# TERMO DE REFERÊNCIA

## Implantação do Sistema Integrado de Segurança das vias de acesso, perímetro e áreas comuns

## Anexo III – MD e Especificações para o Sistema de Controle de Acesso.

Salvador, 28 de abril de 2022

**Sumário**

## Anexo III – MD e Especificações para o Sistema de Controle de Acesso.

O presente a documento é parte integrante do TERMO DE REFERÊNCIA para implantação do Sistema Integrado de Segurança das vias de acesso, perímetro e áreas comuns do edifício sede do TECNOCENTRO e apresenta as informações necessárias para fornecimento e instalação do Sistema de Controle de Acessos, conforme soluções definidas a seguir.

### 1. Cenário Atual.

O TECNOCENTRO é um edifício de ocupação comercial, voltado a empresas de tecnologia, selecionadas a partir de critérios previamente estabelecidos através de editais específicos.

Atualmente o empreendimento conta apenas com segurança humana, fornecido através de efetivo contratado por uma empresa de segurança de iniciativa privada.

Em função da extensão, da localização, dos diversos pontos de acessos, e da consequente vulnerabilidade, torna-se extremamente necessário a implantação de sistemas complementares que venham a garantir a plena segurança do empreendimento. Para tanto, propõe-se a implantação de sistemas eletrônicos de Videomonitoramento, baseado em um Circuito Interno de Televisão – CFTV, e Controle de Acessos baseado em terminais com leitores e unidades de reconhecimento facial.

### 2. Projeto.

A empresa pretendente deverá visitar o local, avaliar toda a estrutura e dificuldades existentes e propor a solução baseada nas atuais necessidades do TECNOCENTRO, levando em consideração as premissas básicas estabelecidas no presente documento.

O TECNOCENTRO apresentará projeto básico contendo informações de localização de pontos previstos para toda a solução. A empresa contratada deverá desenvolver o projeto executivo, contendo todas as informações necessárias a implantação da solução proposta.

A solução proposta, além de atender às necessidades de videomonitoramento, deverá ser plenamente integrada ao Sistema de Controle de Acesso, parte da solução proposta, em uma plataforma única, mantendo a compatibilidade e a facilidade operacional da equipe de segurança.

Toda a solução deverá trafegar em Rede de Cabeamento Estruturado. Para tanto, a empresa pretendente deverá avaliar as condições da atual infraestrutura (existente), prevendo todas as intervenções necessárias para atender às novas soluções.

### 3. Arquitetura do sistema.

A solução implantada deverá formar uma plataforma única Sistema de Videomonitoramento, mantendo a compatibilidade e a facilidade operacional da equipe de segurança.

A empresa contratada deverá apresentar o projeto executivo de implantação no prazo máximo de 10 (dez), contendo todas as informações de localização de equipamentos, delineamento de áreas de cobertura, detalhes de instalação e configuração do sistema. Não será autorizado o fornecimento de materiais e início dos serviços de implantação sem a devida aprovação do projeto pela comissão de avaliação do TECNOCENTRO.

Todo o sistema operará por rede de comunicação TCP/IP. O Sistema será descentralizado, prevendo-se controladoras autônomas instaladas nos diversos locais sujeitos ao controle de acessos, interligadas pela rede Ethernet TCP/IP de a um Servidor de Acessos que exerce a função de gestão geral do sistema, através de um software específico e dedicado. Em caso de falta de comunicação com servidor, por serem autônomas, as controladoras continuarão operando, tendo como única limitação a atualização do seu banco de dados. Uma vez reestabelecida a comunicação, a atualização dos bancos de dados das controladoras acontecerá automaticamente.

O servidor do sistema será o mesmo do Circuito Fechado de Televisão, instalado na Central de Segurança do condomínio, operando na mesma plataforma, com total compatibilidade.

Definição do tipo de acesso.

- ✔ O Controle de Acesso de pedestres será realizado através de duas recepções monitoradas por Leitor de Proximidade e/ou Reconhecimento Facial, sendo uma no pavimento Térreo e outra na Garagem I.
- ✔ O Controle de Acesso com veículos ocorrerá através de um único acesso localizado na Garagem I, utilizando portões e/ou cancelas.
- ✔ As "rotas de fuga" para emergências e demais acessos secundários, serão controladas e monitoradas pelo sistema, mantendo-se travadas, com liberação automática em casos de situações de emergências.

## 4. Base de dados

A base de dados do Sistema de Controle de Acesso, disporá de recursos de armazenamento de dados nas próprias Unidades Controladoras, de forma a registrar o histórico de transações ocorridas durante uma indisponibilidade da rede de comunicação, e de atualização automática do histórico de transações, assim que a comunicação com a rede for restabelecida.

A base de dados será do tipo distribuída, isto é, permitirá ou negará o acesso a cada área, independentemente da disponibilidade da rede de comunicação com o servidor, para isto, possuirá base de dados redundante, de forma que a perda da base de dados de uma controladora possa ser recuperada no servidor central do sistema.

O Sistema de Controle de Acesso será composto por um banco de dados cadastral, constituído por um banco de imagens integrado ao banco de dados de cadastro dos usuários, disponível para outros aplicativos em rede mediante acesso através de logins de segurança.

## 5. Especificações e Características Técnicas.

As especificações a seguir estabelecem condições e características técnicas mínimas necessários para os equipamentos que irão compor o Sistema de controle de Acesso.

### 5.1 Terminal de Reconhecimento Facial.

- ✔ Pro Face Access Terminal.
- ✔ Tela sensível ao toque de 7 polegadas, lente grande angular de 2 megapixels;
- ✔ Ajusta o brilho da luz suplementar manualmente;
- ✔ Reconhecimento de rosto em ambiente escuro;

