Sistema de Controle de Acesso
IPX-S-SWACSS

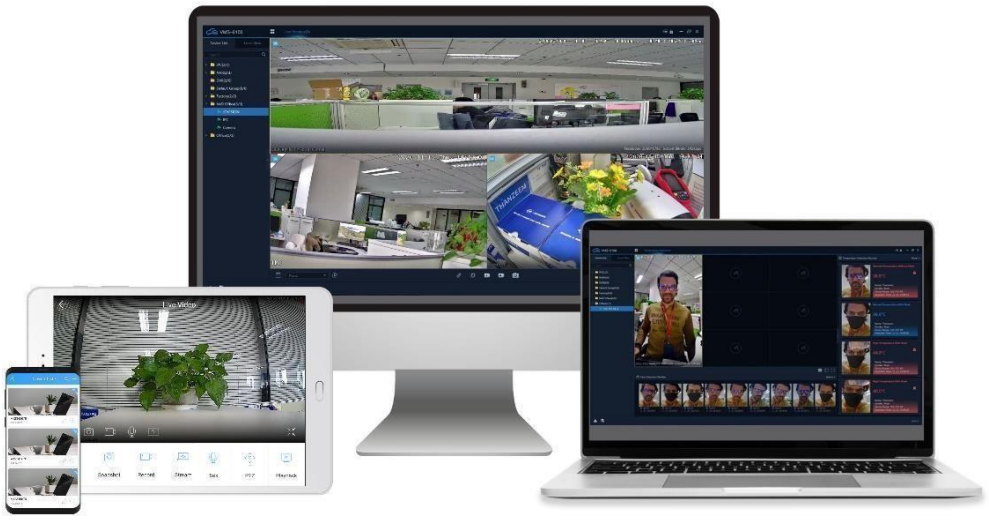

*Imagem ilustrativa.

Visão Geral

O Sistema de Gerenciamento de Controle de Acesso da INPEX foi desenvolvido para atender as exigências do mercado nacional e clientes de todos os tamanhos e ramos de atividade.

Sua principal característica é o poder de customização o que o torna adaptável a qualquer ramo de negócio como se fosse um produto desenvolvido sobre medida para sua empresa.

Com ele é possível criar diferentes tipos de usuários, layouts customizáveis com regras de validações especiais, relatórios e gráfico customizáveis, mapas de monitoramento, etc.

Um sistema único e escalável feito para crescer junto com seu negócio ou no seu ritmo. Podendo começar controlando uma pequena área com alguns usuários e crescer até controlar milhares de leitores e centenas de milhares de usuários com o mesmo sistema.

Integre nosso sistema com outros sistemas de segurança (CFTV, Incêndio, Alarme, etc.), controle (Elevadores, Automação, etc.) ou gestão (RH, Restaurante, Segurança do Trabalho, Veículos, Active Directory, etc.)

Compartilhe informações com outros sistemas e automatize a tomada de decisões.

Extraia informações através de relatórios customizados e obtenhas informações em tempo real através do monitor de alarmes e dashboards customizados.

Conta com os principais métodos de acesso do mercado, podendo-se citar os Cartões de Proximidade, Tags UHF, Reconhecimento Biométrico, Reconhecimento Facial, QR Code, entre outros.

Possui uma visão geral de todos os acessos por meio de logs e diretorias, dos usuários que possuem cadastro temporário, ou não, seja esse contendo acesso físico ou veicular.

Extensões

- Arquivos e relatórios, em geral, podem ser exportados, importados e visualizados nas principais extensões como, por exemplo: CSV, PDF, XML, TXT, DWF, URL, JPEG, XLS.
- Dados podem ser enviados via e-mail limitando-se a até 3 documentos em anexo e pode ser classificado como:
- Documento Compartilhado – compartilhado entre usuários da rede;
- Documento Privado – limitado a uma lista de acesso personalizável.

Protocolos

- A comunicação entre o sistema de gerenciamento e a composição da solução de acesso é feita através de protocolos como, por exemplo: TCP/IP, OSDP, IPv4/v6.

- TCP/IP wireless para a comunicação sob WAN/LAN com conexões 10/100/1000Mbps;
- A segurança do sistema é mantida por meio de protocolos de criptografia garantindo seu funcionamento integral de forma segura por TLS 1.2, SSL, AES-128, AES-256.

