

# Manual do Usuário

## MA300 (PUSH)

Data: Outubro 2023

Versão do Documento: 3.0

Idioma: Português

Obrigado por escolher nosso produto. Por favor, leia atentamente as instruções antes de operá-lo. Siga estas instruções para garantir que o produto esteja funcionando corretamente. As imagens mostradas neste manual são apenas ilustrativas.



Para obter mais detalhes, visite o site de nossa empresa em [www.zkteco.com.br](http://www.zkteco.com.br).

Copyright © 2022 ZKTECO CO., LTD. Todos os direitos reservados.

Sem o consentimento prévio por escrito da ZKTeco, nenhuma parte deste manual pode ser copiada ou encaminhada de qualquer forma ou forma. Todas as partes deste manual pertencem à ZKTeco e suas subsidiárias (doravante "Empresa" ou "ZKTeco").

## Marca registrada

**ZKTeco** é uma marca registrada da ZKTeco. Outras marcas mencionadas neste manual são propriedades de seus respectivos proprietários.

## Responsabilidade

Este manual contém informações sobre a operação e manutenção dos produtos ZKTeco. Os direitos de propriedade intelectual de todos os documentos, desenhos, etc., em relação aos produtos fornecidos pela ZKTeco são de propriedade da ZKTeco. O conteúdo deste documento não deve ser usado ou compartilhado pelo receptor com terceiros sem a permissão expressa por escrito da ZKTeco.

O conteúdo deste manual deve ser lido na íntegra antes de iniciar a utilização e manutenção do produto adquirido. Se algum dos conteúdos do manual parecer pouco claro ou incompleto, entre em contato com a ZKTeco antes de iniciar a utilização e/ou manutenção do referido produto.

É um pré-requisito essencial para a operação e/ou manutenção corretas/ adequadas, que a equipe que irá utilizar e/ou dar manutenção, esteja totalmente familiarizado com o projeto e que esta equipe tenha recebido um treinamento completo da utilização e/ou manutenção da máquina / unidade / produto. É ainda essencial para a utilização segura da máquina / unidade / produto que a equipe tenha lido, compreendido e seguido as instruções de segurança contidas no manual.

Em caso de qualquer conflito entre os termos e condições deste manual e as especificações de fichas- técnicas, desenhos, folhas de instruções ou quaisquer outros documentos acordados entre as partes relacionados ao produto, as condições de tais documentos devem prevalecer em relação ao manual.

A responsabilidade da ZKTeco em relação ao presente manual e ao produto está detalhada nos termos de sua respectiva Garantia.

A ZKTeco reserva-se o direito de adicionar, apagar, alterar ou modificar as informações contidas no manual de tempos em tempos, independente de aviso prévio, por meio de circulares, cartas, notas e/ou novas edições do manual, visando a melhor utilização e/ou segurança do produto. Os mais recentes procedimentos de utilização e documentos relevantes estão disponíveis em <http://www.zkteco.com.br> sendo de responsabilidade do usuário verificar eventuais atualizações e informes, especialmente se o produto indicar problemas no funcionamento ou se restarem dúvidas sobre sua instalação, manejo, armazenamento, operação e/ou manutenção. Se houver algum problema relacionado ao produto, entre em contato conosco.

## ZKTeco Filial Brasil

**Endereço**      **Vespasiano:** Rodovia MG-010, KM 26 - Loteamento 12 - Bairro Angicos, Vespasiano - MG | CEP: 33.206-240

**Telefone**      (31) 3055-3530

Para questões comerciais, por favor entre em contato conosco pelo e-mail:

[comercial.brasil@zkteco.com](mailto:comercial.brasil@zkteco.com).

Para saber mais sobre nossas filiais globais, visite [www.zkteco.com](http://www.zkteco.com).

## Sobre a Empresa

A ZKTeco é um dos maiores fabricantes de leitores RFID e biométricos (impressão digital, facial, veia do dedo) do mundo. Nossos produtos incluem leitores e painéis de controle de acesso, câmeras de reconhecimento facial de curta e longa distância, controladores de acesso para elevadores e pisos, catracas, controladores de portão para reconhecimento de placas de veículos e produtos de consumo, como fechaduras de porta com leitor de impressão digital e reconhecimento facial alimentadas por bateria. Nossas soluções de segurança são multilíngues e localizadas em mais de 18 idiomas diferentes. Em nossas instalações de fabricação de última geração, certificadas pela ISO9001 e com área de 700.000 pés quadrados, controlamos a fabricação, o design do produto, a montagem de componentes e a logística/envio, tudo sob um mesmo teto.

Os fundadores da ZKTeco sempre se dedicaram à pesquisa e desenvolvimento independentes de procedimentos de autenticação biométrica e à produção de SDK de verificação biométrica, que inicialmente foram amplamente aplicados em segurança de PC e autenticação de identidade. Com o contínuo aprimoramento do desenvolvimento e diversas aplicações de mercado, a equipe gradualmente construiu um ecossistema de autenticação de identidade e um ecossistema de segurança inteligente, baseados em técnicas de verificação biométrica. Com anos de experiência na industrialização de verificações biométricas, a ZKTeco foi oficialmente estabelecida em 2007 e se tornou uma das principais empresas do mundo no setor de verificação biométrica, possuindo diversas patentes e sendo selecionada como Empresa Nacional de Alta Tecnologia por 6 anos consecutivos. Nossos produtos são protegidos por direitos de propriedade intelectual.


## Sobre o Manual


Este manual apresenta as operações do **MA300**.

Todas as imagens exibidas são apenas para fins ilustrativos. As imagens neste manual podem não ser exatamente consistentes com os produtos reais.

## Convenções do Documento

Este documento inclui convenções notacionais, como dicas, avisos importantes e precauções. As notações contidas neste manual incluem:

 : indica informações importantes, incluindo precauções, que devem ser lidas atentamente para obter o desempenho ideal do equipamento.

 : indica o aviso de voz gerado pelo dispositivo. Em caso de discrepância entre os avisos de voz neste documento e os gerados pelos produtos reais, estes últimos prevalecerão.

Este produto pode conter um ou mais módulos listados abaixo, de acordo com o modelo adquirido por você.



Módulo: DXYBT02  
"Incorpora produto homologado pela ANATEL sob número 03313-20-07632"



Módulo: A08  
"Incorpora produto homologado pela ANATEL sob número 09598-19-07632"



Módulo: B06  
"Incorpora produto homologado pela ANATEL sob número 11500-20-12720"

Este equipamento não tem direito à proteção contra interferência prejudicial e não pode causar interferência em sistemas devidamente autorizados.

# Índice

<b>1</b>	<b>INSTRUÇÕES DE USO .....</b>	<b>8</b>
1.1	BAE;5;A@3? 7@FA 6A 676A .....	*
1.2	;@EFDGÊÛ7E B3D3 B3EE3DA 53DFÊA .....	+
1.3	BD753GÊÛ7E .....	+
<b>2</b>	<b>INTRODUÇÃO DO DISPOSITIVO DE CONTROLE DE ACESSO .....</b>	<b>10</b>
2.1	H;ÊA 97D3>63E 8G@ÊÛ7E 6A 6;EBAE;F;HA .....	#"
2.2	3B3DÍ @5;3 6A BDA 6GFA .....	##
2.3	53DFÊA 67 97D7@5;3? 7@FA .....	#&
2.4	F;? 7AGF 67AB7D3ÊÊA .....	#'
<b>3</b>	<b>OPERAÇÕES DE DISPOSITIVO .....</b>	<b>16</b>
3.1	53DFÊA 67 97D7@5;3? 7@FA .....	#(
3.1.1	CADASTRAR CARTÃO DE GERENCIAMENTO .....	16
3.1.2	CADASTRAR USUÁRIO COMUM .....	17
3.1.3	EXCLUIR UM ÚNICO USUÁRIO .....	23
3.2	3GF7@F;53ÊÊA 67 GEGÂD;A .....	\$(
3.3	6;E5A GE4 .....	\$*
3.4	;@F7DDGBFADF3? B7D .....	+\$
<b>4</b>	<b>SERVIDOR WEB .....</b>	<b>31</b>
4.1	>A9;@ .....	%#
4.2	6;EBAE;F;HA .....	%%
4.2.1	ESTADO DO DISPOSITIVO .....	33
4.2.2	ALTERAR SENHA .....	33
4.3	5A@89GD3ÊÛ7E .....	%&
4.3.1	CONFIGURAÇÕES DE COMUNICAÇÃO .....	34
4.3.2	CONFIGURAÇÕES DE NUVEM .....	35

4.3.3	CONFIGURAÇÕES DO SISTEMA.....	36
4.3.4	DATA E HORA .....	36
4.3.5	REGISTROS DE OPERAÇÃO .....	37
4.4	GERENCIAMENTO DE DISPOSITIVOS .....	37
4.4.1	ATUALIZAÇÃO E REDEFINIÇÃO .....	37
4.4.2	CARREGAR CERTIFICADOS.....	38
<b>5</b>	<b>CONECTAR AO SOFTWARE ZKBIOACCESS.....</b>	<b>39</b>
5.1	DEFINA O ENDEREÇO DE COMUNICAÇÃO .....	39
5.2	ADICIONAR DISPOSITIVO AO SOFTWARE.....	40
5.3	ADICIONAR PESSOAS AO SOFTWARE .....	41
<b>6</b>	<b>APÊNDICE.....</b>	<b>42</b>
6.1	LISTA DE PARÂMETROS.....	42
6.2	POLÍTICA DE PRIVACIDADE .....	43
6.3	OPERAÇÃO ECOLOGICAMENTE CORRETA .....	47
	GARANTIA .....	49



# 1 Instruções de Uso

Antes de conhecer as características e funções do dispositivo, é recomendado familiarizar-se com os fundamentos abaixo.

## 1.1 Posicionamento do dedo

**Dedos recomendados:** Indicador, médio ou anelar; Evite usar o polegar ou o mindinho no leitor de impressões digitais, pois é difícil pressioná-los com precisão.



Muito baixo

Muito próximo da borda



Vertical

**Observação:** Por favor, utilize o método correto ao pressionar seus dedos no leitor de impressões digitais para registro e identificação. Nossa empresa não assumirá nenhuma responsabilidade por problemas de reconhecimento que possam resultar do uso incorreto do produto. Reservamo-nos o direito de interpretação final e modificação relacionados a esse ponto.

## 1.2 Instruções para Deslizar o Cartão

Integrado com um módulo leitor de cartão RF sem contato, este dispositivo suporta cartões de identificação e cartões IC/HID (opcional). Ao oferecer vários modos de autenticação, como autenticação por impressão digital e autenticação por cartão RF, este dispositivo pode atender a diversas necessidades dos usuários.

