



Manual do usuário
Manual del usuario

InControl Web

Índice

Português	6
1. Instalação	7
1.1. Especificação do servidor	7
1.2. Especificação da máquina cliente	8
1.3. Processo de instalação	8
1.4. Verificando a instalação	10
1.5. Limitações do software InControl	12
1.6. Primeiros Passos para aplicações em condomínios residenciais	13
1.7. Primeiros Passos para organizações ou empresas	13
2. Ambientação	14
2.1. Login	14
2.2. Tela Inicial	15
2.3. Painel de controle	17
2.4. Log de eventos	18
2.5. Perfil	18
2.6. Cor de Fundo	22
2.7. Linguagem	24
2.8. Monitoramento de sincronismo	25
3. Usuários	26
3.1. Cadastro de usuários	26
3.2. Cadastro de departamentos	49
3.3. Cadastro de visitantes	51
3.4. Cadastro de credenciais	60
3.5. Cadastro de Operadores do sistema	63
3.6. Cadastro de Perfis para operadores do sistema	65
3.7. Cadastro de sites	69

4. Dispositivos	71
4.1. Cadastro de Áreas	71
4.2. Cadastro de Dispositivos	75
5. Controle de acesso	79
5.1. Zonas de tempo	80
5.2. Pontos de acesso	83
5.3. Grupo de pontos de acesso	85
6. Feriados	86
6.1. Ações vinculadas a eventos	88
6.2. Intertravamento	90
7. Relatórios	92
7.1. Eventos de usuários	92
7.2. Eventos de operadores	94
7.3. Monitoramento	95
7.4. Monitoramento de área	96
8. Sistema	98
8.1. Gerenciamento de banco de dados	98
8.2. Configurações	102
8.3. Acesso via web	106
8.4. Atualizações	106
Política de privacidade	108
Termos de uso de software	112

1. Instalación	120
1.1. Especificación del servidor	120
1.2. Especificación de la máquina cliente	121
1.3. Proceso de instalación	121
1.4. Verificando la instalación	123
1.5. Limitaciones del software InControl	125
1.6. Primeros Pasos para aplicaciones en condominios residenciales	126
1.7. Primeros Pasos para organizaciones o empresas	127
2. Ambientación	128
2.1. Login	128
2.2. Pantalla Inicial	128
2.3. Panel de control	130
2.4. Log de eventos	131
2.5. Perfil	131
2.6. Color de Fondo	135
2.7. Lenguaje	137
3. Usuarios	138
3.1. Registro de usuarios	138
3.2. Registro de departamentos	163
3.3. Registro de visitantes	166
3.4. Registro de credenciales	174
3.5. Registro de Operadores del sistema	176
3.6. Registro de Perfiles para operadores del sistema	179

4. Dispositivos	183
4.1. Registro de Áreas	183
4.2. Registro de Dispositivos	186
5. Control de acceso	191
5.1. Zonas de tiempo	191
5.2. Puntos de acceso	194
5.3. Grupo de puntos de acceso	198
6. Feriados	200
6.1. Acciones vinculadas a eventos	201
6.2. Intertrabado.	203
7. Informes	205
7.1. Eventos de usuarios	205
7.2. Eventos de operadores.	206
7.3. Monitoreo	207
8. Sistema	209
8.1. Gerenciamiento de base de datos.	209
8.2. Configuraciones.	212
8.3. Acceso via web	215
8.4. Actualizaciones	216
Política de privacidad	218
Términos de utilización de software	222

intelbras

InControl Web Software

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

O software InControl Web é uma plataforma de gerenciamento e controle de acesso para dispositivos controladores de acesso com comunicação TCP/IP fabricados pela Intelbras nos modelos suportados pelo software. Com ele, é possível acompanhar os logs de eventos de acesso em tempo real por todas as telas e janelas do software, efetuar cadastros de usuários, credenciais de acesso, visitantes, bem como suas respectivas regras de acesso.

Através de uma plataforma web interativa, o operador possui opções de adequação de sua ambientação para uma experiência mais confortável a cada perfil. Por ser um software versátil, é possível acessar a sua plataforma de qualquer ambiente através dos navegadores de internet Google Chrome®, Firefox® e Safari® em rede local o que torna as consultas e o gerenciamento mais ágeis.

Possui um Banco de Dados robusto com suporte a várias interações de cadastro e autonomia para até 80 dispositivos controladores de acesso.

Para o acesso de sua plataforma via web, é necessário que o sistema esteja instalado em um servidor específico que hospedará a aplicação e seu respectivo banco de dados, sendo possível acessar sua interface através do endereço do IP do servidor e de sua porta de comunicação no qual o sistema está instalado ou pelo *Nome do Servidor*.

O software é compatível com sistema operacional Windows® nas versões 7 e 10 bem com as suas derivações destas versões.

A composição da solução InControl se mostra versátil também para desenvolvedores parceiros da Intelbras que contam com módulos disponíveis para conexões com seus próprios softwares e aplicações de mercado, tornando assim a Intelbras *Sempre Próxima*.

1. Instalação

A instalação da solução no servidor deve ser feita exclusivamente em Sistema Operacional Windows nas suas versões 7 e 10.

1.1. Especificação do servidor

Especificação do servidor para até 20 dispositivos:

- » Processador com 2 núcleos de 2,5 GHz
- » 2 Gb de RAM DDR 3
- » 60 Gb de HD

Especificação do servidor para até 40 dispositivos:

- » Processador com 4 núcleos de 2,5 GHz
- » 4 Gb de RAM DDR 3
- » 120 Gb de HD SATA 3

Especificação do servidor para até 60 dispositivos:

- » Processador com 8 núcleos de 2,5 GHz
- » 6 Gb de RAM DDR 4
- » 180 Gb de HD SATA 3

Especificação do servidor para até 80 dispositivos:

- » Processador com 8 núcleos de 2,5 GHz
- » 8 Gb de RAM DDR 4
- » 240 Gb de HD SSD

Obs.: as especificações de servidor são referentes ao consumo de recursos por parte do sistema Incontrol. A máquina deve ser dimensionada considerando-se também as exigências de hardware dos demais sistemas instalados no servidor, ou seja, além dos recursos do Incontrol, deve-se levar em conta os recursos do sistema operacional, dos softwares antivírus e de backup, entre outros. É altamente recomendado que o servidor seja uma máquina dedicada a controle de acesso.

1.2. Especificação da máquina cliente

Abaixo as configurações necessárias para a máquina Cliente separados por sistema operacional:

Windows 7 64 bits SP1

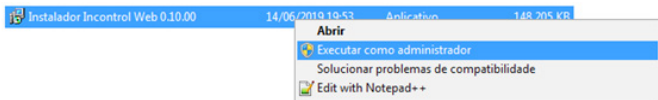
- » Processador core I3;
- » Memória RAM de 8 Gb;
- » HD 500 Gb;
- » Navegador Google Chrome®: Versão 75.0.3770.142 (oficial) 64 bits ou superior;
- » Navegador Firefox®: Quantum, versão 66.0.3 (64 bits).
- » Navegador Safari®: Versão 13.0.5 (64 bits) ou superior.

Windows 10 64 bits

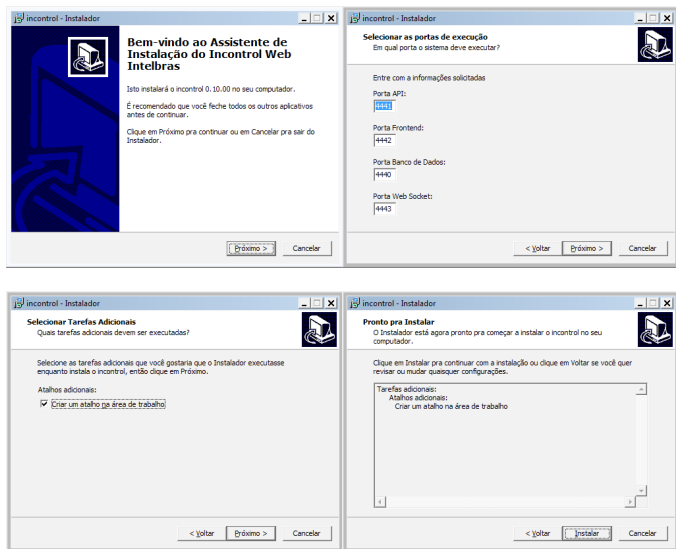
- » Processador core I3;
- » Memória RAM de 8GB;
- » HD 500 Gb;
- » Navegador Google Chrome®: Versão 75.0.3770.100 (oficial) 64 bits ou superior;
- » Navegador Firefox®: Quantum, versão 68.0.3 (64 bits).
- » Navegador Safari®: Versão 13.0.5 (64 bits) ou superior.

1.3. Processo de instalação

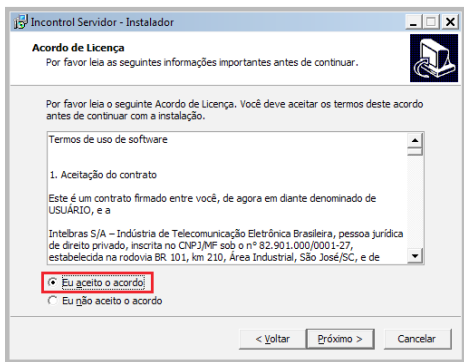
Após efetuar o download do instalador do software no site www.intelbras.com.br, é necessário descompactar o pacote e na sequência, clicar sobre o ícone de instalação com o botão direito do mouse e selecionar a opção *Executar como Administrador*.



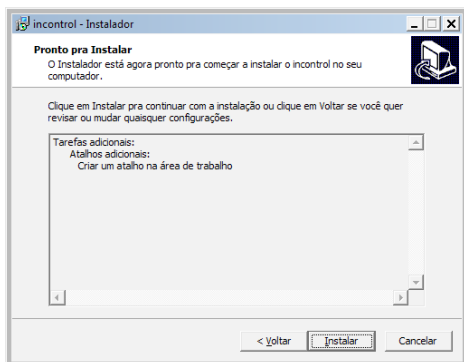
Uma nova janela se abrirá e será necessário clicar no botão *Próximo* a medida em que for pedido, para que o processo seja executado.



Importante: as portas de comunicação já vêm pré-configuradas por padrão de fábrica. Estas são as comumente compatíveis com o software e dispositivos. Recomendamos a não alteração das mesmas.



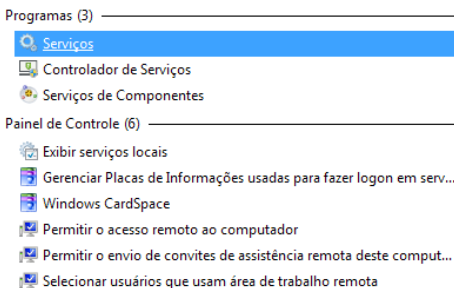
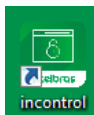
Leia os termos de uso e o aceite para iniciar a instalação. Após o término da instalação, clique no botão *Fechar* para encerrar o instalador.



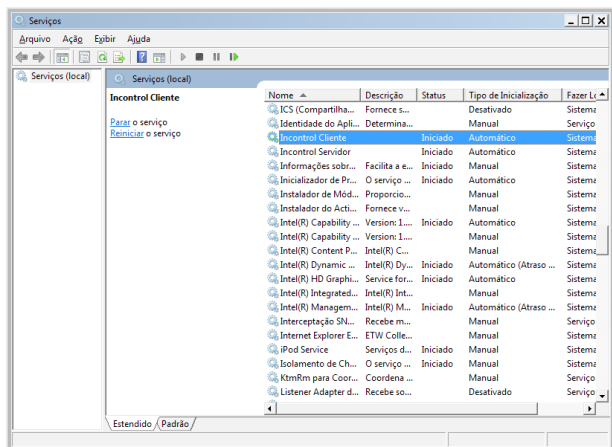
1.4. Verificando a instalação

Confira após a instalação, se o ícone do software foi criado na área de trabalho no computador.

Confira se foi criado o serviço do Windows® de nome *InControl Service* e se o mesmo está em execução. Para isso, clique no botão *Iniciar* na barra de tarefas do Windows®, e no campo de pesquisa, digite *Serviços*.

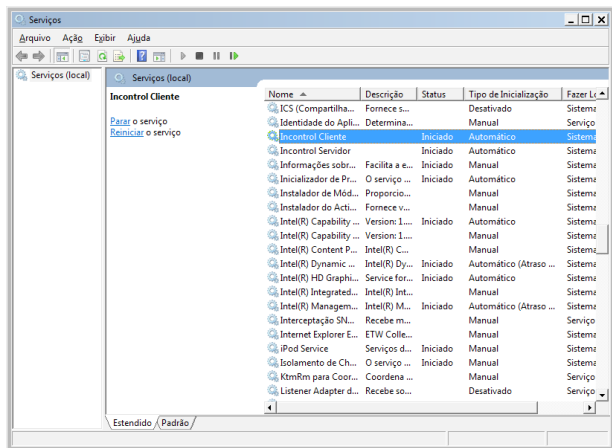


Na nova janela verifique se o serviço InControl servidor foi criado e se encontra em execução.



Importante: para o software funcionar corretamente, é necessário que o serviço do software esteja sendo executado ou iniciado.

É possível identificar também se o serviço do cadastrador de mesa está instalado no computador. Serviço *Incontrol Cliente*.



Importante:

- » O serviço InControl Cliente só será instalado após fazer o download do instalador na tela de cadastro de credenciais do tipo Digital em *Credenciais* ou durante o cadastro de Usuários.
- » A desinstalação do software deve acontecer via *Painel de Controle* do Windows® utilizando a função *Adicionar/Remover programas*.
- » Para o funcionamento correto do software é recomendado que a comunicação com o servidor e os dispositivos seja feita via rede ethernet.

1.5. Limitações do software InControl

- » Número máximo de dispositivos: 80 dispositivos controladores de acesso (controladoras);
- » Número de máquinas cliente: 20 máquinas por servidor;
- » Limite de zonas de tempo: 16 zonas de tempo com até 3 períodos cada.
- » Navegadores web: Chrome®, Firefox® e Safari®;
- » Sistemas operacionais compatíveis: Windows® 7 64 bits SP1 e Windows® 10 64 bits.
- » Banco de dados compatível: PostgreSQL.
- » Dispositivos suportados: CT 500 Series, SS 120, SS 230, SS 230 MF, SS 311 E, SS 311 MF, SS 320, SS 320 MF, SS 411 E, SS 420, SS 420 MF e SS 5520.

1.6. Primeiros Passos para aplicações em condomínios residenciais

1. Efetue o cadastro das áreas do condomínio onde os dispositivos controladores de acesso estarão instalados, (mais informações consulte o capítulo *Áreas* deste manual).
2. Após cadastrar as áreas do condomínio, efetue a adição dos dispositivos de controle de acesso, vinculando as suas respectivas áreas cadastradas previamente, (mais informações consulte o capítulo *Dispositivos* deste manual).
3. Cadastre o Grupo de Pontos de acesso vinculando as zonas de tempo necessárias e os dispositivos do sistema, (mais informações, consulte o capítulo *Grupo de Pontos de Acesso* deste manual).
4. Com as áreas e dispositivos cadastrados, insira os departamentos do seu condomínio, que podem ser os blocos existentes por exemplo, (mais informações, consulte o capítulo *Departamentos* deste manual).
5. Cadastre os usuários que terão acesso aos dispositivos de controle, vinculando-os aos departamentos cadastrados, (mais informações consulte a seção *Usuários* deste manual).
6. Cadastre também os perfis de operadores do sistema ou crie novos, concedendo acesso a diferentes seções do software conforme a sua necessidade, (mais informações, consulte o capítulo *Perfil de Operadores* deste manual).
7. Por fim, cadastre os demais operadores do sistema com login e senha diferente ao operador Admin, (mais informações, consulte ao capítulo *Operadores* deste manual).

1.7. Primeiros Passos para organizações ou empresas

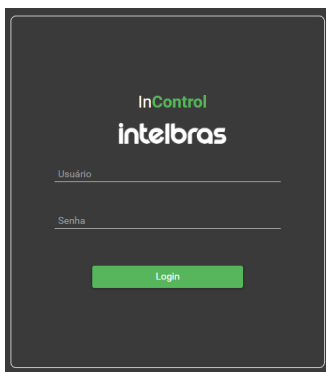
1. Efetue o cadastro das áreas da empresa onde os dispositivos controladores de acesso estarão instalados, (mais informações consulte o capítulo *Áreas* deste manual).
2. Após cadastrar as áreas da empresa, efetue a adição dos dispositivos de controle de acesso, vinculando as suas respectivas áreas cadastradas previamente, (mais informações consulte o capítulo *Dispositivos* deste manual).
3. Cadastre o Grupo de Pontos de acesso vinculando as zonas de tempo necessárias e os dispositivos do sistema, (mais informações, consulte o capítulo *Grupo de Pontos de Acesso* deste manual).
4. Com as áreas e dispositivos cadastrados, insira os departamentos da sua empresa, que serão os setores existentes na mesma, (mais informações, consulte o capítulo *Departamentos* deste manual).
5. Cadastre os usuários que terão acesso aos dispositivos de controle, vinculando-os aos departamentos cadastrados, (mais informações consulte a seção *Usuários* deste manual).

6. Cadastre também os perfis de operadores do sistema ou crie novos, concedendo acesso a diferentes seções do software conforme a sua necessidade, (mais informações, consulte o capítulo *Perfil de Operadores* deste manual).
7. Por fim, cadastre os demais operadores do sistema com login e senha diferente ao operador Admin, (mais informações, consulte ao capítulo *Operadores* deste manual).

2. Ambientação

2.1. Login

Para acessar a plataforma via navegador web, de um duplo clique no atalho do software criado na área de trabalho do servidor. Após acessar a interface via navegador de internet o operador é direcionado a uma tela de login onde deverá inserir suas credenciais e senha para acessar as funções do software.



O padrão de fábrica de usuário e senha é:

- » **Usuário:** admin
- » **Senha:** admin

Importante: recomendamos que após o primeiro login seja alterado o padrão de credenciais de fábrica para informações que não sejam de conhecimento comum.

2.2. Tela Inicial

Após o login no software o operador será direcionado para a tela inicial do software. Nesta tela podem ser acessadas todas as funções através do Menu lateral.

Na barra superior, estão disponíveis as funções relativas ao perfil do operador, tema do software, tradução do software, etc.

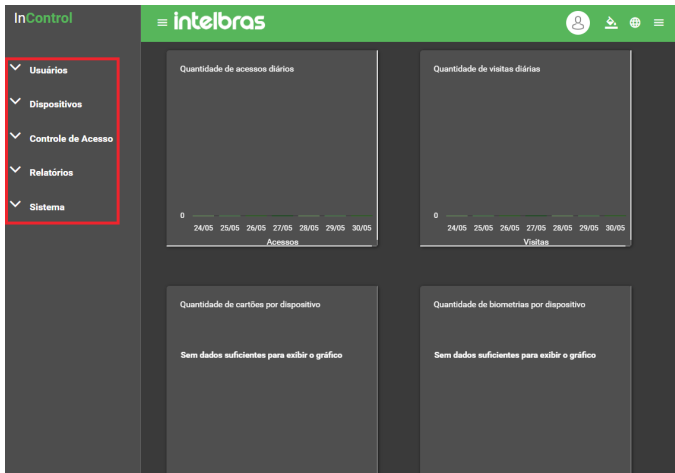
Na tela inicial estão representados o Painel de Controle com dados relativos ao sistema de controle de acesso, tais como acessos gerados, número de usuários, número de dispositivos, etc.

Na barra lateral direita, está disponível um *Log de Eventos* que exhibe todos os últimos acessos ou tentativas de acessos à medida que vão sendo gerados.



Barra de funcionalidades

A barra de funcionalidades proporciona ao operador do software navegar por todas as funcionalidades do sistema de controle de acesso de modo que ao clicar nos títulos, suas subseções são disponibilizadas para a navegação. Como demonstrado na figura abaixo:



A medida que as subseções são exibidas, os títulos das seções subsequentes vão sendo deslocadas mais para baixo na janela do navegador web.

Importante: recomendamos que após o término das configurações de uma seção, a mesma seja *fechada* antes da abertura da próxima, para garantir a visualização das sub opções das funcionalidades *macro* que estão localizadas na parte inferior da Barra de Funcionalidades.

2.3. Painel de controle

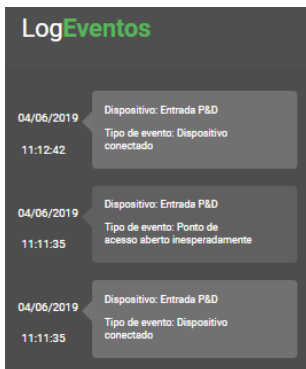
No painel de controle são exibidos dados estatísticos do sistema de controle de acesso como um todo. Esta seção, faz parte da tela inicial do sistema e nela o operador, pode ter algumas informações gerenciais de forma mais dinâmica e imediata. Nesta seção, estão exibidos os seguintes dados:

- » Quantidade de visitas na semana: demonstra dia a dia quantas visitas que houveram;
- » Quantidade de acessos na semana: demonstra dia a dia quantas acessos que houveram;
- » Quantidade de biometrias X Capacidade por dispositivo: Ilustra para o operador o número de credenciais biométricas já estão cadastradas no dispositivo e qual o espaço ainda disponível.
- » Quantidade de credenciais RFID X Capacidade do dispositivo: ilustra para o operador o número de credenciais RFID que já estão cadastradas no dispositivo e qual o espaço ainda disponível.



2.4. Log de eventos

Na aba lateral do sistema está localizada a barra de Log de Eventos, nela são exibidos os últimos eventos de acesso que forem ocorrendo durante a operação do sistema.

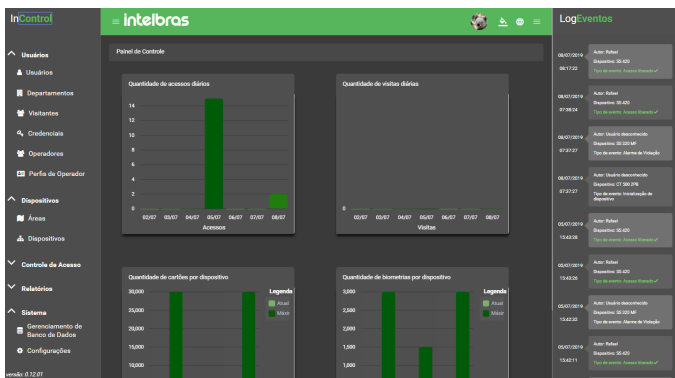


2.5. Perfil

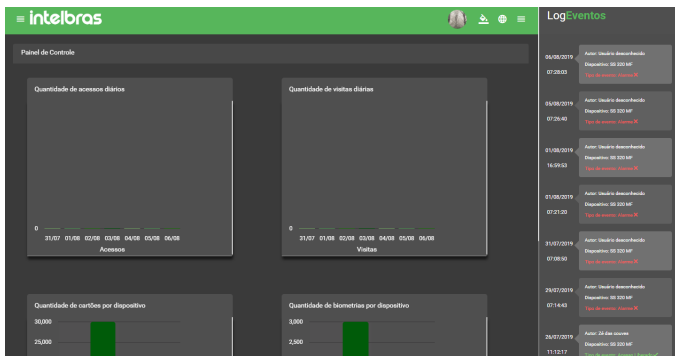
Na parte superior da tela do software está disponível as opções de personalização nas questões de visualização e de perfil do operador. Ao lado da logo *Intelbras*, é possível visualizar um ícone de 3 traços que quando acionado, possibilita uma expansão da tela para o lado esquerdo, ocultando a barra lateral de funcionalidades.



A visualização padrão da tela inicial é semelhante a imagem que segue abaixo:



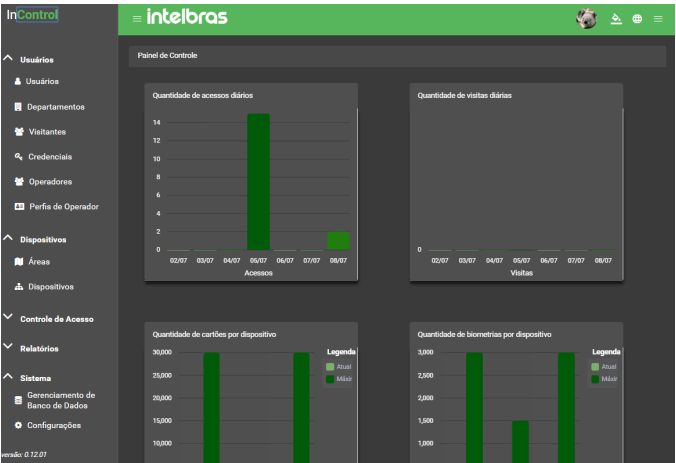
Após o acionamento do ícone de expansão de tela a barra de funcionalidades é ocultada e a tela passa a ocupar mais espaço de exibição.



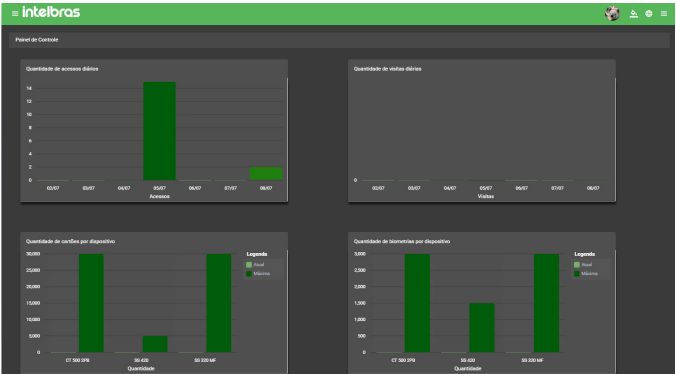
Da mesma forma, no canto direito da barra superior do software, existe um segundo botão de expansão da tela, que ao ser acionado, oculta a barra de log de eventos.



Após o acionamento deste botão, a tela se expande para o lado direito com a representação abaixo:



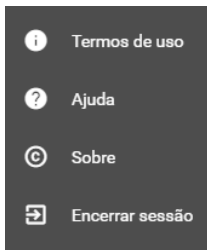
Por fim, com ambos os botões acionados a tela inicial ocupa toda a extensão da tela de exibição.



Na barra superior é possível selecionar, algumas opções referentes ao perfil do operador do sistema, este botão é representado pelo ícone descrito na figura abaixo:

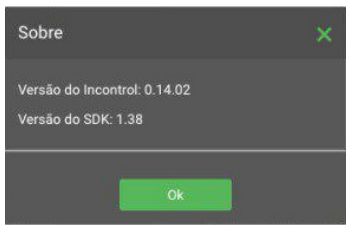


Clicando sobre o botão referente ao perfil do operador do sistema, serão exibidas as opções para consulta e acesso: Termos de uso, manual do software (Ajuda), informações referentes a versão do software instalada (Sobre) e a opção de sair do software (Encerrar sessão).

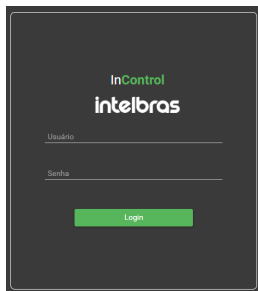


Clicando sobre o botão *Ajuda*, é possível fazer o download do manual do usuário do software, do documento de Termos de uso do software InControl e da Política de privacidade do software inControl.

Clicando sobre o botão *Sobre* será exibida para o operador, uma nova janela que exibe as informações sobre o pacote de instalação do software InControl.



Clicando sobre o botão *Encerrar sessão*, o operador encerra a sua sessão no software e volta à tela de Login.



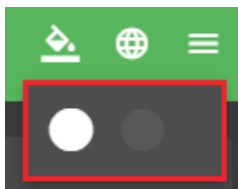
Importante: de volta a tela do login do software, será necessário digitar as credenciais de acesso do operador do sistema novamente para ter acesso às funções do sistema.

2.6. Cor de Fundo

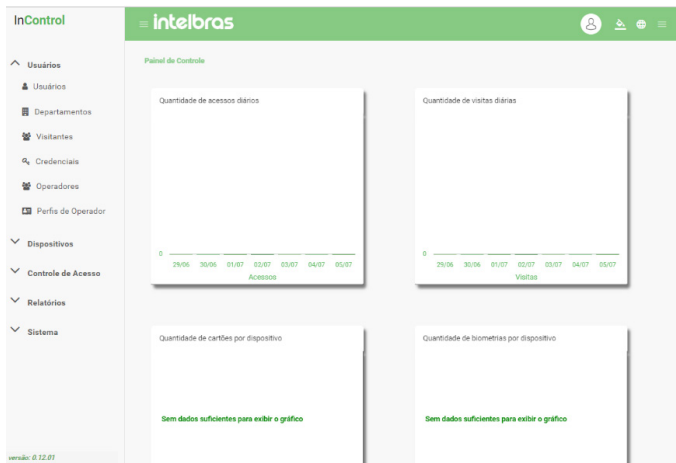
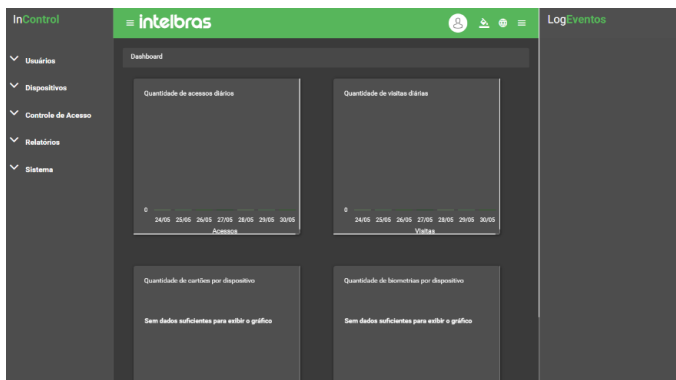
Na barra superior do software, é possível acionar o botão de alteração da *cor de fundo* do software InControl, esta função, dá ao operador a opção de duas cores de fundo para visualização dos ícones em todas as demais telas do software. As opções são:

- » Preto: (Opção padrão do software);
- » Branco.

Para selecionar uma ou outra opção, basta clicar sobre o ícone na barra superior ilustrado abaixo e na nova janela que se abrirá, fazer a opção de melhor preferência do operador do sistema.



Abaixo está representada a tela inicial do software na cor padrão e na cor branca.



2.7. Linguagem

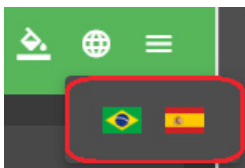
O software InControl, traz ao operador algumas opções de tradução de linguagem. São elas:

- » Português (Brasileiro);
- » Espanhol.

A linguagem padrão do software é o Português brasileiro, para alterar este idioma, basta clicar sobre o botão de linguagem localizado na barra superior do software.



Na nova janela, escolha a opção de linguagem para que as telas sejam traduzidas.



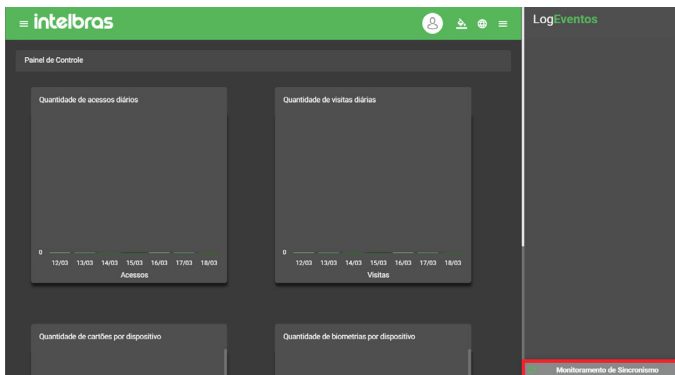
A tela do software traduzida na linguagem selecionada é exibida abaixo:

Nombre de usuario	Email	RG	CPF	Teléfono Celular	Matrícula	Estado	Fecha de Validez Inicial	Fecha de Validez Final	Nota	Tipo de usuario	Grupo de Acceso	Departamento
Scarlet						Activo	16-07-2019	16-07-2099		Normal	Total	Colaboradores
Rafael						Activo	16-07-2019	16-07-2099		Normal	Total	Colaboradores

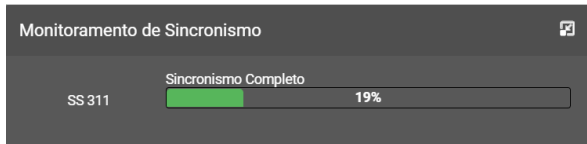
Importante: quando selecionado a opção de linguagem espanhol, o arquivo do manual que estará disponível na função *Ayuda* também será a versão traduzida para o espanhol.

2.8. Monitoramento de sincronismo

A área de monitoramento de sincronismo é responsável por sempre informar quando um processo de comunicação com o dispositivos estiverem sendo executados.



Para expandir e ter acesso ao monitoramento clique no ícone ao lado de Monitoramento de Sincronismo.



3. Usuários

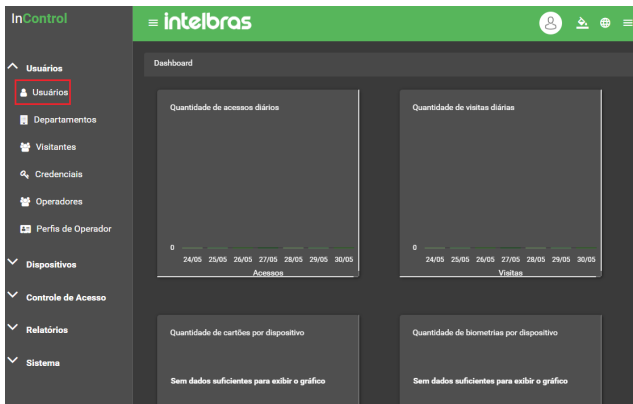
A seção *Usuários* oferece ao operador todas as subseções que estão conectadas ao perfil do usuário do sistema de controle de acesso. As opções cadastradas nestas seções serão enviadas diretamente aos dispositivos controladores de acesso que fizerem parte do sistema.

Abaixo, estão detalhadas cada subseção da seção Usuários, contudo, o cadastro de um ou mais perfis pode variar de acordo com a preferência do operador do sistema. Ou seja, há subseções que o software já traz opções padrão de fábrica para que sejam vinculadas ao cadastro do usuário posteriormente. A edição das funções padrão do software ou o cadastro de novos sub perfis está a cargo do operador do sistema de controle de acesso.

Também há nesta seção, uma subseção que possibilita ao operador admin do sistema criar novos perfis de operadores do sistema com permissões diferentes voltadas para necessidades específicas do software durante a operação.

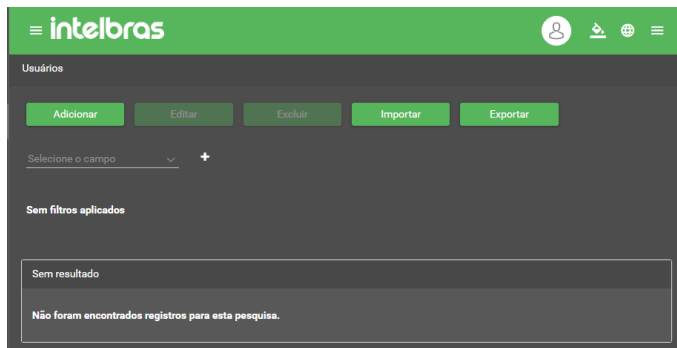
3.1. Cadastro de usuários

A subseção Usuários, pode ser encontrada na barra de funções do software, localizada na barra lateral esquerda do software e possibilita o cadastro de novos usuários. Veja a representação de sua localização na figura abaixo:

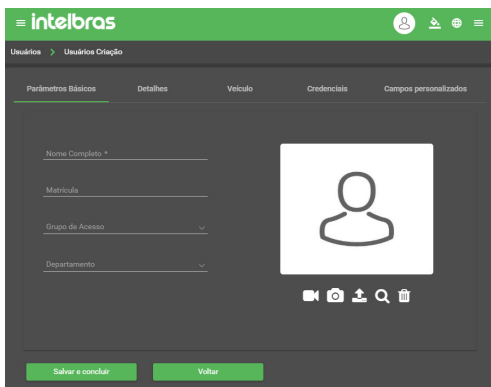


Ao selecionar a subseção *Usuários*, uma nova janela se abrirá, possibilitando ao operador, navegar pelas “abas” do cadastro de usuário inserindo as informações que irão compor o cadastro do usuário..

Na nova tela de cadastro de usuários, esta exibida a lista de todos os usuários presentes no sistema. Nesta tela, o operador poderá Adicionar, Editar, Excluir, Importar ou Exportar a lista de usuários do sistema.



Ao clicar em *Adicionar*, uma nova janela se abrirá contendo todas as abas necessárias para o cadastro do usuário.



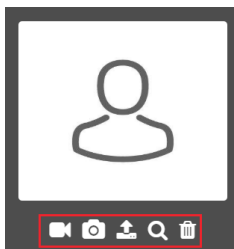
Na aba *Parâmetros Básicos* insira os dados:

- » Nome completo;
- » Matrícula;
- » Grupo de acesso em que o usuário participará;
- » O departamento na qual o usuário pertence;
- » Foto do perfil do usuário;

É possível cadastrar a foto do usuário de algumas formas diferentes. São elas:

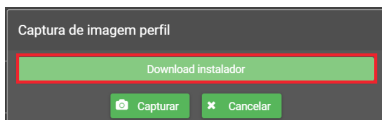
- » Captura da imagem utilizando uma câmera de segurança IP Intelbras do sistema de CFTV local;
- » Captura de imagem utilizando um webcam;
- » Upload de arquivo de imagem diretamente do computador.

É possível também excluir uma imagem prévia que por ventura já esteja vinculada.

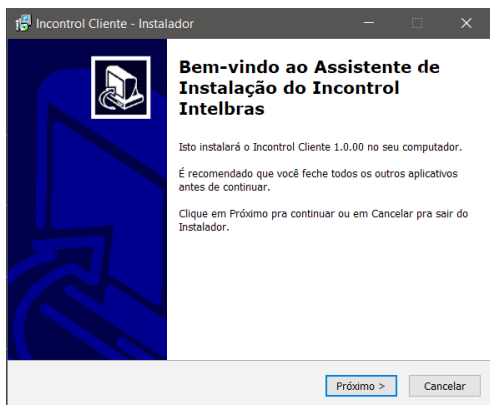


Importante: é possível ampliar a imagem capturada clicando sobre a mesma na aba de *Parâmetros Básicos*.

Ao clicar em captura de imagem utilizando webcam será necessário realizar a instalação do serviço do incontrol responsável por esta aplicação, para isso clique no ícone de cadastro via webcam e após clique na opção Download do Instalador e aguarde o download.



Após o download do arquivo de instalação, de um duplo clique no arquivo compactado e na nova pasta, clique por duas vezes sobre o arquivo de instalação, execute a instalação conforme orientado no instalador.



Após finalizar a instalação atualize a tela do seu navegador, acesse novamente a página de cadastro de usuário e clique no botão de cadastro via webcam para ter acesso a captura.

Na aba *Detalhes* é possível definir as seguintes características ao cadastro de usuários:

- » Tipo do usuário: normal ou terceirizado;
- » Data de validade: data inicial e data final;
- » CPF: apenas números;
- » RG: números e letras;
- » Celular: número de telefone celular;
- » E-mail: endereço eletrônico de e-mail;
- » Observações: caracteres em geral.
- » Caixa de seleção ativa: sempre marcado por padrão, caso seja desmarcado o usuário não poderá acessar aos dispositivos do sistema de controle de acesso.

The screenshot shows the Intelbras user management interface. The top navigation bar is green with the Intelbras logo and a user profile icon. Below it, a breadcrumb trail shows 'Usuários' > 'Usuários Criação'. The main content area has a dark grey background with a light grey border. At the top of this area, there are five tabs: 'Parâmetros Básicos', 'Detalhes' (selected), 'Veículo', 'Credenciais', and 'Campos personalizados'. The 'Detalhes' tab contains the following fields:

- Tipo de usuário:** A dropdown menu with 'Normal' selected.
- Data Inicial de Validade:** A text field with '30/05/2019' entered.
- Data Final de Validade:** A text field with '30/05/2099' entered.
- CPF:** A text field.
- RG:** A text field.
- Celular:** A text field.
- E-mail:** A text field.
- Observações:** A text area.
- Ativo:** A checkbox that is checked, with the label 'Ativo' next to it.

At the bottom of the form, there are two green buttons: 'Salvar e concluir' and 'Voltar'.

A aba *Veículo* é possível cadastrar os dados do veículo do usuário caso este acesse as dependências controladas pelo sistema de controle de acesso. As informações passíveis de serem cadastradas são:

- » Letras da placa;
- » Número da placa;
- » Cor do veículo;
- » Marca;
- » Modelo do veículo;
- » Foto.

intelbras

Usuários > Usuários Criação

Parâmetros Básicos Detalhes **Veículo** Credenciais Campos personalizados

Letras da Placa

Número da Placa

Cor

Marca

Modelo

Salvar e concluir Voltar

Importante:

- » Os métodos de captura de imagem para o veículo são exatamente os mesmos que os métodos para captura de imagem do usuário.
- » É possível ampliar a imagem capturada clicando sobre a mesma na aba de *Veículo*.

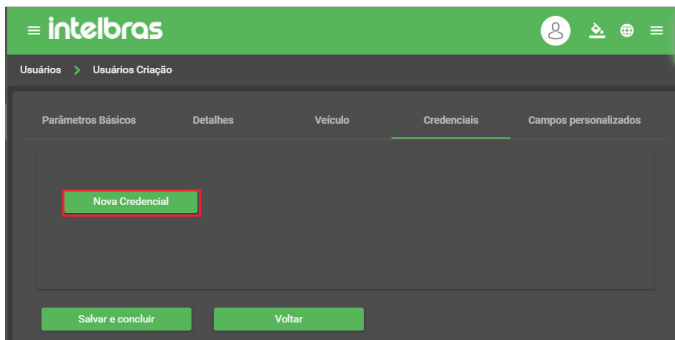
Ao clicar em *Nova Credencial*, caso o operador do sistema ainda não tenha salvo o cadastro do usuário, será exibido uma janela com a opção de salvar o cadastro efetuado até então para o posterior vínculo das credenciais. Clique no botão *Ok* caso já tenha preenchido todas as informações anteriores.

Usuário não salvo

O usuário ainda não foi salvo, para criar vincular credenciais é necessário ter o usuário salvo. Deseja salvar?

Ok Cancelar

Na aba *Credenciais*, clique no botão *Nova Credencial* para abrir o cadastro de credenciais.



Na nova janela, é possível cadastrar alguns tipos de credenciais para o usuário. São elas:

- » Nível da credencial: credencial de usuário normal ou de terceiros;
- » Tipo da credencial:
 - » Cartão (RFID);
 - » Digital (biometria) 10 por usuário;
 - » Senha (numérica)
 - » Tag UHF (tag veicular)

Importante: exceto a credencial do tipo Digital, o restante dos tipos de credencial de usuários (senha, cartão e tag UHF), não possuem limite de cadastro por usuário definido por software. Esta definição se limita à capacidade do dispositivo controlador de acesso que o usuário terá acesso. Por exemplo:

Um dispositivo que possua capacidade para armazenar 30.000 usuários com cartão e senha terá sua capacidade reduzida à medida que mais cartões, tags UHF ou senhas sejam cadastrados para um mesmo usuário. Então considerando um cenário em que temos um dispositivo com capacidade de 30.000 usuário com cartão e senha e apenas dois usuários cadastrados no sistema podemos cadastrar 15.000 cartões, tags UHF ou senhas para cada usuário o que totalizará a capacidade de 30.000 usuários do dispositivo.

Cada tipo de credencial escolhida, disponibiliza opções diferentes ao operador no cadastro do usuário.

- » Tipo credencial cartão: neste tipo de credencial, uma pré-visualização da credencial é exibida na tela e o operador pode cadastrar de algumas formas a chave da credencial:
 - » Manualmente: digitando o código em hexadecimal, ou decimal bem como o padrão de leitura (26 bits ou 34 bits).
 - » Via leitor RFID da porta: automaticamente aproximando o cartão RFID do leitor escravo ou dispositivo fixado na porta do ambiente.
 - » Via cadastrador de mesa: automaticamente aproximando o cartão RFID do cadastrador de mesa para o preenchimento da chave.
 - » Administrador: nesta caixa de seleção é possível determinar se a credencial cadastrada será adicionada como administrador do dispositivo.

Após o cadastro do credencial tipo cartão RFID, as informações inseridas estarão representadas na ilustração do cartão na tela.

Pré-visualização da credencial

www.intelbras.com.br

Via cadastrador Via dispositivo Cadastrar em Lote

Nível da credencial * Normal

Tipo de credencial * Cartão

☐ Administrador

Detalhes da credencial

Código Hexa Código Decimal *

Observação Tamanho * 34 bits

Salvar credencial Cancelar

Cadastro de credencial tipo *Cartão via dispositivo*

Para cadastrar uma credencial do tipo cartão via dispositivo, na tela principal do credencial cartão, clique no botão *Via dispositivo* e na nova janela, selecione um dos dispositivos disponíveis para efetuar a captura.

Após a seleção do dispositivo, aproxime o cartão do mesmo e veja a credencial ser capturada e demonstrada na tela do software.

Seleção o ponto de acesso

← Reiniciar processo

Pré-visualização da credencial

H 05F72B51 D: 3865000785
www.intelbras.com.br

Pontos de acesso

Nível da credencial *
Normal

Tipo da credencial *
Cartão

☐ Administrador

Detalhes da credencial

Código Hexa
e65f3b51

Código Decimal *
3865000785

Tamanho *
34 bits

Observação

Importante: selecione o padrão de leitura de 34 bits ou 26bits antes de efetuar a captura da credencial do tipo cartão. Consulte o manual do dispositivo e da tag utilizada. Clique em *Salvar Credencial* e veja a representação da mesma na lista de credenciais vinculadas ao usuário.

Credenciais do usuário

Tipo da credencial

Id: 1
No: 2

Id: 1
No: 1

Id: 1
7752311570

Id: 1

Nova Credencial

Salvar e concluir

Voltar

Clique no botão *Salvar e concluir* para finalizar a operação.

Cadastro de credencia de tipo Cartão via Cadastrador de mesa

Para capturar uma credencial do tipo cartão via cadastrador de mesa, selecione a opção *Via cadastrador*, na tela principal da credencial do tipo cartão.

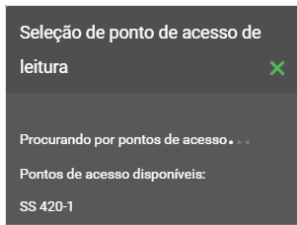
A interface de usuário para a captura de credencial do tipo cartão via cadastrador de mesa. No topo, há um título "Selecione o modo de captura" e um botão "← Reiniciar processo". Abaixo, há uma área de visualização da credencial, atualmente vazia, com o endereço "www.intelbras.com.br" no canto inferior direito. Abaixo da visualização, há dois botões: "Via cadastrador" (destacado com uma borda vermelha) e "Via dispositivo". Abaixo dos botões, há dois campos de seleção: "Nível de credencial *" com o valor "Normal" e "Tipo de credencial *" com o valor "Cartão". Abaixo desses campos, há uma caixa de seleção "Administrador" desmarcada. Na parte inferior, há uma seção "Detalhes da credencial" com campos para "Código Hexa", "Código Decimal *", "Tamanho *" (com o valor "34 bits") e "Observação".

Posicione o cursor sobre o campo *Código Decimal* e aproxime o cartão do cadastrador de mesa para que seja capturada a credencial.

Para finalizar o processo, clique em *Salvar e concluir*.

Importante: selecione o padrão de leitura de 34 bits ou 26 bits antes de efetuar a captura da credencial do tipo cartão. Consulte o manual do dispositivo e da tag utilizada.

- » **Tipo credencial digital:** neste tipo de credencial, é exibido uma representação de duas mãos do usuário para seleção do dedo que será cadastrado. O cadastro da digital poderá ser feito via cadastrador de mesa ou através do dispositivo controlador de acesso.



Importante:

- » Os dispositivos disponíveis na janela de *Seleção de ponto de acesso de leitura*, podem variar de acordo com os dispositivos adicionados no sistema.
- » Apenas dispositivos de protocolo STD SDK possuem a função de captura de biometria digital via software.

Após a seleção do dispositivo para captura, selecione o dedo que deseja cadastrar na representação gráfica do software e faça 3 leituras consecutivas no dispositivo instalado.

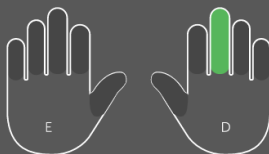


Após efetuar as 3 leituras no dispositivo, verifique se o dedo selecionado mudou a sua cor de azul para verde. Por fim clique no botão de *Salvar Credencial* para voltar a tela principal da lista de credenciais do usuário.

Cadastro de nova credencial

Digital obtida ✓

Pré visualização da credencial



Pontos de acesso

Nível da credencial *

Normal

Tipo de credencial *

Digital

Escutando o ponto de acesso

SS 420-1

Detalhes da credencial

Biometria

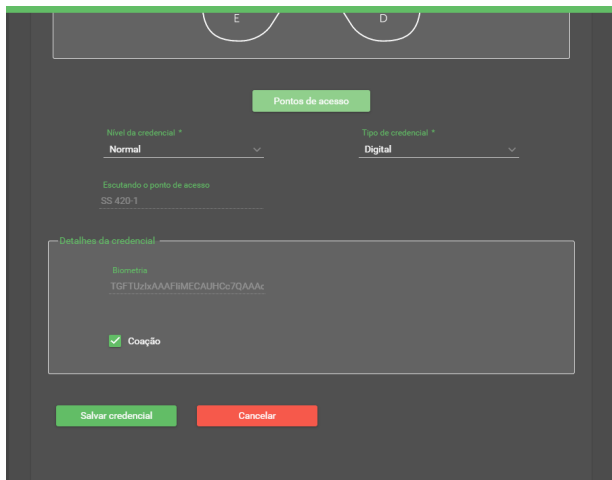
TGFTUzIxAAAFiiMECAUHC07QAAAc

☐ Coação

Salvar credencial

Cancelar

Caso deseje utilizar a digital cadastrada como uma digital de coação, marque a caixa de opção **Coação** na tela de digital antes de salvar a mesma.



Pontos de acesso

Nível da credencial *
Normal

Tipo de credencial *
Digital

Escutando o ponto de acesso
SS 420-1

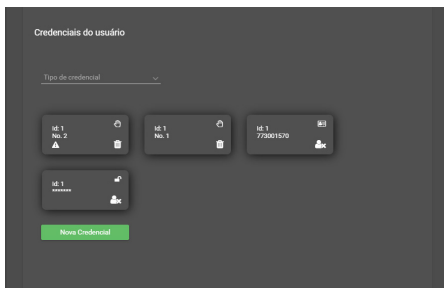
Detalhes da credencial

Biometria
TGFTUzlxAAAFliMECAUHCc7QAAAc

☒ Coação

Salvar credencial Cancelar

Por fim, veja a credencial cadastrada na lista de credenciais vinculadas ao usuário.



Credenciais do usuário

Tipo de credencial

Id: 1
No. 2

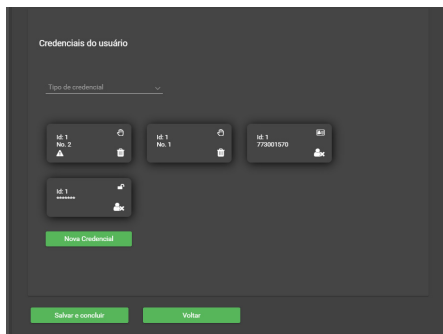
Id: 1
No. 1

Id: 1
773061570

Id: 1
773061570

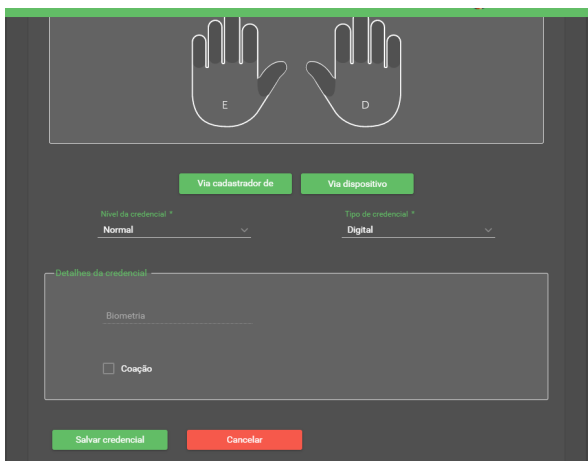
Nova Credencial

Para finalizar o processo, clique na opção *Salvar e Concluir* e volte a tela principal de usuários.

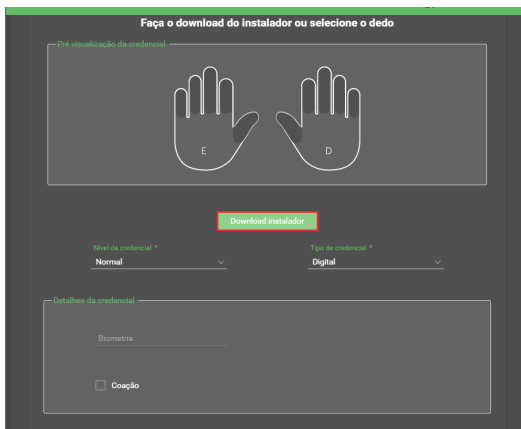


Captura via cadastrador de mesa

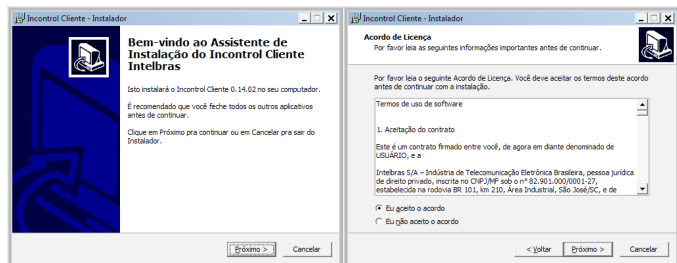
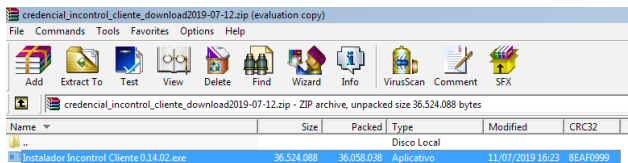
Para efetuar a captura de uma digital via cadastrador de mesa, na tela principal de credencial de tipo digital, selecione a opção *Via Cadastrador de Mesa*.

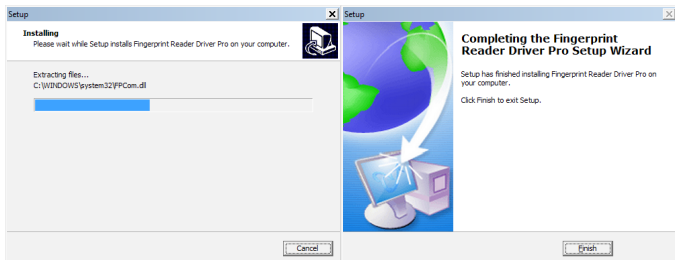
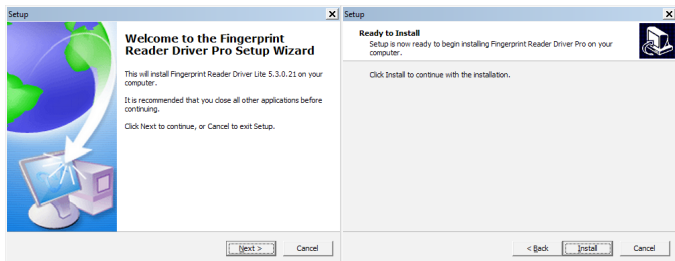
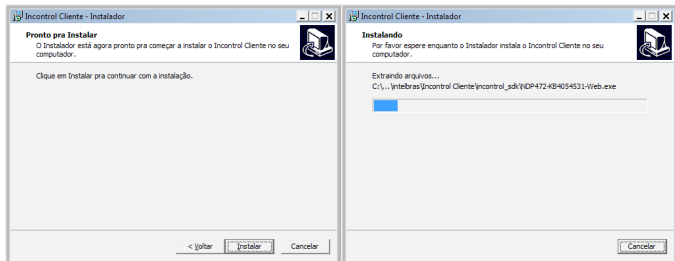


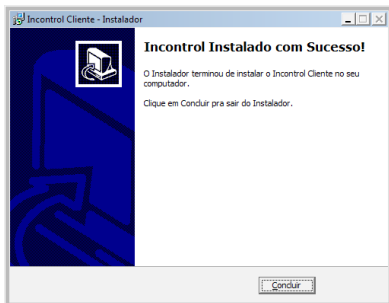
Caso esteja utilizando o cadastrador de mesa pela primeira vez, é necessário instalar o software de comunicação com o cadastrador de mesa. Clique no botão *Download instalador* e acompanhe o processo na janela do navegador da web.



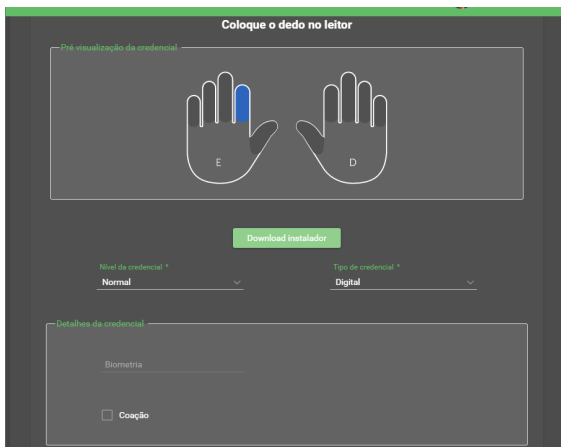
Após o download do arquivo de instalação do cadastrador de mesa, de um duplo clique no arquivo compactado e na nova pasta, clique por duas vezes sobre o arquivo de instalação.







Faça a leitura dos termos de uso do serviço e clique na caixa de seleção de aceite dos mesmos para continuar a instalação. Após clicar no botão *Concluir*, volte a tela de cadastros de digital do usuário no software InControl e selecione o dedo desejado para o cadastro na representação gráfica do software.



Efetue as 3 leituras consecutivas da digital no cadastrador de mesa e verifique se a cor do dedo selecionado, alterou de azul para verde.

Digital obtida ✓

Pré-visualização da credencial

Download instalador

Nível da credencial *
Normal

Tipo de credencial *
Digital

Detalhes da credencial

Biometria
TFNTUjlyAAAFEBQFBQUHCc7QAAA/

☐ Coação

Caso deseje utilizar a digital cadastrada como uma credencial de coação, marque a caixa de opção *Coação* na tela de digital antes de salvar a mesma.

Importante: apenas credenciais do tipo digital podem ser caracterizadas como *Coação*.

Pontos de acesso

Nível da credencial *
Normal

Tipo de credencial *
Digital

Escutando o ponto de acesso
SS 420-1

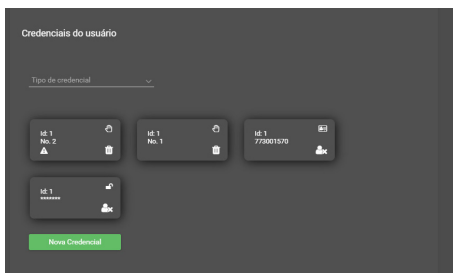
Detalhes da credencial

Biometria
TGFTUzbxAAAFiIMECAUHCc7QAAA/

☒ Coação

Salvar credencial Cancelar

Por fim, veja a credencial cadastrada na lista de credenciais vinculadas ao usuário.



Para finalizar o processo, clique na opção *Salvar e Concluir* e volte a tela principal de usuários.

- » **Tipo de credencial senha:** neste tipo de credencial é necessário atribuir uma senha numérica de 4 a 6 dígitos.

A interface 'Cadastro de nova credencial' do sistema intelbras possui um cabeçalho verde com o logo 'intelbras' e ícones de perfil, upload, idioma e menu. O formulário contém: um campo 'Pré visualização da credencial' com um ícone de cadeado e a senha '*****'; dois campos de seleção 'Nível da credencial' (Normal) e 'Tipo de credencial' (Senha); um campo 'Detalhes da credencial' com o rótulo 'Senha'; e dois botões de ação: 'Salvar credencial' (verde) e 'Cancelar' (vermelho).

- » **Tipo de credencial tag UHF:** neste modelo de credencial o operador poderá digitar a chave da tag veicular UHF em Hexadecimal ou em decimal, também deverá selecionar o padrão de leitura das tags em 26 bits ou 34 bits.

Selezione o modo de captura

Pré visualização da credencial

Nível da credencial *
Normal

Tipo de credencial *
Tag UHF

Detalhes da credencial

Código Hexa

Código Decimal

Observação

Tamanho *
26 bits

Salvar credencial Cancelar

Importante: a leitura das tags veiculares UHF são feitas através de leitores veiculares UHF.

Na aba *Campos personalizados*, o operador do sistema pode inserir dados extras que julgar relevantes no cadastro do usuário. Estas informações estarão atreladas ao cadastro assim que o botão *Salvar e concluir* for pressionado. Para isso, o operador do sistema conta com 5 campos de texto e números para o preenchimento de informações.

Campos personalizados

Apartamento

Bloco

Características

Tipo de autenticação

Observações

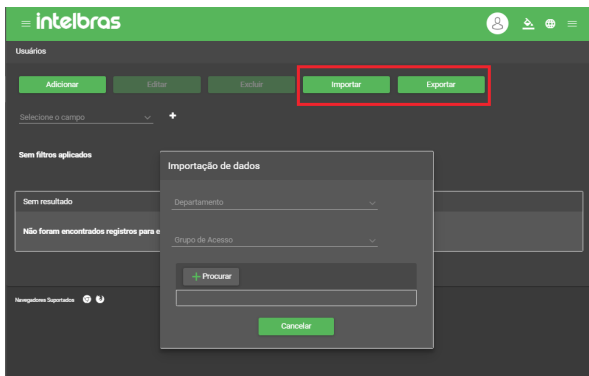
Salvar e concluir Voltar

Importante: as credenciais cadastradas dentro da subseção usuários, serão automaticamente atreladas ao cadastro do usuário em questão. Eventualmente caso seja necessário, essas credenciais podem ser desvinculadas do cadastro para serem atreladas a outros usuários do sistema.

- » **Importar e exportar:** estas funções possibilitam ao operador que exporte um arquivo contendo as informações de usuário em um arquivo com o padrão de informações do software InControl. Isto possibilita o arquivamento dessas informações em arquivos compatíveis com Excel.

É possível importar as informações de usuários do software SoapAdmin3.5, para isso, é necessário selecionar a função *Exportação Avançada* do software SoapAdmin 3.5, que garantirá que as informações sejam enviadas de modo compatível com o software InControl.

Após gerar o arquivo advindo do software SoapAdmin 3.5, clique na opção importar e selecione o departamento em que os usuários que serão importados pertencerão bem como o Grupo de pontos de acesso na qual eles poderão acessar.



Importante:

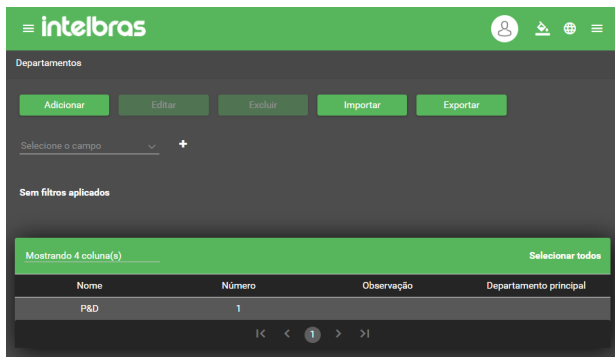
- » A função *Exportação Avançada* do software SoapAdmin é uma função exclusiva para exportar as informações de usuários em formato compatível com software InControl. Maiores informações consulte o manual do software SoapAdmin3.5.
- » Caso o operador não selecione o departamento ou grupos de pontos de acessos no software InControl, os usuários importados precisarão ter essas informações ajustadas posteriormente de maneira individual para que possam acessar aos dispositivos do sistema.

- » O Processo de Importação/Exportação de Usuários descrito acima é exclusivo para a sessão de *Cadastros de Usuários* do sistema InControl.

3.2. Cadastro de departamentos

Departamentos são necessários para a organização geral do sistema de controle de acesso, nesta seção, o operador do sistema pode criar quantos departamentos forem necessários para que posteriormente sejam vinculados ao cadastro dos usuários.

Para incluir um novo departamento, clique no botão *Adicionar*.



Na nova janela, selecione as informações e ao final clique em *Salvar e concluir*.

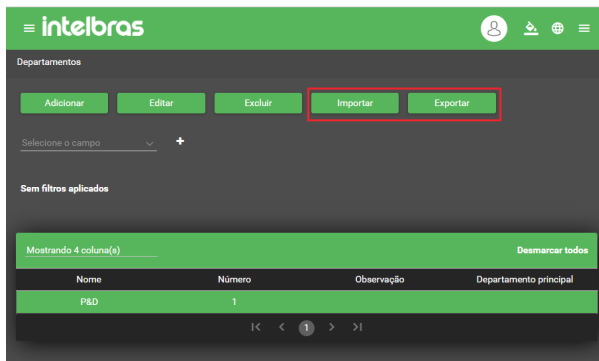
- » Departamento principal: selecione a qual departamento cadastrado anteriormente este departamento estará vinculado;
- » Nome do departamento;
- » Número do departamento (sequencial);
- » Observações.

Importante: o cadastro de ao menos um departamento é indicado para o correto vínculo dos usuários em seus respectivos departamentos no sistema InControl.

Após o cadastro da lista de departamentos, é possível editar ou excluir o departamento criado, selecionando-o na lista abaixo e clicando nos botões *Editar* ou *Excluir*.

Nome	Número	Observação	Departamento principal
P&D	1		

- » **Importar e Exportar:** é possível importar ou exportar uma lista de departamentos de um arquivo Excel ou para um arquivo de Excel. Para isso, basta clicar em um dos botões *Importar* ou *Exportar* localizados na seção *Departamentos*.



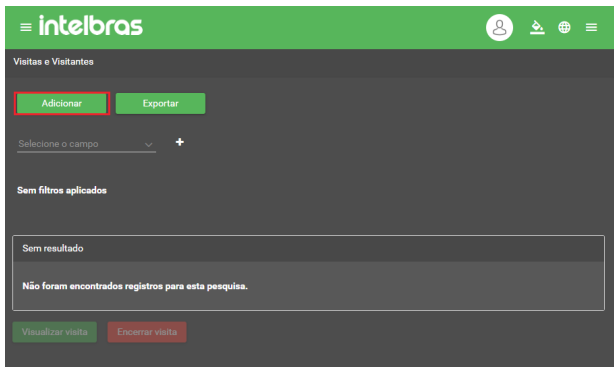
Importante: caso o operador do sistema deseje criar uma lista de departamentos em Excel e posteriormente importa-la para o sistema, recomendamos que seja cadastrado o primeiro da lista via software, exportado para o arquivo Excel, para que então ele possa inserir os demais departamentos nas colunas padrão do software.

3.3. Cadastro de visitantes

O cadastro de visitantes é semelhante ao cadastro de usuários comuns ou terceirizados do sistema, contudo, o visitante tem por definição um período pré-estipulado de validade dentro do sistema e quando findado este período o mesmo não poderá mais acessar aos ambientes controlados.

Há também a possibilidades de inserção de outras informações no cadastro de visitantes tais como visitado e período em que a visita acontece.

Para cadastrar uma nova visita, clique no botão *Adicionar* na seção *Visitantes*.



Na nova janela, a primeira aba *Dados Visitante* possibilita ao operador do sistema cadastrar as seguintes informações:

- » Caixa de seleção para marcação se o visitante já fora cadastrado anteriormente;
- » Nome completo;
- » Documento de RG;
- » Documento de CPF;
- » Endereço eletrônico E-mail;
- » Seleção dos Grupos de acesso;
- » Foto.

intelbras



Visitas e Visitantes > Visitas e Visitantes Criação

Dados Visitante

Dados Visita

Veículo

Credenciais

☐ Visitante já cadastrado?

Nome Completo

RG

CPF

E-mail

Grupo de Acesso

Copiar última visita





Para a captura da foto, são válidos os mesmos métodos disponíveis na seção de cadastro de usuários.



Importante: caso seja selecionado a caixa de seleção *Visitante já cadastrado?*, será aberta uma janela de busca no campo *Nome* para selecionar um dos cadastros da lista de *Visitantes*.

Na aba *Dados Visita*, estão disponíveis para inclusão os dados referentes ao visitado. Os dados são:

- » Visitado;
- » Tipo de usuário;
- » Início e fim da validade da visita;
- » Data da última visita e último visitado;
- » Observações.

Dados Visitante **Dados Visita** Veículo Credenciais

E-mail _____

Tipo de usuário
Visitante _____

Início validade
09/03/2020 00:00 _____

Fim validade
09/03/2020 23:59 _____

As funcionalidades de validade da visita só funcionam corretamente com o dispositivo conectado.

Data última visita _____

Último visitado _____

Observações _____

Salvar e concluir Voltar

Importante: os campos *Data última visita* e *Último visitado* só estarão disponíveis caso o cadastro do visitante já tenha sido feito anteriormente.

A aba veículo, possibilita o registro do veículo do visitante caso seja necessário. As informações disponíveis para registro são:

- » Letras da placa;
- » Número da placa;
- » Cor;
- » Marca;
- » Modelo;
- » Foto.

intelbras



Usuários > Usuários Criação

Parâmetros Básicos

Detalhes

Veículo

Credenciais

Campos personalizados

Letras da Placa

Número da Placa

Cor

Marca

Modelo



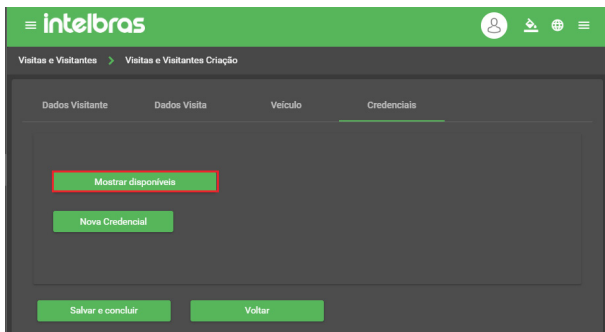


Salvar e concluir

Voltar

Importante: para a captura da foto do veículo estão disponíveis os mesmos recursos da captura da foto do cadastro de usuários.

A aba *Credenciais*, possibilita que sejam atribuídas novas credenciais ao cadastro do visitante e também possibilita a utilização de eventuais credencias cadastradas previamente para o cadastro do visitante em questão. Para consultar a existência de credencias disponíveis no sistema, clique no botão *Mostrar disponíveis*.



Caso precise cadastrar uma nova credencial, basta clicar sobre o botão *Nova credencial* e inserir os dados e posteriormente clicar no botão *Salvar credencial* para concluir o processo:

- » Nível de Credencial;
- » Tipo de Credencial:
 - » Cartão;
 - » Digital;
 - » Senha;
 - » Tag UHF.

The screenshot shows the 'Visitas e Visitantes' (Visits and Visitors) section of the Intelbras system. The breadcrumb trail is 'Visitas e Visitantes > Visitas e Visitantes Criação'. The 'Credenciais' (Credentials) tab is selected. A green button labeled 'Mostrar disponíveis' (Show available) is at the top. Below it, the heading 'Cadastro de nova credencial' (New credential registration) is displayed. Two dropdown menus are shown: 'Nível da credencial' (Credential level) with 'Visitante' (Visitor) selected, and 'Tipo de credencial' (Credential type). At the bottom, there are two buttons: 'Salvar credencial' (Save credential) in green and 'Cancelar' (Cancel) in red.

Importante:

- » O processo de cadastro de credenciais para os visitantes, segue o mesmo fluxo do processo de cadastro de credencias do cadastro de usuários.
- » As credenciais cadastradas nesta seção são automaticamente atreladas ao cadastro do visitante em questão.

Não é possível excluir um cadastro de visitante. Somente encerrar a visita. Isso pode ser feito de forma manual ou por data. Para encerrar uma visita manualmente, selecione o cadastro na tela principal de visitantes e clique no botão *Encerrar Visita*.

Visitas e Visitantes

Adicionar

Exportar

Selecione o campo

+

Sem filtros aplicados

Mostrando 10 coluna(s)

Nome do Visitante	Data última visita	Nome do Visitado	CPF do Visitado	CPF do visitante	RG	Ativa	Início validade	Fim validade	Observações
Scarlet	12-07-2019	Rafael		000.000.000-00		Sim	12-07-2019	12-07-2019	

<

<

1

>

>

Visualizar visita

Encerrar visita

Para visualizar visitas encerradas é necessário aplicar o filtro de visitas ativas na tela inicial de visitantes.

Visitas e Visitantes

Adicionar

Exportar

Selecione o campo

+

Ativa: Não

Mostrando 10 coluna(s)

Nome do Visitante	Data última visita	Nome do Visitado	CPF do Visitado	CPF do visitante	RG	Ativa	Início validade	Fim validade	Observações
Zé das couves		Scarlet		000.000.000-00		Não	26-07-2019	26-07-2019	

Visualizar visita

Encerrar visita

Navegadores Suportados:

InControl - Intelbras S/A todos os direitos reservados.

Importante:

- » Os campos de filtro possuem várias opções que podem ser aplicadas para visualizar apenas o que se deseja.
- » Após cadastrar um visitante, não é possível editar esse cadastro, apenas visualizá-lo posteriormente.
- » As visitas são encerradas automaticamente pelo software assim que o seu período de validade expira. Para garantir que estas informações sejam corretamente atualizadas nos dispositivos de controle de acesso do sistema, é necessário que os mesmos estejam conectados à rede local e devidamente online.

3.4. Cadastro de credenciais

Nesta seção, são cadastradas as credenciais independente de cadastros de usuários ou visitantes. As credenciais cadastradas nesta seção, ficam disponíveis para a associação com outros usuários ou visitantes posteriormente. Para cadastrar uma nova credencial, clique no botão *Adicionar*.

Credenciais

Adicionar

Editar

Excluir

Selecione o campo

+

Sem filtros aplicados

Mostrando 6 coluna(s)

Nível	Tipo	Código Decimal	Nome Completo	Observação	Coação
Normal	Tag UHF		Gerente		Não
Normal	Cartão		Gerente		Não
Normal	Cartão	866624342			Não
Normal	Cartão	859099650			Não
Normal	Cartão	3668452458			Não
Normal	Cartão	2166803615			Não

Na nova janela, selecione o nível da credencial e o seu tipo, consequentemente preencha os campos referente ao tipo da credencial escolhida. Por fim, clique em *Salvar credencial* para concluir o processo de cadastro.

← Reiniciar processo

Pré visualização da credencial



www.intelbras.com.br

Via cadastrador
Via dispositivo
☐ Cadastrar em Lote

Nível da credencial *

Normal

Tipo de credencial *

Cartão

Nome do usuário

☐ Administrador

Detalhes da credencial

Código Hexa

Código Decimal *

Observação

Tamanho *

26 bits

Salvar credencial

Na janela inicial das seções de *Credenciais*, note que a mesma aparece listada na tabela de credenciais disponíveis abaixo:

← Reiniciar processo

Pré visualização da credencial



www.intelbras.com.br

Via cadastrador
Via dispositivo
☐ Cadastrar em Lote

Nível da credencial *

Normal

Tipo de credencial *

Cartão

Nome do usuário

☐ Administrador

Detalhes da credencial

Código Hexa

Código Decimal *

Observação

Tamanho *

26 bits

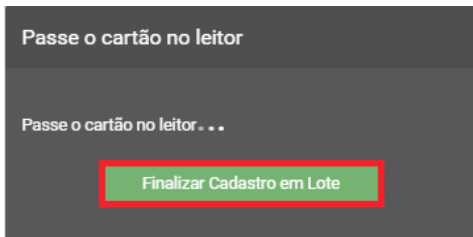
Salvar credencial

Importante: o processo de cadastro de credenciais, segue o mesmo fluxo do processo de cadastro de credencias do cadastro de usuários.

Também é possível realizar o cadastro em lote de credenciais do tipo cartão e tag, para isso marque a opção cadastro em lote e selecione o cadastro via dispositivo ou cadastrador de mesa

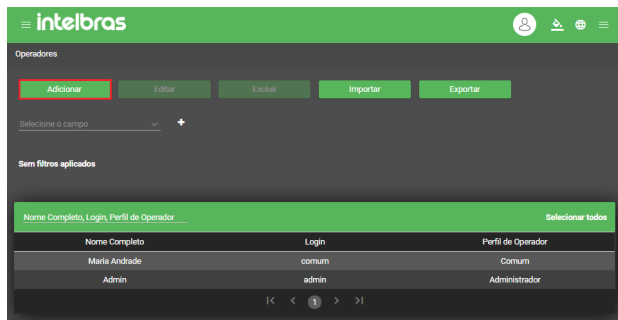


Após passe os cartões que deseje cadastrar o sistema irá informar a mensagem de Solicitação realizada quando o cadastro ocorrer corretamente, após finalizar o cadastro das credenciais selecione a opção Finalizar Cadastro em Lote para encerrar o processo e salvar as credenciais.



3.5. Cadastro de Operadores do sistema

Nesta seção, estão listados os operadores do sistema que já foram cadastrados, inclusive o operador admin que é o operador padrão do sistema. Para efetuar um cadastro de operador novo, clique no botão *Adicionar*.



Na nova janela, insira os parâmetros e clique no botão *Salvar e concluir*.

- » Nome do Perfil;
- » Login;
- » Senha;
- » Confirmação de Senha;
- » E-mail;
- » Perfil de Operador;
 - » Recepção;
 - » Portaria;
 - » Administrador.

Importante: novos perfis de operadores poderão ser incluídos conforme a necessidade. Os perfis acima estão pré cadastrados e podem ser alterados.

- » Foto.

≡ intelbras



Operadores > Operadores Criação

Parâmetros Básicos

Nome *

Login *

Senha *

Confirmação de senha

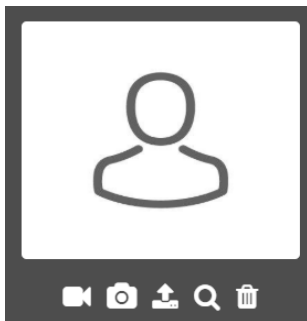
E-mail

Perfil



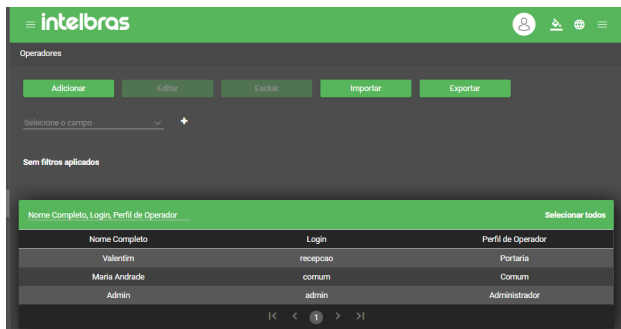


Status:
☒ Ativo



Importante: para a captura da foto do operador estão disponíveis os mesmos recursos da captura da foto do cadastro de usuários.

Confira o cadastro efetuado na lista de operadores do sistema da seção *Operadores*.



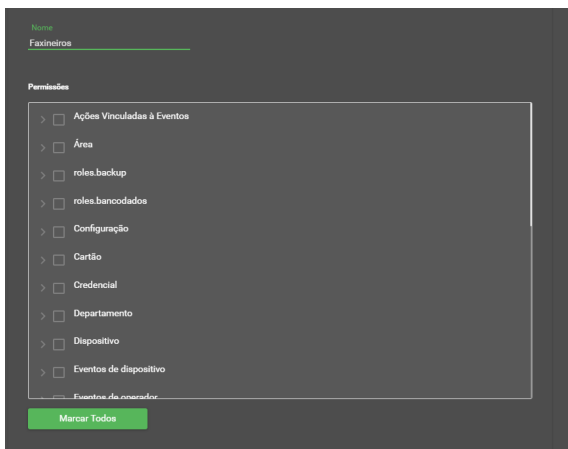
3.6. Cadastro de Perfis para operadores do sistema

Nesta seção o sistema possibilita ao operador, criar Perfis de acesso onde os cadastros de operadores do sistema serão vinculados durante o registro. Esses perfis basicamente limitam o acesso dos operadores a uma ou mais seções do sistema de controle de acesso e servem também para garantir a segurança do sistema de modo que os operadores acessem as seções que tenham familiaridade com as rotinas do seu dia a dia.

O sistema traz como padrão de fábrica, quatro perfis de operadores previamente cadastrados. São eles:

- » Recepção;
- » Portaria;
- » Administrador.

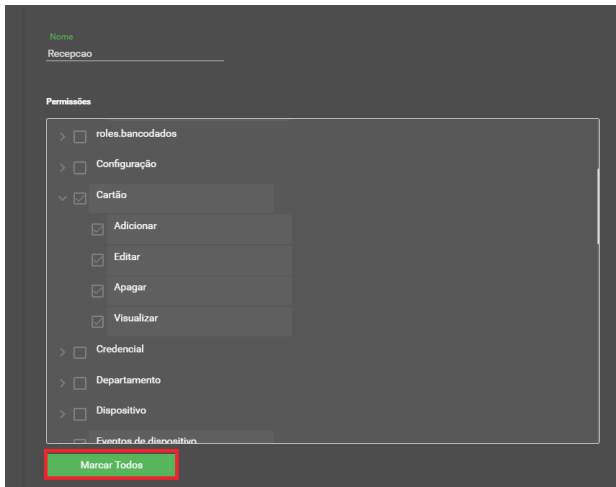
Cada um desses perfis listados acima, possuem permissões de acesso diferentes. Confira o exemplo do perfil *Recepção* nas imagens abaixo:



The image shows a dark-themed user interface for configuring a user profile. At the top, the profile name 'Faxineiros' is displayed. Below it, a section titled 'Permissões' (Permissions) contains a list of system functions, each with a checkbox and a right-pointing arrow. The functions listed are: 'Ações Vinculadas à Eventos', 'Área', 'roles.backup', 'roles.bancodados', 'Configuração', 'Cartão', 'Credencial', 'Departamento', 'Dispositivo', and 'Eventos de dispositivo'. A partially visible item 'Eventos de operador' is at the bottom of the list. A green button labeled 'Marcar Todos' (Mark All) is located at the bottom of the permissions list.

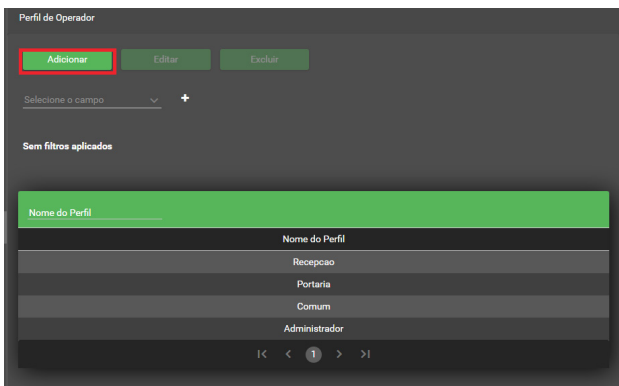
As funções disponíveis do sistema, estão representadas por uma caixa de seleção que uma vez marcada, o perfil passará a ter acesso a estas áreas. O contrário também é verdade, ou seja, uma vez desmarcados, o operador atrelado a este perfil não terá mais acesso a seção referente.

Existe a possibilidade de marcar todas as caixas de seleção, clicando no botão *Marcar Todos* no final da janela. Após as devidas marcações, é necessário clicar no botão *Salvar* e concluir para finalizar o processo.



Para adicionar um novo perfil de sua preferência, clique no botão *Adicionar* e preencha os campos indicados na tela de perfil tais como:

- » Nome do Perfil;
- » Permissões desejadas.



Nome
Faxineiros

Permissões

- > ☐ Ações Vinculadas à Eventos
- > ☐ Área
- > ☐ roles.backup
- > ☐ roles.bancodados
- > ☐ Configuração
- > ☐ Cartão
- > ☐ Credencial
- > ☐ Departamento
- > ☐ Dispositivo
- > ☐ Eventos de dispositivo
- > ☐ Eventos de operador

Marcar Todos

Os três perfis padrão do sistema podem ser editados. Para isso, basta selecionar um deles na lista de perfis disponíveis e clicar no botão *Editar*.

intelbros

Perfil de Operador

Adicionar Editar Excluir

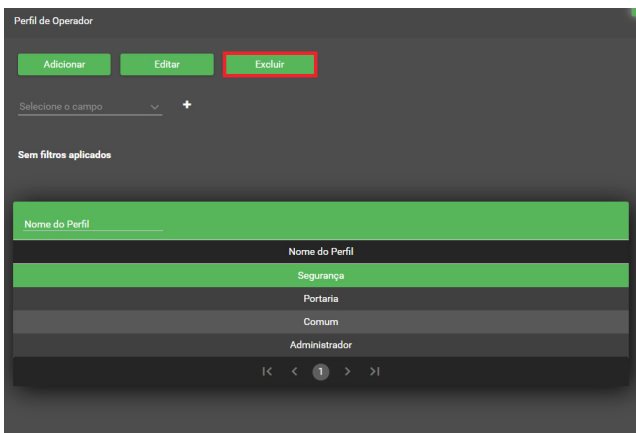
Selecione o campo

Sem filtros aplicados

fields.name	Selecionar todos
fields.name	
Recepcao	
Portaria	
Comum	
Administrador	

1

Caso deseje excluir um dos perfis criados, selecione-o na lista e clique no botão *Excluir*.



Importante: os três perfis padrão do software podem ser editados mas não podem ser excluídos.

3.7. Cadastro de sites

Nesta seção o sistema possibilita a adição de um outro servidor remoto InControl permitindo a importação de todos usuários e suas credenciais de acesso. Para adicionar um novo servidor clique em *Adicionar* e após preencha os seguintes campos:

A interface 'Cadastro de sites' mostra a seção 'Parâmetros Básicos' com campos para 'Nome *', 'Ip *', 'Porta *', 'Login *', 'Senha *' e 'Horário Sinc.'. Um botão 'Testar conexão' está abaixo dos campos de login e senha. No rodapé, há dois botões: 'Salvar e concluir' e 'Voltar'.

» Nome;

- » IP do Servidor;
- » Porta: Padrão 4441;
- » Login;
- » Senha;
- » Horário de sincronismo.

Para determinar se há conexão com o servidor clique em *Testar Conexão*, caso haja conexão com o servidor clique em *Salvar e Concluir*.

Parâmetros Básicos

Nome *	IP *	Porta *
InControl Servidor - Filial Empresa	10.1.54.144	4441
Login *	Senha *	Horário Sinc.
admin	admin	10:06

Testar conexão

Salvar e concluir Voltar

Após o sincronismo todos os usuários importados irão aparecer na área de Usuários e as credenciais na área Credenciais sendo identificados como importados pelo símbolo »» caso o mapeamento do servidor seja excluído, todos os usuários e credenciais que foram importados serão excluídos da instância local.

Mostrando 5 coluna(s)					
☐	Nome do usuário	Estado	Tipo de usuário	Grupo de Acesso	Departamento
☐	»» Pedro Alves	Ativo	Normal		
☐	»» Andreza Duarte	Ativo	Normal		

< < 1 > >

Total: 2

Para permitir o acesso dos usuários importados aos dispositivos locais, selecione o usuário e clique em Editar após selecione o Grupo de Acesso ao qual este usuário fará parte.

4. Dispositivos

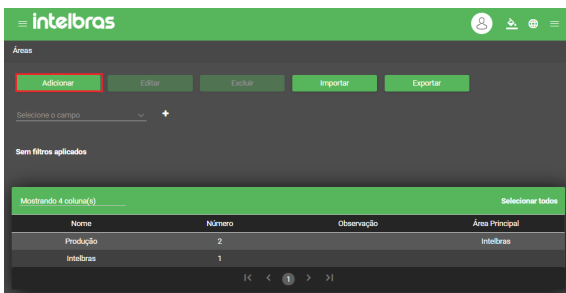
Dispositivos são equipamentos que controlam as portas das áreas do sistema de controle de acesso. Esses dispositivos são adicionados ao sistema InControl atrelados as áreas controladas. Para validar os acessos dos usuários, os dispositivos possuem métodos de autenticação diferentes que no sistema de controle de acesso são caracterizadas como *Credenciais* que podem ser (Biometrias digitais, Biometrias Faciais, Cartão RFID, Senha numérica, Tag UHF).

A capacidade de usuários e credenciais, variam de acordo com os dispositivos, assim como o número de portas controladas que variam de uma porta a quatro portas de forma autônoma dependendo do modelo do dispositivo.

Importante: o cadastro de biometrias faciais necessita ser feito diretamente no dispositivo físico e não poderá ser feito via software.

4.1. Cadastro de Áreas

Áreas são os locais em que os dispositivos estão instalados. É necessário cadastrar uma área antes de adicionar um dispositivo, porque será necessário atrelar a área no cadastro de dispositivos. Para adicionar uma nova área dentro da seção *Áreas*, clique no botão *Adicionar*.



Na nova tela, selecione as informações necessárias para o cadastro da área e ao final clique quem *Salvar* e *concluir* para finalizar o processo.

- » Selecione a área principal: caso essa área pertença a outra de maior relevância;
- » Nome;
- » Número: Identificador da área sempre numérico e sequencial;
- » Observação.

Parâmetros Básicos Monitoramento de área

Área Principal

Nome *

Número

Observação

Salvar e concluir Voltar

- » **Importar e Exportar:** é possível importar ou exportar uma lista de áreas do sistema de um arquivo Excel ou para um arquivo de Excel. Para isso, basta clicar em um dos botões *Importar* ou *Exportar* localizados na seção *Áreas*.

intelbras

Áreas

Adicionar Editar Excluir **Importar** **Exportar**

Selecione o campo +

Sem filtros aplicados

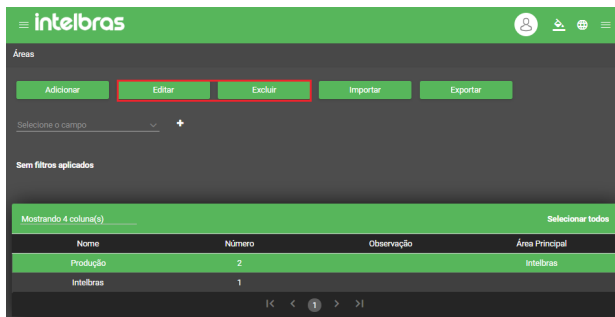
Mostrando 4 coluna(s) Selecionar todos

Nome	Número	Observação	Área Principal
Produção	2		Intelbras
Intelbras	1		

< < 1 > >>

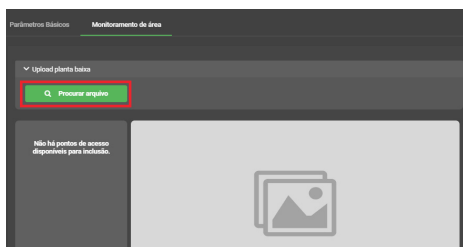
Importante: caso o operador do sistema deseje criar uma lista de áreas em Excel e posteriormente importa-la para o sistema, recomendamos que seja cadastrado a primeira da lista via software, exportado para o arquivo Excel, para que então ele possa inserir as demais áreas nas colunas padrão do software.

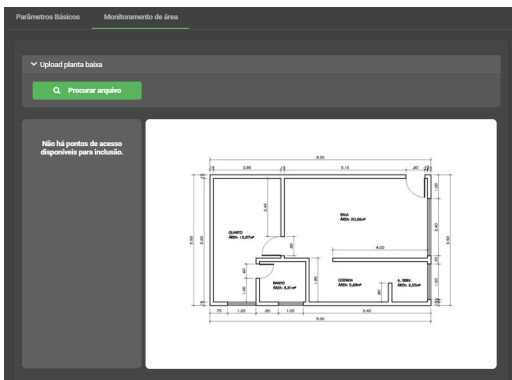
Na tela inicial da seção de *Áreas* é possível visualizar todas as áreas já cadastradas no sistema. É possível que as áreas cadastradas sejam excluídas ou editadas. Para isso, selecione uma das áreas cadastradas na lista e clique nos botões *Editar* ou *Excluir*.



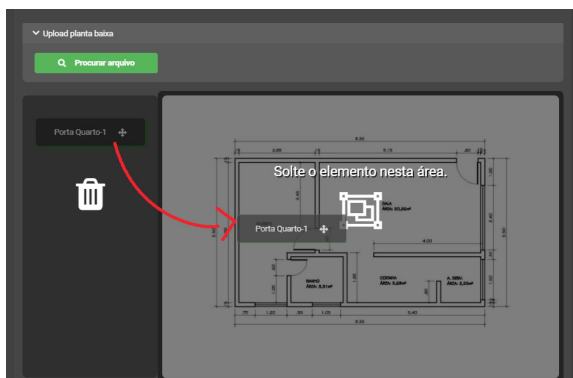
Importante: antes de excluir uma área, verifique se a mesma não está vinculada a um dispositivo e desvincule-a primeiramente. É necessário que haja pelo menos uma área cadastrada no sistema.

Na aba *Monitoramento de Área* é possível realizar o cadastro de uma planta baixa do local e adicionar os pontos de acesso para o monitoramento dos eventos desta área, para adicionar a imagem da área clique na opção *Procurar arquivo* e selecione a imagem da planta baixa do local.





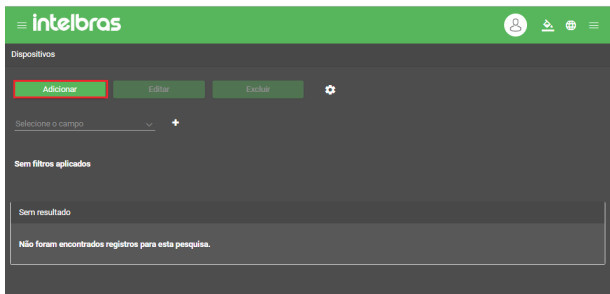
Após adicione o dispositivo a área como descrito no tópico *Cadastro de Dispositivos* deste manual, após o vínculo do dispositivo a área, será possível arrastar e soltar o ponto de acesso ao respectivo local indicado na imagem abaixo:



O monitoramento dos eventos deve ser realizado no menu *Monitoramento de Áreas*.

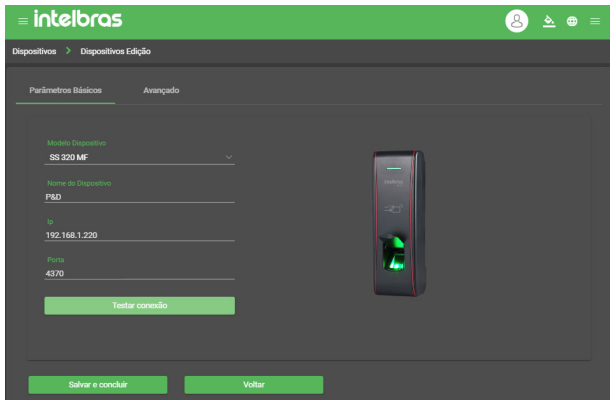
4.2. Cadastro de Dispositivos

Nesta seção é possível cadastrar os dispositivos que farão parte do sistema de controle de acesso. Para iniciar o cadastro, clique no botão *Adicionar*.



Na nova janela, na aba *Parâmetros básicos* insira as informações descritas abaixo. Para testar a comunicação do dispositivo com o software, após preencher as informações, clique no botão *Testar conexão*.

- » Selecione o modelo do dispositivo;
- » Nome do dispositivo;
- » Endereço IP;
- » Porta de comunicação.



Importante:

- » Confira se a imagem referente ao modelo do dispositivo é igual ao dispositivo físico instalado.
- » Os dispositivos suportados pelo software InControl são os disponíveis na opção *Modelo do dispositivo* na aba *Parâmetros básicos*.

Na aba *Avançado* é possível inserir as informações complementares tais como: senha de comunicação e a área que o dispositivo pertencerá. Também é possível marcar o checkbox *Excluir dados ao salvar?*, que zera todas as informações cadastradas no dispositivo antes de inseri-lo no banco de dados do sistema.

A captura de tela mostra a interface de configuração do sistema InControl, especificamente a aba "Avançado". No topo, há duas abas: "Parâmetros Básicos" e "Avançado", com "Avançado" selecionado. O formulário contém os seguintes elementos:

- Um campo de texto rotulado "Senha de Comunicação" com caracteres ocultos por pontos.
- Um menu suspenso rotulado "Produção" com uma seta para baixo.
- Um checkbox rotulado "Excluir dados ao salvar?" que está marcado com um ícone de check verde.
- Um campo rotulado "Tipo de Controle" com o valor "Pull" exibido.

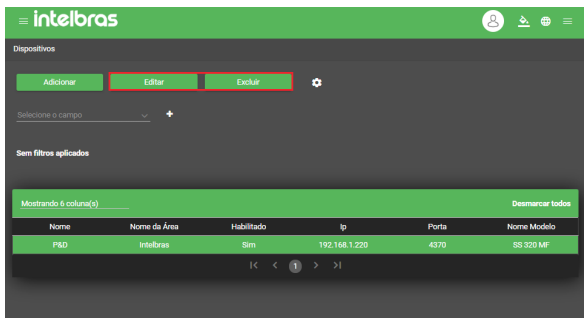
Na base do formulário, há dois botões verdes: "Salvar e concluir" e "Voltar".

Nesta aba também é exibido o tipo de controle existente no dispositivo, esta informação é automaticamente carregada conforme o modelo selecionado. Para finalizar o cadastro clique no botão *Salvar e concluir*.

Esta captura de tela mostra a mesma interface da aba "Avançado" do sistema InControl. Neste momento, o checkbox "Excluir dados ao salvar?" permanece marcado. O elemento principal desta imagem é o botão "Salvar e concluir" na base do formulário, que está circulado por um retângulo vermelho para destacar a ação final de salvar o cadastro.

Confira o dispositivo cadastrado na lista de dispositivos do sistema na tela principal da seção *Dispositivos*. Caso seja necessário editar ou excluir o dispositivo cadastrado, selecione-o na lista dos dispositivos disponíveis e clique nos botões *Editar* ou *Excluir*.

Importante: é recomendado sempre marcar a opção *Excluir dados ao salvar?*, pois a lista de usuários e configurações principal será sempre a existente no software. Caso não seja marcado esta opção e haja usuários cadastrados no dispositivo, os mesmos serão sobre – escritos considerando a lista já existente de usuários no sistema.



A seção *Dispositivos* também possibilita com que o operador do sistema efetue uma série de ajustes nos dispositivos cadastrados e ou outras formas de adicionar dispositivos tal como *Procura de dispositivos na rede*. Confira a lista de funções disponíveis abaixo:

- » **Desabilitar:** remove da lista de dispositivos ativos o dispositivo selecionado. Nesta condição o dispositivo não receberá o sincronismo das atualizações feitas no sistema;
- » **Habilitar:** insere novamente o dispositivo selecionado na lista de dispositivos ativos do sistema. Nesta condição o dispositivo passa a receber as atualizações de sincronismo do sistema de controle de acesso. Assim que for habilitada as informações do dispositivo, serão apagadas e enviadas as informações do software novamente.
- » **Atualizar firmware:** possibilita que novas versões de firmware do dispositivo selecionado seja atualizado automaticamente através do software de controle de acesso. Esta função varia de acordo com o modelo do dispositivo adicionado. É necessário consultar o manual do dispositivo de hardware para garantir a existência desta funcionalidade;
- » **Alterar endereço IP:** modifica o endereço do IP físico do dispositivo selecionado para uma outra faixa específica definida pelo operador do sistema.

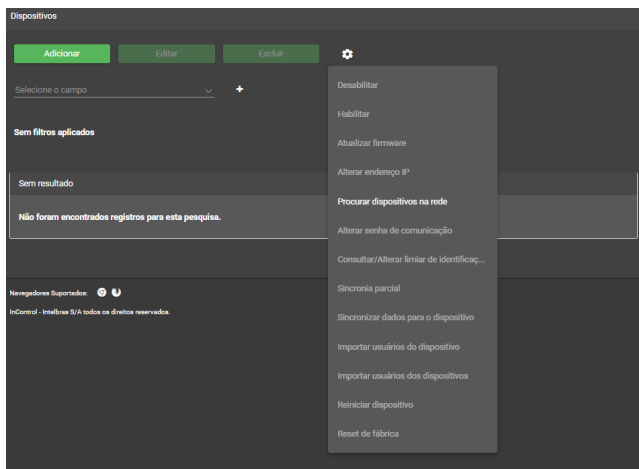
- » **Procurar dispositivos na rede:** efetua uma varredura de todos os dispositivos ativos que estejam disponíveis e conectados na rede do sistema;
- » **Alterar senha de comunicação:** esta função possibilita a modificação da senha de comunicação definida para o dispositivo selecionado no momento de seu cadastro. Esta senha caso atribuída ao dispositivo, será necessária para estabelecer a comunicação física com o dispositivo de hardware.
- » **Consultar / Alterar limiar de identificação:** esta função aumenta ou diminui a criticidade de verificação dos módulos biométricos facial e digital, ou seja, a medida que o limiar de identificação aumenta mais pontos serão verificados na leitura da credencial e à medida que este limiar de identificação diminui, menos pontos de verificação na credencial biométrica são necessários para a liberação do acesso.
- » **Sincronismos pendentes:** sincroniza para os dispositivos eventuais informações que ainda não tenham sido enviadas a partir do software para os dispositivos adicionados.
- » **Sincronizar dados para o dispositivo:** sincroniza para o dispositivo adicionalado, todas as informações atuais do software atualizando o seu banco de dados.
Importante: esta opção irá apagar todos usuários cadastrados no dispositivo e após realizar o reenvio dos usuários do software ao dispositivo selecionado, antes de realizar este procedimento certifique que não há divergências de usuários.
- » **Importar usuários do dispositivo:** importa para o sistema as informações de cadastros e configurações do dispositivo selecionado. Usuários que existem no dispositivo mas não existem no Software recebem um grupo criado automaticamente. Quando o usuário existe no Incontrol e no dispositivo, a importação mantém o usuário do Incontrol inalterado, porém não altera o usuário no dispositivo;

Importante:

- » O processo de Importação de usuários deve ser feito quando não há cadastros anteriores já feitos na base dos dados do sistema, pois o sistema sempre terá prioridade no número dos ID's dos usuários e suas credenciais. Ou seja, caso seja feita a importação de mais de um dispositivo que tenham usuários diferentes, porém com ID's iguais nas respectivas memórias dos dispositivos, será considerado como ID válido, o primeiro dispositivo que for feita a importação, os usuários de mesmo ID do segundo dispositivo serão ignorados e não serão importados pelo sistema. Reforçamos a importância de todos os cadastros serem feitos diretamente no sistema InControl.
- » Caso seja feito o processo de importação de dois dispositivos com usuários diferentes e com ID's iguais, o primeiro dispositivo será considerado e o segundo será ignorado. Contudo se no cadastro do segundo dispositivo houver uma credencial de tipo diferente do tipo de credencial presente no primeiro dispositivo importado, ela será atribuída ao usuário de mesmo ID do primeiro dispositivo, exceto configurações de rede.

- » **Reiniciar dispositivo:** reinicia o dispositivo selecionado;
- » **Reset de fábrica:** retorna ao padrão de fábrica todas as configurações do dispositivo selecionado, apagando inclusive todos os usuários e credenciais da memória do dispositivo, exceto configurações de rede.

Estas funções acima podem ser acessadas após selecionar o dispositivo em questão na lista de dispositivos disponíveis e posteriormente, clicar no botão de engrenagem na parte superior da seção *Dispositivos*.



Importante: as funções listadas acima variam de acordo com o modelo do produto.

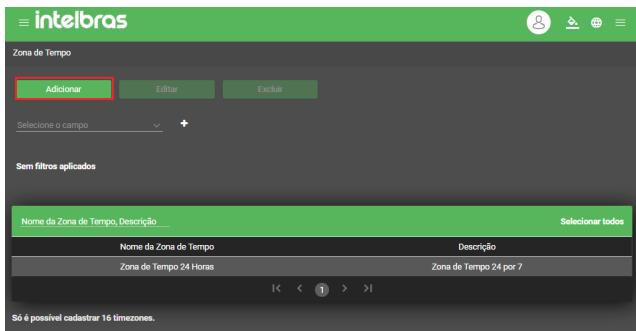
5. Controle de acesso

Esta seção do software traz ao operador do sistema uma gama de funções que visam organizar e instaurar as regras necessárias para que os usuários do sistema e os dispositivos controladores de acesso operem de forma correta possibilitando uma maior segurança de informações e do sistema de um modo geral.

5.1. Zonas de tempo

A seção zona de tempo possibilita ao operador do sistema, cadastrar faixas de horários semanais onde o sistema de controle de acesso estará ativo. Ou seja, usuários que fizerem parte desta zona de tempo, poderão acessar aos ambientes controlados e tentativas de acesso fora destes períodos serão bloqueadas.

O sistema já traz a zona de tempo 24 h cadastrada por padrão, contudo, é possível cadastrar novas zonas de tempo que atendam às necessidades desejadas. O sistema suporta até 16 zonas de tempo cadastradas no total. Para adicionar uma nova zona de tempo, na tela inicial, clique no botão *Adicionar*.



Na nova tela, defina o nome da zona de tempo e acrescente uma descrição caso necessário, selecione um dos dias da semana e defina os períodos de tempo para ele.

Importante: são permitidos no máximo 3 períodos de tempo por dia da semana.
Ao final da tela, uma representação gráfica do período selecionada é demonstrada ao operador para conferência.

Para replicar o período cadastrado para os demais dias da semana, clique sobre o botão *Copiar para demais dias* e posteriormente clique em *Salvar e concluir* para finalizar o processo.

intelbras

[Copiar para demais dias](#)

Zonas de tempo por dia da semana

Domingo Segunda-feira Terça-feira Quarta-feira Quinta-feira Sexta-feira Sábado

☒ Hora inicial 08:00 Hora final 18:00

☐ Hora inicial Hora final

☐ Hora inicial Hora final

Prévia da zonas de tempo configuradas para Segunda-feira

0h 4h 8h 12h 16h 20h 23h

Salvar e concluir Voltar

A nova zona de tempo cadastrada poderá ser editada ou excluída, para isso, basta selecionar a zona de tempo na tela inicial e clicar nos botões *Editar* ou *Excluir*.

intelbras

Zona de Tempo

Adicionar Editar Excluir

Selecione o campo +

Sem filtros aplicados

Nome da Zona de Tempo, Descrição	Selecionar todos
Nome da Zona de Tempo	Descrição
Intelbras	Horário Comercial
Zona de Tempo 24 Horas	Zona de Tempo 24 por 7

<< < 1 > >>

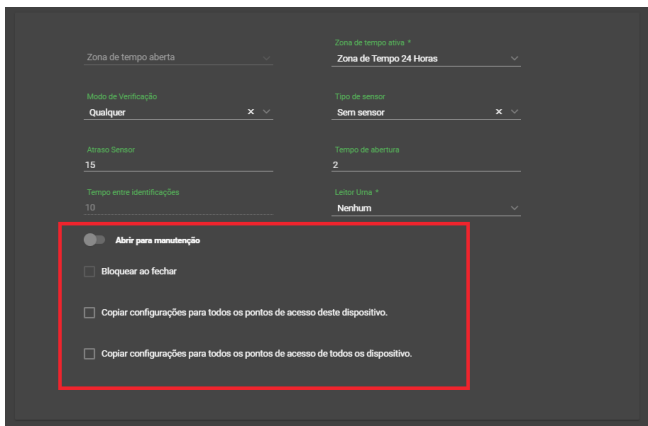
Só é possível cadastrar 16 timezones.

Importante: a zona de tempo 24h padrão do sistema não pode ser excluída.

5.2. Pontos de acesso

Pontos de acesso, são efetivamente as *portas* que estão sendo controladas pelos dispositivos controladores de acesso (hardware), para acessar os detalhes de configuração dessa seção, é necessário que um dispositivo controlador de acesso esteja devidamente adicionado ao sistema.

Selecione na tela inicial, o ponto de acesso que deseja alterar e clique no botão *Editar* para ter acesso as configurações da porta.



Na nova janela, é possível configurar na aba *Parâmetros básicos* as informações:

- » **Ponto de acesso:** nome que o operador do sistema deseja atribuir a porta;
- » **Tipo de ponto de acesso:** *Catraca, Portão, Porta e Cancela*.
- » **Câmera de monitoramento:** câmera do DVR que ficara vinculada aos eventos da porta.

Também é ilustrado o número da porta que é cadastrado automaticamente e a representação gráfica do tipo da porta escolhida.

Na aba *Detalhes* é possível configurar os seguintes parâmetros;

- » **Zona de tempo aberta:** período em que a porta permanecerá aberta sem controle.
- » **Método de verificação:** tipos de credenciais que serão válidas na verificação do acesso no dispositivo.
- » **Atraso do sensor de fechadura:** tempo em segundos que o alarme de porta aberta irá aguardar para disparar, caso a porta seja deixada aberta.
- » **Tempo entre identificações:** intervalo de tempo entre leituras de verificação de acesso em segundos.
- » **Zona de tempo da porta:** período de tempo em que a porta estará ativa. Ou seja, para que uma porta esteja ativa, ele deve estar vinculada a uma zona de tempo válida no sistema.
- » **Tipo de sensor de fechadura:** tipo de sensor da fechadura da porta (Normalmente aberto, normalmente fechado ou sem sensor).
- » **Tempo de abertura de porta:** tempo em segundos em que a porta permanecerá aberta após um evento de acesso liberado.

Também é possível marcar as seguintes caixas de seleção:

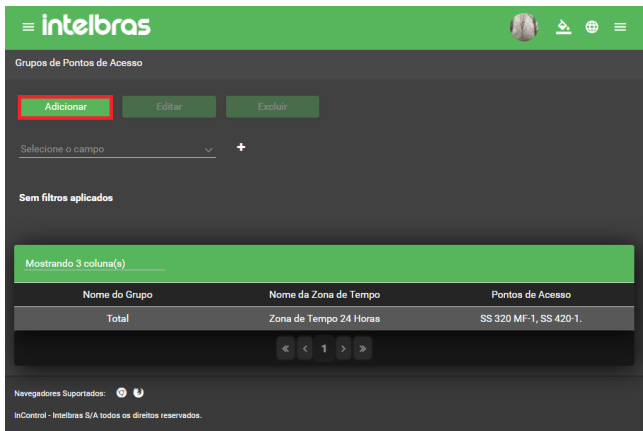
- » **Bloquear ao fechar:** esta função faz com que a porta seja trancada imediatamente no momento em que o sensor de fechadura, identifica que a porta fechou.
- » **Copiar configurações para todos os pontos de acesso deste dispositivo:** copia todas as configurações da porta, para todas as portas do dispositivo controlador de acesso.
- » **Copiar configurações para todos os pontos de acesso de todos os dispositivos:** copia todas as configurações da porta, para todas as portas de todos os dispositivos controladores de acesso de todo o sistema.
- » **Abrir para manutenção:** esta função permite deixar a porta aberta por tempo indeterminado.

Ao final das configurações, clique no botão *Salvar e concluir* para finalizar o processo.

Importante: o número de portas varia de acordo com o modelo do dispositivo.

5.3. Grupo de pontos de acesso

Grupos de pontos de acesso são grupos organizados que tem por função básica, unir os dispositivos controladores de acesso com os usuários do sistema de controle de acesso. Para cadastrar um grupo de pontos de acesso, na tela inicial desta seção clique em *Adicionar*.



Na nova janela, em *Parâmetros básicos* insira as informações e posteriormente clique no botão *Salvar e concluir* para finalizar o processo.

- » **Nome do Grupo do ponto de acesso;**
- » **Selecione o ponto de acesso:** ponto de acesso (porta) configurado no item anterior;
- » **Zona de tempo do grupo;**
- » **Nível do Grupo:** normal ou visitantes.

intelbras



Grupos de Pontos de Acesso > Grupos de Pontos de Acesso Edição

Parâmetros Básicos

Nome do Grupo

Total

Zona de Tempo *

Zona de Tempo 24 Horas

SS 320 MF-1, SS 420-1

Pontos de acesso selecionados:

 SS 320 MF-1

 SS 420-1

Salvar e concluir

Voltar

Navegadores Suportados:  

InControl - Intelbras S/A todos os direitos reservados.

6. Feriados

Feriados são datas pré-estabelecidas em que não haverá acesso permitido por parte dos usuários do sistema aos ambientes controlados. Para adicionar um feriado, na tela inicial, clique no botão *Adicionar*.

intelbras



Feriados

Adicionar

Editar

Excluir

Selecione o campo

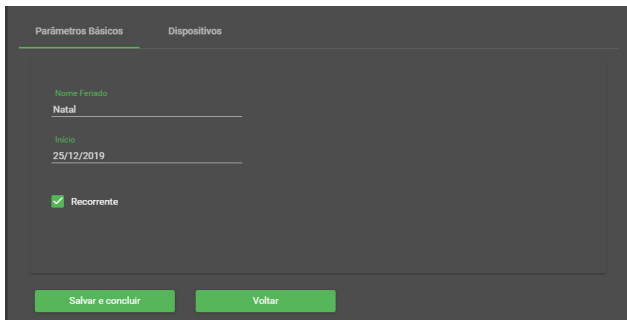
+

Sem filtros aplicados

Sem resultado

Não foram encontrados registros para esta pesquisa.

Na nova janela, na aba *Parâmetros Básicos*, preencha o nome do feriado, a data de início do feriado e marque o checkbox *Recorrente* caso este feriado se repita em outros anos.



Parâmetros Básicos Dispositivos

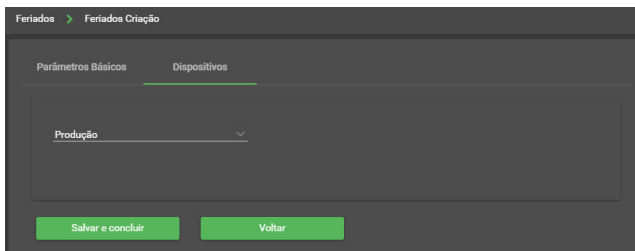
Nome Feriado
Natal

Início
25/12/2019

☒ Recorrente

Salvar e concluir Voltar

Na aba *Dispositivos* selecione qual dos dispositivos o feriado cadastrado será aplicado. Por fim, clique no botão *Salvar e concluir* para finalizar o processo.



Feriados > Feriados Criação

Parâmetros Básicos Dispositivos

Produção

Salvar e concluir Voltar

Importante:

- » É necessário que o dispositivo selecionado já tenha sido cadastrado no sistema anteriormente.
- » Caso um novo dispositivo seja adicionado ao software, é necessário editar o feriado para inclui-lo aos demais dispositivos pertencentes ao mesmo caso necessário.
- » Nem todos os dispositivos de controle de acesso suportam o cadastro de feriados. Nesta seção, serão demonstrados apenas os dispositivos que suportam essa funcionalidade.

6.1. Ações vinculadas a eventos

Esta seção, possibilita o acionamento de outras áreas dos dispositivos controladores de acesso a partir de gatilhos de eventos do sistema. Ou seja, quando houver um acesso negado pode ser acionado uma saída auxiliar do dispositivo que estará conectada a um outro sistema por exemplo.

Para cadastrar uma destas ações, na tela principal, clique no botão *Adicionar*.

Na nova janela insira as informações pertinentes e ao final clique no botão *Salvar* para finalizar o processo.

- » Nome da ação;
- » Tipo de evento gatilho;
- » Ponto de acesso que recebe o gatilho;
- » Ponto de acesso que será acionado;
- » Tipo de saída acionada;
- » Tempo em segundos de acionamento.

Parâmetros Básicos

Nome
Ação 1

Abertura Normal Produção-1

Produção-1 Saída auxiliar

Tempo de Acionamento
10

Salvar Voltar

É possível editar ou excluir uma ação, para isso, selecione-a na lista de ações cadastradas na tela principal, e clique nos botões *Editar* ou *Excluir*.

Importante: apenas dispositivos PULL SDK suportam essa funcionalidade.

intelbras

Ações Vinculadas à Eventos

Adicionar Editar Excluir

Selecione o campo +

Sem filtros aplicados

Nome	Gatilho	Nome Porta	Tipo Saída	Tempo de abertura
Intelbras	Abertura Normal	P&D-1	Saída auxiliar	10

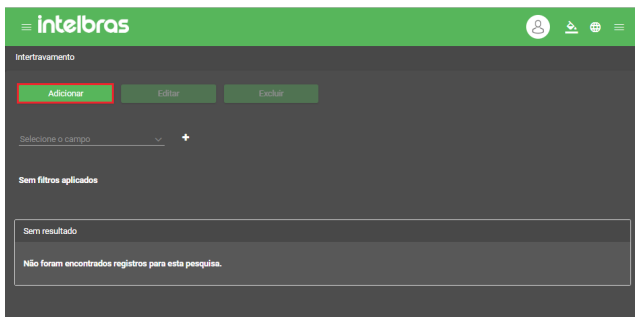
Mostrando 5 coluna(s) Desmarcar todos

< 1 >

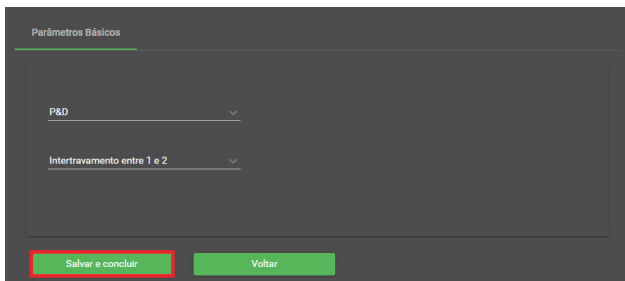
6.2. Intertravamento

Essa seção é restrita a linha CT 500 Intelbras, mais especificamente a partir do modelo CT 500 2P, de modo que com ela, é possível criar uma condição em que o segundo ponto de acesso (porta) só será liberado pelo evento de acesso quando o primeiro ponto de acesso (portar) estiver fechada e vice e versa.

Para cadastrar uma regra de Intertravamento, clique no botão *Adicionar* na tela principal de seção de Intertravamento.

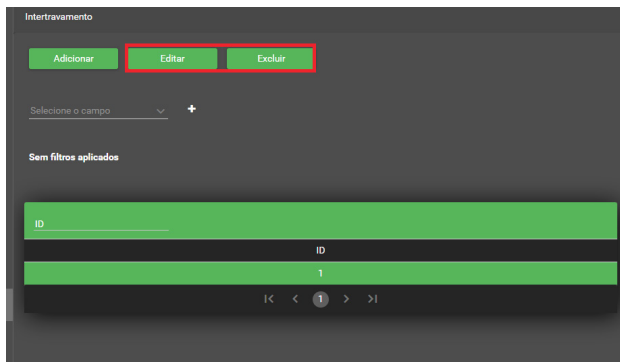


Na nova janela, selecione o tipo do dispositivo que receberá a nova regra de Intertravamento e a os pontos de acesso deste dispositivo que terão a regra instaurada. Por exemplo: entre ponto de acesso 1 e 2 (portas) ou entre pontos de acesso 3 e 4 (portas), para o caso do dispositivo CT 500 4P ou 4PB. Por fim clique em *Salvar e concluir* para finalizar o processo.



Importante: caso seja selecionado um dispositivo diferente da série CT 500 Intelbras, será exibido uma mensagem de erro e não será possível cadastrar as regras de Intertravamento.

É possível editar ou excluir a regra de Intertravamento cadastrada. Para isso, selecione-a na lista de regras disponíveis e clique nos botões *Editar* ou *Excluir*.



Importante: esta funcionalidade só está disponível para controladoras de linha CT 500 Intelbras.

7. Relatórios

Relatórios são informações gerenciais do sistema de controle de acesso de modo que os eventos de acesso, alarmes, aberturas remotas podem ser consolidados e eventualmente exportados para arquivos em Excel para uma posterior análise.

7.1. Eventos de usuários

Eventos de usuário, são todas as informações relativas aos pontos de acesso (portas), ou seja, acessos liberados, acessos negados, tentativas de acesso desconhecidas, eventos de alarmes, aberturas remotas, etc.

Na tela inicial, são exibidas todas as informações referentes aos pontos de acesso (porta) e para exportar as informações para um arquivo em Excel, clique no botão *Exportar*.

Nome do usuário	Tipo	Nome do Dispositivo	Data Evento	Tipo de evento	Observações
Usuário desconhecido	Credencial desconhecida	CT 500 4 PB	15-07-2019 14:12:03.000	Acesso Negado	
Usuário desconhecido	Credencial desconhecida	CT 500 4 PB	15-07-2019 14:12:03.000	Acesso Negado	
Douglas de Moraes	Cartão	CT 500 4 PB	15-07-2019 14:11:59.000	Acesso Liberado	
Usuário desconhecido	Credencial desconhecida	CT 500 4 PB	15-07-2019 14:11:56.000	Acesso Negado	
Usuário desconhecido	Credencial desconhecida	CT 500 4 PB	15-07-2019 14:11:56.000	Acesso Negado	
Usuário desconhecido	Credencial desconhecida	CT 500 4 PB	15-07-2019 14:11:53.000	Acesso Negado	
Usuário desconhecido	Credencial desconhecida	CT 500 4 PB	15-07-2019 14:11:53.000	Acesso Negado	

Ao clicar sobre o evento caso tenha uma câmera de monitoramento vinculada ao dispositivo, será possível verificar a gravação da imagem 5 segundos antes e após o evento seguido da imagem de contexto e foto do usuário, na opção *Download* é possível realizar o download do vídeo relacionado ao evento.

Mostrando 8 coluna(s) ▼

	Nome do usuário	Tipo	Código da Credencial	Acesso	Nome do Dispositivo	Data Evento	Tipo de evento	Observações
☐	Desconhecido	Desconhecida		Entrada	FACE	09-03-2020 09:23:56:000	Evento de Acesso	
☒	Desconhecido	Desconhecida		Entrada	FACE	09-03-2020 09:23:10:000	Evento de Acesso	

Imagem Contexto



Foto do Usuário



NVD 3208 P



Download

☐	Desconhecido	Desconhecida		Entrada	Desconhecido	09-03-2020 08:57:42:000	Evento de Acesso	
--------------------------	--------------	--------------	--	---------	--------------	----------------------------	------------------	--

Mostrando 8 coluna(s) ▼

	Nome do usuário	Tipo	Código da Credencial	Acesso	Nome do Dispositivo	Data Evento	Tipo de evento	Observações
☐	Desconhecido	Desconhecida		Entrada	FACE	09-03-2020 09:23:56:000	Evento de Acesso	
☒	Desconhecido	Desconhecida		Entrada	FACE	09-03-2020 09:23:10:000	Evento de Acesso	

Imagem Contexto



Foto do Usuário



NVD 3208 P



Download

☐	Desconhecido	Desconhecida		Entrada	Desconhecido	09-03-2020 08:57:42:000	Evento de Acesso	
☐	Desconhecido	Desconhecida		Entrada	Desconhecido	09-03-2020 08:57:23:000	Evento de Acesso	

Importante: para o funcionamento correto o DVR e o servidor InControl devem estar com o horário sincronizados, recomendamos a utilização de um servidor NTP para esta aplicação.

7.2. Eventos de operadores

Esta seção exibe na tela inicial todos os eventos, ou seja, ações executadas pelos Operadores do sistema. Essas informações podem ser exportadas para um arquivo em Excel para posteriores consultas. Para isso, clique no botão *Exportar* para gerar o arquivo.

intelbras



Eventos de Operador

Exportar

Selecione o campo  

Sem filtros aplicados

Mostrando 5 coluna(s)

Selecionar todos

Operador	Ação	Data Evento	Objeto Afetado	Tipo Objeto
Admin	Alterar	31-05-2019 01:41	Intelbras	GrupoPontosAcesso
Admin	Alterar	31-05-2019 01:40	Intelbras	Dispositivo
Admin	Alterar	31-05-2019 01:40	RAFAEL NAPOLI ARTONI	Usuario
Admin	Inserir	31-05-2019 01:39	Intelbras	GrupoPontosAcesso
Admin	Inserir	31-05-2019 01:39	Intelbras	Dispositivo
Admin	Alterar	31-05-2019 01:38	RAFAEL NAPOLI ARTONI	Usuario
Admin	Inserir	31-05-2019 01:38	RAFAEL NAPOLI ARTONI	Usuario
Admin	Deletar	31-05-2019 08:39	Usuario Normal Padrao	Usuario
Admin	Deletar	31-05-2019 08:39	Usuario Terceirizado Padrao	Usuario

|<

<

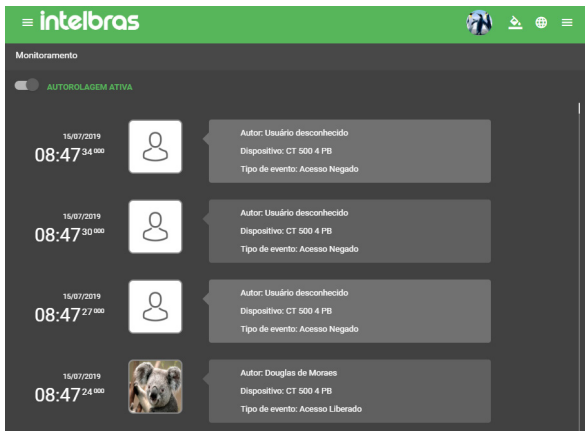


>

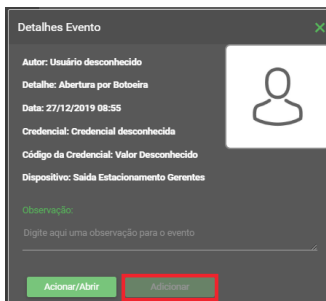
>|

7.3. Monitoramento

Nesta seção estão apresentados todos os eventos de acesso do sistema de modo que o operador pode acompanhar as informações em tempo real, também são exibidos atrelados ao evento de acesso dos usuários as suas respectivas fotos que foram cadastradas em seus perfis para auxiliar na identificação dos mesmos.



É possível adicionar uma observação no evento. Para isso, basta efetuar um duplo clique sobre o evento desejado e na nova janela, digitar as informações pertinentes sobre o evento de acesso e clique no botão **Adicionar** para salvar as observações inseridas.



Nesta tela também é possível efetuar uma abertura remota na porta controlada pelo dispositivo de controle de acesso em questão. Para isso, clique no botão *Adicionar / Abrir* para efetuar a abertura da porta remotamente.

Detalhes Evento

Autor: Usuário desconhecido

Detalhe: Abertura por Botoeira

Data: 27/12/2019 08:55

Credencial: Credencial desconhecida

Código da Credencial: Valor Desconhecido

Dispositivo: Saida Estacionamento Gerentes

Observação:
Digite aqui uma observação para o evento

Acionar/Abrir

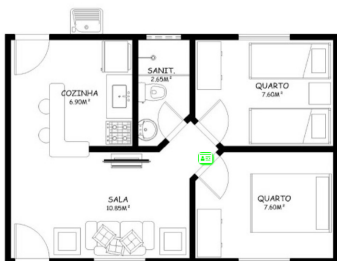
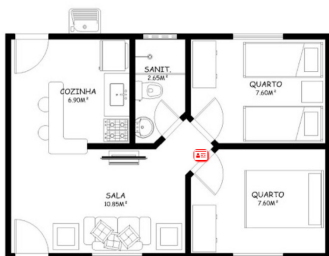
Adicionar

7.4. Monitoramento de área

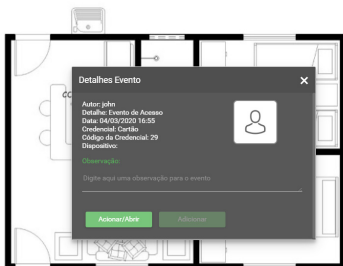
Nesta seção será possível acompanhar os eventos em tempo real através da adição da planta baixa do local, como configurado anteriormente nas opções de área, ao selecionar a área será exibido a planta baixa juntamente com as portas cadastradas



Os eventos serão apresentados com as cores verde (Acesso liberado) ou vermelho (Acesso Negado).



Para visualizar os detalhes do evento basta clicar duas vezes com o botão esquerdo do mouse sob o evento e será apresentada as informações.



8. Sistema

Nesta seção estão listadas as funções que proporcionam a configuração geral do sistema no que diz respeito ao Gerenciamento de banco de dados e configuração dos campos personalizados do cadastro de usuário.

8.1. Gerenciamento de banco de dados

Nesta seção é possível visualizar a instância do banco de dados ativa para o banco de dados do software. Para isso, na tela inicial, clique no botão *Visualizar*.

Gerenciamento de Banco de Dados

Visualizar ⚙️

Selecione o campo ▾ +

Sem filtros aplicados

Mostrando 8 coluna(s)

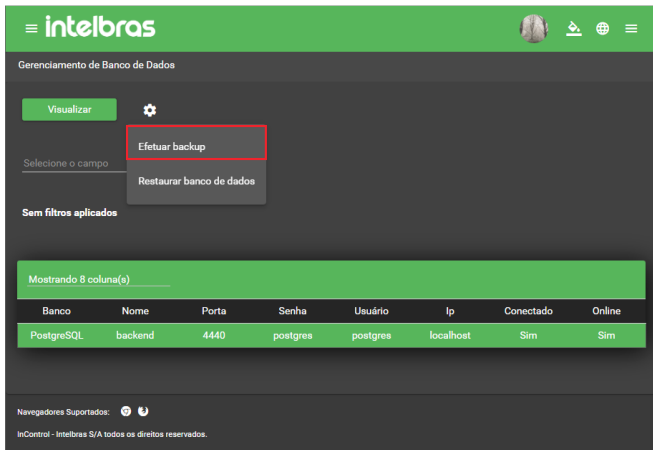
Banco	Nome	Porta	Senha	Usuário	Ip	Conectado	Online
PostgreSQL	backend	4440	postgres	postgres	localhost	Sim	Sim

Navegadores Suportados 🌐 📱

No ícone de engrenagem, é possível selecionar quatro opções referentes ao banco de dados:

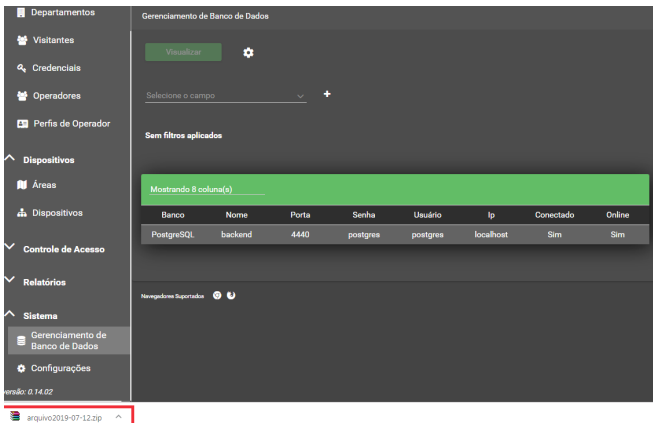
- » Efetuar Backup;
- » Restaurar Banco de dados;
- » Reset banco de dados;
- » Reparar banco de dados.

Ao selecionar a opção *Efetuar backup*, um arquivo compactado será baixado em seu computador. Basta acompanhar este processo e salvar o arquivo compactado em uma pasta do servidor.



The screenshot shows the Intelbras InControl web interface. At the top, there's a green header with the Intelbras logo and navigation icons. Below the header, the main section is titled 'Gerenciamento de Banco de Dados'. It features a 'Visualizar' button and a settings gear icon. A dropdown menu is open, showing 'Efetuar backup' (highlighted with a red box) and 'Restaurar banco de dados'. Below this, there's a section 'Mostrando 8 coluna(s)' followed by a table with 8 columns: Banco, Nome, Porta, Senha, Usuário, Ip, Conectado, and Online. The table contains one row of data for PostgreSQL. At the bottom, it says 'Navegadores Suportados' with icons for Chrome and Firefox, and a footer with 'InControl - Intelbras S/A todos os direitos reservados.'

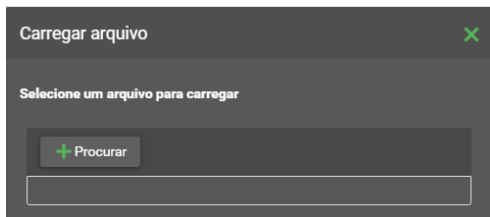
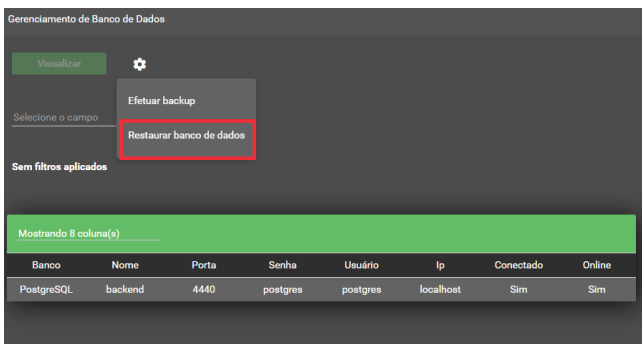
Banco	Nome	Porta	Senha	Usuário	Ip	Conectado	Online
PostgreSQL	backend	4440	postgres	postgres	localhost	Sim	Sim



This screenshot shows the same Intelbras InControl interface but with a sidebar menu on the left. The sidebar includes sections like 'Departamentos', 'Visitantes', 'Credenciais', 'Operadores', 'Perfis de Operador', 'Dispositivos', 'Áreas', 'Dispositivos', 'Controle de Acesso', 'Relatórios', and 'Sistema'. Under 'Sistema', 'Gerenciamento de Banco de Dados' is selected. The main content area is identical to the previous screenshot, showing the 'Gerenciamento de Banco de Dados' section with the 'Efetuar backup' button highlighted. At the bottom left, there's a version number 'versão: 0.14.02' and a download link 'arquivo2019-07-12.zip' highlighted with a red box.

Banco	Nome	Porta	Senha	Usuário	Ip	Conectado	Online
PostgreSQL	backend	4440	postgres	postgres	localhost	Sim	Sim

Para restaurar um banco de dados, selecione a opção *Restaurar banco de dados* e na nova janela, carregue o arquivo compactado disponibilizado na etapa de backup.

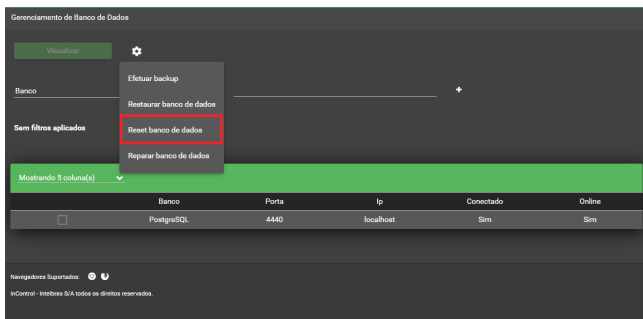


Após a seleção do arquivo, acompanhe a progressão do processo e verifique se os dados estão condizentes aos dados do momento em que foi feito o backup do banco.

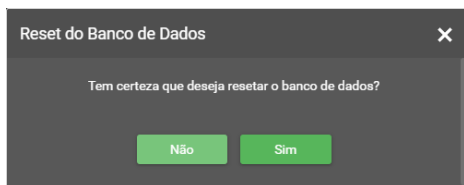
Importante:

- » A restauração do banco de dados só pode ser feita ao carregar o arquivo compactado inteiro.
- » Não é possível criar uma nova instância para o banco de dados sem efetuar a desinstalação do software por completo.

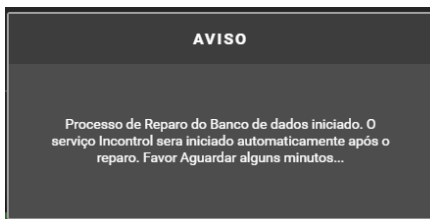
A opção *Reset banco de dados* permite que todos os dados contidos no banco do InControl sejam apagados, retornando o software as configurações padrões.



Ao selecionar esta opção será mostrado uma mensagem perguntando se realmente deseja realizar este procedimento, após o procedimento de reset o software irá retornar a tela inicial de login.



A opção *Reparar banco* de dados inicia um processo de prevenção e manutenção do banco, corrigindo possíveis arquivos danificados ou corrompidos.



O processo de reparo irá demorar conforme o tamanho do banco de dados, após a finalização do processo atualize a página do navegador para acessar novamente o software.

8.2. Configurações

Na aba *Ambiente* é possível personalizar o tipo de ambiente ao qual o sistema irá ser utilizado, os tipos de ambientes são: Condomínio Vertical, Condomínio Horizontal, Empresa Padrão. Ao selecionar um determinado ambiente as telas cadastro de usuário irão alterar os seus campos de acordo com o ambiente selecionado.

The screenshot shows the 'Ambiente' configuration screen for 'Empresa Padrão'. The interface has a dark theme with a top navigation bar containing four tabs: 'Ambiente' (selected), 'Campos personalizados', 'Padrão do cartão', and 'Configurações de backup'. Below the tabs, the 'Ambiente' dropdown is set to 'Empresa Padrão'. A green box highlights the main form area, which includes input fields for 'Nome Completo *', 'Matrícula', 'Grupo de Acesso', 'Departamento', and 'Unidade'. The 'Departamento' and 'Unidade' fields are highlighted with a red box. To the right of the form is a user profile card with a placeholder icon and icons for video, photo, upload, search, and delete. At the bottom is a green 'Salvar configuração' button.

The screenshot shows the 'Ambiente' configuration screen for 'Condomínio Vertical'. The interface is identical to the previous one, but the 'Ambiente' dropdown is set to 'Condomínio Vertical'. The green box highlights the main form area, which includes input fields for 'Nome Completo *', 'Matrícula', 'Grupo de Acesso', 'Bloco', and 'Apartamento'. The 'Bloco' and 'Apartamento' fields are highlighted with a red box. To the right of the form is a user profile card with a placeholder icon and icons for video, photo, upload, search, and delete. At the bottom is a green 'Salvar configuração' button.

Na aba *Campos personalizados* será possível, nomear os campos personalizados que estão disponíveis no cadastro de usuários, basta preencher os nomes nos campos disponíveis.

A interface mostra o menu "Configurações" com a aba "Campos personalizados" selecionada. O conteúdo principal é uma caixa de configuração com o título "Configuração de campos personalizados". Dentro, há cinco campos de texto, cada um com o rótulo "Nome do campo" em verde e o placeholder "Campo personalizado X" (onde X varia de 1 a 5). Abaixo da caixa, há um botão verde com o texto "Salvar configuração".

Na aba *Padrão do cartão* pode ser definido qual o tipo de leitura será considerado padrão do sistema. As opções são:

- » 26 bits;
- » 34 bits.

Após a definição, é necessário clicar no botão *Salvar configuração* para finalizar o processo.

A interface mostra o menu "Configurações" com a aba "Padrão do cartão" selecionada. O conteúdo principal é uma caixa de configuração com o rótulo "Tamanho *" em verde e um menu suspenso com a opção "26 bits" selecionada. Abaixo da caixa, há um botão verde com o texto "Salvar configuração", que está destacado por um retângulo vermelho.

Na aba *Configurações de backup*, é possível configurar os seguintes parâmetros para o backup do banco de dados:

- » Na aba *Configurações de backup*, é possível configurar os seguintes parâmetros para o backup do banco de dados:
- » Caminho de backup: local onde serão salvos os arquivos de backup do banco de dados comumente.
- » Periodicidade: diário ou semanal, possibilitando selecionar os dias da semana em que ocorrerão o backup.
- » Horário do backup: horário de início da rotina de backup do banco de dados.
- » Quantidade máxima de backups: quantidades de arquivos de backups que serão gerados pelo sistema.

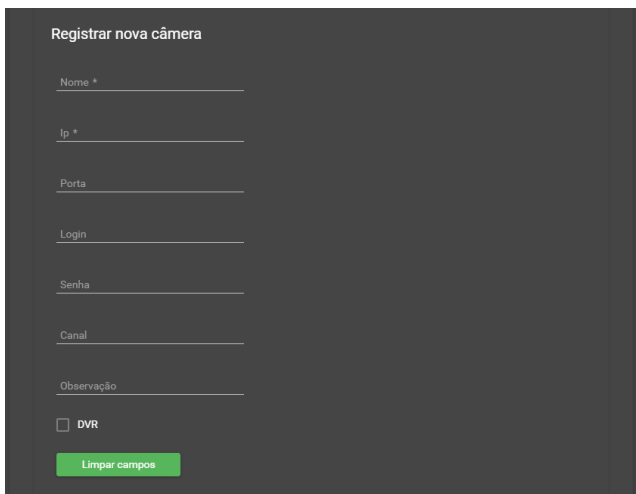
Ao final, clique na opção *Salvar* a configuração para concluir as configurações de backup.

A imagem mostra a interface de configuração de backup de um sistema. No topo, há uma barra de navegação com as seguintes abas: Ambiente, Campos personalizados, Padrão do cartão, Configurações de backup (destacada com uma linha verde), Câmeras de Monitoramento e Atualizações. Abaixo, o formulário de configuração contém os seguintes campos: 1. 'Caminho de backup' com um campo de texto e um botão verde 'Testar Caminho'. 2. 'Periodicidade *' com um menu suspenso selecionando 'Semanal'. 3. Uma linha de dias da semana com checkboxes: Segunda (desselecado), Terça (selecado), Quarta (desselecado), Quinta (selecado), Sexta (desselecado), Sábado (selecado) e Domingo (desselecado). 4. 'Horário do backup' com um campo de texto contendo '00:00'. 5. 'Quantidade máxima de backups' com um campo de texto contendo '10'. 6. Um botão verde 'Salvar configuração' na base do formulário.

É possível cadastrar as câmeras de monitoramento do ambiente no sistema para que posteriormente possa ser feito a captura das imagens de usuários e veículos. Para isso, na aba *Câmeras de monitoramento* insira as informações demandadas:

- » Nome da câmera;
- » Endereço de IP;
- » Login;
- » Senha;
- » Canal;
- » Observação;
- » DVR.

Para salvar as configurações clique no botão *Adicionar câmera*.



Registrar nova câmera

Nome *

Ip *

Porta

Login

Senha

Canal

Observação

☐ DVR

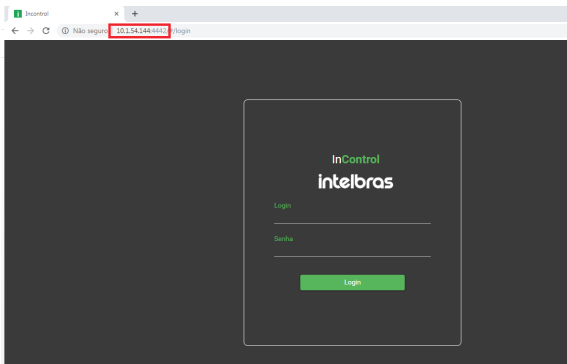
Limpar campos

Importante:

- » **Dispositivos não suportados:** linha Mibo, VIP 1020 B/D, VIP 1220 B/D, VIP 1120 B/D, VIP 1130 VF, VIP 1130 D VF, VIP 3230 VF.
- » **Câmeras homologadas:** VIP S4020 G2, VIP 3020 G1/G2, VIP 3240, VIP 3230 B/D G2, VIP 3220 B/D, VIP 3430 B/D.

8.3. Acesso via web

O Software InControl é um software web, o que possibilita acessar ao software instalado no servidor de forma prática e rápida via navegador web. Para isso, na tela principal do navegador web, digite o endereço de IP da máquina Servidor em que o Incontrol está rodando e a sua respectiva porta.

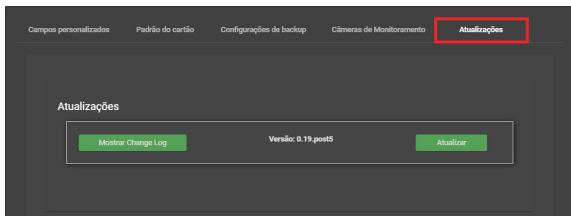


Para acessar e fazer login utilize as credenciais de operadores que fazem parte do mesmo banco de dados da instancia ativa no servidor do software.

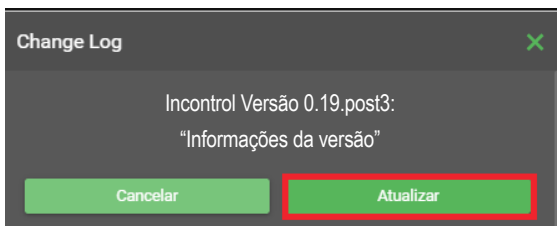
Importante: é necessário que a máquina Cliente esteja na mesma rede (LAN) do servidor do software.

8.4. Atualizações

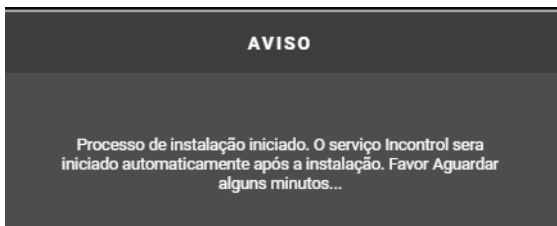
Ao clicar na aba de Atualizações o sistema irá verificar se há uma nova versão disponível, as atualizações incluem melhorias, novas funcionalidades e correções de bugs. É recomendado sempre manter o sistema atualizado em sua última versão.



Caso houver alguma atualização disponível, selecione a opção *Mostrar Change Log* para consultar a lista com as mudanças desta versão, pressione o botão *Atualizar* para iniciar o processo.



Após clicar em atualizar o sistema irá reiniciar automaticamente, o processo de atualização pode levar alguns minutos variando de acordo com alguns fatores como velocidade de conexão e recursos do servidor.



Importante: antes de realizar a atualização, é recomendado realizar o backup do banco de dados como descrito neste documento.

Política de privacidade

Esta é a Política de privacidade ("Política") que é firmada entre você, de agora em diante denominado Usuário, e a Intelbras S/A - Indústria de Telecomunicação Eletrônica Brasileira, pessoa jurídica de direito privado, inscrita no CNPJ/MF sob o nº 82.901.000/0001-27, estabelecida na rodovia BR 101, km 210, Área Industrial, São José/SC, representando, neste ato, todas as suas filiais, de agora em diante denominada INTELBRAS. Esta Política foi projetada para regular a coleta, o armazenamento, o uso e o compartilhamento de informações compartilhadas com a INTELBRAS. Ao aceitar esta Política, o Usuário reconhece que analisou e concordou com as condições descritas, e permite que a INTELBRAS colete, armazene, use e compartilhe suas informações de acordo com os termos desta Política, bem como manifesta ciência de que a Política pode ser modificada, a qualquer tempo, com todas as atualizações publicadas nesta página. Sendo usuário menor de idade ou incapaz em quaisquer aspectos, precisará da permissão de seus pais ou responsáveis, que também deverão concordar com a Política e suas condições.

Qualquer dúvida em relação à Política de Privacidade pode ser esclarecida nos contatos:

E-mail: privacidade@intelbras.com.br

1. Coleta de informações

Ao utilizar o software disponibilizado pela INTELBRAS, fica o Usuário ciente de que a INTELBRAS poderá coletar as informações de acesso e de cadastro, tais como nome, telefone, e-mail, endereço, conforme descrito nesta Política. As informações podem ser classificadas em dois tipos: pessoais e não pessoais.

Informações pessoais são dados que estão relacionados ao Usuário, e que permitem a sua identificação, incluindo, mas não se limitando ao nome, data de nascimento, endereço de contato, número de contato, endereço de e-mail e arquivos de conteúdo em vídeo que podem conter informações de identidade visual pessoal.

Informações não pessoais são dados que não estabelecem qualquer relação com um indivíduo específico, como ocupação, idioma, código de área, números de série do produto, URLs, comportamento do usuário, arquivos de conteúdo em vídeo que não contenham informações de identidade visual pessoais, etc.

2. Armazenamento de informações pessoais

Conforme estipulado na Política, a INTELBRAS armazenará suas informações pessoais por determinado período de tempo e utilizará as tecnologias disponíveis para evitar a perda de dados, o uso indevido, a divulgação não autorizada e outros problemas relativos à segurança da informação, e também realizará uma revisão periódica da eficácia dos atuais métodos de armazenamento e tratamento, incluindo precauções de segurança física, para evitar o acesso não autorizado.

A INTELBRAS possui as melhores práticas, incluindo tecnologias e estratégias razoáveis para a proteção dos dados, mas a INTELBRAS não pode garantir que suas informações pessoais estejam sob segurança absoluta, tendo em vista a tecnologia de segurança da informação existente. O Usuário reconhece que a INTELBRAS não se responsabiliza por quaisquer perdas no caso de suas informações pessoais serem reveladas, furtadas ou roubadas por motivo de força maior ou problemas de segurança que não tenham sido causados pela INTELBRAS.

3. Uso de informações pessoais

A fim de proporcionar uma melhor experiência ao usuário, a INTELBRAS poderá usar suas informações pessoais para os seguintes propósitos:

- » Viabilizar o uso do software com todas as suas soluções e funcionalidades, armazenando o histórico necessário para o seu funcionamento e melhor experiência do Usuário.
- » Aumentar a segurança do aplicativo e de outros serviços prestados pela INTELBRAS, tais como autenticação de usuários, proteção de segurança, detecção de fraudes, arquivamento e backups.
- » A menos que o Usuário opte por cancelar a inscrição, a INTELBRAS poderá contatá-lo enviando comunicações eletrônicas para informar sobre novos produtos e serviços. A INTELBRAS também poderá utilizar informações pessoais para fins internos, tais como auditorias, análise de dados e pesquisas.

4. Compartilhamento de informações pessoais

A INTELBRAS não divulgará suas informações pessoais, a menos que (i) tenha seu consentimento prévio por escrito; (ii) esteja de acordo com as leis e regulamentos aplicáveis ou exigidos pelas autoridades; (iii) seja obrigada por decisão judicial; (iv) esteja de acordo com os termos da Política; (v) seja essencial para a proteção dos interesses legítimos da INTELBRAS.

A INTELBRAS poderá permitir que seus funcionários acessem os dados em ocasiões específicas com base na necessidade de conhecimento, e assegurará que cumpram com as obrigações no mesmo nível estabelecido pela Política.

Além disso, a INTELBRAS pode disponibilizar certas informações a parceiros estratégicos confiáveis que ocasionalmente trabalham com a INTELBRAS para proporcionar uma melhor experiência ao Usuário e aumentar a qualidade dos serviços do software. Sob essas circunstâncias, a aceitação da Política significa que o Usuário concorda e autoriza a INTELBRAS a fornecer suas informações a tais terceiros.

5. Âmbito de aplicação

Esta Política diz respeito a todos os aplicativos, sites e outros serviços prestados pela INTELBRAS, exceto quando indicado de outra forma.

Os sites da INTELBRAS podem conter links para serviços fornecidos por terceiros. As informações dos usuários podem ser coletadas por terceiros quando do uso destes links, portanto, a INTELBRAS recomenda que o Usuário conheça suas práticas de privacidade.

As informações não pessoais não são regidas pela Política, além disso, você concorda que a INTELBRAS tem o direito de coletar, armazenar, usar e compartilhar suas informações não pessoais para quaisquer e todos os fins, incluindo, sem limitação:

- » Entender o comportamento do usuário, a fim de otimizar sua experiência, aperfeiçoar o design funcional, e fornecer melhores serviços;
- » Analisar o banco de dados, em parte ou no todo, para fins comerciais, incluindo, mas não se limitando a: análise de dados e uso dos dados obtidos a partir do número de visitas do usuário, período das visitas, preferências do usuário e outros dados.

6. Cookies e tecnologias semelhantes

A INTELBRAS usa cookies (pequenos arquivos de texto inseridos no dispositivo do usuário) e tecnologias semelhantes para fornecer serviços online e sites e ajudar a coletar dados. Os cookies armazenam as preferências e configurações do usuário, permitindo, entre outras ações: iniciar a sessão rapidamente, identificar os interesses dos usuários e promover anúncios com base nesses interesses, combater fraudes e analisar o desempenho de sites e serviços online.

A INTELBRAS usa web beacons para ajudar a enviar cookies e a reunir dados de desempenho. Os sites podem incluir web beacons e cookies de fornecedores de serviços de terceiros.

O usuário tem à sua disposição uma variedade de ferramentas para controlar os cookies, web beacons e tecnologias semelhantes, incluindo controles de navegador para bloquear e eliminar cookies e controles de provedores de serviços de análise de terceiros para recusar a coleta de dados através de web beacons e tecnologias semelhantes. O navegador e outras escolhas do usuário podem ter impacto em suas experiências com o uso deste aplicativo, software ou serviço.

7. Atualizações na Política de Privacidade

Esta Política passa por constantes atualizações, assim, a INTELBRAS recomenda rever periodicamente esta página para acompanhar e estar ciente das modificações. Caso sejam feitas alterações relevantes nos termos desta Política, a INTELBRAS publicará a nova Política, notificando o Usuário.

Se você suspeitar de que suas informações pessoais estejam sendo coletadas ou utilizadas de maneira ilegal, ou que qualquer regra desta Política esteja sendo infringida de qualquer maneira, entre em contato com a INTELBRAS, imediatamente, através do site www.intelbras.com.br ou e-mail privacidade@intelbras.com.br.

Termos de uso de software

1. Aceitação do contrato

Este é um contrato firmado entre você, de agora em diante denominado de USUÁRIO, e a Intelbras S/A – Indústria de Telecomunicação Eletrônica Brasileira, pessoa jurídica de direito privado, inscrita no CNPJ/MF sob o nº 82.901.000/0001-27, estabelecida na rodovia BR 101, km 210, Área Industrial, São José/SC, e de agora em diante denominada simplesmente de Intelbras. Estes Termos de uso de serviço regem o uso do serviço disponibilizado gratuitamente pela Intelbras e/ou seus parceiros, denominado INTELBRAS INCONTROL WEB, desenvolvido para computadores em LAN. Se você não concordar com estes termos não use esse serviço. Leia-as atentamente, pois, se você começou a usar esse serviço, ficará configurado que aceitou todos os termos e concorda em cumpri-los. Se você, usuário, for menor de idade ou declarado incapaz em quaisquer aspectos, precisará da permissão de seus pais ou responsáveis, que também deverão concordar com estes mesmos termos e condições.

2. Licença limitada

Você recebeu uma licença limitada, não transferível, não exclusiva, livre de royalties e revogável, para baixar, instalar, executar e utilizar esse serviço em seu dispositivo. Você reconhece e concorda que a Intelbras concede ao usuário uma licença exclusiva para uso e, dessa forma, não lhe transfere os direitos sobre o produto. O serviço deverá ser utilizado por você, usuário. A venda, transferência, modificação, engenharia reversa ou distribuição, bem como a cópia de textos, imagens ou quaisquer itens contidos no software são expressamente proibidas. Você reconhece que a Intelbras é proprietária de todos os direitos, títulos e interesses referentes ao INTELBRAS INCONTROL WEB e ao software relacionado. INTELBRAS INCONTROL WEB é a marca comercial ou registrada da Intelbras. Você não pode alterar, destruir, ocultar ou remover de outra forma qualquer as informações sobre direito autoral, os rótulos ou avisos de propriedade dos softwares da Intelbras.

3. Do Cadastro

Para a acesso ao software é necessário que o USUÁRIO realize um cadastro prévio onde forneça voluntariamente informações sobre si, tais como: USUÁRIO, senha, endereço de e-mail (*Dados*). O USUÁRIO declara que os Dados fornecidos são fiéis e verdadeiros e compromete-se a manter seus dados sempre atualizados.

INTELBRAS não é responsável pelas informações prestadas, mas se reserva o direito de verificar, a qualquer momento, a veracidade de tais informações e solicitar, a seu

exclusivo critério, a documentação suporte que julgar necessária para a devida comprovação das informações prestadas. Caso a INTELBRAS detecte alguma conta feita a partir de informações falsas, o cadastro do USUÁRIO será automaticamente cancelado de forma que o USUÁRIO não terá mais acesso ao uso dos Serviços, não assistindo ao USUÁRIO, por este motivo, qualquer direito de indenização ou ressarcimento.

O titular e administrador da conta será aquele definido no momento do cadastro, a partir dos Dados oferecidos pelo USUÁRIO. A conta é pessoal e poderá ser acessada unicamente mediante a utilização do USUÁRIO e senha criados pelo próprio USUÁRIO no momento do cadastro, sendo este o único e exclusivo responsável por manter o sigilo de seu USUÁRIO e senha, a fim de garantir a segurança de sua conta e impedir o acesso não autorizado por terceiros. O USUÁRIO é o único responsável por todas as atividades associadas a sua conta.

O USUÁRIO deverá seguir os padrões de segurança de registro de senha e realizar a troca imediata da senha padrão.

4. Direitos autorais

O USUÁRIO não adquire, pelo presente instrumento ou pela utilização do SOFTWARE, nenhum direito de propriedade intelectual ou outros direitos exclusivos, incluindo patentes, desenhos, marcas, direitos autorais ou quaisquer direitos sobre informações confidenciais ou segredos de negócio, bem como sobre o conteúdo disponibilizado no software, incluindo, mas não se limitando a textos, gráficos, imagens, logotipos, ícones, fotografias, conteúdo editorial, notificações, softwares e qualquer outro material, sobre a INTELBRAS ou relacionados a ele ou a qualquer parte dele. O USUÁRIO também não adquire nenhum direito sobre o SOFTWARE ou relacionado a ele ou a qualquer componente dele, além dos direitos expressamente licenciados ao USUÁRIO neste Termo ou em qualquer outro contrato mutuamente acordado por escrito entre as partes.

Ao utilizar o SOFTWARE, o USUÁRIO concorda em cumprir com as seguintes diretrizes:

I. Não é permitido postar ou transmitir informação, dado, texto, software, gráficos, sons, fotografias, vídeos, mensagens ou outro conteúdo que seja ilegal, ofensivo, impreciso, difamatório, obsceno, fraudulento, prejudicial, ameaçador ou abusivo.

II. Não interferir no uso de outros usuários do SOFTWARE.

III. Não postar ou fazer upload de qualquer vírus, worms, arquivo corrompido ou outro software capaz de perturbar, incapacitar ou prejudicar o funcionamento do SOFTWARE.

- IV. Cumprir com este Termo e quaisquer leis ou regulamentos aplicáveis;
- V. Não se passar por qualquer pessoa ou entidade, declarar falsamente ou deturpar sua afiliação com uma pessoa ou entidade.
- VI. Não enviar ou transmitir conteúdo que o USUÁRIO não tem o direito de publicar ou transmitir sob qualquer lei ou sob relações contratuais ou fiduciárias (tais como informação privilegiada, informações confidenciais, etc).
- VII. Não usar o SOFTWARE para solicitar, obter ou armazenar dados pessoais ou senhas de outros usuários.

5. Alterações, modificações e rescisão

A Intelbras reserva-se o direito de, a qualquer tempo, modificar estes termos, seja incluindo, removendo ou alterando quaisquer de suas cláusulas. Tais modificações terão efeito imediato após a publicação. Ao continuar com o uso do serviço você terá aceitado e concordado em cumprir os termos modificados. Assim como, a Intelbras pode, de tempos em tempos, modificar ou descontinuar (temporária ou permanentemente) a distribuição ou a atualização desse serviço. O USUÁRIO não poderá responsabilizar a Intelbras nem seus diretores, executivos, funcionários, afiliados, agentes, contratados ou licenciadores por quaisquer modificações, suspensões ou descontinuidade do serviço.

Para fins contratuais, o USUÁRIO concorda em receber comunicações da INTELBRAS de forma eletrônica (termos e condições, acordos, notificações, divulgações e outras comunicações da INTELBRAS), seja por e-mail ou comunicação interna no próprio SOFTWARE e que, desta forma estabelecida, as comunicações da INTELBRAS satisfaçam e cumprem com os requisitos legais, como se fosse em via impressa.

6. Indenização

Em nenhum caso a INTELBRAS será responsável por danos pessoais ou qualquer prejuízo incidental, especial, indireto ou consequente, incluindo, sem limitação, prejuízos por perda de lucro, corrupção ou perda de dados, falha de transmissão ou recepção de dados, não continuidade do negócio ou qualquer outro prejuízo ou perda comercial, decorrentes ou relacionados ao uso do SOFTWARE ou a sua incapacidade em usar o SOFTWARE, por qualquer motivo.

7. Consentimento para coleta e proteção do uso de dados

O USUÁRIO concorda que a INTELBRAS pode coletar os dados pessoais de cadastro e perfil, e usar dados técnicos de seu dispositivo, tais como especificações, configurações, versões de sistema operacional, tipo de conexão à internet e afins.

Os dados pessoais coletados do USUÁRIO serão exclusivamente utilizados para fins de execução do presente contrato, com o objetivo principal de ativação das funcionalidades do SOFTWARE, sendo que o uso destes dados é intrínseco ao próprio funcionamento do SOFTWARE, e para uso e benefícios do titular. Ainda, alguns recursos do SOFTWARE poderão solicitar dados adicionais do USUÁRIO, tais como, nome, telefone, endereço, funcionários, instaladores, serviços prestados, região de atendimento, treinamentos realizados, clientes atendidos, e todos outros dados vinculados à sua atividade comercial. O aceite do USUÁRIO ao presente Contrato desde já autoriza a INTELBRAS a indicar o USUÁRIO como parceiro da INTELBRAS e publicar os dados públicos de contato nos sites, softwares e demais mídias sociais da INTELBRAS, de acordo com a previsão do Manual do Programa de Canais e demais políticas definidas pela INTELBRAS e compartilhadas previamente com o USUÁRIO.

No desenvolvimento de quaisquer atividades relacionadas com a execução do presente Contrato, as Partes observam o regime legal de proteção de dados pessoais, empenhando-se em proceder a todo o tratamento de dados pessoais que venha a mostrar-se necessário ao desenvolvimento do Contrato no estrito e rigoroso cumprimento da Lei.

Os dados pessoais aqui elencados consideram-se os dados das próprias Partes ou mesmo os dados pessoais de seus colaboradores, contratados ou subcontratados.

A fim de garantir a proteção dos dados, o USUÁRIO obriga-se a:

- a. Tratar e usar os dados pessoais da INTELBRAS ou de seus PARCEIROS nos termos legalmente permitidos, em especial recolhendo, registrando, organizando, conservando, consultando ou transmitindo os mesmos, apenas e somente nos casos em que seu titular tenha dado o consentimento expresso e inequívoco, ou nos casos legalmente previstos;
- b. Tratar os dados de modo compatível com as finalidades para os quais tenha sido recolhidos;
- c. Conservar os dados apenas durante o período necessário à prossecução das finalidades da recolha ou do tratamento posterior, garantindo a sua confidencialidade;
- d. Implementar as medidas técnicas e organizativas necessárias para proteger os dados contra a destruição, acidental ou ilícita, a perda acidental, a alteração, a difusão ou o acesso não autorizada, bem como contra qualquer outra forma de tratamento ilícito dos mesmos;

e. Informar imediatamente a INTELBRAS, devendo prestar toda a colaboração necessária a qualquer investigação que venha a ser realizada, caso exista alguma quebra de segurança, ou suspeita da mesma, independentemente de colocar ou não em causa a segurança e integridade dos dados pessoais;

f. Garantir o exercício, pelos titulares, dos respectivos direitos de informação, acesso e oposição;

g. Assegurar que os seus colaboradores, contratados ou subcontratados que venham a ter acesso a dados pessoais no contexto deste Contrato cumpram as disposições legais aplicáveis em matéria de proteção de dados pessoais, e as disposições contratuais aqui elencadas, não cedendo, vendendo, compartilhando ou divulgando tais dados a terceiros, nem deles fazendo uso para quaisquer fins que não os estritamente consentidos pelos respectivos titulares.

O USUÁRIO será responsabilizado perante a INTELBRAS ou terceiros em caso de qualquer violação, compartilhamento, exclusão, cessão, venda, alteração automática dos dados sem prévio e expresse consentimento do seu titular.

8. Marcas Registradas e Direitos de Propriedade Intelectual da Intelbras

O USUÁRIO reconhece que as *Marcas Registradas* e os *Direitos de Propriedade Intelectual* da INTELBRAS representam um dos ativos estratégicos da INTELBRAS sendo de exclusiva propriedade da mesma.

Durante a vigência deste Termo, será concedido ao USUÁRIO o direito de uso não exclusivo das Marcas Registradas e outros Direitos de Propriedade Intelectual da INTELBRAS, sendo que o USUÁRIO deverá utilizá-los estritamente de acordo com o (i) “Manual da Marca Intelbras”; e (ii) quaisquer outras instruções recebidas da INTELBRAS. O LICENCIADO também garante que suas atividades de propaganda e promocionais cumpram com o (i) Manual da Marca Intelbras; (ii) Programa de Canais Intelbras; e (iii) e a legislação aplicável.

O USUÁRIO não poderá registrar quaisquer Direitos de Propriedade Intelectual da INTELBRAS, tais como qualquer palavra, símbolo, marca identificativa ou nome semelhante às Marcas Registradas da INTELBRAS ou nome de domínio durante a vigência deste contrato ou mesmo após o seu encerramento.

Todo e qualquer direito do USUÁRIO de utilizar as Marcas Registradas e outros Direitos de Propriedade Intelectual da INTELBRAS cessará automaticamente quando do encerramento do presente termo.

O USUÁRIO deverá prontamente notificar a INTELBRAS, por escrito, de qualquer suspeita de uso não autorizado ou infração aos Direitos de Propriedade Intelectual da INTELBRAS e que venha a ter conhecimento. Se solicitado pela INTELBRAS, o USUÁRIO deverá auxiliar a INTELBRAS em quaisquer investigações, negociações ou procedimentos judiciais em virtude de qualquer alegação de uso indevido ou de violação aos Direitos de Propriedade Intelectual da INTELBRAS.

O USUÁRIO compromete-se a não fazer qualquer tipo de anúncio, propaganda, material publicitário dos Produtos Intelbras, contemplando preços e condições de pagamento vinculando produtos INTELBRAS com produtos de concorrentes, devendo tais propagandas serem feitas de forma separada, sem vinculação de qualquer produto concorrente. A INTELBRAS recomenda que o USUÁRIO não faça mala direta constando preços dos produtos.

É vedada a cópia ou qualquer outra forma de reprodução das informações, manuais, literatura técnica e outros documentos fornecidos pela INTELBRAS, exceto para o cumprimento de obrigações estabelecidas nos termos deste instrumento, e de acordo com a legislação aplicável relativamente a direitos autorais e propriedade intelectual.

As obrigações estabelecidas na presente cláusula obrigam o USUÁRIO durante a vigência do presente instrumento, bem como após seu encerramento ou rescisão manutenção da confidencialidade.

9. Isenção de garantias e limitações de responsabilidade

Esse serviço estará em contínuo desenvolvimento e pode conter erros, por isso, o uso é fornecido *no estado em que se encontra* e sob risco do usuário final. Na extensão máxima permitida pela legislação aplicável, a INTELBRAS e seus fornecedores isentam-se de quaisquer garantias e condições expressas ou implícitas incluindo, sem limitação, garantias de comercialização, adequação a um propósito específico, titularidade e não violação no que diz respeito ao serviço e a qualquer um de seus componentes ou ainda à prestação ou não de serviços de suporte. A INTELBRAS não garante que a operação desse serviço seja contínua e sem defeitos. Com exceção do estabelecido neste documento, não há outras garantias, condições ou promessas vinculadas ao serviço, expressas ou implícitas, e todas essas garantias, condições e promessas podem ser excluídas de acordo com o que é permitido por lei sem prejuízo à Intelbras e a seus colaboradores.

I. A INTELBRAS não garante, declara ou assegura que o uso desse serviço será ininterrupto ou livre de erros e você concorda que a Intelbras poderá remover por períodos indefinidos ou cancelar esse serviço a qualquer momento sem que você seja avisado.

II. A INTELBRAS não garante, declara nem assegura que esse serviço esteja livre de perda, interrupção, ataque, vírus, interferência, pirataria ou outra ameaça à segurança e isenta-se de qualquer responsabilidade em relação a essas questões. Você é responsável pelo backup dos arquivos armazenados em seu dispositivo.

III. Em hipótese alguma a INTELBRAS, bem como seus diretores, executivos, funcionários, afiliadas, agentes, contratados ou licenciadores responsabilizar-se-ão por perdas ou danos causados pelo uso do serviço.

10. Validade técnica

Fica estipulado que a INTELBRAS, seus fornecedores ou distribuidores não oferecem um período de validade técnica do SOFTWARE. Não se pode considerar que o programa esteja isento de erros, que seu funcionamento seja ininterrupto ou que suas funções satisfaçam os requisitos dos usuários, razão pela qual fica expressamente estipulado que o licenciado o utiliza por sua conta e risco. Devido à complexidade da relação entre software e hardware, a INTELBRAS não garante que o SOFTWARE INTELBRAS INCONTROL WEB será compatível com todos os sistemas de software e hardware, que irá operar corretamente ou atender às suas expectativas.

11. Foro para dirimir controvérsias

Estes Termos de uso serão regidos e interpretados de acordo com as leis do Brasil. As partes se submetem à jurisdição exclusiva dos tribunais do Brasil. Para dirimir eventuais dúvidas acerca do presente instrumento, bem como de qualquer evento relacionado à utilização de nossos serviços, fica desde logo eleito o foro da comarca de São José, estado de Santa Catarina, por mais privilegiado que outro foro seja. Se você ainda possui alguma dúvida sobre a forma de utilização de nosso produto, sobre nossos Termos de uso ou sobre nossa Política de privacidade, entre em contato com a Intelbras. Ficaremos felizes com o seu contato.

intelbras

InControl Web Software

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

El software InControl Web es una plataforma de gerenciamiento y control de acceso para dispositivos controladores de acceso con comunicación TCP/IP fabricados por Intelbras en los modelos soportados por el software. Con él es posible seguir los logs de eventos de acceso en tiempo real por todas las pantallas y ventanas del software, efectuar registros de usuarios, credenciales de acceso, visitantes, así como sus respectivas reglas de acceso.

A través de una plataforma web interactiva, el operador posee opciones de adecuación de su ambientación para una experiencia más cómoda para cada perfil. Por ser un software versátil, es posible acceder a su plataforma de cualquier ambiente a través de los navegadores de internet Google Chrome® y Firefox® en red local, lo que hace con que las consultas y el gerenciamiento sean más ágiles.

Posee una Base de Datos robusta, con soporte para varias interacciones de registros con autonomía de hasta 80 dispositivos controladores de acceso. Para el acceso de su plataforma vía web es necesario que el sistema esté instalado en un servidor específico que hospedaré la aplicación y su respectiva base de datos, siendo posible acceder a su interfaz a través de la dirección de IP del servidor y de su puerta de comunicación en el cual el sistema está instalado o por el *Nombre del Servidor*. El software es compatible con el sistema operacional Windows®, en las versiones 7 y 10, así como sus derivaciones de estas versiones.

La composición de la solución InControl se muestra versátil también para desarrolladores aliados de Intelbras que cuentan con módulos disponibles para conexiones con sus propios softwares y aplicaciones de mercado, haciendo así con que Intelbras esté *Siempre Cerca*.

1. Instalación

La instalación de la solución en el servidor se debe hacer exclusivamente en Sistema Operacional Windows, en sus versiones 7 y 10.

1.1. Especificación del servidor

Especificación del servidor para hasta 20 dispositivos:

- » Procesador de 2 núcleos a 2.5 GHz
- » 2 Gb DDR RAM 3
- » 60 Gb HD

Especificación del servidor para hasta 40 dispositivos:

- » Procesador de 4 núcleos a 2.5 GHz
- » 4 Gb DDR RAM 3
- » 120 Gb SATA HD 3

Especificación del servidor para hasta 60 dispositivos:

- » Procesador de 8 núcleos a 2.5 GHz
- » 6 Gb DDR RAM 4
- » 180 Gb HD SATA 3

Especificación del servidor para hasta 80 dispositivos:

- » Procesador de 8 núcleos a 2.5 GHz
- » 8 Gb DDR RAM 4
- » SSD de 240 Gb HD

Obs.: las especificaciones del servidor son referentes al consumo de recursos por parte del sistema Incontrol. La máquina debe ser dimensionada considerando también las exigencias del hardware de los demás sistemas instalados en el servidor, además de los recursos del Incontrol, debe tener en cuenta los recursos del sistema operativo, software, antivirus y de backup, entre otros. Es altamente recomendado que el servidor sea una máquina dedicada para el control de acceso.

1.2. Especificación de la máquina cliente

A continuación se presentan las configuraciones necesarias para la máquina Cliente separadas por sistema operacional:

Windows 7 64 bits SP1

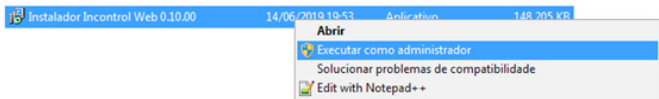
- » Procesador core I3;
- » Memoria RAM de 8 Gb;
- » HD 500 Gb;
- » Navegador Google Chrome®: Versión 75.0.3770.142 (oficial) 64 bits o superior;
- » Navegador Firefox®: Quantum, versión 66.0.3 (64 bits).

Windows 10 64 bits

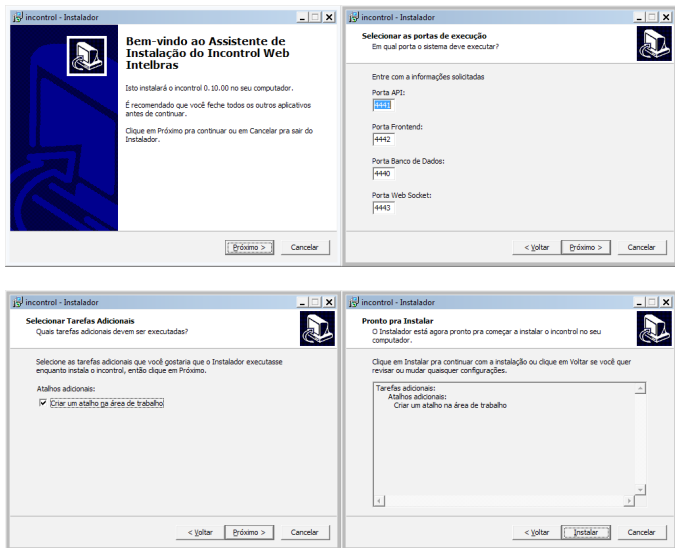
- » Procesador core I3;
- » Memoria RAM de 8GB;
- » HD 500 Gb;
- » Navegador Google Chrome®: Versión 75.0.3770.100 (oficial) 64 bits o superior;
- » Navegador Firefox®: Quantum, versión 68.0.3 (64 bits).

1.3. Proceso de instalación

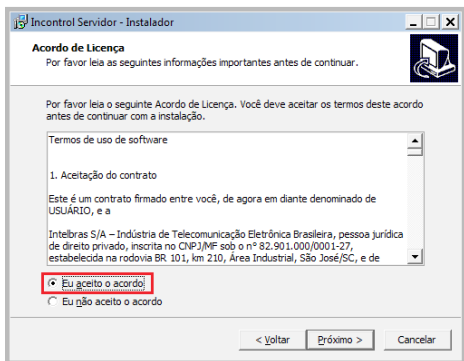
Tras efectuar el download del instalador del software en el sitio www.intelbras.com.br necesario descompactar el paquete y, en la secuencia, hacer un clic sobre el ícono de instalación con el botón derecho del mouse y seleccionar la opción *Ejecutar como Administrador*.



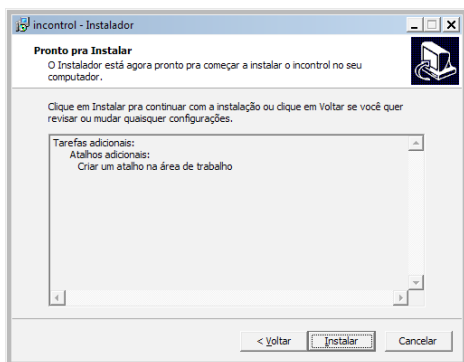
Una nueva ventana se abrirá y será necesario hacer un clic en el botón Próximo a medida que se solicite, para que se ejecute el proceso.



Importante: las puertas de comunicación ya vienen preconfiguradas como estándar de fábrica. Ellas son las comúnmente compatibles con el software y dispositivos. Recomendamos no cambiarlas.



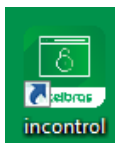
Lea los términos de uso y acéptelo para comenzar la instalación. Tras el término de la instalación, haga un clic en el botón *Cerrar* para cerrar el instalador.

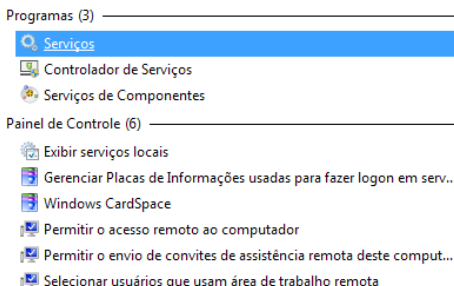


1.4. Verificando la instalación

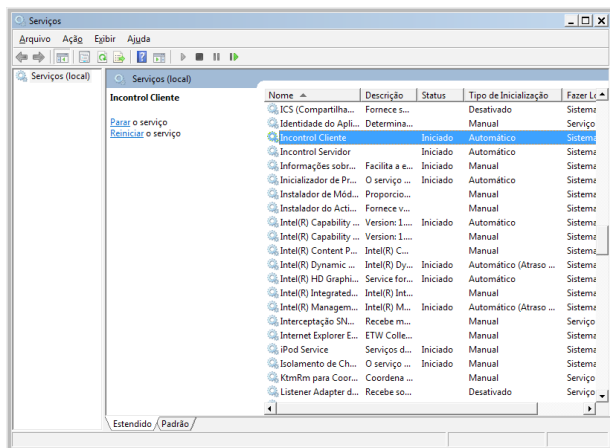
Verifique, tras la instalación, si se creó el ícono del software en el área de trabajo en la computadora.

Verifique si se creó el servicio del Windows® de nombre *InControl Service* y si él está en ejecución. Para eso, haga un clic en el botón *Iniciar*, en la barra de tareas del Windows®, y en el campo de investigación, inserte *Servicios*.



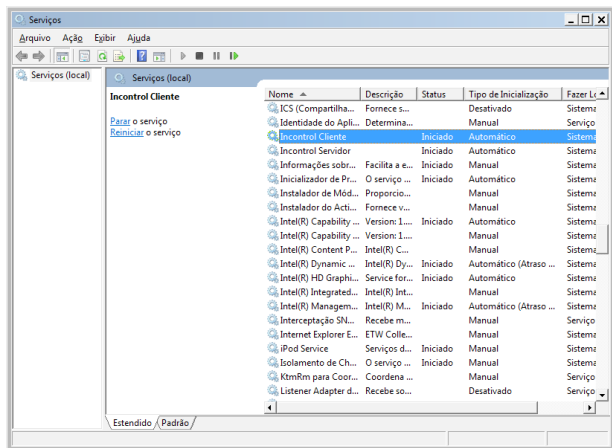


En la nueva ventana, verifique si se creó el servicio InControl servidor y si está en ejecución.



Importante: para que el software funcione correctamente es necesario que el servicio del software se esté ejecutando o iniciando.

Es posible identificar también si el servicio del registrador de mesa está instalado en la computadora. Servicio *Incontrol Cliente*.



Importante:

- » El servicio InControl Cliente sólo se instalará tras hacer el download del instalador en la pantalla de registro de credenciales del tipo Digital en Credenciales o durante el registro de Usuarios.
- » La desinstalación del software se debe hacer vía Panel de Control del Windows®, utilizando la función *Agregar/Remover programas*.

1.5. Limitaciones del software InControl

- » Número máximo de dispositivos: 80 dispositivos controladores de acceso (controladoras);
- » Número de máquinas cliente: 20 máquinas por servidor;
- » Cantidad de eventos por instancia de base de datos: 130 mil eventos por mes;
- » Límite de zonas de tiempo: 16 zonas de tiempo con hasta 3 períodos cada una.
- » Navegadores web: Chrome® y Firefox®;
- » Sistemas operacionales compatibles: Windows® 7 64 bits SP1 y Windows® 10 64 bits.
- » Base de datos compatible: PostgreSQL.

1.6. Primeros Pasos para aplicaciones en condominios residenciales

1. Efectúe el registro de las áreas del condominio donde se instalarán los dispositivos controladores de acceso (para obtener más informaciones consulte el capítulo *Áreas* de este manual).
2. Tras registrar las áreas del condominio, agregue los dispositivos de control de acceso, vinculando sus respectivas áreas registradas previamente (para obtener más informaciones consulte el capítulo *Dispositivos* de este manual).
3. Registre el Grupo de Puntos de acceso vinculando las zonas de tiempo necesarias y los dispositivos del sistema (para obtener más informaciones consulte el capítulo *Grupo de Puntos de Acceso* de este manual).
4. Con las áreas y dispositivos registrados, inserte los departamentos de su condominio, que pueden ser los bloques existentes, por ejemplo (para obtener más informaciones consulte el capítulo *Departamentos* de este manual).
5. Registre los usuarios que tendrán acceso a los dispositivos de control, vinculándolos a los departamentos registrados (para obtener más informaciones consulte la sección *Usuarios* de este manual).
6. Registre también los perfiles de operadores del sistema o cree nuevos, concediendo acceso a distintas secciones del software según su necesidad (para obtener más informaciones consulte el capítulo *Perfil de Operadores* de este manual).
7. Por fin, registre los demás operadores del sistema con login y clave distinta del operador Admin. (para obtener más informaciones consulte el capítulo *Operadores* de este manual).

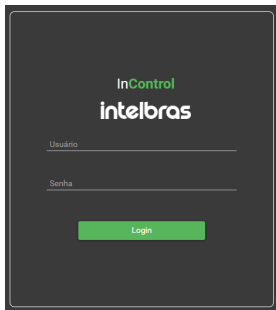
1.7. Primeros Pasos para organizaciones o empresas

1. Efectúe el registro de las áreas de la empresa donde se instalarán los dispositivos controladores de acceso (para obtener más informaciones consulte el capítulo *Áreas* de este manual).
2. Tras registrar las áreas de la empresa, agregue los dispositivos de control de acceso, vinculando sus respectivas áreas registradas previamente (para obtener más informaciones consulte el capítulo *Dispositivos* de este manual).
3. Registre el Grupo de Puntos de acceso vinculando las zonas de tiempo necesarias y los dispositivos del sistema (para obtener más informaciones consulte el capítulo *Grupo de Puntos de Acceso* de este manual).
4. Con las áreas y dispositivos registrados, inserte los departamentos de su empresa, que serán los sectores existentes en ella (para obtener más informaciones consulte el capítulo *Departamentos* de este manual).
5. Registre los usuarios que tendrán acceso a los dispositivos de control, vinculándolos a los departamentos registrados (para obtener más informaciones consulte la sección *Usuarios* de este manual).
6. Registre también los perfiles de operadores del sistema o cree nuevos, concediendo acceso a distintas secciones del software según su necesidad (para obtener más informaciones consulte el capítulo *Perfil de Operadores* de este manual).
7. Por fin, registre los demás operadores del sistema con login y clave distinta del operador Admin. (para obtener más informaciones consulte el capítulo *Operadores* de este manual).

2. Ambientación

2.1. Login

Para acceder a la plataforma vía navegador web, haga un doble clic en el atajo del software creado en el área de trabajo del servidor. Tras acceder a la interfaz vía navegador de internet, el operador es dirigido hacia una pantalla de login donde deberá insertar sus credenciales y clave para acceder a las funciones del software.



El estándar de fábrica de usuario y clave es:

- » **Usuario:** admin
- » **Clave:** admin

Importante: recomendamos que tras el primer login se modifique el estándar de credenciales de fábrica para informaciones que no sean de conocimiento común.

2.2. Pantalla Inicial

Tras el login en el software, el operador será dirigido hacia la pantalla inicial del software.

En esta pantalla se puede acceder a todas las funciones a través del Menú lateral.

En la barra superior están disponibles las funciones relativas al perfil del operador, tema del software, traducción del software, etc.

En la pantalla inicial están representados el Panel de Control con datos relativos al sistema de control de acceso, tales como accesos generados, número de usuarios, número de dispositivos, etc.

En la barra lateral derecha está disponible un *Log de Eventos* que exhibe todos los últimos accesos o intentos de accesos a medida que se generan.



Barra de funcionalidades

La barra de funcionalidades le proporciona al operador del software navegar por todas las funcionalidades del sistema de control de acceso de tal forma que al hacer un clic en los títulos, sus subsecciones se ponen a disposición para la navegación. Como se demuestra en la figura siguiente:



A medida que se exhiben las subsecciones, los títulos de las secciones subsecuentes se desplazan para abajo en la ventana del navegador web.

Importante: recomendamos que tras el término de las configuraciones de una sección ella se cierre antes de la abertura de la próxima, para garantizar la visualización de las sub-opciones de las funcionalidades *macro* que están localizadas en la parte inferior de la Barra de Funcionalidades.

2.3. Panel de control

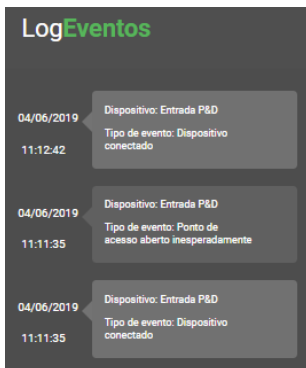
En el panel de control se exhiben datos estadísticos del sistema de control de acceso como un todo. Esta sección forma parte de la pantalla inicial del sistema y en ella el operador puede tener algunas informaciones gerenciales de forma más dinámica e inmediata. En esta sección se exhiben los siguientes datos:

- » Cantidad de visitas en la semana: demuestra día a día cuantas visitas hubo;
- » Cantidad de accesos en la semana: demuestra día a día cuantos accesos hubo;
- » Cantidad de biometrías X Capacidad por dispositivo: Le ilustra al operador el número de credenciales biométricas que ya están registradas en el dispositivo y cuál es el espacio que todavía está disponible.
- » Cantidad de credenciales RFID X Capacidad del dispositivo: le ilustra al operador el número de credenciales RFID que ya están registradas en el dispositivo y cuál es el espacio que todavía está disponible.



2.4. Log de eventos

En la pestaña lateral del sistema está localizada la barra de Log de Eventos. En ella se exhiben los últimos eventos de acceso que suceden durante la operación del sistema.



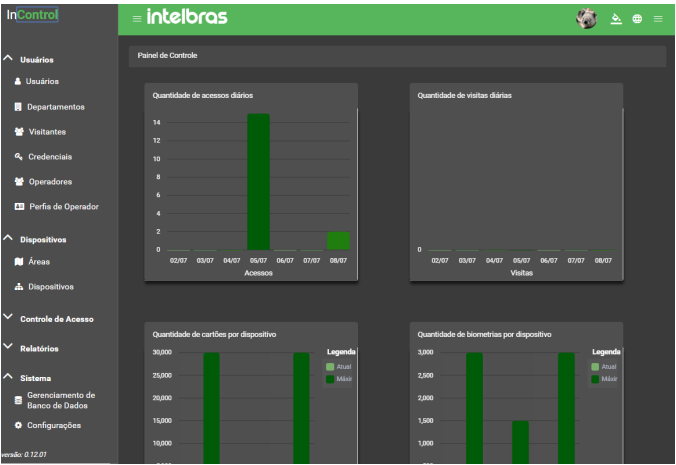
2.5. Perfil

En la parte superior de la pantalla del software están disponible las opciones de personalización en las cuestiones de visualización y de perfil del operador. Al lado del logo *Intelbras* es posible visualizar un ícono de 3 trazos que, cuando se acciona, posibilita una expansión de la pantalla hacia el lado izquierdo, ocultando la barra lateral de funcionalidades.

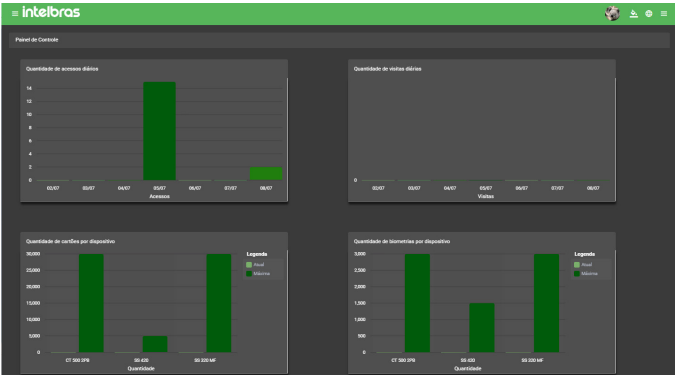


La visualización estándar de la pantalla inicial es semejante a la imagen siguiente:

Tras el accionamiento de este botón, la pantalla se expande hacia el lado derecho, con la siguiente representación:



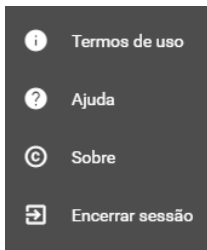
Por fin, con ambos botones accionados, la pantalla inicial ocupa toda la extensión de la pantalla de exhibición.



En la barra superior es posible seleccionar algunas opciones referentes al perfil del operador del sistema. Este botón está representado por el ícono descrito en la figura siguiente:

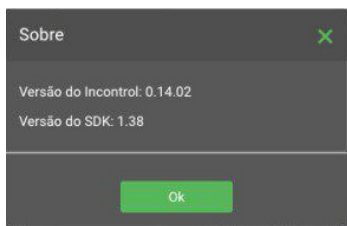


Haciendo un clic sobre el botón referente al perfil del operador del sistema se exhibirán las opciones para consulta y acceso: Términos de uso, manual del software (Ayuda), informaciones referentes a la versión del software instalada (Sobre) y la opción de salir del software (Cerrar sesión).

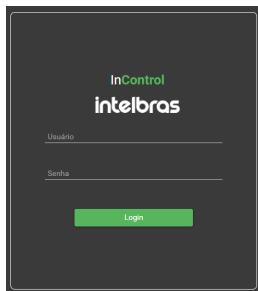


Haciendo un clic sobre el botón Ayuda es posible hacer el download del manual del usuario del software, del documento de Términos de uso del software InControl y de la Política de privacidad del software inControl.

Haciendo un clic sobre el botón Sobre se le exhibirá al operador una nueva ventana que exhibe las informaciones sobre el paquete de instalación del software InControl.



Haciendo un clic sobre el botón *Cerrar sesión* el operador cierra su sesión en el software y vuelve a la pantalla de Login.



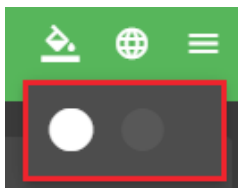
Importante: de vuelta a la pantalla del login del software, será necesario insertar las credenciales de acceso del operador del sistema nuevamente para tener acceso a las funciones del sistema.

2.6. Color de Fondo

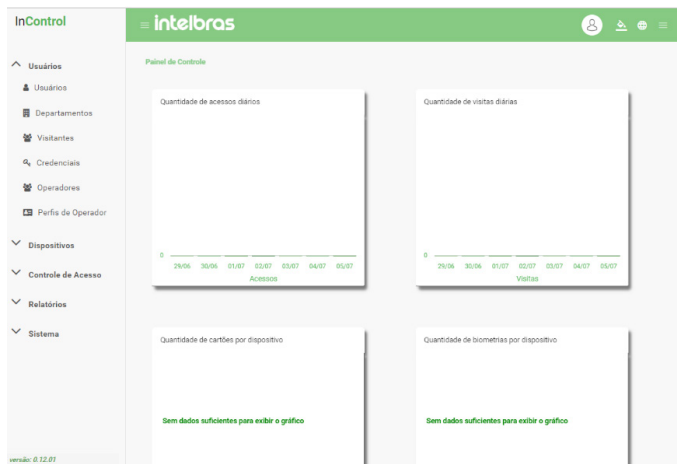
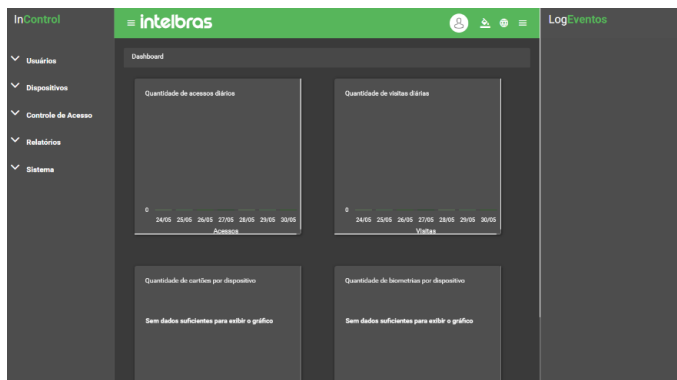
En la barra superior del software es posible accionar el botón de modificación del color de fondo del software InControl. Esta función le da al operador la opción de dos colores de fondo para visualización de los Íconos en todas las demás pantallas del software. Las opciones son:

- » Negro: (Opción estándar del software);
- » Blanco.

Para seleccionar una u otra opción basta hacer un clic sobre el ícono en la barra superior, ilustrado a continuación, y, en la nueva ventana que abrirá, elegir la que el operador del sistema prefiera.



A continuación está representada la pantalla inicial del software en el color estándar y en el color blanco.



2.7. Lenguaje

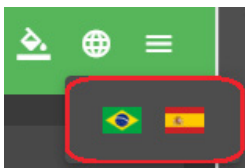
El software InControl le trae al operador algunas opciones de traducción de lenguaje. Ellas son:

- » Portugués (Brasileño);
- » Español.

El lenguaje estándar del software es el Portugués brasileño. Para cambiar este idioma basta hacer un clic sobre el botón de lenguaje localizado en la barra superior del software.



En la nueva ventana, elija la opción de lenguaje para que se traduzcan las pantallas.



La pantalla del software traducida al lenguaje seleccionado se exhibe a continuación:

Usuarios

Añadir Editar Borrar Importación Exportación

Selecciona el campo +

No se aplican filtros

Mostrando 13 columna(s)

Nombre de usuario	E-mail	RG	CPF	Teléfono Celular	Matrícula	Estado	Fecha de Validez Inicial	Fecha de Validez Final	Nota	Tipo de usuario	Grupo de Acceso	Departamento
Scarlet						Activo	16-07-2019	16-07-2099		Normal	Total	Colaborador
Rafael						Activo	16-07-2019	16-07-2099		Normal	Total	Colaborador

Navigation: < < 1 > >

Buscadores Soportados: [iconos]

InControl - Intelbras S/A todos os direitos reservados.

LogEventos

- 16/07/2019 Autor: Scarlet Dispositivo: 99-430 Tipo de evento: Acceso Normal ✓
- 16/07/2019 Autor: João Dispositivo: 99-430 Tipo de evento: Acceso Normal ✓
- 16/07/2019 Autor: João Dispositivo: 01 368 376 Tipo de evento: Acceso Normal ✓
- 16/07/2019 Autor: João Dispositivo: 99-430 Tipo de evento: Acceso Normal ✓
- 16/07/2019 Autor: João Dispositivo: 99-430 Tipo de evento: Acceso Normal ✓
- 16/07/2019 Autor: João Dispositivo: 99-430 Tipo de evento: Acceso Normal ✓
- 16/07/2019 Autor: João Dispositivo: 99-430 Tipo de evento: Acceso Normal ✓
- 16/07/2019 Autor: João Dispositivo: 99-430 Tipo de evento: Acceso Normal ✓

versão: 0.16.00

Importante: cuando se seleccione la opción de lenguaje español, el archivo del manual que estará disponible en la función Ayuda también será la versión traducida al español.

3. Usuarios

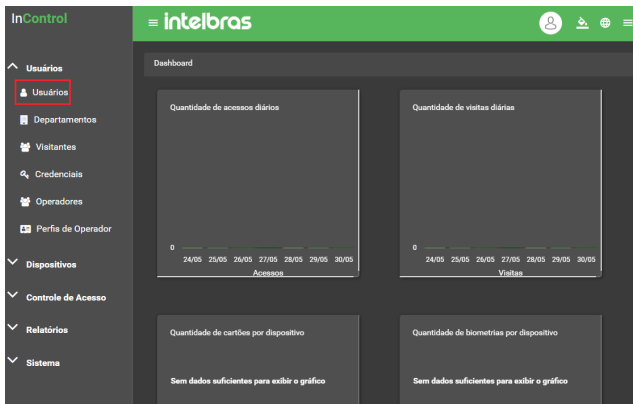
La sección *Usuarios* le ofrece al operador todas las subsecciones que están conectadas al perfil del usuario del sistema de control de acceso. Las opciones registradas en estas secciones se enviarán directamente a los dispositivos controladores de acceso que formen parte del sistema.

A continuación está detallada cada subsección de la sección Usuarios, sin embargo, el registro de uno o más perfiles puede variar de acuerdo con la preferencia del operador del sistema. Es decir, hay subsecciones en que el software ya trae opciones estándar de fábrica para que se vinculen al registro del usuario posteriormente. La edición de las funciones estándar del software o el registro de nuevos sub-perfiles queda a cargo del operador del sistema de control de acceso.

En esta sección también hay una subsección que le permite al operador administrador del sistema crear nuevos perfiles de operadores del sistema con permisos distintos para necesidades específicas del software durante la operación.

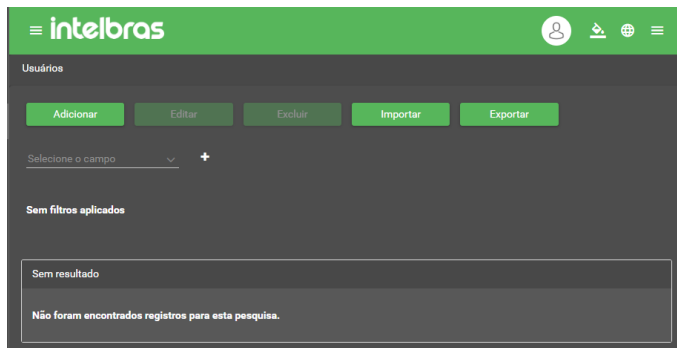
3.1. Registro de usuarios

La subsección Usuarios está en la barra de funciones del software, localizada en la barra lateral izquierda del software, y posibilita el registro de nuevos usuarios. Vea la representación de su localización en la figura siguiente:

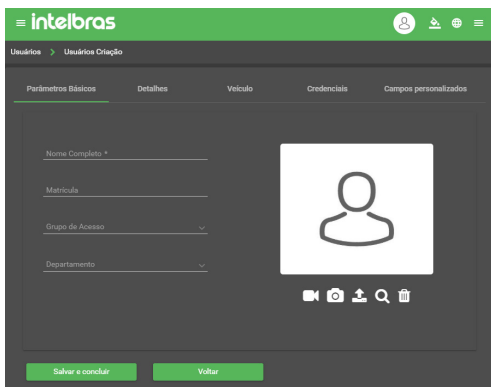


Al seleccionar la subsección Usuarios se abrirá una nueva ventana, permitiéndole al operador navegar por las “pestañas” del registro de usuario, insertando la información que compondrá el registro de usuario.

En la nueva pantalla de registro de usuarios se exhibe la lista de todos los usuarios presentes en el sistema. En esta pantalla el operador podrá Agregar, Editar, Excluir, Importar o Exportar la lista de usuarios del sistema.



Al hacer un clic en *Agregar* se abrirá una nueva ventana conteniendo todas las pestañas necesarias para el registro del usuario.



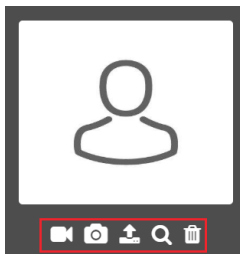
En la pestaña *Parámetros Básicos* inserte los datos:

- » Nombre completo;
- » Matrícula;
- » Grupo de acceso en que el usuario participará;
- » El departamento al cual el usuario pertenece;
- » Foto del perfil del usuario;

Es posible registrar la foto del usuario de algunas formas distintas. Ellas son:

- » Captura de la imagen utilizando una cámara de seguridad IP Intelbras del sistema de CFTV local;
- » Captura de imagen utilizando una webcam;
- » Upload de archivo de imagen directamente de la computadora.

Es posible también excluir una imagen previa que por acaso ya esté vinculada.



Importante: es posible ampliar la imagen capturada haciendo un clic sobre ella en la pestaña de *Parámetros Básicos*.

En la pestaña *Detalles* es posible definir las siguientes características para el registro de usuarios:

- » Tipo de usuario: normal o tercerizado;
- » Fecha de validez: fecha inicial y fecha final;
- » CPF: apenas números;
- » CI: números y letras;
- » Celular: número de teléfono celular;
- » E-mail: dirección electrónica de e-mail;
- » Observaciones: caracteres en general.
- » Casilla de verificación activa: siempre marcado por estándar. En caso que se desmarque, el usuario no podrá acceder a los dispositivos del sistema de control de acceso.

The screenshot shows the Intelbras web interface for user management. The top navigation bar is green with the Intelbras logo and icons for user profile, settings, and a menu. The breadcrumb trail indicates the path: 'Usuários > Usuários Criação'. Below this, there are five tabs: 'Parâmetros Básicos', 'Detalhes' (which is selected), 'Veículo', 'Credenciais', and 'Campos personalizados'. The 'Detalhes' tab contains a form with the following fields:

- Tipo de usuário:** A dropdown menu with 'Normal' selected.
- Data Inicial de Validade:** A date field with '30/05/2019' entered.
- Data Final de Validade:** A date field with '30/05/2099' entered.
- CPF:** An empty text field.
- RG:** An empty text field.
- Celular:** An empty text field.
- E-mail:** An empty text field.
- Observações:** An empty text area.
- Ativo:** A checkbox that is checked, with the label 'Ativo' next to it.

At the bottom of the form, there are two green buttons: 'Salvar e concluir' and 'Voltar'.

En la pestaña *Veículo* es posible registrar los datos del vehículo del usuario en caso que él acceda a las dependencias controladas por el sistema de control de acceso. Las informaciones pasibles de registro son:

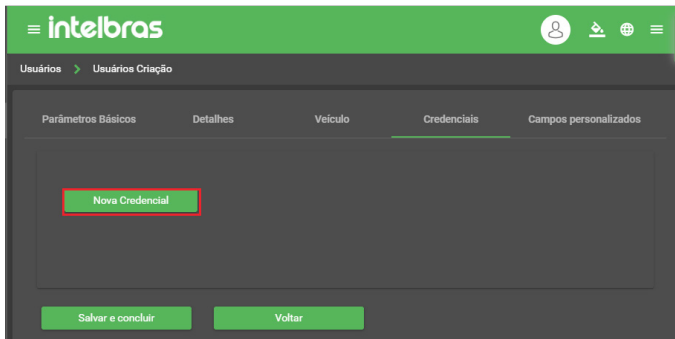
- » Letras de la chapa;
- » Número de la chapa;
- » Color del vehículo;
- » Marca;
- » Modelo del vehículo;
- » Foto.

Importante:

- » Los métodos de captura de imagen para el vehículo son exactamente los mismos que los métodos para captura de imagen del usuario.
- » Es posible ampliar la imagen capturada haciendo un clic sobre ella en la pestaña de *Veículo*.

Al hacer clic en *Nueva credencial*, en caso que el operador del sistema todavía no haya guardado el registro del usuario, se exhibirá una ventana con la opción de guardar el registro efectuado hasta entonces para el posterior vínculo de las credenciales. Haga un clic en el botón Ok en caso que ya haya llenado todas las informaciones anteriores.

En la pestaña *Credenciais*, haga un clic en el botón Nueva Credencial para abrir el registro de credenciales.



En la nueva ventana es posible registrar algunos tipos de credenciales para el usuario. Ellas son:

- » Nivel de la credencial: credencial de usuario normal o de terceros;
- » Tipo de la credencial:
- » Tarjeta (RFID);
- » Digital (biometría) 10 por usuario;
- » Clave (numérica);
- » Tag UHF (tag vehicular).

Importante: excepto la credencial del tipo Digital, el resto de los tipos de credencial de usuarios (clave, tarjeta y tag UHF) no posee límite de registro por usuario definido por software. Esta definición se limita a la capacidad del dispositivo controlador de acceso que el usuario tendrá acceso. Por ejemplo:

Un dispositivo que posea capacidad para almacenar 30.000 usuarios con tarjeta y clave tendrá su capacidad reducida a medida que se registren más tarjetas, tags UHF o claves para un mismo usuario. Entonces, considerando un escenario en que tenemos un dispositivo con capacidad de 30.000 usuario con tarjeta y clave y apenas dos usuarios registrados en el sistema, podemos registrar 15.000 tarjetas, tags UHF o claves para cada usuario, lo que totalizará la capacidad de 30.000 usuarios del dispositivo.

Cada tipo de credencial elegida pone a disposición opciones distintas para el operador en el registro del usuario.

- » Tipo credencial tarjeta: en este tipo de credencial se exhibe una previsualización de la credencial en la pantalla y el operador puede registrar de algunas formas la clave de la credencial:
 - » Manualmente: digitando el código en hexadecimal, o decimal, así como el estándar de lectura (26 bits o 34 bits).
 - » Vía lector RFID de la puerta: automáticamente acercando la tarjeta RFID al lector esclavo o dispositivo fijado en la puerta del ambiente.
 - » Vía registrador de mesa: automáticamente acercando la tarjeta RFID al registrador de mesa para el llenado de la clave.

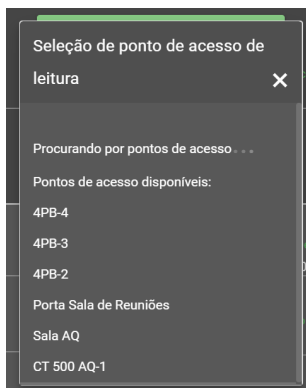
Tras el registro de la credencial tipo tarjeta RFID, las informaciones insertadas estarán representadas en la ilustración de la tarjeta en la pantalla.

The screenshot shows the Intelbras web interface for credential registration. At the top is a green header with the Intelbras logo and navigation icons. Below the header is a large white box displaying the URL www.intelbras.com.br. The main content area has a dark gray background and is titled "Selecione o modo de captura" (Select the capture mode). There are two green buttons: "Captura local" (Local capture) and "Captura remota" (Remote capture). Below these are two dropdown menus: "Nível da credencial" (Credential level) set to "Normal" and "Tipo de credencial" (Credential type) set to "Cartão" (Card). There is also a text input field for "Nome do usuário" (User name) with a clear button (X) and a dropdown arrow. A section titled "Detalhes da credencial" (Credential details) contains two text input fields for "Código Hexa" (Hex code) and "Código Decimal" (Decimal code), a text input field for "Observação" (Observation), and a dropdown menu for "Tamanho" (Size) set to "26 bits". There is also a checkbox for "Coação" (Coercion). At the bottom is a green button labeled "Salvar credencial" (Save credential).

Registro de credencial tipo *Tarjeta vía dispositivo*

Para registrar una credencial del tipo tarjeta vía dispositivo, en la pantalla principal de la credencial tarjeta, haga un clic en el botón *Vía dispositivo* y, en la nueva ventana, seleccione uno de los dispositivos disponibles para efectuar la captura.

The screenshot shows a software window titled "Selecione o modo de captura" (Select the capture mode). Below the title is a button "Reiniciar processo" (Restart process). A placeholder for a credential image is shown with the text "H: E1027851 D: 18605050705 www.intelbras.com.br". Below this are two buttons: "Via cadastrador" (highlighted in green) and "Via dispositivo" (highlighted with a red rectangle). Under "Via cadastrador", there is a dropdown for "Nível da credencial" (Normal) and a checkbox for "Administrador". Under "Via dispositivo", there is a dropdown for "Tipo de credencial" (Cartão). Below these are fields for "Código Hexa", "Código Decimal", "Observação", and "Tamanho" (34 bits).



Tras la selección del dispositivo, acerque la tarjeta a él y vea la captura de la credencial demostrada en la pantalla del software.

Selecione o ponto de acesso
← Reiniciar processo


 N: E6575B51 D: 3865000785
 www.intelbras.com.br

Pontos de acesso

Nível de credencial *

Normal

☐ Administrador

Tipo de credencial *

Cartão

Detalhes da credencial

Código Nova *

e6593b51

Código Resenha *

3865000785

Observação

Arquiteto *

34 bits

Importante: seleccione el estándar de lectura de 34 bits o 26bits antes de efectuar la captura de la credencial del tipo tarjeta.

Consulte el manual del dispositivo y de la tag utilizada. Haga un clic en *Guardar Credencial* y vea la representación de la misma en la lista de credenciales vinculadas al usuario.

Credenciais do usuário

Tipo de credencial

M. 1
No. 2


M. 1
No. 1


M. 1
7738011570


M. 1
Resenha


Nova Credencial

Salvar e concluir

Voltar

Haga un clic en el botón Guardar y concluir para finalizar la operación.

Registro de credencial de tipo Tarjeta vía Registrador de mesa

Para capturar una credencial del tipo tarjeta vía registrador de mesa, seleccione la opción *Vía registrador* en la pantalla principal de la credencial del tipo tarjeta.

The screenshot displays a software interface for credential registration. At the top, the title is 'Selecione o modo de captura' with a back arrow and 'Reiniciar processo'. Below this is a 'Pré visualização da credencial' section showing a placeholder for a credential card with the URL 'www.intelbras.com.br'. Two green buttons are present: 'Via cadastrador' (highlighted with a red rectangle) and 'Via dispositivo'. Below these are two dropdown menus: 'Nível de credencial *' set to 'Normal' and 'Tipo de credencial *' set to 'Cartão'. There is an unchecked checkbox for 'Administrador'. The bottom section, 'Detalhes da credencial', contains four input fields: 'Código Hexa', 'Código Decimal *', 'Observação', and 'Tamanho *' (set to '34 bits').

Posicione el cursor sobre el campo *Código Decimal* y acerque la tarjeta del registrador de mesa para que se capture la credencial.

Para finalizar el proceso, haga un clic en *Guardar y concluir*.

Importante: seleccione el estándar de lectura de 34 bits o 26 bits antes de efectuar la captura de la credencial del tipo tarjeta. Consulte el manual del dispositivo y de la tag utilizada.

- » **Tipo credencial digital:** en este tipo de credencial se exhibe una representación de dos manos del usuario para la selección del dedo que se registrará. El registro de la digital se podrá hacer vía registrador de mesa o a través del dispositivo controlador de acceso.

The screenshot shows the Intelbras web interface for user management. The top navigation bar is green with the Intelbras logo and a user profile icon. Below it, a breadcrumb trail shows 'Usuários > Usuários Edição'. A horizontal menu contains 'Parâmetros Básicos', 'Detalhes', 'Valores', 'Credenciais', and 'Campos personalizados', with 'Credenciais' being the active tab. The main content area is titled 'Cadastro de nova credencial'. It features a large box for 'Pré visualização da credencial' showing two hands with fingers labeled 'I' and 'D'. Below this is a 'Seleção o modo de captura' section with two buttons: 'Captura local' and 'Captura remota'. Under 'Captura local', there is a 'Modo de credencial' dropdown set to 'Normal'. Under 'Captura remota', there is a 'Modo de credencial' dropdown set to 'Digital'. A 'Detalhes da credencial' section contains a 'Documento' input field and a 'Geração' checkbox. At the bottom are two buttons: 'Salvar credencial' (green) and 'Cancelar' (red).

Importante: verifique si entre las funciones del dispositivo controlador de acceso hay compatibilidad para el registro de la biometría remotamente.

Captura vía dispositivo de acceso

En la ventana de credenciales del tipo *Digital*, marque la opción Vía dispositivo y vea en la nueva ventana los dispositivos previamente agregados al sistema que hacen posible la captura de la digital del usuario a través del software.

Seleção de modo de captura

Pré-visualização da credencial

Via cadastrador Via dispositivo

Nível de credencial *
Normal

Tipo de credencial *
Digital

☐ Administrador

Detalhes da credencial

Biometria

☐ Coeção

Seleção de ponto de acesso de leitura

Procurando por pontos de acesso...

Pontos de acesso disponíveis:

SS 420-1

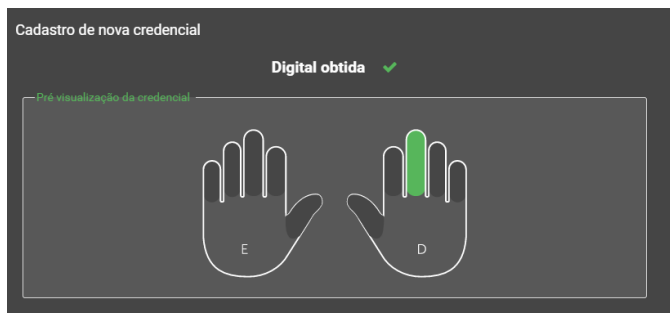
Importante:

- » Los dispositivos disponibles en la ventana de *Selección de punto de acceso de lectura* pueden variar de acuerdo con los dispositivos agregados en el sistema.
- » Apenas dispositivos de protocolo STD SDK poseen la función de captura de biometría digital vía software.

Tras la selección del dispositivo para captura, seleccione el dedo que desea registrar en la representación gráfica del software y haga 3 lecturas consecutivas en el dispositivo instalado.



Tras efectuar las 3 lecturas en el dispositivo, verifique si el dedo seleccionado cambió su color de azul a verde. Finalmente, haga un clic en el botón de *Guardar Credencial* para volver a la pantalla principal de la lista de credenciales del usuario.



Pontos de acesso

Nível da credencial *
Normal

Tipo de credencial *
Digital

Escutando o ponto de acesso
SS 420-1

Detalhes da credencial

Biometria
TGFTUzlxAAAFiiMECAUHCc7QAAAç

☐ Coação

Salvar credencial Cancelar

En caso que desee utilizar la digital registrada como una digital de coacción, marque la caja de opción *Coacción* en la pantalla de digital antes de guardarla.

Pontos de acesso

Nível da credencial *
Normal

Tipo de credencial *
Digital

Escutando o ponto de acesso
SS 420-1

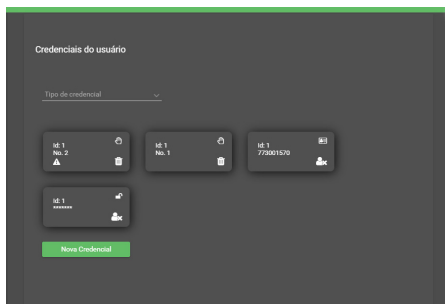
Detalhes da credencial

Biometria
TGFTUzlxAAAFiiMECAUHCc7QAAAç

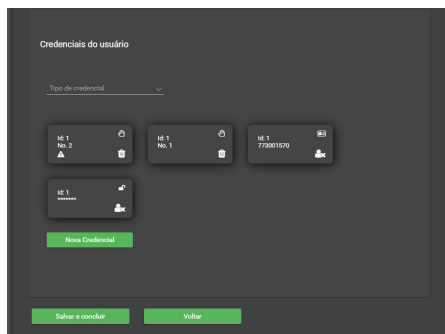
☒ Coação

Salvar credencial Cancelar

Finalmente, vea la credencial registrada en la lista de credenciales vinculadas al usuario.

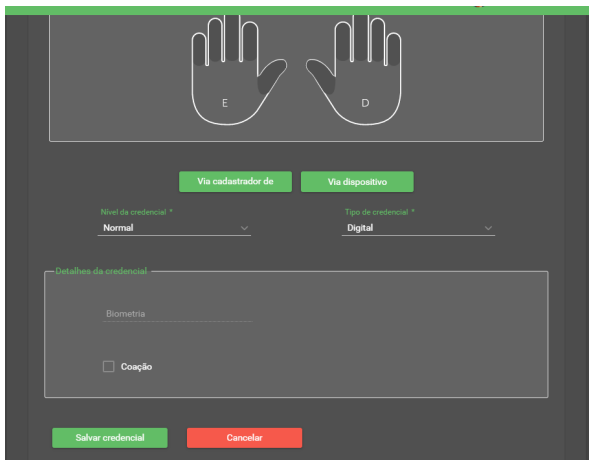


Para finalizar el proceso, haga un clic en la opción *Guardar y Concluir* y vuelva a la pantalla principal de usuarios.



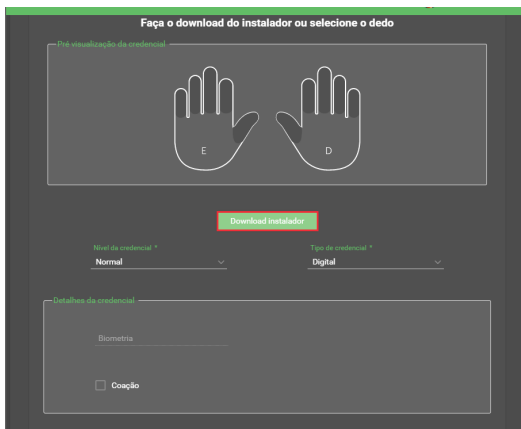
Captura vía registrador de mesa

Para efectuar la captura de una digital vía registrador de mesa, en la pantalla principal de credencial de tipo digital, seleccione la opción *Via Registrador de Mesa*.

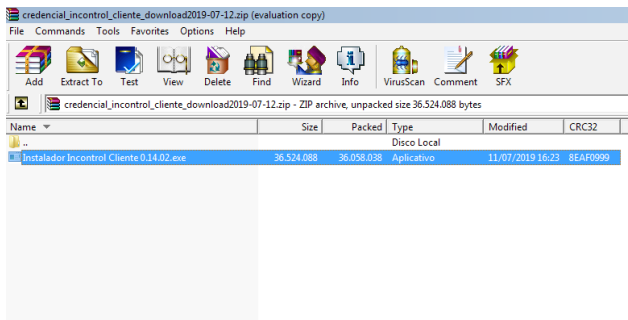


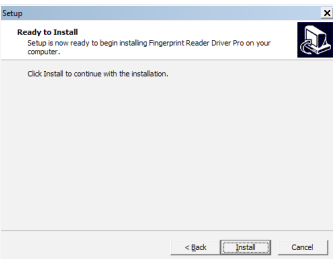
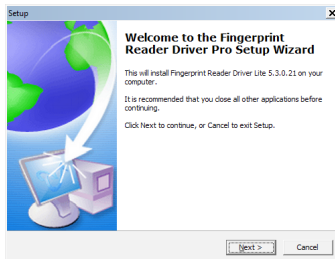
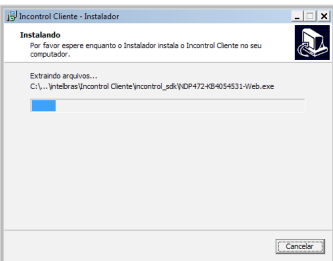
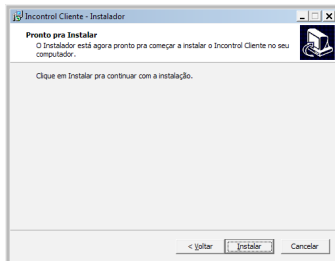
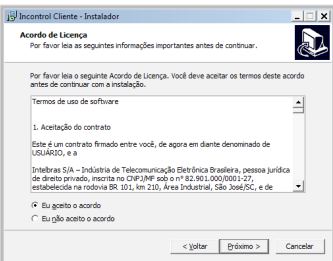
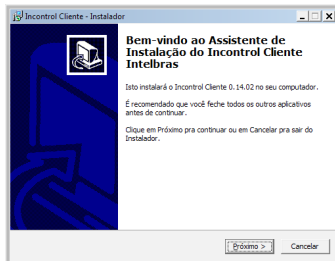
The screenshot shows a web interface for capturing a digital credential. At the top, there are two hand icons labeled 'E' and 'D'. Below them are two green buttons: 'Via cadastrador de' and 'Via dispositivo'. Under these buttons are two dropdown menus: 'Nível de credencial *' with 'Normal' selected, and 'Tipo de credencial *' with 'Digital' selected. Below these is a section titled 'Detalhes da credencial' containing a 'Biometria' label and a checkbox labeled 'Coação'. At the bottom are two buttons: 'Salvar credencial' (green) and 'Cancelar' (red).

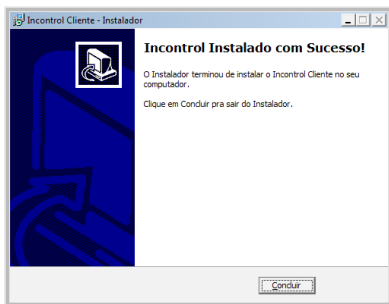
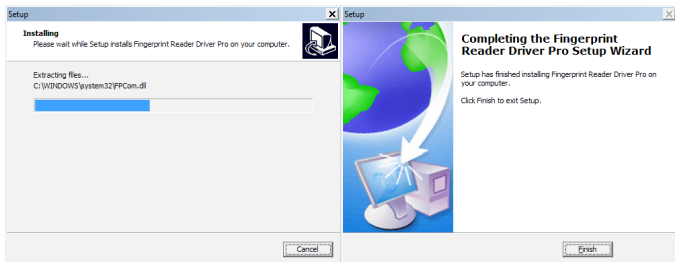
En caso que esté utilizando el registrador de mesa por primera vez, es necesario instalar el software de comunicación con el registrador de mesa. Haga un clic en el botón *Download instalador* y siga el proceso en la ventana del navegador de la web.



Tras el download del archivo de instalación del registrador de mesa, haga un doble clic en el archivo compactado y en la nueva carpeta, haga un clic dos veces sobre el archivo de instalación.



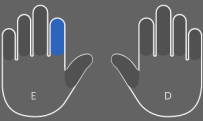




Haga la lectura de los términos de uso del servicio y haga un clic en el checkbox de aceptación de los mismos para seguir con la instalación. Tras hacer un clic en el botón *Concluir*, vuelva a la pantalla de registros de digital del usuario en el software InControl y seleccione el dedo deseado para el registro en la representación gráfica del software.

Coloque o dedo no leitor

Pré visualização da credencial



Download instalador

Nível da credencial *
Normal

Tipo de credencial *
Digital

Detalhes da credencial

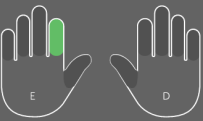
Biometria

☐ Coação

Efectúe las 3 lecturas consecutivas de la digital en el registrador de mesa y verifique si el color del dedo seleccionando cambió de azul a verde.

Digital obtida ✓

Pré visualização da credencial



Download instalador

Nível da credencial *
Normal

Tipo de credencial *
Digital

Detalhes da credencial

Biometria
TFNTUjlyAAAFEBQFBQUHCc7QAAA/

☐ Coação

En caso que desee utilizar la digital registrada como una credencial de coacción, marque la caja de opción *Coacción* en la pantalla de digital antes de guardarla.

Importante: apenas credenciales del tipo digital se pueden caracterizar como *Coacción*.

Pontos de acesso

Nível da credencial *
Normal

Tipo de credencial *
Digital

Escutando o ponto de acesso
SS 420-1

Detalhes da credencial

Biometria
TGFTUzixAAAF8IMECAU8HCg7QAAA...

☒ Coação

Salvar credencial Cancelar

Finalmente, vea la credencial registrada en la lista de credenciales vinculadas al usuario.

Credenciais do usuário

Tipo de credencial

Id: 1
No. 2

Id: 1
No. 1

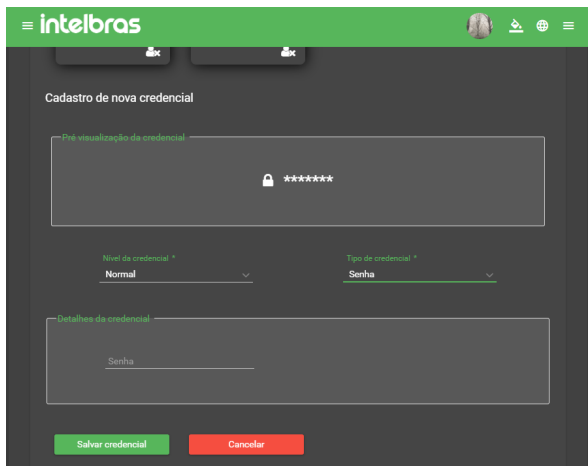
Id: 1
773001570

Id: 1
[Masked]

Nova Credencial

Para finalizar el proceso, haga un clic en la opción Guardar y Concluir y vuelva a la pantalla principal de usuarios.

- » **Tipo de credencial clave:** en este tipo de credencial es necesario atribuir una clave numérica de 4 a 6 dígitos.



The screenshot shows the 'Cadastro de nova credencial' (New Credential Registration) screen in the Intelbras system. The interface has a green header with the Intelbras logo and navigation icons. The main content area is dark gray and contains the following elements:

- Cadastro de nova credencial**: The title of the form.
- Pré visualização da credencial**: A section for previewing the credential, showing a lock icon and the text '*****'.
- Nível da credencial ***: A dropdown menu currently set to 'Normal'.
- Tipo de credencial ***: A dropdown menu currently set to 'Senha' (Password).
- Detalhes da credencial**: A section for entering details, with a 'Senha' (Password) input field.
- Buttons**: Two buttons at the bottom: 'Salvar credencial' (Save credential) in green and 'Cancelar' (Cancel) in red.

- » **Tipo de credencial tag UHF:** en este modelo de credencial el operador podrá insertar la clave de la tag vehicular UHF en Hexadecimal o en decimal; también deberá seleccionar el estándar de lectura de las tags en 26 bits o 34 bits.

The screenshot shows the 'Cadastro de nova credencial' (New Credential Registration) screen in the Intelbras system. The interface is in Portuguese and features a green header with the Intelbras logo and navigation icons. The main content area is titled 'Selecione o modo de captura' (Select the capture mode). It includes a 'Pré visualização da credencial' (Credential preview) section showing a black tag with the Intelbras logo and a car icon. Below this, there are two dropdown menus: 'Nível da credencial *' (Credential level) set to 'Normal' and 'Tipo de credencial *' (Credential type) set to 'Tag UHF'. A 'Detalhes da credencial' (Credential details) section contains four input fields: 'Código Hexa' (Hex code), 'Código Decimal' (Decimal code), 'Observação' (Observation), and 'Tamanho *' (Size) set to '26 bits'. At the bottom, there are two buttons: 'Salvar credencial' (Save credential) in green and 'Cancelar' (Cancel) in red.

Importante: la lectura de las tags vehiculares UHF se hace a través de lectores vehiculares UHF.

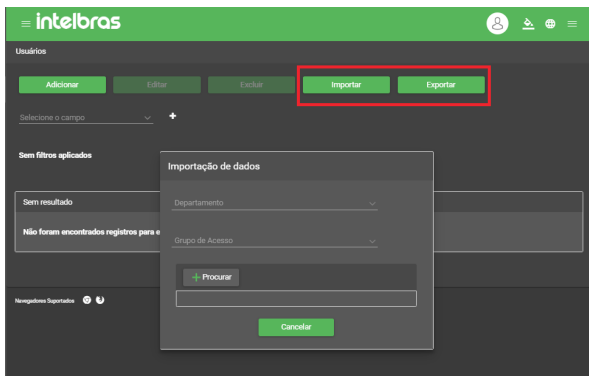
En la pestaña *Campos personalizados*, el operador del sistema puede insertar datos extras que considere relevantes en el registro del usuario. Estas informaciones estarán vinculadas al registro así que se apriete el botón *Guardar y concluir*. Para eso, el operador del sistema cuenta con 5 campos de texto y números para el llenado de informaciones.

Importante: las credenciales registradas dentro de la subsección usuarios se vincularán automáticamente al registro del usuario en cuestión. Eventualmente, si es necesario, esas credenciales se pueden desvincular del registro para vincularse a otros usuarios del sistema.

- » **Importar y exportar:** estas funciones permiten que el operador exporte un archivo conteniendo las informaciones de usuario en un archivo con el estándar de informaciones del software InControl. Esto posibilita el archivado de esas informaciones en archivos compatibles con Excel.

Es posible importar las informaciones de usuarios del software SoapAdmin3.5; para eso es necesario seleccionar la función *Exportación Avanzada* del software SoapAdmin 3.5, que garantizará que las informaciones se envíen de forma compatible con el software inControl.

Tras generar el archivo proveniente del software SoapAdmin 3.5, haga un clic en la opción importar y seleccione el departamento al cual los usuarios que se importarán pertenecerán, así como el Grupo de puntos de acceso al cual ellos podrán acceder.



Importante:

- » La función *Exportación Avanzada* del software SoapAdmin es una función exclusiva para exportar las informaciones de usuarios en formato compatible con el software InControl. Para obtener más informaciones consulte el manual del software SoapAdmin3.5.
- » En caso que el operador no seleccione el departamento y los grupos de puntos de accesos en el software InControl, los usuarios importados precisarán ajustar esas informaciones posteriormente, de manera individual, para que puedan acceder a los dispositivos del sistema.
- » El Proceso de Importación/Exportación de Usuarios descrito anteriormente es exclusivo para la sesión de Registros de Usuarios del sistema InControl.

3.2. Registro de departamentos

Departamentos son necesarios para la organización general del sistema de control de acceso. En esta sección, el operador del sistema puede crear cuantos departamentos sean necesarios para que posteriormente se vinculen al registro de los usuarios.

Para incluir un nuevo departamento, haga un clic en el botón *Agregar*.

Departamentos

Adicionar Editar Excluir Importar Exportar

Selecione o campo +

Sem filtros aplicados

Mostrando 4 coluna(s) Selecionar todos

Nome	Número	Observação	Departamento principal
P&D	1		

1 < > >>

En la nueva ventana, seleccione las informaciones y al final haga un clic en *Guardar y concluir*.

- » Departamento principal: seleccione a que departamento registrado anteriormente este departamento estará vinculado;
- » Nombre del departamento;
- » Número del departamento (secuencial);
- » Observaciones.

Departamentos > Departamentos Edição

Parâmetros Básicos

Departamento principal

Nome *

Colaboradores

Número

1

Observação

Salvar e concluir Voltar

Importante: el registro de por lo menos un departamento está indicado para el correcto vínculo de los usuarios en sus respectivos departamentos en el sistema InControl. Tras el registro de la lista de departamentos es posible editar o excluir el departamento creado, seleccionándolo en la lista siguiente y haciendo un clic en los botones *Editar* o *Excluir*.

Departamentos

Adicionar Editar Excluir Importar Exportar

Selecione o campo +

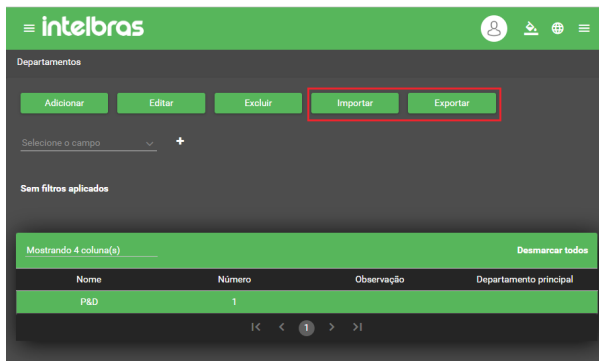
Sem filtros aplicados

Mostrando 4 coluna(s) Desmarcar todos

Nome	Número	Observação	Departamento principal
P&D	1		

1

- » **Importar y Exportar:** es posible importar o exportar una lista de departamentos de un archivo Excel o a un archivo de Excel. Para eso basta hacer un clic en uno de los botones *Importar* o *Exportar* localizados en la sección *Departamentos*.



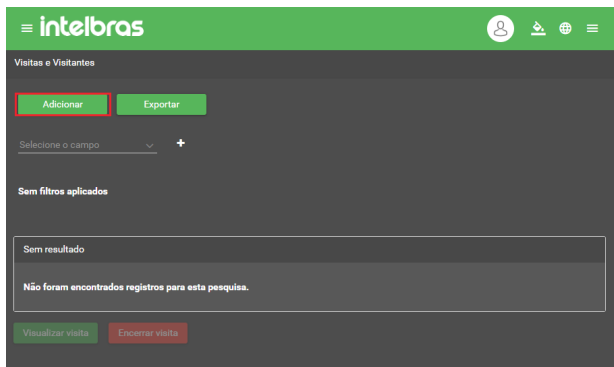
Importante: en caso que el operador del sistema desee crear una lista de departamentos en Excel y posteriormente importarla al sistema, recomendamos que se registre el primero de la lista vía software, exportado al archivo Excel, para que entonces él pueda insertar los demás departamentos en las columnas estándar del software.

3.3. Registro de visitantes

El registro de visitantes es semejante al registro de usuarios comunes o tercerizados del sistema, pero, sin embargo, el visitante tiene por definición un período previamente estipulado de validez dentro del sistema y, cuando termina este período, él no podrá más acceder a los ambientes controlados.

Está también la posibilidades de inserción de otras informaciones en el registro de visitantes, tales como visitado y período en el que se realiza la visita.

Para registrar una nueva visita, haga un clic en el botón Agregar en la sección *Visitantes*.

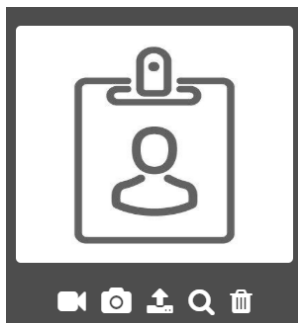


En la nueva ventana, la primera pestaña Datos Visitante posibilita que el operador del sistema registre las siguientes informaciones:

- » Casilla de verificación para marcado si el visitante ya se registró anteriormente;
- » Nombre completo;
- » Documento de CI;
- » Documento de CPF;
- » Dirección electrónica E-mail;
- » Selección de los Grupos de acceso;
- » Foto.

The screenshot shows the Intelbras web application interface. At the top is a green header with the Intelbras logo and navigation icons. Below the header, the breadcrumb trail reads 'Visitas e Visitantes > Visitas e Visitantes Criação'. The main content area has four tabs: 'Dados Visitante' (selected), 'Dados Visita', 'Veículo', and 'Credenciais'. Under the 'Dados Visitante' tab, there is a form with the following elements: a checkbox labeled 'Visitante já cadastrado?'; a text input field for 'Nome Completo'; a text input field for 'RG'; a text input field for 'CPF' with a green checkmark icon; a text input field for 'E-mail'; a dropdown menu for 'Grupo de Acesso'; and a green button labeled 'Copiar última visita'. To the right of the form is a large white square placeholder for a photo, featuring a clipboard icon with a person silhouette. Below the photo placeholder are five icons: a video camera, a photo camera, an upload arrow, a magnifying glass, and a trash can.

Para la captura de la foto son válidos los mismos métodos disponibles en la sección de registro de usuarios.



Importante: en caso que se seleccione el casilla de verificación *¿Visitante ya registrado?*, abrirá una ventana de búsqueda en el campo Nombre para seleccionar uno de los registros de la lista de *Visitantes*.

intelbras

Visitas e Visitantes > Visitas e Visitantes Criação

Dados Visitante

Dados Visita

Veículo

Credenciais

☒ Visitante já cadastrado?

Nome do usuário *

Procurar

José Alves

CPF

Visitado

Grupo de Acesso

Copiar última visita

En la pestaña *Datos Visita* están disponibles para inclusión los datos referentes al visitado.

Los datos son:

- » Visitado;
- » Tipo de usuario;
- » Inicio y fin de la validez de la visita;
- » Fecha de la última visita y último visitado;
- » Observaciones.

The screenshot shows a web application interface with a dark theme. At the top, there is a breadcrumb navigation: 'Visitas e Visitantes' followed by a right-pointing arrow and 'Visitas e Visitantes Criação'. Below this is a horizontal tab bar with four tabs: 'Dados Visitante', 'Dados Visita' (which is highlighted with a green underline), 'Veículo', and 'Credenciais'. The main content area is a light gray rectangle containing several input fields. On the left side, there is an 'E-mail' field, an 'Início validade' field with the date '30/07/2019', a 'Data última visita' field, and an 'Observações' field. On the right side, there is a 'Tipo de usuário' field with the value 'Visitante', a 'Fim validade' field with the date '30/07/2019', and an 'Último visitado' field. A green message line reads: 'As funcionalidades de validade da visita só funcionam corretamente com o dispositivo conectado.' At the bottom of the form, there are two green buttons: 'Salvar e concluir' on the left and 'Voltar' on the right.

Importante: los campos *Fecha última visita* y *Último visitado* sólo estarán disponibles en caso que el registro del visitante ya se haya hecho anteriormente.

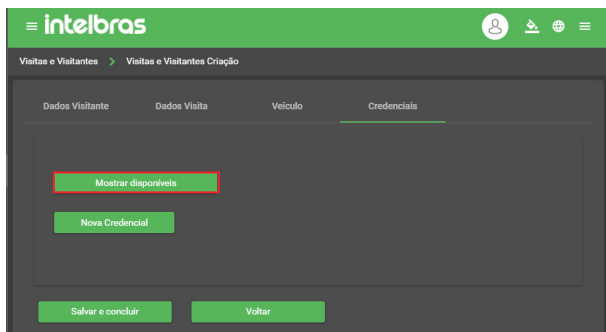
La pestaña vehículo posibilita el registro del vehículo del visitante en caso que sea necesario. Las informaciones disponibles para registro son:

- » Letras de la chapa;
- » Número de la chapa;
- » Color;
- » Marca;
- » Modelo;
- » Foto.

The screenshot shows the 'Usuários Criação' (User Creation) interface with the 'Veículo' tab selected. The interface includes a green header with the 'intelbras' logo and navigation icons. Below the header, there are tabs for 'Parâmetros Básicos', 'Detalhes', 'Veículo', 'Credenciais', and 'Campos personalizados'. The 'Veículo' tab contains several input fields for vehicle information: 'Letras da Placa', 'Número da Placa', 'Cor', 'Marca' (with a dropdown arrow), and 'Modelo'. To the right of these fields is a large square area for a vehicle photo, which currently displays a car icon. Below the photo area are icons for video, photo, upload, search, and delete. At the bottom of the form are two green buttons: 'Salvar e concluir' and 'Voltar'.

Importante: para la captura de la foto del vehículo están disponibles los mismos recursos de la captura de la foto del registro de usuarios.

La pestaña *Credenciales* posibilita que se atribuyan nuevas credenciales al registro del visitante y también posibilita la utilización de eventuales credenciales registradas previamente para el registro del visitante en cuestión. Para consultar la existencia de credenciales disponibles en el sistema, haga un clic en el botón *Mostrar disponibles*.



En caso que necesite registrar una nueva credencial, basta hacer un clic sobre el botón *Nueva credencial* e insertar los datos y posteriormente hacer un clic en el botón *Guardar credencial* para concluir el proceso:

- » Nivel de Credencial;
- » Tipo de Credencial:
 - » Tarjeta;
 - » Digital;
 - » Clave;
 - » Tag UHF.

The screenshot shows the Intelbras web application interface. At the top is a green header with the Intelbras logo and navigation icons. Below the header, the breadcrumb trail reads "Visitas e Visitantes > Visitas e Visitantes Criação". The main content area has four tabs: "Dados Visitante", "Dados Visita", "Veículo", and "Credenciais", with "Credenciais" being the active tab. A green button labeled "Mostrar disponíveis" is at the top of the form. Below it, the text "Cadastro de nova credencial" is displayed. The form contains two dropdown menus: "Nível da credencial" with "Visitante" selected, and "Tipo de credencial". At the bottom of the form are two buttons: "Salvar credencial" (green) and "Cancelar" (red).

Importante:

- » El proceso de registro de credenciales para los visitantes sigue el mismo flujo del proceso de registro de credenciales del registro de usuarios.
- » Las credenciales registradas en esta sección se vinculan automáticamente al registro del visitante en cuestión.

No es posible excluir un registro de visitante. Solamente cerrar la visita. Eso se puede hacer de forma manual o por fecha. Para cerrar una visita manualmente, seleccione el registro en la pantalla principal de visitantes y haga un clic en el botón *Cerrar Visita*.

Visitas e Visitantes

Adicionar Exportar

Selecione o campo +

Sem filtros aplicados

Mostrando 10 coluna(s)

Nome do Visitante	Data última visita	Nome do Visitado	CPF do Visitado	CPF do visitante	RG	Ativa	Início validade	Fim validade	Observações
Scarlet	12-07-2019	Rafael		000.000.000-00		Sim	12-07-2019	12-07-2019	

< < 1 > >

Visualizar visita Encerrar visita

Para visualizar visitas cerradas es necesario aplicar el filtro de visitas activas en la pantalla inicial de visitantes.

intelbras

Visitas e Visitantes

Adicionar Exportar

Selecione o campo +

Ativa: Não ✕

Mostrando 10 coluna(s)

Nome do Visitante	Data última visita	Nome do Visitado	CPF do Visitado	CPF do visitante	RG	Ativa	Início validade	Fim validade	Observações
Zé das couves		Scarlet		000.000.000-00		Não	26-07-2019	26-07-2019	

Visualizar visita Encerrar visita

Navegadores Suportados:  

InControl - Intelbras S/A todos os direitos reservados.

Importante:

- » Los campos de filtro poseen varias opciones que se pueden aplicar para visualizar apenas lo que se desea.
- » Tras registrar un visitante, no es posible editar ese registro, apenas visualizarlo posteriormente.
- » Las visitas las cierra automáticamente el software, así que su período de validez expira. Para garantizar que estas informaciones se actualicen correctamente en los dispositivos de control de acceso del sistema es necesario que estén conectados a la red local y debidamente online.

3.4. Registro de credenciales

En esta sección se registran las credenciales, independiente de registros de usuarios o visitantes. Las credenciales registradas en esta sección quedan disponibles para asociación con otros usuarios o visitantes posteriormente. Para registrar una nueva credencial haga un clic en el botón *Agregar*.

Nível	Tipo	Código Decimal	Nome Completo	Observação	Coação
Normal	Tag UHF		Gerente		Não
Normal	Cartão		Gerente		Não
Normal	Cartão	866624342			Não
Normal	Cartão	859099650			Não
Normal	Cartão	3668452458			Não
Normal	Cartão	2166803615			Não
Normal	Cartão	30043264238			Não

En la nueva ventana, seleccione el nivel de la credencial y su tipo; consecuentemente llene los campos referentes al tipo de la credencial elegida. Finalmente, haga un clic en *Guardar credencial* para concluir el proceso de registro.

The screenshot shows the Intelbras web interface. At the top is a green header with the Intelbras logo and navigation icons. Below the header is a white box containing the URL `www.intelbras.com.br`. The main content area has a dark gray background. It features a section titled "Selecione o modo de captura" (Select the capture mode) with two buttons: "Captura local" (Local capture) and "Captura remota" (Remote capture). Below this, there are two columns of settings. The left column has "Nível de credencial" (Credential level) set to "Normal" and "Nome do usuário" (User name) with a search icon. The right column has "Tipo de credencial" (Credential type) set to "Cartão" (Card) and "Tamanho" (Size) set to "26 bits". A "Detalhes da credencial" (Credential details) section contains fields for "Código Hexa" (Hex code), "Código Decimal" (Decimal code), "Observação" (Observation), and a checkbox for "Coação" (Coercion). At the bottom is a green button labeled "Salvar credencial" (Save credential).

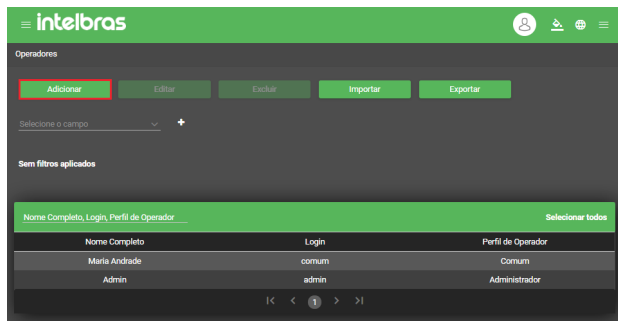
En la ventana inicial de las secciones de *Credenciales*, note que ella aparece citada en la tabla de credenciales disponibles siguiente:

This screenshot is identical to the one above, showing the Intelbras web interface for credential capture settings. It includes the header, the URL box, the capture mode selection, the credential level and type settings, the details section with various codes and checkboxes, and the save button.

Importante: el proceso de registro de credenciales sigue el mismo flujo del proceso de registro de credenciales del registro de usuarios.

3.5. Registro de Operadores del sistema

En esta sección se citan los operadores del sistema que ya se registraron, inclusive el operador administrador, que es el operador estándar del sistema. Para efectuar un registro de operador nuevo haga un clic en el botón *Agregar*.



En la nueva ventana, inserte los parámetros y haga un clic en el botón *Guardar y concluir*.

- » Nombre del Perfil;
- » Login;
- » Clave;
- » Confirmación de Clave;
- » E-mail;
- » Perfil de Operador;
 - » Recepción;
 - » Portería;
 - » Común.
 - » Administrador.
- » » Foto.

Importante: nuevos perfiles de operadores se podrán incluir según la necesidad. Los perfiles anteriormente mencionados están previamente registrados y se pueden modificar.

» Foto.

intelbras

Operadores > Operadores Criação

Parâmetros Básicos

Nome *

Login *

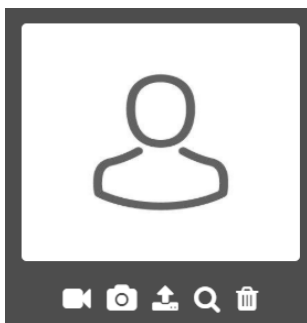
Senha *

Confirmação de senha

E-mail

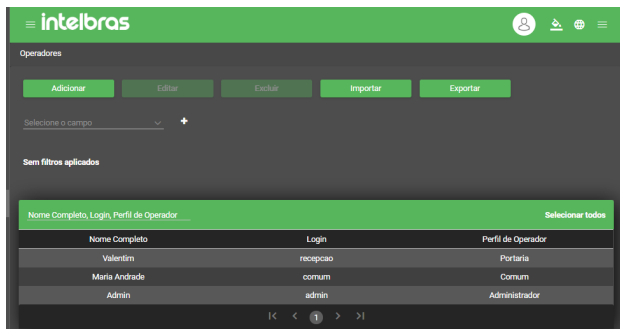
Perfil

Status:
☒ Ativo

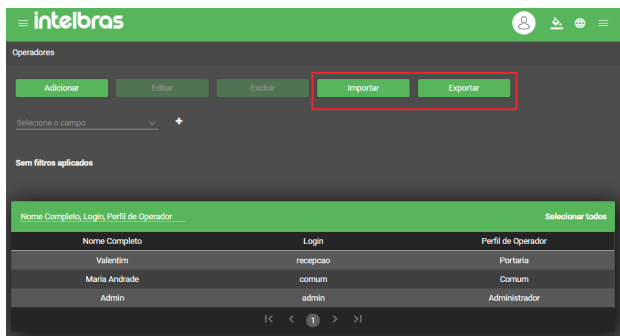


Importante: para la captura de la foto del operador están disponibles los mismos recursos de la captura de la foto del registro de usuarios.

Verifique el registro efectuado en la lista de operadores del sistema de la sección *Operadores*.



- » **Importar y Exportar:** es posible importar o exportar una lista de operadores del sistema de un archivo Excel o a un archivo de Excel. Para eso, basta hacer un clic en uno de los botones *Importar* o *Exportar* localizados en la sección *Operadores*.



Importante: en caso que el operador del sistema desee crear una lista de Operadores de Sistema en Excel y posteriormente importarla al sistema, recomendamos que se registre el primero de la lista vía software, exportado al archivo Excel, para que entonces él pueda insertar los demás operadores en las columnas estándar del software.

3.6. Registro de Perfiles para operadores del sistema

En esta sección el sistema posibilita que el operador cree Perfiles de acceso donde los registros de operadores del sistema estarán vinculados durante el registro. Esos perfiles básicamente limitan el acceso de los operadores a una o más secciones del sistema de control de acceso y sirven también para garantizar la seguridad del sistema de tal forma que los operadores accedan a las secciones que tengan familiaridad con las rutinas de su día a día.

El sistema trae como estándar de fábrica cuatro perfiles de operadores previamente registrados. Ellos son:

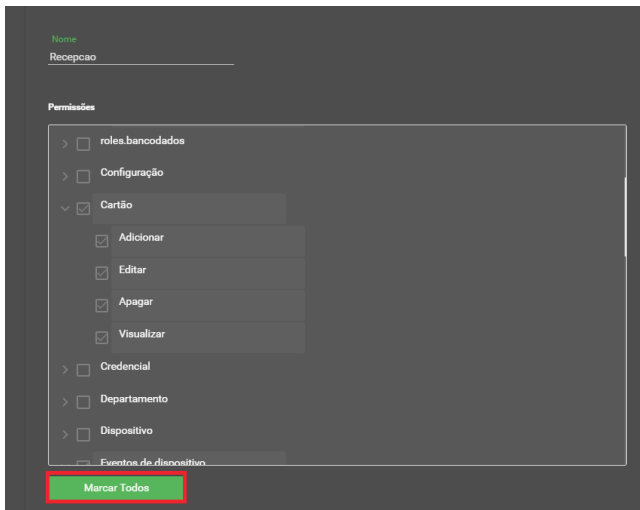
- » Recepción;
- » Portería;
- » Administrador.

Cada uno de esos perfiles citados anteriormente posee permisos de acceso distintos. Verifique el ejemplo del perfil *Recepción* en las imágenes siguientes:

The screenshot shows a web interface for configuring user permissions. At the top, the user's name 'Faxineiros' is displayed. Below it, a section titled 'Permissões' (Permissions) contains a list of system functions, each with an unchecked checkbox and a right-pointing arrow. The functions listed are: 'Ações Vinculadas à Eventos', 'Área', 'roles.backup', 'roles.bancodados', 'Configuração', 'Cartão', 'Credencial', 'Departamento', 'Dispositivo', and 'Eventos de dispositivo'. At the bottom of the list is a partially visible option 'Eventos de operador'. A green button labeled 'Marcar Todos' (Mark All) is located at the bottom left of the permissions list area.

Las funciones disponibles del sistema están representadas con Checkbox que, una vez marcados, el perfil pasará a tener acceso a estas áreas. Lo contrario también es verdad, es decir, una vez desmarcados, el operador vinculado a este perfil no tendrá más acceso a la sección referente.

Existe la posibilidad de marcar todos los casillas de verificación haciendo un clic en el botón *Marcar Todos* al final de la ventana. Tras las debidas marcas es necesario hacer un clic en el botón *Guardar y concluir* para finalizar el proceso.



The screenshot shows a user profile configuration interface. At the top, there is a label 'Nome' in green and a text input field containing 'Recepcao'. Below this is a section titled 'Permissões' (Permissions). Inside this section is a list of permissions, each with a checkbox and a right-pointing arrow. The permissions are: 'roles.bancodados', 'Configuração', 'Cartão', 'Adicionar', 'Editar', 'Apagar', 'Visualizar', 'Credencial', 'Departamento', 'Dispositivo', and 'Eventos de dispositivo'. The 'Cartão' permission is selected, and its sub-permissions 'Adicionar', 'Editar', 'Apagar', and 'Visualizar' are also selected. At the bottom of the permissions list is a green button labeled 'Marcar Todos' (Mark All), which is highlighted with a red rectangle.

Para agregar un nuevo perfil de su preferencia, haga un clic en el botón *Agregar* y llene los campos indicados en la pantalla de perfil, tales como:

- » Nombre del Perfil;
- » Permisos deseados.

Perfil de Operador

Adicionar

Editar

Excluir

Selecione o campo



Sem filtros aplicados

Nome do Perfil

Nome do Perfil

Recepcao

Portaria

Comum

Administrador

|< < 1 > >|

Nome

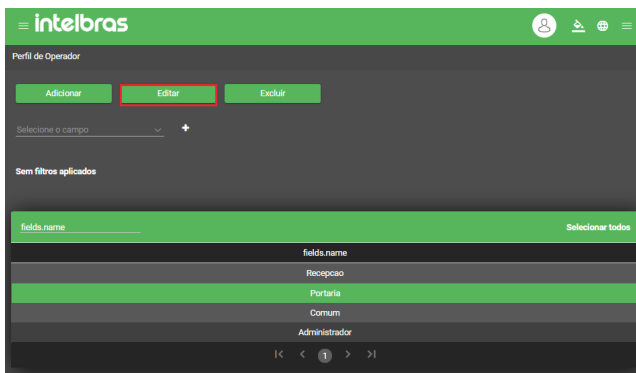
Faxineiros

Permissões

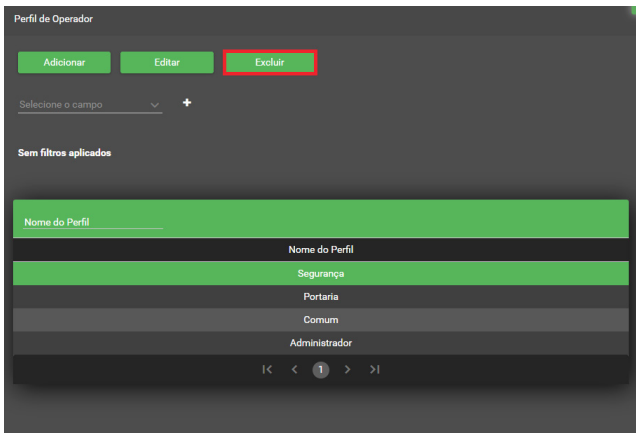
- > ☐ Ações Vinculadas à Eventos
- > ☐ Área
- > ☐ roles.backup
- > ☐ roles.bancodados
- > ☐ Configuração
- > ☐ Cartão
- > ☐ Credencial
- > ☐ Departamento
- > ☐ Dispositivo
- > ☐ Eventos de dispositivo
- > ☐ Eventos de operador

Marcar Todos

Los cuatro perfiles estándar del sistema se pueden modificar. Para eso, basta seleccionar uno de ellos a la lista de perfiles disponibles y hacer un clic en el botón *Editar*.



En caso que desee excluir uno de los perfiles creados, selecciónelo en la lista y haga un clic en el botón *Excluir*.



Importante: los cuatro perfiles estándar del software se pueden editar, pero no se pueden excluir.

4. Dispositivos

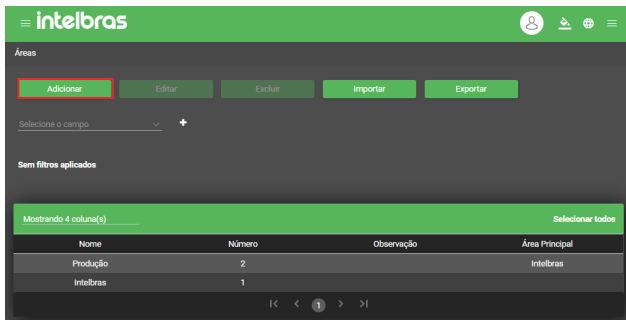
Dispositivos son equipos que controlan las puertas de las áreas del sistema de control de acceso. Esos dispositivos se agregan al sistema InControl vinculados a las áreas controladas. Para validar los accesos de los usuarios, los dispositivos poseen métodos de autenticación distintos que, en el sistema de control de acceso, están caracterizadas como *Credenciales*, que pueden ser (Biometrías digitales, Biometrías Faciales, Tarjeta RFID, Clave numérica, Tag UHF).

La capacidad de usuarios y credenciales varía de acuerdo con los dispositivos, así como el número de puertas controladas que varía de una puerta a cuatro puertas autónomamente, dependiendo del modelo del dispositivo.

Importante: el registro de biometrías faciales se tiene que hacer directamente en el dispositivo físico y no se podrá hacer vía software.

4.1. Registro de Áreas

Áreas son los lugares en que los dispositivos están instalados. Es necesario registrar un área antes de agregar un dispositivo, porque será necesario vincular el área en el registro de dispositivos. Para agregar una nueva área dentro de la sección Áreas, haga un clic en el botón *Agregar*.



Áreas

Adicionar Editar Excluir Importar Exportar

Selecione o campo ▼ +

Sem filtros aplicados

Mostrando 4 coluna(s) Selecionar todos

Nome	Número	Observação	Área Principal
Produção	2		Intelbras
Intelbras	1		

< > 1 >

En la nueva pantalla, seleccione las informaciones necesarias para el registro del área y al final haga un clic en *Guardar y concluir* para finalizar el proceso.

- » Seleccione el área principal: en caso que esa área pertenezca a otra de más relevancia;
- » Nombre;
- » Número: Identificador del área siempre numérico y secuencial;
- » Observación.

Parâmetros Básicos

Fábrica

Nome
Produção

Número
2

Observação
Setor Industrial

Salvar e concluir Voltar

- » **Importar y Exportar:** es posible importar o exportar una lista de áreas del sistema de un archivo Excel o a un archivo de Excel. Para eso basta hacer un clic en uno de los botones *Importar* o *Exportar* localizados en la sección *Áreas*.

intelbras

Áreas

Adicionar Editar Excluir Importar Exportar

Selecione o campo +

Sem filtros aplicados

Mostrando 4 coluna(s) Selecionar todos

Nome	Número	Observação	Área Principal
Produção	2		Intelbras
Intelbras	1		

< < 1 > >

Importante: en caso que el operador del sistema desee crear una lista de áreas en Excel y posteriormente importarla al sistema, recomendamos que se registre la primera de la lista vía software, exportado al archivo Excel, para que entonces él pueda insertar las demás áreas en las columnas estándar del software.

En la pantalla inicial de la sección de Áreas es posible visualizar todas las áreas ya registradas en el sistema. Es posible que las áreas registradas se excluyan o editen. Para eso, seleccione una de las áreas registradas en la lista y haga un clic en los botones *Editar* o *Excluir*.

Áreas

Adicionar Editar Excluir Importar Exportar

Selecione o campo +

Sem filtros aplicados

Mostrando 4 coluna(s) Selecionar todos

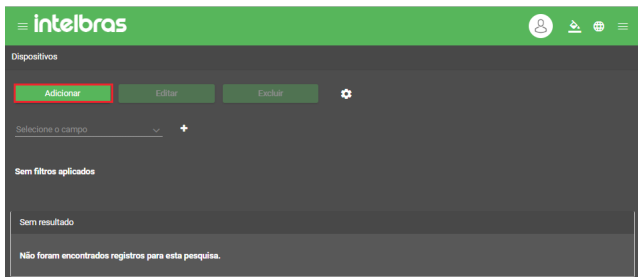
Nome	Número	Observação	Área Principal
Produção	2		Intelbras
Intelbras	1		

< > 1 >

Importante: antes de excluir un área, verifique si ella no está vinculada a un dispositivo y desvincúlela primero. Es necesario que haya por lo menos un área registrada en el sistema.

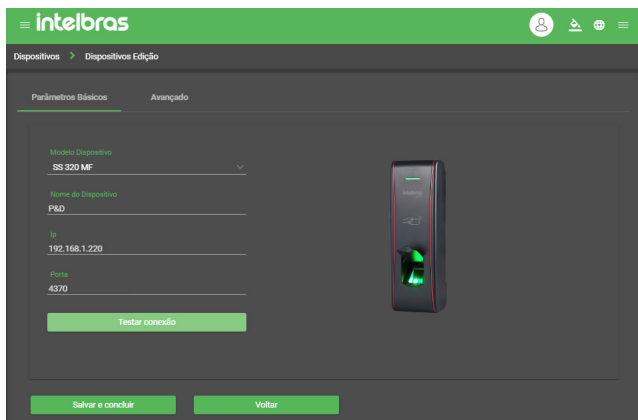
4.2. Registro de Dispositivos

En esta sección es posible registrar los dispositivos que formarán parte del sistema de control de acceso. Para iniciar el registro, haga un clic en el botón *Agregar*.



En la nueva ventana, en la pestaña *Parâmetros básicos*, inserte las informaciones descritas a continuación. Para probar la comunicación del dispositivo con el software, tras llenar las informaciones, haga un clic en el botón *Probar conexión*.

- » Seleccione el modelo del dispositivo;
- » Nombre del dispositivo;
- » Dirección IP;
- » Puerta de comunicación.



Importante:

- » Verifique si la imagen referente al modelo del dispositivo es igual al dispositivo físico instalado.
- » Los dispositivos soportados por el software InControl son los disponibles en la opción *Modelo del dispositivo*, en la pestaña *Parámetros básicos*.

En la pestaña *Avanzado* es posible insertar las informaciones complementarias, tales como: clave de comunicación y el área a la cual pertenecerá el dispositivo. También es posible marcar el checkbox *¿Excluir datos al guardar?*, que lleva a cero todas las informaciones registradas en el dispositivo antes de insertarlo en la base de datos del sistema.

La imagen muestra la interfaz de usuario de InControl, específicamente la pestaña **Avanzado**. En la parte superior, hay dos pestañas: **Parâmetros Básicos** y **Avançado**, con la segunda activa. El formulario contiene los siguientes campos:

- Senha de Comunicação:** Un campo de texto con caracteres ocultos por asteriscos.
- Produção:** Un menú desplegable con una flecha hacia abajo.
- ¿Excluir dados ao salvar?:** Un checkbox marcado con una 'x' verde, rodeado por un recuadro rojo.
- Tipo de Controle:** Un campo con el valor 'Pull'.

En la parte inferior del formulario, hay dos botones verdes: **Salvar e concluir** y **Voltar**.

En esta pestaña también se exhibe el tipo de control existente en el dispositivo. Esta información se carga automáticamente según el modelo seleccionado. Para finalizar el registro haga un clic en el botón *Guardar y concluir*.

Parâmetros Básicos Avançado

Senha de Comunicação

Produção ▾

☒ Excluir dados ao salvar?

Tipo de Controle
Pull

Salvar e concluir Voltar

Verifique el dispositivo registrado en la lista de dispositivos del sistema en la pantalla principal de la sección *Dispositivos*. En caso que sea necesario editar o excluir el dispositivo registrado, selecciónelo en la lista de los dispositivos disponibles y haga un clic en los botones *Editar* o *Excluir*.

Importante: se recomienda siempre marcar la opción *¿Excluir datos al guardar?*, pues la lista de usuarios y configuraciones principal siempre será la existente en el software. En caso que no se marque esta opción y haya usuarios registrados en el dispositivo, ellos quedarán sobrescritos, considerando la lista ya existente de usuarios en el sistema.

intelbras

Dispositivos

Adicionar Editar Excluir ⚙️

Selecione o campo ▾ +

Sem filtros aplicados

Mostrando 6 coluna(s)						Desmarcar todos
Nome	Nome da Área	Habilitado	Ip	Porta	Nome Modelo	
P&D	Intelbras	Sim	192.168.1.220	4370	SS 320 MF	

1

La sección Dispositivos también posibilita que el operador del sistema efectúe una serie de ajustes en los dispositivos registrados y/u otras formas de agregar dispositivos, tal como *Búsqueda de dispositivos en la red*. Verifique la lista de funciones disponibles siguiente:

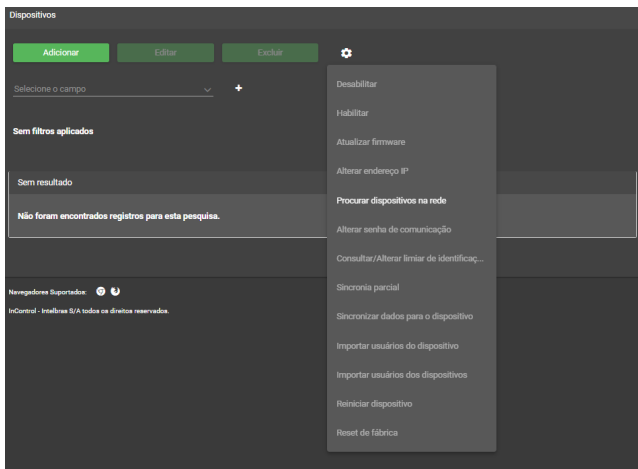
- » **Deshabilitar:** remueve de la lista de dispositivos activos el dispositivo seleccionado. En esta condición el dispositivo no recibirá el sincronismo de las actualizaciones hechas en el sistema;
- » **Habilitar:** inserte nuevamente el dispositivo seleccionado en la lista de dispositivos activos del sistema. En esta condición el dispositivo pasa a recibir las actualizaciones de sincronismo del sistema de control de acceso. Una vez que se habilita la información del dispositivo, la información del software se eliminará y se enviará nuevamente;
- » **Actualizar firmware:** posibilita que nuevas versiones de firmware del dispositivo seleccionado se actualicen automáticamente a través del software de control de acceso. Esta función varía de acuerdo con el modelo del dispositivo agregado. Es necesario consultar el manual del dispositivo de hardware para garantizar la existencia de esta funcionalidad;
- » **Modificar dirección IP:** modifica la dirección del IP físico del dispositivo seleccionado para otro rango específico definido por el operador del sistema.
- » **Buscar dispositivos en la red:** efectúa una barradura de todos los dispositivos activos que están disponibles y conectados a la red del sistema;
- » **Modificar clave de comunicación:** esta función posibilita la modificación de la clave de comunicación definida para el dispositivo seleccionado en el momento de su registro. Esta clave, en caso que se atribuya al dispositivo, será necesaria para establecer la comunicación física con el dispositivo de hardware.
- » **Consultar / Modificar límite de identificación:** esta función aumenta o disminuye la criticidad de verificación de los módulos biométricos facial y digital, es decir, a medida que el límite de identificación aumenta, más puntos se verificarán en la lectura de la credencial y, a medida que este límite de identificación disminuye, menos puntos de verificación en la credencial biométrica son necesarios para la liberación del acceso.
- » **Tiempos pendientes:** sincroniza para los dispositivos eventuales informaciones que todavía no se hayan enviado a partir del software a los dispositivos adicionales.
- » **Sincronizar datos para el dispositivo:** sincroniza para el dispositivo agregado todas las informaciones actuales del software, actualizando su base de datos.

- » **Importar usuarios del dispositivo:** importa al sistema las informaciones de registros y configuraciones del dispositivo seleccionado. Usuario que existen en el dispositivo pero no existen en el Software, reciben un grupo creado automáticamente. Cuando el usuario existe en Incontrol y en el dispositivo, la importación mantiene al usuario de InControl sin cambios, pero no cambia al usuario en el dispositivo.

Importante:

- » El proceso de Importación de usuarios se debe hacer cuando no hay registros anteriores ya hechos en la base de datos del sistema, pues el sistema siempre tendrá prioridad en el número de los ID's de los usuarios y sus credenciales. Es decir, en caso que se haga la importación de más de un dispositivo que tenga usuarios distintos, pero con ID's iguales en las respectivas memorias de los dispositivos, se considerará como ID válido el primer dispositivo en que se haga la importación. Los usuarios con el mismo ID del segundo dispositivo se ignorarán y el sistema no los importará. Reforzamos la importancia de que todos los registros se hagan directamente en el sistema InControl.
- » En caso que se haga el proceso de importación de dos dispositivos con usuarios distintos y con ID's iguales, el primer dispositivo se considerará y el segundo se ignorará. Sin embargo, si en el registro del segundo dispositivo hay una credencial con un tipo distinto del tipo de credencial presente en el primer dispositivo importado, ella se atribuirá al usuario con el mismo ID del primer dispositivo.
- » **Reiniciar dispositivo:** reinicia el dispositivo seleccionado;
- » **Reset de fábrica:** vuelve al estándar de fábrica todas las configuraciones del dispositivo seleccionado, borrando inclusive todos los usuarios y credenciales de la memoria del dispositivo, excepto configuraciones de red.

A estas funciones se puede acceder tras seleccionar el dispositivo en cuestión en la lista de dispositivos disponibles y, posteriormente, hacer un clic en el botón de engranaje en la parte superior de la *sección Dispositivos*.



Importante: las funciones citadas anteriormente varían de acuerdo con el modelo del producto.

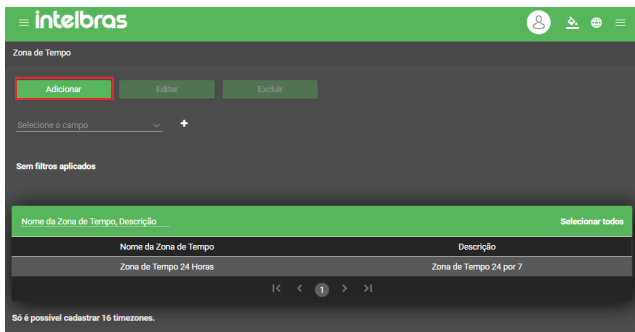
5. Control de acceso

Esta sección del software le trae al operador del sistema una gama de funciones que buscan organizar e instaurar las reglas necesarias para que los usuarios del sistema y los dispositivos controladores de acceso operen de forma correcta, posibilitando una mayor seguridad de informaciones y del sistema de forma general.

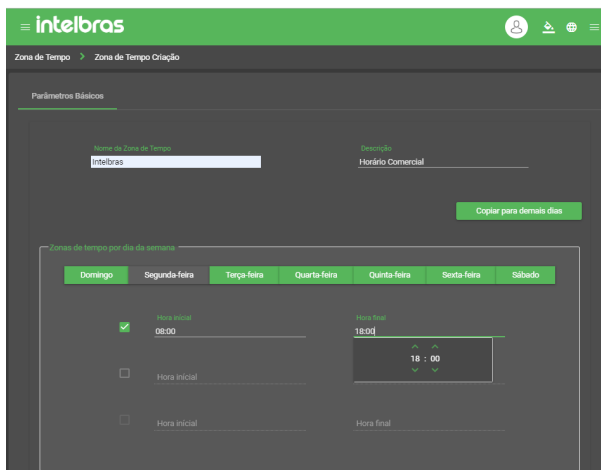
5.1. Zonas de tiempo

La sección zona de tiempo permite que el operador del sistema registre rangos de horarios semanales donde el sistema de control de acceso estará activo. Es decir, usuarios que formen parte de esta zona de tiempo podrán acceder a los ambientes controlados y se bloquearán intentos de acceso fuera de estos períodos.

El sistema ya trae la zona de tiempo 24 h registrada por estándar, sin embargo, es posible registrar nuevas zonas de tiempo que atiendan las necesidades deseadas. El sistema soporta hasta 16 zonas de tiempo registradas en total. Para agregar una nueva zona de tiempo, en la pantalla inicial, haga un clic en el botón *Agregar*.



En la nueva pantalla, defina el nombre de la zona de tiempo y agregue una descripción. En caso que sea necesario, seleccione uno de los días de la semana y defina los períodos de tiempo para él.



Importante: están permitidos como máximo 3 períodos de tiempo por día de la semana. Al final de la pantalla se le presenta al operador, para cotejo, una representación gráfica del período seleccionado.

intelbras

Copiar para demais dias

Zonas de tempo por dia da semana

Domingo Segunda-feira Terça-feira Quarta-feira Quinta-feira Sexta-feira Sábado

☒ Hora inicial 08:00 Hora final 18:00

☐ Hora inicial Hora final

☐ Hora inicial Hora final

Prévia da zonas de tempo configuradas para Segunda-feira

0h 4h 8h 12h 16h 20h 23h

Para replicar el período registrado a los demás días de la semana, haga un clic sobre el botón *Copiar para los demás días* y posteriormente haga un clic en *Guardar y concluir* para finalizar el proceso.

intelbras

Copiar para demais dias

Zonas de tempo por dia da semana

Domingo Segunda-feira Terça-feira Quarta-feira Quinta-feira Sexta-feira Sábado

☒ Hora inicial 08:00 Hora final 18:00

☐ Hora inicial Hora final

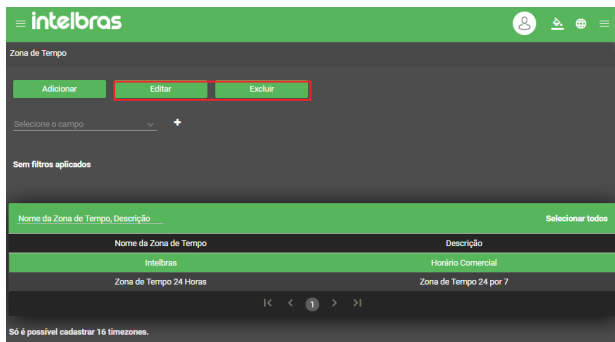
☐ Hora inicial Hora final

Prévia da zonas de tempo configuradas para Segunda-feira

0h 4h 8h 12h 16h 20h 23h

Salvar e concluir Voltar

La nueva zona de tiempo registrada se podrá editar o excluir. Para eso, basta seleccionar la zona de tiempo en la pantalla inicial y hacer un clic en los botones *Editar* o *Excluir*.



Importante: la zona de tiempo de 24h estándar del sistema no se puede excluir.

5.2. Puntos de acceso

Puntos de acceso son efectivamente las puertas que están siendo controladas por los dispositivos controladores de acceso (hardware). Para acceder a los detalles de configuración de esa sección es necesario que se agregue un dispositivo controlador de acceso debidamente al sistema.

Seleccione en la pantalla inicial el punto de acceso que desea modificar y haga un clic en el botón *Editar* para tener acceso a las configuraciones de la puerta.

Pontos de Acesso

Editar

Selecione o campo ▼ +

Sem filtros aplicados

Mostrando 13 coluna(s)

Nome Porta	N. Porta	Nome do Dispositivo	Nome da Zona Tempo Ativa	Nome da Zona tempo Aberta	Tipo de sensor	Modo de Verificação	Tipo Ponto de Acesso	Atraso Sensor	Bloquear ao fechar	Tempo de abertura	Tempo de Fechadura	Tempo entre identificação
Produção-1	1	Produção	Zona de Tempo 24 Horas		Sem sensor	Apenas biométrica	Porta	15	Não	10		10

◀ < 1 > ▶

En la nueva ventana es posible configurar, en la pestaña Parámetros básicos, las informaciones:

- » **Nombre de la puerta:** nombre que el operador del sistema desea atribuirle a la puerta;
- » **Tipo de puerta:** Carraca, Portón y Trampilla.

También se ilustra el número de la puerta que se registra automáticamente y la representación gráfica del tipo de puerta elegida.

Parâmetros Básicos Detalhes

Nome Porta
Produção-1

Porta ▼

N. Porta
1



Salvar e concluir **Voltar**

En la pestaña Detalles es posible configurar los siguientes parámetros;

- » **Zona de tiempo abierta:** período en que la puerta permanecerá abierta sin control.
- » **Método de verificación:** tipos de credenciales que serán válidas en la verificación del acceso en el dispositivo.
- » **Atraso del sensor de cerradura:** tiempo en segundos que la alarma de puerta abierta aguardará para disparar, en caso que la puerta se deje abierta.
- » **Tiempo entre identificaciones:** intervalo de tiempo entre lecturas de verificación de acceso en segundos.
- » **Zona de tiempo de la puerta:** período de tiempo en que la puerta estará activa. Es decir, para que una puerta esté activa, debe estar vinculada a una zona de tiempo válida en el sistema.
- » **Tipo de sensor de cerradura:** tipo de sensor de la cerradura de la puerta (normalmente abierto, normalmente cerrado o sin sensor).
- » **Tiempo de abertura de puerta:** tiempo en segundos en que la puerta permanecerá abierta tras un evento de acceso liberado.

También es posible marcar los casillas de verificación:

- » **Bloquear al cerrar:** esta función hace con que la puerta se tranque inmediatamente en el momento en que el sensor de cerradura identifica que la puerta se cerró.
- » **Copiar configuraciones para todos los puntos de acceso de este dispositivo:** copia todas las configuraciones de la puerta para todas las portas del dispositivo controlador de acceso.
- » **Copiar configuraciones para todos los puntos de acceso de todos los dispositivos:** copia todas las configuraciones de la puerta, para todas las puertas de todos los dispositivos controladores de acceso de todo el sistema.

Al final de las configuraciones, haga un clic en el botón Guardar y concluir para finalizar el proceso.

Parâmetros Básicos

Detalhes

Zona de tempo aberta

Zona de Tempo 24 Horas

Cartão RFID e Biometria Digital

Normalmente fechado

Atraso Sensor

Tempo de abertura

Tempo entre identificações

☒ Bloquear ao fechar

☒ Copiar configurações para todos os pontos de acesso deste dispositivo.

☐ Copiar configurações para todos os pontos de acesso de todos os dispositivo.

Salvar e concluir

Voltar

Importante: el número de puertas varía de acuerdo con el modelo del dispositivo.

5.3. Grupo de puntos de acceso

Grupos de puntos de acceso son grupos organizados que tienen como función básica unir los dispositivos controladores de acceso con los usuarios del sistema de control de acceso. Para registrar un grupo de puntos de acceso, en la pantalla inicial de esta sección, haga un clic en *Agregar*.

The screenshot shows the 'Grupos de Pontos de Acesso' (Access Point Groups) management page in the Intelbras InControl system. The interface has a green header with the Intelbras logo and navigation icons. Below the header, there are three buttons: 'Adicionar' (Add), 'Editar' (Edit), and 'Excluir' (Delete). The 'Adicionar' button is highlighted with a red rectangle. Below these buttons is a dropdown menu labeled 'Selecione o campo' (Select the field) with a plus sign to its right. A message 'Sem filtros aplicados' (No filters applied) is displayed. A table is shown with the caption 'Mostrando 3 coluna(s)' (Showing 3 column(s)). The table has three columns: 'Nome do Grupo' (Group Name), 'Nome da Zona de Tempo' (Time Zone Name), and 'Pontos de Acesso' (Access Points). The table contains one row with the following data: 'Total' for the group name, 'Zona de Tempo 24 Horas' for the time zone name, and 'SS 320 MF-1, SS 420-1.' for the access points. Below the table, there are navigation controls: '<<', '<', '1', '>', and '>>'. At the bottom of the page, it says 'Navegadores Suportados:' (Supported Browsers:) with icons for Chrome and Firefox, and a footer note: 'InControl - Intelbras S/A todos os direitos reservados.' (InControl - Intelbras S/A all rights reserved.).

Grupos de Pontos de Acesso

Adicionar Editar Excluir

Selecione o campo +

Sem filtros aplicados

Mostrando 3 coluna(s)

Nome do Grupo	Nome da Zona de Tempo	Pontos de Acesso
Total	Zona de Tempo 24 Horas	SS 320 MF-1, SS 420-1.

<< < 1 > >>

Navegadores Suportados:

InControl - Intelbras S/A todos os direitos reservados.

En la nueva ventana, en *Parâmetros básicos*, inserte las informaciones y posteriormente haga un clic en el botón *Guardar y concluir* para finalizar el proceso.

- » **Nombre del Grupo del punto de acceso;**
- » **Seleccione el punto de acceso:** punto de acceso (puerta) configurado en el ítem anterior;
- » **Zona de tiempo del grupo.**

intelbras

Grupos de Pontos de Acesso > Grupos de Pontos de Acesso Edição

Parâmetros Básicos

Nome do Grupo
Total

Zona de Tempo *
Zona de Tempo 24 Horas

SS 320 MF-1, SS 420-1

Pontos de acesso selecionados:

- Q SS 320 MF-1
- Q SS 420-1

Salvar e concluir Voltar

Navegadores Suportados:

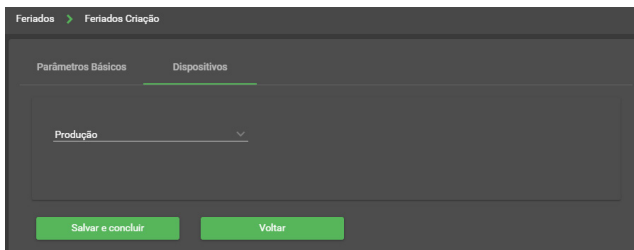
InControl - Intelbras S/A todos os direitos reservados.

6. Feriados

Feriados son fechas previamente establecidas donde no habrá acceso permitido por parte de los usuarios del sistema a los ambientes controlados. Para agregar un feriado, en la pantalla inicial, haga un clic en el botón *Agregar*.

En la nueva ventana, en la pestaña *Parâmetros Básicos*, llene el nombre del feriado, la fecha de inicio del feriado y marque el checkbox *Recorrente* en caso que este feriado se repita en otros años.

En la pestaña *Dispositivos*, seleccione en cuál de los dispositivos se aplicará el feriado registrado. Por fin, haga un clic en el botón *Guardar y concluir* para finalizar el proceso.



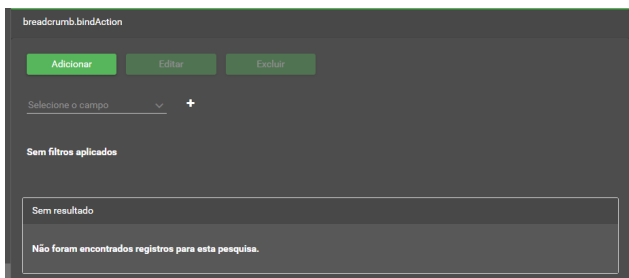
Importante:

- » Es necesario que el dispositivo seleccionado ya se haya registrado en el sistema anteriormente.
- » En caso que se agregue un nuevo dispositivo al software, es necesario editar el feriado para incluirlo a los demás dispositivos pertenecientes a él, en caso que sea necesario.
- » No todos los dispositivos de control de acceso soportan el registro de feriados. En esta sección se demostrarán apenas los dispositivos que soportan esa funcionalidad.

6.1. Acciones vinculadas a eventos

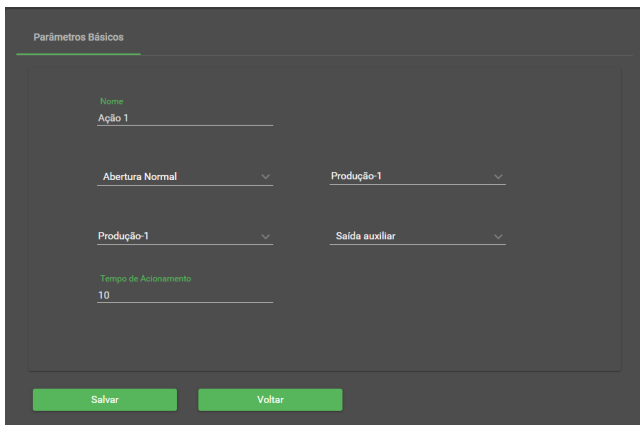
Esta sección posibilita el accionamiento de otras áreas de los dispositivos controladores de acceso a partir de gatillos de eventos del sistema. Es decir, cuando hay un acceso negado se puede accionar una salida auxiliar del dispositivo que estará conectada a otro sistema, por ejemplo.

Para registrar una de estas acciones, en la pantalla principal, haga un clic en el botón *Agregar*.



En la nueva ventana inserte las informaciones pertinentes y al final haga un clic en el botón *Guardar* para finalizar el proceso.

- » Nombre de la acción;
- » Tipo de evento gatillo;
- » Punto de acceso que recibe el gatillo;
- » Punto de acceso que se accionará;
- » Tipo de salida accionada;
- » Tiempo en segundos de accionamiento.



Parâmetros Básicos

Nome
Ação 1

Abertura Normal ▼

Produção-1 ▼

Produção-1 ▼

Saída auxiliar ▼

Tempo de Accionamento
10

Salvar Voltar

Es posible editar o excluir una acción, para eso, selecciónela en la lista de acciones registradas en la pantalla principal y haga un clic en los botones *Editar* o *Excluir*.

Importante: apenas dispositivos PULL SDK soportan esa funcionalidad.

Ações Vinculadas à Eventos

Adicionar
Editar
Excluir

Selecione o campo

Sem filtros aplicados

Mostrando 5 coluna(s)
Desmarcar todos

Nome	Gatilho	Nome Porta	Tipo Saída	Tempo de abertura
Intelbras	Abertura Normal	P&D-1	Saída auxiliar	10

6.2. Intertrabado

Esta seção se restringe a la línea CT 500 Intelbras, más específicamente a partir del modelo CT 500 2P, de tal forma que con ella es posible crear una condición en que el segundo punto de acceso (puerta) sólo se liberará por el evento de acceso cuando el primer punto de acceso (puerta) esté cerrada y viceversa.

Para registrar una regla de Intertrabado, haga un clic en el botón *Agregar* en la pantalla principal de sección de Intertrabado.

Intertravamento

Adicionar
Editar
Excluir

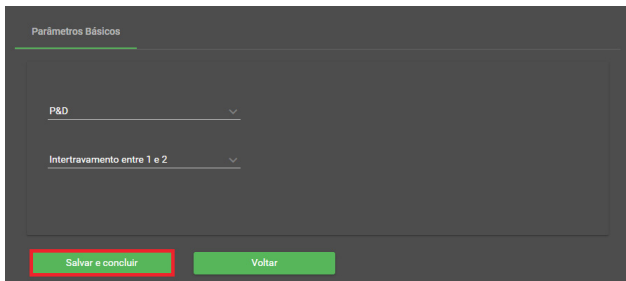
Selecione o campo

Sem filtros aplicados

Sem resultado

Não foram encontrados registros para esta pesquisa.

En la nueva ventana, seleccione el tipo de dispositivo que recibirá la nueva regla de Intertrabado y los puntos de acceso de este dispositivo en que se instaurará la regla. Por ejemplo: entre el punto de acceso 1 y 2 (puertas) o entre puntos de acceso 3 y 4 (puertas), para el caso del dispositivo CT 500 4P o 4PB. Finalmente, haga un clic en Guardar y concluir para finalizar el proceso.



Parâmetros Básicos

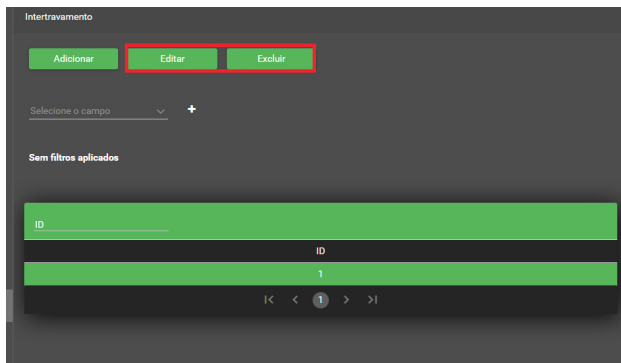
P&D

Intertravamento entre 1 e 2

Salvar e concluir Voltar

Importante: en caso que se seleccione un dispositivo distinto de la serie CT 500 Intelbras, se exhibirá un mensaje de error y no será posible registrar las reglas de Intertrabado.

Es posible editar o excluir la regla de Intertrabado registrada. Para eso, seleccionarla en la lista de reglas disponibles y haga un clic en los botones *Editar* o *Excluir*.



Intertravamento

Adicionar Editar Excluir

Selecione o campo +

Sem filtros aplicados

ID	ID
1	

<< < 1 > >>

Importante: esta funcionalidad sólo está disponible para controladoras de línea CT 500 Intelbras.

7. Informes

Informes son informaciones gerenciales del sistema de control de acceso de tal forma que los eventos de acceso, alarmas, aberturas remotas se pueden consolidar y eventualmente exportar a archivos en Excel para un posterior análisis.

7.1. Eventos de usuarios

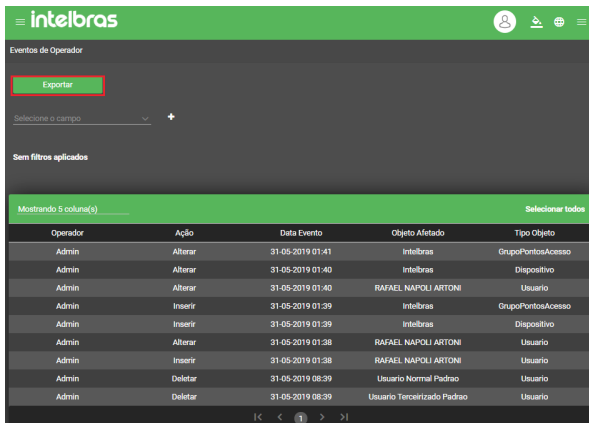
Eventos de usuario son todas las informaciones relativas a los puntos de acceso (puertas), es decir, accesos liberados, accesos negados, intentos de acceso desconocidos, eventos de alarmas, aberturas remotas, etc.