- ✔ Distância de reconhecimento facial: 0,3m a 3m;
- ✔ Altura sugerida para reconhecimento facial entre 1,4 m e 1,9 m;
- ✔ Algoritmo de aprendizagem profunda;
- ✔ Capacidade de 6.000 faces, capacidade de 5.000 impressões digitais e capacidade de 50.000 eventos;
- ✔ Anti-spoofing facial;
- ✔ Vários modos de autenticação;
- ✔ Duração do reconhecimento facial ＜ 0,2 s / Usuário; taxa de precisão de reconhecimento de rosto ≥ 99%;
- ✔ Operação autônoma;
- ✔ Transmite dados para o software cliente via comunicação TCP / IP e salva os dados no software cliente;
- ✔ Captura de ligação e salvamento de fotos capturadas;
- ✔ Gerenciar, pesquisar e definir dados do dispositivo após fazer login no dispositivo localmente;
- ✔ Conecta-se a um leitor de cartão externo ou controlador de acesso via protocolo RS-485;
- ✔ Conecta-se ao controlador de acesso externo ou leitor de cartão Wiegand via protocolo Wiegand;
- ✔ Conecta-se à unidade de controle de porta segura via protocolo RS-485 para evitar a abertura da porta quando o terminal é destruído;
- ✔ Áudio bidirecional com software cliente, estação interna e estação mestre;
- ✔ Visualização remota ao vivo via protocolo RTSP; modo de codificação: H.264;
- ✔ NTP, sincronização de tempo manual e sincronização automática;
- ✔ Prompt de áudio;
- ✔ Design de cão de guarda e função de violação;
- ✔ Suporta 6 status de presença, incluindo check in, check out, break in, break out, hora extra de entrada, hora extra de saída;
- ✔ Suporta vários idiomas: inglês, espanhol, árabe, tailandês, indonésio e russo;
- ✔ Suporta EHome 5.0 (ISUP 5.0) e protocolo ISAPI;
- ✔ Configuração via navegador da web;

**5.2 Leitor de Catão por Aproximação.**

Leitor para ambientes externos, com proteção IP-65, frequência de leitura 13,56Mhz/125Khz. Comunica-se com o controlador de acesso via protocolo RS-485. Caixa de proteção para uso interno à prova de violações e proteção do leitor de cartão contra danos maliciosos.

**Principais características:**

- ✔ Comunicação RS-485;

- ✔ Taxa de transmissão de 19.200bps-N-8-1;
- ✔ Module Módulo óptico de impressão digital CMOS;
- ✔ Tempo de comparação das impressões digitais: 1: 1≤1s/1: 1000≤1s/FRR≤0,01%/FAR≤0,001%;
- ✔ Teclado numérico para inserção de senhas;
- ✔ Sinalização acústica incorporada para indicação de status
- ✔ Função à prova de adulteração.

### 5.3 Fechadura Eletromagnética

Serão para aplicação nas portas, funcionando como retentores/bloqueadores eletromagnéticos, possuindo incorporados contatos magnéticos de alarme.

**Especificações - Portas Simples:**

- ✔ Tensão: 12VCC @ 500mA;
- ✔ Força de Tração: 270kgf;
- ✔ Com sensor magnético interno tipo contato seco;
- ✔ Deverá possuir supressor interno de pico de tensão.

**Especificações - Portas Duplas:**

- ✔ Tensão: 12VCC @ 2x500mA;
- ✔ Força de Tração: 2x270kgf;
- ✔ Com 2 sensores magnético interno tipo contato seco;
- ✔ Deverá possuir supressor interno de pico de tensão.

### 5.4 Controladora

A Controladora funciona com servidor para áreas específicas, integrados à rede local, através de uma porta TCP/IP 10/100/1000Mbits. Possuem processamento e banco de dados próprio, atualizados e supervisionados pelo Servidor Central do Sistema de Controle de Acessos (SCA).

Cada Controladora realiza o processamento informações de uma determinada área, através do grupo de acessórios instalados nos pontos de acesso da sua área de abrangência, tomando as decisões necessárias para a liberação ou bloqueio dos acessos às áreas a ela atreladas.

A controladora possui alimentação elétrica exclusiva, com fonte alternativa através de baterias com carregamento automático e autonomia mínima para 6,0 (seis) horas

**Principais características:**

- ✔ Processador de alta velocidade de 32 bits;
- ✔ Communication Comunicação de rede TCP / IP, com interface de rede auto adaptável;
- ✔ Dados de comunicação criptografados para garantir segurança da informação;

- ✔ Suporta interface RS-485 e Wiegand para acessar leitoras;
- ✔ Storage Armazenamento massivo para até 10.000 usuários e 50.000 registros de leitura;
- ✔ Suporte a função de primeiro cartão, supercartão e função super senha, função de atualização online e controle remoto on-line das portas;
- ✔ Suporte vários tipos registros, tais como normais, desativado, lista negra, patrulha, visitante, coação, etc.
- ✔ Suporte alarme inviolável para leitora, alarme de porta não segura, porta de entrada forçada alarme, alarme para tempo limite de abertura da porta, alarme forçado e alarme para cadastro inválido, alarme de armazenamento insuficiente para evento offline, alarme de quebra de rede, etc.;
- ✔ Suporte a operação em modo de online e offline;
- ✔ Suporte à sincronização de hora via NTP, método manual ou automático;
- ✔ Possibilidade de salvar dados permanentemente, mesmo quando o controlador de acesso estiver desligado;

### 5.5 Estações de trabalho

A arquitetura de gestão de segurança que se preconiza, para o Sistema de Controle de Acessos (SCA), prevê a instalação de uma ET (Estação de Trabalho) principal, localizada Central de Segurança, permitindo o monitoramento global de todo o sistema SCA e respectiva interligação funcional com os restantes sistemas de segurança.

Está previsto a instalação de 6 (seis) Estações de Credenciamento na Sala de Atendimento/Espera, para efetuar o credenciamento de funcionários e visitantes, mediante o registro de digitais atrelado ao banco de dados com informações pessoais de cada pessoa cadastrada.

### 5.6 Hardware e software.

O sistema será composto de hardware, software e demais dispositivos necessários para o gerenciamento do sistema, garantindo todos os recursos associados a um sistema desta natureza, tais como:

- ✔ Cadastramento de usuários;
- ✔ Definição de níveis de acesso;
- ✔ Horários de acesso;
- ✔ Captação e consulta de dados, de fotos digitais, e de relatórios;
- ✔ Emissão de identificação autoadesiva para identificação visual de visitantes;
- ✔ Confecção dos cartões de identificação para funcionários;
- ✔ Integração com os dispositivos de campo (leitoras, controladoras, fechaduras, etc.).

#### 5.6.1 Software plataforma de integração.

O software da Plataforma de Integração encontra no âmbito do escopo de fornecimento do Sistema de Videomonitoramento (CFTV).