Deslize o seu cartão pela área do sensor seguindo as instruções de voz e remova-o após o dispositivo detectá-lo. Para a área de deslize, consulte a seção [2.2 Aparência do Produto](#).

Proteja o dispositivo contra exposição direta à luz solar ou feixes intensos, pois feixes intensos afetam significativamente a coleta de impressões digitais e podem resultar em falhas na autenticação por impressão digital.

Para obter os melhores resultados, o dispositivo deve ser utilizado em temperaturas que variam de 0°C a 50°C. É aconselhável adotar uma proteção contra o sol e instalações de dissipação de calor se o dispositivo ficar exposto ao ar livre por um longo período de tempo, pois temperaturas extremamente altas ou baixas podem reduzir o desempenho do dispositivo e resultar em uma taxa elevada de rejeição falsa (FRR) e taxa de aceitação falsa (FAR).

Ao instalar o dispositivo de controle de acesso, conecte o cabo de energia após conectar os outros cabos. Se o dispositivo não funcionar corretamente, certifique-se de desligar a fonte de alimentação antes de realizar a inspeção necessária. Note que qualquer trabalho em linha viva pode danificar o dispositivo e danos causados ao dispositivo devido ao trabalho em linha viva estão além do escopo de nossa garantia normal.

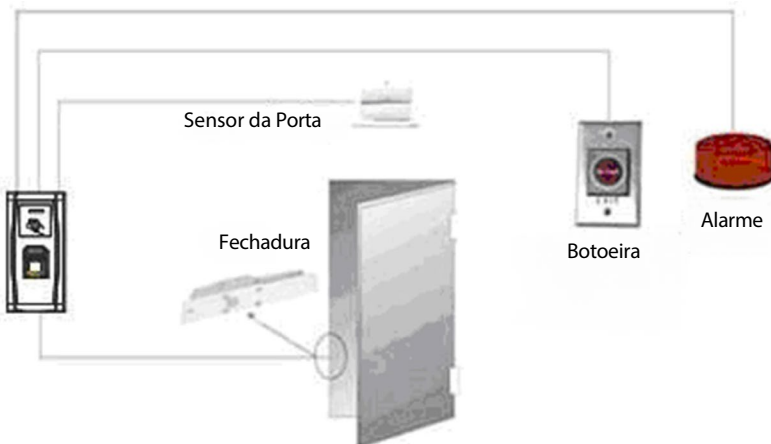
Para assuntos não abordados neste documento, consulte materiais relacionados, incluindo o Guia de Instalação e o Manual do Usuário do ZKBioAccess.

## 2 Introdução do Dispositivo de Controle de Acesso

### 2.1 Visão geral das funções do dispositivo

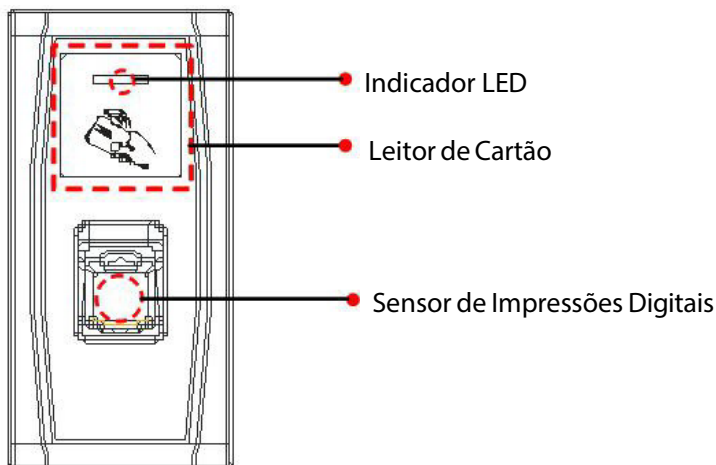
Nosso produto pode ser utilizado com uma fechadura eletrônica ou um controlador de acesso como um dispositivo combinado de controle de acesso e impressão digital. Esse dispositivo possibilita o uso de cartões de gerenciamento e possui operações fáceis e flexíveis. Você pode utilizar um cartão de gerenciamento para realizar tarefas como cadastro offline, cadastro de usuários e administração via U-disk. Sem a necessidade de uma tela, as instruções de voz guiarão você em todas as operações. Esse dispositivo não possui teclado. Ele suporta múltiplos modos de comunicação. O U-disk apresenta operações simples e convenientes. O design à prova d'água e a carcaça de metal do dispositivo permitem que ele resista a impactos fortes sem ser danificado.

Apresentando um design compacto e simples, esse dispositivo permite que os usuários conectem vários dispositivos através de um PC e realizem monitoramento em tempo real.



## 2.2 Aparência do Produto

Visão frontal:



- ❖ **Indicador LED:** O indicador LED é usado para exibir os resultados das operações do dispositivo e os status excepcionais, que são definidos da seguinte forma:

**Regras comuns:** Se uma operação for bem-sucedida, o indicador verde fica aceso por um segundo; caso contrário, o indicador vermelho fica aceso por um segundo.

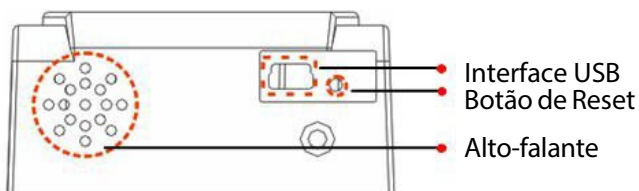
**Estado de Cadastro:** O LED verde pisca três vezes a cada três segundos.

**Exclusão de Usuário Individual:** O LED vermelho pisca três vezes a cada três segundos.

**Estado de Autenticação:** O LED verde pisca uma vez a cada dois segundos.

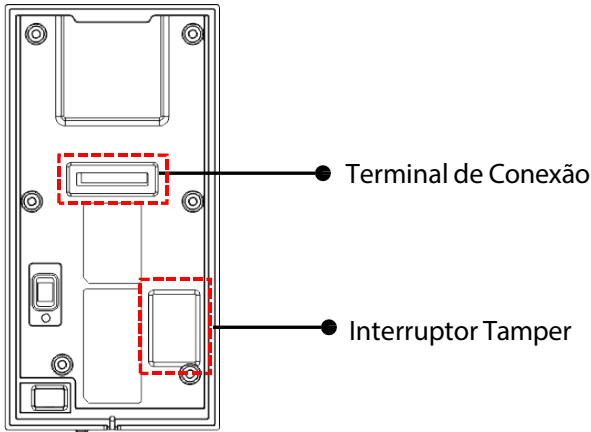
- ❖ **Leitor de Cartão:** Refere-se à área delimitada pela linha vermelha tracejada, conforme mostrado na figura acima.
- ❖ **Sensor de Impressão Digital:** Usado para coletar e comparar impressões digitais e excluir usuários.

Visão inferior:



- ❖ **Interface USB:** Usada para conectar com um U-disk.
- ❖ **Botão de Reset:** Usado para reiniciar o dispositivo.
- ❖ **Alto-falante:** Usado para reproduzir o som BEEP e as instruções de voz. Se um usuário passar na autenticação, o alto-falante emite um bipe e mostra a mensagem "Obrigado". Se o usuário não passar na autenticação pela impressão digital, o alto-falante emite um bipe e mostra a mensagem "Por favor, tente novamente". Se o usuário não passar na autenticação pelo cartão, o alto-falante emite dois bipes. As mensagens padrão durante a operação são: Bipe + instruções de voz.

Visão traseira:



- ❖ **Terminal de Conexão:** Conecta-se com fechaduras, fonte de alimentação e um PC através de cabos (para conexão detalhada, consulte o Guia de Instalação).
- ❖ **Interruptor de Violação:** Usado para gerar um alarme de violação. Para mais detalhes, consulte a seção [3.4 Interruptor de Violação](#).

**Estado de Autenticação:** Se você tiver realizado o cadastro ou cadastrado com sucesso em um cartão de gerenciamento, ou se alguma operação expirar, o dispositivo entra no estado de autenticação assim que for ligado.

Todos os usuários podem verificar sua identificação e desbloquear no estado de autenticação (o administrador com um cartão de gerenciamento só pode desbloquear usando suas impressões digitais previamente cadastradas); o administrador pode realizar operações como cadastro/exclusão de usuários e gerenciamento do U-disk.

**Observação:** Um cartão de gerenciamento funciona apenas no MA300.

## 2.3 Cartão de Gerenciamento

Os usuários do dispositivo são classificados em administradores e usuários comuns.

**Administrador:** Um administrador tem permissão para realizar todas as operações, incluindo cadastro ou exclusão de usuários (excluindo todos os outros usuários, exceto ele/ela) e gerenciamento do U-disk. Os privilégios do administrador do dispositivo são implementados através do cartão de gerenciamento.

**Usuários Comuns:** Usuários comuns só têm permissão para verificar sua identidade e desbloquear o dispositivo.

Um cartão de gerenciamento é um cartão especialmente designado para um superadministrador. Cada dispositivo deve cadastrar um cartão de gerenciamento. Se nenhum cartão de gerenciamento for cadastrado, você não poderá realizar nenhuma operação e o sistema emitirá uma mensagem de voz “🔊: Por favor, cadastre o cartão de gerenciamento”.



**Você pode executar diferentes funções ao passar um cartão de gerenciamento várias vezes seguidas:**

### **Nenhum Disco USB está conectado:**

- Ao aproximar o cartão de gerenciamento uma vez, você pode entrar no estado de cadastro de usuário único.
- Ao aproximar o cartão de gerenciamento cinco vezes seguidas, você pode entrar no estado de exclusão de usuário único.

### **Um Disco USB está conectado**

- Ao aproximar o cartão de gerenciamento uma vez, você pode entrar no estado de gerenciamento do Disco USB.

**Passagens consecutivas:** Passagens consecutivas significam que o intervalo entre duas passagens consecutivas é menor que 5 segundos.

O cartão de gerenciamento pode ser excluído através do software. Para mais detalhes, consulte o Manual do Usuário do ZKBioAccess.

As impressões digitais do usuário que possui um cartão de gerenciamento só podem ser cadastradas através do software. Para mais detalhes, consulte a seção [5.3.5.3](#).



**Dica:** Os usuários que possuem cartões de gerenciamento só podem autenticar sua identidade e desbloquear utilizando as impressões digitais previamente cadastradas.