Compatibilidade

- Microcard de até 256 bits.
- Comporta número ilimitado de cartões ponta a ponta.
- Comporta até 10 formatos de cartões por leitora.
- Cadastro de templates biométricos.
- Protocolo Wiegand embarcado para teclados com matrizes 3x4, 9x16.
- Capacidade de alternar modos de operação das leitoras;
- Comunica-se com equipamentos de controle de acesso por Wiegand e OSDP:
- Leitores Faciais;
- Leitores Digitais;
- Leitores de Proximidade;
- Leitores Smartcard;
- Leitores com Teclado;
- Leitores QR CODE;
- Leitores com inteligências combinadas – QR CODE + Facial; Facial + Digital, etc.
- Compatível com os formatos de leitores e cartões:
- Mifare;
- Desfire EV1;
- Proximity;
- Prox;
- iClass;
- Magnético.
- HID Corporate 1000
- Controlador local presente possui capacidade de gerenciar 130.000 usuários e 63.000 eventos de forma autônoma.
- Software comporta até 20 leitores e possibilidade de expansão para 10.000 leitores.
- Compatibilidade com aplicativos e softwares externos com integração via API, SDK e Servidor SQL. Toda e qualquer ação de integração terá armazenamento em histórico e em caso de erros, os usuários responsáveis receberão um e-mail sendo informados do que se passa no sistema.
- Totalmente compatível com controladoras de porta via TCP/IP, permite ao sistema operar de forma autônoma e integral ao controlar eventos, alarmes, avisos, solicitações, usuários e comunicações de emergência em caso de perda de comunicação.
- Documentos elaborados em fases de testes e homologações, podem ser exportados e importados posteriormente, conforme necessidade.
- Possui integração com serviço de terceiros, o qual permite a exportação de eventos e alarmes para contas client, com possível automação de processo. Seja de incêndio, segurança pessoal ou comunicação.
- Interface visual para configuração geral de forma prévia para integrações, evitando configurações no momento da integração.
- Devido aos seus múltiplos recursos e por ser um sistema versátil, o software de controle de acesso pode ser aplicado em meios acadêmicos, empresariais e residenciais.
- Mais comum em meios empresariais, o sistema auxilia em demandas de equipes de Administração, Segurança e, até mesmo, Recursos Humanos para um maior controle de tudo que se deseja ter acesso com modelos de gestão e layouts previamente configurados.
- Através da Interface Web, é possível visualizar e alterar informações de usuários no banco de dados, seja ele exportado ou não, tais como: cargo, data de criação da credencial, dados pessoais, status, lotação e permissões.

Cliente Web

- Cliente Web é um recurso de controle e gerenciamento remoto disponibilizado ao cliente, através desta ferramenta é possível ter uma visão abrangente do que se deseja. Além disso, possui criptografia de ponta a ponta o que garante a sua segurança integral.
- Dentre os principais recursos do Cliente Web, pode-se citar:
- Interface Web com rolamento de tela por mouse, teclas “Page UP/DOWN” e função “CONGELAR” através dos navegadores Google Chrome 12.0, Firefox 3.5, Internet Explorer 9.0, Windows 8.3 para fácil acesso e visualização dos dados que pode ser acessada através de autenticação por usuário e senha, com tempo de resposta inferior a 1 segundo.
- Permite até 12 clientes simultâneos;
- Permite ao cliente cadastro personalizado de visitantes, colaboradores e prestadores de serviço por meio dos campos de Registro Geral, Passaporte e Cadastro de Pessoas Físicas e atribuição de cartões de acesso aos mesmos.
- Permite ao cliente o gerenciamento de cartões de proximidade personalizados com criações, alterações e exclusões com extensão .NET.
- Permite ao cliente um controle geral do sistema como controle de portas, eventos e relatórios, os quais possuem dados de auditoria e usuários com a classificação de dados na interface.
- Interface gráfica para visualização do design final.

- Permite ao cliente a criação de:
- Acesso e bloqueio temporário de pessoas portadoras do cartão/QR CODE por meio de horários, dias, meses, etc;
- Incluir e excluir acessos ativando ou desativando os respectivos cartões com indicadores de vigência e término do acesso
- Permite ao cliente a alteração e visualização de dados das credenciais, conforme necessário.
- Permite ao cliente a criação de níveis hierárquicos que limitem, ou não, acesso aos operadores, disponibilizando apenas documentos que serão consultados e alterados pelo mesmo.
- Permite a solicitação de acesso a determinada área, de um usuário que eventualmente não possua autorização, gerando a necessidade de aprovação conforme nível hierárquico da área.
- Permite ao cliente o particionamento e distribuição de operadores para as áreas definidas
- Acesso aos relatórios e visualizações dinâmicas de forma criptografada de ponta a ponta por meio de protocolo TLS 1.2.
- Maior autonomia para controlar, elaborar e visualizar portas para acesso/restrição.
- Gestão completa de eventos e relatórios visuais:
- Desempenho e atividades de determinada pessoa/ponto de acesso em uma tela a parte;
- Histórico com filtros de pessoas, ordem crescente, ordem decrescente conforme necessidade e personalização.
- Liberação de um grupo de pessoas de forma simultânea para maior praticidade no controle, sejam eles portadores de cartões ou QR CODES;
- Recurso de exclusão por inatividade: Ao ficar ausente pelo tempo determinado pelo operador o cartão/QR CODE será inativado por mecanismo “log-off”.
- Acesso remoto de até 12 usuários, em tempo real.
- Permissão para usuários gerenciarem a própria agenda com liberações individuais ou coletivas.
- Permissão ao cliente o upgrade remoto de software, firmware e adição de licenças, de forma manual ou automática.
- Visualização e controle de estações.
- Gerenciamento de ativos, com possibilidade de cadastro de ativos, para rastreamento dos mesmos.
- Interface para geração de relatórios de atribuição e histórico de movimentação e alocação.
- Módulo de evacuação de usuários:
- Reconhecimento de agrupamento para identificar automaticamente os que estão no local durante um incidente;
- Operação em todo caso de incidente;
- Operação automática sinalizado por hardware ou manual sinalizado pelo operador;
- Operação Manual sinalizada por comando do operador;
- Permitir reinicialização manual ou automática;
- Destaque a locais de risco no sistema;
- Definição de locais de evacuação;
- Geração de relatórios e alarmes para eventos relacionados a evacuação;
- Notificação em todas as estações em caso de evacuação;
- Visualização da localização de cada usuário no momento do alerta com base nas leituras de cada ponto de acesso;
- Cliente Web, possui funcionalidade de log-off conforme inatividade dos usuários;
- Visualização por parte dos operadores do status de hardware bem como contagem de usuários relacionados ao evento e visualização de mapas gráficos.