**5.6.2 Software de controle de acessos.**

O software de Controle de Acesso deverá plena compatibilidade e integração com as controladoras do sistema, apresentando as características e capacidade de gestão discriminadas nos itens a seguir:

- ✔ Deverá ser de uso fácil e intuitivo, devendo possuir sistema de telas e ícones, para inicialização e operação do sistema.
- ✔ Acesso através de fornecimento de usuário (login) e senha (password), com registro em log de eventos.
- ✔ O software de gerenciamento deverá disponibilizar todas as funções no console do operador, tais como apresentação de alarmes e outras informações de status do sistema em telas coloridas no monitor de vídeo, tendo a opção de imprimi-las em papel via impressora. A aplicação deverá requerer um mínimo de operação via teclado.
- ✔ O sistema deverá permitir a operação através do uso de mouse e teclado. A interface fará uso de ícones, sub-menus e/ou menus, como forma de acesso às funções e recursos disponíveis ao usuário do sistema.
- ✔ O sistema terá um menu principal, no qual deverá constar uma seção de ajuda ao usuário. Deverá apresentar continuamente, uma barra de diagnósticos na parte interna da tela do monitor de vídeo. O diagnóstico deverá incluir, dentre outras, as operações do sistema, e as falhas de comunicação, de status do banco de dados, dos aplicativos e das unidades processadoras.
- ✔ Diagnósticos mais detalhados deverão ser disponibilizados em telas separadas por itens, como por exemplo, o estado atual de dispositivos em alarmes sonoros e indicadores de erros.
- ✔ O Sistema processará todas as mudanças de estado detectadas pelas unidades remotas e qualquer mudança de estado, deverá ser comunicada ao servidor, processada e apresentada na tela da estação de trabalho, do operador do sistema. Todas as mudanças de estado deverão ser registradas com as informações de dia, mês e horário em que a mudança ocorreu.
- ✔ O software de controle de acesso terá a função de permitir o cadastro, controle de acesso e supervisão em tempo real. Podendo operar as portas, cadastrar usuários com diversos níveis de acesso e possuir rastreamento de usuários, visitantes e contratados.

Para efeitos desta Especificação Técnica, os componentes de software deverão desempenhar as seguintes funções de geração de credenciais, monitoração e controle de acesso:

- ✔ Possibilidade de monitoramento dos eventos de acessos, alarmes e imagens do Sistema de Videomonitoramento de qualquer estação cliente do software, com limitação de acesso controlada de acordo com as permissões do usuário;
- ✔ Importação de cadastros de usuários da Base dados;
- ✔ Levantamento da identificação dos usuários que tiveram solicitações de acesso negadas;
- ✔ Possibilidade de programação de controle de acesso, a determinado local, em função de calendário, horário, ou políticas de segurança;
- ✔ Possibilidade de bloqueio de acesso local, através de comandos na estação de controle;
- ✔ Possibilidade de bloqueio de usuários ou credenciais, através da estação de controle;
- ✔ Restrição de acesso ao software através de senhas e níveis de acesso para os operadores;

- ✔ Quatro níveis de acesso ao sistema, sendo eles: administração, operação, identificação e supervisão;
- ✔ Registro de comandos executados pelo operador do sistema;
- ✔ Programação de data de ativação e validade das credenciais de acesso, bloqueando automaticamente o mesmo quando do vencimento desta;
- ✔ Possibilidade de alteração na programação das leitoras;
- ✔ Alarme com indicação da leitora de credenciais onde houve tentativa de acesso indevido;
- ✔ Registro do alarme de acesso negado, com informação do motivo pelo qual a solicitação de acesso não foi concedida (local não autorizado; horário não autorizado; senha inválida; etc.);
- ✔ Registro dos acessos em cada leitora, vinculando aos dados da credencial, ao horário, leitora e local;
- ✔ Recurso para consulta, dos dados do usuário de credencial através de qualquer estação do software, fornecendo os dados de acesso a determinado local;
- ✔ Possibilidade de programação de rondas de guarda baseado em leitores de acesso e pontos de alarme;
- ✔ O sistema deverá possuir menus de ajuda do tipo “pop-up” para assistir o operador na operação do sistema, de forma clara e rápida. O acesso será feito via ponteiro do mouse ou através de menu padrão Windows ou pela tecla F1 do teclado;
- ✔ Os registros de acesso devem ser armazenados no servidor;
- ✔ A capacidade de armazenamento, dos registros de acesso deve ser elevada;
- ✔ Facilidade para a emissão imediata de relatórios de todos os registros de acesso armazenados;
- ✔ Alarmes de arrombamento e porta aberta;
- ✔ As telas devem ter identificação das portas de acordo com a planta do local;
- ✔ Habilitação de novas credenciais e cancelamento das mesmas, através do módulo supervisor, ou seja, no módulo Identificação somente é permitida a inclusão de novas credenciais, mas as permissões de acesso só podem ser liberadas no módulo supervisão;
- ✔ Possibilidade de criação de rotinas de acionamento com acionamento de portas de um mesmo grupo, para situações de evacuação, emergências, etc...
- ✔ Captação e consulta de dados, de fotos digitais e de relatórios;

**Especificações mínimas do software:**

- ✔ Possuir interface Web;
- ✔ Base de dados SQL Server 2014 ou superior;
- ✔ Permitir idioma em português;
- ✔ Possuir controle automático de fuso-horário e horário de verão;
- ✔ Possuir relatórios completos, totalmente customizáveis, com exportação para diversos formatos;

