ADITIVO AO CONTRATO DE PRESTAÇÃO DE SERVIÇOS ESPECIALIZADOS EM SEGURANÇA ELETRÔNICA (locação de equipamentos, atualização de software, manutenção dos equipamentos e sistema, suporte telefônico e treinamento) firmado em 01 de maio de 2013– (PREÂMBULO – RESUMO).

1. **PARTES:**

Contratante: Instituto de Gestão e Humanização – IGH.
CNPJ: 11.858.570/0001-33
Contratado: Star Segurança Eletrônica LTDA.
CNPJ: 02.713.790/0001-88

TOMBO 034 / HMI-A
VISTO
DATA 12 / 11 / 14

2. **OBJETO:**

Contrato de Prestação de serviços de segurança eletrônica, rastreamento veicular e controle de acesso.

3. **LOCAL DA EXECUÇÃO DOS SERVIÇOS:**

Hospital Materno Infantil – HMI, registrado no CNES sob o nº 2339196, com sede Av. Perimetral - Setor Oeste, Goiânia - GO, 74125-120.

4. **VALOR DO CONTRATO:**

Valor mensal de R$ 8.727,68 (Oito mil setecentos e vinte e sete reais e sessenta e oito centavos).

5. **PRAZO DE VIGÊNCIA DO CONTRATO:**

1 (um) ano, podendo ser renovado por igual período à critério do Contratante.

6. **Forma de pagamento:**

O pagamento da fatura ocorrerá todo dia 10 (dez) do mês subsequente ao início da prestação dos serviços.

Pelo presente instrumento, de um lado, o **INSTITUTO DE GESTÃO E HUMANIZAÇÃO – IGH** (doravante designado "**Contratante**"), inscrito no CNPJ/MF sob o nº 11.858.570/0001-33, com sede na Rua das Rosas, nº 622, Pituba, Salvador, Bahia, representado neste ato pelo seu Superintendente, **Paulo Brito Bittencourt**, Administrador de Empresas e Advogado, portador do documento de identidade 0354215507 SSP/BA, inscrito no CPF/MF sob o nº 457.702.205-20, residente e domiciliado em Salvador/BA, e, de outro lado, **STAR SEGURANÇA ELETRÔNICA LTDA -EPP**, pessoa jurídica de Direito Privado, devidamente inscrita no CNPJ nº 02.713.790/0001-88, situada no Setor de Armazenagem e Abastecimento, Quadra 01, nº 1100, Parte D, Asa Norte, Brasília – DF, CEP: 70.632-100, neste ato representada consoante contrato social em anexo, (doravante designado "**Contratada**"), mediante consenso que entre si mutuamente aceitam e outorgam, resolvem celebrar o presente **Aditivo ao Contrato de Prestação de Serviços Especializados em Segurança Eletrônica (locação de equipamentos, atualização de software, manutenção dos equipamentos e sistema, suporte telefônico e treinamento) firmado em 01 de maio de 2013**, fazendo-o reger-se pelas seguintes cláusulas e condições:

Cláusula 1. Premissas.

1.1. São premissas influentes e substanciais do presente contrato as seguintes considerações:

a) O **Contratante** é gestora de renomada instituição hospitalar que necessita de implantação e gerenciamento de sistema de segurança eletrônica;

b) O **Contratante** publicou em diário oficial, jornal de grande circulação local e *website* institucional Processo Seletivo para Contratação de serviços especializados em segurança eletrônica, tendo a **Contratada** apresentado melhor proposta;

c) Considerando a decisão posterior da Diretoria Geral do Hospital Materno Infantil - HMI em investir em segurança e controle de acesso na unidade;

d) Considerando que a Contratada é atual prestadora de serviços de segurança eletrônica no Hospital Materno Infantil - HMI;

e) Considerando que os serviços ora contratados estão diretamente relacionados com os serviços contratados em 01 de maio de 2013;

f) Considerando que o valor do presente aditivo não excede a 25% (vinte e cinco por cento) do valor estabelecido em contrato principal;

g) O **Contratado** tem interesse em assistir o **Contratante** em suas necessidades conforme as tratativas mantidas com a mesma;

h) O **Contratado** declara ter ciência do inteiro teor do contrato de gestão tombado sob o nº 131/2012-SES-GO.

Cláusula 2. Objeto.

2.1. O objeto do presente **Contrato de Prestação de serviços de segurança eletrônica e controle de acesso** para o Hospital Materno Infantil – HMI, registrado no CNES sob o nº 2339196, com sede Av. Perimetral - Setor Oeste, Goiânia - GO, 74125-120, atualmente sob gestão, em regime de OS, pelo **Contratante** em contrato de gestão firmado com a **Secretaria de Saúde do Estado de Goiás**.

Cláusula 3. Do valor do contrato e prazo para pagamento:

3.1. Pela prestação dos Serviços a **CONTRATANTE** pagará à **CONTRATADA**, o valor mensal de R$ 8.727,68 (Oito mil setecentos e vinte e sete reais e sessenta e oito centavos), mediante apresentação, pela **CONTRATADA**, de fatura acompanhada de Nota fiscal.

3.2. O pagamento da fatura ocorrerá todo dia 10 (dez) do mês subsequente ao início da prestação dos serviços, devendo a Contratada apresentar até o dia 5º (quinto) dia do mês subsequente a prestação dos serviços, boleto bancário à Contratante, sob pena de prorrogação proporcional do prazo de pagamento.

3.3. A Nota Fiscal deverá ser acompanhada de certidões que comprovem regularidade fiscal da Contratada em âmbito Federal, Estadual e municipal, Justiça do Trabalho, além de certidões que comprovem regularidade de contribuições relativas a FGTS e INSS.

3.4. O pagamento somente será efetuado mediante crédito em conta bancária de titularidade da Contratada, sendo vedada emissão de boletos.

Cláusula 4. Obrigações do Contratado.

4.1. Caberá a **Contratada**, dentre outras obrigações legais e ou constantes do presente contrato:

a) Implantar o sistema de controle de acesso no Hospital Materno Infantil - HMI, obedecendo aos ditames prescritos em proposta comercial também colacionada aos autos do PROSEL 015/2013;

b) Instalar e fornecer, de imediato, às suas expensas, os seguintes equipamentos: 10 (dez) leitoras de catracas de acesso; 02 (duas) catracas gabinetes com corpo em inox e cofre coletor; 01 (uma) catraca pedestal especial com braço que cai; 01 (uma) catraca para PNE total inox; 02 (dois) software da controladora de catraca; 02 (dois) software da controlada de catraca; 02 (dois) braços que cai para catraca; 03 (três) integrações de leitora; 04 (quatro) controle de catracas ou torniquetes: Placa controladora SCAIIP-CF-PCB ETHERNET - TCP/IP NATIVO 10/100MBPS com fonte 20A com carregador de bateria incorporada 12IN / 02 out monit. alimentação AC/DC; 04 (quatro) placas de expansão de relés para controlador de catraca para cofre ou visitante para qualquer catraca; 04 (quatro) transformadores 145VCA 3A; 04 (quatro) baterias seladas 12VCC 7AH; 01 (um) software SCAIIP-TCP/IP - módulo de aplicação de global anti-passback; 02 (dois) software SCAIIP-TCP/IP - Módulo de aplicação de liberação integrada com incêndio; (05) cinco software

SCAIIP web based para navegador web TCP/IP, incluindo integração com CFTV híbrido: analógico e IP quadro sinótico emissão de relatórios, cadastramento e gerenciamento de usuários, com licença de porta; 03 (três) hardware cadastro de acesso e visitantes; 05 (cinco) software pack para gerenciamento de 01 canal IP, e 01 licença;

c) Promover a atualização dos softwares sempre que necessário, havendo ou não, solicitação da Contratante, devendo a Contratada arcar integralmente com custos de mão de obra, transporte, impostos, taxas, contribuições e insumos porventura necessários;

d) Promover a manutenção preventiva e corretiva nos equipamentos descritos em proposta comercial também colacionada ao PROSEL 015/2013, arcando integralmente com custos de mão de obra, transporte, impostos, taxas, contribuições e insumos porventura necessários;

e) Prestar suporte técnico presencial e por telefone, sempre que solicitado pela Contratante;

f) Promover, às suas expensas, treinamento de pessoal vinculado à Contratante para melhor utilização dos equipamentos ora fornecidos, instalados e configurados pela Contratada;

g) Promover a imediata substituição dos equipamentos locados acima descritos e em proposta comercial também colacionada ao PROSEL 015/2013, sempre que estes apresentem defeitos ou anomalias que impeçam o seu regular funcionamento;

h) Orientar seus empregados e prepostos à comparecerem à Unidade Hospitalar devidamente uniformizados e portando crachá de identificação, sendo a mencionada indumentária fornecida pela Contratada;

i) Promover periodicamente a substituição de fardamento, de forma a conservar a boa apresentação de seus empregados e prepostos;

j) Observar rigorosamente as normas e resoluções legais, além de determinações e regimentos perpetrados pelo Estado de Goiás e Município de Goiânia;

k) A **Contratada** arcará exclusivamente com o custeio de mão de obra, transporte, instalação e manutenção dos equipamentos necessários para o desenvolvimento de suas atividades;

l) A **Contratada** disponibilizará suporte 24h, em tempo integral, à **Contratante**;

m) Observar integralmente as normas de segurança, conduta e disciplina estabelecidas pela **CONTRATANTE**, bem como facilitar o acompanhamento da **CONTRATANTE** na sua execução;

n) Comunicar prontamente à **CONTRATANTE** sobre a existência de problemas que possam interferir no andamento dos Serviços eventualmente contratados;

o) Todo e qualquer serviço ou atividade que a **CONTRATADA** empregue para o cumprimento do contrato, ainda que não esteja especificado, deverá observar as normas vigentes, inclusive normativos que regulamentem os serviços ou atividades efetivamente desempenhados, que de natureza ambiental, administrativa e civil. A não observância ou a

não regularização poderá ensejar a rescisão contratual e incidência de demais sanções cabíveis;

p) Assumir exclusivamente a responsabilidade e custeio com transportes e fretes necessários para prestação do serviço ora contratado;

q) Assumir exclusivamente a responsabilidade pela manutenção da regularidade de documentos perante as esferas Federal, Estadual e Municipal, devendo pagar, nos respectivos vencimentos, os tributos e encargos, incidentes ou que venham a incidir, direta ou indiretamente, sobre a prestação do serviço objeto do presente Contrato, devendo apresentar, de imediato, certidões de regularidade fiscal, trabalhista e previdenciária, sempre que solicitado pela CONTRATANTE, sob pena de suspensão do pagamento decorrente das obrigações contratuais.

