

## PROCESSO SELETIVO Nº 018/2013-HUAPA

O **Instituto de Gestão e Humanização – IGH**, torna público para conhecimento dos interessados, que fará realizar **Processo Seletivo** objetivando a Contratação de Empresa para a prestação de Serviços Especializados em Segurança Eletrônica, serviços esses a serem realizados na unidade hospitalar denominada **Hospital de Urgência de Aparecida de Goiânia - HUAPA**, registrado no CNES sob o nº 5419662, com sede no Setor Conde dos Arcos, S/N, Aparecida de Goiânia, Goiás, CEP: 749.692-210, atualmente sob gestão do **Contratante**, conforme contrato de gestão tombado sob o nº **002/2013-SES-GO**, atualmente sob gestão do **Contratante** em convênio com a **Secretaria de Saúde do Estado de Goiás**, conforme especificações constantes dos Anexos deste Edital.

### ANEXOS:

I - Termo de Referência.

II – Minuta de Contrato.

### 1. INFORMAÇÕES PRELIMINARES.

1.1. Data para apresentação de propostas: 20 de setembro de 2013, até 14h.

1.2. Local: Hospital Materno Infantil, Av. Perimetral - Setor Oeste, Goiânia - GO, 74125-120, (Setor: Diretoria Geral);

### 2. DA PARTICIPAÇÃO.

2.1. Podem participar do presente Processo Seletivo os interessados que atendam a todas as condições e exigências deste Edital.

2.2. Não será admitida neste processo a participação de empresas, na qualidade de proponentes, que:

- a) Estejam reunidas em consórcio e sejam controladoras, coligadas ou subsidiárias entre si, qualquer que seja sua forma de constituição;
- b) Concorratórias ou em processo de falência, sob concurso de credores, em dissolução ou em liquidação;
- c) Que estejam com o direito de licitar e contratar com a Administração Pública suspenso, ou que por esta tenham sido declaradas inidôneas;
- d) Estrangeiras que não funcionem no País.

### 3. DA PROPOSTA.

3.1. A Proposta deve ser enviada nos termos exigidos neste Edital, redigida com clareza, em língua portuguesa, devendo ainda necessariamente:

- a) Ser apresentada, impressa, em envelope, lacrado;
- b) Conter todos os itens técnicos de acordo com o Termo de Referência (Anexo I), com seus respectivos preços, inclusive todas as despesas, de qualquer natureza, incidentes sobre o objeto deste Processo Seletivo;
- c) Conter as especificações técnicas dos equipamentos e serviços de forma clara, descrevendo detalhadamente as características técnicas da oferta;

- d) O prazo de validade da proposta, não inferior a 60 (sessenta) dias, a contar da data de apresentação da proposta.
  - e) Relatório de vistoria presencial da unidade, que servirá para elaboração da proposta, devidamente protocolado pela Diretoria Administrativa do HUAPA;
- 3.2.** A Proposta deverá conter ainda:
- a) Declaração de total conhecimento e concordância com os termos deste Edital e seus anexos.
  - b) Identificação da proponente, com a indicação do nome empresarial, com endereço completo (incluindo CEP), telefone, fax, CNPJ, endereço eletrônico para contato;
  - c) Quaisquer outras informações afins que julgar imprescindíveis para a correta análise da proposta.
- 3.3.** A avaliação das propostas será feita com a observância no conjunto de melhor técnica e preço relativos aos serviços e estrutura ofertados.
- 3.4.** Serão desclassificadas as propostas elaboradas em desacordo com este Edital.

#### **4. DA HABILITAÇÃO.**

- 4.1.** Quanto à Habilitação Jurídica, será exigida a seguinte documentação:
- a) Cédula de identidade do representante legal da empresa devidamente autenticada;
  - b) Ato constitutivo, estatuto ou contrato social em vigor, devidamente registrado, acompanhado dos documentos comprobatórios de eleição de seus administradores devidamente autenticado.
  - c) Cartão de CNPJ (Comprovante de inscrição e situação cadastral);
- 4.2.** Quanto à Habilitação Qualificação Técnica, será exigida:
- a) comprovação de aptidão no desempenho de atividade pertinente compatível em características com o objeto desta licitação.
  - b) Termo de realização de Vistoria.
  - c) Balanço contábil e patrimonial.
  - d) Certificação expedida pela Secretaria de Segurança Pública do Estado de Goiás;
  - e) Declarações de fabricantes dos equipamentos a serem utilizados, contendo detalhamento técnico e prospectos;
  - f) Indicação de Engenheiro responsável técnico;
- 4.3.** Quanto à Regularidade Fiscal, será exigida a seguinte documentação:
- a) Prova de inscrição no Cadastro Nacional de Pessoa Jurídica (CNPJ/MF);
  - b) Prova de inscrição no cadastro de contribuintes estadual ou municipal, se houver, relativa ao domicílio ou sede do proponente, pertinente ao seu ramo de atividade e compatível com o objeto contratual;
  - c) Prova de regularidade perante a Fazenda Federal, Estadual e Municipal do domicílio ou sede do proponente, ou outra equivalente, na forma da lei;
  - d) Prova de regularidade relativa à Seguridade Social: Certidão Negativa de Débito – CND, emitida pelo Instituto Nacional do Seguro Social – INSS;
  - e) Prova de regularidade relativa ao Fundo de Garantia por Tempo de Serviço (FGTS) e Certidão de Regularidade de Fornecedor – CRF, emitida pela Caixa Econômica Federal.
  - f) Prova de regularidade perante a Justiça do Trabalho (Certidão Negativa BNDT).
- 4.4.** Os documentos deverão ser apresentados em original ou por qualquer processo em cópia autenticada.
- 4.5.** Os documentos deverão ser enviados, em envelope lacrado contendo a seguinte identificação:

## INSTITUTO DE GESTÃO E HUMANIZAÇÃO – IGH

### PROCESSO SELETIVO Nº. 018/2013

#### PROPONENTE: RAZÃO SOCIAL DA EMPRESA E CNPJ

- 4.6. A não apresentação da totalidade dos documentos exigidos no dia **20/09/2013 às 14h**, ou ainda a apresentação de documentos ou certidões vencidas, poderá importar em imediata inabilitação do licitante.

#### 5. DO JULGAMENTO E ANÁLISE

- 5.1. O Processo Seletivo será processado e julgado, e serão classificadas as propostas que estiverem de acordo com os critérios de avaliação constantes deste Processo Seletivo.
- 5.2. Serão desclassificadas as propostas de preços:
- Que não atendam às exigências deste Processo;
  - Que não apresentem os documentos conforme solicitados no item 04 deste Edital;
  - Com preços excessivos ou manifestamente inexeqüíveis.
- 5.3. Será considerado “melhor preço” proposto àquele que resultar no menor valor GLOBAL para execução dos serviços hora licitados, observadas, inclusive, a melhor técnica proposta.
- 5.4. O IGH se reserva ao direito de realizar, se necessária, eventual negociação para obtenção de condições mais vantajosas, junto às empresas classificadas.
- 5.5. A obtenção de propostas substitutivas mais vantajosas importará na obrigatoriedade de sua apresentação escrita e assinada pelo Proponente, não cabendo qualquer direito de reclamação às demais Licitantes.
- 5.6. O IGH publicará em seu *website* institucional (<http://www.igh.org.br>) a empresa vencedora.
- 5.7. O IGH poderá, a qualquer tempo que anteceda a celebração do instrumento contratual e a seu exclusivo critério, cancelar o Processo Seletivo, sem que caibam aos participantes quaisquer direitos, vantagens ou indenizações.
- 5.8. Após publicação de resultado, será concedido prazo de 02 (dois) dias úteis para interposição de recurso escrito e protocolado na Diretoria Geral, contendo qualificação das partes e razões recursais, sendo este julgado pela Diretoria Geral num prazo de até 05 (cinco) dias úteis, estando a decisão disponível em setor jurídico da Unidade.
- 5.9. Havendo interposição recursal, será automaticamente suspenso o prazo para homologação insculpido em art. 6.2, até que haja julgamento do mérito recursal, e confirmação da empresa vencedora.

#### 6. DO CONTRATO:

- 6.1. As obrigações decorrentes do presente processo seletivo serão formalizadas através da assinatura de contrato de prestação de serviços, do qual fará parte, independentemente de transcrição, o presente Edital, seus anexos e a proposta do Contratado, no que couber.
- 6.2. Após a homologação da licitação, o proponente vencedor será convocado por escrito, para, no **prazo de até 02 (dois) dias úteis**, retirar, assinar e devolver o instrumento contratual.
- 6.3. A minuta poderá, à critério do IGH, ser encaminhada por e-mail.

## 7. DISPOSIÇÕES GERAIS:

- 7.1. É assegurado ao **IGH**, o direito de revogar ou anular, no todo ou em parte, o presente processo seletivo, dando ciência aos participantes, na forma da legislação vigente.
- 7.2. A vistoria técnica da Unidade Hospitalar deverá ser efetuada mediante agendamento e preenchimento de ficha de interesse que estará disponível em Diretoria Administrativa, devendo a proponente munir-se de protocolo.
- 7.3. É facultado ao **IGH**, em qualquer fase do presente Processo Seletivo, promover diligências com o fim de esclarecer ou complementar a instrução do processo.
- 7.4. As decisões referentes a este Processo Seletivo poderão ser comunicadas aos proponentes por qualquer meio de comunicação que comprove o recebimento ou, ainda, mediante publicação no *website* <http://www.igh.org.br>.
- 7.5. Os casos não previstos neste Edital serão decididos exclusivamente pelo **Instituto de Gestão e Humanização – IGH**.

Goiânia/GO, 12 de setembro de 2013.