- ✔ Possuir cadastro com campos customizáveis;
- ✔ Possuir campos para busca rápida configuráveis por tipo de usuário;
- ✔ Possuir busca avançada de usuários com edição em lotes;
- ✔ Permitir até quatro fotos por usuário;
- ✔ Possuir ferramenta de design integrada para layout da tela de cadastro;
- ✔ Possuir tela auxiliar de cadastro totalmente customizável;
- ✔ Possuir controle de Visitantes, Funcionários, Contratados;
- ✔ Possuir controle de Ativos, Veículos, Empresas, Entrada e saída de materiais;
- ✔ Implementar controle de usuários e empresas com restrições de acesso (lista negra);
- ✔ Implementar datas de validade de usuários e cartões, além de cartões provisórios
- ✔ Implementar diferentes situações para controle de usuários (ativos, inativos, férias, desligados, etc);
- ✔ Possuir controle de acesso através de local e horário, com combinações ilimitadas;
- ✔ Implementar tipos de ações que podem ser iniciadas a partir de eventos;
- ✔ Implementar pelo menos 3 tipos de anti-passback, que podem impedir o acesso, gerar um alarme ou ambos;
- ✔ Permitir contagem máxima e mínima de usuários em uma zona, que pode impedir o acesso, gerar um alarme ou ambos;
- ✔ Permitir contagem de marcações;
- ✔ Permitir controle de ronda;
- ✔ Possibilitar controle de horários e estações permitidos de login;
- ✔ Implementar políticas de complexidade e validade de senhas configuráveis;
- ✔ Permitir suporte a perfis de acesso ao sistema ilimitados e detalhados;
- ✔ Permitir base de dados particionada, possibilitando o compartilhamento do sistema entre diferentes clientes;
- ✔ Implementar auditoria completa das ações do operador;
- ✔ Permitir supervisão e controle de todos os dispositivos do sistema através de telas gráficas customizáveis por ferramenta de design integrada;
- ✔ Permitir suporte a alarmes configuráveis em diversos níveis e individualmente para controladores, leitoras, entradas, saídas e usuários;
- ✔ Possuir tela que permita o acompanhamento em tempo real de todas as transações de cartões e eventos do sistema;
- ✔ Possuir tela de alarmes em tempo real com registro de reconhecimento e diversos níveis de prioridade;

✔ Possuir configuração de envio de e-mails em caso de eventos ou alarmes;

**Telas de Operação.**
Todas as telas de operação, manuais e boletins técnicos de consulta deverão estar, obrigatoriamente, em língua portuguesa. Em relação ao software, no mínimo, deverão ser entregues os seguintes documentos:

✔ Documento de Visão: Descrição completa do produto ofertado em termos de necessidades e características funcionais do sistema.

✔ Documento de Regras de Negócios: Identificação e descrição das regras de negócios.

✔ Especificação de Casos de Uso: Identificação dos atores, descrição do fluxo básico, descrição de fluxos alternativos, identificação das pré-condições, identificação das pós-condições e identificação de referências.

✔ Modelo de Dados: Descrição do modelo de representação lógica e física dos dados persistentes do sistema, abrangendo também qualquer comportamento definido no banco de dados, tais como: tablespaces de dados e índices (nome/tamanho), com a previsão de crescimento calculada, scripts de criação dos objetos do banco, procedimentos armazenados, triggers, etc.

✔ Dicionário de Dados: Definição precisa sobre os elementos de dados, perfis de usuários, papéis e privilégios, descrição de objetos, integridade de restrições, stores procedures e triggers, estrutura geral da base de dados.

**Projeto Arquitetural.**

✔ Manual do Usuário: Descrição completa dos procedimentos para ajudar a operar o sistema no ambiente do cliente.

✔ Manual de Operação e Produção: Descrição dos procedimentos de instalação/configuração do sistema, procedimentos para manter o sistema em produção (monitoramento, backup, limpeza de arquivos temporários, log, etc.) e com informações para um atendimento de primeiro nível a ser prestado pela Central de Atendimento.

**Características funcionais mínimas da solução:**
A solução deverá disponibilizar, no mínimo, as seguintes características funcionais, sem exclusão de outras:

✔ Deverá combinar todos os recursos/ferramentas de segurança em um ambiente operacional, do tipo multitarefa e multiusuário e utilizar sistema de arquitetura aberta e padrão de mercado, de configuração modular, que atenda as necessidades, atuais e futuras, do usuário;

✔ Deverá dispor de interface de usuário, do tipo gráfica, que permita ao operador responder alarmes, investigar ocorrências e gerenciar solicitações de relatórios rotineiros com rapidez e precisão, bem como capacidade de edição, pelo usuário, de mapas coloridos e de, dentre outros, os seguintes recursos:

- Processamento avançado de eventos;
- Editor abrangente de geração de relatórios;
- Janelas de apresentação de todos os “status” do sistema;
- Facilidades de instruções de alarmes e relatórios de respostas definidas pelo usuário;

- Interface para bip (“pager”), sintetizador de voz, telefone, etc., configurada pelo usuário;
- Capacidade de visualizar, reconhecer e responder a todos os alarmes a partir de uma mesma tela;
- Capacidade de monitorar alarmes a partir de mapas interativos, de tempo real, com identificação imediata e localização exata da ocorrência;
- Utilizar mapas para realizar funções de entradas e saídas (I/O) do sistema;
- Apresentação, na tela, da imagem dos detentores de cartão de acesso, para qualquer transação do cartão, em tempo real, com recursos de filtragem, pelo operador, de quem, em que condições, aonde ou quando;
- Tela de configuração intuitiva, fácil e rápida, do “hardware”, inclusive das Unidades Controladoras de Área;
- Telas que descrevam em detalhes (profundidade) as descrições, o histórico e as atividades de resposta de todos os alarmes;
- Recursos de endereçar (predeterminar) alarmes para ocorrerem na tela de operadores especificados;
- Telas que apresentem todas as atividades do sistema;
- Telas que apresentem o desempenho da Estação de Trabalho, bem como “status” de todas as interfaces, os carregamentos (“downloads”) e espaço disponível em disco;
- Telas que apresentem em tempo real, “status” de:
  a) Unidades Controladoras;
  b) Leitores;
  c) módulos de entradas e saídas digitais.