## 2.4 Timeout de Operação

O tempo limite de operação padrão é de 30 segundos. Se não houver nenhuma operação ao cadastrar um cartão de gerenciamento ou ao excluir/cadastrar um usuário, o sistema emite um aviso a cada 10 segundos e, após três avisos, retorna ao estado de autenticação. A mensagem de voz é "Tempo limite de operação. O sistema retorna ao estado de autenticação".



## 3 Operações de Dispositivo

### 3.1 Cartão de Gerenciamento

#### 3.1.1 Cadastrar Cartão de Gerenciamento

**Para cadastrar um cartão de gerenciamento, siga as instruções a seguir:**

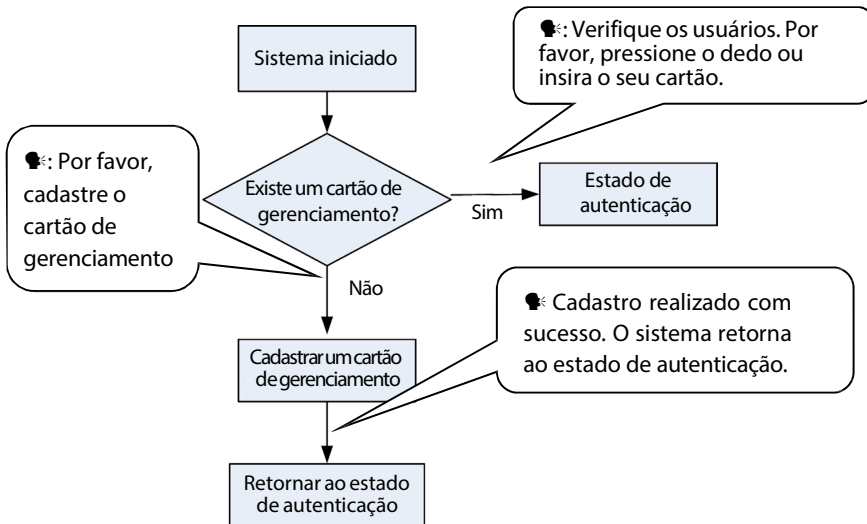
1. O dispositivo detecta automaticamente se existe um cartão de gerenciamento.
2. Se o dispositivo não detectar a presença de um cartão de gerenciamento, ele entra no estado de cadastro do cartão de gerenciamento. Prossiga para o passo 3; caso contrário, pule para o passo 5.
3. Após o sistema emitir a mensagem de voz "🔊: Por favor, cadastre o cartão de gerenciamento", deslize o seu cartão na área do sensor.



**Dica:** O dispositivo permanecerá no estado de cadastro do cartão de gerenciamento até que o seu cartão seja registrado com sucesso.

4. Se o cadastro for bem-sucedido, o sistema emitirá a mensagem de voz "🔊: "Cadastro realizado com sucesso. O sistema retorna ao estado de autenticação".
5. Após retornar ao estado de autenticação, o sistema emitirá a mensagem de voz "🔊: "Verifique os usuários. Por favor, pressione o dedo ou passe o cartão".

**O fluxograma de cadastro do cartão de gerenciamento é mostrado abaixo:**

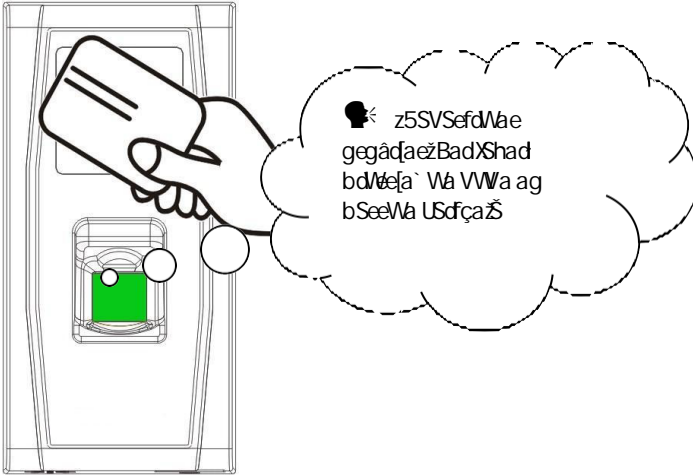


### 3.1.2 Cadastrar Usuário Comum

Cada vez que você entra no estado de cadastro, apenas um usuário pode ser cadastrado. Ao cadastrar um novo usuário, o sistema atribui automaticamente um ID ocioso mínimo ao usuário. Cada usuário pode cadastrar no máximo 10 impressões digitais e um cartão.

**Para cadastrar um usuário, siga as instruções a seguir:**

1. No estado de verificação, o sistema entra no estado de cadastro do usuário comum após você passar o cartão de gerenciamento uma vez (No estado de cadastro, passar o cartão de gerenciamento uma vez retornará você ao estado de verificação).
2. Após o sistema emitir a mensagem de voz "🔊: Cadastre os usuários. Por favor, pressione o dedo ou insira o cartão", você pode iniciar o cadastro do usuário. Existem os seguintes dois casos:



**(1).. Passe o cartão primeiro**

**Sž** CgS` Va haUë bSeeSda eVg` aha USçã WLa` eVg[d USVSeFdSd g\_ gegãda a V[ebae[f]ha [dã YVsdg\_ Sh[ea VVhal z☛, Gegãda `ø\_ Wã ffz5SVSeFdã dVŠ`! SVa La\_ egUWãã` /fFl dVWãZãVWa :6 SfdTgiVa Sgfa\_ Sf[US\_ W fWsa gegãda bWã e[eW S\_ Wã\_ a STSj afil WãUë baVWbdãeVg[dbScS S VŠbSTž

**Tž** 3bòa V[ebae[f]ha YVsdã Sh[ea VVhal z☛, DW[efcSžBadXshad bdWãja` Wã eVg VVWa` a e[eW S W fS` a WfSva VV USVSeFdS\_ Wfa VV\_ bdWãça V[Y[fS^ãWãV]XUSVãZbdWãja` Wã \_ Wã\_ a VVã eaTdã eW eadfehVWã eVg[ Va Se[` efdgëVã VV hal ž

**Už** EWã USVSeFdS\_ Wfa VS[\_ bdWãça V[Y[fS^ãdTW\_ žegUW[Vã a e[eW S YVWã a Sh[ea VVhal z☛, 5SVSeFdã dVŠ`! SVa La\_ egUWããž DW[efcSžBadXshad bdWãja` Wã eVg VVWa` WV fS V[dVŠ\_ W fW a bobj[\_ a WfSva VVUSVSeFdS\_ Wfa VV\_ bdWãça V[Y[fS^ãWã USVSeFdS\_ Wfa VS[\_ bdWãça V[Y[fS^ãSZSdã e[eW S YVWã a Sh[ea VVhal z☛, BadXshad bdWãja` Wã eVg VVWa` ahS\_ W fW WãVãVWã VŠbSTž

- d. O sistema retorna automaticamente ao estado de autenticação quando os 10 dedos e o cartão são cadastrados, o cartão de gerenciamento é passado uma vez ou a operação expira por tempo limite.

## (2)...**Pressione o(s) dedo(s) primeiro.**

- a. Pressione o mesmo dedo sobre o sensor três vezes, seguindo as instruções de voz e adotando a colocação correta da impressão digital. Se o cadastramento da impressão digital for bem-sucedido, o sistema gera o aviso de voz "🔊: Usuário número \*\*. Cadastro realizado com sucesso" e você pode prosseguir para a etapa b; se o registro da impressão digital falhar, o sistema gera o aviso de voz: "🔊: Por favor, pressione o seu dedo novamente" e retorna ao estado de cadastramento, aguardando que você pressione o dedo ou passe o cartão.
- b. Após gerar o aviso de voz "🔊: Registrar. Por favor, pressione o seu dedo ou passe o cartão", o sistema entra no estado de cadastramento das informações do usuário especificadas, aguardando que você passe o novo cartão ou pressione o dedo.
- c. Se o cadastramento do cartão for bem-sucedido, o sistema gera o aviso de voz "🔊: Cadastro realizado com sucesso. Registrar. Por favor, pressione o seu dedo" e entra diretamente no estado de cadastramento de impressão digital; se você pressionar um dedo que não foi cadastrado anteriormente e obter sucesso no cadastramento deste dedo, o sistema gera o aviso de voz: "🔊: Cadastro realizado com sucesso. Por favor, pressione o seu dedo ou passe o cartão" e você pode continuar cadastrando novas impressões digitais e cartão. Após cadastrar 10 impressões digitais, o sistema gera o aviso de voz "🔊: Registrar. Por favor, passe o seu cartão" para cadastrar o seu cartão, caso ele não tenha sido cadastrado anteriormente.

- d. O sistema retorna automaticamente ao estado de autenticação quando os 10 dedos e o cartão são cadastrados, o cartão de gerenciamento é passado uma vez ou a operação expira por tempo limite.
3. Se você já possui um ID atribuído, existem dois casos para você cadastrar sua(s) impressão(ões) digital(is) ou cartão:

