



## TERMO DE REFERÊNCIA

### 1. OBJETO

1.1 Contratação de serviço integrado de segurança incluindo monitoramento por circuito fechado de televisão (CFTV), sistema de controle de acesso (SCA) e *digital signage*, caracterizado por operação em regime de tempo integral (24x7), composto por instalação, configurações, testes, treinamento, operação assistida, suporte técnico, manutenção preventiva e corretiva de toda solução instalada e o fornecimento de todos os equipamentos, softwares, recursos de rede, licenças de uso, recursos para armazenamento e funcionamento dos sistemas de uso sob o regime de COMODATO;

1.2 O contrato terá prazo de vigência de 60 (sessenta) meses;

1.3 Serão considerados 30 (trinta) dias para a elaboração e entrega do projeto executivo do Sistema de Controle de Acesso e *Digital Signage*, e até 60 (sessenta) dias para implantação do projeto após sua aprovação. Para o CFTV os prazos serão de até 30 (trinta) dias para entrega do projeto executivo e até 90 (noventa) dias após a aprovação do projeto para a instalação e configuração de câmeras e sistemas.

### 2. FUNDAMENTAÇÃO DA CONTRATAÇÃO

#### 2.1 Justificativa e necessidade

A instalação e manutenção de Circuito Fechado de TV e Sistema de Controle de Acesso visa proporcionar maior segurança às pessoas e ao patrimônio público com o estabelecimento de barreiras físicas e dotadas de sistemas inteligentes para controle de acesso de pessoas às áreas internas e por meio do videomonitoramento ativo da circulação de pessoas e de alertas provenientes de programas de identificação de incidentes de segurança embarcados nas câmeras, possibilitando ações mais eficientes por parte dos vigilantes e equipe de segurança. A integração desses dois objetos possibilita a atuação preventiva contra danos ao patrimônio público e à integridade material e física das pessoas que transitam e trabalham no Centro Administrativo Fernando Ferrari (CAFF), na Avenida Borges de Medeiros, nº 1501, em Porto Alegre.

O último contrato firmado para o objeto de CFTV foi em 16/01/2013 para aquisição e instalação de sistema CFTV IP. Desde o vencimento do contrato não houve renovação, nem a contratação para manutenção ou atualização do sistema instalado. Atualmente, são 95 câmeras instaladas, mas verificou-se, no mês de abril de 2023, 51 inoperantes. A estrutura conta com baixa cobertura das áreas externas, principalmente, em razão do não funcionamento das câmeras via rádio. Por andar, estão instaladas 3 câmeras nos corredores principais, deixando um corredor sem cobertura.

Não há atualmente implementado Sistema de Controle de Acesso aos prédios. O serviço contratado de vigilância cobre e monitora o fluxo de transeuntes, carros e incidentes por meio de vigilantes que circulam na área a ser protegida, em período noturno e diurno, e o serviço de apoio cobre a portaria, no entanto não há impeditivos físicos para entrada sem identificação prévia. No estacionamento estão instaladas cancelas de acesso monitorados por câmeras em



serviço prestado por empresa contratada em Termo de Cooperação com a PROCERGS. Este serviço tem como objetivo somente a organização da utilização do espaço e a segurança material dos veículos.

Justifica-se a contratação pelo acima exposto, com o objetivo da proteção do patrimônio público, pela visibilidade do prédio e do fluxo de 4500 agentes públicos e 1500 visitantes (conforme dados de acesso de 2017), da implantação e integração dos sistemas de Controle de Acesso e de Circuito Fechado de TV. A identificação dos servidores e funcionários, o cadastramento de visitantes, a ampliação do número de câmeras e a detecção de eventos programados no CFTV permitirá maior atuação preventiva contra incidentes de segurança que afetem a vida do público no Centro Administrativo e o patrimônio do Estado.

O serviço de *digital signage* justifica-se como uma ferramenta de organização de fluxo, principalmente, de visitantes e usuários não frequentes das instalações do prédio. Nesse serviço são instaladas telas nos corredores para geração de informações, entre elas, de localização dos órgãos, departamentos, divisões e outras estruturas administrativas lotados no prédio. Isto evita o fluxo errado de visitantes e usuários não frequentes para locais diferentes daqueles informados e autorizados durante o cadastro de acesso. O serviço ainda pode ser utilizado para comunicação em casos de emergência ou incidentes de segurança. Em levantamento de mercado, percebeu-se que muitas empresas responsáveis pelo oferecimento dos sistemas de CFTV e Controle de Acesso também fornecem, dada a sinergia encontrada entre tecnologias, o serviço de *Digital Signage*.

A contratação da manutenção corretiva e preventiva garante o funcionamento contínuo desses sistemas de segurança. Atualmente, não há disponível servidores, nem pessoal contratado especializado para a oferta de tal serviço de manutenção de equipamentos, sendo realizada somente a troca, se possível, das câmeras identificadas como fora de operação, ou manutenção de cabeamento e rede, pelos funcionários da equipe contratada de manutenção predial.