✔ Computador Central com configuração totalmente redundante;

✔ Disponibilidade de ampla biblioteca de relatórios padrões e editor de relatórios de fácil uso;

✔ Deverá possuir dispositivos que detectarão a presença de alguém no ambiente controlado e/ou a abertura de uma porta por meios alheios ao SCA e serão supervisionados pela unidade controladora, a qual tomará as medidas cabíveis, conforme programado, tão logo verifica a mudança de estado destes dispositivos;

✔ Suportar várias tecnologias de leitores de cartões, de forma a oferecer o máximo de flexibilidade ao usuário;

✔ Opções de agendamentos programáveis por portas e por áreas, para atender os requisitos particulares/próprios das edificações do usuário;

✔ Facilidade de expansão com a simples adição modular de placas, controladores e/ou “software”;

✔ Controle de estado de portas, em modo controlado, em modo destravado e em modo travado, com determinação do intervalo de tempo para o estado selecionado pelo operador;

✔ Configurar zonas de tempo para determinados usuários, em determinados leitores e em determinados horários (com vários intervalos de início e fim e vários dias);

✔ Permitir abertura e fechamento de portas através da Central de Operação de forma automática;

✔ Permitir abertura e fechamento de portas de forma manual em caso de PANE no sistema por qualquer motivo;

✔ Facilidade de subdividir a edificação em áreas lógicas de segurança, as quais deverão ser dinamicamente ilustradas no “display” central (tela principal), de forma a facilitar ao operador a visualização das informações de acesso e facilidade em responder mais rapidamente aos eventos;

- ✔ Possibilidade de pesquisa e visualização imediata da constatação de quais detentores de cartões de controle de acesso estão na área selecionada;
- ✔ Indicação gráfica da localização da presença de usuários e possibilidade de rastreamento, pelo operador, da rota percorrida pelo usuário até chegar na área em que o mesmo se encontra;
- ✔ Facilidade e rapidez de pesquisa, classificação e atendimento a condições estabelecidas pelo operador, das informações de transações dos detentores de cartões de acesso, registradas no banco de dados relacional;
- ✔ Ferramenta de emissão de relatórios gerenciais, que possibilitem o monitoramento das atividades do operador, o movimento dos usuários selecionados e as transações de todo o sistema;
- ✔ Lista de tempo real que apresente todas as atividades do sistema, no horário em que as mesmas ocorrem, com recursos de filtragem para incluir na lista apenas as mais importantes para o operador, ou todas as transações do sistema;
- ✔ Possibilidade de se estabelecer regras que garantam, dentre outras, que para áreas determinadas, somente será permitido acesso se dois ou mais usuários estiverem presente;
- ✔ Dispor de recurso de “anti-passback”, de forma que qualquer usuário só possa validar um novo acesso a uma área em que ele recém ingressou, somente se estiver previamente validado o seu egresso daquela mesma área;
- ✔ Permitir ao operador designar convenientemente qualquer combinação de portas para cada usuário (agrupamento de acesso);
- ✔ Carregar (“download”) a base de dados nas unidades controladoras a partir do computador central e disponibilizar autonomia nas unidades controladoras para tomar todas as decisões de controle de acesso, independentemente de o computador central estar “on-line”;
- ✔ Permitir que várias estações de trabalho distribuídas em rede TCP/IP, operem simultaneamente o sistema;
- ✔ Impressão em tempo real;
- ✔ Permitir que o usuário crie mapas coloridos para apresentação de alarmes;
- ✔ Dispor de ajuda e de manuais de operação/assessoramento técnico “on-line”;
- ✔ Deverá requerer para configuração do sistema, apenas a denominação dos leitores e dos pontos de entrada e de saída, pontos digitais;
- ✔ Integração com o Sistema de Detecção e Alarme de Incêndio, com o Sistema de Captação de Imagens (fotografia digital) e Edição de Cartões e Banco de Imagens, com o Sistema de TV de Vigilância;
- ✔ Base de Dados distribuídos nas Unidades Controladoras, as quais deverão permanecer funcionando e tomando decisões, fundamentadas na sua base de dados residente, mesmo nas circunstâncias em que haja perda de comunicação com o computador central;
- ✔ Capacidade de operação no modo autônomo (standalone), de forma que a unidade controladora de área possa assumir o comando da área abrangida pela mesma, independentemente da atuação do computador central;

- ✔ Proteção dos dados históricos das unidades controladoras em memória não volátil e recursos de enviar os dados das transações ocorridas no transcorrer da interrupção da comunicação com o computador central, tão logo a comunicação entre ambos seja reestabelecida.
- ✔ Deverá utilizar arquitetura Cliente/Servidor;
- ✔ Plano de atualização de software por um período mínimo de 36 (trinta e seis) meses, garantindo o fornecimento de todas as novas versões e correções liberadas pelo fabricante do software e sem nenhum ônus adicional;
- ✔ Integração com SQL Server para gerenciamento da Base de Dados;

**Apresentação de Alarmes:**

- ✔ Uma janela inicial de apresentação de alarmes deverá identificar de forma automática e inconfundível, os novos alarmes e seus graus de prioridades. A apresentação dos alarmes na tela do monitor é acompanhada de uma indicação audível (a ser configurado pelo operador). É necessária a intervenção do operador, para se efetuar o silenciamento.
- ✔ O operador terá a possibilidade de definir a importância de cada alarme de acordo com um código de cores personalizado, bem como selecionar quais os tipos de eventos que deverão ser exibidos nesta janela.
- ✔ Para o reconhecimento do alarme tem de existir intervenção do operador. O reconhecimento de alarmes é permitido a partir da tela de apresentação inicial, ou a partir de qualquer nível de hierarquia de apresentação de alarmes. O reconhecimento de um alarme causa, para todas as indicações de condição de alarme, que o referido alarme está no estado de reconhecimento.
- ✔ O sistema permite que o operador possa digitar uma informação de resposta ao sistema de uma lista predefinida de causa provável de alarme, permitindo também a inclusão de outras respostas à lista existente.
- ✔ A remoção de qualquer alarme de uma lista de alarmes ativos só ocorre através da intervenção do operador.
- ✔ Todas as informações de alarmes, inclusive data e hora, são armazenadas no banco de dados do sistema.
- ✔ Qualquer mal funcionamento e anormalidades relacionadas com as Controladoras, linhas de comunicações e demais periféricos / dispositivos do sistema, deverão ser comunicadas ao operador.

**O sistema possibilita ao operador a emissão dos seguintes relatórios:**

- ✔ Por pessoas;
- ✔ De configuração;
- ✔ De status de dispositivos;
- ✔ De informações históricas;
- ✔ De atividades do usuário;
- ✔ De atividade de alarme;

✔ De atividade do operador (por forma a auditar o operador).

A geração dos relatórios não causa qualquer degradação no desempenho do sistema.

O sistema deverá ser programado para relatórios pré-configurados. Sendo necessário, deverá ser possível criar novos relatórios.

O editor de relatórios deverá possibilitar o agrupamento e a seleção de relatórios, por qualquer campo dentro dos mesmos e nomeá-los em conjunto para um arquivo com um único nome definido pelo operador.

O editor de relatórios deverá possibilitar que com o uso de "macros" se elabore, de forma simples e rápida, formatos complexos de relatórios.