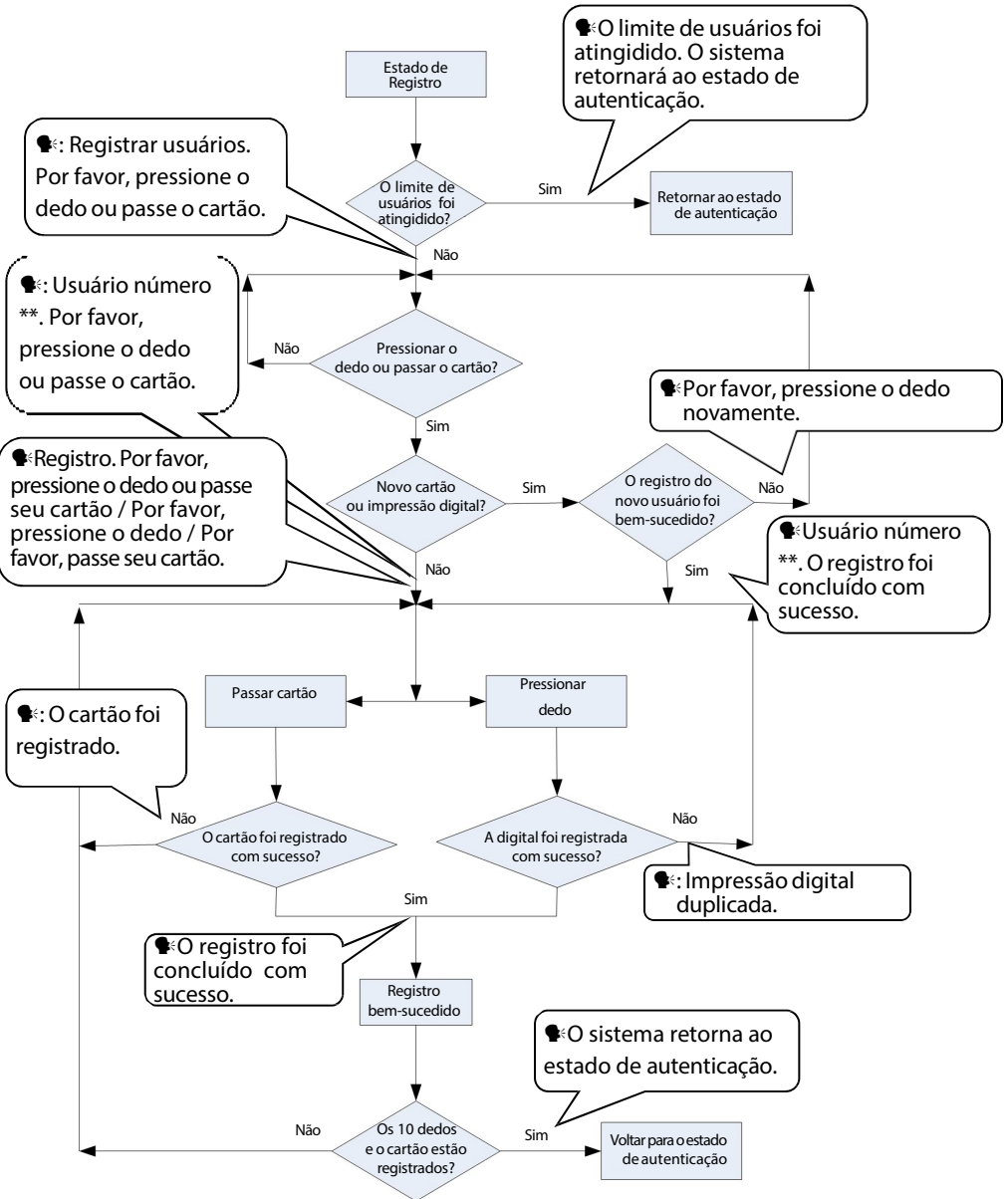
### **(1)... Cadastrar impressão digital quando você já possui um cartão cadastrado:**

- a. Após passar o cartão já cadastrado, o sistema irá gerar o aviso de voz "🔊: O cartão foi registrado. Usuário número . Registrar. Por favor, pressione o seu dedo" ( se refere ao ID atribuído a você; mesmo abaixo) e entrará no estado de cadastramento de impressão digital. Suas impressões digitais cadastradas irão substituir todas as impressões digitais anteriores.
  - b. Pressione o mesmo dedo sobre o sensor três vezes, seguindo as instruções de voz e adotando a colocação correta da impressão digital. Se o cadastramento da impressão digital for bem-sucedido, o sistema gera o aviso de voz "🔊: Cadastro realizado com sucesso. Por favor, pressione o seu dedo" e fica pronto para cadastrar a próxima impressão digital.
  - c. O sistema retorna automaticamente ao estado de autenticação quando 10 impressões digitais são cadastradas, o cartão de gerenciamento é passado uma vez ou a operação expira por tempo limite.
3. **Dicas:**
- As impressões digitais cadastradas nesta etapa não irão substituir todas as impressões digitais cadastradas anteriormente.
  - Nesse modo, a impressão digital do usuário que possui o cartão de gerenciamento não pode ser cadastrada, pois passar o cartão de gerenciamento irá retornar o sistema automaticamente ao estado de autenticação.

## **(2)... Registrar cartão e impressão digital quando você já possui impressão digital registrada.**

- a. Pressione o dedo com a impressão digital já registrada três vezes, seguindo as instruções de voz. Se você for identificado como a mesma pessoa em cada tentativa de autenticação, o sistema entrará no estado de registro de impressão digital.
- b. Após a geração do comando de voz “🗨️: Usuário número \*\*.  
Registrar. Por favor, pressione o dedo ou passe o cartão”, o sistema inicia o registro da sua impressão digital ou cartão. Suas impressões digitais registradas nesta etapa substituirão todas as suas impressões digitais anteriores.
- c. Caso o registro do cartão seja bem-sucedido, o sistema gera o comando de voz “🗨️: Registro realizado com sucesso. Registrar. Por favor, pressione o dedo” e entra diretamente no estado de registro de impressão digital; se você pressionar um dedo que não foi registrado anteriormente e conseguir registrar esse dedo, o sistema gera o comando de voz: “🗨️: Registro realizado com sucesso. Por favor, pressione o dedo ou passe o cartão” e você pode continuar registrando novas impressões digitais e o cartão. Após registrar 10 impressões digitais, o sistema gera o comando de voz “🗨️: Registrar. Por favor, passe o cartão” para registrar o seu cartão, caso ele ainda não tenha sido registrado.
- d. O sistema retorna automaticamente ao estado de autenticação quando são registrados 10 dedos e o cartão, o cartão de administração é passado uma vez ou o tempo de operação expira.

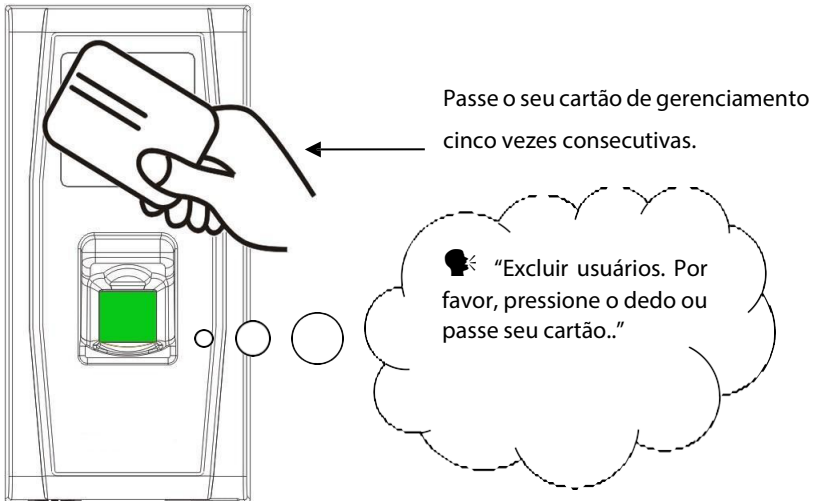
O fluxograma é mostrado abaixo:



### 3.1.3 Excluir um único usuário

**Os passos de operação para a exclusão simples de um único usuário são:**

1. No estado de autenticação, passe o seu cartão de gestão cinco vezes consecutivas para entrar no estado de exclusão simples de um único usuário (passe o seu cartão mais uma vez para retornar ao estado de autenticação).



2. Pressione o dedo no sensor de impressão digital ou passe o cartão sobre o leitor de cartões.

#### **(1)..Pressione o dedo no sensor para excluir um usuário.**

Pressione um dos seus dedos cadastrados corretamente no sensor. Se a autenticação for bem-sucedida, o sistema gerará o aviso sonoro “🔔: Usuário número. Exclusão realizada com sucesso. Excluir usuários. Por favor, pressione o dedo ou passe seu cartão.” ( indica o número de identificação do usuário) e retornará automaticamente ao estado de exclusão. Se a autenticação falhar, o sistema emitirá o aviso sonoro “🔔: Por favor, tente novamente.”



**(2). .Passe o seu cartão sobre o leitor para excluir um usuário.**

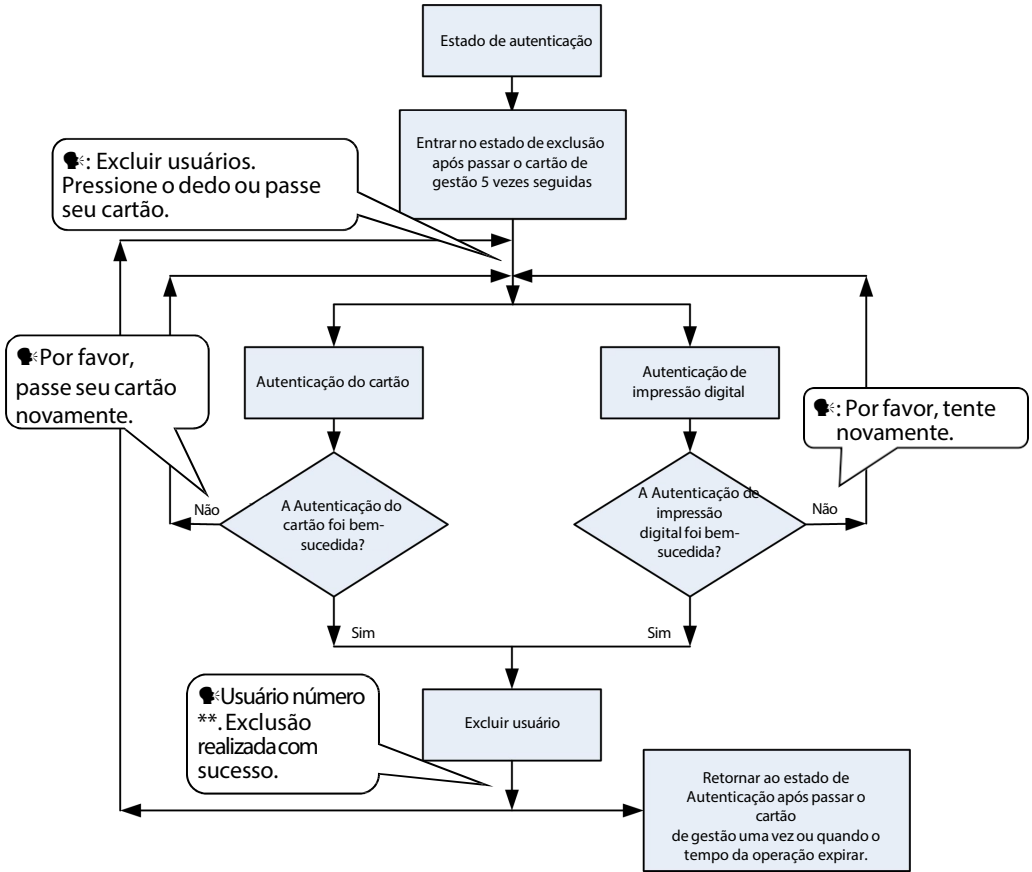
Passar um cartão registrado sobre o leitor. Se a autenticação for bem-sucedida, o sistema gerará o aviso sonoro "🔊: Usuário número \*\*. Exclusão realizada com sucesso. Excluir usuários. Por favor, pressione o dedo ou passe seu cartão." e retornará automaticamente ao estado de exclusão. Se a autenticação falhar, o sistema emitirá o aviso sonoro "🔊: Por favor, passe seu cartão novamente."