---

Paulo Bittencourt - Superintendente

## ANEXO I

### PROCESSO SELETIVO N° 018/2013 - HUAPA

#### TERMO DE REFERÊNCIA:

O Instituto de Gestão e Humanização – IGH realiza **Processo Seletivo** objetivando a Contratação de Empresa para a prestação de Serviços Especializados em Segurança Eletrônica, serviços esses a serem realizados na unidade hospitalar denominada **Hospital de Urgência de Aparecida de Goiânia - HUAPA**, com sede em Goiânia no Estado de Goiás, atualmente sob administração do IGH, conforme as seguintes especificações a serem consignadas pelo PROPONENTE em proposta:

#### **g) Sobre o objeto contratual:**

1. O objeto desta convocação é a Contratação de Empresa para a prestação de Serviços Especializados em Segurança Eletrônica, mediante locação de equipamentos que compõem o sistema de visualização e gerenciamento de imagens do Hospital de Urgência de Aparecida de Goiânia - HUAPA.

#### **b) Finalidade:**

2. Promover a Instalação, configuração, treinamento, manutenção e locação dos equipamentos que compõem o sistema de visualização e gerenciamento de imagens do Hospital de Urgência de Aparecida de Goiânia - HUAPA.

#### **c) Requisitos técnicos:**

Todas as Câmeras possuam *Infra-Red* com Visão Noturna;

Servidores para recepção das imagens com armazenamento de até 60 dias;

Gravação das imagens 24 (Vinte e quatro) horas;

#### **d) Dos materiais e despesas com instalação.**

#### Especificações Catraca Pedestal

- Catraca tipo pedestal com estrutura monobloco em aço carbono pintado com tinta epóxi a pó, configurada a laser, resistente a choques, vibrações e elementos ácidos alcalinos;
- Tampa superior em aço inox escovado com pictogramas operacionais com leds de alto brilho.
- Cantos arredondados com raios de 18 mm, os quais oferecem maior segurança aos usuários evitando danos físicos em eventual colisão com os equipamentos. Tampa superior tem suas extremidades frontais chanfradas a 45°.
- Tampa e portinholas providas de dobradiças internas para facilitar o processo de manutenção e evitar acidentes durante o processo;
- Mecanismo com tratamento superficial de zincagem eletrolítica trivalente que propicia durabilidade, resistência à corrosão com menor impacto ambiental, por ser livre de metais pesados.

- Dispositivo anti-retorno do tipo disco-catraca, travado por trique anti-retorno, com capacidade de suportar torques pesados de até 2000 Nm;
- Mecanismo rolamentado com eixo central em aço-liga SAE 8640, resistente à tração e torção;
- Mecanismo provido de amortecimento progressivo de giro de braço, através de desacelerador linear. Este mecanismo possui ação específica de desacelerar gradativamente o movimento do braço e freá-lo no final do giro, evitando o contragolpe e aumentando a durabilidade do mecanismo;
- Bloqueio de giro por sistema de travamento, o qual é acionado apenas quando do acesso não validado. Este recurso permite a economia de energia, redução de desgastes das peças e maior durabilidade do conjunto;
- Sistema de travamento com dois solenóides, que controlam o fluxo de usuários de forma independente (entrada e saída).
- Sensores indutivos para monitoramento do giro, os quais oferecem maior durabilidade e menor intervenções de manutenção.
- Braços em tubos de aço inox 304 fixados em espigas de aço e roscados no cabeçote, com parafusos de trava sem cabeça de difícil acesso;
- Além do sistema de travamento permitir na falta de energia o livre fluxo de pessoas, o equipamento deve permitir um sistema antipânico denominado Braço-Que-Cai. Na ocorrência de situações emergenciais (tumultos, incêndios ou calamidades), comunicadas através de sinais enviados por alarmes próprios ou por detectores de incêndio (fumaça e calor), é acionado um dispositivo eletromecânico mecânico que desarticula o braço, em posição horizontal, fazendo-o cair, tornando livre a ultrapassagem das pessoas;
- Pictograma de orientação com leds de alto brilho.
- Índice de proteção (IP) 42;
- MCBF superior a 1 milhão;
- Tempo médio para reparo (MTTR): máx. 30 min;
- Temperatura de trabalho: -10 à 55°C;
- Dimensões: largura 730 mm; altura 975 mm; comprimento 1100 mm.

### Especificações Catraca para Deficientes Físicos

- Catraca tipo pedestal para acesso PNE
- Estrutura monobloco com acabamento totalmente em aço inox escovado longitudinalmente, configurada a laser, resistente a choques, vibrações e elementos ácidos e alcalinos;
- Tampa superior basculante, totalmente em inox, para facilitar a manutenção do mecanismo.
- Na coluna existe uma portinhola provida de fechadura que permite o acesso às placas eletrônicas e facilita o acesso a fixação do equipamento no solo;
- Todos os cantos são arredondados com raios de 18 mm, sendo que a tampa tem sua extremidade frontal chanfrada a 45°. A tampa e a portinhola são providas de dobradiças internas;
- Porta de Bloqueio - A porta de bloqueio é composta por uma estrutura de tubos em aço inox AISI 304 Ø 32 mm com comprimento de 0,875 metros (espaço suficiente para uma cadeira de rodas), sua abertura se dá de forma manual ou eletrônica (o usuário aproxima o cartão ao validador) deslocando-se num ângulo de 90°, que de forma alguma limita a passagem do deficiente físico. A parte central da porta é composta por uma placa de acrílico com espessura de 5 mm onde é fixado o adesivo identificando o acesso de pessoas com eficiência física;

- Sensores indutivos para controle da abertura e fechamento do braço de bloqueio;
- Bloqueio de movimento por sistema de travamento;
- Ângulo de abertura do braço de bloqueio: 180°;
- Placa de interface catraca-validador com múltiplas funções;
- Sistema de travamento com dois solenóides, que controlam o fluxo de usuários de forma independente (entrada e saída);
- Mecanismo provido de “desacelerador” linear, que funciona como um amortecimento do retorno do braço, para possibilitar o retorno automático do braço, não causar impacto ao usuário e reduzir o esforço no mecanismo;
- Tempo médio para reparo (MTTR): máx. 20 min;
- Temperatura de trabalho: -10 à 55°C;
- Peso aproximado de 30 Kg.

### Especificações Cancelas

- Bloqueio para veículos (cancela);
- Gabinete em aço carbono com pintura epóxi na cor amarela;
- Braço em alumínio, na cor branca com faixas refletoras na cor amarela
- Braço de 3 metros com articulação de 180 graus, auxilia o acesso de veículos altos, deixando o pé-direito do local como limitador de altura;
- Dispositivo de embreagem manual: No caso de uma queda de energia ou desligamento, destravar o dispositivo da embreagem e erguer o braço manualmente;
- Quando a energia for restabelecida, travar o dispositivo de embreagem para fazê-lo funcionar normalmente;
- Sistema de balanceamento por molas: Sistema que utiliza duas molas de compressão protegidas por uma capa e que pode ser ajustado conforme carga necessária. O uso de molas de compressão evitam acidentes ocasionados por quebras indesejáveis, comuns em molas de tração.
- Controle remoto sem fio, com alcance de 50 metros. Possui três botões de controle: para levantamento, descida e pausa do braço;
- Função anti-esmagamento: o braço irá se levantar se o mesmo atingir algo quando estiver descendo;
- Entrada para sinais de fotocélula infravermelha: para evitar o impacto quando o braço estiver descendo, para prevenir que os veículos sejam pressionados;
- Entrada para sinais de detector tipo laço indutivo;

### **ESPECIFICAÇÕES TÉCNICAS DAS CÂMERAS DO TIPO IP FIXA, Quantidade de câmeras – 48 (quarenta e oito)**

- Câmera IP do tipo Bullet HD com 3 opções de codecs JPEG, MPEG-4 e H.264.
- Permitir 2 codecs simultâneos (JPEG, MPEG-4 e H.264) em qualquer combinação inclusive do mesmo codec.
- Possuir proteção IP66.
- Possuir sensor CMOS Exmor de 1/3” com 1,4 Megapixels.
- Possuir função Day/Night, sendo sensível a infravermelho.

- Possuir luz infravermelha e possuir função de sincronismo com a função Day/Night. Possuir função de controle de intensidade das luzes infravermelhas.
- Possuir luz infravermelho com comprimento de onda de 850 nm, permitido captura de imagem de objetos a 30 metros de distância em 0 lux.
- Possuir tecnologia que reproduza imagem com Wide Dynamic Range de até 130 dB.
- Possuir função para otimização do brilho e reprodução de cor dinamicamente para oferecer melhor qualidade de imagem em condições de iluminação pobre.
- Possuir função para cancelamento de ruídos.
- Iluminação mínima de 0,22 lux (50IRE) no modo colorido e 0 lux (50IRE) no modo Branco e Preto.
- Possuir lente CS-Mount Varifocal de 2,9X, distância focal de 3,1 a 8,9 mm.
- Possuir ângulo de visualização de 85,4° a 31,2°.
- Interface de rede Ethernet 10Base-T/100Base-TX.
- Permitir resolução 1280 x 720 ou 1280 x 1024 em qualquer codec.
- Taxa Máxima de Quadros: 30 quadros por segundo em JPEG na resolução 1280 x 1024.
- Compressão JPEG com 10 níveis selecionáveis de compressão.
- Possuir pan/tilt/zoom eletrônico.
- Suportar até 8 posições de preset (PTZ eletrônico).
- Possuir no mínimo 5 rondas de seguranças pré programadas e cada uma possuir no mínimo 16 presets de posição com PTZ eletrônico.
- Permitir recorte de imagem em todos os codecs, de tal forma que apenas a área de interesse é transmitida, para reduzir os requisitos de largura de banda e armazenamento.
- Possuir facilidade de acesso via web browser, podendo ser configurada e visualizada.
- Ser capaz de gerar código HTML para a imagem de vídeo, permitindo fácil integração com página da WEB.
- Permite acesso simultâneo de até 10 usuários.
- Possuir 6 níveis de acesso a câmera, para que possa limitar privilégios a cada usuário.
- Capacidade de Unicast e Multicast.
- Integração Dinâmica de Quadros para melhora da imagem em movimento.
- Função de detecção de Movimento e Objeto e processamento das imagens incorporado à câmera em qualquer codec selecionado, minimizando assim disparos de alarme falsos, além de reduzir o processamento nos servidores.
- Possuir filtros de movimento como, por exemplo, objeto que invade determinada área, objetos retirados de uma área, objetos que permanecem por um longo período, número de objeto numa área excede, objetos ultrapassam linhas virtuais criadas.
- Possuir detecção de ruídos através de um microfone externo, para disparar o alarme ou ação da câmera.
- Possuir detecção de adulteração da câmera, incluindo pulverização da lente da câmera, mudança de direção da montagem, impedimento da lente.
- Suporte aos protocolos: TCP, IPv4, IPv6, DNS, RTP/RTCP, RTSP, UDP, ARP, HTTP, HTTPS, ICMP, IGMPv3, SMTP, FTPc, DHCP, NTP e SNMP (MIB-2).
- Compatível com a especificação ONVIF (Open Network Vídeo Interface Fórum).
- Capacidade de configuração de porta de uso.
- Capacidade de envio de e-mail na troca do IP dinâmico da câmera.
- Envio de email nas seguintes situações: disparo de alarme e com foto anexada do momento do disparo e fotos periódicas.