### 5.6.3 Módulo de software para credenciamento

O aplicativo deverá ser instalado nas estações de credenciamento dos usuários. Estas estações deverão integrar a base de dados do Servidor Principal, lendo e gravando informações na base de dados (Microsoft SQL Server).

A aplicação deverá correr em cima de sistema operacional Windows em português (Brasil).

## 5.7 Cancelas Automáticas.

As cancelas serão instaladas nas vias de acesso de veículos para a GARAGEM 1, controladas pelo Sistema de Controle de Acessos.

Deverão fornecidas 2 (duas) cancelas novas (Entrada e Saída da G1). Em função da altura de "pé direito" dos Pavimentos de Garagens, deverão ser utilizadas cancelas articuladas, ou, a alternativa de utilizar 2 (duas) cancelas na mesma via de acesso, sendo uma de cada lado da via, formando uma barreira única. Neste caso, serão o total de 4(quatro) cancelas.

Todas as cancelas deverão ser de um único fabricante, facilitando a reposição de peças e manutenção dos equipamentos;

As cancelas existentes no condomínio deverão passar por processo de manutenção, visando o pleno e perfeito funcionamento. As cancelas que apresentarem alto índice de defeitos serão descartadas. As cancelas recuperadas ficarão com reserva, para futura aplicação em caso de defeitos nas operacionais.

**Características gerais.**

- Braço de até 4m;
- Sistema Swing-Away, evita que o braço e a cancela sejam danificados na passagem não permitida ou forçada;
- Facilidade de inversão na direção do braço. (posicionado à esquerda ou à direita no mecanismo);
- A unidade de controle da cancela com 7 modos distintos de operação;
- Tempos de abertura e fechamento de até 0,9 segundos;
- Possibilidade de programação de tempo de abertura e fechamento de até 4 segundos;
- Acionamento eletromecânico que permita um movimento dinâmico, sem vibrações, oscilações ou escorregamentos da haste;
- Braço cilíndrico com até 4,0m de comprimento na cor branca e faixas refletivas na cor vermelha;
- Disponibilidade para iluminação de LED no braço;
- Gabinete confeccionado em aço com tratamento anticorrosivo e pintura eletrostática a pó de alta aderência, montagem monobloco com cantos arredondados para prevenção de acidentes;

**Características Técnicas.**

- Alimentação: 85 – 264 VAC, 50/60 Hz;
- Consumo Energético: de95 a 225W, conforme modelo;
- Ciclo de Trabalho: 100%;
- Índice de Proteção: IP-54
- Faixa de temperatura: −30 a +55 °C

**5.8 Acesso por TAG.**

As cancelas serão comandadas por leitores de aproximação (RFID)., com antenas de leitura tipo TAG. Serão utilizados leitores de longa distância, tornando a solução eficiente e confortável aos usuários.

Os leitores de cartões TAG serão aplicados nas vias de acesso para veículos, motos, bicicletas ou outros que portem o cartão, com leitura bidirecional, ou seja, entrada e saída, utilizando dois leitores para cada via de acesso.

O edifício do TECNOCENTRO possui uma única via de acesso às garagens, com “Entrada” e “Saída”, conforme caracterizado no desenho inserido no final deste Anexo.

**Características Gerais:**

- ✔ Leitor de longa distância, com capacidade de leitura de até 6m (seis metros), com proteção para utilização em ambientes externos;
- ✔ Capacidade de leitura de cartões TAG de mercado, inclusive dos utilizados em sistemas de passagem em pedágios e estacionamentos;
- ✔ Software de configuração com parâmetros de leitura do equipamento via RS232, possibilitando a configuração de cartões de outros fabricantes.

**Características Técnicas do Leitor.**

- ✔ Alcance potente e de alta precisão;
- ✔ Frequência de operação: 915 a 928 MHz;
- ✔ Software para configurar parâmetros de leitura do equipamento via RS232;
- ✔ Compatível com a linha de controladoras de acesso;
    - Tensão de alimentação: 9 a 16Vdc;
    - Corrente máxima de consumo: 980mA;
    - Frequência de operação: 915 a 928 MHz;
    - Distância de operação: Até 6m;
    - Temperatura de operação: -20 °C a 55 °C

- Interface de comunicação: Wiegand 26 ou Wiegand 34;
- Comunicação PC: RS232;
- Máxima distância de cabeamento de dados: 25 m;
- Proteção: IP-65.

Produto de referência: LE 150 EP UHF – Intelbrás.

**Características Técnicas do cartão - TAG.**

✔ Etiqueta de acionamento RFID veicular 900 MHz;

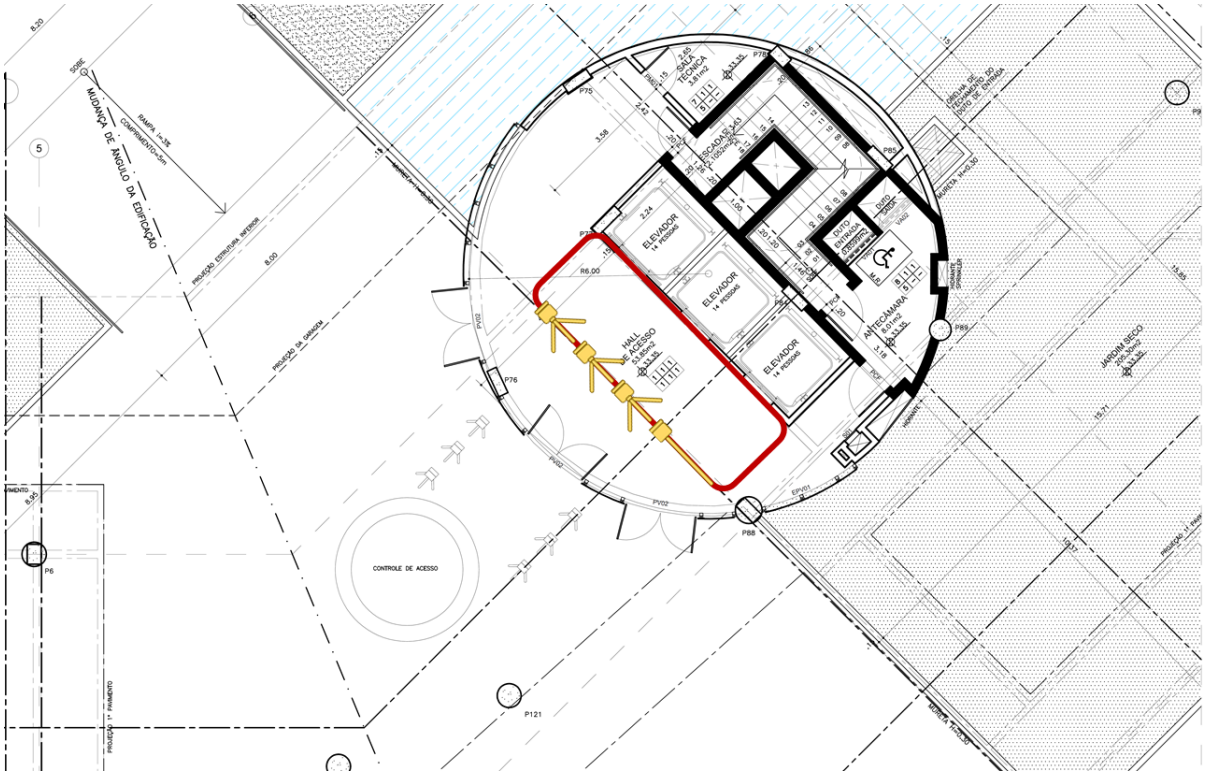
✔ Uso externo IP65;