## **2.2 Referências legais para a contratação**

Lei 14.133, de 1º de abril de 2021: estabelece normas gerais de licitação e contratação para as Administrações Públicas diretas, autárquicas e fundacionais da União, dos Estados, do Distrito Federal e dos Municípios;

Lei Complementar nº 123, de 14 de dezembro de 2006: estabelece normas gerais relativas ao tratamento diferenciado e favorecido a ser dispensado às microempresas e empresas de pequeno porte no âmbito dos Poderes da União, dos Estados, do Distrito Federal e dos Municípios;

Lei Estadual nº 13.706, de 06 de abril de 2011: dispõe sobre a concessão de tratamento diferenciado e simplificado para as microempresas e empresas de pequeno porte nas licitações públicas, no âmbito da Administração Pública Estadual;

Decreto nº 53.355, de 21 de dezembro de 2016: institui a Gestão Centralizada de Compras e de Alienações do Estado, e o Sistema Gestão de Compras do Estado – GCE;



Instrução Normativa CELIC/SPGG nº 003/2023, de 07 de março de 2023: institui o Portal do Fornecedor do Estado do Rio Grande do Sul, estabelece as suas normas e dá outras providências.

Lei nº 13.709, de 14 de agosto de 2018: Lei Geral de Proteção de Dados Pessoais (LGPD);

Decreto nº 56.106, de 24 de setembro de 2021: institui a Política de Tecnologia da Informação e Comunicação no âmbito da administração pública estadual direta, autárquica e fundacional;

Decreto nº 56.804, de 29 de dezembro de 2022: institui a Política de Segurança da Informação do Estado no âmbito da administração pública estadual direta, autárquica e fundacional;

Instrução Normativa CELIC nº 08, de 02 de setembro de 2020: dispõe sobre os critérios de sustentabilidade ambiental para a aquisição de bens e contratação de serviços e obras relativamente às licitações realizadas pela Secretaria de Planejamento, Orçamento e Gestão por intermédio da Subsecretaria da Administração Central de Licitações - CELIC e dá outras providências.

Instrução Normativa CAGE Nº 3, de 25 de maio de 2023: Estabelece regras e diretrizes para gestão e fiscalização de contratos administrativos de prestação de serviços e fornecimento de bens no âmbito da Administração Pública Estadual.

### **3. LOCAL DA PRESTAÇÃO DOS SERVIÇOS**

O serviço será executado no Centro Administrativo Fernando Ferrari, inclusos prédios Anexos Escola de Educação Infantil (ESEDI), Manutenção e Secretaria de Educação, localizado na Avenida Borges de Medeiros, 1501 – Centro Histórico, Porto Alegre/RS (CEP: 90020-020).

### **4. REQUISITOS DA CONTRATAÇÃO**

#### **4.1 Requisitos gerais**

4.1.1 Todos os sistemas que compõem o escopo deste fornecimento deverão ser fornecidos completos, em todos os seus recursos (hardware e software) de modo a garantir a sua correta operação. Deste modo o sistema de videomonitoramento (CFTV) deverá ser composto por câmeras IP, servidor de gerenciamento, servidores de armazenamento, estação de monitoramento, switches, infraestrutura e serviços necessários, de acordo com as especificações técnicas apresentadas neste Termo de Referência;

4.1.2 Da mesma forma, o sistema de controle de acesso (SCA) deverá ser composto por todos os elementos necessários ao pleno funcionamento do sistema, tais como controladores, terminais faciais, estações de cadastramento, switches, infraestrutura completa e serviços. Os controladores deverão possuir capacidade e características suficientes para gerenciar todos os dispositivos de acesso relacionados abaixo:



a) Porta de acesso com autenticação facial, com sensor de abertura (intrusão): 01 (uma) unidade;

b) Bloqueios com autenticação facial: 15 (quinze) unidades.

4.1.3 A inexistência de qualquer especificação não poderá ser adotada como alegação para o não fornecimento, devendo a CONTRATADA dimensionar tais elementos de forma a atender os requisitos funcionais dos serviços contratados, indicando marca e modelo dos itens ofertados, juntamente com documentação técnica comprobatória, de forma que possa ser feita a validação técnica pela área competente. Tais prerrogativas são válidas para as três partes que compõem a solução: CFTV, SCA e *Digital Signage*;

4.1.4 O Sistema de CFTV deverá permitir integração bidirecional com o SCA, que deverá ser comprovada no site de ambos os fabricantes;

4.1.5 O SCA deverá ser integrado ao Sistema de CFTV, de forma que eventos gerados sejam associados às respectivas gravações provenientes das câmeras posicionadas mais próximas às áreas de acesso, nos seguintes casos: biometria facial inválida, violação de portas e tentativa de acesso forçada;

4.1.6 Os sistemas deverão permitir operação de forma independente, permanecendo em funcionamento mesmo que um dos sistemas tenha o funcionamento interrompido;