Dispositivos Remotos

- Possuem conectividade wireless através de redes Wi-fi e 4G com proteção pelo protocolo SSL.
- Possuem Interface Web através de Safari e Google Chrome com layouts em espanhol, inglês e português.
- Permite ao cliente a expansão da capacidade de dispositivos móveis em rede de acordo com o licenciamento solicitado.
- Permite ao cliente acessar diversas aplicações via Interface Web, incluindo o monitoramento de ações e eventos dentro do sistema em funcionamento.
- Uso opcional de módulo integrado ao software para atribuições remotas e/ou locais com seus principais recursos de gerenciamento para credenciais dos usuários e importação e exportação de dados.
- Permite ao cliente atribuições remotas, como:
- Definição de operador e controlador;
- Ações manuais e/ou automáticas;
- Ativar e/ou desativar dispositivos;
- Criar e/ou modificar cadastros com informações pessoais e imagem através de leitoras de cartões móveis ou não;
- Sincronização das informações recebidas através das leitoras de cartões móveis com o sistema e banco de dados do sistema;
- Consultar histórico e conexões de auditoria/eventos;
- Consulta e auditoria nas alterações do banco de dados;
- Monitorar os eventos em tempo real;
- Monitorar as informações de acesso de todas as credenciais em tempo real, seguidos de alarme pré-programado, ou não.

- Vincular ou excluir um cadastro à um usuário já existente;
- Usar filtros diários, semanais, mensais e anuais;
- Usuários existentes e classificação – visitante, colaborador ou prestador de serviço;
- Visualizar e personalizar pontos de acesso – leitores, portas de entradas e saídas, controladores, elevadores e sensores.

*Ações citadas anteriormente podem ser feitas de forma automática ou manual.

Recursos Gráficos e Visuais

Para uma melhor performance, o software IPX-S-SWACSS conta com mapas e dashboards que auxiliam visualmente e tecnicamente uma análise e ciência mais profunda do que ocorre no local pré-estabelecido que se deseja verificar com o uso de indicadores e ícones.

- Cadastro de templates e layouts em modelos biométricos faciais e digitais.
- Visualização de plantas baixas e localização de eventos disparados por alarmes.
- Elaboração de mensagens instrutivas pós-disparo.
- Configuração de mapas em centros de monitoramento remotos.
- Acesso simultâneo a múltiplos mapas e gráficos para comparativos por meio do controle “arrasta e solta” dos ícones:
- Entrada de alarme;
- Saída de alarme;
- Leitores;
- Portas;
- Elevadores;
- Adicionar Mapa;
- Excluir Mapa;
- Sobrepor mapa;
- Conectar mapa;
- Visualização 3D.

LDAP

A solução conta com o protocolo aberto de aplicação LDAP para uma distribuição de informação de diretório de maneira clara e automatizada. Ademais, conta com diversos recursos para um maior domínio, como:

- Direcionamento autônomo de acessos, os quais podem ser automáticos e baseados em campos de dois lados;
- Direcionamento de funções aos usuários;
- Palavra-chave para pesquisas;
- Autenticidade de usuário por meio de protocolos SSL e LDAP com nome de usuário singular;
- Filtros de pesquisas LDAP em níveis e subníveis do diretório;
- Nomeação LDAP e número de porta personalizável;
- Previsão de dados de importação e exportação;
- Importação automática de entradas advindas do diretório;

Armazenamento e Transferência

Todos os dados de informações são armazenados e gerenciados no próprio banco de dados da solução com recurso de backup para futuras recuperações. Por sua vez, o banco de dados é versátil podendo ser instalado no servidor local, em um servidor próprio para o banco e em um banco de dados corporativo já existente.

- Visualização e armazenamento do histórico de dados com uma capacidade de 53 milhões podendo, ou não, ser expandida por hardware externo.
- Salvamento, recuperação de dados do software, bem como, seu histórico e eventos para discos rígidos e/ou nuvem.
- Downloads automáticos instantâneos, conforme alterações do sistema e em painéis inteligentes que emitam solicitações de alteração na base de dados, o qual pode-se ser efetuado o download de forma manual ou automática.

Cadastros e Informações Pessoais

O campo de cadastros é extenso e personalizável conforme necessidade do cliente com diversas abas, contendo campos pré-definidos, ou não, podendo estes serem modificados de acordo com o objetivo necessário por pessoas autorizadas.

- Todos os campos abaixo podem ser mandatórios ou únicos, com máscaras personalizáveis pelo operador.
- <u>Campos pré-estabelecidos pelo sistema:</u>
  - Nome;
  - Data de nascimento;
  - RG;
  - CPF;
  - Número de Telefone Residencial;
  - Número de Telefone Celular;
  - Código Postal;
  - Endereço;
  - CEP;
- <u>Campos personalizáveis</u>**:**
  - Numerais – Inteiros, Fracionários, Decimais.
  - Lógico;
  - Símbolos e Caracteres;
  - Data, Hora, Data + Hora;
  - Listas com letras maiúsculas, minúsculas, mescladas entre si;
  - Listas numéricas em ordem crescente, decrescente;
  - Textos com linhas ilimitadas;

- Textos com letras, números e mesclados entre si.
- Relatórios programados para rápida exportação:
  - Históricos de credenciais;
  - Históricos de proprietário;
  - Histórico do operador;
  - Histórico de eventos e alarmes;
  - Histórico de programações do sistema;
  - Histórico de administração e configurações dos componentes do sistema de acesso;
  - Acesso a leitoras;
  - Acesso a andares;
  - Frequência, Tempo e Intervalos;
- Permite ao cliente a criação de inúmeros níveis de acesso, gerenciamento e controle.
- Permite ao cliente a criação de usuários sem a vinculação a um cartão de acesso.
- Permite ao cliente a associação de usuários a mais de um direito de acesso e cartões.