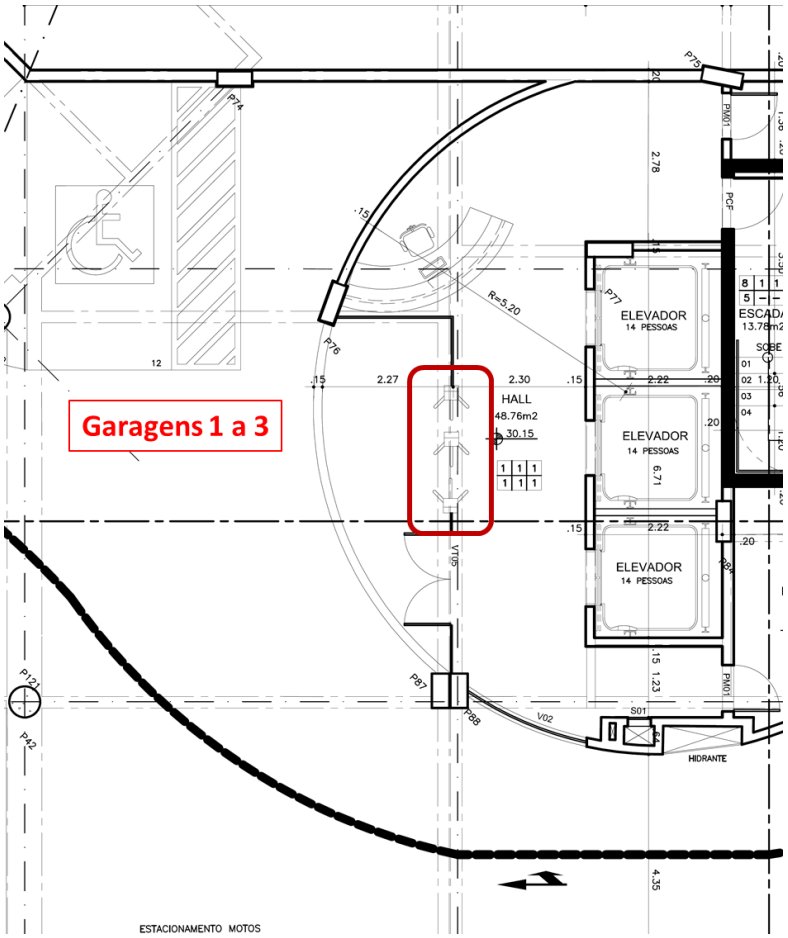
✔ Utilizada em carros e motos e outros meios.

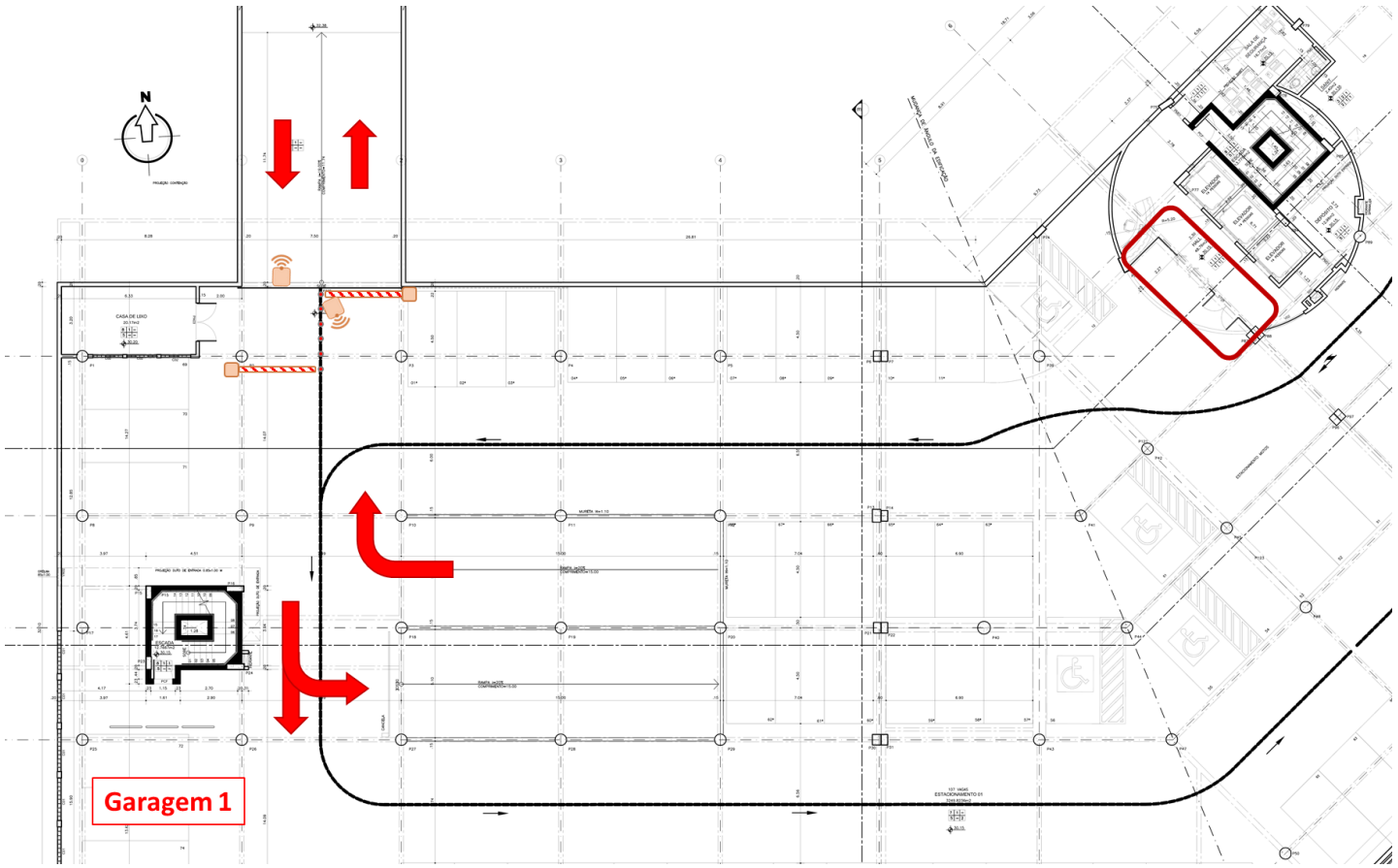
- Frequência: 860 ~ 960 MHz;
- Dimensão: (L × A × P) 135 × 22 × 13 mm;
- Peso: 18 g;
- Temperatura de operação: -10 ºC ~ 60 ºC;
- Distância de leitura: 6 m.