r) Permitir e facilitar a inspeção dos serviços, prestando todas as informações e apresentando todos os documentos que lhe forem solicitados;

s) Zelar e manter em perfeitas condições de higiene e conservação a área física cedida pelo **Contratante**;

t) Observar e fazer cumprir todas as normas legais relativas às atividades desenvolvidas, respondendo integralmente por quaisquer prejuízos ocasionados a pacientes e ao **Contratante** pela inobservância dessas obrigações;

u) Responder, exclusivamente, pelas ações e omissões de seus empregados e prepostos, indenizando pacientes e o **Contratante** por eventuais prejuízos que lhe forem ocasionados durante o período de vigência do presente contrato;

v) A **Contratada** declara ser única e exclusivamente responsável por quaisquer obrigações de natureza cível, trabalhista, previdenciária e social, que sejam ou venham a ser relacionados, direta ou indiretamente, aos profissionais à serviço do presente contrato.

Cláusula 5. Obrigações do Contratante.

5.1. Caberá ao **Contratante**, às suas expensas, dentre outras obrigações legais e ou constantes do presente contrato:

a) Remunerar o **Contratado**;

b) Promover as facilidades necessárias para o livre acesso dos profissionais do **Contratado** às suas instalações, desde quando devidamente identificados;

c) Fornecer água encanada e energia elétrica;

Cláusula 6. Vigência e Prazo.

6.1. O presente contrato vigorará pelo prazo de 12 (doze) meses, podendo ser renovado por igual período, caso haja manifestação expressa das partes.

6.2. Em não havendo manifestação expressa das partes no sentido de renovação contratual por igual período, este vigorará por tempo indeterminado;

§1º Na hipótese do **Contratado** pretender descontinuar a prestação de serviços no curso da vigência inicial, compromete-se a conceder o aviso prévio de 30 (trinta) dias ao **Contratante**.

6.3. O presente contrato poderá ainda ser rescindido, nas seguintes hipóteses:

a) Se qualquer das partes ceder ou transferir o presente contrato à terceiros, sem a prévia anuência da outra parte, por escrito;

b) Se qualquer das partes se tornar comprovadamente insolvente, requerer recuperação judicial ou extrajudicial ou autofalência, ou ter a sua falência requerida ou decretada;

c) Deixar, qualquer das partes, de cumprir, ou mesmo cumprir irregularmente, cláusulas contratuais, prazos e especificações;

6.4. O presente contrato poderá ainda ser resolvido, sem que haja, incidência de cláusula penal insculpida em item 6.6, nas seguintes hipóteses:

a) Perda do direito de Gestão da unidade hospitalar pela Contratante.

b) Na superveniência de caso fortuito, de força maior ou fato impeditivo à consecução dos objetivos sociais das partes, em razão de decisão judicial ou por ordem dos poderes públicos competentes, que inviabilizem a continuidade de execução do presente contrato.

c) Por exclusivo critério de conveniência e oportunidade da Contratante;

6.5. Em qualquer das hipóteses de encerramento do presente contrato será obrigação comum às partes a realização da devida prestação de contas, no prazo máximo de 30 (trinta) dias subsequentes, abrangendo os aspectos físicos e financeiros do relacionamento. Nesse sentido, será assegurado ao **Contratado** o direito ao recebimento da remuneração correspondente aos serviços efetivamente até aí prestados, não obstante o encerramento do Contrato.

Cláusula 7. Disposições Gerais.

7.1. Em decorrência da presente contratação, sob qualquer hipótese ou em qualquer situação, não se presumirá a eventual existência, ou se estabelecerá a presunção de qualquer vínculo societário e ou empregatício, ou obrigações de caráter trabalhista e previdenciário entre as partes, por si, seus contratados, prepostos e ou empregados, e não serão fiadoras das obrigações e encargos trabalhistas e sociais uma da outra, cabendo a cada sociedade a exclusividade e responsabilidade por tais obrigações, inclusive nas esferas civil e penal;

7.2. A CONTRATADA possui inteiro conhecimento de que a CONTRATANTE não será responsável pela quitação de faturas emitidas após eventual rescisão do Contrato de Gestão tombado sob o nº 131/2012-SES-GO, devendo a CONTRATADA promover a cobrança / execução em desfavor do

Estado de Goiás, ou de qualquer outro que venha a assumir a gestão do Hospital Materno Infantil – HMI

7.3. A CONTRATADA concorda em manter regularmente os serviços prestados, ainda que haja atraso em pagamento de fatura por prazo não superior a 60 (sessenta) dias;

7.4. Cada parte responderá individualmente por quaisquer perdas e danos, materiais ou pessoais, oriundos de suas respectivas ações ou omissões, bem como dos profissionais a si vinculados, que venham a ser causados aos pacientes ou terceiros, sendo de responsabilidade exclusiva e indelegável da parte culpada e causadora do prejuízo responder perante terceiros e à parte inocente, nas hipóteses capazes de configurar imperícia, imprudência ou negligência, obrigando-se, a parte culpada a ressarcir à outra parte inocente, se esta vier a ser acionada por ação ou omissão da culpada e causadora do dano.

7.5. A eventual tolerância a infrações a qualquer das cláusulas deste instrumento ou o não exercício de qualquer direito nele previsto constituirá liberalidade, não implicando em novação ou transação de qualquer espécie.

7.6. O presente Contrato não obriga as partes a qualquer compromisso de exclusividade;

7.7. Fica eleito o foro da Comarca de Goiânia-GO como o único competente para o exercício e cumprimento dos direitos e obrigações decorrentes do presente instrumento, renunciando as partes a qualquer outro, por mais privilegiado que seja, independentemente dos seus atuais ou futuros domicílios.

E por estarem assim justas e contratadas as partes assinam o presente instrumento em 02 (duas) vias de igual teor e forma e para o mesmo fim, na presença das testemunhas abaixo identificadas e assinadas, para que se produzam seus jurídicos e legais efeitos.

Goiânia (GO), 01 de setembro de 2013.

IGH – Contratante

STAR SEGURANÇA ELETRÔNICA LTDA – Contratada

Testemunhas:

1.
Nome: Vinicius Itapuca
CPF: 050.557.605-43
RG:

2.
Nome: Jahan O. de Andrade
060627534.55

CPF:

RG:

Missão:

Promover a saúde da mulher e da criança por meio das ações sócio-educativas e assistência médico-hospitalar, no contexto da saúde pública do Estado de Goiás e contribuir para o desenvolvimento científico através do ensino e pesquisa.

Visão:

Ser referência em serviços especializados nas áreas da saúde da mulher e da criança, com enfoque na humanização da assistência integral aos seus clientes.

PROPOSTA COMERCIAL

GOIANIA – GO, 05 de Junho de 2013.

Ao
INSTITUTO GESTAO E HUMANIZAÇAO
REF. HOSPITAL MATERNO INFANTIL - GO

A **STAR SEGURANÇA ELETRONICA LTDA.**, empresa especializada em prestação de Serviços de Segurança Eletrônica, Rastreamento Veicular e Controle de Acesso, C.N.P.J sob nº 02.713.790/0001-88 com seu escritório na AV. T 63 nº 1296, Ed. New World, sala 504 – Setor Bueno – Goiânia/GO, vem através desta apresentar proposta para prestação de serviços de acordo com o que segue:

01 – OBJETO

Prestação dos Serviços de Instalação, configuração, treinamento, manutenção e locação dos equipamentos que compõem o sistema de controle de acesso do Hospital Materno Infantil de Goiânia.

Objetivo:

1. Maior eficiência na gestão de acessos e controle do fluxo de pessoas nas dependências do HMI.
2. Redução dos custos e gastos com pessoal nas entradas de acesso ao HMI, conforme exemplo das imagens abaixo:

02- DISCRIMINAÇÕES DOS SERVIÇOS

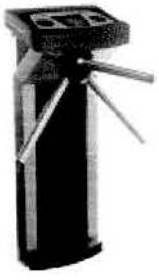
- Controle de acesso de pessoas e veículos;
- Servidores para gerenciamento do sistema de controle de acesso;
- Gravação Backup e armazenamento de dados;
- Acesso remoto
- Demais componentes e serviços na planilha de custos abaixo.