Credenciais

O sistema incorpora um módulo de administração integrada e transparente de credenciais, cuja função principal reside na supervisão dos usuários de cartões. Essa supervisão abrange a aquisição de imagens, dados biométricos e caso necessário imagens relevantes. Ademais, o sistema possibilita a importação e exportação eficientes de dados de funcionários, permitindo a modificação dos privilégios de acesso dos usuários do cartão de acesso, conforme detalhes abaixo:

Cada Registro Geral se limitará a 7 cartões de identificação e/ou QR CODE, sejam eles ativos ou expirados e terão seu tempo de vigência previamente estabelecidos em horas, dias, meses e/ou anos com a possibilidade de renovação ou exclusão no cadastro do usuário. Conta também com os seguintes recursos:

- Liberações temporárias para visitantes e prestadores de serviço sem a necessidade de cadastro.
- Cartões de acesso inativos por um determinado podem ser excluídos de forma simultânea, caso necessário.
- Os 7 acessos podem se estender à dispositivos mobiles e veículos que terão uma tag própria.
- Usuários podem ser criados de forma antecipada, sem a necessidade de vinculação instantânea à um meio de acesso.
- Restrições à um ou mais usuários com áreas configuradas permitindo um limite mínimo e máximo monitorado de forma autônoma num determinado espaço de tempo. Perímetro sujeito a alarmes, caso descumpridas as regras criadas e notificação direta ao responsável do local.
- Eventos configurados nos seguintes parâmetros:
- Contagem de pessoas no perímetro;
- Status de máxima e mínima ocupação individual;
- Status de máxima e mínima ocupação coletiva;
- Notificação de violação (Anti retorno e violação de acesso).
- Níveis de acesso são criados com um limite de ativação intermediado por data e hora. Podendo-se renovar ao expirar.
- Níveis de acesso podem ser concedidos e removidos de forma simultânea a mais de uma pessoa.
- Atribuição de ativos com possibilidade de restrição de saída em caso de o usuário estar portando ativo não atribuído a credencial.
- Direitos podem ser definidos por meio de associação de leitores e horários, contendo em sua configuração, data, dia e hora.
- Credenciais novas associadas a um usuário existente irão adquirir as permissões de forma automática.

Configurações de Serviço

- O serviço de configuração do software prevê a configuração de layouts e modelos, estes podendo ser definidos pelo operador para uma padronização, o que possibilita associações de dados, como: entradas e saídas, intervalos, usuários e portas.
- Objetos do sistema podem ser classificados como:
  - Monitorados;
  - Controlados;
  - Monitorados e controlados.
- Número ilimitado de usuários que podem ser classificados como provedores limitando-os, ou não, pela liberdade de controle, que pode ser restringido pelo nível de acesso concedido.
- Navegação e árvore hierárquica para estabelecimento de níveis.
- Software e Firmware podem ser atualizados remotamente por pessoas previamente autorizadas.
- Software e Firmware possuem mecanismo de atualização e programação de forma automática e manual.
- Servidores Failover escalonados com iniciação automática que impede a ausência do sistema.
- Configuração de definição de áreas, as quais, subentendem-se por locais físicos. Cada evento na porta da área será armazenado para a geração de análises e relatórios, pois, não há a possibilidade de acesso/saída sem o cartão de acesso.