3. Se você passar o seu cartão de gestão mais uma vez ou se o tempo de operação expirar, o sistema retornará ao estado de autenticação.



**Dica:** No modo de exclusão simples de um único usuário, o usuário do cartão de gestão não pode ser excluído, pois passar o cartão de gestão fará com que o sistema retorne ao estado de autenticação.

### Procedimento de Exclusão de um Único Usuário:



## 3.2 Autenticação de Usuário

### Passos de Operação:

1. Quando o dispositivo estiver no estado de autenticação, o sistema emitirá o aviso sonoro "🔔: Verificar usuários. Por favor, pressione o dedo ou passe seu cartão."
2. Iniciar a autenticação do usuário. O dispositivo suporta dois modos de autenticação, autenticação de impressão digital e autenticação de cartão.

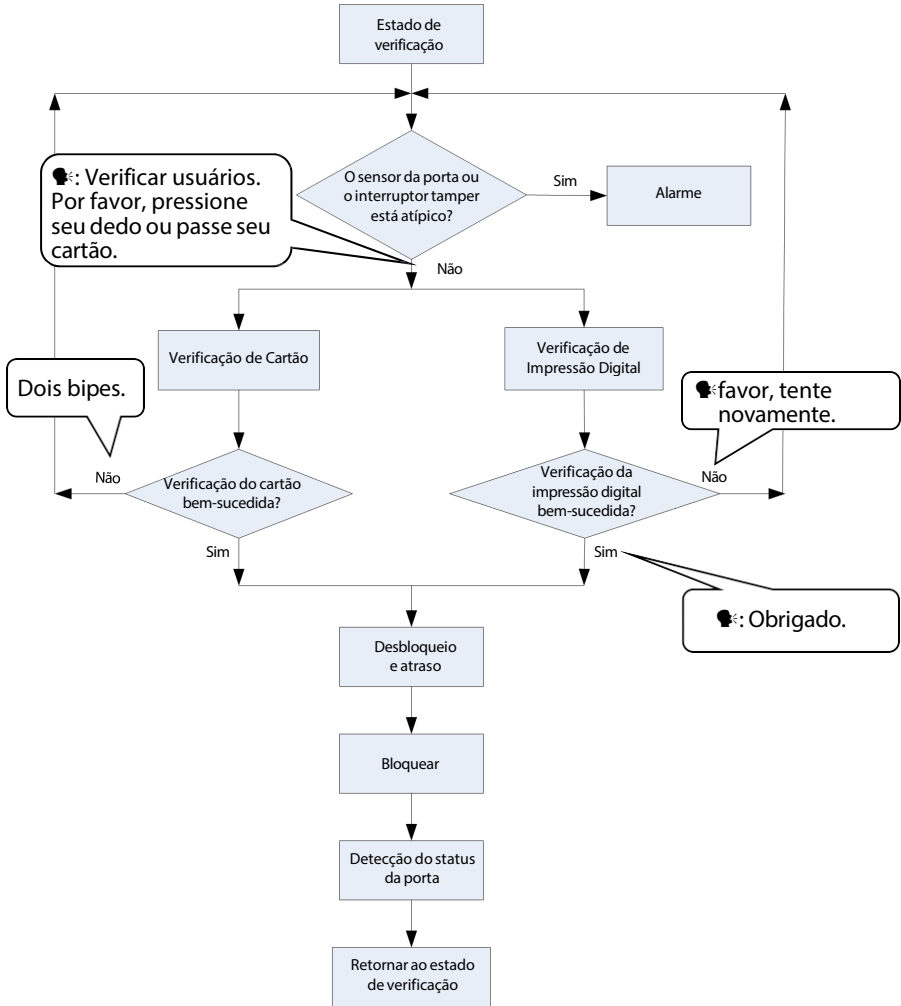
#### (1)..Autenticação de Impressão Digital


Pressione o dedo no sensor de impressão digital de forma adequada. Se a autenticação for bem-sucedida, o sistema emitirá o aviso sonoro "🔔: Obrigado" e simultaneamente acionará um sinal de desbloqueio. Se a autenticação falhar, o sistema emitirá o aviso sonoro "🔔: Por favor, tente novamente."

#### (2)..Autenticação de Cartão

Passe o cartão sobre o leitor de cartões. Se a autenticação for bem-sucedida, o sistema gera o aviso de voz "🔔: Obrigado." e, simultaneamente, aciona um sinal de desbloqueio. Se a autenticação falhar, o sistema emite dois bipes.

**O fluxograma de verificação do usuário é mostrado abaixo:**



 **Dica:** O administrador pode desbloquear utilizando suas impressões digitais registradas em vez de um cartão de gerenciamento.

### 3.3 Disco USB

O usuário pode realizar o download de registros, o download de usuários, o upload de usuários e a atualização de firmware através de um disco USB.

- a. **Download de Registros:** Faça o download dos registros de acesso de todos os usuários do dispositivo para um disco USB.
- b. **Download de Usuários:** Faça o download de todas as informações dos usuários, como impressões digitais e números de cartão, do dispositivo para um disco USB.
- c. **Upload de Usuários:** Faça o upload das informações do usuário de um disco USB para o dispositivo.
- d. **Atualização de Firmware:** Atualize o firmware do dispositivo através de um disco USB.

#### Operações do disco USB:

Se você conectar um disco USB ao dispositivo, o sistema irá automaticamente apresentar as operações em sequência.

- (1). Após conectar um U-disk ao dispositivo, você pode passar o cartão de gerenciamento uma vez para entrar no estado de gerenciamento do disco USB.
- (2). O sistema gera o aviso de voz "🔊: \*\*\*\*. Por favor, passe o seu cartão gerenciamento para confirmação." (\*\*\*\* indica os quatro itens de operação dos passos A - D em sequência; mesmo abaixo)
- (3). Se você deseja realizar a operação, passe o cartão de gerenciamento para confirmação. Se a sua operação for bem-sucedida, o sistema irá gerar o aviso de voz "🔊: operação foi concluída com sucesso." e solicitará que você prossiga para o próximo passo. Após concluir os quatro itens,

o sistema gera o aviso de voz " 🔔: O sistema retorna ao estado de verificação." Se a sua operação falhar, o sistema irá gerar o aviso de voz " 🔔: A operação falhou. O sistema retorna ao estado de verificação

- (4). Se você não passar o cartão de gerenciamento, o sistema irá automaticamente pular esta etapa em 5 segundos e o guiará para o próximo passo. Após concluir os quatro itens, o sistema retornará automaticamente ao estado de verificação.



Por favor, não atualize o firmware por conta própria, pois isso pode causar problemas e afetar o uso normal do dispositivo. Entre em contato com nossos distribuidores para suporte técnico ou notificação de atualização.

## 3.4 Interruptor Tamper

O interruptor de violação é pressionado e mantido pressionado com a tampa traseira. Quando o dispositivo é desmontado, o interruptor de violação será levantado e, em seguida, enviará um sinal de alarme para acionar um alarme.

**Limpar Alarme:** O usuário pode limpar o alarme colocando o ímã de volta no interruptor de violação.

**Restaurar Configurações de Fábrica:** As configurações de fábrica podem ser restauradas através do interruptor de violação. Ligue o dispositivo, coloque o ímã no interruptor de violação seis vezes após ele exibir a mensagem "Verificar usuários. Por favor, pressione seu dedo ou passe seu cartão", em seguida, pressione o dedo ou passe o cartão por 30 segundos, mas não mais do que 60

segundos. Após a restauração bem-sucedida, o dispositivo irá reiniciar automaticamente.

**Dicas:**

1. Os dados do usuário serão apagados, incluindo o administrador e os usuários comuns.
2. O endereço IP do dispositivo não será restaurado.

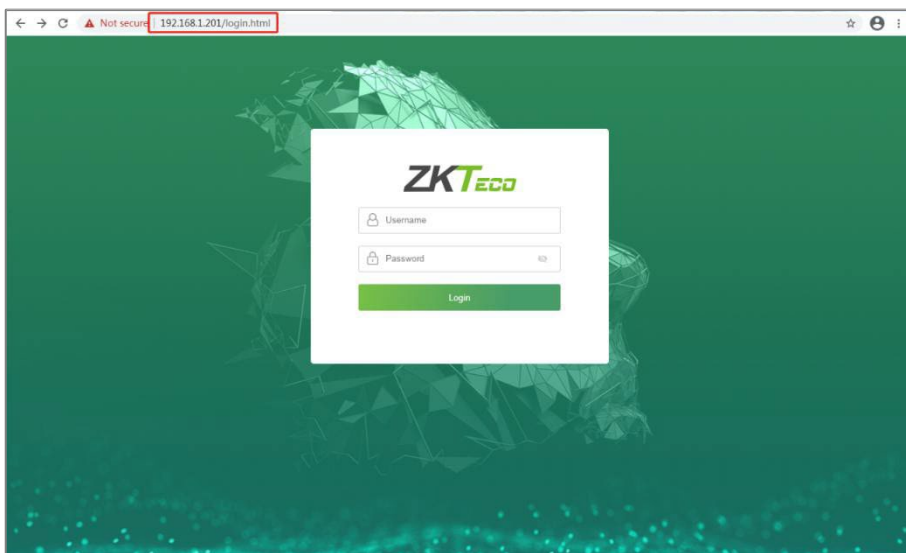
## 4 Servidor Web

O usuário pode abrir a aplicação web para configurar os parâmetros relevantes do dispositivo.

### 4.1 Login

Primeiro, conecte o dispositivo à Internet. Abra um navegador e digite o link: [https://endereço IP \(do dispositivo\)](https://endereço IP (do dispositivo)) para acessar a interface de login. (por exemplo, o endereço IP padrão do dispositivo é 192.168.1.201 e o link do servidor web é <https://192.168.1.201>).

**Observação:** O endereço IP do seu PC e do dispositivo devem estar na mesma segmento de rede, caso contrário, você não poderá abrir o link. Se você modificar o endereço IP do dispositivo em Configurações - Configurações de Comunicação, o link do servidor web será alterado de acordo.