- Alimentação PoE (Power Over Ethernet), com a conformidade IEEE 802.3af.
- Possuir aquecedor que é ativado automaticamente quando a temperatura interna cai abaixo de um limiar predefinido.
- Possuir 8 máscaras de privacidade.
- Capacidade de exibição de informações: nome da câmera, taxa de quadro, taxa de banda, etc.
- Obturador eletrônico com ajuste mínimo de 1s e máximo de 1/10.000s.
- Possuir 1 entradas e 2 saída de sensores. Podendo ser configurado “Normalmente aberto” ou “Normalmente Fechado”.
- Possuir filtro de IP para acesso à câmera, podendo ser definido até 10 grupos, através de intervalos de endereços IP.
- Possuir 8 MB de memória interna para imagens em JPEG/MPEG4/H.264 e áudio.
- Capacidade de armazenamento de pré e pós alarme.
- Suporte a áudio bi-direcional integrado a câmera. Possuir 1 entrada e 1 saída de áudio.
- Ser capaz de armazenar 3 arquivos de áudio, para ser reproduzindo como alarmes.
- Possuir slot de Compact Flash para expansão de memória.
- Possuir saída de vídeo analógico.
- Alimentação: 24V AC, 12V DC e PoE.
- Consumo máximo de potência: 30W.
- Peso máximo de 1,650 Kg.
- Possuir suporte de montagem em teto ou parede integrado na própria câmera.
- Temperatura máxima de operação: -30°C a 50°C.

### **ESPECIFICAÇÕES TÉCNICAS DO SOFTWARE DE MONITORAMENTO CFTV, Quantidade de licenças – 48 (quarenta e oito)**

Deverá possuir:

- Suporte de até 64 canais por servidor, com suporte à áudio bidirecional;
- Suporte à câmeras Megapixel;
- Suporte aos formatos de compressão H.264, Mpeg4 e MJPEG;
- Suporte à triplo monitor, com disposição selecionável por monitor;
- Suporte à Joystick Plug&Play Windows;
- Função de mapa sinótico (E-map);
- Função de agendamento de gravação por câmera, com agenda diária, semanal e de feriados;
- PTZ digital e multi-view;
- Vídeo Analítico (seis funções básicas: movimentação geral, perda de sinal, objeto perdido, objeto estranho, perda de foco de câmera e oclusão de câmera) com dez respostas imediatas (enviar email, enviar SMS, chamada telefônica, enviar alarme à cliente remoto, pop-up de E-map, acionamento automático de de saída digital, alarme sonoro, acionamento de preset de PTZ e de patrulhamento PTZ, apresentação de mensagem de alarme em tela, envio de foto de evento para site FTP);
- Eventos de sistema (quatro eventos básicos de alarme: espaço em disco exaurido, temperatura da CPU não usual, carga da CPU não usual e congestionamento de banda de rede) com dez respostas imediatas (enviar email, enviar SMS, chamada telefônica, enviar alarme à cliente remoto, pop-up de E-map, acionamento automático de de saída digital, alarme sonoro,

acionamento de preset de PTZ e de patrulhamento PTZ, apresentação de mensagem de alarme em tela, envio de foto de evento para site FTP);

- Eventos de entradas digitais com dez respostas imediatas (enviar email, enviar SMS, chamada telefônica, enviar alarme à cliente remoto, pop-up de E-map, acionamento automático de saída digital, alarme sonoro, acionamento de preset de PTZ e de patrulhamento PTZ, apresentação de mensagem de alarme em tela, envio de foto de evento para site FTP);
- Aplicação de contagem (pessoas, veículos);
- Reprodução (playback) multicanal (até 16 canais simultâneos) inteligente com pelo menos cinco tipos de busca analítica: movimentação geral, objeto perdido, objeto estranho, oclusão de câmera e perda de sinal);
- Integração de entradas e saídas digitais (I/O);
- Integração de ponto de venda (POS), com filtros básicos e customizados e log inteligente de busca com imagens;
- Cliente Remoto ao Vivo, Cliente Remoto de Reprodução, Painel de Controle Remoto de I/O, Cliente Remoto de Celular (com controle de PTZ e de I/O's no celular, bem como visualização de mais de um canal simultâneo – multiplexação);
- Suporte à múltiplos modelos e marcas de fabricantes de câmeras: no mínimo 100 marcas e 2200 modelos de câmeras;
- Software deverá permitir sistema híbrido via integração com placas de captura de sinais analógicos de vídeo (a serem instaladas no próprio servidor NVR), e controlar câmeras analógicas como se fossem câmeras digitais (IP);
- Integração com Microsoft Active Directory – MSAD, com atualização automática direto do servidor AD.
- Sistema de aviso automático de novas versões do software, para atualização.
- Função *Boosting Record* – Sistema de aumento automático da taxa de quadros de gravação quando da ocorrência de algum evento / alarme pré-programado, voltando à taxa normal de quadros quando o evento / alarme se encerra.
- Sistema de interpretação de dados e integração tipo Metadados (Metadata).
- Função *Motion on Edge* – Além da capacidade de gravação por movimento via software, o Sistema deverá permitir que se configure o mesmo para gravar imagens usando o sistema de detecção de movimento dos dispositivos da ponta, tais como câmeras e vídeo encoders, liberando o processamento do servidor de gravação da tarefa de gravação por movimento.
- Múltiplas zonas de detecção de movimento com sensibilidade individual por zona (mínimo de dez zonas com sensibilidade independente).
- Suporte à múltiplos idiomas (pelo menos 20 idiomas).
- Sistema operacional necessário: Windows XP, Server 2003, Vista, Windows 7 ou Windows Server 2008 R2.
- **Plataforma Aberta:** suporte à mais de 2200 modelos de câmeras, de mais de 100 fabricantes;
- **Multi-site / Multi-servidor:** cada NVR pode suportar até 64 canais de câmeras IP ou encoders de vídeo, e pode ser gerenciado por Cliente Remoto de Visualização padrão ou por Sistema de Gerenciamento Global/Central de Imagens (este com gerenciamento de ao menos 30 tipos de alarmes em até quatro níveis de prioridade, com armazenamento e busca de alarmes em banco de dados SQL);
- **Múltiplos Clientes de Vídeo:** o software NVR deve gerar múltiplos streams de vídeo para múltiplos clientes remotos, clientes web e clientes móveis (PDA e Celular);

- **Vídeo Analítico Inteligente:** suporte de ao menos seis funções básicas: movimentação geral, perda de sinal, objeto perdido, objeto estranho, perda de foco de câmera e oclusão de câmera). Cada função de vídeo analítico pode gerar até dez respostas instantâneas: enviar email, enviar SMS, chamada telefônica, enviar alarme à cliente remoto, pop-up de E-map, acionamento automático de saída digital, alarme sonoro, acionamento de preset de PTZ e de patrulhamento PTZ, apresentação de mensagem de alarme em tela, envio de foto de evento para site FTP;
- **PTZ Inteligente:** Suporte de Joystick Plug&Play Windows bem como de PTZ digital (na tela do aplicativo), com pontos de preset e agendamento de patrulha;
- **Agendamento de Gravação Inteligente – GUI:** função de agendamento de gravação inteligente por câmera, com agenda diária, semanal e de feriados. Cada câmera pode ser configurada para gravação em até três modos no mesmo dia (por movimento, contínua ou por evento de entrada digital ou vídeo analítico), com diferentes taxas de quadros, resolução, codificação de compressão e com configuração de período de gravação de pré-alarme e pós-alarme;
- **Monitor Triplo:** Até 64 canais de vídeo ao vivo podem ser visualizados em cada monitor. Monitor 1 ou monitor 2 podem visualizar o vídeo ao vivo, ou atuar como monitor de alarme, enquanto o monitor 3 pode ser utilizado para a reprodução (playback);
- **Transcoding:** gravação pode ser feita em uma taxa de quadros e resolução, enquanto que a transmissão para clientes remotos é feita em outra resolução e taxa de quadros; Também permite que uma câmera IP MJPEG seja gravada como MPEG4.
- **Perfis de Streaming (fluxo de vídeo):** geração de no mínimo cinco diferentes perfis de streaming de vídeo, para serem selecionados por clientes remotos de visualização de vídeo ao vivo, via navegador de internet, aplicativo cliente dedicado ou cliente móvel celular;
- **E-map Avançado, com pré-visualização de vídeo:** quadro sinótico com liberdade para importação de imagens em pelo menos dois formatos: JPG ou BMP. Múltiplas camadas de mapa (pelo menos dez camadas). Câmeras e dispositivos de entradas e saídas digitais (I/O) podem ser posicionados nas plantas, para se poder visualizar rapidamente onde eventos estão ocorrendo, com uma conveniente janela de pré-visualização do vídeo ao vivo;
- **Interface Amigável:** funções de arrastar e soltar, interface de gravação, painel digital de controle de I/O e controle de PTZ;
- **Detecção Automática de Modelo de Câmera:** busca automática de câmeras digitais (IP) na rede, com detecção automático do modelo (para tal a câmera deve ter suporte ao protocolo UPnP). Para câmeras sem suporte ao UPnP, o usuário pode adicioná-las manualmente. Mesmo quando adicionada manualmente, o software deverá proporcionar função de auto detecção do modelo e marca da câmera, após a inserção de seu número IP;
- **Aplicação de Contagem:** aplicação inteligente de duplo sentido (dentro e fora) de contagem, para objetos, veículos ou pessoas, com definição de área de cobertura e de tamanho de objeto a ser contado;
- **Gerenciamento de Permissões de Usuário:** suporte a um ilimitado número de usuários, com customização detalhada e individual de privilégios;
- **Monitor de Fluxo de Rede:** cada stream de dados para cada cliente remoto pode ser monitorado e/ou bloqueado, quando o fluxo de dados é muito alto;
- **Auto Reciclagem:** recicla automaticamente os arquivos gravados, quando o disco encontra-se cheio. Opções de configuração independente e individual de reciclagem para imagens, log de eventos, log de sistema e aplicação de contagem;
- **Monitoramento de Saúde do Sistema:** monitoramento e geração de alarmes automáticos (a serem enviados para o Cliente Remoto) referente à condição de operação do servidor, incluindo