- Geração de relatório pré-definido, ou seja, listagem dos acessos de determinado grupo/pessoa em tempo real ou anterior.
- Visualização de presença através de plantas baixas e mapas dinâmicos para identificação da localização por meio de biometria ou cartões, seguindo em tempo real seu próprio deslocamento e atualização automática.
- 03 modos de operação para o local desejado pelo operador que continuam em funcionamento mesmo em falha de comunicação:
  - Modo Livre – Nenhum modo é acionado e o sistema atua livremente;
  - Ant i Retorno – Utilizado para controle e visualização em tempo real dos portadores de cartões e acessórios de acesso, o usuário que tentar entrar novamente no local sem ter apresentado a credencial na saída, o mesmo terá a entrada recusada. Estes por sua vez, poderão ser liberados de acordo com a regra do provedor que poderá estabelecer, por exemplo, um período de espera. Além disso, essa configuração pode ser personalizada de várias maneiras, tais como: subníveis de sistema e controle de fuso horário.
  - Ant i Retorno Temporizado – Utilizado para controle e visualização em tempo real dos portadores de cartões de maneira temporizada, o usuário que tentar entrar novamente no local sem ter apresentado a credencial na saída, o mesmo terá a entrada recusada dentro do limite estabelecido pelo provedor. Estes por sua vez, poderão ser liberados de acordo com a regra do provedor que poderá estabelecer, por exemplo, um período de espera. Além disso, essa configuração pode ser personalizada de várias maneiras, tais como: subníveis de sistema e controle de fuso horário.
- Controle de acesso veicular – Gerenciamento dos veículos vinculados aos usuários, controlando entrada e saída de acordo com o número de vagas disponíveis no interior no estacionamento. Seu reconhecimento também pode ser feito por câmeras com tecnologia de Reconhecimento de Placa Veicular, que ligado nas cancelas, irão autorizar ou não a entrada do usuário.
- Gerenciamento de visitantes facilitado com o automático Check-In e Check-Out.
- Ao ser descartada nas urnas, as credenciais estarão disponíveis novamente para vínculo de usuário.
- Comunicação direta com o posto de atendimento, responsável por liberar visitantes em sequência do Check-In e notificação de chegada de visitante ao usuário responsável.
- Gerir visitantes em módulo dedicado possibilitando:
  - Agendamento prévio por parte do cliente;
  - Monitorar visitante nas dependências do cliente;
  - Registro de chegada/saída;
  - Registro com imagem e dados pessoais, de forma antecipada.
- Sistema anti-fake – O sistema verifica a veracidade dos principais meios de liberação de acesso combinados entre si, tais como: Dados Pessoais, Face, Digital, PIN, Cartões de Proximidade temporários e definitivos.
- Recurso Standalone – O sistema continua operando de forma autônoma, em caso de perda de energia, por meio de armazenamento de, aproximadamente, 7.000 acessos. Em caso de conexão das controladoras locais, todos os usuários armazenados terão seus acessos liberados, podendo-se ainda, manter qualquer das 3 operações configuráveis.
- Programações Agendadas – Programações podem ser configuradas por data, hora, período e modo de forma ilimitada e com seleção múltipla dos recursos, citados anteriormente.
- Totem de Autoatendimento – possibilita que o visitante realize check-in de forma autônoma validando os dados do pré-cadastro.
- Monitoramento de eventos e alarmes – Notificações em tempo real para o operador por meio de pop-ups e e-mail com classificação e gerenciamento de alarmes ilimitados através dos seguintes parâmetros:
  - Usuário;
  - Data e hora;
  - Descrição do alarme;
  - Prioridade;
  - Gerenciamento;
  - Leitor/Ponto de acesso disparado;
  - Entradas e Saídas;

*Alarmes e eventos são cíclicos no interior do armazenamento, sobrepondo-se conforme seu limite.

Equipamentos do Controle de Acesso

As controladoras que atuam juntos com leitores e demais dispositivos do sistema de acesso comportam, em conjunto, 1.600 níveis de acesso total e 120 níveis de acesso por usuário.

Oferece suporte a gravadores digitais de diversos fabricantes presentes no mercado, além de ser compatível com câmeras IP e codificadores de vídeo também de diferentes fabricantes.

Eventos

Gerenciamento de Vídeo Digital: viabiliza a integração eficaz com sistemas de gerenciamento de vídeo em tempo real, associando-se a cada alarme, e possibilita a configuração personalizada de segmentos de vídeo gravado. Isso inclui a definição da duração para períodos pré e pós-alarme de maneira específica.

Os eventos são ilimitados e contam com diversas configurações, agendados ou não, com ações engatilhadas pelo disparo do mesmo. Há níveis de prioridade que podem ser criados, conforme necessidade e layouts personalizáveis por nomes, cores e tags.

Configurações de Eventos

- Classificações de eventos por:
  - Espaço de tempo (data/hora);
  - Prioridade;
  - Nome do evento;
  - Estado.
- Pendências de aceite ou não por parte do operador para liberar e limpar o evento.
- Opção de pedido para que o operador deixe uma nota para reconhecimento do evento.
- Opção de pedido para que o operador deixa uma nota para limpeza do evento.
- Encaminhamento para responsáveis baseado em nível de prioridade e escala de carga horária por dia e hora.
- Visualização ou não de ativação de evento.
- Visualização ou não de nota criada pelo operador na ativação do evento.
- Visualização ou não de nota criada pelo operador na desativação do evento.
- Reset de evento após reconhecimento do causador do mesmo.
- Vinculação com um mapa específico, que será exibido no momento de disparo do evento.
- Ativação de evento sequencial quando o primeiro não for reconhecido num limite de tempo previamente estabelecido.
- Ativação de evento sequencial quando o primeiro for reconhecido num limite de tempo previamente estabelecido, porém limpo por um determinado tempo.
- Associação de arquivos de voz a um ou mais eventos.
- Configuração de intervalo mínimo para ativação do evento e atraso do mesmo.
- Importação e exportação de eventos e arquivos.
- Emissão e exclusão de relatórios com os dados desejados para análise e controle.
- Inclusão de notas para cada evento aparentes na tela ao ser ativado.
- Interação de eventos com botões manuais: travar, destravar, alternar e auxiliar.
- Monitoramento do funcionamento integral de todas as áreas de segurança em tempo real, com notificações audiovisuais quando houver qualquer alteração de status do software ativo.
- Administração de detecção de intrusão: possibilita a integração transparente com painéis de detecção de intrusão avançados, provenientes de diversos fabricantes.
- Monitoramento de todos os usuários, assim como, suas ações no interior da solução ativa dentro da companhia com um histórico online, podendo ser acessado por pessoas com a autorização concedida.
- Eventos programáveis por dia e horário, sendo possível configurar múltiplos eventos:
  - Configuração de equipamentos para um funcionamento em conjunto nos pontos de acesso.
  - Escolha do modo de operação dos equipamentos de acesso, podendo eles serem combinados;
  - Comunicação programada direta ao host;
  - Reiniciar os modos de operação (Livre, Antiretorno, Temporizado);
  - Reiniciar os status de todos as credenciais do sistema.