4.1.7 Em caso de incidentes, o serviço de *digital signage* deve permitir a exibição de mensagens pré-programadas com instruções de circulação;

4.1.8 As soluções instaladas deverão ter registro de *log* com informação de disponibilidade e resposta das câmeras, dispositivos de *digital signage* e equipamentos de controle de acesso. Não deverá ser possível alteração dos registros de *logs*;

4.1.9 Durante os finais de semana, feriados e turno da noite nos dias de trabalho o controle perimetral das edificações será realizado por meio de vídeo analítico, de modo a identificar nas áreas externas e internas a circulação não autorizada de pessoas;

4.1.10 As listas cadastrais deverão permitir edição a qualquer tempo para inclusão ou exclusão de pessoas nas estações de cadastramento instaladas;

4.1.11 Os equipamentos, produtos, peças ou softwares necessários à solução deverão ser novos e de primeiro uso e não constar, no momento da apresentação da proposta, em listas de *end of sale*, *end of support* ou *end of life* do fabricante, ou seja, não poderão ter previsão de descontinuidade de fornecimento, suporte ou vida, devendo estar em linha de produção do fabricante;

4.1.12 Toda a infraestrutura de rede (switches, racks, servidores, etc), assim como eletrodutos, cabos, caixas, tomadas, interruptores, entre outros, e qualquer comunicação necessária para o funcionamento dos sistemas envolvendo softwares e hardwares deverão ser fornecidos e executados por conta da CONTRATADA com especificações adequadas ao correto e contínuo funcionamento do sistema. O sistema deverá ser operado somente por rede lógica com forma de acesso do tipo *intranet*;



4.1.13 Deverão ser fornecidos quaisquer materiais e acessórios requeridos para o funcionamento pleno do objeto da contratação, tais como: cabos de alimentação, conectores, dutos, bases de apoio, abraçadeiras e conversores;

4.1.14 As especificações e quantitativos de servidores para atendimento do CFTV, Sistema de Controle de Acesso e *Digital Signage* ficarão a cargo da CONTRATADA, a qual deverá apresentar e justificar em projeto executivo de acordo com o pleno funcionamento da estrutura de CFTV;

4.1.15 Deverá ser instalada, em local indicado pela CONTRATANTE, uma sala de controle para os sistemas de segurança instalados, para a qual a CONTRATADA deverá fornecer os equipamentos e softwares necessários para a função de monitoramento. Como requisito mínimo, a estrutura de monitoramento fornecida pela CONTRATADA deverá conter:

- a) um computador ou módulo controlador, com especificações e softwares adequados, que permita o controle das câmeras e a gestão dos analíticos (quando disponíveis) e do controle de acesso;
- b) estrutura de telas em formato de videowall;
- c) Todos os sistemas que compõem o escopo do fornecimento do videowall deverão ser fornecidos completos, em todos os seus recursos (hardware e software) de modo a garantir a sua correta operação. Deste modo o sistema de videowall 2x1 deverá ser composto por dois monitores profissionais de 55” com junção entre as bordas de no máximo 1,8mm, e um servidor de gerenciamento gráfico dedicado baseado em estação de trabalho profissional catalogado por um fabricante de computadores;

4.1.16 Sistemas e equipamentos devem ter manual e passo a passo em português.

## **4.2 Requisitos para Circuito Fechado de Televisão**

4.2.1 O Sistema de Monitoramento por Circuito Fechado de TV (VMS - Solução de Vídeo Monitoramento Profissional) deverá permitir monitoramento 24 horas por dia nos 7 dias da semana com geração de imagens ao vivo constantemente, não somente por evento. Seu armazenamento deverá prover gravação de todas as câmeras por 20 dias, 24 horas por dia a 20 FPS, resolução de 1920×1080, compressão em H.265, com ciclo de movimento de 50%;

4.2.2 O processamento de vídeo-analíticos poderá ser realizado nas câmeras, em *appliances* ou nos servidores desde que cumpridos os requisitos de cobertura, armazenamento, e demais especificações da solução;

4.2.3 Em casos de sinistro (como invasão ao prédio, incêndio, alagamento, etc., ou outros que venham a ser definidos pela CONTRATANTE) as imagens, áudios, textos ou outros, ficarão armazenados por período configurável pelo usuário, sendo o parâmetro mínimo de tempo o prazo contratual;

4.2.4 Deverá utilizar protocolos de rede de comunicação UDP/TCP/IP sobre LANs e WANs, com a largura de banda apropriada;



4.2.5 Deverá dar suporte a software para execução em computadores equipados com os sistemas operacionais Microsoft Windows, versões adequadas ao uso de toda capacidade do Sistema. O Software de controle (VMS) deverá:

- I) apresentar arquitetura cliente-servidor, suportar implantação distribuída e de LAN/WAN;
- II) permitir o gerenciamento de dispositivos, permissões de usuários e administradores;
- III) gerenciar e configurar tipos de alarmes, priorização e associações;
- IV) permitir *backup* da base de dados;
- V) apresentar janela de notificação para o operador;
- VI) a instalação, configuração e o cadastro inicial de usuários devem ser do tipo assistida, com repasse de informações aos servidores e funcionários designados pela CONTRATANTE;
- VII) possuir ferramenta para a geração de relatórios gerenciais a partir da extração de dados do sistema contendo as seguintes informações: hora, data e nome do usuário que o extraiu a informação, além do intervalo de tempo, data e câmera a qual foi extraída a informação, podendo exportar ao menos para formatos: PDF pesquisável, XLS, DOC, CSV;

4.2.6 Deverá permitir a criação e edição de mapas gráficos, hierarquizáveis, que proporcionem uma visualização rápida do status e das câmeras;

4.2.7 Deverá possibilitar a identificação de pessoas;

4.2.8 Deverá permitir ao menos as seguintes funcionalidades:

- I) Alerta para intrusão de área e detecção de faces;
- II) Inteligência para correta diferenciação entre pessoas, animais e objetos de forma a evitar falsos alertas;
- III) Busca de imagens baseadas em data, hora, câmera e tipo de incidentes;
- IV) Compensação de luminosidade;
- V) Permissão de recuperação de imagens dos servidores de gravação;
- VI) Detecção de usuários com máscaras respiratórias.

4.2.9 Deverá ser por alimentação *Power Over Ethernet* (POE). Desse modo, câmeras e estrutura de rede e cabeamento instalados devem ser adequados a tal padrão tecnológico;

4.2.10 A operação assistida por 60 dias deverá conter disponibilização de pessoal da CONTRATADA para auxílio aos operadores do sistema da CONTRATANTE quanto a



utilização do sistema, do controle das imagens e dos vídeo-analíticos, assim como, para configuração dos alarmes e alertas provenientes do CFTV;

4.2.11 A empresa CONTRATADA ficará responsável pela configuração da base de dados gerados pela solução de CFTV;

4.2.12 Deverão ser retiradas e acondicionadas em corretas condições para posterior avaliação de uso pela CONTRATANTE as 95 câmeras atualmente instaladas no Centro Administrativo;

4.2.13 Na recepção da ESEDI deverá ser possível utilizar estação de trabalho para visualizar as imagens de videomonitoramento capturadas nas câmeras do entorno da própria ESEDI;

4.2.14 Equipamento instalado na recepção da ESEDI deve permitir a emissão de alertas sonoros e por mensagem em tela nos casos de sinistros, intrusões e outras ocorrências na área da escola;

4.2.15 Em razão da necessidade de funcionamento contínuo dos equipamentos de CFTV instalados, tais devem conter contingência em caso de interrupção no fornecimento de energia elétrica da rede, suprimindo seu funcionamento emergencial por pelo menos 4 horas;

4.2.16 Equipamentos deverão ser dotados de proteção antissurto de no mínimo 15kV.

### **4.3 Requisitos para SCA**

O software de controle de acesso deverá ofertar minimamente os seguintes módulos:

I) Cadastro e gestão de servidores, funcionários, estagiários e visitantes;

II) Módulo do operador e do administrador do sistema;

4.3.2 O SCA deverá emitir alerta na sala de controle nos casos de: biometria facial inválida, violação de portas, tentativa de acesso a um ambiente não autorizado;

4.3.3 O sistema deverá permitir o cadastro simultâneo em mesma base de dados em todas as estações de cadastramento;

4.3.4 O software e hardware de gerenciamento do sistema de controle de acesso predial deverá ser integrado com o sistema de incêndio e alarmes de emergência fornecido pela Delta Fire, ou outro que venha a ser instalado pela CONTRATANTE, e estar de acordo com o Plano de Prevenção Contra Incêndios (PPCI) do prédio. Deverá ser instalado um “botão de pânico” na Central de Segurança que faça liberação simultânea e independente de energia elétrica e rede lógica de todos os dispositivos de controle de acesso em casos de emergência;

4.3.5 O sistema deverá suportar diversos acessos simultâneos nas diferentes catracas a fim de evitar filas;

4.3.6 O SCA deve manter um *log* com histórico de eventos de auditoria de todas as ações executadas, contendo data e hora, usuário responsável por qualquer inclusão, alteração e exclusão de dados e possibilidade de consulta e pesquisa do conteúdo;





4.3.7 As informações geradas durante o funcionamento do sistema de controle de acesso deverão ser armazenadas por toda a duração do contrato;

4.3.8 O software de controle deverá permitir além do cadastramento de usuários, a geração de relatórios de acesso detalhados, o gerenciamento de permissões de acesso, tempo de expiração das permissões, bloqueio por usuário, alarmes de acesso não autorizado;

4.3.9 O sistema deve permitir a geração de relatórios para a extração de dados do sistema, criados de forma personalizada, podendo exportar para formatos: PDF pesquisável, XLS, DOC, CSV;

4.3.10 O acesso às informações do banco de dados deverá ser garantido ao final do contrato, com disponibilização e integração entre banco de dados;

4.3.11 A empresa CONTRATADA ficará responsável pela configuração da base de dados para alimentação do sistema de acesso. Uma base de dados inicial dos funcionários lotados no Centro Administrativo será fornecida pela CONTRATANTE para inserção no sistema de Controle de Acesso no momento de sua implementação. Tal base será atualizada e complementada pelas informações e novos acessos cadastrados nas estações de trabalho de cadastramento;

4.3.12 O sistema para registro dos servidores, funcionários e estagiários lotados no Centro Administrativo seja pelas estações de cadastramento, seja pelo aplicativo, para cadastro prévio, deve ter como dados obrigatórios: nome completo, ID, CPF, órgão de lotação, foto para biometria facial, e-mail, telefone;

4.3.13 O sistema para registro dos visitantes pelas estações de cadastramento deve ter como dados obrigatórios: nome completo, CPF ou RG, foto para biometria facial, e-mail, telefone, nome completo de servidor que autorizou acesso, órgão que será visitado;

4.3.14 Os leitores devem estar associados ao sentido de entrada e ao sentido de saída das catracas;

4.3.15 O SCA deverá ter botões disponíveis para os operadores monitorarem o estado das portas controladas, incluindo: desativar, bloquear, desbloquear e permitir;

4.3.16 Os locais de instalação de controle de acesso deverão conter catracas ou portinholas eletrônicas de balcão incluindo acesso adequado para portadores de necessidades especiais (PNE);

4.3.17 Deverão ser instaladas estações de trabalho na recepção com sistema e estrutura para cadastro de visitantes, servidores, funcionários e estagiários. Estas deverão conter computador, leitor e gravador de cartão de acesso compatível com os demais itens da solução e webcam. Todos os acessórios citados deverão ser compatíveis com os requisitos e funcionalidades do sistema de cadastro e identificação facial;

4.3.18 Conjuntamente as estações de trabalho para cadastro, deverão ser instaladas impressoras para cartão de acesso compatível com os demais itens da solução, sendo uma para cada ala,





Norte e Sul, do Centro Administrativo Fernando Ferrari. O fornecimento de cartões, conforme seção 8 deste documento, deverá ser realizado pela CONTRATADA a partir de demanda da CONTRATANTE;

4.3.19 A porta controlada pelo SCA, com fechadura de eletroímã e identificação de acesso, na ESEDI terá gestão realizada por ponto focal lotado na ESEDI que poderá conceder ou retirar permissão de acesso a esta determinada porta. Tal concessão deverá ser possível tanto no computador instalado na ESEDI para gerenciamento das imagens na tela instalada no local, quanto através de demanda para estações de cadastramento;

4.3.20 A contratação deverá conter operação assistida por 60 dias, a contar do início da operação, com disponibilização de pessoal da CONTRATADA para auxílio aos operadores/recepcionistas da CONTRATANTE no cadastramento dos servidores, funcionários e estagiários lotados no Centro Administrativo;

#### **4.4 Requisitos para *Digital Signage***

4.4.1 Deverão ser fornecidos para solução de comunicação digital (*digital signage*) monitores profissionais em número a ser determinado e alocado por pavimento, acompanhados de dispositivo controlador (*player*), que poderá ser embarcado no próprio monitor ou não, para a funcionalidade de sinalização digital e software para *digital signage*, bem como os serviços de montagem, instalação, configuração, manutenção, suporte técnico e treinamento. Deverá ser fornecida estação de trabalho dedicada para instalação do software de gerenciamento das telas de comunicação digital. Todos os equipamentos deverão ser novos, de primeiro uso e estar em linha de fabricação na data da contratação;

4.4.2 Equipamentos oferecidos em quantidade maior que 1 (um) devem ser da mesma marca, modelo e cor;

4.4.3 Funcionamento da solução deverá permitir conectividade Wi-Fi, Ethernet (LAN), ao menos 01 (uma) entrada HDMI e 01 (uma) entrada USB;

4.4.4 Em caso de incidentes de segurança ou sinistros o sistema deverá permitir a exibição de avisos pré-programados nas telas;

4.4.5 Os leiautes e informações a serem exibidos pela estrutura de *digital signage* serão fornecidos e controlados por setor responsável da CONTRATANTE, o qual terá total acesso para implementação das funcionalidades.

#### **4.5 Requisitos de manutenção e suporte técnico**

4.5.1 Os serviços de reparo, manutenção e suporte, em caso de não funcionamento, mau funcionamento ou falha técnica da solução instalada devem ser solicitados por abertura de chamado efetuado por servidores da CONTRATANTE, via chamada telefônica local, a cobrar ou gratuita, *e-mail*, aplicativo ou *website* da CONTRATADA, 24 horas por dia, todos os dias da semana, podendo a chamada ser atendida por Central de Atendimento e/ou pelo preposto indicado pela CONTRATADA;



4.5.2 Os serviços de assistência técnica e manutenção especializados devem ser prestados pela CONTRATADA no local de instalação, para todos os equipamentos, acessórios, softwares e hardwares fornecidos. Caso necessário a remoção do equipamento para assistência técnica deverá ser alocado equipamento substituto e equivalente em seu lugar;

4.5.3 Os componentes danificados devem ser substituídos, entregues, instalados e configurados, de modo a deixar a solução em perfeitas condições de uso e com todas as funcionalidades operacionais, nas dependências da CONTRATANTE, no prazo estabelecido para solução de chamados, sem a cobrança de quaisquer custos adicionais, inclusive frete, seguro, etc.;

4.5.4 Os componentes, peças ou materiais que substituírem os defeituosos devem ser originais da fabricante, novos, de primeiro uso, e com qualidade e características técnicas idênticas ou superiores aos existentes;

4.5.5 Em caso de indisponibilidade no mercado nacional e internacional e/ou descontinuidade na fabricação, devidamente atestada pela fabricante, podem ser utilizados, com a concordância prévia da CONTRATANTE, componentes, peças ou materiais similares, de outras fabricantes, ou reconicionados, mas que sejam necessariamente compatíveis, em qualidade, aparência e características técnicas, com os originais, e que ainda demonstrem ter passado por rigoroso processo de preparação para reutilização nas soluções ofertadas;

4.5.6 A CONTRATADA deverá registrar, em sistema informatizado, e disponibilizar quando solicitada, para fins de controle e acompanhamento, todos os dados e informações de chamados técnicos abertos pela CONTRATANTE em relatório;

4.5.7 A CONTRATADA deverá fornecer, instalar e configurar todas as correções e atualizações dos softwares e aplicativos instalados, sem nenhum custo adicional à CONTRATANTE;

4.5.8 Os serviços de manutenção preventiva deverão ser executados em frequência estabelecida em projeto executivo pela CONTRATADA e aprovado pela CONTRATANTE de modo a não causar transtornos ao fluxo de pessoas, ao monitoramento por vídeo e à utilização do *digital signage*, principalmente, para este último serviço, no horário de trabalho do Centro Administrativo Fernando Ferrari e anexos citados neste documento.

## **4.6 Requisitos Mínimos para a Infraestrutura Lógica**

4.6.1 Por infraestrutura considera-se todo o conjunto de componentes necessários ao encaminhamento e passagem dos cabos, para aplicações multimídia, em todo os pontos das edificações, assim como todos os acessórios e/ou dispositivos necessários à instalação dos componentes ativos do sistema que compõem a rede. Portanto a CONTRATADA deverá desenvolver o projeto executivo de toda a solução, incluindo infraestrutura lógica necessária. Sendo, também de responsabilidade da CONTRATADA o fornecimento e instalação de todos os componentes desta infraestrutura, desde eletrodutos, cabos metálicos ou em fibra óptica, Patch Panels, caixas de passagem, etc, sem se limitar somente aos citados;



4.6.2 Todo o projeto e seus componentes deverão atender às normas vigentes, sendo as principais: ANSI/EIA/TIA-568 e ANSI/EIA/TIA-569;

4.6.3 Todos os componentes da solução de cabeamento estruturado devem ser do mesmo fabricante, com exceção dos racks, como forma de garantir compatibilidade e melhor performance em toda a solução.

#### **4.7 Requisitos de segurança da informação**

4.7.1 Incidentes que envolvam vazamentos de dados, indisponibilidade ou comprometimento da informação relacionados à Solução de TIC deverão ser reportados imediatamente à CONTRATANTE;

4.7.2 A gestão dos dados pessoais decorrentes do contrato deverá ocorrer com base nas Diretrizes e Normas Gerais da LGPD – Lei Geral de Proteção de Dados, nº 13.079/2018, que, segundo seu artigo primeiro, dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural;

4.7.3 Os dados pessoais envolvidos no objeto deste contrato não serão utilizados para compartilhamento com terceiros alheios ao objeto de contratação, tampouco serão utilizados para finalidade avessa à estipulada por este documento, salvo casos previstos em lei;

4.7.4 A execução do objeto da contratação deverá estar plenamente adequada à LGPD, permitindo assim auditorias solicitadas pela CONTRATANTE;

4.7.5 A CONTRATADA deverá manter o mais completo e absoluto sigilo em relação aos dados, informações e/ou documentos de qualquer natureza, exibidos, manuseados ou dos quais, por qualquer outro modo, venha a tomar conhecimento em razão dos serviços que lhe foram confiados, ficando, por força da lei, civil, administrativa e criminalmente responsável por sua indevida divulgação, sem prejuízo de responsabilidade por perdas e danos a que der causa;

4.7.6 Deverá ser definido e executado, por parte da CONTRATADA, o procedimento de descarte seguro dos dados pessoais e/ou sigilosos da CONTRATANTE ao encerrar a execução do contrato e/ou quando for necessária a substituição de equipamentos que armazenem dados e informações;

4.7.7 A utilização de serviços de terceiros para sustentar ou viabilizar o funcionamento da Solução de TIC dependerá de anuência da CONTRATANTE;

4.7.8 Toda e qualquer informação e documentação que comprovem a implementação dos requisitos de segurança da informação e privacidade especificados na contratação deverão ser apresentadas à CONTRATANTE sempre que solicitadas, de forma a assegurar a auditoria do objeto contratado, bem como demais dispositivos legais aplicáveis;

4.7.9 Todos os recursos necessários deverão ser disponibilizados para que a CONTRATANTE, ou outra entidade por ela indicada, realize atividade continuada de auditoria de segurança da informação e privacidade relacionadas ao objeto do contrato;



4.7.10 É vedado à CONTRATADA armazenar, distribuir ou veicular materiais, imagens e áudios produzidos e utilizados durante o uso dos equipamentos da solução contratada, ou acessá-los por via remota sem prévia autorização da CONTRATANTE.

#### **4.8 Requisitos de responsabilidade ambiental e sustentabilidade**

A proposta do licitante deverá estar de acordo, no que couber (não adstrito aos itens subsequentes a este), com o disposto na Instrução Normativa 08/2020, publicada na página 8 (oito) do Diário Oficial do Rio Grande do Sul de 02/09/2020.

#### **4.9 Requisitos de treinamento**

4.9.1 Treinamento sobre o sistema de CFTV e SCA deverá ser oferecido para ao menos 20 (vinte) funcionários indicados pela CONTRATANTE e durar o tempo necessário para que todo o pessoal treinado esteja capacitado e apto para operar o sistema. O treinamento deve contemplar:

- I) introdução às funcionalidades das soluções;
- II) configuração dos módulos e operações que compõem a solução;
- III) administração de perfis de acesso de usuários e grupos e envio de notificações;
- IV) abertura de chamados;
- V) administração do sistema e obtenção e visualização de relatórios.

4.9.2 O curso oferecido para treinamento em *digital signage*, ministrado nas dependências do CAFF, com material didático fornecido pela CONTRATADA, deverá ter, no mínimo, 8 (oito) horas e abordar, no mínimo, as seguintes atividades:

- I) conceitos gerais adotados nas instalações;
- II) procedimentos de operação; modos de operação;
- III) especificações técnicas;
- IV) abertura de chamados, manutenções preventivas e corretivas;
- V) aulas práticas.

4.9.3 Os cursos oferecidos, deverão ser ministrados por pessoas qualificadas e homologadas para efetuarem treinamentos em nome das fabricantes dos equipamentos. Não serão aceitos ministradores sem as devidas qualificações exigidas.

### **5 DA VISITA TÉCNICA**

5.1 O prazo para visita técnica iniciar-se-á no dia útil seguinte ao da publicação do Edital, estendendo-se até o dia útil anterior à data prevista para a abertura da sessão pública.



5.2 Para auxiliar no dimensionamento e elaboração de sua proposta, a licitante poderá realizar visita técnica/vistoria nas instalações do local de execução dos serviços, acompanhado por servidor designado para esse fim, de segunda à sexta-feira, das 9h às 11h30 e das 14h às 17h, mediante prévio agendamento de horário junto à Divisão de Engenharia e Projetos, pelo endereço de e-mail [diep@spgg.rs.gov.br](mailto:diep@spgg.rs.gov.br) ou pelo telefone (51) 3288-1361.

5.3 As visitas destinam-se à vistoria, avaliação e ciência das empresas interessadas acerca das condições do local e peculiaridades atinentes à realização dos serviços que compõem o objeto da licitação, para fins de elaboração da proposta e demais efeitos decorrentes desse Termo de Referência;

5.4 As visitas deverão ser feitas por profissional qualificado da empresa interessada, o qual deverá estar munido de documento de identificação e de instrumento que o habilite à representação legal da empresa;

5.5 No dia e hora agendados, servidor designado pelo Chefe da Divisão de Engenharia e Projetos da CONTRATANTE irá acompanhar a visita das empresas interessadas, emitindo a cada uma delas um “Atestado de Visita”;

5.6 Todos os custos diretos e/ou indiretos para a realização de visita técnica são de inteira responsabilidade da proponente;

5.7 A visita técnica poderá ser substituída por declaração formal assinada pelo responsável técnico da licitante afirmando o pleno conhecimento das condições e peculiaridades inerentes à realização dos serviços.