temperatura da CPU, temperatura da placa mãe, velocidade da ventoinha da CPU e da fonte de energia, espaço em disco exaurido, carga da CPU e congestionamento de rede;

- **Suporte à Integração:** disponibilização de SDK para integração com sistemas de terceiros, como controle de acesso, automação, alarmes de intrusão, vídeo analíticos e outros.
- **Multi-visualização:** Pode-se duplicar / clonar o mesmo canal de vídeo em vários outros canais de visualização ao vivo, podendo-se realizar Pan, Tilt e Zoom digital nas imagens, e assim observar detalhes das imagens, sem prejuízo à visualização do canal de vídeo original;
- **PTZ Inteligente:** Suporte de Joystick Plug&Play Windows bem como de PTZ digital (na tela do aplicativo), com pontos de preset e agendamento de patrulha;
- **Resolução de Monitor:** suporte às resoluções 1024×768, 1200×900, 1280×1024 e 1600×1200 pixels;
- **E-map Avançado, com pré-visualização de vídeo:** quadro sinótico com liberdade para importação de imagens em pelo menos dois formatos: JPG ou BMP. Múltiplas camadas de mapa (pelo menos dez camadas). Câmeras e dispositivos de entradas e saídas digitais (I/O) podem ser posicionados nas plantas, para se poder visualizar rapidamente onde eventos estão ocorrendo, com uma conveniente janela de pré-visualização do vídeo ao vivo;
- **Monitor de Banda de Rede:** monitora e apresenta a utilização de banda de cada canal de vídeo e de clientes remotos de monitoramento;
- **Áudio Bi-direcional:** permite escutar e gravar áudio proveniente de microfones de câmeras;
- **Visualização:** isualização simultânea de 1, 4, 6, 9, 10, 13, 16, 25, 36, 49 ou 64 imagens;
- **Perfis de Streaming (fluxo de vídeo):** geração de no mínimo cinco diferentes perfis de streaming de vídeo, para serem selecionados por clientes remotos de visualização de vídeo ao vivo, via navegador de internet, aplicativo cliente dedicado ou cliente móvel celular;
- Suporte à áudio bidirecional.
- **Processamento Pós-gravação:** cinco tipos de busca analítica nas imagens gravadas: movimentação geral, objeto perdido, objeto estranho, oclusão de câmera e perda de sinal. Permite a utilização de ferramentas de PTZ digital e de melhoria de qualidade de imagem nas imagens gravadas;
- **.Reprodução Multi-canal:** visualização de até 16 canais simultâneos de playback, local e remoto;
- **.Ferramenta de Melhoria de Qualidade de Imagem:** sintonia fina de qualidade de imagem, com controles individuais de visibilidade, nitidez, brilho, contraste e escala de cinza;
- **Busca Inteligente:** cinco tipos de procura de eventos especiais (movimentação geral, objeto perdido, objeto estranho, oclusão de câmera, e perda de sinal) em vídeos gravados, com data, hora e log de eventos, bem como marcações gráficas legendadas por cores;
- **Exportação de vídeo:** exportação uma foto em formato JPEG / BMP; exportação de clipe de vídeo em formato AVI / ASF, com áudio sincronizado, log de POS e log de eventos;
- **Backup manual e automático:** backup de gravação para propósitos de armazenagem; backup de gravação em um sistema de reprodução autônomo, para que se possa assistir ao vídeo gravado ou realizar buscas inteligentes e analíticas das imagens gravadas em qualquer computador que não possua o software NVR instalado; suporte de backup local e remoto para disco rígido local, disco rígido na rede ou CD. O backup automático permite que se faça o agendamento diário do backup de segurança do dia anterior.
- **Log de Dados:** log de eventos não usuais, log de sistema e log de aplicação de contagem podem ser exportados para arquivos XLS ou TXT;

- **Marca D'água:** proteção das imagens gravadas contra adulterações com ferramenta de verificação de autenticidade;
- **Ferramenta de Banco de Dados:** reconstrução, reparo ou realocação das gravações em disco rígido local, externo ou de rede;
- **Suporte à Gravação Remota:** pode-se implementar um servidor remoto redundante de gravação (através da aquisição de licenças adicionais de câmeras IP) para gravar em redundância as imagens armazenadas em um ou mais servidores de gravação, sendo que esta gravação pode ser na mesma resolução e taxa de quadros da gravação original, ou pode-se configurar uma outra resolução e taxa de quadros específica, para redução do consumo de banda.
- **Múltiplo Display de Vídeo ao Vivo:** múltiplos canais simultâneos de vídeo ao vivo de múltiplos servidores (NVR's, NDVR's ou DVR's compatíveis com o software) podem ser visualizados. Modo de monitor duplo para visualizar até 128 canais simultâneos de vídeo ao vivo (64 canais por monitor);
- **Display de Reprodução Multi-canal:** visualização de até 16 canais simultâneos de playback de servidores de gravação remoto (NVR's, NDVR's ou DVR's) compatíveis com o software;
- **PTZ Inteligente:** Suporte de Joystick Plug&Play Windows bem como de PTZ digital (na tela do aplicativo), com pontos de preset e agendamento de patrulha;
- **Interface de Controle de I/O's:** painel digital de controle de I/O's para rapidamente ativar saídas digitais ou de relé e monitorar entradas digitais;
- **E-map Avançado, com pré-visualização de vídeo:** quadro sinótico com liberdade para importação de imagens em pelo menos dois formatos: JPG ou BMP. Múltiplas camadas de mapa (pelo menos dez camadas). Câmeras e dispositivos de entradas e saídas digitais (I/O) podem ser posicionados nas plantas, para se poder visualizar rapidamente onde eventos estão ocorrendo, com uma conveniente janela de pré-visualização do vídeo ao vivo;
- **Backup Remoto:** backup de gravação para propósitos de armazenagem; backup de gravação em .DAT com um sistema de reprodução autônomo, para que se possa assistir ao vídeo gravado ou realizar buscas inteligentes e analíticas das imagens gravadas em qualquer computador que não possua o software NVR instalado;
- **Cliente tipo Navegador de Internet (Web Client):** visualização de até 16 canais de stream de vídeo ao vivo ou playback no Internet Explorer, de qualquer servidor de gravação compatível;
- **Cliente PDA ou Celular:** até 16 canais multiplexados de "snapshot" ou 01 canal de vídeo ao vivo; controle de PTZ para câmeras móveis e controle de dispositivos de entradas e saídas digitais ou de relé (I/O);
- **Suporte à Gravação Remota:** pode-se implementar um servidor remoto redundante de gravação (através da aquisição de licenças adicionais de câmeras IP) para gravar em redundância as imagens armazenadas em um ou mais servidores de gravação, sendo que esta gravação pode ser na mesma resolução e taxa de quadros da gravação original, ou pode-se configurar uma outra resolução e taxa de quadros específica, para redução do consumo de banda.
- **Serviço 3GPP:** suporte de dispositivos móveis celulares via serviço 3GPP embutido no software, para stream de vídeo ao vivo;
- **Serviço de Desktop Remoto (Estação de Trabalho Remota):** serviço de controle de desktop remoto embutido no software, para configuração remota do servidor de gravação;
- **Serviço CMS:** serviço de suporte à Central de Gerenciamento Global - CMS (ferramenta opcional), ferramenta esta que permite o controle de múltiplos sites e servidores de câmeras e dispositivos, em projetos de grande porte.