SISTEMA DE CONTROLE DE ACESSO - HOSPITAL MATERNO INFANTIL GO			
ITEM	**DESCRICAO**	**QUANT.**	**UNID. MEDIDA**
1	LEITORAS CATRACAS DE ACESSO	10	unidade
2	CATRACA GABINETE COM CORPO EM INOX E COFRE COLETOR	2	unidade
3	CATRACA PEDESTAL ESPECIAL COM BRAÇO QUE CAI	1	unidade
4	CATRACA PARA PNE TOTAL INOX	1	unidade
5	SOFTWARE DA CONTROLADORA DA CATRACA	2	unidade
6	SOFTWARE DA CONTROLADORA DA CATRACA	2	unidade
7	BRAÇO QUE CAI PARA CATRACA	2	unidade
8	INTEGRAÇÃO DE LEITORA	3	unidade
9	CONTROLE DE CATRACAS OU TORNIQUETES: PLACA CONTROLADORA SCAIIP-CF-PCB ETHERNET - TCP/IP NATIVO 10/100MBPS COM FONTE 20A C/CARREGADOR DE BATERIA INCORPORADA 12 IN / 02 OUT MONIT. ALIMENTAÇÃO AC/DC.	4	unidade
10	PLACA DE EXPANSÃO DE RELÉS P/CONTROLAD. DE CATRACA P/COFRE OU VISITANTE P/QUALQUER CATRACA.	4	unidade
11	TRANSFORMADOR 145VCA 3A. OBS: NECESSÁRIO 01 POR PLACA CONTROLADORA SCAIIP-CF-PCB.	4	unidade
12	BATERIA DE GEL SELADA 12VCC 7AH.	4	unidade
13	SOFTWARE SCAIIP-TCP/IP - MÓDULO DE APLICAÇÃO DE GLOBAL ANTI-PASSBACK.	1	unidade
14	SOFTWARE SCAIIP-TCP/IP - MÓDULO DE CADASTRAM. E GERENCIAMENTO DE VISITANTES P/CLIENT.	2	unidade
15	SOFTWARE SCAIIP-TCP/IP - MÓDULO DE APLICAÇÃO DE LIBERAÇÃO INTEGRADA COM INCÊNDIO.	1	unidade
16	SOFTWARE SCAIIP WEB BASED PARA NAVEGADOR WEB TCP/IP. INCLUI INTEGRAÇÃO COM CFTV HÍBRIDO: ANALÓGICO E IP QUADRO SINÓTICO EMISSÃO DE RELATÓRIOS CADASTRAMENTO E GERENCIAMENTO DE USUÁRIOS. LICENÇA POR PORTA.	5	unidade
17	SERVIDOR DE GERENCIAMENTO E GRAVACAO	0	unidade
18	HARDWARE CADASTRO ACESSOS E VISITANTES	3	unidade
19	SOFTWARE PACK PARA GERENCIAMENTO DE 01 CANAL IP 01 LICENÇA.	5	unidade

Valor Mensal Locação dos Equipamentos, Atualização de Software, Manutenção dos equipamentos e sistema, Suporte telefônico e Treinamento.	**8.727,68**

Modelos de equipamentos a serem implantados:

- 



- 

CARACTERÍSTICAS

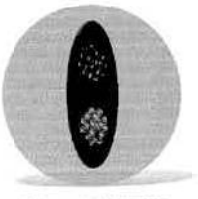
- Gabinete monobloque en total acero inox AISI 304 o en acero 1010/20 pintado con tinta Epoxi ADO, con 1,5 mm de espesura, configurada a láser, resistente a choques, vibraciones, elemento ácidos y alcalinos.
- Retirada completa del mecanismo por la parte frontal del bloqueo para facilitar el mantenimiento;
- Sistema de amortiguación de giro provisto de Desaceleración Linear;
- Número de pasadas/minuto 40 a 45; (limitado al sistema de control);
- Mecanismo provisto de sistema de trabamiento, que en la falta de energía, el equipamiento queda destrabado, para atender normas de seguridad;
- Mecanismo con tratamiento anti-corrosión;
- Todas las esquinas son redondeadas con rayos de 18 mm, siendo que la tapa tiene sus extremidades frontales pulidas a 45 .
- Sistema de trabamiento con dos solenoides, que controlan el flujo de usuarios de forma independiente (entrada y salida);
- Índice de protección (IP) 42
- Capaz de soportar el bloqueo de una persona de 130 Kg a 5Km/h.

INTERFAZ ELECTRÓNICA

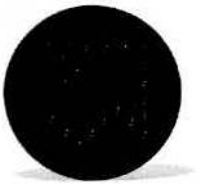
Módulo de control PWAC / WKC, responsable por la interfaz con cualquier módulo operacional (sistema de validez del billete) y por la administración autónoma de todos los funcionamientos de las tomas;

- Dispositivo del giro de los brazos;
- Control de los solenoides de trabamiento;
- Control de los pictogrammes de operación y orientación;
- Desarrollo de los contadores digitales;
- Envío de las informaciones de pasajes a los sistemas de validez;
- Firmware totalmente configurable.
- Puerta serial para comunicación directa a ordenadores, pudiendo atender a diversas necesidades específicos del sistema de validez del billete.

Esquinas redondeadas y seguro tarjetas de colección



Pictogramas de operación



Pictogramas de orientación

Lucha contra el pánico
Brazo de la caída

MODELOS DISPONIBLES

- Slim Evolution Total Inox
- Slim Evolution Mixta

TERMINACIONES

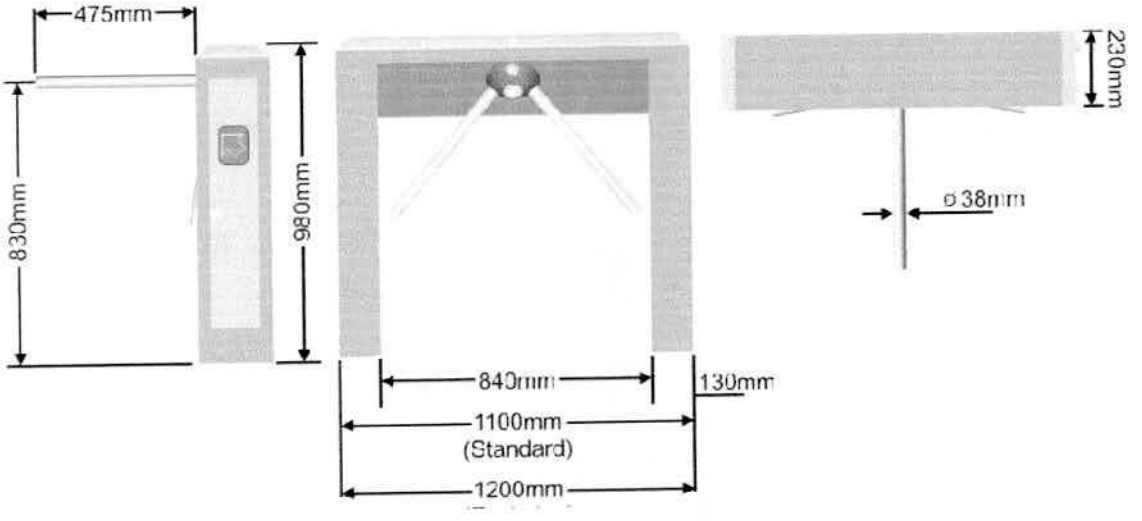
- Gabinete totalmente en acero inox cepillado o gabinete en acero carbono pintado con tapa superior en acero inox;
- Cantos redondeados del gabinete con raya de 18mm;
- Brazos en tubos de acero inox con refuerzo interno en acero, rosqueados en el cabezote y fijos con tornillos sin cabeza de difícil acceso.

OPCIONALES

- Pictogramas de orientación con leds de alto brillo;
- Contador LCD de 8 (ocho) dígitos con batería para 10 (diez)años;
- Cofre colector para tarjetas de visitantes;
- Sistema de Emergencia anti-pánico (Brazo que cae);
- Encerramiento de la parte trasera en el mismo material del equipamiento

BENEFICIOS

- Excelente costo beneficio;
- Mayor robustez;
- Design Moderno;
- Integración con diversos módulos operacionales (validez);
- Espacio interno para placas electrónicas y colocación de tarjetas;
- MCBF superior a 1.000.000 de ciclos;
- Tiempo medio para reparación (MTTR): max. 15 min.



CARACTERÍSTICAS

- Estrutura tubular em aço carbono pintado e carenagem com acabamento customizado;
- Braços em tubo de aço inox, escovados;
- Came de repouso que determina o ponto de parada, provido de desacelerador linear;
- Módulos configurados a laser, resistentes a choques;
- Mecanismo rolamentado com eixo central em aço-liga, resistente à tração e torção, sendo seus componentes bicromatizados;
- Dispositivo anti-retorno, em aço modular, com capacidade para torques pesados de até 2000Nm;
- Todas as peças são intercambiáveis, permitindo alterações estruturais e funcionais;
- Tampo e portinholas providas de fechos tipo Castelo (padrão) ou chave tipo Yale, para limitar o acesso ao mecanismo e cofre, facilitar a fixação do equipamento no solo, a manutenção do mecanismo e dos pictogramas orientativos;
- Pictogramas de operação e display inovadores;
- Bloqueio do giro por sistema de travamento ou destravamento através de dois triques e dois solenóides;
- Monitoramento do giro por sensores indutivos.

Sistema anti-pânico
Braço que cai

Pictograma de orientação
pulsante e de alto brilho

Teclado de membrana
e pictograma de operação

INTERFACE ELETRÔNICA

- Módulo de controle PWAC / WKC, responsável pelo interfaceamento com qualquer módulo operacional (sistema de validação de cartões) e pelo gerenciamento autônomo de todas as funções da catraca;
- Sensoriamento do giro dos braços;
- Controle dos solenóides de travamento;
- Controle dos pictogramas de operação e orientação;
- Envio das informações de passagem aos sistemas de validação;
- Firmware totalmente configurável;
- Porta serial para comunicação direta a computadores, podendo atender a diversas necessidades específicas do sistema de validação de cartões.