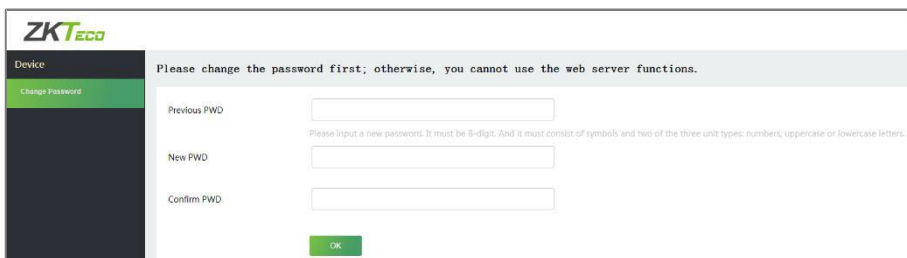


Digite o nome de usuário e senha

**Nome de usuário:** admin (padrão)

**Senha:** admin@123 (padrão)

Após fazer o login com sucesso, você será redirecionado para a página de **Alteração de Senha**. Digite sua senha anterior, nova senha e confirme a nova senha. Em seguida, clique em **OK**, como mostrado abaixo:



The screenshot shows a web interface for changing a password. At the top left is the ZKTECO logo. Below it is a dark sidebar with a 'Device' menu and a 'Change Password' option highlighted in green. The main content area has a light gray header with the message: 'Please change the password first; otherwise, you cannot use the web server functions.' Below this, there are three input fields: 'Previous PWD', 'New PWD', and 'Confirm PWD'. A small note below the 'New PWD' field states: 'Please input a new password. It must be 8-digit. And it must consist of symbols and two of the three unit types: numbers, uppercase or lowercase letters.' At the bottom right of the form is a green 'OK' button.

### **Observação:**

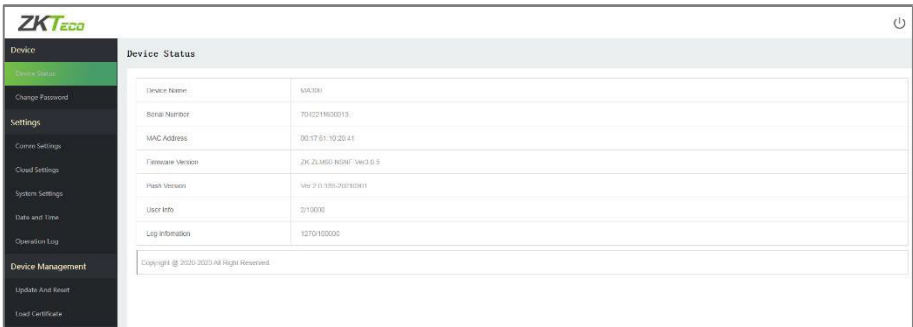
1. A senha deve ser alterada ao fazer o login pela primeira vez.
2. A nova senha deve ter 8 dígitos e deve conter símbolos e pelo menos dois dos três tipos de caracteres: números, letras maiúsculas ou letras minúsculas.
3. Se você esquecer a senha do servidor web, entre em contato com nossa equipe de pós-vendas.

Após a modificação ser bem-sucedida, você será redirecionado para a interface de login.

## 4.2 Dispositivo

### 4.2.1 Estado do Dispositivo

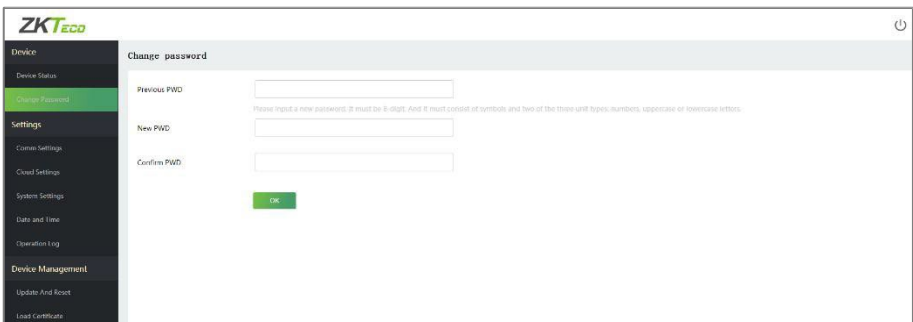
Clique em **Estado do Dispositivo** para visualizar o nome do dispositivo, número de série, endereço MAC, etc. do dispositivo atual.



### 4.2.2 Alterar Senha

Clique em **Alterar Senha** para modificar a senha do usuário.

Digite sua senha anterior, nova senha e confirme a senha, em seguida, clique em **OK**.



## 4.3 Configurações

### 4.3.1 Configurações de Comunicação

Quando o dispositivo precisa se comunicar com a rede, é necessário configurar as configurações de IP.



#### A descrição dos campos é a seguinte

**DHCP:** O DHCP (Protocolo de Configuração Dinâmica de Host) aloca dinamicamente os endereços IP para os clientes por meio do servidor. Se o DHCP estiver habilitado, os endereços IP não podem ser configurados manualmente.

**Endereço IP:** O valor padrão é 192.168.1.201, ele pode ser modificado de acordo com os parâmetros de rede disponíveis.

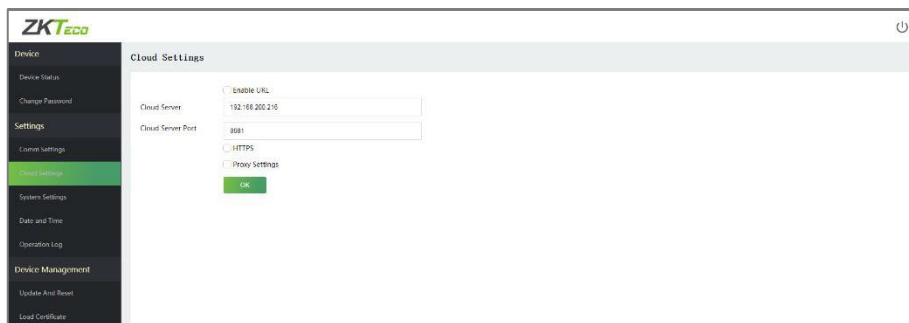
**Máscara de Sub-rede:** O valor padrão é 255.255.255.0, ele pode ser modificado de acordo com os parâmetros de rede disponíveis.

**Gateway:** O valor padrão é 192.168.1.1, ele pode ser modificado de acordo com os parâmetros de rede disponíveis.

**DNS:** O endereço DNS padrão é 0.0.0.0. Ele pode ser modificado de acordo com a disponibilidade da rede.

## 4.3.2 Configurações de Nuvem

Podemos nos conectar ao servidor em nuvem configurando as Configurações do Servidor em Nuvem.



**A descrição dos campos é a seguinte:**

**Habilitar URL:** Quando essa função está habilitada, o modo de nome de domínio "http://..." é usado, como http://www.XYZ.com (XYZ representa o nome de domínio). Quando esse modo está DESATIVADO, você precisa inserir o endereço IP e a porta para se conectar ao servidor web.

**Servidor em Nuvem:** O endereço IP do servidor.

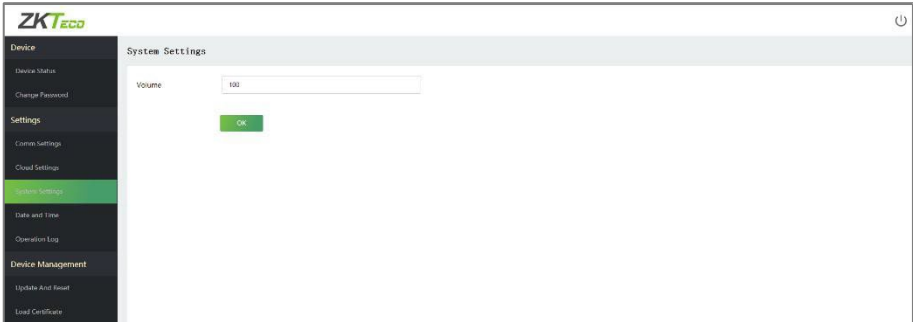
**Porta do Servidor em Nuvem:** A porta do servidor.

**HTTPS:** Habilita o modo HTTPS ao marcar a caixa de seleção. Isso ajuda a se conectar ao software ZKBioAccess (que é a versão https).

**Configurações de Proxy:** O endereço IP e o número da porta do servidor de proxy são definidos manualmente quando o proxy está habilitado.

### 4.3.3 Configurações do Sistema

Clique em **Configurações do Sistema** para definir o volume do dispositivo.  
Digite o valor do volume e clique em **OK**.

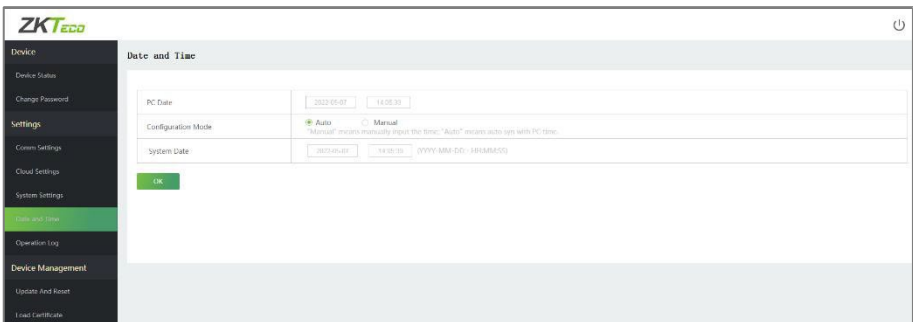


A descrição dos campos é a seguinte:

**Volume:** Ajuste o volume do dispositivo, que pode ser definido entre 0 e 100.

### 4.3.4 Data e Hora

Clique em **Data e Hora** para definir a data e hora do dispositivo.



A descrição dos campos é a seguinte:

**Automático:** Sincroniza automaticamente a hora do PC.

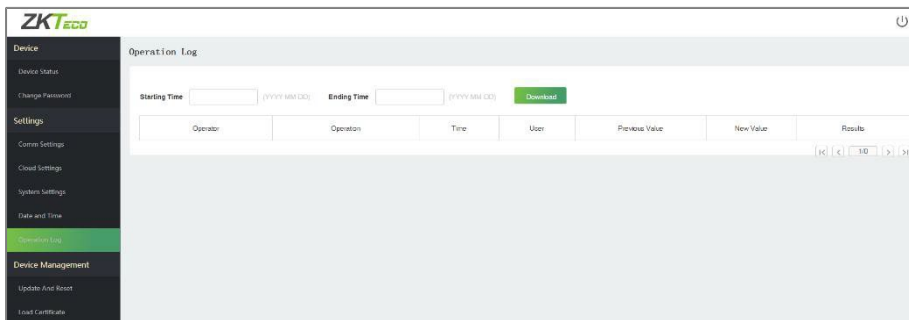
**Manual:** É necessário inserir manualmente a data e a hora.