- **Suporte a POS (Ponto de Venda):** software inclui licença suporte à dispositivos POS, tais como caixas registradoras, caixas de banco, etc., bastando para isso a aquisição opcional de interface serial/IP. Os textos de transações da registradora são apresentados de forma superposta nos canais de vídeo ao vivo, permitindo mensagens de alarme por eventos básicos e/ou customizáveis (mínimo de 10 customizações) e, bem como buscas inteligentes de imagens indexadas pelos eventos de texto;
- **Suporte a Dispositivos I/O (entradas e saídas digitais ou de relé):** software inclui licença suporte à dispositivos I/O's, para controle remoto de entradas e saídas digitais ou de relé (ex. controle de automação e entradas de alarmes), bastando para isso a aquisição opcional de tais dispositivos.
- **Suporte à lentes panorâmicas / panamórficas:** ao equipar-se a câmeras IP fixas com lentes óticas panamórficas 360°, permite que se faça uso de recurso de operação destas, e deverá disponibilizar imagem em modo panamórfico (original de 360° com distorção ótica elíptica), modo de PTZ (navegação renderizada 3D de 360° com pan, tilt e zoom digital, com correção de distorção ótica), modo quad (navegação com quatro vistas independentes da mesma imagem em um canal, renderizada 3D de 360° com pan, tilt e zoom digital, com correção de distorção ótica) e em modo perímetro (navegação com duas vistas independentes da mesma imagem em um canal, cada uma renderizada 2D de 180° com pan e tilt).
- **Detecção inteligente:** detecção inteligente de 6 tipos de evento, 14 diferentes tipos de eventos POS definidos pelo usuário e 4 eventos de sistema, promovendo ferramentas adequadas de resposta imediata (no mínimo 10 tipos de respostas, podendo ser configuradas como individuais ou simultâneas).
- **Eventos de câmeras detectáveis:**
- **Movimentação Geral:** detecção de movimento em áreas previamente selecionadas, com configuração de sensibilidade e tempo de evento;
- **Objeto Perdido:** detecção da remoção de um ou mais objetos de área protegida, marcando no display a posição em que o(s) objeto(s) se encontrava(m), com configuração de sensibilidade e tempo de evento;
- **Objeto Estranho:** detecção da inserção de um ou mais objetos em área protegida, com configuração de seleção de área protegida dentro da imagem, tamanho do objeto, sensibilidade e tempo de evento;
- **Perda de foco:** detecção de perda de foco de câmera;
- **Perda de sinal:** detecção de perda de sinal de câmera;
- **Oclusão de câmera:** detecção de oclusão do campo de visão total ou parcial de uma câmera, com configuração de sensibilidade e tempo de evento.
- **Eventos de Entrada de Sinais Digitais:**
- Detecção de entradas de sinais provenientes de módulos de entradas / saídas digitais (I/O) opcionais ou de I/O's de câmeras digitais ou de entradas provenientes de painéis de alarmes de mercado (estes equipados com saídas seriais de protocolo de comunicação).
- **Eventos de Sistema:**
- Alarme de Sistema quando do espaço em disco (armazenamento) exaurido;
- Alarme de Sistema quando da saúde não usual do sistema, incluindo temperatura da CPU e da placa-mãe, velocidade da ventoinha da fonte de energia e da CPU;
- Alarme de Sistema quando do excessivo uso de recursos do Sistema (carga da CPU);
- Alarme de Sistema quando do congestionamento de rede.

- Detecção de desconexão com servidor POS;
  - Detecção de Abertura de Caixa Registradora;
  - Detecção de início e fim de transação;
  - Detecção de pelo menos 10 tipos de eventos customizados pelo usuário.
- 
- **Alarme de Notificação Instantânea:** alarme rápido para pronta resposta de qualquer evento de detecção inteligente.
- 
- **Mensagem Instantânea no Display:** apresentação de mensagem customizável sobre o vídeo ao vivo de uma câmera, quando do evento detectado;
  - **Tocar Alarme:** configuração para tocar automaticamente um arquivo de som ou gravação customizável, quando do evento detectado;
  - **Envio de Email:** configuração para enviar automaticamente um email a um usuário ou grupo de usuários pré-definidos (usuário ou grupo podem ser definidos por tipo de alarme), quando do evento detectado;
  - **Envio de SMS:** configuração para enviar automaticamente uma mensagem de texto a um usuário ou grupo de usuários pré-definidos (usuário ou grupo podem ser definidos por tipo de alarme), quando do evento detectado – atenção: é necessária a utilização de um modem 3GPP opcional, para que esta função possa ser utilizada;
  - **Chamada Telefônica:** configuração para efetuar automaticamente uma chamada telefônica ao número de um usuário ou grupo de usuários pré-definidos (usuário ou grupo podem ser definidos por tipo de alarme), quando do evento detectado, contendo uma mensagem pré-gravada;
  - **Chamada de Preset ou de Patrulha PTZ:** configuração para efetuar automaticamente um preset de ponto PTZ ou efetuar um grupo de presets na forma de patrulha pré definida, quando do evento detectado;
  - **Ativação de Saída Digital ou de Relé:** configuração para ativar automaticamente uma ou mais saídas digitais ou de relé, conforme o caso, quando do evento detectado;
  - **Envio de Alarme à CMS:** configuração para enviar automaticamente um sinal de alarme para Sistema de Gerenciamento Global, tipo CMS, quando do evento detectado – atenção: é necessária a utilização de um sistema CMS compatível e opcional;
  - **Envio de Foto (Snapshot) para Site FTP:** configuração para enviar automaticamente uma sequência de fotos instantâneas do evento de alarme para um site FTP, quando do evento detectado, permitindo ainda a configuração individual do número e do intervalo de frames a serem enviados, bem como a sua resolução (até resolução D1);
  - **Pop-up de E-map:** configuração para abrir automaticamente uma janela pop-up de mapa sinótico (mapa gráfico), com posição exata da câmera ou dispositivo I/O apresentada na forma de ícone, no mapa, bem como uma janela de vídeo ao vivo, com imagem da câmera em alarme, quando do evento detectado.

## ESPECIFICAÇÕES TÉCNICAS DO SISTEMA CENTRAL DE MONITORAMENTO

Deverá possuir:

### GERAL – Principais Características

- Sistema de gerenciamento central integrado de vídeo digital, áudio e dados, para instalações de larga escala. Projetado para os grandes projetos empresariais e de alto nível, com suporte à servidores NVR – Servidor de Gravação Digital de Vídeo para câmeras IP, DVR – Servidor de Gravação Digital de Vídeo para câmeras Analógicas, NDVR – Servidor de Gravação Digital de Vídeo para câmeras IP e Analógicas, e NVR *Standalone* (autônomo) – Servidor NAS (com Sistema Operacional Linux embarcado) de Gravação Digital de Vídeo para câmeras IP, dispositivos I/O (entradas e saídas digitais) e dispositivos POS (dispositivos de interface com sistemas seriais, tais como caixas rápidos – ATM's e caixas registradoras);
- Solução para gerenciamento de ilimitados servidores de gravação e canais de vídeo, dispositivos I/O, dados e áudio;
- Autêntica arquitetura cliente-servidor, com suporte à ilimitados clientes de mapas, alarmes e matrizes de visualização – um servidor CMS pode conectar-se à ilimitadas estações cliente CMS;
- Suporte à câmeras megapixel;
- Suporte às compressões de vídeo H.264, MPEG4, MJPEG e MxPEG;
- Servidor de Matriz Virtual de Vídeo, com suporte à ilimitado número de matrizes / monitores. Cada matriz pode suportar até 64 (sessenta e quatro) canais de vídeo ao vivo simultâneos em cada monitor. Suporte à *video wall*;
- Sistema de gerenciamento avançado de alarmes em tempo real, com interface gráfica intuitiva que exibe todos os dispositivos do sistema (câmeras, servidores, entradas e saídas digitais – I/O's). O operador do sistema pode operar de forma completa o sistema de gerenciamento de alarme, reconhecendo ocorrências e atualizando o status (estado) das mesmas de maneira rápida e eficiente;
- Banco de Dados SQL Server 2005 Express;
- Suporte e Gerenciamento de Fuso Horário entre servidor CMS, servidores de gravação de vídeo e estações cliente;
- Ferramenta de *Data Mining* (busca de dados);
- Diferentes níveis de privilégio por operador de estação cliente, para acesso de servidores, câmeras, alarmes, logs de eventos e dispositivos;
- Ferramenta embarcada de configuração remota de servidores de gravação de vídeo. O operador pode configurar remotamente qualquer servidor de gravação conectado ao sistema, desde que possua os privilégios para tal;
- Suporte à múltiplos idiomas (pelo menos 09 idiomas);
- Priorização de controle PTZ;
- Integração total com MSAD (Microsoft Active Directory);
- Sistema operacional necessário: Windows XP, 2003 ou Vista.
- Estação de gerenciamento centralizado suporta um número ilimitado de servidores gravação;