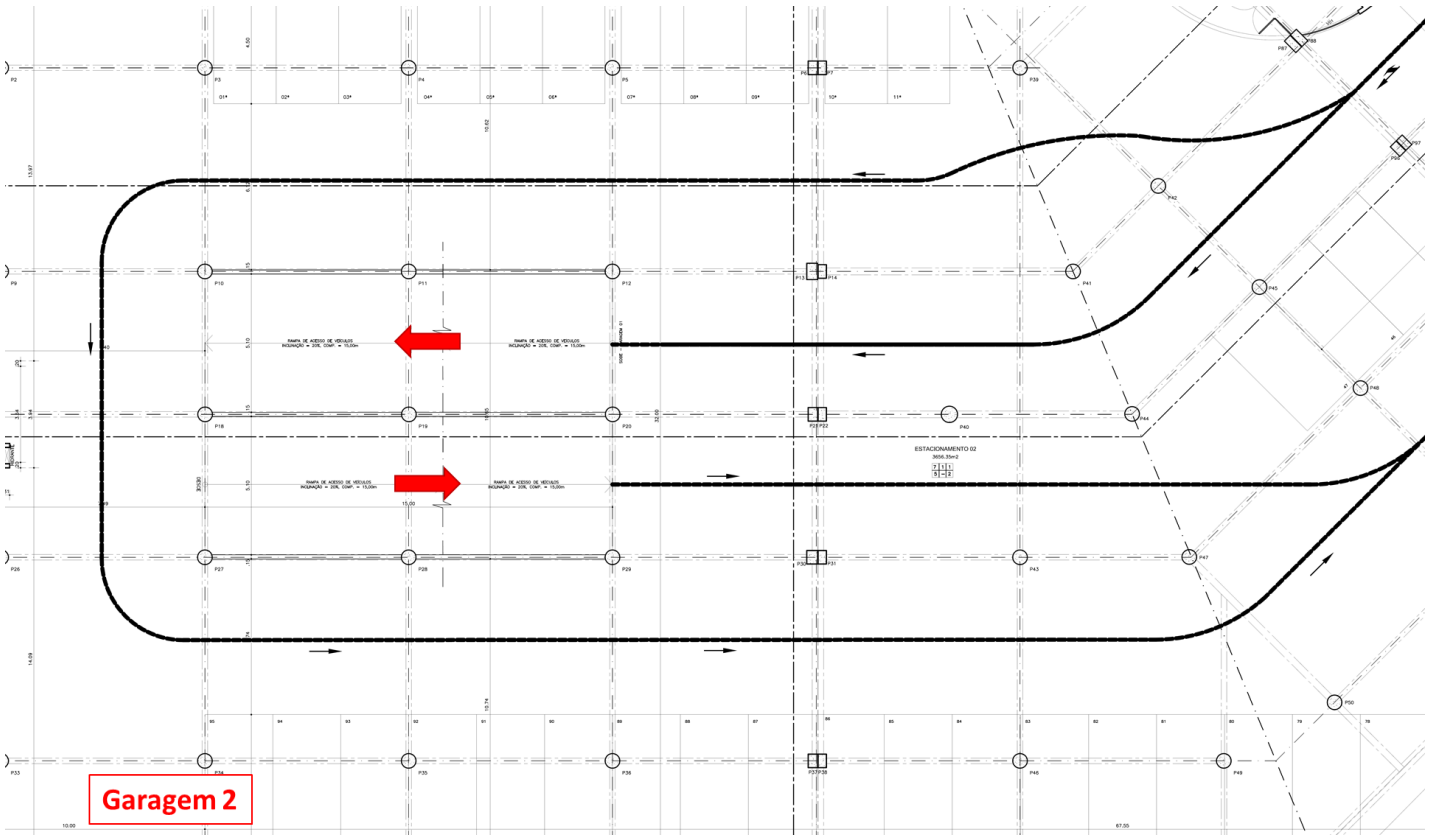
Produto de referência: TAG TH 3020 UHF.

## 6. Imagens do Projeto




N
Garagem 1


RAMPA DE ACESSO DE VEÍCULOS
INCLINAÇÃO = 20%, COMP. = 15,00m
RAMPA DE ACESSO DE VEÍCULOS
INCLINAÇÃO = 20%, COMP. = 15,00m
RAMPA DE ACESSO DE VEÍCULOS
INCLINAÇÃO = 20%, COMP. = 15,00m
RAMPA DE ACESSO DE VEÍCULOS
INCLINAÇÃO = 20%, COMP. = 15,00m
ESTACIONAMENTO 02
3656.35m2
Garagem 2

Garagem 2