**Observação:** O formato de data deve ser YYYY-MM-DD-HH:MM:SS.

### 4.3.5 Registros de Operação

Clique em **Registro de Operação** para visualizar todos os registros de operação do dispositivo.

**Download:** Selecione o horário de início e término e clique em download. O registro de operação do tempo selecionado será baixado automaticamente.



## 4.4 Gerenciamento de Dispositivos

### 4.4.1 Atualização e Redefinição

Clique em **Atualização e Redefinição** para configurar as opções de atualização, restauração de fábrica e reinicialização do dispositivo.



### A descrição dos campos é a seguinte:

**Atualização:** Clique em **Por favor, selecione um arquivo**, o formato do arquivo deve ser emfw.cfg e o tamanho deve ser inferior a 200 MB.

Clique em **OK** para concluir a operação de atualização do firmware.

**Redefinição de Fábrica:** A função de Redefinição de Fábrica restaura as configurações do dispositivo, como configurações de comunicação e configurações do sistema, para as configurações padrão de fábrica.



#### Observação:

1. A senha do servidor web e o endereço IP do dispositivo serão restaurados para o padrão.
2. Os dados do usuário não serão apagados.

**Reinicialização:** Reinicia o dispositivo.

## 4.4.2 Carregar Certificados

Clique em **Carregar Certificado** para enviar o arquivo de certificado do dispositivo e o arquivo de chave privada. Clique em **Por favor, selecione um arquivo**, faça o upload do arquivo de certificado e do arquivo de chave privada e clique em **OK** para concluir a operação de envio de arquivo.

The screenshot shows the 'Load Certificate' interface in the ZKTeco Device Management system. It features a sidebar on the left with the following menu items: Device, Device Status, Change Password, Settings (selected), Common Settings, Cloud Settings, System Settings, Date and Time, Operation Log, Device Management, and Update Fw/Boot. The 'Load Certificate' option is highlighted in green. The main content area is titled 'Load Certificate' and includes a red warning note: 'Note: Please load the certificate file first and then load the private key file.' Below the note, there are two file selection sections. The first section is for the certificate file, with the label 'Please specify a certificate file (.cer)', a green 'Please select a file.' button, and a text input field for 'File Name:'. A green 'OK' button is located to the right of the input field. The second section is for the private key file, with the label 'Please specify the private key file (.key)', a green 'Please select a file.' button, and a text input field for 'File Name:'. A green 'OK' button is located to the right of the input field.

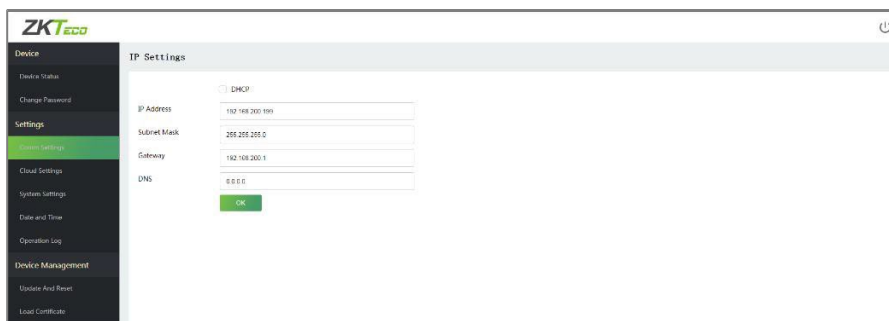


**Observação:** Por favor, carregue primeiro o arquivo de certificado e, em seguida, o arquivo de chave privada.

## 5 Conectar ao Software ZKBioAccess

### 5.1 Defina o Endereço de Comunicação

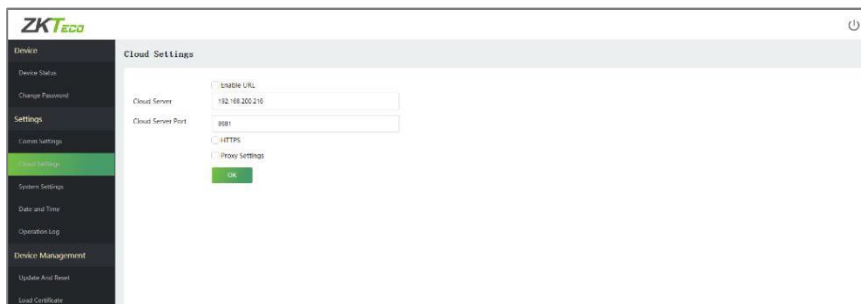
1. Faça login no servidor web. Clique em Configurações de Comunicação para definir o endereço IP e o Gateway do dispositivo. (**Observação:** O endereço IP deve ser capaz de se comunicar com o servidor ZKBioAccess, preferencialmente na mesma segmento de rede que o endereço do servidor)



2. Clique em **Configurações de Nuvem** para definir o endereço do servidor e a porta do servidor.

**Servidor de Nuvem:** Defina como o endereço IP do servidor ZKBioAccess.

**Porta do Servidor de Nuvem:** Defina como a porta de serviço do ZKBioAccess (O valor padrão é 8088).

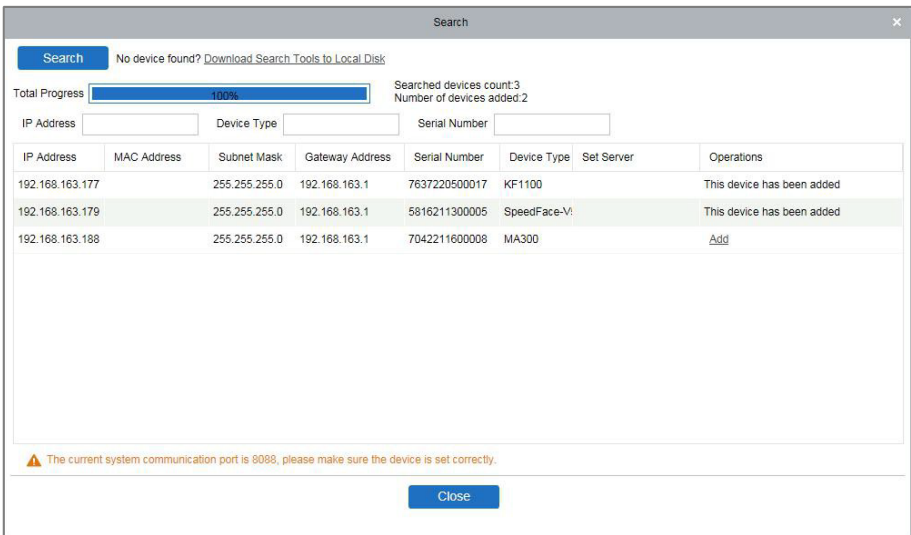




## 5.2 Adicionar Dispositivo ao Software

Você pode adicionar um dispositivo por meio de uma busca. O processo é o seguinte:

1. Clique em **Controle de Acesso > Dispositivo > Buscar Dispositivo**, para abrir a interface de busca.
2. Clique em **Buscar**, e será exibida a mensagem "**Buscando...**"
3. Após a busca, a lista e o número total de controladores de acesso serão exibidos.



The screenshot shows a window titled "Search" with a search button and a progress bar at 100%. Below the progress bar, there are input fields for IP Address, Device Type, and Serial Number. A table displays the search results with columns for IP Address, MAC Address, Subnet Mask, Gateway Address, Serial Number, Device Type, Set Server, and Operations. A warning message at the bottom states: "The current system communication port is 8088, please make sure the device is set correctly." A "Close" button is located at the bottom right of the window.

IP Address	MAC Address	Subnet Mask	Gateway Address	Serial Number	Device Type	Set Server	Operations
192.168.163.177		255.255.255.0	192.168.163.1	7637220500017	KF1100		This device has been added
192.168.163.179		255.255.255.0	192.168.163.1	5816211300005	SpeedFace-VI		This device has been added
192.168.163.188		255.255.255.0	192.168.163.1	7042211600008	MA300		<a href="#">Add</a>

4. Clique em **Adicionar** para adicionar o dispositivo.
5. Após a adição ser bem-sucedida, o dispositivo será exibido na lista de dispositivos.

## 5.3 Adicionar Pessoas ao Software

1. Clique em **Pessoal > Pessoa > Nova**.

2. Insira os detalhes necessários do usuário e clique em **OK** para salvar o usuário.
3. Clique em **Acesso > Dispositivo > Controle > Sincronizar Todos os Dados** nos Dispositivos para sincronizar todos os dados com o dispositivo.

**Observação:** Para outras operações específicas, por favor consulte o Manual do Usuário do ZKBioAccess.

## 6 Apêndice

### 6.1 Lista de Parâmetros

A tabela a seguir lista os parâmetros funcionais básicos do dispositivo.

Item	Descrição
Alimentação	12V, 3A
Função	Dispositivo de controle de acesso, status da porta/ alarme/fechadura/chave de controle de acesso
	Uma entrada Wiegand e uma saída Wiegand
Quantidade de usuários	10.000 (impressão digital e cartão de identificação)
Capacidade de registros	100.000 registros
Capacidade de registro (impressão digital/cartão)	1.500 impressões digitais / 10.000 cartões
Modo de verificação	Cartão ID (IC / HID), impressão digital
Comunicação	TCP / IP, RS485, Disco USB
Alto-falante	Indicação de voz
LED	Indicação bicolor (vermelho/verde)

## 6.2 Política de Privacidade

### Aviso:

Para ajudá-lo a utilizar melhor os produtos e serviços da ZKTeco e suas afiliadas, doravante referidos como "nós", "nossa" ou "nossos", o provedor de serviços inteligentes, coletamos consistentemente suas informações pessoais. Como entendemos a importância de suas informações pessoais, levamos sua privacidade a sério e formulamos esta política de privacidade para proteger suas informações pessoais. Listamos abaixo as políticas de privacidade para compreender precisamente os dados e as medidas de proteção de privacidade relacionadas aos nossos produtos e serviços inteligentes.

**Antes de usar nossos produtos e serviços, leia atentamente e entenda todas as regras e disposições desta Política de Privacidade. Se você não concordar com o acordo relevante ou qualquer um de seus termos, deverá interromper o uso de nossos produtos e serviços.**

### I. Informações Coletadas

Para garantir o funcionamento normal do produto e ajudar na melhoria do serviço, coletaremos as informações fornecidas voluntariamente por você ou fornecidas com sua autorização durante o registro e uso, ou geradas como resultado do seu uso dos serviços.

1. Informações de Registro do Usuário: No seu primeiro registro, o modelo de características (modelo de impressão digital/modelo de rosto/modelo de palma) será salvo no dispositivo de acordo com o tipo de dispositivo selecionado para verificar a semelhança única entre você e o ID de usuário que você registrou. Você pode opcionalmente inserir seu Nome e Código. As informações acima são necessárias para você usar nossos produtos.

Se você não fornecer tais informações, não poderá usar algumas funcionalidades do produto regularmente.

2. **Informações do produto:** De acordo com o modelo do produto e a permissão concedida por você ao instalar e usar nossos serviços, as informações relacionadas ao produto em que nossos serviços são utilizados serão coletadas quando o produto estiver conectado ao software, incluindo o Modelo do Produto, Número da Versão do Firmware, Número de Série do Produto e Informações de Capacidade do Produto. Ao conectar seu produto ao software, leia atentamente a política de privacidade específica do software.

## **II. Segurança e Gerenciamento do Produto**

1. Ao usar nossos produtos pela primeira vez, você deve configurar o privilégio de administrador antes de realizar operações específicas. Caso contrário, você receberá lembretes frequentes para definir o privilégio de administrador ao entrar na interface do menu principal. Se você ainda não definir o privilégio de administrador após receber o aviso do sistema, você deve estar ciente do possível risco de segurança (por exemplo, os dados podem ser modificados manualmente).
2. Todas as funções de exibição de informações biométricas estão desativadas em nossos produtos por padrão. Você pode escolher Menu > Configurações do Sistema para definir se deseja exibir as informações biométricas. Se você habilitar essas funções, assumimos que você está ciente dos riscos de segurança da privacidade pessoal especificados na política de privacidade.
3. Por padrão, apenas o seu ID de usuário é exibido. Você pode configurar se deseja exibir outras informações de verificação do

usuário (como Nome, Departamento, Foto, etc.) sob o privilégio de Administrador. **Se você optar por exibir tais informações, assumimos que você está ciente dos possíveis riscos de segurança (por exemplo, sua foto será exibida na interface do dispositivo).**

4. A função da câmera está desativada em nossos produtos por padrão. Se você deseja habilitar essa função para tirar fotos de si mesmo para registro de presença ou tirar fotos de pessoas desconhecidas para controle de acesso, o produto ativará o tom de aviso da câmera. **Uma vez que você habilitar essa função, assumimos que você está ciente dos possíveis riscos de segurança.**
5. Todos os dados coletados por nossos produtos são criptografados utilizando o algoritmo AES 256. Todos os dados enviados pelo Administrador para nossos produtos são automaticamente criptografados usando o algoritmo AES 256 e armazenados com segurança. Se o Administrador fizer o download de dados de nossos produtos, assumimos que você precisa processar os dados e está ciente do potencial risco de segurança. Nesse caso, você assume a responsabilidade pelo armazenamento dos dados. Você deve estar ciente de que alguns dados não podem ser baixados por motivos de segurança dos dados.
6. Todas as informações pessoais em nossos produtos podem ser consultadas, modificadas ou excluídas. Se você não usar mais nossos produtos, por favor, apague seus dados pessoais.

### III. Como lidamos com informações pessoais de menores de idade

Nossos produtos, site e serviços são principalmente projetados para adultos. Sem o consentimento dos pais ou responsáveis legais, os

menores não devem criar sua própria conta. Se você é menor de idade, é recomendado que você peça aos seus pais ou responsáveis legais para lerem atentamente esta Política e que você só utilize nossos serviços ou informações fornecidas por nós com o consentimento deles.

Iremos utilizar ou divulgar informações pessoais de menores de idade coletadas com o consentimento de seus pais ou responsáveis legais somente se e na medida em que tal uso ou divulgação for permitido por lei, ou se obtivermos o consentimento explícito de seus pais ou responsáveis legais, e se tal uso ou divulgação tiver como objetivo proteger os menores.

Ao percebermos que coletamos informações pessoais de menores de idade sem o consentimento prévio de pais verificáveis, iremos excluir tais informações o mais rápido possível.

#### **IV. Outros**

Você pode visitar o site

[https://www.zkteco.com/cn/index/Index/privacy\\_protection.html](https://www.zkteco.com/cn/index/Index/privacy_protection.html) to

para obter mais informações sobre como coletamos, usamos e armazenamos com segurança suas informações pessoais. Para acompanhar o rápido desenvolvimento da tecnologia, ajustar as operações comerciais e atender às necessidades dos clientes, iremos constantemente deliberar e otimizar nossas medidas e políticas de proteção de privacidade. Fique à vontade para visitar nosso site oficial a qualquer momento para conhecer nossa política de privacidade mais recente.

## 6.3 Operação Ecologicamente Correta



O "período de operação ecologicamente correto" do produto refere-se ao tempo durante o qual este produto não liberará nenhuma substância tóxica ou perigosa quando usado de acordo com os pré-requisitos deste manual. O período de operação ecologicamente correto especificado para este produto não inclui baterias ou outros componentes que se desgastam facilmente e devem ser substituídos periodicamente. O período operacional ecologicamente correto da bateria é de 5 anos.

### Substâncias tóxicas ou perigosas e suas quantidades

Nome do Componente	Substância/Elemento Perigoso/Tóxico					
	Chumbo (Pb)	Mercúrio (Hg)	Cádmio (Cd)	Cromo hexavalente (Cr6+)	Bifenilos polibromados (PBB)	Éteres difenílicos polibromados (PBDE)
Resistores	x	o	o	o	o	o
Capacitores	x	o	o	o	o	o
Indutores	x	o	o	o	o	o
Diodo	x	o	o	o	o	o
Componentes ESD	x	o	o	o	o	o
Buzzer	x	o	o	o	o	o



Adaptador	×	○	○	○	○	○
Parafusos	○	○	○	×	○	○

○: indica que a quantidade total de conteúdo tóxico em todos os materiais homogêneos está abaixo do limite, conforme especificado no SJ/T 11363—2006.

×: indica que a quantidade total de conteúdo tóxico em todos os materiais homogêneos excede o limite, conforme especificado no SJ/T 11363—2006.

**Observação:** 80% dos componentes deste produto são fabricados utilizando materiais que não são tóxicos e ecologicamente corretos. Os componentes que contêm toxinas ou elementos nocivos são incluídos devido às atuais limitações econômicas ou técnicas que impedem sua substituição por materiais não tóxicos.

# Garantia

**Este produto é garantido pela ZKTeco por um período de 3 meses (garantia legal), acrescidos de 9 meses de garantia adicional (garantia contratual), em um total de 1 ano, contra eventuais defeitos de material ou fabricação, desde que observadas as seguintes condições:**

- a) A garantia se aplica exclusivamente a produtos fornecidos pela ZKTeco do Brasil ou por Revenda Autorizada ZKTeco no Brasil.
- b) O período de garantia será contado a partir da data de emissão da nota fiscal do produto.
- c) Durante a garantia legal estão cobertos os custos de peças e serviços de reparo, que deverão ser realizados obrigatoriamente em Assistência Técnica ZKTeco ou na própria fábrica, conforme orientação da ZKTeco. Para o período de garantia contratual estão cobertos apenas os custos de peças que eventualmente necessitem substituição para reparo do produto, ficando excluídos os custos em relação aos serviços de manutenção (mão de obra), a remoção do produto (envio e retorno) e a visita/estadia de técnico especializado, se aplicável.
- d) Detectado o defeito no produto, o usuário deverá entrar em contato com a ZKTeco nos canais de comunicação disponíveis em <https://www.zkteco.com.br/suporte/>, fornecendo informações sobre os produtos e problemas observados por meio do preenchimento e envio do formulário de Remessa de Material para Assistência Técnica (RMA) disponível em <https://www.zkteco.com.br/manutencao/>.
- e) Recebidas as informações e o RMA, a ZKTeco analisará o caso e informará ao usuário sobre os próximos passos, bem como sobre a documentação que deve ser encaminhada em caso de envio do produto para a ZKTeco ou Assistência Técnica ZKTeco e/ou sobre opções para agendamento de visita técnica, quando aplicável.
- f) Produtos enviados para a ZKTeco ou para Assistência Técnica ZKTeco sem notificação prévia e expressa autorização da ZKTeco não serão recebidos.
- g) O produto e as peças substituídas serão garantidas pelo restante do prazo original, sendo que as peças retiradas dos produtos e/ou produtos eventualmente descartados serão de propriedade da ZKTeco.
- h) Em caso de dúvidas o usuário deverá entrar em contato com a ZKTeco nos canais de comunicação disponíveis em <https://www.zkteco.com.br/suporte/>

**Resultará nula e sem efeito esta garantia em caso de:**

- a) Produto que apresente lacres rompidos e/ou etiqueta de identificação violada.
- b) Uso anormal do produto, inclusive em desconformidade com seu manual, especificações, desenhos, folhas de instruções ou quaisquer outros documentos relacionados, bem como em capacidade além de seus limites e taxas prescritas.
- c) Uso indevido ou erro de instalação, operação, testes, armazenamento e/ou manuseio do produto.
- d) Manutenção e/ou alteração no produto não aprovada previamente pela ZKTeco.
- e) Defeitos e danos causados por agentes naturais (enchente, maresia e outros) ou exposição excessiva ao calor.
- f) Defeitos e danos causados pelo uso de software e/ou hardware não compatíveis com especificações do produto.
- g) Surtos e/ou picos de tensão na rede elétrica típicos de algumas regiões, para as quais deve-se utilizar dispositivos de proteção contra surtos elétricos.
- h) Fatos ou eventos imprevisíveis ou de difícil previsão e de força maior.
- i) Transporte do produto em embalagem ou de forma inadequada.
- j) Furto ou roubo.
- k) Desgaste natural do produto.
- l) Danos exclusivamente causados pelo usuário ou por terceiros.

Em nenhum caso a ZKTeco será responsável por indenização superior ao preço da compra do produto, por qualquer perda de uso, perda de tempo, inconveniência, prejuízo comercial, perda de lucros ou economias ou outros danos diretos ou indiretos, decorrentes do uso ou impossibilidade de uso do produto.

A ZKTeco reserva-se o direito de alterar as condições e procedimentos aqui estabelecidos independente de aviso prévio, sendo de responsabilidade do usuário verificar periodicamente eventuais atualizações, que estarão disponíveis em <https://www.zkteco.com.br/manutencao/>. Nenhuma Revenda Credenciada ou Assistência Técnica ZKTeco tem autorização para modificar as condições aqui estabelecidas ou assumir outros compromissos em nome da ZKTeco.

Telefone: (31) 3055-3530  
Endereço: Rodovia MG-010, KM 26  
Loteamento 12 - Bairro Angicos  
Vespasiano - MG - CEP: 33.206-240

[www.zkteco.com.br](http://www.zkteco.com.br)