- Autêntica arquitetura Cliente-Servidor. O cliente CMS possui recursos de janela popup instantânea de vídeo ao vivo, playback (reprodução remota). Aplicativo de playback remoto e busca inteligente na reprodução para ocorrências (eventos especiais);
- Banco de Dados SQL Server 2005 Express;
- Ferramenta inteligente de fusos horários: o software CMS é projetado para gerenciar servidores em diferentes fusos horários. Dispõe de Tempo Universal Coordenado (CUT) e pode converter a hora local no local do servidor de gravação para o horário do site do servidor de fuso horário da estação de gerenciamento central;
- Sistema de gerenciamento de licenças: o sistema permite sua expansão através da ativação de licenças adicionais de controle de câmeras, dispositivos I/O e dispositivos POS, através da Internet, sem a necessidade de instalação de softwares ou plug-ins.
- Modo de operação com cenários multi-monitor. Cada PC pode conectar-se fisicamente a até três monitores e pode-se obter cenários de ilimitados monitores através de matrizes virtuais de múltiplos PC's e monitores acoplados.
- Operação intuitiva centrada em mapa: todas as funções do software CMS podem ser obtidas diretamente do E-map;
- Inicialização e login automáticos: Servidor de Alarmes, Estação Cliente e Console de Matriz podem iniciar e fazer *login* automaticamente, quando da inicialização do PC;
- Sincronização automática de dispositivos: sincronização automática de todas as câmeras IP, dispositivos I/O, dispositivos POS, nos servidores.
- Ilimitadas camadas de mapas dinâmicos, com árvore hierárquica de navegação;
- Suporte aos formatos de imagem: BMP, GIF, JPEG, PNG e TIFF;
- Ferramenta de interface gráfica de mapa amigável: O usuário pode editar mapas, servidores, câmeras e dispositivos de I/O. Ao sincronizar os servidores, o usuário recebe acesso aos dispositivos remotos, podendo selecionar e arrastar os mesmos para as regiões de mapas;
- Ferramentas de zoom, arraste e rotação para ícones e mapas;
- Cada dispositivo pode ser inserido no mapa através de um ícone específico padrão ou customizado;
- Ferramenta gráfica de exibição do alcance e área de cobertura das câmeras;
- Ao clicar-se com o botão direito do mouse sobre qualquer dispositivo, diversas operações podem ser executadas imediatamente (por exemplo, ao executar esta tarefa para um ícone de câmera, pode-se selecionar imediatamente: “recuperar vídeo gravado”, “exibir janela de vídeo ao vivo”, “recuperar últimos alarmes abertos”, “recuperar alarmes de uma determinada data”);
- Realce de cada dispositivo quando o mesmo é selecionado no mapa;
- Árvore Hierárquica de Mapas – o usuário pode editar ilimitados mapas multi-nível, para rastrear qualquer ocorrência da forma mais eficiente possível;
- O Sistema de Notificação Instantânea de Status apresenta no mapa um ícone ao lado do dispositivo ou câmera em alarme, informando o estado de alarme ou ativação deste dispositivo ou câmera. Alarmes novos são apresentados por este ícone em uma cor, enquanto os alarmes em progresso são apresentados em cor diferente, para um gerenciamento rápido e eficiente de ocorrências;
- Operações Intuitivas de Mapas – quando um alarme é disparado, o usuário pode reagir rapidamente ao obter as informações do mesmo, ativando vídeo ao vivo ou playback (reprodução) de vídeo gravado do alarme de forma instantânea.
- Suporte e gerenciamento de até 45 (quarenta e cinco) tipos de alarmes, 6 (seis) tipos de vídeo analítico, estado de alarmes, cobertura independente de alarmes por operador;

- Prioridade de alarmes: 4 (quatro) níveis de prioridade de alarmes (crítico, alto, normal e baixo) com filtro, para aumentar a eficiência de pronta resposta e busca avançada de ocorrências;
- Ferramenta de *Data Mining* para que o usuário possa rapidamente buscar o histórico de alarmes, filtrando por nome de alarme, nome do operador, estado (*status*) do alarme, prioridade de alarme, intervalo de tempo (data e hora), dispositivo fonte, tipo de alarme e palavra-chave na nota de ocorrência;
- Cobertura: agendamento de cada alarme individualmente, para ser ativado em horário ou intervalos específicos;
- Guia de gerenciamento de alarmes para anexar um guia de procedimentos customizável que o operador deve seguir em caso de ocorrências, para que o operador possa saber o que fazer em caso da ativação de um alarme. Ao se passar o cursor do mouse sobre o ícone em alarme, automaticamente a guia de procedimentos se faz visível;
- Notificações por alarme: para cada alarme apresentado na estação cliente, pode-se programar a abertura automática de uma janela de vídeo ao vivo, a emissão de alarme sonoro, ativar um monitor de alarme (*spot monitor*) em um monitor de matriz de vídeo, enviar um email ou sms no momento de disparo do alarme;
- Impressão rápida de alarme: a estação cliente CMS pode imprimir um relatório detalhado do alarme, com foto do vídeo relacionado, guia de procedimento, carimbo de data e hora e mensagem escrita sobre a ocorrência e situação de alarme;
- Exportação do histórico de cada alarme ou de um grupo de alarmes para uma tabela Excel (.xls).
- Criação de grupos de alarmes que podem ser armados ou desarmados manualmente com rearme manual ou automático, para que se desabilite a apresentação destes na interface gráfica de monitoramento por determinados períodos.
- Sistema de Matriz Virtual IP, com ilimitados monitores distribuídos em rede Ethernet;
- Permite a apresentação de *stream* de vídeo de qualquer servidor integrado ao sistema, tais como com suporte à servidores NVR – Servidor de Gravação Digital de Vídeo para câmeras IP, DVR – Servidor de Gravação Digital de Vídeo para câmeras Analógicas, NDVR – Servidor de Gravação Digital de Vídeo para câmeras IP e Analógicas, e NVR *Standalone* (autônomo) – Servidor NAS (com Sistema Operacional Linux embarcado) de Gravação Digital de Vídeo para câmeras IP;
- Vídeo ao vivo multicanal, onde cada monitor de matriz pode apresentar até 64 (sessenta e quatro) canais simultâneos de vídeo, com suporte a multi-monitor;
- Ao menos 9 (nove) tipos de mosaicos (*layouts*) de vídeo: 1, 4, 9, 12+1, 16, 25, 36, 49 e 64 canais por monitor matriz;
- Controle de PTZ totalmente funcional, para PAN, TILT e ZOOM de câmeras móveis, bem como chamar monitores de matriz específicos e mosaicos de câmeras através dos botões de um *Joystick* USB, padrão Windows *Plug&Play*;
- Alarme matricial: o servidor de matriz pode chamar um popup de canal de vídeo para um “*call monitor* ou *spot monitor*” em determinado monitor de matriz virtual, com uma legenda trazendo o nome do servidor e da câmera em alarme, na cor vermelha;
- Perfil de matriz: onde para cada usuário pode ser atribuído um perfil específico, com privilégios individuais de visualização;
- *Transcoding* (transcodificação): pode-se selecionar diferentes perfis de streaming de vídeo ao vivo para uma mesma câmera, a fim de se gerenciar o consumo de banda;
- Canal de áudio para se escutar áudio proveniente de câmeras com microfones integrados.

- Recurso de Carrocel: permite criar vistas de diferentes números de câmeras, de diferentes servidores, a serem apresentados sequencialmente em determinados monitores tipo matriz.
- Controle Remoto de Servidores embarcado, para configurar qualquer servidor de vídeo remoto, diretamente da central de gerenciamento.
- Playback remoto multi-canal, onde se pode reproduzir simultaneamente 16 canais de vídeo proveniente de servidores NVR – Servidor de Gravação Digital de Vídeo para câmeras IP, DVR – Servidor de Gravação Digital de Vídeo para câmeras Analógicas, NDVR – Servidor de Gravação Digital de Vídeo para câmeras IP e Analógicas, e NVR *Standalone* (autônomo) – Servidor NAS (com Sistema Operacional Linux embarcado) de Gravação Digital de Vídeo para câmeras IP;
- Diversos mosaicos de Playback: 1, 4, 9 ou 16 canais simultâneos;
- Exportação foto em formato JPEG ou de vídeo para os formatos AVI ou ASF, com marca d'água digital;
- Busca Inteligente por Análise de Vídeo, para 5 (cinco) diferentes eventos especiais: movimentação geral, objeto perdido, objeto estranho, oclusão de câmera e perda de sinal), em arquivos com data, hora e log de arquivos;

## **RESUMO – DETALHES TÉCNICOS**

### **Cenário de Triplo Monitor por PC (Estação)**

- Monitor#1: Painel de Navegação / Mapa Seção
- Monitor#2: Sistema de Matriz Virtual de Vídeo ao Vivo
- Monitor#3: Lista Alarme / Lista de mensagens / Playback Remoto

### **Servidor**

- Banco de Dados: SQL Server 2005 Express para armazenar todos os alarmes;
- Servidor Central: Armazena os dados de mapa através de estruturas hierárquicas; Conectar diretamente ao servidor de vigilância para receber notificações de alarme; Fornece o serviço TCP para acesso dos clientes CMS através da rede Ethernet; Registro de diferentes fusos horários em formato UTC;
- Tipos de Notificação Suportados: E-mail / SMS

### **E-Map (Mapa Gráfico – Quadro Sinótico Digital)**

- Árvore Hierárquica de Mapas: ilimitados níveis e camadas de mapas;
- Formato de imagem de mapas: BMP, GIF, JPEG, PNG e TIFF;
- Definição de Servidores de Vídeo: Novo / Editar / Apagar / Desabilitar / Habilitar;
- Definição de Câmeras: Novo / Editar / Apagar / Desabilitar / Habilitar;
- Ferramentas de Navegação: afastar zoom, aproximar zoom, e arraste;
- Indicadores no mapa: ícones para servidores, câmeras, entradas digitais, saídas digitais, dispositivo POS. Ícones com suporte ao formato de imagem TIFF. Apresentação gráfica do raio de cobertura das câmeras. Realce do ícone selecionado no mapa. Customização de ícones;
- Notificador de Status Instantâneo: mostra ícone animado ao lado do ícone de câmera ou dispositivo, para notificar o operador de eventos em andamento e o estado do mesmo;
- Operações Intuitivas de Mapas: ao se clicar com o botão direito do mouse sobre o ícone, seleciona-se abrir último alarme; abrir janela de vídeo ao vivo; abrir janela de playback

instantânea; realizar backup de vídeo gravado; ver relatório de status do servidor de vídeo (com detalhamento de canais ativos e inativos, I/O's acionados, estado do HD, etc.); buscar dados de transações POS;

- Popup de Janela de Vídeo ao Vivo: para ver instantaneamente imagem da câmera selecionada no mapa, independente da matriz virtual de vídeo, com controle PTZ; habilitação de canal de áudio da câmera; Definição rápida de perfil de stream de vídeo, para gerenciar consumo de banda; foto instantânea; apresentação sobrescrita de transações POS;
- Popup de Janela de Playback: popup de janela de playback remoto de vídeo e áudio; Exportação para formatos AVI ou ASF e foto, com marca d'água digital para impedir adulteração de vídeo;

### **Gerenciamento de Alarmes**

- Tipos de alarmes suportados: Sinal de vídeo anormal; gatilho de entrada digital; gatilho de alarme POS; estado anormal da rede ethernet; estado anormal do DVR ou NVR (saúde do sistema, tais como: velocidade da ventoinha da placa-mãe, velocidade da ventoinha da fonte, temperatura da CPU, etc.); vídeos analíticos de movimentação geral, objeto perdido, objeto estranho, perda de foco de câmera, oclusão de câmera; espaço em disco exaurido;
- Ações instantâneas em alarmes: notificação instantânea nos mapas e lista de eventos em tempo real; direcionamento à camada de mapa específica; toque de sons customizados para cada tipo de alarme; popup de janela de vídeo ao vivo; popup de imagem em matriz de vídeo ao vivo; envio de mensagem SMS; envio de mensagem de email;
- Busca de alarmes: ferramentas de Data Mining para pesquisa de histórico de alarmes;
- Popup de Detalhes de Alarme: para visualizar ou imprimir um alarme em específico com pré-visualização de imagens;
- Criação de grupos de alarmes que podem ser armados ou desarmados manualmente com rearme manual ou automático, para que se desabilite a apresentação destes na interface gráfica de monitoramento por determinados períodos.