Importação e Exportação de Dados

- E-mails podem ser automatizados, os mesmos são enviados via SMTP ao evento ser disparado.
- Importação e exportação de e-mails, dados e relatórios, em geral de forma automática e/ou manual.
- A importação de um banco de dados externo é feita de forma automática contendo as respectivas informações contidas, evitando assim, o recadastramento de todos os funcionários.
- Interface gráfica contendo ferramentas que parametrizam quais dados e em quanto tempo as ações serão inicializadas e finalizadas.

Controle de Software

O controle de software é flexível devido a inúmeras opções presentes para se configurar. Através de controles remotos e locais, o operador consegue ter uma visão ampla e um maior controle sobre todo o sistema em funcionamento.

O host, administrador do sistema, atuará na base de dados tomando as decisões necessárias para um bom desempenho do sistema, por meio de painéis inteligentes com interfaces de apoio para qualquer sistema de segurança implantado no software.

Controle integral de entradas e saídas dos painéis inteligentes de controle.

- O host tem a capacidade e opção de criação de inúmeros níveis de acesso, conforme políticas de acesso e da companhia.
- Qualquer modificação que saia das políticas pré-estabelecidas, gera uma notificação e a regra retorna ao padrão.
- Interface de controle com os seguintes recursos e parâmetros:
  - Acesso via web por navegadores Windows, Firefox e Internet Explorer;
  - Múltiplas abas de navegação;
  - Autenticação de host por meio de Servidor Directory Ativo;
- Configuração lógica dos equipamentos parametrizando acessos, alarmes, intertravamentos e mecanismos de segurança, podendo ainda, combinar esses recursos entre si.
- Controle total de equipamentos do sistema de acesso pela estação de monitoramento local utilizando-se dos recursos disponíveis no sistema, como: ações manuais e automáticas, eventos, solicitações, alarmes e listas de causas.

Operador

- O operador, responsável pelas decisões e operações no sistema, atuará em conjunto com o host para a gestão do sistema permitindo, ou não, níveis de acesso, gerenciando status remotamente ou presencialmente de forma automática e manual com uma visão geral de alarmes e eventos.
- Liberdade de alterações nos cadastros e informações pessoais dos demais usuários cadastrados no sistema de forma múltipla e unitária, como:
  - Adição;
  - Exclusão;
  - Alteração.
- Esses recursos podem ser feitos livres de solicitações de atribuição à usuário, com os seguintes campos pré-definidos:
  - Data de emissão;
  - Data de expiração;
  - Data para retorno;
  - Status do cartão;
  - Status do usuário;
  - Numeração do cartão;
  - Descritivo;
  - Atribuição de usuário.
- O operador será o responsável pelas transações dentro da solução, tais como:
  - Permitir e restringir acessos;
  - Armar e desarmar locais com sensores de presença (Intrusão) de forma remota e local;
  - Controlar os relés e saídas dos controladores e leitores nos pontos de acesso.

*Todas as ações serão tomadas de acordo com o direito atribuído ao usuário.
*Arme e desarme dos locais com sensores podem ser feitas de forma auto/manual.

- Monitoramento e controle de todas as áreas, portas, leitoras, entradas, saídas, elevadores e controladoras do sistema, exibindo status de atividade dos pontos de acesso e enviando os sinais necessários ao sistema para liberação dos usuários.
- Monitoramento e controle de comunicação e conectividade do sistema pela estação de monitoramento, com alarmes audiovisuais em caso de anormalidades.
- Entrada e saída configuráveis por modo livre, anti retorno, anti retorno temporizado.
- Importação, exportação e impressão de dados em diversos destinos, bem como:
  - WORD;
  - EXCEL;
  - POWERPOINT;
  - Notas pendentes de formatação;
  - Formato Data Interchange;
  - Crystal Reports;
  - HTML;
  - ODBC.

Base de Dados

Na base de dados ocorrerá qualquer tipo de programação automática e manual advinda do funcionamento do sistema, o qualreceberá respostas da base de dados sem afetar o funcionamento.
O sistema irá continuar funcionando mesmo em caso de queda de energia ou comicação.
A solução conta com as seguintes programações sincronizadas com o servidor central:

- Data: dd/mm/aaaa;
- Hora: HH:MM:SS;
- Intervalos.

Programações por horário podem ser configuradas diariamente e semanalmente, contendo intervalos nas programações que serão usadas em controles, como:

- Acesso ao usuário autorizado nos pontos de acesso de forma remota e local;
- Rotatividade de transações de acesso e alarmes de forma remota e local;
- Ligar e desligar controladoras de forma remota e local;
- Ligar e desligar leitores de forma remota e local;
- Ligar e desligar catracas de forma remota e local;
- Ligar e desligar sistemas de alarme de forma remota e local;
- Ligar e desligar entradas de forma remota e local;

Dados poderão ser integrados de forma autônoma através de configurações pré-definidas, de acordo com o período selecionado pelo operador, com uma interface que atribua os dados obtidos externamente em campos do sistema atual.

ESPECIFICAÇÕES ADICIONAIS:

O sistema IPX-S-SWACSS é uma solução abrangente que integra diversas funcionalidades de controle de acesso em uma plataforma unificada, atendendo plenamente às exigências de um Sistema de Controle de Acesso (SCA) conforme descrito. Sua arquitetura modular permite a união de diferentes componentes para formar um sistema coeso e eficaz.