ACABAMENTOS

- Corpo em aço carbono pintado com detalhes de acabamentos frontais em resina; laterais, tampa superior e braços em aço inox.

OPCIONAIS

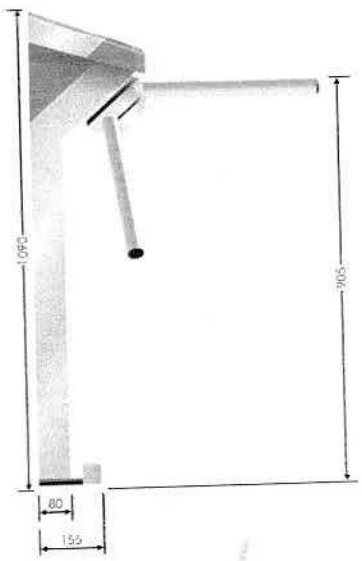
- Cofre receptador de cartões.
- Controle de revista aleatório.
- Modelos de leitoras: smartcard, proximidade e biometria.
- Sistema anti-pânico (braço que cai).
- Braços em acrílico.
- Módulos de controle: PWAC e WKC.

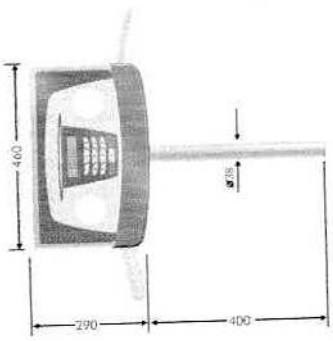
BENEFÍCIO

- Design revolucionário, integrando com ambientes sofisticados, seguindo as novas tendências do mercado;
- Aceita integração com qualquer sistema/controlador de terceiros;
- Baixo custo de manutenção pelos altos índices de desempenho: MTBF (20.000 hs), MCBF (1.000.000 de ciclos e MTTR (60 minutos).

Dimensões

* Medidas em (mm)





Controle de Acesso (Especificaçoes)

Total controle e vigilância de todos os acessos às áreas seguras diretamente de qualquer uma das estações clientes. Todas as atividades de acesso são transmitidas diretamente à tela do computador. Deverá enviar comandos específicos para as portas configuradas, tais como abrí-las e fechá-las diretamente, selá-las temporariamente, etc...

Algumas funcionalidades compreendem:

- Anti-passback (anti-dupla entrada): para evitar que um cartão usado para entrada/saída seja reutilizado, impedindo que mais de uma pessoa tenha acesso à um mesmo local usando o mesmo cartão. O Anti-passback impede que este cartão passe duas vezes, em seqüência, pela mesma leitora.
- Anti-passback GLOBAL: previne que um mesmo cartão seja usado por mais de uma pessoa, mais de uma vez, em um grupo de portas / área de acesso, em uma seqüência previamente programável.

Tanto o *Anti-passback* como *o Anti-passback GLOBAL* deverão permanecer funcionando de forma integral, independentemente do PC Servidor, no caso que queda do mesmo.

Monitoramento de CFTV

A integração com o Sistema de CFTV permite a observação de múltiplos vídeos em tempo real dentro da interface gráfica do Sistema, provenientes de câmeras analógicas ou câmeras IP (simultâneamente, se for o caso, através de sistema híbrido). Câmeras poderão ser programadas para reagir à alarmes específicos. Gravação digital de imagens. Permite que se recupere em um clique sobre qualquer evento de acesso ou de alarme, o vídeo gravado deste evento ou o vídeo correspondente em tempo real, desde que haja uma câmera previamente relacionada para a controladora correspondente, na programação.

Monitoramento de Alarmes em Tempo Real

Para atuação com controladoras específicas de alarme. Fornece mensagens de alerta sobre violações de segurança, como entradas não autorizadas, porta deixada aberta, entrada forçada, cartões inválidos, violação de dispositivos, etc., visualiza o local da ocorrência através de ícone animado em um mapa gráfico (planta de pavimento), diretamente na tela de seu computador em tempo real, reduzindo falsos alarmes e otimizando seu tempo de resposta para as diversas ocorrências. Controladoras específicas (para controle de portas e sensores de alarme adicionais) permitem que leitoras de proximidade (ou outra tecnologia) pré-programadas possam substituir as funções de teclado de arme e desarme alarme.

Ronda de Guarda

Possui um módulo de Ronda de Guardas, funcionalidade adicional opcional que envolve o monitoramento detalhado de patrulha de seguranças, ao longo de suas rotas pré-programadas de vigilância. Durante sua ronda, os guardas passam seus cartões em leitoras específicas, registrando seus movimentos em sua interface de segurança. Cada segurança tem seu cronograma particular, com uma lista de intervalos de passagem entre leitoras. Se um guarda se atrasa na passagem por uma das leitoras atribuídas à uma ronda, o sistema assume, automaticamente, que algum problema pode ter ocorrido, ativando um alerta e informando outros seguranças, se assim for programado.

Controle de Veículos / Estacionamento

Controle do acesso ao estacionamento através do uso de cartões de usuários e visitantes. O sistema anti-passback também se aplica aos veículos, ou seja, uma vez que o usuário entrou com seu veículo no estacionamento, seu cartão só poderá ser usado para sair. Monitora também o tráfego de veículos e se desejar, controla cancelas e portões diretamente da estação cliente. Mantém arquivo de registros de tráfego, de acordo com cartões, datas, horas de entrada e saída, etc. Comanda a abertura e fechamento de acessos em ocasiões especiais, tais como facilitar a passagem de comboios de veículos ou entradas rápidas.

Gerenciamento de Visitantes

Sistema totalmente integrado ao software de controle de acesso, permite o cadastramento de visitantes com foto; é compatível com cartões de proximidade, Mifare ou outros tipos de tecnologia; capacidade para gerenciar e rastrear rapidamente os visitantes; inclui módulo de cadastramento de ativos que acompanham o visitante (chapelaria), baixa automática do cartão de acesso ao se passar o mesmo por leitora específica (programada no sistema), ou através de rotina programável para expiração do mesmo com dia e hora de validade.

1. CARACTERISTICAS GERAIS DO SISTEMA DE CONTROLE DE ACESSO

O Sistema de controle de acesso deverá ser via rede Ethernet permitindo escalabilidade de uma até centenas de portas, em incrementos de controladoras, uma a uma.

Comunicação em alta velocidade de 10/100 Mbps para reduzir a utilização da banda de transmissão de dados.

Cada porta deverá ser assistida por controladora individual em TCP/IP nativo. Não serão aceitos sistemas com arquitetura que compreenda redes RS-232, RS-422, RS-485 ou outras redes seriais, ou concentradores TCP/IP e redes seriais entre estes e módulos de portas, de forma a não prejudicarem a performance e velocidade de transmissão de dados no sistema, bem como prejudicarem sua escalabilidade, flexibilidade e manutenção.

O incremento de portas e outras barreiras no Sistema deverá ser feito um a um, de forma a agilizar e trazer ótima relação custo-benefício em caso de ampliação do mesmo.

O sistema deverá possui comunicação em alta velocidade para reduzir a utilização da banda de transmissão de dados transmitidos em pacotes, otimizando a velocidade de transmissão entre as controladoras e o servidor, provendo transações em tempo real até para o usuário.

O sistema deverá permitir a reunião de controladoras em grupos de duas ou mais unidades, para atuação das funcionalidades de anti-passback global ou de integração com sistema de incêndio.

O anti-passback global deve funcionar sem a necessidade do PC servidor de controle de acesso estar on-line 24 hs, eliminando falhas do sistema ou interrupções de fluxo, mesmo com os servidor de controle de acesso fora do ar. Portas e área de acesso podem ser agrupadas em um grupo previamente programável, mesmo em locais remotos.

A baixa automática de cartão de visitante deve funcionar sem a necessidade do PC servidor de controle de acesso estar on-line 24 hs, eliminando falhas do sistema ou interrupções de fluxo, mesmo com o servidor de controle de acesso fora do ar. Controladoras de acesso podem ser agrupadas em um grupo previamente programável, onde a baixa de cartões será executada somente nestas.

Deverá possuir função de integração com sistemas de incêndio através de uma entrada digital na controladora, sem a necessidade do PC servidor de controle de acesso estar on-line 24 hs. A controladora, ao receber sinal proveniente de um módulo de central de incêndio, comunica-se peer-to-peer (ponto a ponto) com outras controladoras de seu grupo, através da rede Ethernet, liberando todas as fechaduras até que o operador as rearme pelo sistema.

O sistema deverá permitir a utilização de redes sem fio, reduzindo custos com passagem de cabos, ou viabilizando áreas onde a passagem dos mesmos é muito difícil.

As controladoras deverão comunicar-se, entre si, sem a necessidade do PC servidor de controle de acesso estar on-line, ou seja, ponto a ponto (peer-to-peer). Sinais de alarme de incêndio (opcional) ou outras funcionalidades poderão ser transmitidas entre as mesmas a qualquer momento.

Cada controladora deverá possui memória residente não volátil (EPROM e Flash) para armazenar o mínimo de 70.000 (setenta mil) usuários e 40.000 (quarenta mil) eventos em sua memória (buffer) – em modo multiformato de cartão. Todos os dados (exceto de data e hora) deverão permanecer na memória da controladora de forma definitiva, em caso de queda de energia. O equipamento deverá trabalhar de forma autônoma ou em rede, provendo o acesso a quem cotidianamente utiliza-se do sistema. Em caso de queda da rede ou do PC servidor, cada controladora deverá continuar funcionando autonomamente com todas as últimas instruções e permissões. Não é permitida a utilização de sistemas de listas brancas e listas negras em caso de queda da rede ou do servidor.

O sistema deverá permitir que uma controladora não afete o funcionamento de outra, como no caso de redes em "daisy-chain" ou "looping", fazendo assim com que a manutenção se torna muito mais simples e rápida, e o sistema mais estável.

No sistema, as controladoras deverão monitorar e reportar ao PC servidor de controle de acesso a falha de AC (alimentação elétrica) e baixa carga ou esgotamento da bateria de back-up, com isso eliminando a possibilidade da controladora parar ou mesmo tornar-se instável, quando houver a falta de energia elétrica por um período limitado, sem que se proceda uma rotina de manutenção, e, depois de restabelecida a energia, não deverá haver instabilidade ou sobrecarga na saída de alimentação das fechaduras.

O Sistema deverá permitir a utilização da infra-estrutura de rede já existente, bem como a adição de uma nova rede de dados, para monitorar e controlar o acesso local ou o acesso remoto de filiais, de uma mesma central de segurança, via WAN ou LAN, via VPN.

As controladoras deverão ser instaladas dentro das áreas seguras (nunca nas áreas externas às portas controladas), impedindo a violação dos seus relés, usando-se magnetos ou outros dispositivos.

A instalação deverá ser simples e rápida, não havendo a necessidade de configurar-se jumpers de endereçamento nas mesmas. O sistema deverá ser inteligente o suficiente para auto-detectar o endereço IP "default" de cada controladora e automaticamente adicioná-la no banco de dados, e permitir a mudança manual de endereço IP para adequação dos dispositivos à rede existente. As controladoras (porta a porta) deverão possuir dispositivo TCP/IP nativo, e não híbrido (comunicação serial RS-232, RS-422 ou RS-485 convertidos para TCP/IP), para garantir uma velocidade de comunicação real de 10/100 Mbps.

Para barreiras como catracas, torniquetes, portões, cancelas, elevadores e portas conjugadas com mais de oito entradas de alarme, deverão ser utilizadas controladoras com fonte de alimentação integrada (mínimo de 2A em 12 VCC) e supervisionada e carregador flutuante de bateria; e para o controle de portas deverão ser utilizadas controladoras PoE (Power over Ethernet) com carregador flutuante de bateria. Todas estas controladoras deverão funcionar na mesma rede, simultaneamente, conforme a alternativa de solução mais rápida e prática para ampliação do sistema.

O Sistema deverá possui uma interface gráfica e poderosa e extremamente simples de usar, baseada em sistema operacional Windows, contando com menus intuitivos e com plantas gráficas (quadro sinótico).

O Sistema deverá permitir que informações ou dados coletados no banco de dados do servidor possam ser exportados para softwares de terceiros.

O Sistema deverá ter todos os hardwares e softwares modulares, permitindo assim que o sistema seja expandido conforme a necessidade do Contratante.

O Software de administração e cadastramento deverá ser em língua portuguesa.

O Software de administração deverá permitir a utilização de leitoras de dupla tecnologia de validação, e rastreamento de cartões e transações.

O Sistema deverá permitir abertura de barreiras remotamente, através de acionamento por comando TCP/IP, diretamente da planta (Quadro Sinótico).

1.1. REQUISITOS MÍNIMOS DO SISTEMA DE CONTROLE DE ACESSO.

1.1.1. Equipamentos

Todos os equipamentos fornecidos deverão ser "standard", ou seja, suas aplicabilidades deverão ser originais de fábrica e não customizadas para esta concorrência.

1.1.2. Computador Central – Sistema de Controle de Acesso

O Sistema deverá possuir um computador central, que funcionará como Servidor de Controle de Acesso e Segurança, entretanto, o sistema deverá manter sua funcionalidade, a todo momento, com ou sem o funcionamento deste Servidor.

1.1.3. Integração

O Sistema deverá permitir total integração com controle de iluminação, ventilação, ronda de guardas, sistema de cftv, sistemas de intrusão, barreiras veiculares e controle de visitantes, bem como outras aplicações requeridas, se for o caso, em uma única plataforma.

1.1.4. Modularidade Total

O Sistema deverá apresentar completa modularidade de hardware e software, onde seus componentes são agregados como módulos de expansão e/ou funcionalidade, permitindo futuras modificações e expansões para atender a futuras demandas.

1.1.5. Suprimento de Energia

1.1.5.1. Suprimento de Tensão em Corrente Alternada

Todos as controladoras de campo utilizadas para controlar barreiras como catracas, torniquetes, portões, cancelas, elevadores e portas conjugadas com mais de oito entradas de alarme, deverão possuir transformador para funcionar com tensão de 110/220 VCA +/- 10%. Cada controladora deverá ter a fonte de energia de corrente contínua com carregador flutuante de bateria, incorporados no corpo da mesma, para alimentação dos equipamentos nela acoplados.

Já as controladoras destinadas ao controle de portas deverão ser do tipo PoE (power over ethernet), também com carregador flutuante de bateria incorporado à mesma. Cada controladora PoE deverá fornecer energia para pelo menos quatro leitoras de cartão (duas leitoras de entrada e duas leitoras de saída) e duas fechaduras do tipo eletroímã, podendo então realizar o controle de duas portas. Para tal, os switches ou injetores PoE que fornecerão energia à controladora PoE deverão ser do tipo "Hi PoE" ou "PoE+", com potência de saída por porta RJ45 de 30 W.

1.1.5.2. Baterias

Todos as controladoras de campo deverão ser energizadas através das saídas de corrente alternada e deverão incorporar uma conexão dedicada com bateria selada de pelo menos 7Ah, 12VCC, a fim de prover energia de reserva (backup) e segurança em caso de falha de suprimento de corrente alternada. O equipamento deverá ser equipado com circuito de carregamento flutuante das baterias durante a operação normal.

1.1.6. Detecção de Energia

As controladoras de campo deverão possuir circuito de detecção de falha no fornecimento de energia, bem como estado de bateria com baixa carga e corte de bateria (hardware e software deverão monitorar corrente contínua e alternada). Caso haja um o período de corte de energia, cada controladora afetada deverá enviar um sinal para a Central de Gerenciamento e Monitoramento de Acesso e Segurança, para avisar sobre a falha. O mesmo deverá ocorrer quando as baterias de backup tiverem atingido um nível baixo de carga. Quando na ocorrência de falha no fornecimento de energia e no caso das baterias de backup estiverem com carga baixa e tensão abaixo de 10,5 VCC, as controladoras afetadas deverão liberar suas respectivas portas e reportar seu status à Central de Gerenciamento e Monitoramento de Acesso e Segurança.

Todos os eventos de detecção de falha de fornecimento de energia deverão ser registrados no Sistema e deverão incluir data, hora, unidade que falhou e status.

1.1.7. Cablagem

Para conexões entre as controladoras e as leitoras, as seguintes bitolas de cabos deverão ser utilizadas:

Para distâncias de até 120 metros (dependendo da leitora a ser utilizada): 0,22 mm2. Recomendado cabo tipo Belden 18 AWG.

Cada dispositivo de detecção e alarme deverá estar conectado a uma zona em separado, para monitoramento individual e reporte, a não ser que especificado em contrário.

O Sistema deverá permitir dispositivos de detecção com contatos normalmente aberto (NA) ou normalmente fechados (NF), a serem conectados às entradas das zonas de alarme, do mesmo modo. Um modo de programação deverá ser fornecido para definir cada uma das entradas, e se o dispositivo utiliza saídas NA ou NF.

O Sistema deverá operar, de maneira perfeitamente confiável.

1.2. COMPONENTES DO SISTEMA DE CONTROLE DE ACESSO

1.2.1. Controladora para Catraca ou Torniquete

Cada controladora de catraca ou torniquete deverá armazenar pelo menos 40.000 (quarenta mil) eventos em seu buffer de memória interna (EPROM e FLASH) e deverá também suportar ao menos 70.000 (setenta mil) usuários (mais 5.000 visitantes simultâneos), dada à quantidade e a rotatividade dos mesmos, em modo multiformato de cartão.

O armazenamento das transações em seu buffer deverá ser transferido para o Servidor sempre que o software do Sistema estiver em operação com a rede disponível (on-line) – tecnologia de "pushing".

Cada controladora deverá ser equipada com tranceiver TCP/IP nativo (e não serial convertido para TCP/IP), ou seja, comunicar-se via rede Ethernet a uma velocidade de transmissão de dados de 10/100 Mbps.

Cada controladora deverá possuir quatro entradas para leitoras (duas leitoras de entrada e duas de saída), duas entradas para botão de requisição de saída, uma entrada para tamper, duas entradas para sensores, uma entrada para integração com sistema de incêndio ou emergência, duas saídas de relé comandadas (para controle de giro de entrada e giro de saída), duas saídas de relé em placa de expansão adicional (para controle de solenoide de cofre coletor), controle de pictograma, alerta de giro em sentido invertido e controle de sensor de giro em placa de expansão adicional.

Cada controladora deverá permitir que se possa adicionar uma expansão para segunda catraca independente ou para um cofre coletor.

Cada controladora deverá manter um relógio geral e um RTC (real time clock) incorporado. Tanto a controladora quanto o RTC deverão sincronizar data e horário com o Servidor de Controle de Acesso, sempre este estiver on-line, em intervalos regulares pré-programados. Caso seja interrompida a comunicação entre a controladora e o Servidor, a controladora passará a sincronizar data e horário com o RTC incorporado. Quando voltar a comunicação com o Servidor, ambos o RTC e a controladora passarão a sincronizar data e horário novamente com este.

As controladoras deverão estar ligadas em uma rede que não tenha limite máximo de extensão, obrigatoriamente.

As controladoras deverão ser montadas dentro das catracas, de tamanho suficiente para permitir uma fácil montagem e cablagem de todos os dispositivos das mesmas, bem como espaço para a bateria de backup.

- A controladora deverá possuir fonte de corrente contínua 2A em 12VCC com carregador flutuante de bateria integrada ao seu corpo (esta fonte deverá ser supervisionada pelo software de controle de acesso, para informação de falha de alimentação elétrica ou de carga baixa de bateria), a fim de prover energia para assegurar a integridade das informações nos períodos de falha de suprimento de energia da rede elétrica, e todos os dados da controladora deverão ser armazenados em uma memória não volátil. A bateria de backup deverá ser de no mínimo 12VCC, 7Ah. A bateria de backup deverá prover 12VCC a 1A (max) para até duas fechaduras. A fonte de alimentação deverá prover carga suficiente para baterias de backup de até 12,7Ah.

A Controladora deverá ser compatível com leitoras de cartão ou outros dispositivos leitores, que utilizem protocolo Wiegand 26, 34 ou 42 bits (padrão de fábrica), e ainda permitindo customização para diferentes protocolos.

1.2.2. Controladora PoE para Porta

- Cada controladora de porta deverá armazenar pelo menos 40.000 (quarenta mil) eventos em seu buffer de memória interna (EPROM e FLASH) e deverá também suportar ao menos 70.000 (setenta mil) usuários (mais 5.000 visitantes simultâneos), dada à quantidade e a rotatividade dos mesmos, em modo multiformato de cartão.

O armazenamento das transações em seu buffer deverá ser transferido para o Servidor sempre que o software do Sistema estiver em operação com a rede disponível (on-line) – tecnologia de "pushing".

Cada controladora deverá ser equipada com tranceiver TCP/IP nativo (e não serial convertido para TCP/IP), ou seja, comunicar-se via rede Ethernet a uma velocidade de transmissão de dados de 10/100 Mbps.

Cada controladora deverá possuir quatro entradas para leitoras (duas leitoras de entrada e duas de saída), duas entradas para botão de requisição de saída, uma entrada para tamper, duas entradas para sensor de status de porta/fechadura, duas entradas para integração com sistemas de incêndio ou emergência e duas saídas de relé comandadas (para duas fechaduras).

Cada controladora deverá manter um relógio geral e um RTC (real time clock) incorporado. Tanto a controladora quanto o RTC deverão sincronizar data e horário com o Servidor de Controle de Acesso, sempre este estiver on-line, em intervalos regulares pré-programados. Caso seja interrompida a comunicação entre a controladora e o Servidor, a controladora passará a sincronizar data e horário com o RTC incorporado. Quando voltar a comunicação com o Servidor, ambos o RTC e a controladora passarão a sincronizar data e horário novamente com este.

As controladoras deverão estar ligadas em uma rede que não tenha limite máximo de extensão, obrigatoriamente.

As controladoras deverão ser montadas dentro de caixas apropriadas, de tamanho suficiente para permitir uma fácil montagem e cablagem de todos os dispositivos das mesmas, bem como espaço para a bateria de backup.

A controladora deverá possuir fonte PoE (power over ethernet) com carregador flutuante de bateria integrada ao seu corpo (esta fonte deverá ser supervisionada pelo software de controle de acesso, para informação de falha de alimentação elétrica ou de carga baixa de bateria), a fim de prover energia para assegurar a integridade das informações nos períodos de falha de suprimento de energia da rede elétrica, e todos os dados da controladora deverão ser armazenados em uma memória não volátil. A bateria de backup deverá ser de no mínimo 12VCC, 7Ah. A bateria de backup deverá prover 12VCC a 1A (max) para até duas fechaduras.

A Controladora deverá ser compatível com leitoras de cartão ou outros dispositivos leitores, que utilizem protocolo Wiegand 26, 34 ou 42 bits (padrão de fábrica), e ainda permitindo customização para diferentes protocolos.

1.2.3. Controladora para Porta

Cada controladora de porta deverá armazenar pelo menos 40.000 (quarenta mil) eventos em seu buffer de memória interna (EPROM e FLASH) e deverá também suportar ao menos 70.000 (setenta mil) usuários (mais 5.000 visitantes simultâneos), dada à quantidade e a rotatividade dos mesmos, em modo multiformato de cartão.

O armazenamento das transações em seu buffer deverá ser transferido para o Servidor sempre que o software do Sistema estiver em operação com a rede disponível (on-line) – tecnologia de "pushing".

Cada controladora deverá ser equipada com tranceiver TCP/IP nativo (e não serial convertido para TCP/IP), ou seja, comunicar-se via rede Ethernet a uma velocidade de transmissão de dados de 10/100 Mbps.

Cada controladora deverá possuir quatro entradas para leitoras (duas leitoras de entrada e duas de saída), duas entradas para botão de requisição de saída, uma entrada para tamper, duas entradas para sensor de status de porta/fechadura, duas entradas para integração com sistemas de incêndio ou emergência e duas saídas de relé comandadas (para duas fechaduras).

Cada controladora deverá manter um relógio geral e um RTC (real time clock) incorporado. Tanto a controladora quanto o RTC deverão sincronizar data e horário com o Servidor de Controle de Acesso, sempre este estiver on-line, em intervalos regulares pré-programados. Caso seja interrompida a comunicação entre a controladora e o Servidor, a controladora passará a sincronizar data e horário com o RTC incorporado. Quando voltar a comunicação com o Servidor, ambos o RTC e a controladora passarão a sincronizar data e horário novamente com este.

As controladoras deverão estar ligadas em uma rede que não tenha limite máximo de extensão, obrigatoriamente.

As controladoras deverão ser montadas dentro de caixas apropriadas, de tamanho suficiente para permitir uma fácil montagem e cablagem de todos os dispositivos das mesmas, bem como espaço para a bateria de backup.

A controladora deverá possuir fonte de corrente contínua 2A em 12VCC com carregador flutuante de bateria integrada ao seu corpo (esta fonte deverá ser supervisionada pelo software de controle de acesso, para informação de falha de alimentação elétrica ou de carga baixa de bateria), a fim de prover energia para assegurar a integridade das informações nos períodos de falha de suprimento de energia da rede elétrica, e todos os dados da controladora deverão ser armazenados em uma memória não volátil. A bateria de backup deverá ser de no mínimo 12VCC, 7Ah. A bateria de backup deverá prover 12VCC a 1A (max) para até duas fechaduras. A fonte de alimentação deverá prover carga suficiente para baterias de backup de até 12,7Ah.

A Controladora deverá ser compatível com leitoras de cartão ou outros dispositivos leitores, que utilizem protocolo Wiegand 26, 34 ou 42 bits (padrão de fábrica), e ainda permitindo customização para diferentes protocolos.

1.2.4. Controladora para Barreiras Veiculares

Cada controladora de acesso de estacionamento deverá armazenar pelo menos 40.000 (quarenta mil) eventos em seu buffer de memória interna (EPROM e FLASH) e deverá também suportar ao menos 70.000 (setenta mil) usuários (mais 5.000 visitantes simultâneos), dada à quantidade e a rotatividade dos mesmos, em modo multiformato de cartão.

O armazenamento das transações em seu buffer deverá ser transferido para o Servidor sempre que o software do Sistema estiver funcionando (on-line) – tecnologia de "pushing".

Cada controladora deverá ser equipada com tranceiver TCP/IP nativo (e não serial convertido para TCP/IP), ou seja, comunicar-se via rede Ethernet a uma velocidade de transmissão de dados de 10/100 Mbps.

Cada controladora deverá possuir duas entradas para leitoras (uma leitora de entrada e uma de saída), duas entradas para botão de requisição de saída, uma entrada para tamper, duas entradas para sensor de laço ou similar (para ativar o funcionamento das leitoras), uma entrada para integração com sistemas de incêndio ou emergência e duas saídas de relé comandadas (um relé para barreira de

entrada, ativado pela leitora de entrada, e um relé para barreira de saída, ativado pela leitora de saída).

A controladora de estacionamento deverá controlar uma barreira de entrada e uma de saída, a fim de proporcionar a funcionalidade de Antipassback.

Cada controladora deverá permitir que se possa adicionar uma expansão para um cofre coletor.

Cada controladora deverá manter um relógio geral e um RTC (real time clock) incorporado. Tanto a controladora quanto o RTC deverão sincronizar data e horário com o Servidor de Controle de Acesso, sempre este estiver on-line, em intervalos regulares pré-programados. Caso seja interrompida a comunicação entre a controladora e o Servidor, a controladora passará a sincronizar data e horário com o RTC incorporado. Quando voltar a comunicação com o Servidor, ambos o RTC e a controladora passarão a sincronizar data e horário novamente com este.

A controladora deverá possuir fonte de corrente contínua 2A em 12VCC com carregador flutuante de bateria integrada ao seu corpo (esta fonte deverá ser supervisionada pelo software de controle de acesso, para informação de falha de alimentação elétrica ou de carga baixa de bateria), a fim de prover energia para assegurar a integridade das informações nos períodos de falha de suprimento de energia da rede elétrica, e todos os dados da controladora deverão ser armazenados em uma memória não volátil. A bateria de backup deverá ser de no mínimo 12VCC, 7Ah. A bateria de backup deverá prover 12VCC a 1A (max) para até duas fechaduras. A fonte de alimentação deverá prover carga suficiente para baterias de backup de até 12,7Ah.

A Controladora deverá ser compatível com leitoras de cartão ou outros dispositivos leitores, que utilizem protocolo Wiegand 26, 34 ou 42 bits (padrão de fábrica), e ainda permitindo customização para diferentes protocolos.

1.2.5. Controladora para Porta e Módulo de Sensores de Alarme / Automação

Cada controladora de acesso e alarme deverá armazenar pelo menos 40.000 (quarenta mil) eventos em seu buffer de memória interna (EPROM e FLASH) e deverá também suportar ao menos 70.000 (setenta mil) usuários (mais 5.000 visitantes simultâneos), dada à quantidade e a rotatividade dos mesmos, em modo multiformato de cartão.

O armazenamento das transações em seu buffer deverá ser transferido para o Servidor sempre que o software do Sistema estiver funcionando (on-line) – tecnologia de "pushing".

Cada controladora deverá ser equipada com tranceiver TCP/IP nativo (e não serial convertido para TCP/IP), ou seja, comunicar-se via rede Ethernet a uma velocidade de transmissão de dados de 10/100 Mbps.

Cada controladora deverá possuir duas entradas para leitoras (uma leitora de entrada e uma de saída), uma entrada para botão de requisição de saída, uma entrada para tamper, uma entrada para sensor de status de porta/fechadura, uma entradas para integração com sistemas de incêndio ou emergência, duas saídas de relé comandadas (uma para fechadura e uma auxiliar de alarme) e uma saída de acoplamento de módulo de sensores.

Saídas a Relé – A saída a rélé deverá ser capaz de fornecer até 10A para dispositivos externos, tais como sirene, luz estroboscópica, ou outras.

Deverá armazenar pelo menos 100 (cem) cartões com privilégios de armar e desarmar alarme localmente, bem como pelo menos 10 (dez) senhas numéricas.

Alarmes gerados em cada controladora poderão ser reconhecidos localmente ou remotamente.

As entradas de alarme deverão permitir sua programação através do Sistema de Administração Central, de acordo com a área, e permanecerem sempre ativas.

A controladora de acesso deverá detectar e reportar todas as condições de alarme que poderão ocorrer, tais como requisição de Acesso Válido, Cartão Desconhecido, Zona de Horário Inválida, e violação de leitoras ou caixas (tamper).

O monitoramento de alarme deverá prever condições de porta forçada ou condição de estado da porta. Cada porta ou fechadura de porta deverá ter uma saída a relé livre de tensão ou sensor de status para indicar um sinal de saída desde a abertura da porta até a atracação segura e integral de sua fechadura.

Cada controladora deverá manter um relógio geral e um RTC (real time clock) incorporado. Tanto a controladora quanto o RTC deverão sincronizar data e horário com o Servidor de Controle de Acesso, sempre este estiver on-line, em intervalos regulares pré-programados. Caso seja interrompida a comunicação entre a controladora e o Servidor, a controladora passará a sincronizar data e horário com o RTC incorporado. Quando voltar a comunicação com o Servidor, ambos o RTC e a controladora passarão a sincronizar data e horário novamente com este.

A controladora deverá possuir fonte de corrente contínua 2A em 12VCC com carregador flutuante de bateria integrada ao seu corpo (esta fonte deverá ser supervisionada pelo software de controle de acesso, para informação de falha de alimentação elétrica ou de carga baixa de bateria), a fim de prover energia para assegurar a integridade das informações nos períodos de falha de suprimento de energia da rede elétrica, e todos os dados da controladora deverão ser armazenados em uma memória não volátil. A bateria de backup deverá ser de no mínimo 12VCC, 7Ah. A bateria de backup deverá prover 12VCC a 1A (max) para até duas fechaduras. A fonte de alimentação deverá prover carga suficiente para baterias de backup de até 12,7Ah.

A Controladora deverá ser compatível com leitoras de cartão ou outros dispositivos leitores, que utilizem protocolo Wiegand 26, 34 ou 42 bits (padrão de fábrica), e ainda permitindo customização para diferentes protocolos.

Módulos de expansão de entrada de sensores:

Cada controladora permitirá que se possa conectar até 04 (quatro) módulos de 08 (oito) entradas de sensores cada, em cascata, para assegurar a consistência e facilidade de futuras expansões, totalizando até 32 (trinta e duas) entradas de sensores (zonas de alarme). Cada zona deverá ser uma entrada supervisionada (normal, aberto, curto-circuito).

Estes sinais de alarme deverão ser transmitidos pela rede Ethernet até o Servidor PC, que por sua vez poderá programar cada zona.

A controladora pode ser configurada para armar / desarmar em horário pré-programado.

A controladora pode ser configurada para armar por inatividade de uma determinada zona de alarme.

A controladora pode ser configurada para armar automaticamente após a saída da última pessoa (baseado em contagem de pessoas que entraram menos pessoas que saíram).

A controladora pode ser armada ou desarmada localmente, através de suas leitoras de entrada e saída, através de cartões autorizados ou senhas numéricas (até 100 cartões e 10 senhas). O usuário pode utilizar a leitora de entrada para entrar, somente, ou para entrar e desarmar a controladora de alarme, e pode utilizar a leitora de saída para sair somente, ou sair e armar a controladora de alarme.

Módulos de expansão de saída de relé:

Cada controladora permitirá que se possa conectar até 08 (oito) módulos de 08 (oito) saídas de relé, para assegurar a consistência e facilidade de futuras expansões, totalizando até 64 (sessenta e quatro) saídas de relé NA/NF (normalmente aberto / normalmente fechado). Estes relés podem ser programados através do Software de Controle de Acesso para serem acionados (um ou vários) por ocasião da ativação de uma ou mais entradas de sensores, possibilitando uma matriz de automação de 32 entradas x 64 saídas, inclusive com temporização configurada individualmente por relé.

1.1. SOFTWARE DE CONTROLE DE ACESSO PARA GERENCIAMENTO DO SISTEMA

GERAL

Se o Sistema falhar, cada controladora deverá continuar funcionando autonomamente (stand-alone), tendo em sua base de dados todos os dados de cartões, níveis de acesso, feriados, etc. Não será aceito, em qualquer hipótese, sistema de lista branca ou lista negra.

O Sistema deverá incluir a facilidade de auto-detectar as controladoras através de seus endereços IP.

O software deverá estar na língua portuguesa, e sua interface gráfica deverá ser poderosa e extremamente simples de usar, baseada em sistema operacional Windows, contando com menus intuitivos e com plantas gráficas (quadro sinótico).

O Software de acesso deverá rodar dentro do navegador Web (Internet Explorer 7 ou superior, Mozilla Firefox ou Opera – OBS: para integração com vídeo necessário o Navegador Internet Explorer 7 ou superior) como IIS (Internet Information Service), visando uma arquitetura cliente-servidor realmente distribuída. Qualquer computador conectado à rede poderá funcionar como estação cliente, bastando para isso o usuário inserir o endereço ip do servidor e informar seu nome

de usuário e senha, para então gerir o sistema de acesso de acordo com suas permissões pré-programadas.

O Sistema deverá demonstrar a habilidade de exportar dados, como por exemplo, pacotes estandardizados tipo .xls (documento tipo planilha Excel).

O Sistema deverá ser baseado na plataforma Microsoft Windows, e o banco de dados em SQL ou Oracle versão 10.2.0.1.0.

O Sistema deverá ser instalado em um PC autônomo, o qual deverá suportar processamento de texto e banco de dados.

O Sistema Operacional deverá ser baseado na plataforma Microsoft Windows: Windows 7 Pro 32 ou 64 bits, Windows Server 2003 32 ou 64 bits, Windows Server 2008 R2 32 ou 64 bits;

Banco de Dados SQL Server ou Oracle versão 10.2.0.1.0;

Processador Intel Core i7 980 Extreme ou superior;

Drive CD-ROM/DVD-R para instalação do software;

Mínimo de 8GB de memória RAM;

Porta Ethernet (RJ-45) 10/100 MBits/s.

Espaço de armazenamento (HD) de pelo menos 500 GB apenas para o Sistema Operacional e Software Aplicativo.

Administrador do Sistema – o administrador do sistema deverá programar, monitorar e emitir relatórios através do software central. Também poderá adicionar novos usuários para o software e atribuir níveis de acesso a eles.

Até 100 níveis diferentes de Usuários do Sistema.

Permissão de uso do sistema – O Sistema deverá permitir diferentes níveis de permissão para diferentes grupos de usuários.

O software deverá registrar toda entrada (log) de usuários no Sistema. Cada usuário autorizado deverá digitar seu nome de usuário e sua senha individual.

Departamentos ou Agrupamento de Cartões – Ao se adicionar um novo cartão, senha ou leitura biométrica, dever-se-á ser possível assinalar um departamento e grupo de trabalho ao mesmo. O campo de departamento poderá ser utilizado para determinar o departamento do usuário nos relatórios.

Nível de acesso – O Sistema deverá ter pelo menos 99 níveis de acesso. Cada nível de acesso limita o acesso de um grupo de cartões a uma determinada controladora em uma janela de horário

específica em um determinado dia da semana, de acordo com configurações pré-estabelecidas, conforme segue:

Deverá possuir ao menos 50 configurações de horários diários diferentes, com no mínimo três janelas de horário por dia.

Deverá possuir ao menos 50 configurações de zonas de horário diferentes, zonas de horário estas que sejam formadas pelas configurações de horário acima descritas.

Deverá permitir a definição de pelo menos trinta feriados onde se possa configurar uma zona de horário específica que sobreponha-se à zona de horário corrente.

Deverá ser possível o download de comandos e parâmetros às controladoras, através da rede Ethernet, tais como: pulsar para abrir porta, pulsar para entrar ou sair por barreira (o pulso deverá comandar o sentido de giro de catracas, por exemplo), envio de datas e horários, cartões, níveis de acesso, etc.

-Deverá ser possível o upload de informações contidas nas controladoras, através da rede Ethernet, tais como cartões, níveis de acesso, parâmetros de porta, etc.

Deverá se possível se escolher diferentes cores para diferentes eventos apresentados na lista de transações on-line, a fim de facilitar a identificação de diferentes transações.

Deverá ser possível que se selecionem quais eventos trarão e quais não trarão um pop-up da janela de planta gráfica (quadro sinótico).

Deverá ser possível que se selecionem quais eventos enviarão email ou sms para até cinco usuários diferentes.

Deverá ser possível a seleção de até noventa e nove diferentes grupos de controladoras para a função de Anti-passback Global.

Deverá ser possível a seleção de um grupo de controladoras para a função de integração com sistema de incêndio (rota de fuga).

Deverá ser possível a seleção de um grupo de controladoras para a função de baixa automática de cartão.

Deverá ser possível o rastreamento de cartões e transações.

Deverá possibilitar o cadastramento de cartões provisórios para os usuários normais (colaboradores), com validade definida, caso estes esqueçam seus cartões permanentes, que serão temporariamente desativados automaticamente. Ao se retornar o cartão provisório, o cartão permanente será novamente ativado.

O Sistema deverá permitir que se configure uma data para expiração do crachá de colaborador, ou isentar este usuário da expiração.

O software deverá possuir uma janela de transações on-line, onde deverão ser apresentadas todas as transações ocorridas nas controladoras e no sistema, em tempo real. As transações poderão ter cores específicas, para sua fácil identificação. Ainda deverá ser possível se obter de forma imediata, através de menu flutuante e do módulo de integração de CFTV, imagem de vídeo em tempo real ou imagem gravada do momento do alarme, bem como uma comparação de vídeo de entrada e saída (imagem gravada no momento de entrada × vídeo em tempo real da saída), ou foto do usuário do cartão (caso o alarme esteja relacionado à um cartão específico).

Relatórios em formato de .xls ou .pdf (portable document file) – O Sistema deverá permitir a exportação de dados no formato em formato de .xls ou .pdf (portable document file). Os dados deverão conter data, horário, número de cartão, controladora e tipo de transação, para inclusive servir de base para softwares de ponto.

Foto ID – O Sistema deverá permitir a armazenagem de fotografia do usuário de cartão.

Backup de Banco de Dados – É recomendado que o administrador do Sistema deverá realizar o backup completo do banco de dados semanalmente ou a cada duas semanas. É recomendado o uso de ferramenta padrão de mercado para o gerenciamento de banco de dados SQL para realizar o backup automático ou backup programável das configurações do Sistema. Ainda é recomendado o backup do banco de dados para outro dispositivo de contingência (HD auxiliar) deverá ser executado semanalmente, através de operação manual, pelo administrador do Sistema.

TRATAMENTO DE OCORRÊNCIAS DE ALARMES

Para o completo tratamento de ocorrências de alarmes, o software deverá contar com as seguintes funcionalidades:

Pop-up de janela de navegador contendo planta de pavimento (quadro sinótico) com a sinalização dinâmica do sensor ou porta violado (alarmes de porta deixada aberta, porta forçada, violação de sensores, cartão desconhecido, anti-passback, cartão expirado, falha de alimentação elétrica, bateria baixa, etc.).

Lista específica de transações de alarme (esta lista deverá filtrar e apresentar apenas alarmes), em tempo real, de onde se pode obter de forma imediata, através de menu flutuante, imagem de vídeo em tempo real ou imagem gravada do momento do alarme (módulo de integração de CFTV), ou foto do usuário do cartão (caso o alarme esteja relacionado à um cartão específico).

Nesta mesma lista, e através do mesmo menu flutuante, o operador poderá reconhecer o alarme, abrindo uma janela específica contendo os dados detalhados da porta, barreira ou sensor violado, bem como campo específico para a digitação de texto, justificando o tratamento e fechamento de ocorrência, para posterior pesquisa e auditoria.

O usuário também poderá reconhecer e tratar os alarmes diretamente da planta de pavimento (quadro sinótico), ao se clicar sobre o ícone dinâmico da porta ou sensor de alarme representado nesta planta, abrindo o menu flutuante.

Permite a utilização de tabelas com filtros dinâmicos para busca de alarmes, eventos e quaisquer outras transações efetuadas no sistema.

PLANTA GRÁFICA (quadro sinótico)

Deverá se apresentar na forma de janela on-line individual de navegador Web.

Deverá permitir a importação e adição de inúmeras imagens de plantas de pavimento individuais, em arquivo Jpeg ou BMP.

Deverá permitir que se adicionem ícones individuais para portas e sensores de alarme, que piscarão (ícones dinâmicos) para sinalizar em caso de alarme.

Deverá permitir o rápido acionamento de diversas aplicações, através de menu flutuante, ao se clicar sobre o ícone apresentado na planta gráfica, tais como pulsar abrir porta, configurar parâmetros de controladora, reconhecer alarme, etc.

RELATÓRIOS

Relatório de Transações – O Sistema deverá permitir a visualização de todos os tipos de eventos, bem como disponibilizar a função de procura de eventos. Também deverá permitir a geração de relatórios dentro de períodos de tempo determinados pelo operador. Deverão ser permitidos uma grande gama de filtros de relatórios, compreendendo todas as funções e transações do Sistema. Filtros por data e hora de início, data e hora de fim, número de cartão, nome de empresa, grupo de acesso, acessos válidos de entrada ou saída, zonas de alarme ativadas, bateria baixa, falha de alimentação elétrica, pulsar abrir porta, filtro de relatório por porta ou barreira específica, ou seja, TODAS as transações do sistema deverão poder ser filtradas para relatório específico.

Os relatórios deverão ser apresentados, previamente à sua impressão, na tela do computador, de forma que ainda se possa trabalhar sub-filtros de tabela dinâmica. Nesta tabela dinâmica poder-se-á buscar, por exemplo, a imagem de vídeo (módulo de integração de CFTV) de acesso de um determinado usuário de cartão, em uma controladora que tiver uma câmera analógica ou câmera IP relacionada à mesma.

O relatório deverá ter sua saída de impressão em arquivo PDF (portable document file) ou .xls (planilha Excel).

Deverá ainda possuir um relatório individual para listar, de maneira instantânea, todos os usuários de cartão presentes em um determinado edifício, inclusive mostrando em que sala do prédio o usuário se encontra (para que esta função funcione eficientemente, leitoras de entrada e de saída em cada barreira deverão ser instaladas).

Deverá possuir um módulo de relatório de auditoria, que permite auditar todas as operações e configurações realizadas no software, por usuário, por máquina, por endereço IP, com data e hora.

Pode-se, por exemplo, emitir-se um relatório sobre qual usuário do sistema mudou o nível de acesso (nível X para nível Y) de um usuário de cartão (com nome deste usuário).

Deverá permitir que informações ou dados coletados no banco de dados e mostrados através de relatório possam ser exportados para softwares de ponto (ou outros), através de arquivo .xls.

CADASTRAMENTO DE VISITANTES

Cadastramento e Gerenciamento de Visitantes – O Sistema deverá estar totalmente integrado ao software de controle de acesso, e permitir:

O cadastramento de um número limitado de visitantes, com foto;

Deverá poder criar níveis diferentes de permissão para operadores do software;

Deverá permitir a concessão de diferentes níveis de acesso a diferentes visitantes;

Deverá restringir os níveis de acesso permitidos para diferentes operadores do software (cada operador poderá conceder determinados níveis de acesso a visitantes enquanto que outros níveis de acesso lhe serão negados);

Deverá possuir módulo de controle de ativos que acompanham visitantes (chapelaria);

Deverá possuir módulo de confecção e impressão de crachás;

Baixa do cartão de acesso através de rotina programável para expiração do mesmo com dia e hora de validade.

Baixa automática de cartão em controladoras pré-programadas no Sistema (por exemplo, ao se inserir o cartão em cofre coletor de catraca, o cartão é automaticamente apagado do banco de dados do servidor e da controladora, perdendo suas permissões de acesso, e ficará disponível para utilização por próximo usuário ou visitante).

OUTRAS ESPECIFICAÇÕES GERAIS

Especificações Ethernet (para cada controladora e servidor):

Tranceiver Ethernet 10/100 Mbps (EPHY).

Compatível com IEEE 802.3.

Equalização digital.

Half-duplex e Full-duplex.

Auto-negociação (Auto-negotiation next page ability).

BLW (Baseline wander correction).

125 Mhz (clock generator and timing recovery).

Cirtcuito integrado "wave-shaping".

Modo Loopback.

Nível de Acesso de usuário do Software: 100.

Mapa Gráfico / Quadro Sinótico (Plantas de Pavimento).

Despesas com impostos, taxas, seguros, encargos sociais, trabalhistas, previdenciários e demais despesas eventuais que venham a incidir sobre os referidos serviços, já estão incluídos no preço proposto.

Sem mais para o momento colocamo-nos ao inteiro dispor de V.Sa., para quaisquer esclarecimentos adicionais que se fizerem necessários.

Atenciosamente,

Star Segurança Eletrônica Ltda