### **Sistema de Matriz Virtual de Vídeo**

- Visualização ao Vivo: até 64 (sessenta e quatro) canais de vídeo ao vivo por monitor;
- Mosaicos: 1, 4, 9, 12+1, 16, 25, 36, 49 e 64 canais por monitor matriz;
- Tipos de Visualização: Auto-scan flexível, autoscan de mosaicos individuais tipo Carrocel e modo de tela cheia;
- Pop-up automático: mostra automaticamente vídeo associado à alarmes;
- Painel PTZ: painel PTZ flutuante para manipulação de câmeras móveis nas matrizes virtuais;
- Controle PTZ externo: via Joystick padrão USB Plug&Play Windows, no Cliente CMS;

### **Sistema de Playback Remoto**

- Playback Remoto: 16 canais simultâneos;
- Mosaicos: 1, 4, 9 ou 16 canais simultâneos de Playback;
- Função de Exportação: exportação foto em formato JPEG ou de vídeo para os formatos AVI ou ASF, com marca d'água digital;
- Busca Inteligente por Análise de Vídeo, para 5 (cinco) diferentes eventos especiais: movimentação geral, objeto perdido, objeto estranho, oclusão de câmera e perda de sinal), em arquivos com data, hora e log de arquivos;

## **Controle de Acesso Integrado (Especificações)**

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 (simultaneamente, 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. CARACTERÍSTICAS 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 possuir 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 o 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 possuir 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 possuir 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

Todas 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

Todas 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 mm<sup>2</sup>. 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 transceiver 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 transceiver 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 traseiver 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 relé 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, deverá 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).

Circuito integrado "wave-shaping".

Modo Loopback.

Nível de Acesso de usuário do Software: 100.

Mapa Gráfico / Quadro Sinótico (Plantas de Pavimento).

### Especificações do Servidor de Gerenciamento e Armazenamento

- PowerEdge T110 II Chassis with Cabled 4x3.5 Hard Drives
- Windows Server® 2008 Standard Edition (Inclui 5 CALs)
- ShipGroup Brazil
- 4GB Memory (2x2GB), 1600Mhz, Single Ranked, Low Volt UDIMM (speed is CPU dependent)
- Processador Intel® Xeon® Quad-Core E3-1220V2 (3.10GHz, 8M Cache, Turbo, QUAD CORE/4T (69W)
- HD multi select
- Controladora Onboard SATA
- Gerenciamento on board
- Sem Drive Ótico Interno
- Sem documentação
- Opção de RAID não configurado - com controladora On-Board, 1 a 4 HDs
- Garantia de 1 ano com Diagnóstico Remoto e Serviço Executado no Local
- Sem Instalação
- Maintenance Declined
- Cabo C13 5-15P, 3 Metros
- Disco Rígido de 500GB SATA, 7.2K RPM, 3Gbps, cabeado, 3.5"
- Placa On-Board

### Especificações do Nobreak

#### Entrada

- **Configuração Monofásica** (F+N+T) ou **Bifásica**(F+F+T):Tensões: 220V  $\pm$  20%1 Fator de Potência: 0.99 (sob condições normais)
- **Configuração Trifásica** (F+F+F+T):Tensões: 440 ou 380V ou 220V (trifásica)  $\pm$  20% Fator de potência: 0,94 (sob condições normais)
- **Frequência:** 60Hz  $\pm$  5% faixa de sincronismo ajustável até  $\pm$  5Hz (via software ou painel do no-break)

#### Saída

- **Configuração:** Monofásica (F+N+T) ou Bifásica(F+F+N+T)
- **Tensões** (ajustável e configurável2):Até 12kVA 110 a 127 VCA ou 220 a 230 VCA ou 110+110 a 115+115 VCA - 15 kVA 120 a 127 VCA ou 220 a 230 VCA

- **Regulação Estática:**  $\pm 1\%$
- **Ajuste fino da tensão:** Steps de 1 Volt (via software ou painel do nobreak)
- **Frequência do inversor:** 60 Hz  $\pm 0,1\%$  free running.
- **Regulação dinâmica:**  $\pm 4\%$  (para degraus de 100% de carga)
- **THD (carga linear):**  $< 2\%$
- **Fator de crista:** 3:1 (Máx.)
- **Fator de potência:** 0,8
- **Sobrecarga (via inversor):** 4 a 6kVA até 150% por 20s. Acima de 150% transfere para o bypass. 8 a 12kVA até 120% por 20s. Acima de 125% transfere para o bypass. 15kVA até 110% por 20s. Acima de 110% transfere para o bypass.
- **Tempo de transferência:** Falta e retorno de rede -Zero ms (On-line)

- **Rendimento Inversor/Global**

Entrada monofásica: 91% / 85%: Entrada trifásica: 91% / 87%

- **Bypass:** Automático: Via chave estática Manual (painel): Via chave manual rotativa (opcional)
- **Isolação Galvânica na saída:** Transformador isolador (mesmo na condição de bypass)

#### Proteções

- **Curto-circuito:** Eletrônica
- **Contra picos e sobretensão:** Eletrônica
- **Na entrada:** Disjuntor Bipolar / Tripolar
- **Nas Baterias:** Disjuntor Bipolar
- **Descarga total das baterias:** Eletrônica
- **Temperatura Elevada:** Eletrônica Baterias
- **Tensão DC (nominal):** 192 Vcc até 12 Kva 240 Vcc - 15 kVA
- **Tipo de baterias:** Compatível com baterias seladas (VRLA), estacionárias e automotivas
- **Autonomia:** 1 hora.
- **Baterias internas:** (seladas tipo VRLA)
- **Substituição Hot Swap:** Sim
- **Partida pelas baterias (DC Start):** Sim
- **Possibilidade de Expansão:** Sim.
- **Carregador de baterias:** De 1 a 7 A até 12 kVA; 1 a 5 A -15 kVA (configuração via software ou painel do nobreak)
- **Tempo de recarga:** Após descarga total, repõe 90% da autonomia até 10 horas de carga contínua

- **Teste de baterias:** Via software ou painel Ambientes
- **Temp. ambiente para operação:** 0°C a 40°C
- **Umidade do ar:** 0 a 95% (sem condensação)
- **Ventilação:** Forçada
- **Ruído Audível:** Menor que 55db (A) Interface (incluso): Software para ambiente windows
- **TCP/IP – SNMP:** Opcional
- **Contato seco:** Opcional Sinalizações
- **Visual (leds):** Rede presente / Bateria / Saída / Bypass ativo /retificador / Comunicando e dois bargraps (nível de carga na saída e das baterias)
- **Sonora:**

Nobreak energizado, Bateria em descarga, Bateria em nível crítico (2 min. antes), Falha interna, modo Bypass, Sobrecarga na saída, Curto-circuito na saída, Temperatura ambiente elevada e temperatura do Inversor elevada.

- **Display:**

**Medidas:** Entrada e Saída: tensão, corrente, frequência, fator de potência e fator de crista/ Temperatura ambiente e do Inversor / Autonomia residual / Data e hora / Carga utilizada (%) /Capacidade e tipo de baterias / Rendimento.

**Mensagens:** Faltou/Voltou Rede, Sem Sincronismo, Inversor Ativado/Desativado, Sem Bateria, Autonomia das Baterias, Fim da autonomia das baterias, Bypass, Falha Interna, Sobrecarga, Curto-Circuito na Saída, Manutenção Preventiva, Temperatura Ambiente Alta (configurável), temperatura IGBTs Alta, Modo Econômico, Modo Sleep, Baterias OK, Baterias Ruins e sem condições de teste.

