Ao aparecer uma nova unidade USB de armazenamento chamada "RW ZigLock", apague o arquivo "firmware.bin" que estará nela.
3. Copie a versão mais atual do *firmware* (ex.: "CATRACA_ZIGLOCK_TCP-v3.00.bin") para a mesma unidade USB.
4. Mande ejetar a unidade USB ("RW ZigLock") e desconecte o cabo USB do PC logo em seguida.

Observação	*Neste momento, o equipamento será reiniciado e começará a executar o novo firmware.*

4. Sobre

Permite visualizar a identificação do equipamento, incluindo seu nome, versão e momento da compilação do *firmware* (através do código hexadecimal exibido).

Notas de Revisão

Rev.	Data	Nota
1.0	17/09/13	- Revisão inicial.
1.1	20/12/13	- Mudança do nome *Human* para *Zenvia*. - Enfatização de que o usuário poderá ser bloqueado mesmo sinalizando pânico. - Atualização necessária para acompanhar o software. - Atualização da especificação das ligações elétricas.
1.2	31/01/14	- Inclusão dos modelos de 480 e 1500 digitais do controlador. - Correção da informação a respeito da fonte de alimentação.
1.3	27/08/14	- Exclusão dos modelos de Controlador+
1.4	04/09/14	- Geração de planilhas - Funcionamento do ZigLock Explorer em rede, para consulta de eventos
1.5	29/01/15	- Alteração na descrição da garantia do produto.
1.6	05/02/15	– Atualização das partes que se referem ao teclado da catraca ZigLock TCP destacando que é teclado Externo. – Inclusão da informação que o hamster a ser usado deve ser da Vird, modelo VIRD-FOH02.
1.7	06/05/15	– Removidas as informações referentes ao ZigLock TCP Explorer.

GARANTIA

Assegura-se ao *Controlador de Acesso ZigLock TCP* (modelos: *Controlador ZigLock TCP CARD*, *Controlador ZigLock TCP BIOCARD*, *Catraca ZigLock TCP CARD*, *Catraca ZigLock TCP BIOCARD 480 e Catraca ZigLock TCP BIOCARD 1500*),*a garantia contra qualquer defeito de material de fabricação que nele se apresente no período de 3 (meses) de garantia legal e mais 9 (nove) meses de garantia adicional, contados a partir da data de emissão da nota fiscal.*

A garantia tornar-se-á nula e sem efeito se o produto sofrer (1) qualquer dano provocado por acidentes, agentes da natureza, desgaste natural das peças e componentes, (2) uso abusivo ou em desacordo com as instruções do manual, (3) descuido do usuário no manuseio, transporte ou remoção do aparelho, ou ainda, (4) no caso de apresentar sinais de violação, ajuste ou conserto por pessoas não autorizadas.

A garantia oferecida limita-se ao conserto ou troca do produto adquirido. A RW Tecnologia não se responsabiliza por possíveis danos causados por incidentes, má-fé ou inabilidade no uso do produto.

RW Tecnologia Indústria e Comércio Ltda.
Enterplak Produtos Eletrônicos Ltda.