En la pantalla inicial se exhiben todas las informaciones referentes a los puntos de acceso (puerta) y para exportar las informaciones a un archivo en Excel, haga un clic en el botón *Exportar*.

intelbras					
Eventos de Usuário					
Exportar					
Selecione o campo					
Sem filtros aplicados					
Mostrando 6 coluna(s)					
Nome do usuário	Tipo	Nome do Dispositivo	Data Evento	Tipo de evento	Observações
Usuário desconhecido	Credencial desconhecida	CT 500 4 PB	15-07-2019 14:12:03.000	Acesso Negado	
Usuário desconhecido	Credencial desconhecida	CT 500 4 PB	15-07-2019 14:12:03.000	Acesso Negado	
Douglas de Moraes	Cartão	CT 500 4 PB	15-07-2019 14:11:59.000	Acesso Liberado	
Usuário desconhecido	Credencial desconhecida	CT 500 4 PB	15-07-2019 14:11:56.000	Acesso Negado	
Usuário desconhecido	Credencial desconhecida	CT 500 4 PB	15-07-2019 14:11:53.000	Acesso Negado	
Usuário desconhecido	Credencial desconhecida	CT 500 4 PB	15-07-2019 14:11:53.000	Acesso Negado	
Usuário desconhecido	Credencial desconhecida	CT 500 4 PB	15-07-2019 14:11:53.000	Acesso Negado	

7.2. Eventos de operadores

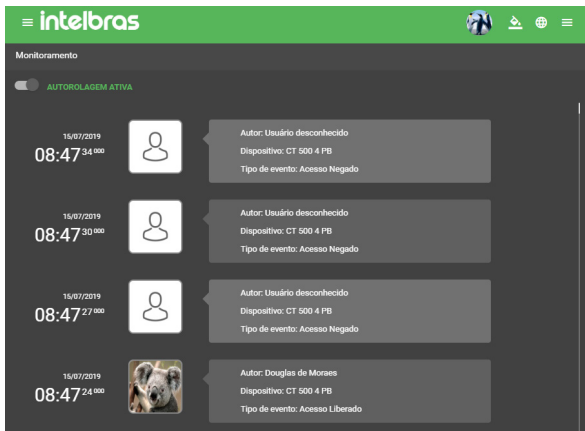
Esta sección exhibe en la pantalla inicial todos los eventos, es decir, acciones ejecutadas por los Operadores del sistema. Esas informaciones se pueden exportar a un archivo en Excel para posteriores consultas. Para eso, haga un clic en el botón *Exportar* para generar el archivo.



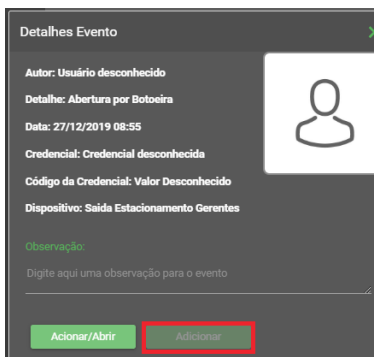
Operador	Ação	Data Evento	Objeto Afetado	Tipo Objeto
Admin	Alterar	31-05-2019 01:41	Intelbras	GrupoPontosAcesso
Admin	Alterar	31-05-2019 01:40	Intelbras	Dispositivo
Admin	Alterar	31-05-2019 01:40	RAFAEL NAPOLI ARTONI	Usuario
Admin	Inserir	31-05-2019 01:39	Intelbras	GrupoPontosAcesso
Admin	Inserir	31-05-2019 01:39	Intelbras	Dispositivo
Admin	Alterar	31-05-2019 01:38	RAFAEL NAPOLI ARTONI	Usuario
Admin	Inserir	31-05-2019 01:38	RAFAEL NAPOLI ARTONI	Usuario
Admin	Deletar	31-05-2019 08:39	Usuario Normal Padrao	Usuario
Admin	Deletar	31-05-2019 08:39	Usuario Terceirizado Padrao	Usuario

7.3. Monitorio

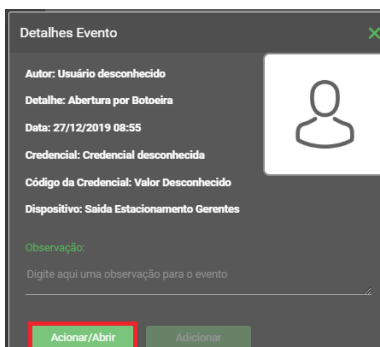
En esta sección se presentan todos los eventos de acceso del sistema, de tal forma que el operador puede seguir las informaciones en tiempo real; también se exhiben, vinculadas al evento de acceso de los usuarios, sus respectivas fotos, que se registraron en sus perfiles, para auxiliar en la identificación de ellos.



Es posible agregar una observación en el evento. Para eso, basta efectuar un doble clic sobre el evento deseado y, en la nueva ventana, insertar las informaciones pertinentes sobre el evento de acceso y hacer un clic en el botón *Agregar* para guardar las observaciones insertadas.



En esta pantalla también es posible efectuar una abertura remota en la puerta controlada por el dispositivo de control de acceso en cuestión. Para eso, haga un clic en el botón *Agregar / Abrir* para efectuar la abertura de la puerta remotamente.



8. Sistema

En esta sección se citan las funciones que proporcionan la configuración general del sistema en lo que dice respecto al Gerenciamiento de base de datos y configuración de los campos personalizados del registro de usuario.

8.1. Gerenciamiento de base de datos

En esta sección es posible visualizar la instancia de la base de datos activa para la base de datos del software. Para eso, en la pantalla inicial, haga un clic en el botón *Visualizar*.

Gerenciamiento de Banco de Datos

Visualizar

Seleccione o campo

Sem filtros aplicados

Mostrando 8 coluna(s)

Banco	Nome	Porta	Senha	Usuário	Ip	Conectado	Online
PostgreSQL	backend	4440	postgres	postgres	localhost	Sim	Sim

Navegadores Suportados

En el ícono de engranaje es posible seleccionar dos opciones referentes a la base de datos:

- » Efectuar Backup;
- » Restaurar Base de datos.

Al seleccionar la opción *Efectuar backup* se cargará un archivo compactado en su computadora. Basta seguir este proceso y guardar el archivo compactado en una carpeta del servidor.

Gerenciamento de Banco de Dados

Visualizar

Efetuar backup

Restaurar banco de dados

Selecione o campo

Sem filtros aplicados

Banco	Nome	Porta	Senha	Usuário	Ip	Conectado	Online
PostgreSQL	backend	4440	postgres	postgres	localhost	Sim	Sim

Navegadores Suportados:

InControl - intelbras S/A todos os direitos reservados.

Departamentos
Visitantes
Credenciais
Operadores
Perfis de Operador
Dispositivos
Áreas
Dispositivos
Controle de Acesso
Relatórios
Sistema
Gerenciamento de Banco de Dados
Configurações

Gerenciamento de Banco de Dados

Visualizar

⚙️

Selecione o campo

Sem filtros aplicados

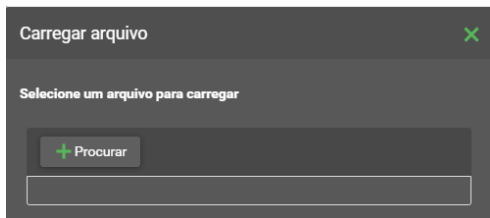
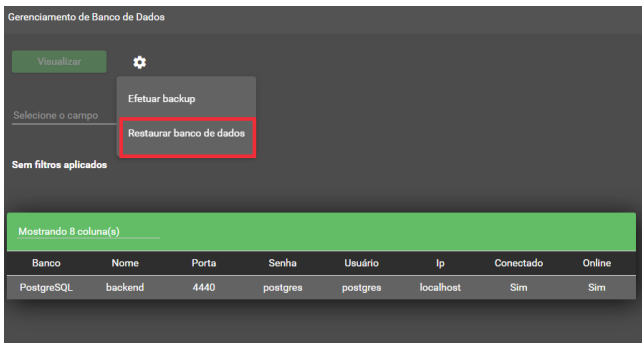
Banco	Nome	Porta	Senha	Usuário	Ip	Conectado	Online
PostgreSQL	backend	4440	postgres	postgres	localhost	Sim	Sim

Navegadores Suportados

versão: 0.14.02

arquivo2019-07-12.zip

Para restaurar una base de datos, seleccione la opción Restaurar base de datos y, en la nueva ventana, cargue el archivo compactado puesto a disposición en la etapa de backup.



Tras la selección del archivo, siga la progresión del proceso y verifique si los datos están de acuerdo con los datos del momento en que se hizo el backup del banco.

Importante:

- » La restauración de la base de datos sólo se puede hacer al cargar el archivo compactado entero.
- » No es posible crear una nueva instancia para la base de datos sin efectuar la desinstalación del software completamente.

8.2. Configuraciones

En esta función será posible nombrar los campos personalizados que están disponibles en el registro de usuarios. Para eso, en la pestaña *Configuração estándar*, basta llenar los nombres en los campos personalizados disponibles.

Configurações

Campos personalizados Padrão do cartão Configurações de backup Câmeras de Monitoramento

Configuração de campos personalizados

Nome do campo
Campo personalizado 1

Nome do campo
Campo personalizado 2

Nome do campo
Campo personalizado 3

Nome do campo
Campo personalizado 4

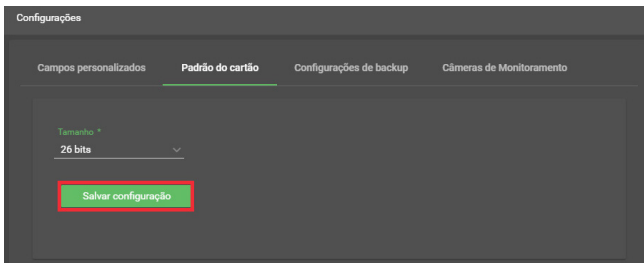
Nome do campo
Campo personalizado 5

Salvar configuração

En la pestaña *Estándar de la tarjeta* se puede definir el tipo de lectura que se considerará estándar del sistema. Las opciones son:

- » 26 bits;
- » 34 bits.

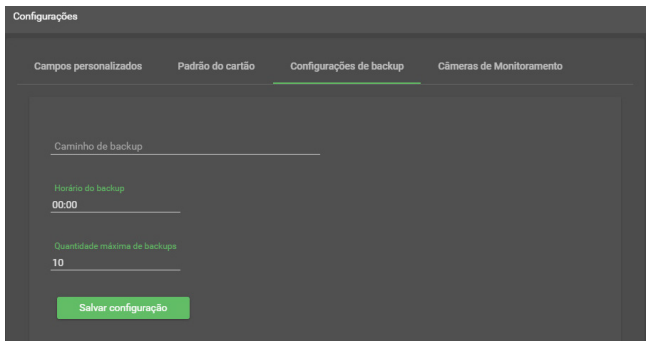
Tras la definición es necesario hacer un clic en el botón Guardar configuración para finalizar el proceso.



En la pestaña Configuraciones de backup es posible configurar los siguientes parámetros para el backup de la base de datos:

- » Camino de backup: lugar donde se guardarán los archivos de backup de la base de datos comúnmente.
- » Horario del backup: horario de inicio de la rutina de backup de la base de datos.
- » Cantidad máxima de backups: cantidades de archivos de backups que el sistema generará.

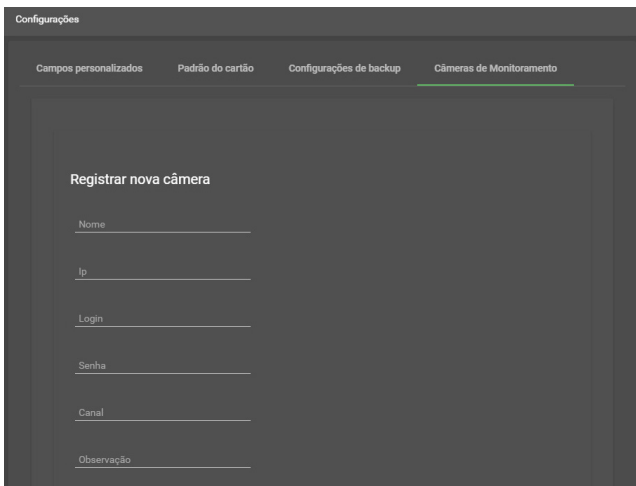
Al final, haga un clic en la opción Guardar la configuración para concluir las configuraciones de backup.



Es posible registrar las cámaras de monitoreo del ambiente en el sistema para que posteriormente se pueda hacer la captura de las imágenes de usuarios y vehículos. Para eso, en la pestaña *Câmeras de monitor*eo, inserte las informaciones demandadas:

- » Nombre de la cámara (limitado a 10 cámaras);
- » Dirección de IP;
- » Login;
- » Clave;
- » Canal;
- » Observación.

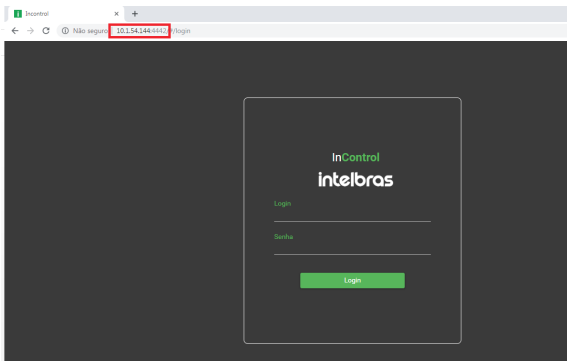
Para salvar las configuraciones haga un clic en el botón *Agregar câ*mera.



The screenshot displays a web interface with a dark theme. At the top, a header bar contains the word 'Configurações'. Below this, a navigation bar features four tabs: 'Campos personalizados', 'Padrão do cartão', 'Configurações de backup', and 'Câmeras de Monitoramento'. The 'Câmeras de Monitoramento' tab is currently selected, indicated by a green underline. The main content area is titled 'Registrar nova câmara' and contains a vertical list of six input fields, each with a label to its left: 'Nome', 'Ip', 'Login', 'Senha', 'Canal', and 'Observação'. The fields are empty and have a light gray border.

8.3. Acceso via web

El Software InControl es un software web, lo que posibilita acceder al software instalado en el servidor de forma práctica y rápida vía navegador web. Para eso, en la pantalla principal del navegador web, inserte la dirección de IP de la máquina Servidor en que Incontrol está rodando y su respectiva puerta.

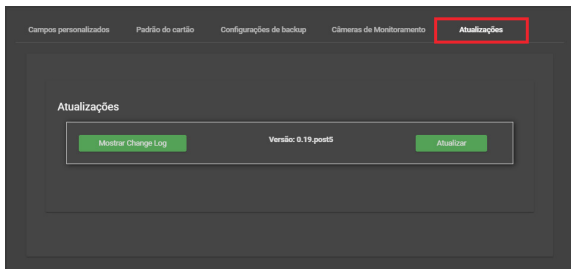


Para acceder y hacer el login utilice las credenciales de operadores que forman parte de la misma base de datos de la instancia activa en el servidor del software.

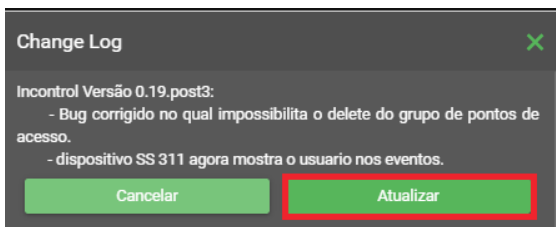
Importante: es necesario que la máquina Cliente esté en la misma red (LAN) del servidor del software.

8.4. Actualizaciones

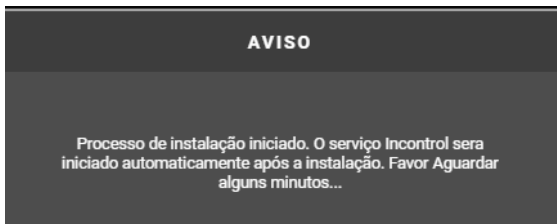
Haga clic en la pestaña de Actualizar el sistema verificara si existe una nueva versión disponible, las actualizaciones incluyen mejoras, nuevas funciones y corrección de bug s. Es recomendado siempre mantener el sistema actualizado en su última versión.



Caso exista alguna actualización disponible, seleccione la opción *Mostrar Change Log* para consultar la lista con las mudanzas de esta versión, presione el botón *Atualizar* para iniciar el proceso.



Después presione en actualizar el sistema y reiniciara automáticamente, el proceso de actualización puede demorar algunos minutos variando de acuerdo con algunos factores como la velocidad de conexión y recursos del servidor.



Importante: antes de realizar la actualización, es recomendado realizar el backup del banco de dados como recomendado en este documento.

Política de privacidad

Esta es la Política de privacidad ("Política") que se firma entre usted, de ahora en adelante denominado Usuario, e Intelbras S/A - Indústria de Telecomunicação Eletrônica Brasileira, persona jurídica de derecho privado, inscrita en el "CNPJ/MF" [Registro Nacional de Persona Jurídica / Ministerio de Hacienda] con el nº 82.901.000/0001-27, establecida en la carretera BR 101, km 210, Área Industrial, São José/SC, representando, en este acto, todas sus filiales, de ahora en adelante denominada INTELBRAS. Esta Política se proyectó para regular la recolección, el almacenamiento, el uso y el compartimiento de informaciones compartidas con INTELBRAS. Al aceptar esta Política, el Usuario reconoce que analizó y está de acuerdo con las condiciones descritas, y permite que INTELBRAS recoja, almacene, use y comparta sus informaciones de acuerdo con los términos de esta Política, así como manifiesta conocimiento de que la Política se puede modificar, a cualquier momento, con todas las actualizaciones publicadas en esta página. Si el usuario es menor de edad o incapaz en cualesquiera aspectos, necesitará el permiso de sus padres o responsables, que también deberán estar acuerdo con la Política y sus condiciones.

Cualquier duda con relación a la Política de Privacidad se puede aclarar en los contactos:

E-mail: *privacidade@intelbras.com.br*

1. Recolección de informaciones

Al utilizar el software que INTELBRAS pone a disposición, el Usuario está consciente de que INTELBRAS podrá recoger las informaciones de acceso y de registro, tales como nombre, teléfono, e-mail y dirección, de acuerdo con lo descrito en esta Política.

Las informaciones se pueden clasificar en dos tipos: personales y no personales. Informaciones personales son datos que están relacionados al Usuario y que permiten su identificación, incluyendo, pero sin limitarse al nombre, fecha de nacimiento, dirección de contacto, número de contacto, dirección de e-mail y archivos de contenido en vídeo que pueden contener informaciones de identidad visual personal.

Informaciones no personales son datos que no establecen ninguna relación con un individuo específico, como ocupación, idioma, código de área, números de serie del producto, URLs, comportamiento del usuario, archivos de contenido en vídeo que no contengan informaciones de identidad visual personales, etc.

2. Almacenamiento de informaciones personales

De acuerdo con lo estipulado en la Política, INTELBRAS almacenará sus informaciones personales por determinado período de tiempo y utilizará las tecnologías disponibles para evitar la pérdida de datos, el uso indebido, la divulgación no autorizada y otros problemas relativos a la seguridad de la información, y también realizará una revisión periódica de la eficacia de los actuales métodos de almacenamiento y tratamiento, incluyendo precauciones de seguridad física, para evitar el acceso no autorizado.

INTELBRAS posee las mejores prácticas, incluyendo tecnologías y estrategias razonables para la protección de los datos, pero INTELBRAS no puede garantizar que sus informaciones personales estén bajo seguridad absoluta, teniendo en vista la tecnología de seguridad de la información existente. El Usuario reconoce que INTELBRAS no se responsabiliza por cualesquiera pérdidas en caso que sus informaciones personales sean reveladas, hurtadas o robadas por motivo de fuerza mayor o problemas de seguridad que no hayan sido causados por INTELBRAS.

3. Uso de informaciones personales

A fin de proporcionar una mejor experiencia al usuario, INTELBRAS podrá usar sus informaciones personales para los siguientes propósitos:

- » Hacer viable el uso del software con todas sus soluciones y funcionalidades, almacenando el historial necesario para su funcionamiento y mejor experiencia del Usuario.
- » Aumentar la seguridad del aplicativo y de otros servicios prestados por INTELBRAS, tales como autenticación de usuarios, protección de seguridad, detección de fraudes, archivo y backups.
- » A menos que el Usuario opte por cancelar la inscripción, INTELBRAS podrá contactarlo enviando comunicaciones electrónicas para informar sobre nuevos productos y servicios. INTELBRAS también podrá utilizar informaciones personales para fines internos, tales como auditorías, análisis de datos e investigaciones.

4. Compartimiento de informaciones personales

INTELBRAS no divulgará sus informaciones personales, a menos que (i) tenga su consentimiento previo por escrito; (ii) esté de acuerdo con las leyes y reglamentos aplicables o exigidos por las autoridades; (iii) esté obligada por decisión judicial; (iv) esté de acuerdo con los términos de la Política; (v) sea esencial para la protección de los intereses legítimos de INTELBRAS.

INTELBRAS podrá permitir que sus funcionarios accedan a los datos en ocasiones específicas con base en la necesidad de conocimiento, y asegurará que cumplan las obligaciones en el mismo nivel establecido por la Política.

Además, la INTELBRAS puede poner a disposición ciertas informaciones a aliados estratégicos confiables que ocasionalmente trabajen con INTELBRAS para proporcionar una mejor experiencia al Usuario y aumentar la calidad de los servicios del software. Bajo esas circunstancias, la aceptación de la Política significa que el Usuario está de acuerdo y autoriza a INTELBRAS a suministrar sus informaciones a tales terceros.

5. Ámbito de aplicación

Esta Política dice respecto a todos los aplicativos, sitios y otros servicios prestados por INTELBRAS, excepto cuando esté indicado de otra forma.

Los sitios de INTELBRAS pueden contener links para servicios suministrados por terceros. Las informaciones de los usuarios pueden ser recogidas por terceros en el momento del uso de estos links, por lo tanto, INTELBRAS recomienda que el Usuario conozca sus prácticas de privacidad.

Las informaciones no personales no se rigen por la Política; además, usted está de acuerdo que INTELBRAS tiene el derecho de recoger, almacenar, usar y compartir sus informaciones no personales para cualesquiera y todos los fines, incluyendo, sin limitación:

- » Entender el comportamiento del usuario, a fin de optimizar su experiencia, perfeccionar el diseño funcional y suministrar mejores servicios;
- » Analizar la base de datos, en parte o en su totalidad, para fines comerciales, incluyendo, pero sin limitarse a: análisis de datos y uso de los datos obtenidos a partir del número de visitas del usuario, período de las visitas, preferencias del usuario y otros datos.

6. Cookies y tecnologías semejantes

INTELBRAS usa cookies (pequeños archivos de texto insertados en el dispositivo del usuario) y tecnologías semejantes para suministrar servicios online y sitios y ayudar a recoger datos. Los cookies almacenan las preferencias y configuraciones del usuario, permitiendo, entre otras acciones: iniciar la sesión rápidamente, identificar los intereses de los usuarios y promover anuncios con base en esos intereses, combatir fraudes y analizar el desempeño de sitios y servicios online.

INTELBRAS usa web beacons para ayudar a enviar cookies y reunir datos de desempeño. Los sitios pueden incluir web beacons y cookies de proveedores de servicios de terceros.

El usuario tiene a su disposición una variedad de herramientas para controlar los cookies, web beacons y tecnologías semejantes, incluyendo controles de navegador para bloquear y eliminar cookies y controles de proveedores de servicios de análisis de terceros para rechazar la recolección de datos a través de web beacons y tecnologías semejantes. El navegador y otras elecciones del usuario pueden tener impacto en sus experiencias con el uso de este aplicativo, software o servicio.

7. Actualizaciones en la Política de Privacidad

Esta Política pasa por constantes actualizaciones, así, INTELBRAS recomienda revisar periódicamente esta página para seguir y estar consciente de las modificaciones. En caso que se hagan modificaciones relevantes en los términos de esta Política, INTELBRAS publicará la nueva Política, notificando al Usuario.

Si usted sospecha que sus informaciones personales se están recogiendo o utilizando de manera ilegal, o que cualquier regla de esta Política se está infringiendo de cualquier manera, entre en contacto con INTELBRAS, inmediatamente, a través del sitio www.intelbras.com.br o e-mail privacidade@intelbras.com.br.

Términos de utilización de software

1. Aceptación del contrato

Este es un contrato celebrado entre usted, en adelante denominado USUARIO, e Intelbras S/A – Indústria de Telecomunicação Eletrônica Brasileira, persona jurídica de derecho privado, inscrita en el CNPJ/MF bajo el n° 82.901.000/0001-27, establecida en la rodovia BR 101, km 210, Área Industrial, São José/SC, y en adelante denominada simplemente Intelbras. Estos Términos de utilización de servicio rigen la utilización del servicio hecho disponible gratuitamente por Intelbras y/o sus asociados, denominado INTELBRAS INCONTROL WEB, desarrollado para computadoras en LAN. En el caso de que usted no esté de acuerdo con los términos no utilice ese servicio. Léalos con atención, porque si usted empezó a utilizar el servicio, se configurará que aceptó todos los términos y está de acuerdo en cumplirlos. Si usted, usuario, es menor de edad o declarado incapaz en cualesquier aspectos, necesitará el permiso de sus padres o responsables, que también deberán estar de acuerdo con estos mismos términos y condiciones.

2. Licencia limitada

Usted recibió una licencia limitada, no transferible, no exclusiva, libre de royalties y revocable, para descargar, instalar, ejecutar y utilizar ese servicio en su dispositivo. Usted reconoce y está de acuerdo que Intelbras concede al usuario una licencia exclusiva para uso y, de esta forma, no le transfiere los derechos sobre el producto. Se deberá utilizar el servicio por usted, usuario. La venta, transferencia, alteración, ingeniería inversa o distribución, así como la copia de textos, imágenes o cualesquier ítems contenidos en el software son expresamente prohibidas. Usted reconoce que Intelbras es propietaria de todos los derechos, títulos e intereses referentes a INTELBRAS INCONTROL WEB y al software relacionado. INTELBRAS INCONTROL WEB es la marca comercial o registrada de Intelbras. Usted no puede alterar, destruir, ocultar o remover de otra forma cualquier las informaciones sobre derecho de autor, los rótulos o avisos de propiedad de los softwares de Intelbras.

3. Del Registro

Para el acceso al software es necesario que el USUARIO realice un registro previo en que suministre voluntariamente informaciones sobre sí, tales como: USUARIO, contraseña, dirección de correo electrónico ("Datos"). El USUARIO declara que los Datos suministrados son exactos y verdaderos y se compromete a mantener sus datos siempre actualizados.

INTELBRAS no es responsable por las informaciones suministradas, pero se reserva el derecho de verificar, a cualquier momento, la veracidad de tales informaciones y solicitar, a su exclusivo criterio, la documentación soporte que sea necesaria para la debida comprobación de las informaciones suministradas. En el caso de que INTELBRAS detecte alguna cuenta creada a partir de informaciones falsas, el catastro del USUARIO será automáticamente cancelado de forma que el USUARIO no tendrá más acceso al uso de los Servicios, no teniendo el USUARIO, por este motivo, cualquier derecho a indemnización o resarcimiento.

El titular y administrador de la cuenta será aquel definido en el momento del registro, a partir de los Datos ofrecidos por el USUARIO. La cuenta es persona y podrá ser accedida únicamente mediante la utilización del USUARIO y contraseñas creados por el propio USUARIO, en el momento del catastro, siendo este el único y exclusivo responsable por mantener el sigilo de su USUARIO y contraseña, a fin de asegurar la seguridad de su cuenta e impedir el acceso no autorizado por terceros. El USUARIO es el único responsable por todas las actividades asociadas a su cuenta.

El USUARIO deberá seguir los estándares de seguridad de registro de contraseña y realizar el cambio inmediato de la contraseña estándar.

4. Derechos de autor

El USUARIO no adquiere, por el presente instrumento o por la utilización del SOFTWARE, cualquier derecho de propiedad intelectual u otros derechos exclusivos, incluso patentes, diseños, marcas, derechos de autor o cualesquier derechos sobre informaciones confidenciales o secretos comerciales, así como sobre el contenido hecho disponible en el software, inclusive, pero no se limitando, a textos, gráficos, imágenes, logotipos, iconos, fotografías, contenido editorial, notificaciones, softwares y cualquier otro material, sobre INTELBRAS o relacionados a él o a cualquier parte de él. El USUARIO también no adquiere cualquier derecho sobre el SOFTWARE o relacionado a él o a cualquier de sus componentes, además de los derechos expresamente licenciados al USUARIO en este Término o en cualquier otro contrato mutuamente celebrado por escrito entre las partes.

Al utilizar el SOFTWARE, el USUARIO está de acuerdo en cumplir con los alineamientos a continuación:

- I. No se permite publicar o transmitir información, dato, texto, software, gráficos, sonidos, fotografías, videos, mensajes y otro contenido que sea ilegal, ofensivo, inexacto, difamatorio, obsceno, fraudulento, perjudicial, amenazador o abusivo.
- II. No interferir en la utilización de otros usuarios del SOFTWARE.
- III. No publicar o realizar upload de cualquier virus, worms, fichero corrompido u otro software capaz de perturbar, incapacitar o perjudicar el funcionamiento del SOFTWARE.
- IV. Cumplir con este Término y cualesquier leyes o reglamentos aplicables;
- V. No se pasar por cualquier persona o entidad, declarar falsamente o deturpar su afiliación con una persona o entidad.
- VI. No enviar o transmitir contenido que el USUARIO no posee derecho de publicar o transmitir bajo cualquier ley o bajo relaciones contractuales o fiduciarias (tales como información privilegiada, informaciones confidenciales, etc.).
- VII. No usar el SOFTWARE para solicitar, obtener o almacenar datos personales o contraseñas de otros usuarios.

5. Alteraciones, modificaciones y rescisión

Intelbras se reserva el derecho de, a cualquier tiempo, alterar estos términos, ya sea incluyendo, removiendo o alterando cualesquier de sus cláusulas. Tales modificaciones tendrán efecto inmediato tras la publicación. Al seguir con el uso del servicio, usted aceptará y estará de acuerdo en cumplir los términos alterados. Como también Intelbras puede, de cuando en cuando, modificar o discontinuar (temporal o permanentemente) la distribución o la actualización de ese servicio. El USUARIO no podrá responsabilizar Intelbras ni sus directores, ejecutivos, funcionarios, afiliados, agentes, contratados o licenciadores por cualesquier modificaciones, suspensiones o discontinuidad del servicio.

Para fines contractuales, el USUARIO está de acuerdo en recibir comunicaciones de INTELBRAS de forma electrónica (términos y condiciones, acuerdos, notificaciones, divulgaciones y otras comunicaciones de INTELBRAS), ya sea por correo electrónico o comunicación interna en el propio SOFTWARE y que, así establecida, las comunicaciones de INTELBRAS satisfacen y cumplen con los requisitos legales, como se fuera en vía impresa.

6. Indemnización

En ningún caso, INTELBRAS será responsable por daños personales o cualquier perjuicio incidental, especial, indirecto o consecuente, inclusive, sin limitación, perjuicios por pérdida de utilidad, corrupción o pérdida de datos, falla de transmisión o recepción de datos, no continuidad del negocio o cualquier otro perjuicio o pérdida comercial, provenientes o relacionados al uso del SOFTWARE o a su inhabilidad en usar el SOFTWARE, por cualquier motivo.

7. Consentimiento para colecta y protección del uso de datos

El USUARIO está de acuerdo que INTELBRAS puede coleccionar los datos personales de catastro y perfil, y usar datos técnicos de su dispositivo, tales como especificaciones, configuraciones, versiones de sistema operativo, tipo de conexión a internet y afines.

Los datos personales coleccionados del USUARIO serán exclusivamente utilizados para fines de ejecución del presente contrato, con el objetivo principal de activación de las funcionalidades del SOFTWARE, siendo que el uso de estos datos es intrínseco al propio funcionamiento del SOFTWARE, y para uso y beneficios del titular. También, algunos recursos del SOFTWARE podrán solicitar datos adicionales del USUARIO, tales como, nombre, teléfono, dirección, funcionarios, instaladores, servicios prestados, región de atención, entrenamientos realizados, clientes atendidos, y todos los otros datos vinculados a su actividad comercial. La aceptación del USUARIO al presente Contrato desde ya autoriza INTELBRAS a indicar el USUARIO como asociado de INTELBRAS y publicar los datos públicos de contacto en los sitios, softwares y demás medias sociales de INTELBRAS, de conformidad con la previsión del Manual del Programa de Canales y demás políticas definidas por INTELBRAS y compartidas previamente con el USUARIO.

En el desarrollo de cualesquier actividades relacionadas con la ejecución del presente Contrato, las Partes observan el régimen legal de protección de datos personales, se empeñando en proceder a todo el tratamiento de datos personales que sea necesario al desarrollo del Contrato en el estricto y riguroso cumplimiento de la Ley.

Los datos personales aquí listados son considerados los datos de las propias Partes o mismo los datos personales de sus colaboradores, contratados o subcontratados.

A fin de asegurar la protección de los datos, el USUARIO se obliga a:

- a. Tratar y utilizar los datos personales de INTELBRAS o de sus ASOCIADOS en los términos legalmente permitidos, en especial los colectando, registrando, organizando, conservando, consultando o transmitiendo, única y solamente en los casos en que su titular tuviera permitido el consentimiento expreso e inequívoco, o en los casos legalmente previstos;
- b. Tratar los datos de forma compatible con las finalidades para los cuales hayan sido colectados;
- c. Conservar los datos solamente durante el período necesario a la persecución de las finalidades de la colecta o del tratamiento posterior, asegurando su confidencialidad;
- d. Implementar las medidas técnicas y organizativas necesarias para proteger los datos contra la destrucción, accidental o ilícita, la pérdida accidental, la alteración, la difusión o el acceso no autorizado, así como contra cualquier otra forma de tratamiento ilícito de ellos;
- e. Informar inmediatamente INTELBRAS, debiendo prestar toda la colaboración necesaria a cualquier investigación que se realice, en el caso de que haya alguna quiebra de seguridad, o sospecha de tal, independientemente de colocar o no en causa la seguridad e integridad de los datos personales;
- f. Asegurar el ejercicio, por los titulares, de los respectivos derechos de información, acceso y oposición;
- g. Asegurar que sus colaboradores, contratados o subcontratados que tengan acceso a datos personales en el contexto de este Contrato cumplan las disposiciones legales aplicables en materia de protección de datos personales, y las disposiciones contractuales aquí listadas, no cediendo, vendiendo, compartiendo o divulgando tales datos a terceros, ni de ellos hacer uso para cualesquier fines que no los estrictamente consentidos por los respectivos titulares.

El USUARIO será responsable ante INTELBRAS o terceros en el caso de cualquier violación, compartimiento, exclusión, cesión, venta, alteración automática de los datos sin previo y expreso consentimiento de su titular.

8. Marcas Registradas y Derechos de Propiedad Intelectual de Intelbras

El USUARIO reconoce que las "Marcas Registradas" y los "Derechos de Propiedad Intelectual" de INTELBRAS representan uno de los activos estratégicos de INTELBRAS siendo de exclusiva propiedad de ella.

Durante la vigencia de este Término, se concederá al USUARIO el derecho de uso no exclusivo de las Marcas Registradas y otros Derechos de Propiedad Intelectual de INTELBRAS, siendo que el USUARIO deberá utilizarlos estrictamente de conformidad con el (i) "Manual de la Marca Intelbras"; y (ii) cualesquier otras instrucciones recibidas de INTELBRAS. El LICENCIADO también asegura que sus actividades de propaganda y promocionales cumplan con el (i) Manual de la Marca Intelbras; (ii) Programa de Canales Intelbras; y (iii) y la legislación aplicable.

El USUARIO no podrá registrar cualesquier Derechos de Propiedad Intelectual de INTELBRAS, tales como cualquier palabra, símbolo, marca de identificación o nombre semejante a las Marcas Registradas de INTELBRAS o nombre de dominio durante la vigencia de este contrato o mismo tras su término.

Todo y cualquier derecho del USUARIO de utilizar las Marcas Registradas y otros Derechos de Propiedad Intelectual de INTELBRAS cesará automáticamente cuando del cierre del presente término.

El USUARIO deberá prontamente notificar INTELBRAS, por escrito, de cualquier sospecha de uso no autorizado o infracción a los Derechos de Propiedad Intelectual de INTELBRAS y tengan conocimiento. Si solicitado por INTELBRAS, el USUARIO deberá auxiliar INTELBRAS en cualesquier investigaciones, negociaciones o procedimientos judiciales en virtud de cualquier alegación de uso indebido o de violación a los Derechos de Propiedad Intelectual de INTELBRAS.

El USUARIO se compromete a no realizar cualquier tipo de anuncio, propaganda, material publicitario de los Productos Intelbras, contemplando precios y condiciones de pago vinculando productos INTELBRAS con productos de competidores, debiendo tales propagandas ser realizadas de forma separada, sin vínculo de cualquier producto competidor. INTELBRAS recomienda que el USUARIO no realice correo el lote en que haya precios de los productos.

Se prohíbe la copia o cualquier otra forma de reproducción de tales informaciones, manuales, literatura, técnica y otros documentos suministrados por INTELBRAS, excepto para el cumplimiento de obligaciones establecidas en los términos de este instrumento, y de conformidad con la legislación aplicable relativamente a derechos de autor y propiedad intelectual.

Las obligaciones establecidas en la presente cláusula obligan al USUARIO durante la vigencia del presente instrumento, así como tras su término o rescisión mantenimiento de la confidencialidad.

9. Exención de garantías y limitaciones de responsabilidad

Ese servicio estará en desarrollo continuado y puede contener errores, por eso, el uso es suministrado “en el estado en que se encuentra” y bajo riesgo del usuario final. En la extensión máxima permitida por la legislación aplicable, INTELBRAS y sus suministradores se exentan de cualesquier garantías y condiciones expresas o implícitas inclusive, sin limitación, garantías de comercialización, adecuación a un propósito específico, titularidad y no violación con respecto al servicio y a cualquier uno de sus componentes o, aún, a la prestación o no de servicios de soporte. INTELBRAS no asegura que la operación de ese servicio sea continuada y sin defectos. Excepto por el establecido en este documento, no existen otras garantías, condiciones o promesas vinculadas al servicio, expresas o implícitas, y todas esas garantías, condiciones y promesas pueden ser excluidas de conformidad con lo que se permite en ley sin perjuicio a Intelbras y a sus colaboradores.

I. INTELBRAS no asegura, declara o garantiza que el uso de esos servicios no será interrumpido o libre de errores y usted está de acuerdo que Intelbras podrá remover por períodos indefinidos o cancelar ese servicio a cualquier momento sin que usted sea avisado.

II. INTELBRAS no garantiza, declara ni asegura que ese servicio esté libre de pérdida, interrupción, ataque, virus, interferencia, piratería u otra amenaza a la seguridad y se exenta de cualquier responsabilidad con respecto a esas cuestiones. Usted es responsable por el backup de los ficheros almacenados en su dispositivo.

III. En ningún caso, INTELBRAS, así como sus directores, ejecutivos, funcionarios, afiliadas, agentes, contratados o licenciadores serán responsables por pérdidas o daños causados por el uso del servicio.

10. Validez técnica

Se establece que INTELBRAS, sus suministradores o distribuidores no ofrecen un período de validez técnica del SOFTWARE. No se puede considerar que el programa esté exento de errores, que su funcionamiento no sea interrumpido o que sus funciones satisfagan los requisitos de los usuarios, motivo por el cual se establece, de forma expresa, que el licenciado lo utiliza por su cuenta y riesgo. Debido a la complejidad de la relación entre software y hardware, INTELBRAS no asegura que el SOFTWARE INTELBRAS INCONTROL WE será compatible con todos los sistemas de software y hardware, que operará correctamente o atender a sus expectativas.

11. Foro para dirimir controversias

Estos Términos de uso serán regidos e interpretados de conformidad con las leyes de Brasil. Las partes se someten a la jurisdicción exclusiva de los tribunales de Brasil. Para dirimir eventuales dudas sobre el presente instrumento, así como de cualquier evento relacionado a la utilización de nuestros servicios, se elige desde ya el foro de la comarca de São José, estado de Santa Catarina, por más privilegiado que otro foro sea. Si usted posee todavía alguna duda sobre la forma de utilización de nuestro producto, sobre nuestros Términos de uso o sobre nuestra Política de privacidad, entre en contacto con Intelbras. Será un placer atenderle.

intelbras



fale com a gente / hable con nosotros

Brasil

Suporte a clientes: (48) 2106 0006

Fórum: forum.intelbras.com.br

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

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

SAC: 0800 7042767

Onde comprar? Quem instala?: 0800 7245115

México

Contactos para clientes en México:

suporte.tec@intelbras.com.mx

Otros países

suporte@intelbras.com

Produzido por: / Producido 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

02.20

Indústria brasileira
Industria brasileña