Características Mecânicas

- **Grau de proteção/pintura:** IP 21 / Eletrostática Pó
- **Cor:** Texturizado Preto
- **Movimentação:** Rodízios
- **Dimensões:** 770 x 335 x 660 (A x L x P) mm

<b><u>PLANILHA DE MATERIAIS E EQUIPAMENTOS - HUAPA</u></b>			
-			
<b>EQUIPAMENTOS CFTV/SCA</b>			
<b>ITEM</b>	<b>DESCRICAO</b>	<b>QUANT.</b>	<b>UNID. MEDIDA</b>
1	Câmeras IP	48	unidade
2	Caixa Proteção e Suporte Poe	48	unidade
3	Software de Monitoramento CFTV PARA CÂMERAS IP	48	unidade

4	Servidor de Gerenciamento e Gravação de Imagens	2	unidade
5	Catraca para pne total inox	2	unidade
6	Catraca pedestal especial com cofre coletor	4	unidade
7	Software da controladora da catraca	6	unidade
8	Braço que cai para catraca	4	unidade
9	Cancela com braço de 4.5 metros para 2 canais inclui laço indutivo de 6 metros	2	unidade
10	Cancela com braço de 3 metros para 1 canal inclui laço indutivo de 6 metros	1	unidade
11	Servidor de gerenciamento SCA	2	unidade
12	Controle remoto para cancela	5	unidade
13	Software pack para gerenciamento de 08 canais ip 08 licenças SCA	2	unidade
14	Web Cam	4	unidade
15	Servidores de cadastros de visitantes	4	unidade
16	Software de licença de fail-over ip para servidor de gravação	2	unidade
17	Tomadas "jacks" mgs600	10	unidade
18	Cartão acesso RFID	3000	unidade
19	Switch Gerenciável POE de 24 portas 10/100	6	unidade
20	Cabo de Energia	7	unidade
21	HD 3TB	10	unidade
22	Nobreak 4.000 KVA	1	unidade
23	Rack Padrão 19" 28UX600MM	1	unidade
24	Bandeja 28U FIXA	5	unidade
25	Monitor LCD 21"	2	unidade
26	TV LCD 42"	2	unidade
27	Fonte de Alimentação 13,8 volts 10A	2	unidade
28	Ar Condicionado 12000 Btu	1	unidade
29	Servidor de Visualização	2	unidade
30	Regua tomada 8 pinos	10	unidade

31	Rack 6U	8	unidade
32	Porca gaiola	50	unidade
33	Conector plug femea	15	unidade
34	Conector plug macho	10	unidade
35	Abraçadeira plastica media	200	unidade
36	Conectores RJ-45	600	unidade
37	Capa rj-45	600	unidade
38	Cabo PP 2,5 mm 3 fios	1.500	metro
39	Cabo UTP CAT 6	8.200	metro
40	Abraçadeira tipo copo 3 4"	2.200	unidade
41	Conector para petrolete tipo x	600	unidade
42	Petrolete tipo X	300	unidade
43	Caixa passagem 40x40 parede	6	unidade
44	Copex revestido prata 3 4	250	metro
45	Box reto 3 4	200	unidade
46	Bucha parafuso s6	500	unidade
47	Tubo 1" galvanizado	1.000	metro
48	Patch cord utp modular gs8e 8ft branco	12	unidade
49	Caixa de passagem 40x40 chão	7	unidade
50	Box reto 1"	25	unidade
51	Protetor de surto	5	unidade
52	Cimento 50 kg	4	unidade
53	Areia para massa 25kg	10	unidade
54	Brita fina 25kg	7	unidade
55	Mangueira canaflex	800	metros
56	Serviço de serralheria	5	serviço
57	Mao de Obra Instalação	1	unidade

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

**R\$**

Mao de Obra de Implantacao, Infra Estrutura, cabeamento, tubulação, conectores, e demais componentes para funcionamento - Parcela Única.

R\$

**g) Do pessoal:**

Indicar quantitativo e qualificação dos profissionais a serem disponibilizados (caso necessário), ressaltando, a exclusiva responsabilidade do PROPONENTE em relação à responsabilidade trabalhista e previdenciária.

**h) Dos custos e despesas:**

Devem estar contidas no preço todas as despesas com folha de pagamento, impostos, taxas, encargos sociais, insumos, materiais, e demais despesas administrativas com exceção da energia elétrica e consumo de água.



## ANEXO II

### PROCESSO SELETIVO Nº 018/2013-HUAPA

#### MINUTA DE CONTRATO:

Pelo presente instrumento, de um lado, o **INSTITUTO DE GESTÃO E HUMANIZAÇÃO – IGH** (doravante designado “**Contratante**”), inscrito no CNPJ/MF sob o nº 11.858.570/0002-14, com sede Av. Perimetral, s/n, qd. 37, lote 14, sala 101, Setor Coimbra, Goiânia/GO, CEP: 74.530-020, representado neste ato pelo seu Superintendente, **Paulo Brito Bittencourt**, profissão, 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, o **CONTRATADO**, (doravante designada “**Contratada**”), mediante consenso que entre si mutuamente aceitam e outorgam, resolvem celebrar o presente **Contrato de Prestação de Serviços**, fazendo-o reger-se pelas seguintes cláusulas e condições:

#### 1. Premissas.

---

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

1. O **Contratante** é gestora de renomada instituição hospitalar que necessita de implantação e gerenciamento de sistema de segurança eletrônica;
2. 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;
3. O **Contratado** tem interesse em assistir o **Contratante** em suas necessidades conforme as tratativas mantidas com a mesma;
4. O **Contratado** declara ter ciência do inteiro teor do contrato de gestão tombado sob o nº 002/2013-SES-GO.

#### • Objeto.

---

1. O objeto do presente **Contrato de Prestação de serviços de segurança eletrônica e controle de acesso** para o Hospital de Urgências de Aparecida de Goiânia - HUAPA, atualmente sob gestão, em regime de OS, pelo **Contratante** em contrato de gestão firmado com a **Secretaria de Saúde do Estado de Goiás**.

#### • Do valor do contrato e prazo para pagamento:

---

1. Pela prestação dos Serviços a **CONTRATANTE** pagará à **CONTRATADA**, o valor mensal de R\$ xxxxxxxxxxxxxxxx (xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx), mediante apresentação, pela **CONTRATADA**, de fatura acompanhada de Nota fiscal.
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. 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.

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

• **Obrigações do Contratado.**

- 
1. Caberá a **Contratada**, dentre outras obrigações legais e ou constantes do presente contrato:
1. Implantar o sistema de controle de acesso e rastreamento veicular Hospital de Urgências de Aparecida de Goiânia - HUAPA, obedecendo aos ditames prescritos em proposta comercial também colacionada aos autos do PROSEL 018/2013-HUAPA;
  2. Instalar e fornecer, de imediato, às suas expensas, os seguintes equipamentos:  
xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx;
  3. 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;
  4. Promover a manutenção preventiva e corretiva nos equipamentos descritos em proposta comercial também colacionada ao PROSEL 018/2013-HUAPA, arcando integralmente com custos de mão de obra, transporte, impostos, taxas, contribuições e insumos porventura necessários;
  5. Prestar suporte técnico presencial e por telefone, sempre que solicitado pela Contratante;
  6. Promover, às suas expensas, treinamento de pessoal vinculado à Contratante para melhor utilização dos equipamentos ora fornecidos, instalados e configurados pela Contratada;
  7. Promover a imediata substituição dos equipamentos locados acima descritos e em proposta comercial também colacionada ao PROSEL 018/2013-HUAPA, sempre que estes apresentem defeitos ou anomalias que impeçam o seu regular funcionamento;
  8. Orientar seus empregados e prepostos à comparecerem à Unidade Hospitalar devidamente uniformizados e portando crachá de identificação, sendo a mencionada indumentária fornecida pela Contratada;
  9. Promover periodicamente a substituição de fardamento, de forma a conservar a boa apresentação de seus empregados e prepostos;
  10. Observar rigorosamente as normas e resoluções legais, além de determinações e regimentos perpetrados pelo Estado de Goiás e Município de Goiânia;
  11. A **Contratada** arcará exclusivamente com o custeio de mão de obra, transporte, instalação e manutenção dos equipamentos necessários para o desenvolvimento de suas atividades;
  12. A **Contratada** disponibilizará suporte 24h, em tempo integral, à **Contratante**;
  13. Observar integralmente as normas de segurança, conduta e disciplina estabelecidas pela **CONTRATANTE**, bem como facilitar o acompanhamento da **CONTRATANTE** na sua execução;
  14. Comunicar prontamente à **CONTRATANTE** sobre a existência de problemas que possam interferir no andamento dos Serviços eventualmente contratados;
  15. 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;

16. Assumir exclusivamente a responsabilidade e custeio com transportes e fretes necessários para prestação do serviço ora contratado;
17. 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.
18. Permitir e facilitar a inspeção dos serviços, prestando todas as informações e apresentando todos os documentos que lhe forem solicitados;
19. Zelar e manter em perfeitas condições de higiene e conservação a área física cedida pelo **Contratante**;
20. 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;
21. 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;
22. 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.

- **Obrigações do Contratante.**

---

1. Caberá ao **Contratante**, às suas expensas, dentre outras obrigações legais e ou constantes do presente contrato:
  1. Remunerar o **Contratado**;
  2. Promover as facilidades necessárias para o livre acesso dos profissionais do **Contratado** às suas instalações, desde quando devidamente identificados;
  3. Fornecer água encanada e energia elétrica;

- **Vigência e Prazo.**

---

1. O presente contrato vigorará pelo prazo de 12 (doze) meses, podendo ser renovado por igual período, caso haja manifestação expressa das partes.
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**.
3. O presente contrato poderá ainda ser rescindido, nas seguintes hipóteses:
  1. Se qualquer das partes ceder ou transferir o presente contrato à terceiros, sem a prévia anuência da outra parte, por escrito;

2. Se qualquer das partes se tornar comprovadamente insolvente, requerer recuperação judicial ou extrajudicial ou autofalência, ou ter a sua falência requerida ou decretada;
3. Deixar, qualquer das partes, de cumprir, ou mesmo cumprir irregularmente, cláusulas contratuais, prazos e especificações;
4. O presente contrato poderá ainda ser resolvido, sem que haja, incidência de cláusula penal insculpida em item 6.6, nas seguintes hipóteses:
  1. Perda do direito de Gestão da unidade hospitalar pela Contratante.
  2. 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.
  3. Por exclusivo critério de conveniência e oportunidade da Contratante;
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.

• **Disposições Gerais.**

- 
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;
  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 002/2013-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 de Urgências de Aparecida de Goiânia – HUAPA;
  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;
  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.
  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.
  6. O presente Contrato não obriga as partes a qualquer compromisso de exclusividade;
  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), xx de setembro de 2013.

---

**IGH – Contratante**

---

**– Contratada**

***Testemunhas:***

1. \_\_\_\_\_

Nome:

CPF:

RG:

2. \_\_\_\_\_

Nome:

CPF:

RG: