intelbras

# Manual do usuário
# Manual del usuario

**SS 3540 MF FACE EX**
**SS 3540 MF FACE BIO EX**

Português

intelbras

**SS 3540 MF FACE EX**
**SS 3540 MF FACE BIO EX**

## Controlador de acesso com reconhecimento facial

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

O dispositivo SS 3540 MF FACE EX / SS 3540 MF FACE BIO EX é um controlador de acesso com autenticação por reconhecimento facial, cartão RFID 13,56 MHz e senha. Com tela sensível ao toque de 4,3", é prático realizar cadastros e alterar configurações. Pode ser instalado em ambientes internos para liberar portas em geral, através do acionamento de fechaduras elétricas, eletroímãs ou solenoides.

ANATEL
11812-21-00160

Este equipamento não tem direito à proteção contra interferência prejudicial e não pode causar interferência em sistemas devidamente autorizados. Este é um produto homologado pela Anatel, o número de homologação se encontra na etiqueta do produto, para consultas utilize o link *sistemas.anatel.gov.br/sch.*

# Cuidados e segurança

- As instruções de segurança e operação devem ser guardadas para referências futuras.
- Use a fonte de alimentação que acompanha o produto.
- O produto deve ser utilizado em ambientes internos e externos com temperatura superior a -30 °C e inferior a 60 °C.
- A tentativa de abrir o produto pode danificá-lo e implica em perda do direito a garantia.
- Cuidado ao manejar os cabos para não danificá-los.
- Não sobrecarregue as tomadas ou extensões, pois pode causar incêndio ou choque elétrico.
- Instale-o em um local seguro.
- Não coloque ou instale o produto em lugares expostos a luz solar ou fontes de calor.
- Mantenha o produto longe de umidade, poeira ou fuligem.
- Instale o produto de forma vertical e em local estável, garantindo a correta fixação para que não caia causando danos ao equipamento.
- Limpe o produto com pano úmido em água ou seco. Não utilize produtos químicos ou abrasivos.
- Instale o produto em local ventilado e não bloqueie a ventilação do controlador de acesso.
- Use apenas acessórios recomendados pelo fabricante.
- LGPD - Lei Geral de Proteção de Dados Pessoais: este produto faz tratamento de dados pessoais, porém a Intelbras não possui acesso aos dados a partir deste produto. Este produto possui criptografia na transmissão e armazenamento dos dados pessoais.

**Atenção:** danos causados pelo não cumprimento das recomendações de instalação ou uso inadequado do produto não são cobertos pela garantia. Vide certificado de garantia do produto.

# Índice

# 1. Especificações técnicas

| Modelo | | SS 3540 MF FACE EX | SS 3540 MF FACE BIO EX |
|---|---|---|---|
| Tensão de alimentação | | 12 Vdc | |
| Potência | | 24 W | |
| Capacidade de chaveamento | | 2 A / 30 Vdc | |
| Temperatura de operação | | -30 °C a 60 °C | |
| Umidade de operação | | 5% a 95% | |
| Display | | 4,3" sensível ao toque (capacitivo) | |
| Câmeras | | 2 MP CMOS RGB e 2 MP CMOS IR | |
| Intervalo de reconhecimento facial | | Distância da câmera à face: 0,3 m a 1,5 m | |
| | | Altura do usuário: 0,9 m a 2,40 m | |
| Tempo de reconhecimento facial | | 0,2s | |
| Métodos de autenticação | | Reconhecimento facial, biometria digital, cartão, senha e QR code | |
| Interface de comunicação | | RS 485 e Wiegand | |
| Capacidade | Usuários | 6.000 | |
| | Faces | 6.000 | |
| | Digitais | 6.000 | |
| | Cartões | 6.000 | |
| | Senhas | 6.000 | |
| | Eventos | 150.000 | |
| Wi-Fi | Antena | Interna | |
| | Padrões | IEEE 802.11b, 802.11g, 802.11n | |
| | Frequência operacional | 2,4 GHz ~ 2,4835 GHz | |
| | Largura de banda | Suporta 20 MHz e 40 MHz | |
| | Protocolo de segurança | 64/128 bit WEP, WPA/WPA2, WPA-PSK/WPA2-PSK | |
| | Taxa de transmissão | 802.11b: até 11 Mbps<br>802.11g: até 54 Mbps<br>802.11n: até 300 Mbps (HT40) | |
| RFID | Modulação | ASK | |
| | Frequência | 13,56 MHz | |
| | Taxa de transmissão | 106 a 848 kbps | |
| | Código de emissão | 13M5K2D | |
| | Tipo antena | Interna | |
| Grau de proteção | | IP65 | |
| Dimensões (L × A × P) | | 87,5 × 174 × 22,5 mm | |

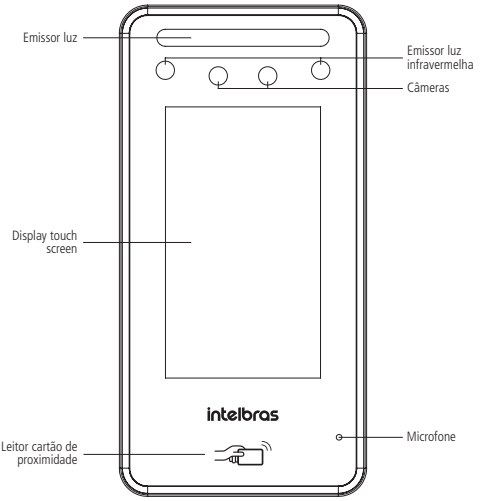
# 2. Características

- Fácil instalação.
- Visual moderno e funcional.
- Compatível e Defense IA.
- Integrado ao sistema MIP 1000 IP.
- Para uso em ambiente externo.
- Função anti-fake que impossibilita a autenticação por vídeo ou foto em meio físico ou digital.
- Suporta reconhecimento facial, biometria digital, leitor RFID, senha e QR code.
- Dupla câmera grande angular de 2 MP: uma de luz visível colorida (RGB) e outra de luz infravermelha (IR).
- Precisão de verificação de face >99,5%.
- Baixo índice de falsa rejeição.

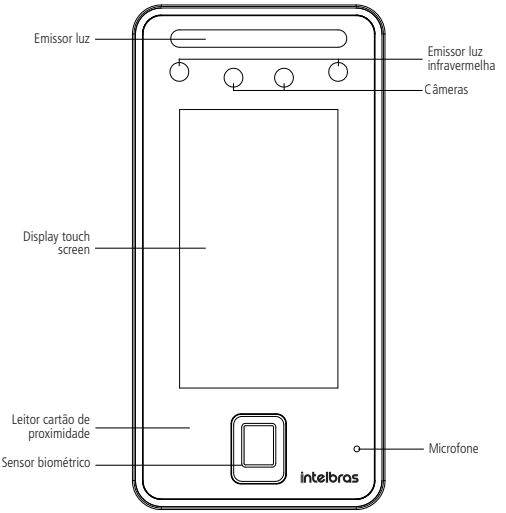
# 3. Conteúdo da embalagem

- 1× controlador de acesso SS 3540 MF FACE EX / SS 3540 MF FACE BIO EX
- 1× conjunto de buchas e parafusos
- 1× suporte para fixação em parede
- 1× fonte de alimentação
- 1× guia do usuário

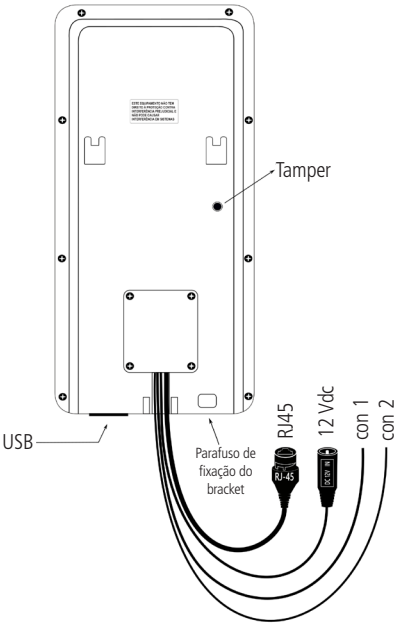
# 4. Produtos




*Visão frontal SS 3540 MF FACE EX*




*Visão frontal SS 3540 MF FACE BIO EX*




*Vista traseira SS 3540 MF FACE EX / SS 3540 MF FACE BIO EX*

## 4.1. Descrição dos cabos

### Interface de leitores (CON1)

| Cor | Nome | Descrição |
|---|---|---|
| Preto/marrom | PORTA_COM | Contato comum do relé de acionamento de liberação de acesso. |
| Preto/Amarelo | PORTA_NA | Contato normalmente aberto do relé de acionamento de liberação de acesso. |
| Preto/Roxo | PORTA_NF | Contato normalmente fechado do relé de acionamento de liberação de acesso. |
| Preto/Azul | GND | Referência para sinal de botão de saída e sensor de porta. |
| Preto/Cinza | SEN | Conexão para sensor de porta. |
| Preto/Verde | BOT | Conexão para botão de saída. |
| Branco/Verde | GND | Referência para a entrada de alarme. |
| Branco/Marrom | ALM_IN | Entrada de alarme. |

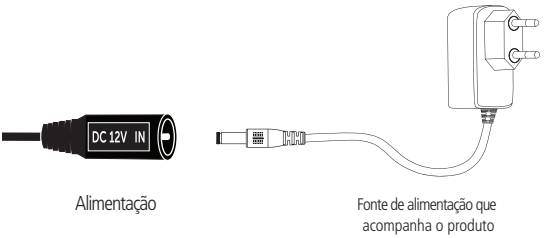
### Interface de leitores (CON2)

| Cor | Nome | Descrição |
|---|---|---|
| Amarelo | 485- | Sinal 485B ou 485- do barramento RS-485 / Saída B para integração com MIP. |
| Roxo | 485+ | Sinal 485A ou 485+ do barramento RS-485 / Saída A para integração com MIP. |
| Branco | WD1 | Entrada Wiegand D1 (para conectar um leitor auxiliar) / Saída Wiegand D1 (para conectar a outro controlador de acesso). |
| Verde | WD0 | Entrada Wiegand D0 (para conectar um leitor auxiliar) / Saída Wiegand D0 (para conectar a outro controlador de acesso). |
| Preto | GND | Referência para o barramento Wiegand. |
| Marrom | LED | Saída para sinalização de acesso para um leitor auxiliar / Entrada para receber a sinalização de acesso. |

# 5. Esquemas de ligação

## 5.1. Fonte de alimentação

Conecte a fonte de alimentação ao dispositivo e, em seguida, ligue-a na tomada.

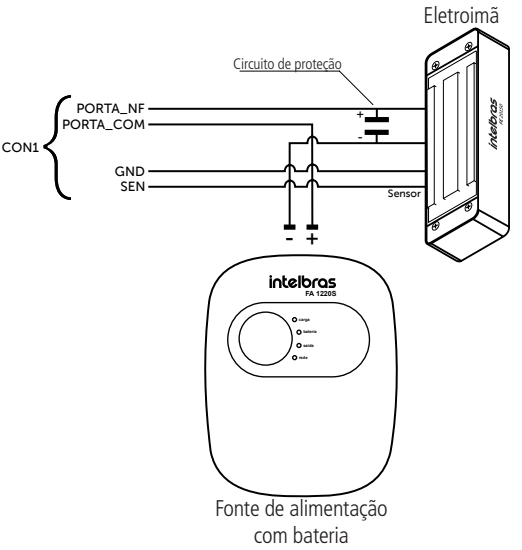



*Alimentação do produto*

***Obs.:*** *recomenda-se o uso de um nobreak para suprir situações de queda de energia.*

## 5.2. Fechaduras

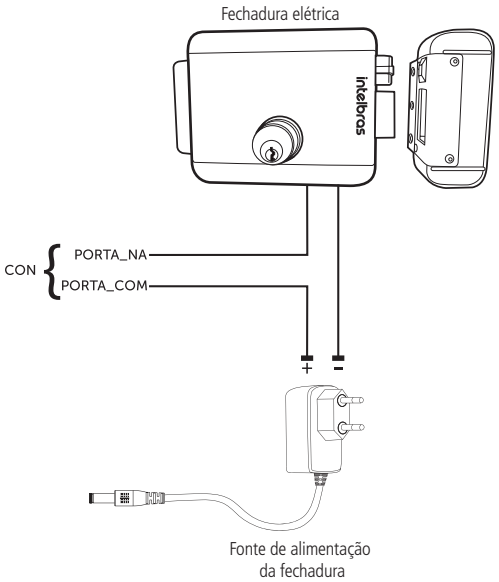
### Fechadura eletroímã



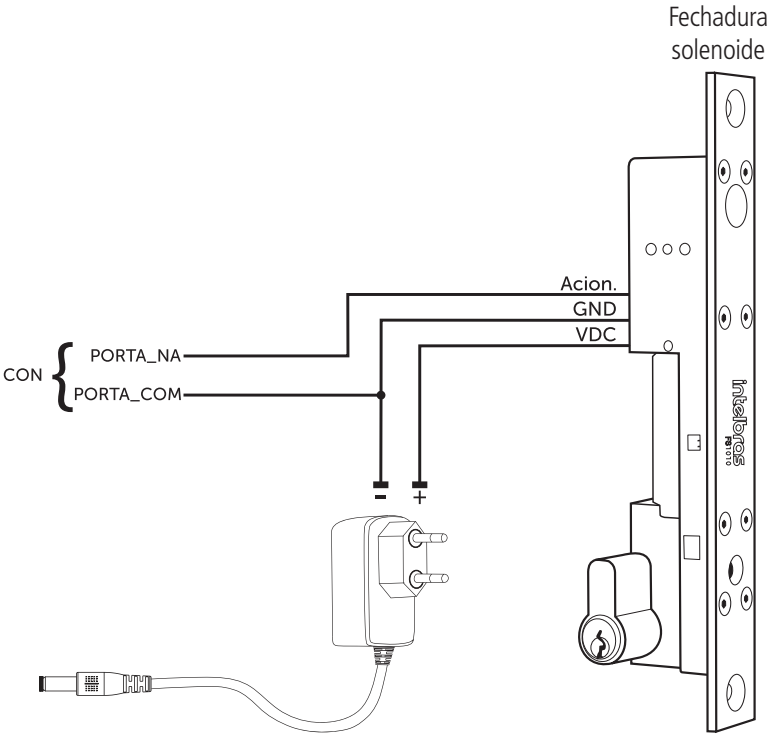

*Exemplo de ligação de fechadura eletroímã*

***Obs.:*** *caso a fechadura não possua sensor, desconsidere a ligação deste.*

**Fechadura elétrica**

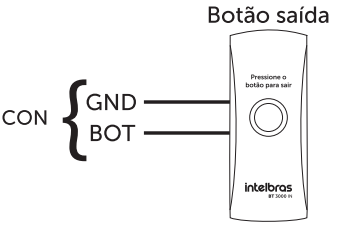



**Fechadura solenoide**




*Exemplo de ligação de fechadura solenoide*

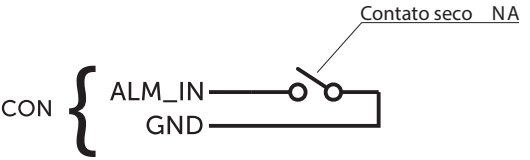
### 5.3. Botão de saída




*Exemplo de ligação de botão de saída*

### 5.4. Alarme

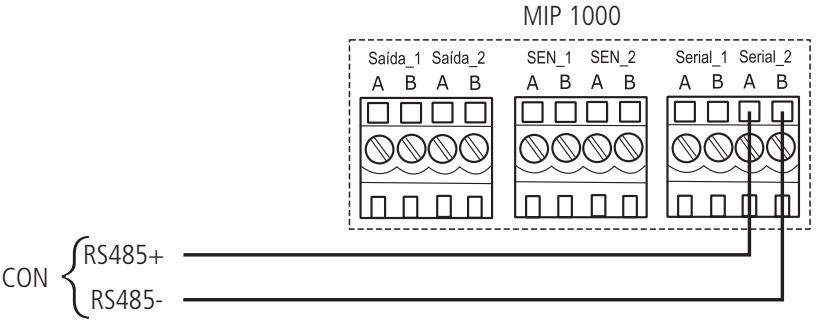
**Entrada de alarme**




*Exemplo de ligação de entrada de alarme*

***Obs.:*** *a entrada de alarme é acionada quando o contato seco for fechado.*

### 5.5. Módulo inteligente de portaria (MIP 1000 IP)



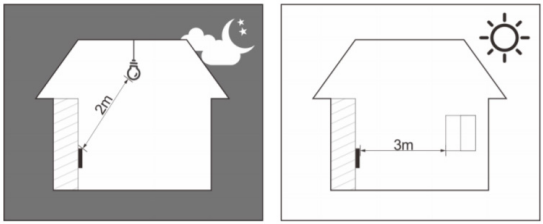

*Exemplo de ligação com MIP 1000 IP*

***Obs.:*** *para ativar o funcionamento com o dispositivo MIP 1000 IP, acesse o menu* Utilidades > MIP.

# 6. Instalação

## 6.1. Locais recomendados

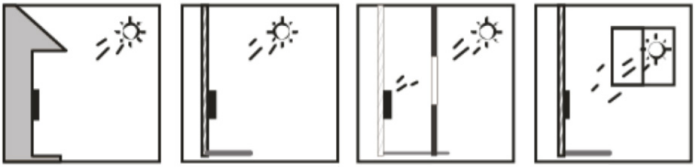
O dispositivo deve ser instalado a pelo menos 2 m de uma lâmpada e a pelo menos 3 metros de um local onde possa entrar claridade proveniente de raios solares.



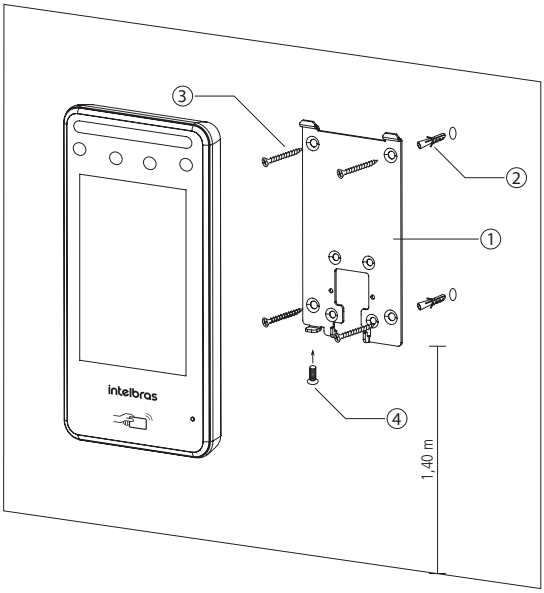

## 6.2. Locais não recomendados

Certifique-se que o dispositivo está instalado em um local onde não fique com muita claridade atrás do rosto a ser identificado e a luz do sol não incida diretamente no dispositivo mesmo que passando através de uma janela.

Cenários como os ilustrados na figura abaixo podem afetar o funcionamento do dispositivo.




## 6.3. Diagrama de instalação




*Modelo de fixação*

1. Remova o suporte (1) do equipamento;
2. Faça cinco orifícios (quatro orifícios de instalação do suporte e uma entrada de cabo) na parede de acordo com os orifícios no suporte e fixe o suporte na parede utilizando as buchas (2) e parafusos (3) que acompanham o produto;
3. Efetue a ligação dos cabos (ver item *5. Esquemas de ligação*);
4. Encaixe o controlador de acesso no suporte e coloque o parafuso de fixação (4).

***Obs.:*** *a altura de instalação indicada na figura visa atender as especificações técnicas, conforme item 1. Especificações técnicas deste manual.*

# 7. Operações do dispositivo

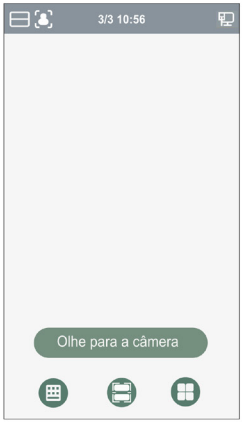
## 7.1. Inicialização do dispositivo

Ao inicializar o dispositivo pela primeira vez escolha o idioma desejado (English, Português ou español (Latinoamérica)) e após ser selecionado se faz necessário a criação de um usuário administrador. Uma senha e um e-mail são de cadastro obrigatório e devem ser definidos na primeira vez que o controlador de acesso é ativado. O nome de usuário do administrador é *admin* por padrão. O controlador de acesso não poderá ser utilizado sem a realização desse cadastro.


**Importante:**

- A senha do administrador pode ser redefinida através do endereço de e-mail digitado, utilize um e-mail válido e ativo.
- A senha deve conter de 8 a 32 caracteres, não pode conter espaços e deve conter pelo menos dois tipos de caracteres entre maiúsculas, minúsculas, número e caracteres especiais (excluindo ' " ; : &).

## 7.2. Tela inicial




*Tela inicial*

Nessa tela inicial o usuário é capaz de fazer a autenticação do seu acesso seja através da face ( ), biometria digital ( )[1], cartão ( ) e/ou senha ( ) como indicado no canto superior esquerdo. À direita são exibidos os ícones de conexão como Ethernet, Wi-Fi e USB.

Na lateral esquerda o ícone para acesso ao menu principal ( ), disponível apenas para o administrador e usuários com esse nível de acesso, e o ícone para acesso por senha ( ).

***Obs.:*** *o ícone de senha deixa de aparecer no canto superior esquerdo caso estejam ativos os quatro métodos de verificaçã*

*[1] Disponível apenas para o modelo SS 3540 MF BIO EX.*

## 7.3. Autenticação

O usuário pode fazer o desbloqueio da porta por reconhecimento facial, biometria digital, senha e/ou cartão.

### Facial

Para autenticar-se por reconhecimento facial basta se posicionar em frente ao equipamento de maneira que o rosto esteja sendo exibido e enquadrado na tela. Um sinal visual é exibido na tela e, de forma opcional, pode haver uma sinalização sonora.

### Biometria digital

Para autenticar-se por reconhecimento biométrico digital basta pressionar levemente o dedo com a digital cadastrada sobre o leitor biométrico. Um sinal visual é exibido na tela e, de forma opcional, pode haver uma sinalização sonora.

### Senha

Para autenticar por senha é preciso acessar o menu *Senha* ( ).

No menu *Senha* duas opções são apresentadas ao usuário: *Senha e senha mestra*.

Na opção *Senha* o usuário poderá autenticar-se utilizando sua ID de usuário e senha cadastrados.

A opção *Senha Mestre* não está relacionada a um usuário específico e necessita ser habilitada pelo administrador do sistema. A senha mestre irá destravar a porta independente dos modos de autenticação ativos, zona de tempo, feriados e regras de anti-passback.

### Cartão

A verificação acontece ao passar o cartão na área indicada no centro direito da tela.

## 7.4. Menu principal

No menu principal pode-se cadastrar usuários, alterar configurações de acesso, conexão e sistema, verificar a capacidade do dispositivo etc.

Para acessar o menu principal se faz necessário autenticar-se como administrador. Essa autenticação pode ser através da face, biometria digital[1], cartão, senha de usuário ou ainda através da senha cadastrada na inicialização do equipamento.

Na tela inicial, abra o menu principal através do ícone ( ).

Se esse for o primeiro acesso ao menu principal, selecione a opção Admin e digite a senha cadastrada na inicialização do dispositivo.


*Métodos de autenticação do menu principal*[1]


*Menu principal*

[1] *Autenticar-se como administrador com biometria digital disponível apenas para o modelo SS 3540 MF BIO EX.*

## 7.5. Gerenciamento de usuários

O menu *Usuário* oferece opção para cadastro de um novo usuário, visualizar e editar lista de usuários e lista de administradores, além de habilitar/desabilitar ou modificar a senha mestra.

### Novo usuário

Ao acesso *Novo usuário* é exibida a tela de cadastro.

- **ID:** número que identifica o usuário. Esse número deve ser único e é incrementado automaticamente, entretanto pode ser personalizado pelo administrador como, por exemplo, a matrícula ou alguma referência ao apartamento, sala etc.
- **Nome:** nome que será exibido para esse usuário.
- **Face:** foto do usuário que será utilizada para identifica-lo através do método de autenticação de reconhecimento facial (ver seção *10. Boas práticas para o Reconhecimento Facial*).
- **Cartão:** permite o cadastro de até 5 cartões ou tags RFID por usuários. Nessa opção é permitido habilitar um desses cadastros como coação (emite um alerta para o software de monitoramento e/ou aciona uma saída de alarme).
- **Imp. digitais:** permite o cadastro de até 3 impressões digitais por usuário. Nessa opção é permitido habilitar um desses cadastros como coação (emite um alerta para o software de monitoramento e/ou aciona uma saída de alarme).
- **Senha:** permite a criação de uma senha de acesso individual de até 8 dígitos numéricos. Para acessar por esse método de autenticação é necessário que o usuário insira também a ID do usuário.
- **Permissão:** esse campo define se esse cadastro será de um Usuário comum ou um Admin. Este último com acesso ao menu principal e todas as configurações do dispositivo.
- **Zona de tempo:** ID da zona de tempo atribuída ao usuário.
- **Plano feriado:** ID do plano de feriado atribuída ao usuário.
- **Validade:** data limite que esse usuário terá acesso. A partir dessa data o usuário continuará cadastrado no dispositivo, mas seu acesso será negado.
- **Perfil:** define o perfil que será atribuído ao usuário. Dos quais:
  - **Geral:** usuários com o perfil Geral podem realizar o acesso normalmente.
  - **Lista negra:** o usuário inserido desse perfil gera um evento de alarme ao efetuar o acesso.
  - **Visitante:** o usuário tem um número limitado de acessos a esse dispositivo.

» **Ronda:** apenas registra evento, não faz nenhum acionamento.
» **VIP:** libera o acesso independente das configurações de zona de tempo ou regra de anti-passback.
» **PcD:** estende o tempo de acionamento em 5 segundos para pessoa com deficiência.
» **Usuário 1:** reservado para customização. Usuários podem realizar o acesso normalmente.
» **Usuário 2:** reservado para customização. Usuários podem realizar o acesso normalmente.

» **Nº de usos:** campo permite selecionar quantos acessos o usuário Visitante (do campo anterior) pode realizar no dispositivo.

**Informações de usuário**

É possível acessar a lista de usuários, lista de usuários administradores e editar suas informações dentro do menu *Usuários*.

***Lista de usuários***

Apresenta a lista de usuários por ordem de cadastro. Não lista os usuários definidos como administradores, ver subseção seguinte. Ao selecionar um usuário é possível editar informações de acesso, exceto o número da ID do usuário.

***Lista de administradores***

Apresenta apenas a lista de usuários definidos com permissão de administradores (Admin). Ao selecionar um usuário é possível editar informações de acesso, exceto o número da ID do usuário.

**Senha mestra**

Nessa opção do menu é possível ativar e desativar a função *Senha mestra,* bem como criar e alterar essa senha.

A opção *Senha mestra* não está relacionada a um usuário específico e irá destravar a porta independente dos modos de autenticação ativos, zona de tempo, feriados e regras de anti-passback.

## 7.6. Gerenciamento de acesso

**Zona de tempo/Feriados**

As zonas de tempos servem para restringir ou liberar grupos específicos de usuários em dias e horários da semana. O mesmo pode ocorrer ao cadastrar um feriado.

*Período NA*

Ao atribuir uma zona de tempo neste campo, a porta permanecerá aberta durante os períodos especificados na zona de tempo configuradas via web.

*Período NF*

Ao atribuir uma zona de tempo neste campo, a porta permanecerá fechada durante os períodos especificados e não poderá ser desbloqueada na zona de tempo configuradas via web.

*Verificação remota*[1]

Na verificação remota, sendo apresentada uma credencial válida, é enviada uma mensagem ao software de gerenciamento solicitando a liberação do acesso. Se confirmado, a porta abre, do contrário nada é exibido ao usuário. Após definir a zona de tempo que funcionará nesse modo é necessário ativá-la 

.

[1] *Função não disponível no software Incontrol Web. Verifique junto ao manual do software que você usa, se há suporte para esta função.*

**Métodos de autenticação**

Ao selecionar a opção *Acesso > Método de autenticação* são apresentadas três opções:

» **Autenticação por usuário:** ao selecionar esse método pode-se optar por realizar a autenticação por Cartão, impressão digital (no modelo SS 3540 MF FACE EX, apenas se houver leitor auxiliar), Face (reconhecimento facial) e senha. Nesse menu também é possível fazer a combinação de acesso. Para abrir a opção pressione sobre o nome Autenticação por usuário. O botão *On/Off* serve para habilitar o método.
  » **Na opção /Ou:** o usuário utiliza de qualquer um dos métodos para realização do acesso, ou seja, considerando as opções *Cartão* e *Face selecionadas*, o usuário terá seu acesso liberado se fazer a verificação apenas da Face e também terá seu acesso liberado se fizer a liberação apenas através do cartão/tag RFID.
  » **Ao utilizar a opção +E:** o usuário terá que utilizar todos os métodos selecionados para que o seu acessa seja liberado, ou seja, caso as opções Cartão e Face estejam selecionadas, o usuário terá que passar seu Cartão/tag RFID e na sequência realizar a verificação da Face. O acesso é liberado ao verificar ambas as credenciais.

**Alarme**

O administrador do sistema pode através do menu *Acesso > Alarme* habilitar ou desabilitar alarmes.

- » **Anti-passback:** após autenticar-se no dispositivo na direção de entrada é necessário autenticar-se para sair antes de uma nova autenticação de entrada e vice-versa. Para tanto, é necessário um leitor auxiliar.
- » **Coação:** biometrias digitais e cartões/tags RFID podem ser cadastrados como credencial de coação. Caso esta opção esteja ativa, além de um evento de coação, também será acionada a saída de alarme se houver um acesso utilizando uma credencial de coação.
- » **Intrusão:** abertura indevida da porta (requer uso do sensor de porta).
- » **Tempo limite do sensor:** define depois de quanto tempo soa um alarme sonoro no próprio dispositivo. Pode ser configurado de 1-9999 segundos.
- » **Sensor de porta:** necessário estar ativado para que o dispositivo detecte abertura indevida da porta ou que a mesma permaneceu aberta.

***Obs.:*** *a integração de alarme do dispositivo e sua configuração (relé de acionamento, evento ou alarme sonoro) requer uso de software.*

**Estado da porta**

São três opções para o estado da porta: *NA, NF e Normal.*

- » **NA:** define que a porta estará sempre aberta, ou seja, relé de acionamento sempre ativo.
- » **NF:** define que a porta estará sempre fechada, ou seja, não haverá acionamento mesmo que uma credencial válida seja verificada.
- » **Normal:** porta será liberada com uma credencial válida.

**Tempo de abertura de porta**

Define o tempo de acionamento do relé de abertura, por padrão 3 segundos.

## 7.7. Configuração de conexão

Através do menu *Conexão* é possível gerenciar conexões de rede e da porta serial.

**Rede**

- » **Rede cabeada:** configurações de endereço de IP, máscara de rede e gateway padrão. Se houver um serviço DHCP na rede é possível ativar esta opção para que um configuração de IP seja atribuída automaticamente.
- » **Registro ativo:** permite conectar o controlador de acesso a plataforma de gerenciamento compatíveis e dessa forma gerenciar o dispositivo. É necessário configurar o endereço IP e porta de comunicação do servidor, além de atribuir uma ID ao dispositivo.
- » **Wi-Fi:** ao ativar o rede Wi-Fi, procure pelas redes disponíveis utilizando o ícone da lupa no canto superior direito. Escolha a SSID desejada e insira a senha. A opção DHCP vem habilitada por padrão.

***Obs.:*** » *Para uso do software InControl Web é necessário um IP fixo. Antes de usar a opção DHCP, certifique-se que sua rede irá atribuir sempre o mesmo IP para esse equipamento.*

» *Para evitar conflitos de IP, certifique-se que configurar a rede cabeada para uma faixa não utilizada em casos que se opte por usar a rede sem fio.*

**Porta serial**

Selecione a opção desejada de acordo com a direção dos dados, entrada ou saída. As opção estão disponíveis através do menu *Conexão > Porta serial.*

Selecione entrada serial quando utilizar um dispositivo externo como o leitor auxiliar 485.

A saída serial enviará as informações de abertura e fechamento para o controlador de acesso. Essas informações podem ser de dois tipos: ID do usuário ou N° do cartão.

Selecionar a opção Entrada OSDP quando utilizar um leitor de cartões com protocolo OSDP conectado ao controlador de acesso.

## 7.8. Sistema

### Data e hora

Para alterar informações de data e hora como ajustar data, formato de data, ajustar hora, horário de verão, serviço NTP e fuso horário, acesse *Sistema > Data e hora*.

### Parâmetros de face

Pressione sobre a(s) opção(ões) que deseja alterar, faça o devido ajuste e pressione salvar  .

- **Limiar de detecção facial:** ajusta a precisão do reconhecimento facial. Quanto maior o valor, maior tem de ser a semelhança da captura do dispositivo com a foto utilizada para realizar o cadastro, ou seja, menor será a tolerância a variações de aparência como expressões faciais, barba, acessórios e idade do cadastro. Valor padrão é de 85.
- **Máx. ângulo de reconhecimento facial:** ajusta o ângulo do perfil aceito pelo dispositivo para iniciar o reconhecimento facial. Valor padrão é 90°.
- **Distância pupilar:** representa a quantidade de pixels na imagem entre os centros das pupilas. O valor muda de acordo com o tamanho da face e a distância entre a face e a lente. Quanto mais próximo o rosto da câmera, maior deve ser esse valor. A distância pupilar para um adulto posicionado a 1,5 metros do dispositivo está entre 50 e 70. Valor padrão é 60.
- **Tempo limite de reconhecimento (s):** tempo limite entre a apresentação para o reconhecimento facial e a mensagem de acesso liberado.
- **Tempo limite para acesso facial negado:** tempo limite entre o momento que se apresenta a face que não tem acesso no dispositivo e a mensagem de acesso negado.
- **Limiar anti-fake:** previne o uso de fotos, imagens ou vídeos em meio impresso ou digital de ter acesso ao dispositivo.
- **Modo máscara:** permite alertar e até bloquear usuários sem máscara. Selecione a opção Não detectar para que o dispositivo não alerte ou bloqueie usuários que não estiverem de máscara. Selecione alertar quando deseja identificar os usuários através de reconhecimento facial e alertar os usuários que não estiverem usando máscara. Caso deseje usar o reconhecimento facial e também bloquear usuários que não estejam de máscara, selecione a opção bloquear.

  ***Obs:*** *para utilizar a opção bloquear usuários sem máscara, será aceito apenas o método de autenticação facial. Na opção alertar, o alerta será dado a todos os usuários que utilizarem métodos alternativos ao reconhecimento facial.*

### Modo de imagem

Em *Sistema > Modo de imagem* selecione a opção que se adequa ao seu cenário. É possível fazer o ajuste da tela para o modo: *Interno, Externo ou Outro*.

### Volume

Utilize as teclas + e – para ajustar o volume do equipamento.

### Parâmetros de Imp. dig.

Ajusta o limiar de reconhecimento biométrico digital. Quanto maior o valor, maior tem de ser a semelhança da captura do dispositivo com o a captura utilizada para realizar o cadastro, ou seja, menor é a tolerância a variações. O valor padrão 3.

### Idioma

As linguagens inglês, espanhol e português estão disponíveis.

***Obs.:*** *é necessário reinicializar o dispositivo.*

### Intensidade da luz infravermelha

Utilize as teclas + e – para ajustar a intensidade da luz infravermelha. Quanto maior o valor atribuído, mais intensa será a emissão da luz infravermelha.

### Configurações de tela

- **Proteção de tela:** configura quanto tempo após nenhuma ação o dispositivo exibirá a proteção de tela. Por padrão esse tempo está em 30 segundos.
- **Tempo limite de tela acesa:** configura quanto tempo após nenhuma ação a tela será desligada. Esse tempo é de 60 segundos na configuração padrão.

***Obs.:*** *ao detectar movimentação o dispositivo retorna a tela de verificação automaticamente.*

**Restaurar padrões de fábrica**

Dados serão perdidos ao selecionar restaurar padrões de fábrica.

As configurações de IP não são alteradas ao restaurar os padrões de fábrica.

Há duas opções para restaurar os padrões de fábrica:

» **Restaurar padrões de fábrica:** restaura as configurações para o padrão e apaga todos os dados do dispositivo.

» **Restaurar padrões de fábrica (manter usuários e eventos):** restaura as configurações para o padrão e mantém os dados de usuário.

Após selecionar a opção desejada, confirme sua escolha.

**Reiniciar**

Selecione *Sistema > Reiniciar e* confirme para que o dispositivo seja reiniciado.

## 7.9. USB

**Atenção:** verifique se o dispositivo de armazenamento USB está corretamente inserido antes de exportar/importar dados de usuário ou atualizar o produto. Nunca remova o dispositivo de armazenamento USB enquanto faz a exportação/importação ou atualização do produto. Do contrário a operação falhará.

É necessário exportar as informações de um controlador de acesso antes de importar essas configurações em outro produto.

A porta USB também pode ser utilizada para atualização de firmware.

**Exportar**

Para exportar dados do dispositivo selecione *USB > Exportar*.

Selecione os dados que deseja exportar e confirme. O administrador pode optar por exportar os usuários, os dados faciais, cartões, impressões digitais (quando houver), eventos ou todas as opções anterior selecionando a opção *Todos.*

***Obs.:*** *o dispositivo de armazenamento deve estar formatado em FAT32*.

**Importar**

Para importar dados para o dispositivo selecione *USB > Importar.*

Selecione os dados que deseja importar e confirme. É possível importar usuários, dados da face, cartão e impressão digital que tenham sido exportados de outro dispositivo. Também é possível importar fotos em formato JPG, onde o nome do arquivo deve ser a ID do usuário. Caso a ID do usuário não exista, uma será criada com a foto disponível. Consulte a seção 10 para mais informações sobre os requisitos das fotos.

**Atualizar**

Para atualizar através de um dispositivo de armazenamento USB renomeie o arquivo de atualização para *update.bin* e salve esse arquivo na raiz do dispositivo USB.

Para atualizar selecione *USB > Atualizar e confirme*.

Ou, com o controlador de acesso desligado, conecte o dispositivo de armazenamento na porta USB e ligue o equipamento. A atualização iniciará automaticamente.

## 7.10. Utilidades

Nesse menu estão as configurações de segurança, opção para inverter o código recebido na entrada Wiegand, habilitar o módulo de segurança, configurar tipo do sensor de porta e o resultado do feedback.

**Configurações de segurança**

» **Habilitar redefinição de senha:** se habilitado, é permitida a redefinição de senha através da interface web.

» **HTTPS:** quando habilitado, o protocolo HTTPS será utilizado para o acesso aos comandos CGI, do contrário será utilizado HTTP. O dispositivo irá reiniciar ao habilitar ou desabilitar o protocolo HTTPS.

» **CGI:** oferece um protocolo para softwares configurarem o dispositivo. Habilita o uso do protocolo CGI.

» **SSH:** habilita o protocolo de segurança SSH.

» **Capturar foto:** o dispositivo irá tirar uma foto do usuário quando houver uma tentativa de acesso.

» **Limpar todas as fotos capturadas:** promove a remoção de todas as capturadas.

**Módulo de segurança**

Habilita o uso de um módulo externo para acionamento da porta. Caso esta opção esteja habilitada e o módulo de segurança não esteja conectado, ou não responda, o acesso será negado mesmo apresentando credenciais válidas.

**Sensor de porta**

O sensor de porta pode ser configurado como NA ou NF.

- **NA:** quando a porta está aberta, o estado do sensor é normalmente aberto ou NA.
- **NF:** quando a porta está aberta, o estado do sensor é normalmente fechado ou NF.

**Resultado do feedback**

- **Sucesso ou falha:** mostra a mensagem *Sucesso!* para acesso liberado e a mensagem *Não autorizado* para acesso negado.
- **Somente nome:** apresenta ID do usuário, nome e horário para o acesso liberado e a mensagem *Não autorizado* e horário para o acesso negado.
- **Foto e nome:** apresenta ID do usuário, nome e horário acompanhado da foto cadastrada para o acesso liberado e a mensagem *Não autorizado* e horário para o acesso negado.
- **Foto, imagem e nome:** apresenta ID do usuário, nome e horário acompanhado da foto cadastrada e da foto atual para o acesso liberado e a mensagem *Não autorizado* e horário acompanhada da foto atual para o acesso negado.

**MIP**

Ao habilitar essa opção o dispositivo utilizará a porta 485 para se comunicar com o dispositivo MIP 1000.

Verifique na seção *5.5. Módulo inteligente de portaria (MIP 1000 IP)* como se dá a ligação dos dispositivos. Para informações de operação e cadastro consulte o manual de usuário do MIP 1000.

### 7.11. Eventos

No menu Eventos é possível visualizar todos os eventos de acesso. É possível fazer busca por ID de usuário ao acessar o ícone de lupa no lado superior direito.

### 7.12. Infor. Sistema

Em informações do sistema é possível consultar a capacidade de armazenamento do dispositivo, número de série, versão de software, versão de firmware e endereço MAC.

## 8. Interface web

O controlador de acesso pode ser configurado e operado na web. Através da web, é possível definir parâmetros de rede e de vídeo de acesso.

A interface web pode ser utilizada para a atualização do sistema.

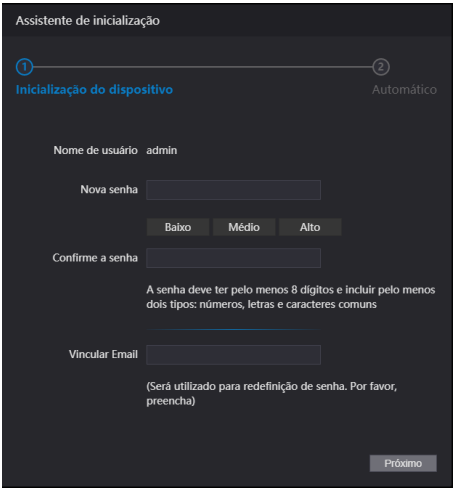
**Importante:** o gerenciamento de usuários só pode ser feito diretamente no dispositivo ou com o auxílio de software, não é possível realizar cadastros de usuário ou exportar/importar dados de usuários através da interface web.

## 8.1. Inicialização

Alternativamente a inicialização do dispositivo em tela (item *7.1. Inicialização do dispositivo*), pode-se cadastrar a senha do administrador do sistema através da interface WEB.

Para isso, abra o navegador e acesse o IP do dispositivo (IP padrão da interface de rede cabeada é 192.168.1.201).

***Obs.:*** *utilize a última versão do Microsoft Edge® ou Chrome®.*




*Tela de inicialização através da Interface web*

Entre com a nova senha, confirme e adicione um e-mail válido e avance para a próxima etapa.

**Importante:**

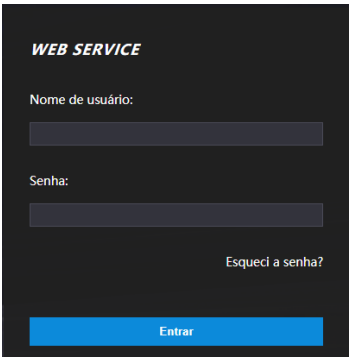
- A senha do administrador pode ser redefinida através do endereço de e-mail digitado, utilize um e-mail válido e ativo.
- A senha deve conter de 8 a 32 caracteres, não pode conter espaços e deve conter pelo menos dois tipos de caracteres entre maiúsculas, minúsculas, número e caracteres especiais (excluindo ' " ; : &).

Na tela seguinte o administrador pode optar por ser informado de uma nova versão quando disponível (exige que o dispositivo esteja conectado a internet).

## 8.2. Login

Abra o navegador e acesse o IP do dispositivo (IP padrão da interface de rede cabeada é 192.168.1.201).

Entre com o *Nome de usuário e Senha* e pressione *Entrar*.




*Tela de login*

**Importante:**

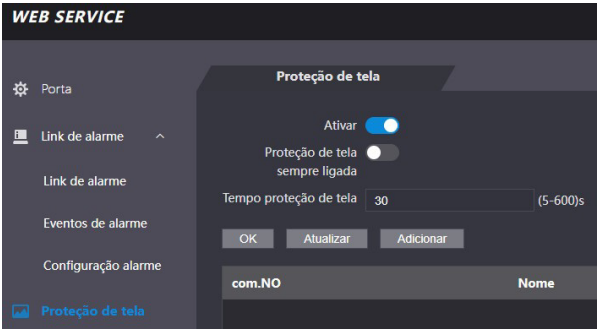
» O nome de usuário padrão do administrador é admin e a senha é criada na inicialização do dispositivo (ver item *7.1. Inicio del dispositivo* ou *8.1. Inicialização*).

» Se a senha de administrador for esquecida, pressione *Esqueci a senha?* na tela de login da interface web e siga as instruções na tela (ver item *Esqueci a senha*).

### Esqueci a senha

Caso tenha esquecido a senha, utilize a opção *Esqueci a senha?* na interface WEB. Utilize a câmera do seu celular para escanear o código QR apresentado e siga as instruções. Uma contrassenha será enviada no endereço de e-mail cadastrado na inicialização do dispositivo. Insira essa contrassenha e uma janela para cadastrar nova senha será exibida. Caso o administrador não esteja mais disponível, tão pouco o e-mail cadastrado, siga os procedimentos apresentados na seção *9. Restaurar senha de administrador*.

## 8.3. Proteção de tela




***Proteção de tela***

» Formato: retrato;

» Arquivo tipo: .JPEG ou .JPG;

» Resolução recomendada: 272 × 480;

» Tamanho máximo do arquivo: 512 KB.

***Obs.:*** *é possível adicionar apenas uma imagem. A proteção de tela será visualizada após o tempo de tela ativa (tempo padrão do dispositivo é de 30 segundos).*

## 8.4. Link de alarme

### Configuração de link de alarme

Dispositivos de alarme podem ser conectados ao controlador de acesso e pode-se configurar a ação do controlador de acesso quando receber uma entrada de alarme.

Em *Link de alarme > Link de alarme* é apresentado o canal de entrada. Para editar pressione o ícone na coluna editar.

» **Entrada:** não pode ser modificado. Entrada 1 refere-se a entrada de alarme ALM_IN.

» **Nome:** insira um nome para a zona de alarme.

» **Tipo de alarme:** selecione de acordo com o sistema de alarme. Ao selecionar NA, o alarme será disparado caso seja detectado o fechamento de um circuito entre GND e a entrada de alarme. Ao selecionar NF, haverá o disparo de um alarme quando for detectado que a entrada de alarme não está conectada ao GND.

» **Ativar link de incêndio:** se o link de incêndio estiver ativo, o controlador de acesso destravará a porta se houver um acionamento na entrada de alarme. Ao ativar o link de incêndio a porta é configurada para sempre aberta. Verifique as demais configurações para a ação desejada.

» **Ativar link de acesso:** quando ativo permite forçar o estado da porta no campo *Tipo de canal*.

» **Tipo de canal:** se NA, abrirá e manterá a porta aberta. Na opção NF manterá a porta fechada e negará qualquer tentativa de acesso.

### Eventos de alarme

Na opção *Eventos de alarme* é possível fazer uma busca por período e por tipo de alarme.

## 8.5. Capacidade

Ao acessar a aba capacidade são apresentadas as quantidades de usuários e credenciais cadastradas no dispositivo.

## 8.6. Config. de vídeo

Estão disponíveis configurações de vídeo, detecção de movimento e modo de imagem.

### Configurações de vídeo

Permite ajustes no streaming de vídeo e na imagem apresentada na tela do dispositivo.

### Detecção de movimento

A área em vermelho representa a área utilizada para detectar objetos em movimento. O gráfico ao lado permite visualizar a interação entre movimento e detecção. Por padrão, todo frame é utilizado para detecção de movimento e os parâmetros Sensibilidade e Limiar com o valor de 50. Para salvar sua alteração pressione *Ok*. Após pressionar *Padrão* para restaurar os padrões de fábrica, também é necessário pressionar *Ok*.

### Modo de imagem

Em *Config. De vídeo > Modo de imagem* selecione a opção que se adequa ao seu cenário. É possível fazer o ajuste da tela para o modo: *Interno, Externo ou Outro.*

## 8.7. Detecção de face

Nessa janela é possível estabelecer uma região para o controle de acesso facial e o tamanho da face (que vai definir a distância de reconhecimento).

Através do botão *Detectar região* é possível ajustar a área da tela em que o dispositivo irá efetuar o reconhecimento facial. Fora dessa área o dispositivo não efetuará o reconhecimento facial.

O botão *Desenhar alvo* permite especificar a partir de qual tamanho o dispositivo efetuará a verificação da face. Quanto maior essa área, mais próximo tem de estar o usuário que será identificado. Quanto menor esse valor, maior a distância que o dispositivo efetuará a leitura da face.

- **Limiar de reconhecimento facial:** ajusta a precisão do reconhecimento facial. Quanto maior o valor, maior tem de ser a semelhança da captura do dispositivo com a foto utilizada para realizar o cadastro, ou seja, menor será a tolerância a variações de aparência como expressões faciais, barba, acessórios e idade do cadastro. Valor padrão é de 85.
- **Máx. ângulo de reconhecimento facial:** ajusta o ângulo do perfil aceito pelo dispositivo para iniciar o reconhecimento facial. Valor padrão é 90°.
- **Limiar anti-fake:** previne o uso de fotos, imagens ou vídeos em meio impresso ou digital de ter acesso ao dispositivo.
- **Luz infravermelha:** ajusta a intensidade da luz infravermelha. Quanto maior o valor atribuído, mais intensa será a emissão da luz infravermelha.
- **Tempo limite de reconhecimento (s):** tempo limite entre a apresentação para o reconhecimento facial e a mensagem de acesso liberado.
- **Tempo limite para acesso facial negado:** tempo limite entre o momento que se apresenta a face que não tem acesso no dispositivo e a mensagem de acesso negado.
- **Distância pupilar:** representa a quantidade de pixels na imagem entre os centros das pupilas. O valor muda de acordo com o tamanho da face e a distância entre a face e a lente. Quanto mais próximo o rosto da câmera, maior deve ser esse valor. A distância pupilar para um adulta posicionado a 1,5 metros do dispositivo está entre 50 e 70. Valor padrão é 60.
- **ID canal:** são duas opções: 1 para a câmera de luz visível e 2 para a câmera de luz infravermelha.
- **Ativar Exp. Facial:** ao ativar essa opção, prepara o dispositivo para funcionar melhor em ambientes mais iluminados como recepções e áreas de acesso a visitantes.

  Para salvar sua alteração pressione *Ok*. Após pressionar *Padrão* para restaurar os padrões de fábrica, também é necessário pressionar *Ok*.
- **Brilho alvo Face:** ajusta o brilho da imagem capturada. O valor padrão é 50.
- **Intervalo de deteção de exposição facial:** depois que um rosto é detectado, o controlador de acesso emitirá luz para iluminar o rosto. O controlador de acesso não emitirá luz novamente até que o intervalo definido tenha passado.

### 8.8. Rede

As configurações de endereço de IP, máscara de rede e gateway padrão podem ser consultadas ou alteradas em *Rede > TCP/IP.* Em *Rede > Portas* é possível estabelecer o número máximo de conexões, portas TCP, HTTP, HTTPS e RTSP. A opção *Rede > Registro,* quando ativa permite conectar o controlador de acesso a plataformas de gerenciamento compatíveis e dessa forma gerenciar o dispositivo. É necessário configurar o endereço IP e porta de comunicação do servidor, além de atribuir uma ID ao dispositivo.

### 8.9. Segurança

Na opção *Segurança > Segurança IP* é possível limitar o acesso ao dispositivo liberando ou bloqueando IPs ou segmentos de IP ou via MAC. Utilize lista branca para liberar ou lista negra para bloquear. É possível configurar para ignorar comandos de PING e impedir semijoin.

Em *Segurança > Serviços* o administrador do dispositivo pode habilitar/desabilitar os protocolos SSH, CGI, HTTPS, bem como habilitar a redefinição de senha através da opção *Esqueci a senha?* da tela de login na interface web.

### 8.10. Configuração de voz

No menu *Config. de voz* pode-se alterar a volume do dispositivo.

### 8.11. Usuários rede

Permite cadastrar outros usuários administradores e editar o usuário admin.

**Importante:** o usuário admin não pode ser excluído.

### 8.12. Manutenção

Define horário para que o dispositivo seja reiniciado automaticamente. Dessa forma o sistema operacional pode fazer os ajustes necessários para melhorar a performance e desempenho. O dispositivo tem por padrão a configuração definida para reiniciar toda terça-feira às duas horas da manhã (de acordo com relógio do dispositivo).

### 8.13. Geren. config.

Permite ao usuário administrador salvar uma cópia das configurações do dispositivo ou restaurar uma configuração previamente criada. Pode ser utilizado quando vários dispositivos necessitam utilizar a mesma configuração. É aqui, também, que pode-se configurar o serviço de eventos.

**Geren. config.**

Para salvar as configurações do seu dispositivo pressione *Exportar configurações* e um arquivo será salvo no seu dispositivo.

A importação pode ser realizada iniciando por Procurar o arquivo desejado e então Importar configurações.

**Serviço de eventos**

Ao ativar o serviço de eventos, o dispositivo passará a enviar os eventos de maneira ativa para o endereço de IP, porta e path configurados nessa página. Para mais informações, consulte em nosso Suporte Técnico a documentação da API/CGI.

### 8.14. Atualizar

**Importante:** utilize apenas arquivos fornecidos pela Intelbras.

Mantenha o dispositivo e o controlador de acesso energizados durante todo o processo de atualização.

A atualização inicia pelo botão *Procurar* para indicar a localização do arquivo. Utilize arquivos locais, arquivos em rede podem causar falha no processo de atualização.

### 8.15. Informações da versão

Apresenta informações do sistema como versão de firmware, da interface web, número de série e MAC.

### 8.16. Usuário online

Ao acessar Usuário online uma lista com o ID do usuário, nome do usuário, endereço de IP e hora do login é exibida.

### 8.17. Eventos

Exibe uma lista com os eventos de administradores e eventos de sistema.

## 9. Restaurar senha de administrador

Caso não se tenha mais a senha do administrador e/ou acesso ao e-mail cadastrado na inicialização do dispositivo, pode-se realizar uma restauração através do hardware. Para isso, siga as etapas listadas abaixo.

1. Desligue o controlador de acesso. Se o seu produto está instalado na parede remova o parafuso de fixação do suporte e remova o dispositivo do suporte.
2. Pressione e segure o botão tamper localizado na parte traseira do equipamento;
3. Ligue o dispositivo;
4. Permaneça com o botão tamper pressionado e aguarde a total inicialização do dispositivo, quando a imagem da câmera é exibida no display;
5. Solte o botão tamper;
6. Aguarde 30 segundos. Observe a mensagem *Por favor, feche a tampa traseira* na tela do dispositivo;
7. Pressione e solte o tamper 3 vezes. A mensagem *Por favor, feche a tampa traseira* será exibida cada vez que o botão tamper é solto;
8. Ao soltar o tamper pela terceira vez o dispositivo reiniciará e voltará na tela de inicialização permitindo o cadastro de uma nova senha de administrador.

***Obs.:*** *todas as configurações são restauradas exceto usuários e eventos. Usuários que tinham privilégio de administrador também são mantidos restaurando apenas a senha de administrador que é cadastrada durante a inicialização do equipamento.*

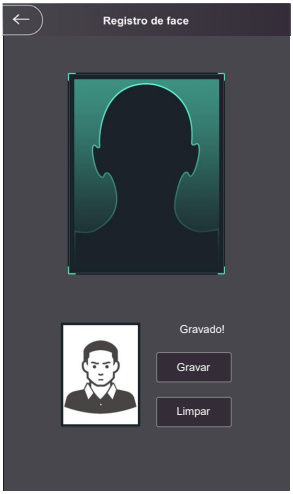
# 10. Boas práticas para o Reconhecimento Facial

## 10.1. Antes do registro

» Óculos, chapéus e barbas podem influenciar o desempenho do reconhecimento de rosto. Não cubra as sobrancelhas ao usar chapéus.
» Atualize o cadastro caso haja uma grande mudança visual, como a retirada da barba, se houver dificuldade no acesso.
» Mantenha seu rosto visível.
» Mantenha o dispositivo a pelo menos dois metros de distância da fonte de luz e a pelo menos três metros de janelas ou portas; caso contrário, a luz solar direta pode influenciar o desempenho do reconhecimento de face do dispositivo.

## 10.2. Durante o registro

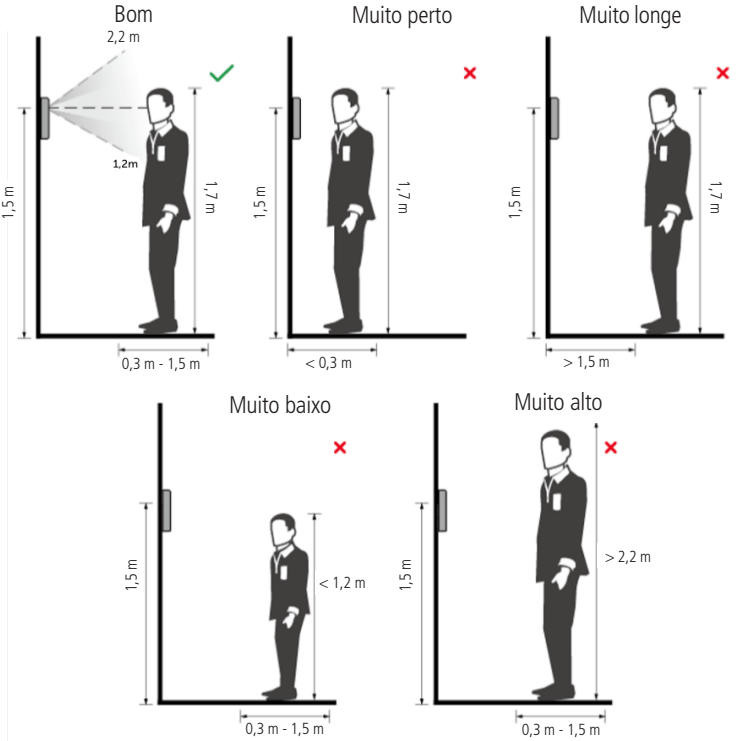
Você pode registrar faces através do controlador de acesso ou através do software. Para registro através do software, consulte o manual do usuário do software. Posicione sua cabeça na moldura de captura de fotos. Uma foto do seu rosto será capturada automaticamente.




» Fique imóvel, não balance a cabeça ou o corpo, pois o registro pode falhar.
» Enquadre todo o rosto, visão frontal e de olhos abertos;
» Enquadre da cabeça aos ombros;
» Dê preferência a um fundo neutro;
» Apenas um rosto deve aparecer na foto;
» Rosto deve estar completamente visível, livre de qualquer objeto que possa cobrí-lo (ex.: máscara);
» Evite sombras no rosto ou ao fundo;
» Faça uma expressão neutra e natural.

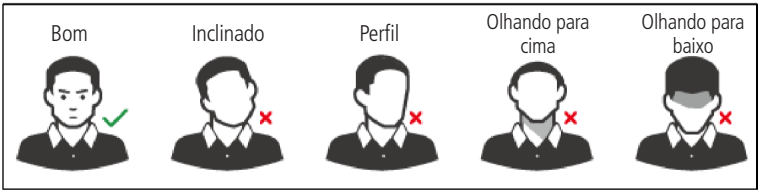
**Posição do rosto**

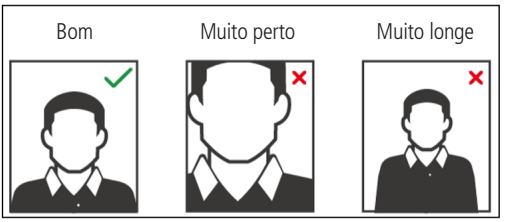
Se seu rosto não estiver na posição apropriada, o efeito de reconhecimento de rosto poderá ser influenciado.



### Requisitos de rostos

- » Verifique se o rosto está visível e se a testa não está coberta por cabelos.
- » Enquadre todo o rosto, olhe para a câmera ou logo abaixo dela no topo da tela e esteja de olhos abertos durante o cadastro.
- » Evite usar óculos e não use chapéus ou outros ornamentos para o rosto que influenciem a gravação da imagem do rosto, o que inclui máscaras faciais.
- » Enquadre da cabeça aos ombros e dê preferência a um fundo neutro ou branco.
- » Evite sombras no seu rosto ou ao fundo.
- » Faça uma expressão neutra e natural e mantenha os braços ao longo do corpo.
- » Ao gravar seu rosto ou durante o reconhecimento de rosto, não o mantenha muito próximo ou muito longe da câmera.




### Requisitos para importação de fotos

Quando importar as fotos de usuários - seja através da porta USB ou utilizando um software de gestão de controle de acesso compatível - recomenda-se a utilização de imagens com resolução superior a 500 × 500 pixels (L × A)[1], onde o rosto não deve ocupar mais de 2/3 da área total da imagem. No caso de bases de dados pré-existente, atente-se para as resoluções mínima e máxima:

- » **Resolução Mínima:** 150 × 300 pixels (L × A)[1]
- » **Resolução Máxima:** 600 × 1200 pixels (L × A)[1]

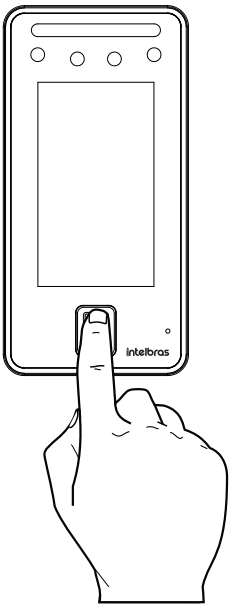
Para todos os casos, o tamanho máximo do arquivo deve ser inferior a 100 KB e estar no formato JPG.

*[1] A altura não deve exceder duas vezes a largura. Por exemplo, se largura for 300 pixels, então a altura poderá ser igual ou inferior a 600 pixels.*

# 11. Boas práticas para o reconhecimento biométrico digital

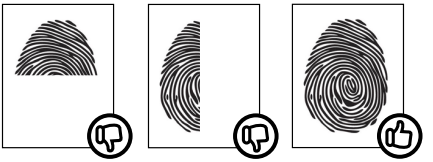
### 11.1. Postura recomendada no momento de cadastro

» Posicione-se na frente do equipamento, coloque o dedo reto sobre o leitor biométrico e aguarde a confrmação de captura do template.

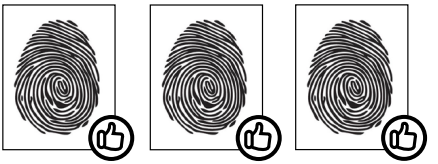



» Não pressione demasiadamente o dedo no sensor biométrico, isso distorce a imagem da digital, não permitindo que o aparelho identifque os pontos formados pelas intersecções das linhas (cristas e vales) que compõem a digital.

» Não posicione o dedo torto ou apenas a ponta do dedo no sensor biométrico. O uso inadequado do sensor biométrico no momento da leitura da digital impede que o sistema transmita uma imagem capaz de ser transformada em um template.



» Siga as instruções visuais e sonoras para realizar as capturas de biometrias digitais.



# Termo de garantia

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

Nome do cliente:

Assinatura do cliente:

Nº da nota fiscal:

Data da compra:

Modelo: Nº de série:

Revendedor:

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

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

Todas as imagens deste manual são ilustrativas.

Español

intelbras

**SS 3540 MF FACE EX**

**SS 3540 MF FACE BIO EX**

**Controlador de acceso con reconocimiento de rostro**

Felicitaciones, acabas de adquirir un producto con la calidad y seguridad Intelbras.

El dispositivo SS 3540 MF FACE EX / SS 3540 MF FACE BIO EX es un controlador de acceso con autenticación por reconocimiento facial, tarjeta RFID de 13,56 MHz y contraseña. Con una pantalla táctil de 4,3", es conveniente registrarse y cambiar la configuración. Se puede instalar en interiores para abrir puertas en general, mediante la activación de cerraduras eléctricas, electroimanes o solenoides.

ANATEL

11812-21-00160

Este equipamiento no tiene derecho a la protección contra interferencia prejudicial y no puede causar interferencia en sistemas debidamente autorizados. Este es un producto homologado por la Anatel, el número de homologación lo encuentras en la etiqueta del producto, para consultas usa el enlace: *sistemas.anatel.gov.br/sch*.

# Cuidados y seguridad

- Debes guardar las instrucciones de seguridad y operación, para referencias futuras.
- Usa la fuente de alimentación que acompaña el producto.
- Debes usar el producto en ambientes internos y externos con temperatura superior a -30 °C e inferior a 60 °C.
- El intento de abrir el producto lo puede dañar e implica en perdida del derecho a la garantía.
- Cuidado al manejar los cables para no dañarlos.
- No sobrecargues las tomas o alargues eléctricos, pues puede causar incendio o una descarga eléctrica.
- Instalarlo en un local seguro.
- No pongas o instales el producto en lugares expuestos a la luz del sol o fuentes de calor.
- Mantenga el producto lejos de humedad, hollín o polvo.
- Instala el producto de forma vertical y en local estable, garantizando la correcta fijación para que no caiga, causando daños al equipamiento.
- Limpia el producto con paño humedecido en agua o seco. No utilice productos químicos fuertes o abrasivos.
- Instale el producto en local ventilado y no bloquees la ventilación del controlador de acceso.
- Usa apenas accesorios recomendados por el fabricante.
- LGPD - Ley General de Protección de Datos Personales: la Intelbras no accede, transfiere, capta, ni realiza cualquier otro tipo de tratamiento de datos personales a partir de este producto. Este producto tiene criptografía en la transmisión y almacenamiento de los datos personales.

**Atención:** daños causados por el no cumplimiento de las recomendaciones de instalación o uso inadecuado del producto no son cubiertos por la garantía. Ver el certificado de garantía del producto.

# 1. Especificaciones técnicas

| Modelo | | SS 3540 MF FACE EX | SS 3540 MF FACE BIO EX |
|---|---|---|---|
| Tensión de alimentación | | 12 Vdc | |
| Potencia | | 24 W | |
| Capacidad de conmutación | | 2 A / 30 Vdc | |
| Temperatura de operación | | -30 °C a 60 °C | |
| Humedad de operación | | 5% a 95% | |
| Pantalla | | 4,3" sensible al toque (capacitivo) | |
| Cámaras | | 2 MP CMOS RGB y 2 MP CMOS IR | |
| Intervalo de reconocimiento facial | | Distancia de la cámara al rostro: 0,3 m a 1,5 m | |
| | | Altura del usuario: 0,9 m a 2,40 m | |
| Tiempo de reconocimiento facial | | 0,2s | |
| Métodos de autenticación | | Reconocimiento facial, biometria digital, tarjeta, contraseña y código QR | |
| Interfaz de comunicación | | RS 485 e Wiegand | |
| Capacidad | Usuarios | 6.000 | |
| | Rostros | 6.000 | |
| | Digital | 6.000 | |
| | Tarjetas | 6.000 | |
| | Contraseñas | 6.000 | |
| | Eventos | 150.000 | |
| Wifi | Antena | Interna | |
| | Estándares | IEEE 802.11b, 802.11g, 802.11n | |
| | Frecuencia operacional | 2,4 GHz ~ 2,4835 GHz | |
| | Ancho de banda | Soporta 20 MHz y 40 MHz | |
| | Protocolo de seguridad | 64/128 bit WEP, WPA/WPA2, WPA-PSK/WPA2-PSK | |
| | Tasa de transmisión | 802.11b: hasta 11 Mbps<br>802.11g: hasta 54 Mbps<br>802.11n: hasta 300 Mbps (HT40) | |
| RFID | Modulación | ASK | |
| | Frecuencia | 13,56 MHz | |
| | Tasa de transmisión | 106 a 848 kbps | |
| | Código de emisión | 13M5K2D | |
| | Tipo antena | Interna | |
| Grado de protección | | IP65 | |
| Dimensiones (A × A × L) | | 87,5 × 174 × 22,5 mm | |

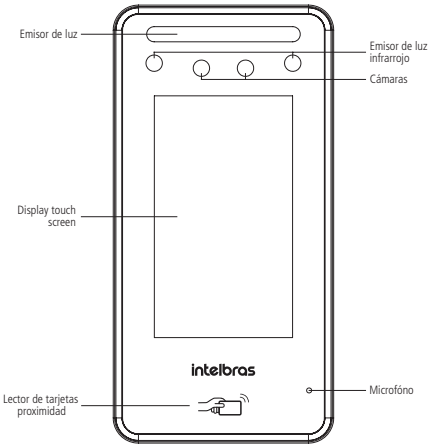
# 2. Características

- Fácil instalación.
- Visual moderno y funcional.
- Compatible con Defense IA.
- Integrado al sistema MIP 1000 IP.
- Para uso en ambiente externo.
- Función anti-falso que imposibilita la autenticación por vídeo o foto en medio físico o digital.
- Soporta reconocimiento facial, biometría digital, lector RFID, contraseña y QR code.
- Cámara doble grande angular de 2 MP: una de luz visible colorida (RGB) y otra de luz infrarroja (IR).
- Precisión de verificación de rostro >99,5%.
- Bajo índice de falso rechazo.

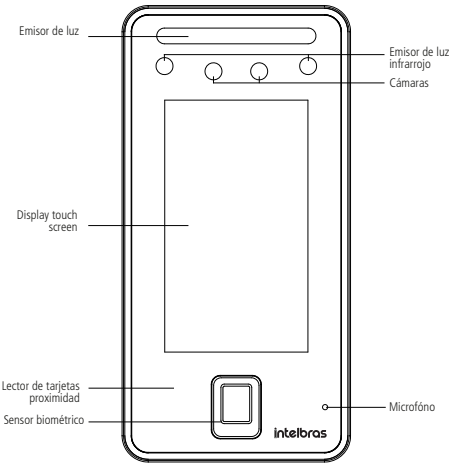
# 3. Contenido del embalaje

» 1× controlador de acceso SS 3540 MF FACE EX / SS 3540 MF FACE BIO EX
» 1× conjunto de tarugos y tornillos
» 1× soporte para fijación en la pared
» 1× fuente de alimentación
» 1× guía del usuario

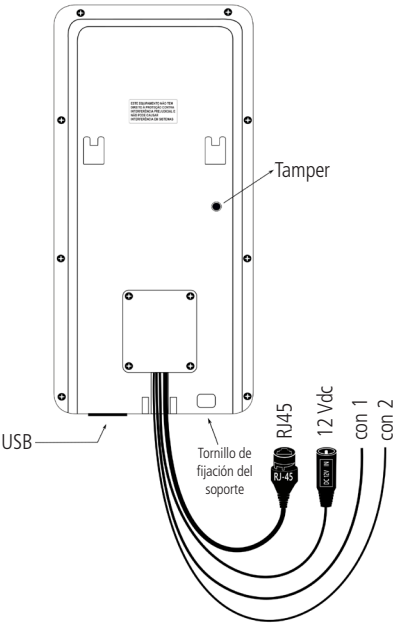
# 4. Productos




*Vista frontal SS 3540 MF FACE EX*




*Visão frontal SS 3540 MF FACE BIO EX*




*Vista trasera SS 3540 MF FACE EX / SS 3540 MF FACE BIO EX*

## 4.1. Descripción de los cables

### Interfaz de lectores (CON)

| Color | Nombre | Descripción |
|---|---|---|
| Marrón oscuro | PORTA_COM | Acceder al contacto común del relé del gatillo de liberación. |
| Amarillo negro | PORTA_NA | Acceda al contacto del relé del gatillo de liberación normalmente abierto. |
| Negro/morado | PORTA_NF | Contacto del relé del gatillo de liberación de acceso normalmente cerrado. |
| Azul negro | GND | Referencia para señal de botón de salida y sensor de puerta. |
| Gris negro | SEN | Conexión para sensor de puerta. |
| Verde negro | BOT | Conexión para botón de salida. |
| Blanco verde | GND | Referencia para la entrada de alarma. |
| Marrón blanco | ALM_IN | Entrada de alarma. |

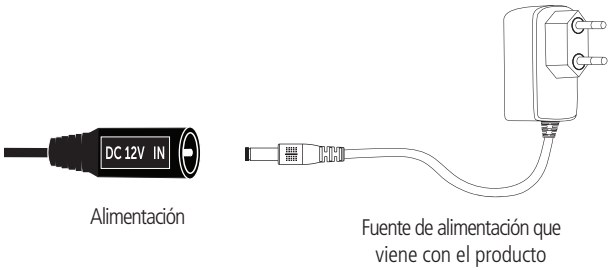
### Interface de leitores (CON2)

| Color | Nombre | Descripción |
|---|---|---|
| Amarillo | 485- | Señal 485B o 485 del bus RS-485 / Salida B para integración MIP. |
| Púrpura | 485+ | Bus RS-485 485A o 485+ señal / Salida A para integración MIP. |
| Blanco | WD1 | Entrada Wiegand D1 (para conectar un lector auxiliar) / Salida Wiegand D1 (para conectar a otro controlador de acceso). |
| Verde | WD0 | Entrada Wiegand D0 (para conectar un lector auxiliar) / Salida Wiegand D0 (para conectar a otro controlador de acceso). |
| Negro | GND | Referencia al bus Wiegand. |
| Marrón | LED | Salida para señalización de acceso para lector auxiliar / Entrada para recepción de señalización de acceso. |

# 5. Esquemáticos de conexión

## 5.1. Fuente de alimentación

Conecte la fuente de alimentación al dispositivo y en seguida, conectarla a la toma eléctrica.

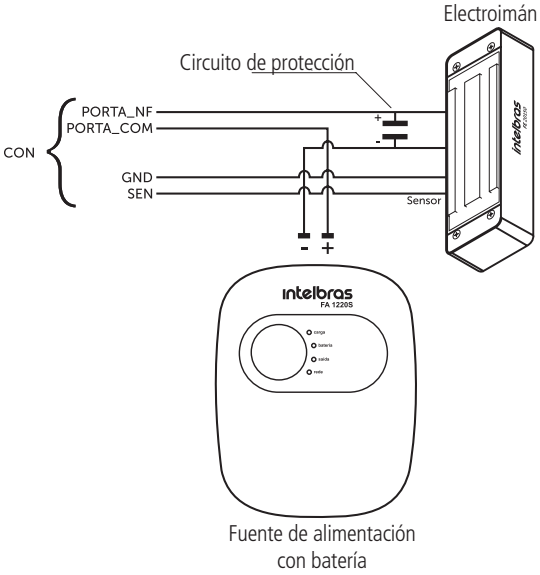



*Alimentación del producto*

***Obs.: se** recomienda el uso de un nobreak para suministrar situaciones de cortes de energía eléctrica.*

## 5.2. Cerraduras

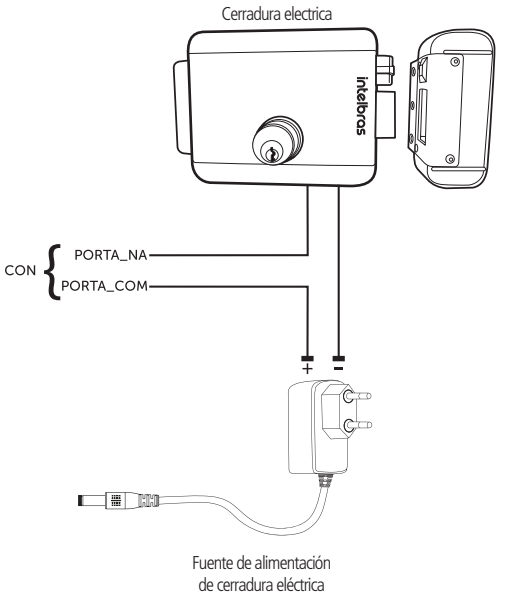
### Cerradura electroimán



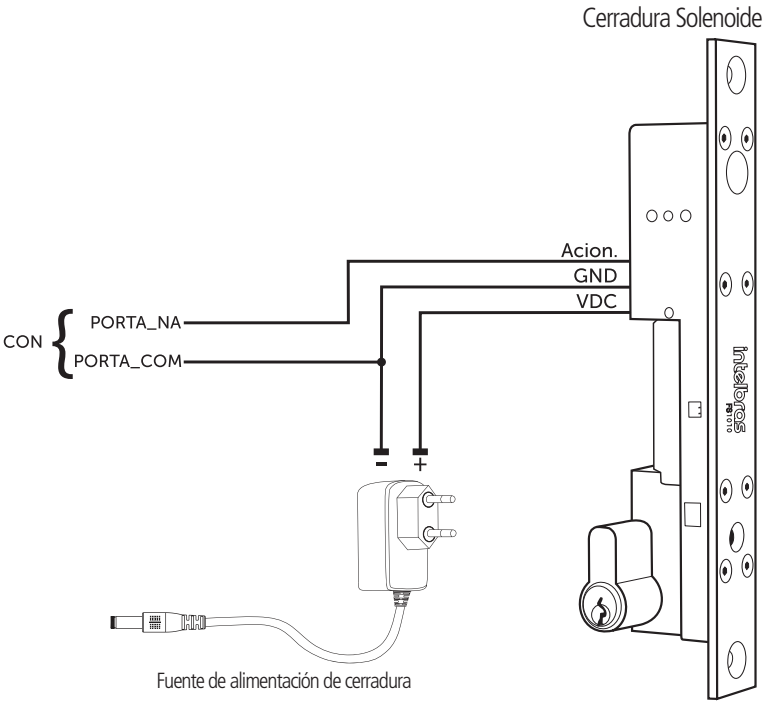

*Ejemplo de conexión de cerradura electroimán*

***Obs.:** si la cerradura no tiene sensor, ignora la conexión de este.*

**Cerradura eléctrica**

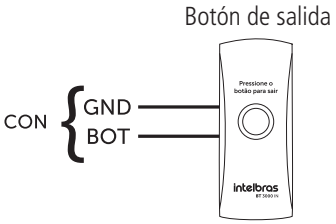



**Cerradura solenoide**




*Ejemplo de conexión de cerradura solenoide*

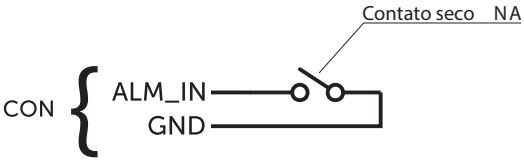
### 5.3. Botón de salida




*Ejemplo de conexión de botón de salida*

### 5.4. Alarma

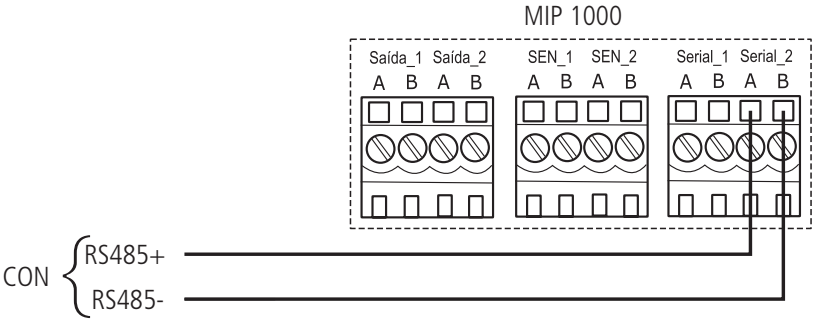
**Entrada de alarma**




*Ejemplo de conexión de entrada de alarma*

***Obs.: I****a entrada de alarma se acciona cuando el contacto seco se cierra.*

### 5.5. Módulo inteligente de portería (MIP 1000 IP)



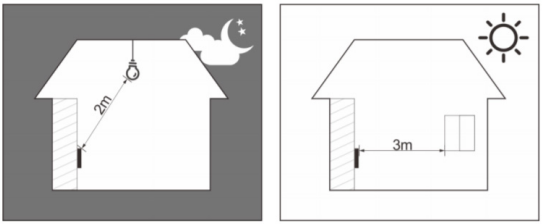

*Ejemplo de conexión con MIP 1000 IP*

***Obs.:*** *para activar el funcionamiento con el dispositivo MIP 1000 IP, accede al menú* Utilidades > MIP.

# 6. Instalación

## 6.1. Locales recomendados

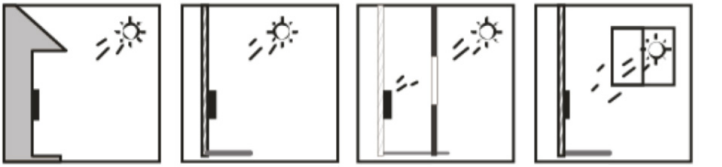
El dispositivo debe instalarse por lo menos a 2 m de una lámpara y por lo menos a 3 metros de un local donde pueda entrar claridad, proveniente de rayos solares.



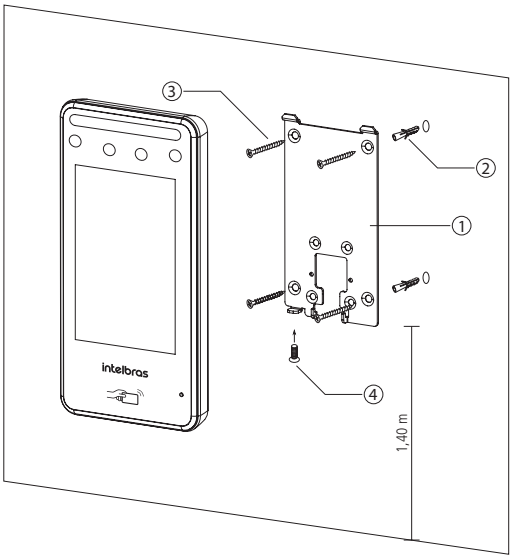

## 6.2. Locales no recomendados

Certifícate de que el dispositivo esté instalado en un local con poca claridad detrás del rostro a ser identificado y la luz del sol no sea directamente sobre el dispositivo mismo que pasando a través de una ventana.

Escenarios como los ilustrados en la figura abajo pueden afectar el funcionamiento del dispositivo.



### 6.3. Diagrama de instalación




*Modelo de fijación*

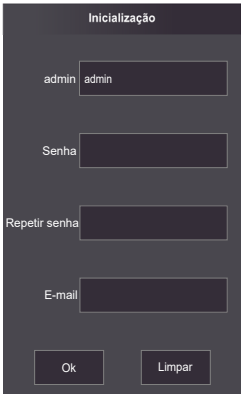
1. Retira el soporte (1) del equipamiento;
2. Haz cinco agujeros (cuatro agujeros de instalación del soporte y una entrada de cable) en la pared de acuerdo con los agujeros en el soporte y fija el soporte en la pared usando los tarugos (2) y tornillos (3) que acompañan el producto;
3. Efectúa la conexión de los cables (ver ítem *5. Esquemáticos de conexión*);
4. Encaja el controlador de acceso en el soporte y coloque el tornillo de fijación (4).

***Obs.: I****a altura de instalación indicada en la figura visa atender las especificaciones técnicas, conforme el ítem 1. Especificaciones técnicas de este manual.*

# 7. Operaciones del dispositivo

### 7.1. Inicio del dispositivo

Al iniciar el dispositivo por primera vez, elija el idioma deseado (inglés, portugués o español (Latinoamérica)) y luego de ser seleccionado, es necesario crear un usuario administrador. Una contraseña y un correo electrónico son de registro obligatorio y deben definirse la primera vez que se activa el controlador de acceso. El nombre de usuario del administrador es admin por defecto. El controlador de acceso no se puede utilizar sin este registro.

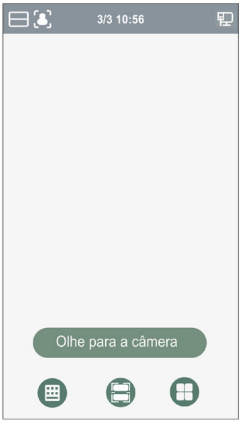


**Importante:**

» Se puede rehacer la contraseña del administrador a través del correo electrónico tecleado, usa un correo electrónico válido y activo.

» La contraseña debe tener de 8 a 32 caracteres, no puede tener espacios y debe tener por lo menos dos tipos de caracteres entre mayúsculas, minúsculas, número y caracteres especiales (excluyendo ' " ; : &).

## 7.2. Pantalla inicial




*Pantalla inicial*

En esta pantalla inicial el usuario es capaz de autenticar su acceso a través del rostro ( ), biometria digital ( )[1], tarjeta ( ) y/o contraseña ( ) como indicado en la esquina superior izquierda. En la derecha se exhiben los íconos de conexión como Ethernet, Wifi y USB.

En la lateral izquierda el ícono para acceso al menú principal ( ), disponible apenas para el administrador y usuarios con ese nivel de acceso, y el ícono para acceso por contraseña ( ).

***Obs.:*** *el ícono de contraseña deja de aparecer en la esquina superior izquierda caso estén activos los cuatro métodos de verificación.*

*[1] Solo disponible para el modelo SS 3540 MF BIO EX.*

## 7.3. Autenticación

El usuario puede desbloquear la puerta por reconocimiento facial, biometria digital, contraseña y/o tarjeta.

### Facial

Para autenticarse por reconocimiento facial basta posicionarse al frente del equipamiento de manera que el rostro sea exhibido y encuadrado en la pantalla. Una señal visual es exhibida en la pantalla y, de forma opcional, puede haber una señalización sonora.

### Biometria digital

Para autenticar-se por reconhecimento biométrico digital basta pressionar levemente o dedo com a digital cadastrada sobre o leitor biométrico. Um sinal visual é exibido na tela e, de forma opcional, pode haver uma sinalização sonora.

### Contraseña

Para autenticar por contraseña es necesario acceder el menú *Contraseña* ( ).

En el menú *Contraseña* dos opciones se presentarán al usuario: *Contraseña y contraseña maestra*.

En la opción *Contraseña* el usuario podrá autenticarse usando su ID de usuario y contraseña registrados.

La opción *Contraseña Maestra* no está relacionada a un usuario específico y necesita estar habilitada por el administrador del sistema. La contraseña maestra destrabará la puerta, independiente de los modos de autenticación activos, zona de tiempo, vacaciones y reglas de anti-passback.

**Tarjeta**

La verificación ocurre al pasar la tarjeta en el área indicada, en el centro derecho de la pantalla.

## 7.4. Menú principal

En el menú principal se pueden registrar usuarios, cambiar configuraciones de acceso, conexión y sistema, verificar la capacidad del dispositivo etc.

Para acceder el menú principal es necesario estar autenticado como administrador. Esa autenticación puede ser a través del rostro, biometria digital[1], tarjeta, contraseña de usuario o a través de la contraseña registrada en el inicio del equipamiento.

En la pantalla inicial, abre el menú principal a través del ícono ( ).

Si es el primer acceso al menú principal, selecciona la opción Admin y teclea la contraseña registrada en el inicio del dispositivo.


*Métodos de autenticación del menú principal[1]*


*Menú principal*

*[1] Inicie sesión como administrador con biometría digital solo disponible para el modelo SS 3540 MF BIO EX.*

## 7.5. Gerencia de usuarios

El menú *Usuario* ofrece opción para registro de un nuevo usuario, ver y modificar lista de usuarios y lista de administradores, además de habilitar/deshabilitar o cambiar la contraseña maestra.

**Nuevo usuario**

Al acceder *Nuevo usuario,* se exhibe la pantalla de registro.

- **ID:** número que identifica el usuario. Ese número debe ser único y se incrementa automáticamente, entretanto puede ser personalizado por el administrador como, por ejemplo, la matrícula o alguna referencia al apartamento, sala etc.
- **Nombre:** nombre que se exhibirá para este usuario.
- **Face:** foto del usuario que se usará para identificarlo a través del método de autenticación de reconocimiento facial (ver sección *10. Buenas prácticas para el Reconocimiento Facial*).
- **Tarjeta:** permite el registro de hasta 5 tarjetas o tags RFID por usuarios. En esa opción es permitido habilitar uno de esos registros como coacción (emite una alerta para el software de monitoreo y/o acciona una salida de alarma).
- **Diablillo. huellas dactilares:** permite el registro de hasta 3 huellas dactilares por usuario. En esta opción está permitido habilitar una de estas entradas como coerción (emite una alerta al software sistema de monitorización y/o activa una salida de alarma).
- **Contraseña:** permite crear una contraseña de acceso individual de hasta 8 dígitos numéricos. Para acceder por este método de autenticación es necesario que el usuario también inserte la ID del usuario.
- **Permiso:** este campo define si este registro será de un Usuario común o un Admin. Este último con acceso al menú principal y todas las configuraciones del dispositivo.
- **Zona de tiempo:** ID de la zona de tiempo atribuida al usuario.

- » **Plano vacación:** ID del plano de vacación atribuida al usuario.
- » **Validad:** fecha límite que este usuario tendrá de acceso. A partir de esta fecha el usuario continuará registrado en el dispositivo, mas su acceso se negará.
- » **Perfil:** define el perfil que se atribuirá al usuario. De los cuales:
  - » **General:** usuarios con el perfil General pueden acceder normalmente.
  - » **Lista negra:** el usuario insertado de este perfil genera un evento de alarma al efectuar el acceso.
  - » **Visitante:** el usuario tiene un número limitado de accesos a este dispositivo.
  - » **Ronda:** apenas registra evento, no hace ningún accionamiento.
  - » **VIP:** libera el acceso independiente de las configuraciones de zona de tiempo o regla de anti-passback.
  - » **PcD:** extiende el tiempo de accionamiento en 5 segundos para persona con deficiencia.
  - » **Usuario 1:** reservado para personalización. Usuarios pueden acceder normalmente.
  - » **Usuario 2:** reservado para personalización. Usuarios pueden acceder normalmente.
- » **Nº de usos:** campo permite seleccionar cuantos accesos el usuario Visitante (del campo anterior) puede realizar en el dispositivo.

**Informaciones de usuario**

Es posible acceder la lista de usuarios, lista de usuarios administradores y modificar sus informaciones dentro del menú *Usuarios*.

***Lista de usuarios***

Presenta la lista de usuarios por orden de registro. No lista los usuarios definidos como administradores, ver siguiente subsección. Al seleccionar un usuario es posible editar informaciones de acceso, excepto el número de la ID del usuario.

***Lista de administradores***

Presenta apenas la lista de usuarios definidos con permiso de administradores (Admin). Al seleccionar un usuario es posible modificar informaciones de acceso, excepto el número de la ID del usuario.

**Contraseña maestra**

En esta opción del menú es posible activar y desactivar la función *Contraseña maestra,* bien como crear y cambiar esa contraseña.

La opción *Contraseña maestra* no está relacionada a un usuario específico y destrabará la puerta independiente de los modos de autenticación activos, zona de tiempo, feriados y reglas de anti-passback.

## 7.6. Gerencia de acceso

**Zona de tiempo/Vacaciones**

Las zonas de tiempo sirven para restringir o liberar grupos específicos de usuarios en días y horarios de la semana. El mismo puede ocurrir al registrar una vacación.

*Período NA*

Al atribuir una zona de tiempo en este campo, la puerta permanecerá abierta durante los períodos especificados en la zona horaria configurada a través de la web.

*Período NC*

Al atribuir una zona de tiempo en este campo, la puerta permanecerá cerrada durante los períodos especificados y no podrá desbloquearse en la zona horaria configurada a través de la web.

*Verificación remota*[1]

En la verificación remota, siendo presentada una credencial válida, se envía un mensaje al software de gerencia, solicitando la liberación del acceso. Si confirmado, la puerta abre, de lo contrario nada se exhibe al usuario. Después de definir la zona de tiempo que funcionará en ese modo es necesario activarla 

.

[1] *Función no disponible en el software Incontrol Web. Verifica junto al manual del software que usas, si hay soporte para esta función.*

**Métodos de autenticación**

Al seleccionar la opción *Acceso > Método de autenticación* son presentadas tres opciones:

» **Autenticación por usuario:** al seleccionar ese método se puede optar por hacer la autenticación por Tarjeta, huella digital (en el modelo SS 3540 MF FACE EX, solo si hay lector auxiliar), Rostro (reconocimiento facial) y contraseña. En este menú también es posible combinar el acceso. Para abrir la opción presiona sobre el nombre Autenticación por usuario. El botón *On/Off* sirve para habilitar el método.

» **En la opción /O:** el usuario usa de cualquier uno de los métodos para realizar el acceso, o sea, considerando las opciones *Tarjeta y Rostro seleccionadas*, el usuario tendrá su acceso liberado si verifica apenas por el Rostro y también tendrá su acceso liberado si hace la liberación apenas a través de la tarjeta/tag RFID.

» **Al usar la opción +E:** el usuario tendrá que utilizar todos los métodos seleccionados para que su acceso se libere, o sea, caso las opciones Tarjeta y Rostro estén seleccionadas, el usuario tendrá que pasar su Tarjeta/tag RFID y en la secuencia verificar por Rostro. El acceso es liberado al verificar ambas las credenciales.

**Alarma**

El administrador del sistema a través del menú *Acceso > Alarma* puede habilitar o deshabilitar alarmas.

» **Anti-passback:** después de autenticarse en el dispositivo en la dirección de entrada, es necesario autenticarse para salir antes de una nueva autenticación de entrada y viceversa. Para eso, es necesario un lector auxiliar.

» **Coacción:** biometría digital y tarjetas/etiquetas RFID se pueden registrar como credencial de coacción. Caso esta opción esté activada, además de un evento de coacción, también se accionará la salida de alarma si hay un acceso utilizando una credencial de coacción.

» **Intrusión:** abertura indebida de la puerta (requiere uso del sensor de puerta).

» **Tiempo limite del sensor:** define después de cuanto tiempo suena la alarma sonora en el propio dispositivo. Puede configurar de 1-9999 segundos.

» **Sensor de puerta:** necesario estar activado para que el dispositivo detecte abertura indebida de la puerta o que la misma permaneció abierta.

***Obs.: l****a integración de alarma del dispositivo y su configuración (relé de accionamiento, evento o alarma sonora) requiere uso de software.*

**Estado de la puerta**

Son tres opciones para el estado de la puerta: *NA, NC y Normal*.

» **NA:** define que la puerta estará siempre abierta, o sea, relé de accionamiento siempre activo.

» **NC:** define que la puerta estará siempre cerrada, o sea, no hay accionamiento, mismo que verifiques en la credencial válida.

» **Normal:** puerta será liberada con una credencial válida.

**Tiempo de abertura de puerta**

Define el tiempo de accionamiento del relé de abertura, por estándar 3 segundos.

## 7.7. Configuración de conexión

A través del menú *Conexión* es posible hacer la gerencia de conexión de red y de la puerta serial.

**Red**

» **Red cableada:** configuraciones de dirección de IP, máscara de red y gateway estándar. Si hay un servicio DHCP en la red es posible activar esta opción para que una configuración de IP se atribuya automáticamente.

» **Registro activo:** permite conectar el controlador de acceso a la plataforma de gerencia compatible y de esa forma hacer la gerencia del dispositivo. Es necesario configurar la dirección IP y puerta de comunicación del servidor, además de atribuir una ID al dispositivo.

» **Wifi:** al activar la red Wifi, busca por las redes disponibles usando el ícono de la lupa en la esquina superior derecha. Elige la SSID deseada e inserte la contraseña. La opción DHCP por estándar viene habilitada.

***Obs.:*** *» Para uso del software InControl Web es necesario un IP fijo. Antes de usar la opción DHCP, certifícate que tu red atribuirá siempre el mismo IP para ese equipamiento.*

» *Para evitar conflictos de IP, certifícate de configurar la red cableada para un rango no usado, en casos que se opte por usar la red inalámbrica.*

### Puerta serial

Selecciona la opción deseada de acuerdo con la dirección de los datos, entrada o salida. Las opciones están disponibles a través del menú *Conexión > Puerta serial.*

Selecciona entrada serial cuando uses un dispositivo externo como el lector auxiliar 485.

La salida serial enviará las informaciones de abertura y cierre para el controlador de acceso. Esas informaciones pueden ser de dos tipos: ID del usuario o N° de la tarjeta.

Seleccionar la opción Entrada OSDP cuando uses un lector de tarjetas con protocolo OSDP conectado al controlador de acceso.

## 7.8. Sistema

### Fecha y hora

Para cambiar informaciones de fecha y hora como ajustar fecha, formato de fecha, ajustar hora, horario de verano, servicio NTP y huso horario, accede *Sistema > Fecha y hora.*

### Parámetros de rostro

Presiona sobre la(s) opción(es) que deseas cambiar, haz el debido ajuste y presiona salvar  .

- » **Umbral de detección facial:** ajusta la precisión del reconocimiento facial. Cuanto mayor el valor, mayor será la semejanza de la captura del dispositivo con la foto usada para el registro, o sea, menor será la tolerancia a variaciones de apariencia como expresiones faciales, barba, accesorios y edad del registro. Valor estándar es de 85.
- » **Máx. ángulo de reconocimiento facial:** ajusta el ángulo del perfil acepto por el dispositivo para iniciar el reconocimiento facial. Valor estándar es 90°.
- » **Distancia pupilar:** representa la cantidad de píxeles en la imagen, entre los centros de las pupilas. El valor muda de acuerdo con el tamaño del rostro y la distancia entre el rostro y la lente. Cuanto más próximo el rostro de la cámara, mayor será ese valor. La distancia pupilar para un adulto posicionado a 1,5 metros del dispositivo está entre 50 y 70. Valor estándar es 60.
- » **Tiempo limite de reconocimiento (s):** tiempo limite entre la presentación para el reconocimiento facial y el mensaje de acceso liberado.
- » **Tiempo limite para acceso facial negado:** tiempo limite entre el momento que se presenta el rostro que no tiene acceso en el dispositivo y el mensaje de acceso negado.
- » **Umbral anti-falso:** previne el uso de fotos, imágenes o vídeos en medio impreso o digital de acceder al dispositivo.
- » **Modo máscara:** permite cambiar y hasta bloquear usuarios sin máscara. Selecciona la opción No detectar para que el dispositivo no cambie o bloquee usuarios que no estén de máscara. Selecciona cambiar cuando deseas identificar los usuarios a través de reconocimiento facial y modificar los usuarios que no estén de máscara. Caso desees usar el reconocimiento facial y también bloquear usuarios que no estén de máscara, selecciona la opción bloquear.

  ***Obs:*** *para usar la opción bloquear usuarios sin máscara, será acepto apenas el método de autenticación facial. En la opción cambiar, se dará la alerta a todos los usuarios que usen métodos alternativos al reconocimiento facial.*

### Modo de imagen

En *Sistema > Modo de imagen* selecciona la opción que se adecua a tu escenario. Es posible ajustar la pantalla para el modo: *Interno, Externo u Otro.*

### Volumen

Usa las teclas + y – para ajustar el volumen del equipamiento.

### Parámetros de Imp. dig.

Ajusta el umbral de reconocimiento biométrico digital. Cuanto mayor sea el valor, mayor será la similitud entre la captura del dispositivo y la captura utilizada para realizar el registro, es decir, menor será la tolerancia a las variaciones. El valor predeterminado 3.

### Idioma

Los idiomas inglés, español y portugués están disponibles.

***Obs.:*** *es necesario reiniciar el dispositivo.*

**Intensidad de luz infrarroja**

Usa las teclas + y – para ajustar la intensidad de la luz infrarroja. Cuanto mayor el valor atribuido, más intensa será la emisión de la luz infrarroja.

**Configuraciones de pantalla**

» **Protección de pantalla:** configura cuanto tiempo después de ninguna acción el dispositivo exhibirá la protección de pantalla. Por estándar ese tiempo está en 30 segundos.

» **Tiempo limite de pantalla prendida:** configura cuanto tiempo después de ninguna acción la pantalla se apagará. Ese tiempo por estándar en la configuración es de 60 segundos.

***Obs.:*** *al detectar movimiento el dispositivo vuelve a la pantalla de verificación automáticamente.*

**Restaurar estándares de fábrica**

Datos se perderán al seleccionar restaurar estándares de fábrica.

Las configuraciones de IP no se modificarán al restaurar los estándares de fábrica.

Hay dos opciones para restaurar los estándares de fábrica:

» **Restaurar estándares de fábrica:** restaura las configuraciones para el **estándar** y borrar todos los datos del dispositivo.

» **Restaurar estándares de fábrica (mantener usuarios y eventos):** restaura las configuraciones para el **estándar** y mantiene los datos de usuario.

Después de seleccionar la opción deseada, confirma tu elección.

**Reiniciar**

Selecciona *Sistema > Reiniciar y* confirma para que el dispositivo se reinicie.

## 7.9. USB

**Atención:** verifica si el dispositivo de almacenamiento USB está correctamente insertado antes de exportar/importar datos de usuario o actualizar el producto. Nunca remuevas el dispositivo de almacenamiento USB mientras hace la exportación/importación o actualización del producto. De lo contrario la operación fallará.

Es necesario exportar las informaciones de un controlador de acceso antes de importar esas configuraciones a otro producto.

La entrada USB también puede ser usada para actualización de firmware.

***Obs.:*** *el dispositivo de almacenamiento debe estar formateado en FAT32.*

**Exportar**

Para exportar datos del dispositivo selecciona *USB > Exportar*.

Selecciona los datos que deseas exportar y confirma. El administrador puede optar por exportar los usuarios, los datos faciales, tarjetas, huellas digitales (cuando hay), eventos o todas las opciones anteriormente seleccionando la opción *Todos.*

**Importar**

Para importar datos para el dispositivo selecciona *USB > Importar.*

Selecciona los datos que deseas importar y confirma. Es posible importar usuarios, datos del rostro, tarjeta y huella digital que hayan sido exportados de otro dispositivo. También es posible importar fotos en formato JPG, donde el nombre del archivo debe ser la ID del usuario. Caso la ID del usuario no exista, una se creará con la foto disponible. Consulta la sección 10 para mas informaciones sobre los requisitos de las fotos.

**Actualizar**

Para actualizar a través de un dispositivo de almacenamiento USB rebautiza el archivo de actualización para *update.bin* y salva ese archivo en la raíz del dispositivo USB.

Para actualizar selecciona *USB > Actualizar y confirma.*

O, con el controlador de acceso apagado, conecte el dispositivo de almacenamiento al puerto USB y encienda el dispositivo. La actualización comenzará automáticamente.

### 7.10. Utilidades

En ese menú están las configuraciones de seguridad, opción para invertir el código recibido en la entrada Wiegand, habilitar el módulo de seguridad, configurar tipo de sensor de puerta y el resultado del feedback.

**Configuraciones de seguridad**

- **Habilitar restablecer la contraseña:** si habilitado, se permite **restablecer la contraseña** a través de la interfaz web.
- **HTTPS:** cuando habilitado, se usará el protocolo HTTPS para el acceso a los comandos CGI, de lo contrario se usará HTTP. El dispositivo reiniciará al habilitar o deshabilitar el protocolo HTTPS.
- **CGI:** ofrece un protocolo para que los softwares configuren el dispositivo. Habilita el uso del protocolo CGI.
- **SSH:** habilita el protocolo de seguridad SSH.
- **Capturar foto:** el dispositivo tomará una foto del usuario cuando hay una tentativa de acceso.
- **Limpiar todas las fotos capturadas:** promueve la remoción de todas las capturas.

**Módulo de seguridad**

Habilita el uso de un módulo externo para accionamiento de la puerta. Caso esta opción esté habilitada y el módulo de seguridad no esté conectado, o no responda, se negará el acceso mismo presentando credenciales válidas.

**Sensor de puerta**

El sensor de puerta se configurará como NA o NC.

- **NA:** cuando la puerta está abierta, el estado del sensor es normalmente abierto o NA.
- **NC:** cuando la puerta está abierta, el estado del sensor es normalmente cerrado o NC.

**Resultado del feedback**

- **Éxito o falla:** muestra el mensaje *¡Éxito!* acceso liberado y el mensaje *No autorizado* para acceso negado.
- **Solo nombre:** presenta ID del usuario, nombre y horario para el acceso liberado y el mensaje *No autorizado* y horario para el acceso negado.
- **Foto y nombre:** presenta ID del usuario, nombre y horario acompañado de la foto registrada para el acceso liberado y el mensaje *No autorizado* y horario para el acceso negado.
- **Foto, imagen y nombre:** presenta ID del usuario, nombre y horario acompañado de la foto registrada y de la foto actual para el acceso liberado y el mensaje *No autorizado* y horario acompañado de la foto actual para el acceso negado.

**MIP**

Al habilitar esta opción el dispositivo usará la entrada 485 para comunicarse con el dispositivo MIP 1000.

Verifica en la sección *5.5. Módulo inteligente de portería (MIP 1000)* como es la conexión de los dispositivos. Para informaciones de operación y registro consulta el manual de usuario del MIP 1000.

### 7.11. Eventos

En el menú Eventos es posible visualizar todos los eventos de acceso. Es posible hacer la busca por ID de usuario al acceder el ícono de lupa en el lado superior derecho.

### 7.12. Info. Sistema

En informaciones del sistema es posible consultar la capacidad de almacenamiento del dispositivo, número de serie, versión de software, versión de firmware y dirección MAC.

## 8. Interfaz web

El controlador de acceso puede configurar y operar en la web. A través de la web, es posible definir parámetros de red y de vídeo de acceso.

La interfaz web se puede usar para la actualización del sistema.

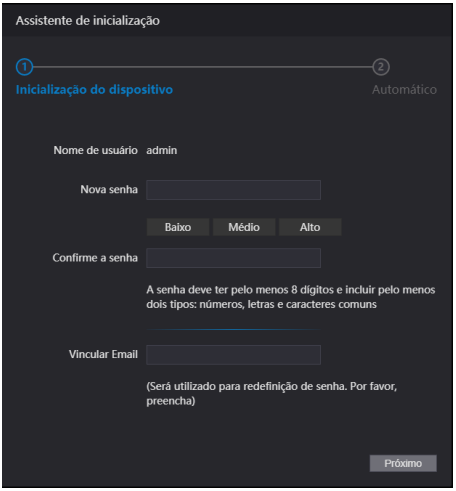
**Importante:** la gerencia de usuarios solo se pode hacer directamente en el dispositivo o con la ayuda de software, no se puede realizar registros de usuario o exportar/importar datos de usuarios a través de la interfaz web.

## 8.1. Inicio

Alternativamente el inicio del dispositivo en pantalla (ítem *7.1. Inicio del dispositivo*), puede registrar la contraseña del administrador del sistema a través de la interfaz WEB.

Para eso, abre el navegador y accede el IP del dispositivo (el IP estándar de la interfaz de red cableada es 192.168.1.201).

***Obs.:*** *usa la última versión del Microsoft Edge® o Chrome®.*




*Pantalla de inicio a través de la Interfaz web*

Entra con la nueva contraseña, confirma y agrega un correo electrónico válido y sigue para la próxima etapa.

**Importante:**

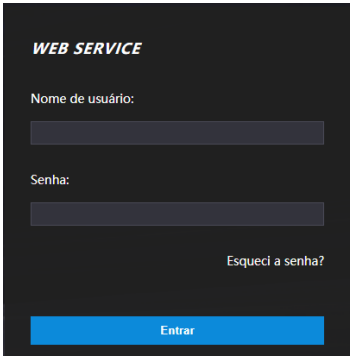
- » La contraseña del administrador se puede restablecer a través del correo electrónico tecleado, usa un correo electrónico válido y activo.
- » La contraseña debe tener de 8 a 32 caracteres, no puede tener espacios y debe tener por lo menos dos tipos de caracteres entre mayúsculas, minúsculas, número y caracteres especiales (excluyendo ' " ; : &).

En la siguiente pantalla el administrador puede optar por estar informado de una nueva versión cuando disponible (exige que el dispositivo esté conectado a la internet).

## 8.2. Login

Abre el navegador y accede el IP del dispositivo (el IP estándar de la interfaz de red cableada es 192.168.1.201).

Entra con el *Nombre de usuario y Contraseña* y presione *Entrar*.




*Pantalla de login*

**Importante:**

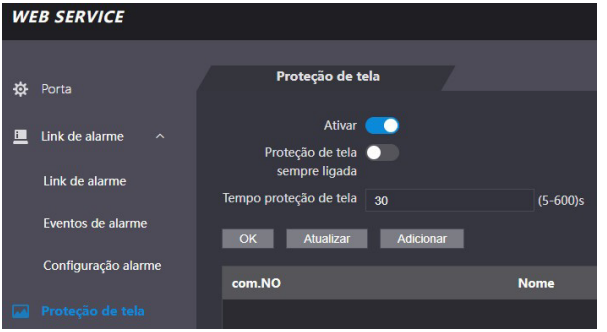
» El nombre de usuario estándar del administrador es admin y la contraseña es creada en el inicio del dispositivo (ver ítem *7.1. Inicio del dispositivo* o *8.1. Inicio*)

» Si te olvidas la contraseña de administrador, presiona *¿Olvidé la contraseña?* en la pantalla de login de la interfaz web y sigue las instrucciones en la pantalla (ver ítem *Olvidé la contraseña*).

### Olvidé la contraseña

Caso hayas olvidado la contraseña, usa la opción *¿Olvidé la contraseña?* en la interfaz WEB. Usa la cámara de tu celular para escanear el código QR presentado y sigue las instrucciones. Se enviará una contraseña en el correo electrónico registrado en el inicio del dispositivo. Inserta esa contraseña y una ventana para registrar una nueva contraseña se exhibirá. Caso el administrador no esté más disponible, ni el correo electrónico registrado, sigue los procedimientos presentados en la sección *9. Restaurar contraseña de administrador*.

## 8.3. Proteccion de pantalla




*Proteccion de pantalla*

» Formato: retrato;

» Tipo de archivo: .JPG o .JPEG;

» Resolución recomendada: 272 × 480;

» Tamaño máximo de archivo: 512 KB.

***Obs.:*** *es posible añadir sólo una imagen. El protector de pantalla se mostrará después del tiempo de pantalla activa (el tiempo predeterminado del dispositivo es de 30 segundos).*

## 8.4. Enlace de alarma

### Configuración de enlace de alarma

Dispositivos de alarma se pueden conectar al controlador de acceso y se puede configurar la acción del controlador de acceso, cuando recibir una entrada de alarma.

En *Enlace de alarma* > *Enlace de alarma* es presentado el canal de entrada. Para modificar presiona el ícono en la columna modificar.

» **Entrada:** no puede ser modificado. La entrada 1 se refiere a la entrada de alarma ALM_IN.

» **Nombre:** inserta un nombre para la zona de alarma.

» **Tipo de alarma:** selecciona de acuerdo con el sistema de alarma. Al seleccionar NA, la alarma se disparará caso se detecte el cierre de un circuito entre GND y la entrada de alarma. Al seleccionar NC, se disparará una alarma cuando es detectado que la entrada de alarma no está conectada al GND.

» **Activar enlace de incendio:** si el enlace de incendio está activo, el controlador de acceso destrabará la puerta si hay un accionamiento en la entrada de alarma. Al activar el enlace de incendio la puerta es configurada para siempre abierta. Verifica las demás configuraciones para la acción deseada.

» **Activar enlace de acceso:** cuando activo permite forzar el estado de la puerta en el campo *Tipo de canal*.

» **Tipo de canal:** si NA, abrirá y mantendrá la puerta abierta. En la opción NC mantendrá la puerta cerrada y negará cualquier intento de acceso.

### Eventos de alarma

En la opción *Eventos de alarma* es posible hacer una búsqueda por período y por tipo de alarma.

## 8.5. Capacidad

Al acceder la pestaña capacidad se presentan las cantidades de usuarios y credenciales registradas en el dispositivo.

## 8.6. Config. de vídeo

Están disponibles configuraciones de vídeo, detección de movimiento y modo de imagen.

### Configuraciones de vídeo

Permite ajustes en el streaming de vídeo y en la imagen presentada en la pantalla del dispositivo.

### Detección de movimiento

El área en rojo representa el área utilizada para detectar objetos en movimiento. El gráfico al lado permite visualizar la interacción entre movimiento y detección. Por estándar, todo frame es utilizado para detección de movimiento y los parámetros Sensibilidad y Umbral con el valor de 50. Para salvar tu modificación presiona *Ok*. Después de presionar *Estándar* para restaurar los estándares de fábrica, también es necesario presionar *Ok*.

### Modo de imagen

En *Config. De vídeo > Modo de imagen* selecciona la opción que se adecua a tu escenario. Es posible ajustar la pantalla para el modo: *Interno, Externo u Otro.*

## 8.7. Detección de rostro

En esa ventana es posible establecer una región para el control de acceso facial y el tamaño del rostro (que definirá la distancia de reconocimiento).

A través del botón *Detectar región* es posible ajustar el área de la pantalla en que el dispositivo efectuará el reconocimiento facial. Afuera de ese área el dispositivo no efectuará el reconocimiento facial.

El botón *Dibujar objetivo* permite especificar a partir de cual tamaño el dispositivo efectuará la verificación del rostro. Cuanto mayor el área, más próximo tiene que estar el usuario a ser identificado. Cuanto menor ese valor, mayor la distancia que el dispositivo efectuará la lectura del rostro.

- **Umbral de reconocimiento facial:** ajusta la precisión del reconocimiento facial. Cuanto mayor el valor, mayor será la semejanza de la captura del dispositivo com la foto usada para realizar el registro, o sea, menor será la tolerancia a variaciones de apariencia como expresiones faciales, barba, accesorios y edad del registro. Valor estándar es de 85.
- **Máx. ángulo de reconocimiento facial:** ajusta el ángulo del perfil acepto por el dispositivo para iniciar el reconocimiento facial. Valor estándar es 90°.
- **Umbral anti-fake:** previne el uso de fotos, imágenes o vídeos en medio impreso o digital de acceder al dispositivo.
- **Luz infrarroja:** ajusta la intensidad de la luz **infrarroja**. Cuanto mayor el valor atribuido, más intensa será la emisión de luz **infrarroja**.
- **Tiempo limite de reconocimiento (s):** tiempo limite entre la presentación para el reconocimiento facial y el mensaje de acceso liberado.
- **Tiempo limite para acceso facial negado:** tiempo limite entre el momento que se presenta el rostro que no tiene acceso en el dispositivo y el mensaje de acceso negado.
- **Distancia pupilar:** representa la cantidad de píxeles en la imagen entre los centros de las pupilas. El valor muda de acuerdo con el tamaño del rostro y la distancia entre el rostro y la lente. Cuanto más próximo el rostro de la cámara, mayor debe ser ese valor. La distancia pupilar para un adulto posicionado a 1,5 metros del dispositivo está entre 50 e 70. Valor estándar es 60.
- **ID canal:** son dos opciones: 1 para la cámara de luz visible y 2 para la cámara de luz infrarroja.
- **Activar Exp. Facial:** al activar esa opción, prepara el dispositivo para funcionar mejor en ambientes más iluminados como recepciones y áreas de acceso a visitantes.

  Para salvar tus cambios presiona *Ok*. Después de presionar Estándar para restaurar los estándares de fábrica, también es necesario presionar *Ok*.
- **Brillo objeto Rostro:** ajusta el brillo de la imagen capturada. El valor estándar es 50.
- **Intervalo de detección de exposición facial:** después que un rostro es detectado, el controlador de acceso emitirá luz para iluminar el rostro. El controlador de acceso no emitirá luz otra vez hasta que el intervalo definido haya pasado.

### 8.8. Red

Las configuraciones de dirección de IP, máscara de red y gateway estándar pueden ser consultadas o cambiadas en *Red > TCP/IP.* En *Red > Puertas* es posible establecer el número máximo de conexiones, puertas TCP, HTTP, HTTPS y RTSP. La opción *Red>Registro,* cuando activa permite conectar el controlador de acceso a plataformas de gerencia compatibles y de esa forma hacer gerencia del dispositivo. Es necesario configurar la dirección IP y puerta de comunicación del servidor, además de atribuir una ID al dispositivo.

### 8.9. Seguridad

En la opción *Seguridad>Seguridad IP* es posible limitar el acceso al dispositivo liberando o bloqueando IPs o segmentos de IP o por MAC. Usa la lista blanca para liberar o la lista negra para bloquear. Es posible configurar para ignorar comandos de PING e impedir semijoin.

En *Seguridad > Servicios* el administrador del dispositivo puede habilitar/deshabilitar los protocolos SSH, CGI, HTTPS, bien como habilitar el reinicio de contraseña a través de la opción *¿Olvidé la contraseña?* de la pantalla de login en la interfaz web.

### 8.10. Configuración de voz

En el menú *Config. de voz* se puede cambiar el volumen del dispositivo.

### 8.11. Usuarios de red

Permite registrar otros usuarios administradores y modificar el usuario admin.

**Importante:** el usuario admin no puede ser excluido.

### 8.12. Manutención

Define horario para que el dispositivo se reinicie automáticamente. De esta forma el sistema operacional se puede ajustar para mejorar la actuación y el desempeño. El dispositivo tiene por estándar la configuración definida para reiniciar todo martes a las dos de la mañana (de acuerdo con el reloj del dispositivo).

### 8.13. Gest. config.

Permite que el usuario administrador salve una copia de las configuraciones del dispositivo o restaurar una configuración previamente creada. Se puede usar cuando varios dispositivos necesitan utilizar la misma configuración.

**Gest. config.**

Para guardar la configuración de su dispositivo presione *Exportar configuraciones* y un archivo se salvará en tu dispositivo.

La importación puede ser realizada iniciando por Buscar el archivo deseado y entonces Importar configuraciones.

**Servicio eventos**

Al activar el servicio de eventos, el dispositivo enviará activamente los eventos a la dirección IP, puerto y Path configurados en esta página. Para obtener más información, consulte nuestro Soporte técnico para la documentación API/CGI.

### 8.14. Actualizar

**Importante:** usa apenas archivos proporcionados por la Intelbras.

Mantiene el dispositivo y el controlador de acceso energizados durante todo el proceso de actualización.

La actualización inicia por el botón *Buscar* para indicar la localización del archivo. Usa archivos locales, archivos en red pueden causar fallas en el proceso de actualización.

### 8.15. Informaciones de la versión

Presenta informaciones del sistema como versión de firmware, de la interfaz web, número de serie y MAC.

### 8.16. Usuario online

Al acceder Usuario online será exhibido una lista con el ID del usuario, nombre del usuario, dirección de IP y hora del login.

### 8.17. Eventos

Exhibe una lista con los eventos de administradores y eventos de sistema.

## 9. Restaurar contraseña de administrador

Caso no tengas más la contraseña del administrador y/o acceso al correo electrónico registrado en el inicio del dispositivo, puedes restaurar a través del hardware. Para eso, sigue las etapas listadas abajo.

1. Apague el controlador de acceso. Si su producto está montado en la pared, retire el tornillo de fijación del soporte y retire el dispositivo del soporte.
2. Mantenga presionado el botón de manipulación ubicado en la parte posterior del equipo;
3. Encienda el dispositivo;
4. Mantenga presionado el botón de manipulación y espere a que el dispositivo se inicie por completo, cuando la imagen de la cámara aparece en la pantalla;
5. Suelte el botón de manipulación;
6. Espere 30 segundos. Tenga en cuenta el mensaje *Cierre la tapa trasera en la pantalla del dispositivo*;
7. Presione y suelte el tamper 3 veces. El mensaje *Cierre la contraportada* se mostrará cada vez que se suelte el botón de manipulación;
8. Al soltar el tamper por tercera vez, el dispositivo se reiniciará y regresará a la pantalla de inicialización, permitiendo el registro de una nueva contraseña de administrador.

***Obs.:*** *todas las configuraciones son restauradas excepto usuarios y eventos. Usuarios que tengan privilegio de administrador también se mantienen restaurando apenas la contraseña de administrador que es registrada durante el inicio del equipamiento.*

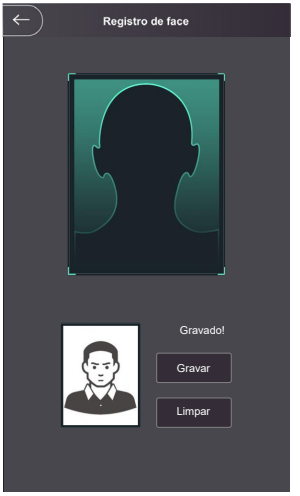
# 10. Buenas prácticas para el reconocimiento facial

## 10.1. Antes del registro

» Lentes, gorros y barbas pueden influenciar el desempeño del reconocimiento de rostro. No cubra las cejas al usar gorros.
» Actualiza el registro caso haya un cambio muy grande en el visual, como la retirada de la barba, si hay dificultad en el acceso.
» Mantenga el rostro visible.
» Mantenga el dispositivo por lo menos a dos metros de distancia de la fuente de luz y por lo menos a tres metros de ventanas o puertas; de lo contrario, la luz solar directa puede influenciar en el desempeño del reconocimiento de rostro del dispositivo.

## 10.2. Durante el registro

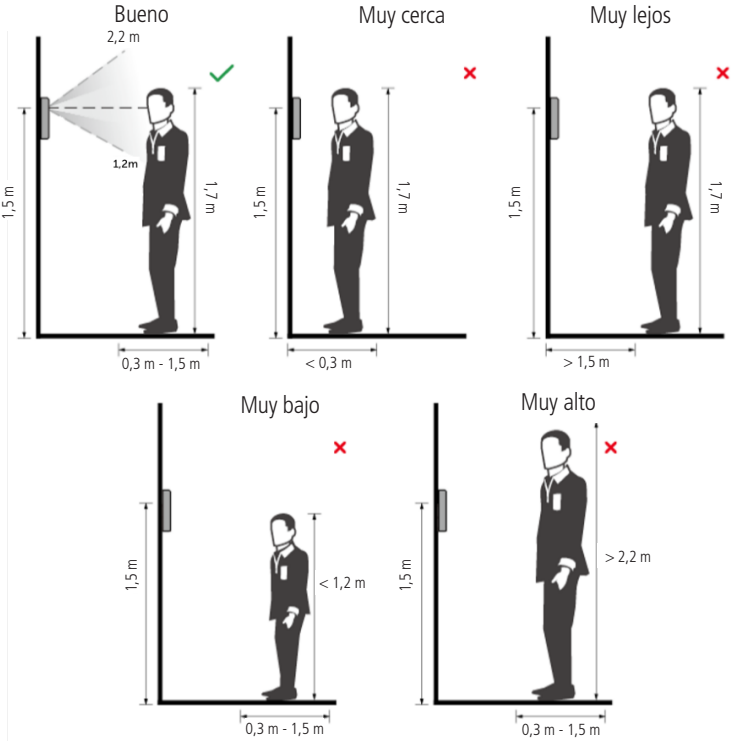
Puedes registrar rostros a través del controlador de acceso o a través del software. Para registro a través del software, consulta el manual del usuario del software. Posiciona la cabeza en la moldura de captura de fotos. Se capturará una foto de tu rostro automáticamente.




» Permanezca inmóvil, no muevas la cabeza o el cuerpo, pues el registro puede fallar.
» Encuadra todo el rostro, visión frontal y de ojos abiertos;
» Encuadra de la cabeza a los hombros;
» Haz preferencia por un fondo neutro;
» Apenas un rostro debe aparecer en la foto;
» El rostro debe estar completamente visible, libre de cualquier objeto que lo pueda cubrir (ej.: máscara);
» Evita sombras en el rostro o al fondo;
» Haz una expresión neutra y natural.

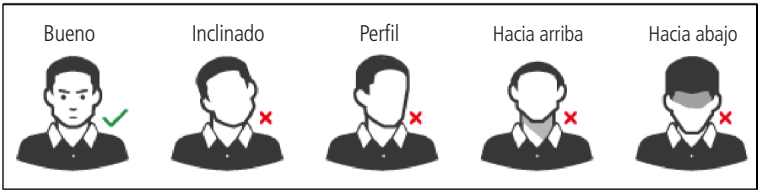
**Posición del rostro**

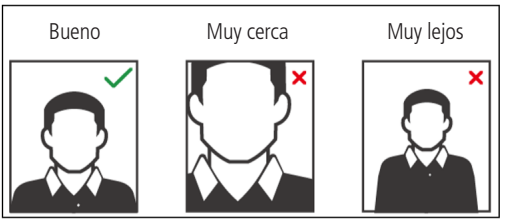
Si tu rostro no está en la posición apropiada, el efecto de reconocimiento de rostro se puede influenciar.



**Requisitos de rostros**

- » Verifica si el rosto está visible y si la frente no está cubierta por cabellos.
- » Encuadra todo el rostro, mirando hacia la cámara o luego abajo de ella en el tope de la pantalla y abre los ojos durante el registro.
- » Evita usar lentes y no uses gorros u otros adornos para el rostro que influencien la grabación de la imagen del rostro, o que incluye máscaras faciales.
- » Encuadra de la cabeza a los hombros y haz preferencia por un fondo neutro o blanco.
- » Evita sombras en tu rostro o en el fondo.
- » Haz una expresión neutra y natural y mantenga los brazos a lo largo del cuerpo.
- » Al gravar tu rostro o durante el reconocimiento de rostro, no lo mantengas muy próximo o muy lejos de la cámara.




**Requisitos para importación de fotos**

Cuando importes las fotos de usuarios - a través de la entrada USB o usando un software de gerencia de control de acceso compatible - se recomienda usar imágenes con resolución superior a 500 × 500 píxeles (L × A)[1], donde el rostro no debe ocupar más que 2/3 del área total de la imagen. En caso de bases de datos preexistente, atenta para las resoluciones mínima y máxima:

- » **Resolución mínima:** 150 × 300 píxeles (L × A)[1]
- » **Resolución Máxima:** 600 × 1200 píxeles (L × A)[1]

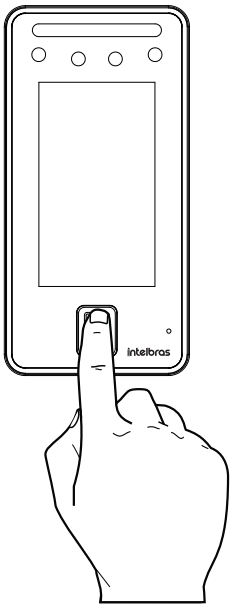
Para todos los casos, el tamaño máximo del archivo debe ser inferior a 100 KB y estar en el formato JPG.

*[1] La altura no debe exceder dos veces el ancho. Por ejemplo, si el ancho es 300 píxeles, entonces la altura podrá ser igual o inferior a 600 píxeles.*

# 11. Buenas prácticas para el reconocimiento biométrico digital

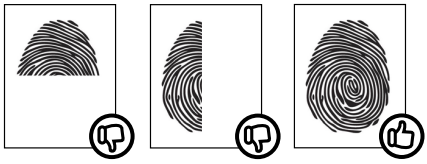
## 11.1. Postura recomendada en el registro

» Colóquese frente al equipo, coloque el dedo directamente sobre el lector biométrico y espere la confirmación de la captura de la plantilla.




» No presione el dedo con demasiada fuerza sobre el sensor biométrico, esto distorsiona la imagen de la huella dactilar y no permite que el dispositivo identifique los puntos formados por las intersecciones de las líneas (crestas y valles) que forman la huella dactilar.

» No coloque el dedo torcido o solo la punta del dedo sobre el sensor biométrico. El uso inapropiado del sensor biométrico en la lectura de la huella dactilar impide que el sistema transmita una imagen susceptible de ser transformada en una plantilla.



» Siga las instrucciones visuales y audibles para realizar capturas biométricas digitales.

# Póliza de garantía

Importado por:

**Intelbras S/A - Industria de Telecomunicación Electrónica Brasileña**

Rodovia SC 281, km 4,5 – Sertão do Maruim – São José/SC – Brasil – 88122-001

CNPJ 82.901.000/0014-41 – www.intelbras.com.br

soporte@intelbras.com | www.intelbras.com

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

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

ESTA GARANTÍA NO ES VÁLIDA EN LOS SIGUIENTES CASOS:

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

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

**Datos del producto y distribuidor.**

| | |
|---|---|
| Producto: | Colonia: |
| Marca: | C.P.: |
| Modelo: | Estado: |
| Número de serie: | Tipo y número de comprobante de compra: |
| Distribuidor: | Fecha de compra: |
| Calle y número: | Sello: |

# Término de garantía

Queda expreso que esta garantía contractual es conferida mediante las siguientes condiciones:

Nombre del cliente:

Firma del cliente:

Nº de la nota fiscal:

Fecha de la compra:

Modelo: Nº de serie:

Revendedor:

1. Todas las partes, piezas y componentes del producto son garantizados contra eventuales vicios de fabricación, que por ventura vengan a presentar, por el plazo de 1 (un) año – siendo este de 90 (noventa) días de garantía legal y 9 (nueve) meses de garantía contractual –, contado a partir de la fecha de la compra del producto por el Señor Consumidor, conforme consta en la nota fiscal de compra del producto, que es parte integrante de este Término en todo el territorio nacional. Esta garantía contractual comprende el cambio gratuito de partes, piezas y componentes que presentaren vicio de fabricación, incluyendo los gastos con la mano de obra utilizada en ese reparo. Caso no sea constatado vicio de fabricación, y si vicio(s) proveniente(s) de uso inadecuado, el Señor Consumidor arcará con esos gastos.
2. La instalación del producto debe ser hecha de acuerdo con el Manual del Producto y/o Guía de Instalación. Caso tu producto necesite la instalación y configuración por un técnico capacitado, busca un profesional idóneo y especializado, siendo que los gastos de esos servicios no están inclusos en el valor del producto.
3. Constatado el vicio, el Señor Consumidor deberá inmediatamente comunicarse con el Servicio Autorizado más próximo que conste en la relación ofrecida por el fabricante – solo estos están autorizados a examinar y sanar el defecto durante el plazo de garantía aquí previsto. Si eso no es respetado, esta garantía perderá su validad, pues estará caracterizada la violación del producto.
4. En la eventualidad del Señor Consumidor solicitar atendimiento domiciliar, deberá encaminarse al Servicio Autorizado más próximo para consulta de la tasa de visita técnica. Caso sea constatada la necesidad de la retirada del producto, los gastos corrientes, como los de transporte y seguridad de ida y vuelta del producto, quedan bajo la responsabilidad del Señor Consumidor.
5. La garantía perderá totalmente su validad en ocurrencia de cualesquiera de las siguientes hipótesis: a) si el vicio no es de fabricación , mas si causado por el Señor Consumidor o por terceros extraños al fabricante; b) si los daños al producto son oriundos de accidentes, siniestros, agentes de la naturaleza (rayos, inundaciones, deslizamientos, etc.), humedad, tensión en la red eléctrica (sobretensión provocada por accidentes o fluctuaciones excesivas en la red), instalación/uso en desacuerdo con el manual del usuario o debido al desgaste natural de las partes, piezas y componentes; c) si el producto haya sufrido influencia de naturaleza química, electromagnética, eléctrica o animal (insectos, etc.); d) si el número de serie del producto fue adulterado o tachado; e) si el aparato fue violado.
6. Esta garantía no cubre pérdida de datos, por lo tanto, se recomienda, si es el caso del producto, que el Consumidor haga una copia de seguridad regularmente de los datos que constan en el producto.
7. La Intelbras no se responsabiliza por la instalación de este producto, y también por eventuales tentativas de fraudes y/o sabotajes en tus productos. Mantenga las actualizaciones del software y aplicaciones utilizados al día, si es el caso, así como las protecciones de red necesarias para protección contra invasiones (hackers). El equipamiento es garantizado contra vicios dentro de sus condiciones normales de uso, siendo importante que se tenga ciencia de que, por ser un equipamiento electrónico, no está libre de fraudes y burlas que puedan interferir en su correcto funcionamiento.
8. Después de su vida útil, el producto debe ser entregue a una asistencia técnica autorizada de la Intelbras o realizar directamente la destinación final ambientalmente adecuada evitando impactos ambientales y a la salud. Caso prefieras, la pila/batería así como demás electrónicos de la marca Intelbras sin uso, puede ser descartado en cualquier punto de colecta de la Green Eletron (gestor de residuos electroelectrónicos a lo cual somos asociados). En caso de duda sobre el proceso de logística reversa, entra en contacto con nosotros por los teléfonos (48) 2106-0006 o 0800 704 2767 (de lunes a viernes, de las 08 a las 20h y a los sábados de las 08 a las 18h) o a través del correo electrónico suporte@intelbras.com.br.

Siendo estas las condiciones de este Término de Garantía complementar, la Intelbras S/A se reserva el derecho de alterar las características generales, técnicas y estéticas de sus productos sin previo aviso.

Todas las imágenes de este manual son ilustrativas.

intelbras

fale com a gente / hable con nosotros

**Brasil**
**Suporte a clientes:** (48) 2106 0006
**Fórum:** forum.intelbras.com.br
**Suporte via chat:** chat.intelbras.com.br
**Suporte via e-mail:** suporte@intelbras.com.br
**SAC:** 0800 7042767
**Onde comprar? Quem instala?:** 0800 7245115

**Otros países**
soporte@intelbras.com

Importado no Brasil por: / Importado en Brasil por:
Intelbras S/A – Indústria de Telecomunicação Eletrônica Brasileira
Rodovia SC 281, km 4,5 – Sertão do Maruim – São José/SC – 88122-001
CNPJ 82.901.000/0014-41 – www.intelbras.com.br | www.intelbras.com

01.22
Origem: China
Fabricado en China