O IPX-S-SWACSS é uma plataforma única e integrada, projetada para minimizar problemas de integração ao consolidar todas as funcionalidades de controle de acesso em um só ambiente, conforme a preferência por uma solução unificada.

O IPX-S-SWACSS ele é flexível e permite a integração com outras ferramentas e softwares especializados, caso haja requisitos específicos que demandem soluções complementares, sem oposição ao uso de múltiplos recursos.

Caso a implementação do IPX-S-SWACSS envolva a utilização de múltiplos sistemas ou ferramentas complementares, a INPEX garante o pleno funcionamento e a integração entre todas as soluções, assumindo a responsabilidade por quaisquer desenvolvimentos, customizações e adequações necessárias, bem como os custos inerentes aos serviços de desenvolvimento e licenças para conexão entre estes softwares.

O SCA IPX-S-SWACSS é inerentemente flexível e escalável, permitindo a expansão contínua do sistema através da adição de licenças e módulos, acompanhando o crescimento das necessidades do cliente. Sua arquitetura suporta desde pequenas instalações até milhares de leitores e centenas de milhares de usuários.

O IPX-S-SWACSS oferece uma interface de usuário centralizada e intuitiva, projetada para gerenciar de forma unificada todos os aspectos dos sistemas de controle de acesso, proporcionando uma experiência de uso consistente e eficiente.

Todas as comunicações dentro do sistema IPX-S-SWACSS, incluindo as interações cliente-servidor e controlador-servidor, são configuradas para utilizar criptografia robusta, como TLS 1.2, SSL, AES-128 e AES-256, garantindo a segurança e a integridade dos dados.

O sistema IPX-S-SWACSS é projetado para alta disponibilidade, incorporando módulos de failover e hot-standby que garantem a continuidade das operações mesmo em caso de falhas, minimizando interrupções e assegurando o acesso ininterrupto.

A interface de usuário do SCA IPX-S-SWACSS possui um menu principal fixo na parte superior, que inclui um link direto para a página inicial e outras opções de navegação essenciais, facilitando o acesso rápido às funcionalidades do sistema.

No menu principal do IPX-S-SWACSS, há um painel adicional que oferece funcionalidades como pesquisa rápida, exibição do status de alarmes, contagem de controladores online e offline, e acesso direto ao perfil do usuário, proporcionando uma visão geral e controle eficiente.

O sistema IPX-S-SWACSS inclui um painel de tarefas rápidas, com atalhos para as funções mais utilizadas, como a adição de novas credenciais e a alteração de senhas de usuários, otimizando a produtividade do operador.

Além do menu principal, o IPX-S-SWACSS oferece métodos alternativos de navegação para seus recursos, garantindo flexibilidade e acessibilidade para diferentes perfis de usuários e preferências de interação.

O sistema IPX-S-SWACSS permite a definição de agendas detalhadas por dia da semana e hora do dia. Essas agendas podem ser anexadas a qualquer Ponto de Acesso dentro de um Grupo de Acesso, proporcionando controle granular sobre os horários de acesso.

O IPX-S-SWACSS suporta a inclusão de feriados como exceções à programação normal. Múltiplos feriados podem ser agrupados e anexados a uma Agenda, permitindo a substituição da programação regular para eventos especiais ou dias não úteis.

O SCA IPX-S-SWACSS permite a criação e o gerenciamento de grupos de acesso, que consistem em um ou mais pontos de acesso e seus planejamentos associados, facilitando a organização e aplicação de políticas de acesso.

No IPX-S-SWACSS, é possível criar perfis de usuário detalhados e atribuir credenciais específicas a cada um. Os indivíduos são então associados a grupos de acesso, garantindo que as permissões sejam aplicadas de forma eficiente e organizada.

O sistema IPX-S-SWACSS oferece funcionalidades completas para o gerenciamento de credenciais de usuários, incluindo a edição de credenciais existentes, bem como a capacidade de desativar ou reativar credenciais conforme a necessidade, assegurando controle total sobre o acesso.

O IPX-S-SWACSS permite o gerenciamento abrangente de fotos dos usuários e a associação de múltiplas notas a cada registro de usuário, facilitando a documentação e o acompanhamento de informações relevantes.

O SCA IPX-S-SWACSS opera com base em grupos de acesso, que definem as permissões de acesso de usuários ou grupos de usuários a recursos específicos em determinados horários. Cada grupo de acesso é composto por uma lista de portas e planejamentos associados, garantindo um controle de acesso preciso.

O sistema IPX-S-SWACSS integra o trabalho com agendas e feriados. As agendas deverão ser aplicadas a pontos de acesso individuais para criar níveis de acesso quando vinculados aos Grupos de Acesso do usuário, e também podem ser vinculadas a pontos de acesso para gerenciar o destravamento de portas.

O IPX-S-SWACSS permite que os agendamentos sejam combinados com as substituições do Grupo de Feriados, oferecendo total flexibilidade no controle de acesso às instalações, incluindo a incorporação de feriados públicos e a criação de feriados individuais atribuíveis a grupos específicos.

O visualizador de eventos do IPX-S-SWACSS registra e exibe todas as interações relevantes, incluindo ações de detentores de credenciais, alterações no status de dispositivos de acesso (locais ou via software), e todos os alarmes gerados, proporcionando um registro completo das atividades do sistema.

O visualizador de eventos do IPX-S-SWACSS exibe eventos relacionados ao software, como logins e falhas de logon de usuários, e alterações em perfis de usuário. Os eventos podem ser filtrados por qualquer combinação de tipo de evento, usuário, controlador, ponto de acesso, entrada, saída ou site, permitindo análises detalhadas.

O instantâneo de eventos do IPX-S-SWACSS pode ser filtrado para incluir apenas informações úteis ao usuário, com opções de filtragem por intervalo de data/hora, tipo de evento, usuário, controlador, ponto de acesso, entrada, saída ou site, garantindo que apenas os dados relevantes sejam analisados.

O SCA IPX-S-SWACSS exibe uma contagem clara de alarmes não processados e oferece uma janela dedicada para adicionar notas, permitindo que os usuários insiram informações contextuais importantes para cada alarme.

O sistema IPX-S-SWACSS permite o encaminhamento de alarmes para outros usuários e mantém um registro completo de todos os alarmes gerados dentro de um período especificado, facilitando o acompanhamento e a auditoria.

As informações de alarmes no IPX-S-SWACSS podem ser filtradas por ponto de acesso, área, tipo de alarme, controlador, entrada ou saída. O sistema suporta a seleção de tipos de alarme como 'Alarme criado', 'Alarme reconhecido', 'Alarme não reconhecido' ou 'Alarme desmarcado', para uma gestão eficiente.

O IPX-S-SWACSS oferece a opção de exportar logs de alarmes e emite um sinal sonoro quando um alarme é gerado. Além disso, suporta a reprodução de texto como som (Text-to-Speech - TTS) para notificações de alarme, garantindo que os alertas sejam percebidos.

O SCA IPX-S-SWACSS incorpora comandos automáticos que permitem a automação de diversas tarefas do usuário e do sistema, como ações em dispositivos, clientes e mensagens, otimizando a operação e reduzindo a necessidade de intervenção manual.

Após a ativação de um gatilho, o sistema IPX-S-SWACSS é capaz de executar comandos automáticos no cliente da aplicação, em dispositivos de controle de acesso, enviar mensagens, executar comandos diversos, integrar-se com sistemas de CFTV e gerenciar comandos de visitante, proporcionando automação completa.

O SCA IPX-S-SWACSS permite o trabalho com áreas, que são utilizadas para controle de ocupação e rastreamento de pessoal, oferecendo uma visão clara da movimentação e presença de indivíduos em diferentes setores.

O IPX-S-SWACSS oferece suporte robusto ao monitoramento de alarmes por meio de áreas, permitindo que alarmes específicos de área sejam gerados por sensores, proporcionando uma resposta rápida e localizada a eventos de segurança.

O sistema IPX-S-SWACSS inclui um sistema de contagem de uso, que permite configurar o número máximo de vezes que uma credencial pode ser utilizada. Uma vez excedida essa contagem, o acesso é automaticamente negado, garantindo o controle de uso de credenciais.

O SCA IPX-S-SWACSS suporta o cadastro de pelo menos 100.000 (cem mil) usuários visitantes, cada um com atributos detalhados, incluindo informações de identificação, credenciais, imagens e associações a Grupos de Acesso. O sistema insere visitantes dinamicamente nos terminais e remove suas credenciais ao término do período de acesso.

O IPX-S-SWACSS é capaz de resgatar cadastros de visitantes inativos dentro de sua capacidade mínima de 100.000. Ao exceder essa capacidade, o sistema substitui os dados dos visitantes inativos mais antigos. A duração da ativação e validade das credenciais são configuráveis, permitindo ativação por períodos específicos.

O SCA IPX-S-SWACSS possui um campo de isenção para Anti-passback e função de desbloqueio estendido para credenciais. Grupos de acesso podem ser utilizados para controlar o nível de acesso associado a cada credencial, oferecendo flexibilidade na gestão de permissões.

No IPX-S-SWACSS, ao selecionar 'acesso completo' em um modelo de credencial, a credencial terá acesso total em Grupos de Acesso. Se 'acesso selecionado' for escolhido com grupos específicos, esses grupos aparecerão ao adicionar credenciais. Usuários podem associar um dispositivo a uma credencial ao adicioná-la.

O SCA IPX-S-SWACSS permite a criação de grupos de usuários, incluindo visitantes permanentes, e possui um sistema de Anti-Passback robusto. Este recurso impede o uso indevido de credenciais, estabelecendo uma sequência de acesso obrigatória para garantir o controle de entrada e saída em áreas controladas.

O SCA IPX-S-SWACSS trabalha com modelos predefinidos de mensagens e notificações, utilizando protocolos como SMTP, HTTP e TCP para envio. A personalização das configurações de dispositivos e a configuração de Inputs e Outputs dos pontos de acesso são possíveis, dependendo da capacidade do dispositivo.

O SCA IPX-S-SWACSS gera relatórios detalhados de entrada e saída, contendo informações sobre os usuários que acessam e deixam a instalação. Esses relatórios incluem dados sobre eventos em pontos de acesso, controladores e entradas, fornecendo uma visão completa do fluxo de pessoas.

O SCA IPX-S-SWACSS inclui uma aplicação embarcada para criação e formatação de modelos de crachá personalizados. Possui também um editor de mapa nativo para criar mapas personalizados, além de permitir a edição de mapas GISMAP diretamente de plataformas como Google Maps ou similares, oferecendo flexibilidade visual.