## **6 DA PROVA DE CONCEITO**

6.1 Após a fase de habilitação o LICITANTE provisoriamente classificado em primeiro lugar será convocado pela CONTRATANTE para a realização de Prova de Conceito da solução ofertada;

6.2 A Prova de Conceito destina-se à comprovação de que a solução proposta atende aos requisitos mínimos, e o seu desatendimento implicará na desclassificação da proponente;

6.3 Deverá ser iniciada pelo LICITANTE no prazo máximo de 10 (dez) dias úteis, contados a partir da data de convocação;

6.4 O LICITANTE terá o prazo máximo de 5 (cinco) dias úteis para finalização de todos os testes após seu início, incluindo possíveis ajustes e correções. Durante o prazo indicado deverá ser comprovado o atendimento das funções básicas componentes da solução de acordo com os requisitos mínimos expostos neste Termo de Referência;

6.5 Os testes deverão ser efetuados em equipamentos disponibilizados pelo LICITANTE, nos quais devem estar devidamente instalados e configurados os produtos que serão avaliados e outros softwares necessários para a comprovação dos requisitos técnicos obrigatórios;

6.6 A CONTRATANTE deverá disponibilizar o espaço físico para a realização do teste;



6.7 A prova de conceito será examinada e avaliada pelos servidores representantes da CONTRATANTE, com o apoio da equipe técnica, e terão o prazo de até 2 (dois) dias úteis para conclusão dos testes;

6.8 Todos os custos relativos à PROVA DE CONCEITO ficarão a cargo do LICITANTE, não havendo qualquer indenização em caso de reprovação;

6.9 Para a prova de conceito deverão ser apresentados no mínimo:

- I) Servidor VMS;
- II) Servidor de Controle de Acesso;
- III) Servidor *Digital Signage*;
- IV) Servidor Local de Gravação;
- V) Switch de rede;
- VI) No mínimo uma Câmera de cada tipo;
- VII) No mínimo um Kit de Acesso de cada tipo;
- VIII) Uma estação de Trabalho configurada com os softwares clientes da solução;
- IX) No mínimo dois kits *Digital Signage* (monitor + player).

6.10 Os seguintes parâmetros deverão ser comprovados durante a POC:

- I. O sistema deve permitir que o usuário crie um evento para atribuição automática a si próprio. O sistema deve assumir a propriedade de eventos não tratados. Esta ação é gerenciada por um privilégio específico;
- II. O sistema deverá permitir amplo acesso aos registros às informações capturadas, estatísticas e outros dados para análises e relatórios;
- III. O Sistema deve prover uma interface integrada de mapa georreferenciado;
- IV. O Sistema deve suportar representações gráficas inteligentes para diferentes tipos de dispositivos (câmeras, sensores, botões de emergência);
- V. Os operadores deverão possuir total interação entre a tela de entrada do evento e apresentação do mapa utilizando uma única estação de trabalho;
- VI. Os alertas devem possuir prioridade.
- VII. Os alertas devem possuir informações sobre o local e hora do alerta, além da prioridade de ação;
- VIII. O sistema deverá permitir a criação de novos eventos a partir de alertas recebidos;
- IX. As informações de criação e atualização de eventos deverão ser automaticamente atualizadas nos terminais apropriados (que tenham acesso à área de atuação designada);
- X. Deverá suportar o cadastro de novos eventos através de ao menos os seguintes métodos:
  - a. Janela de criação de eventos da interface gráfica;



- b. Recebimento de sinal ou mensagem de um sistema externo enviando uma condição de alarme ou evento, por exemplo, o sistema de controle de acesso ou botão de pânico ou detector de movimento;

XI. O sistema deve exibir o relatório do alerta, seus detalhes, localização e vídeo relacionado em uma única tela;

XII. Quando da aplicação de câmera com analíticos internos, deve ser demonstrada a comunicação entre o VMS e a câmera IP;

XIII. Independentemente de o analítico ser processado na câmera ou no Servidor Local, deverá ser demonstrada a geração de alerta a partir do cruzamento de barreira;

XIV. Independentemente de o analítico ser processado na câmera ou no Servidor Local, deverá ser demonstrada a detecção de pessoas e características específicas, tais como uso de máscara;

XV. Deverá ser demonstrada a integração entre todos os sistemas citados: Videomonitoramento, Controle de Acesso, *Digital Signage*.

## **7 DA ENTREGA E EXECUÇÃO DO OBJETO**

### **7.1 Apresentação de Projeto Executivo**

7.1.1 A CONTRATADA deverá apresentar Projeto Executivo com a descrição completa da instalação da solução em até 30 (trinta) dias após a emissão da Ordem de Serviço;

7.1.2 O Projeto Executivo deverá conter:

7.1.2.1 Descrição das etapas e cronograma de execução dos serviços de instalação e treinamento;

7.1.2.2 Descrição detalhada da solução;

7.1.2.3 Desenho esquemático de todas as ligações necessárias ao funcionamento da solução (instalação física, elétrica, lógica, etc.);

7.1.2.4 Indicação dos profissionais que executarão os serviços de instalação e treinamento;

7.1.2.5 Cronograma semestral de manutenção preventiva;

7.1.3 O Projeto Executivo deverá proporcionar o perfeito entendimento dos detalhes da solução instalada, da instalação e da manutenção preventiva por parte da equipe técnica da CONTRATANTE;

7.1.4 A aprovação do Projeto Executivo por parte da CONTRATANTE é pré-requisito para a continuidade das etapas de instalação da solução de sistema integrado de segurança.

### **7.2 Local e prazos de entrega**

7.2.1 A entrega da solução deverá ocorrer no Centro Administrativo Fernando Ferrari, Av. Borges de Medeiros, 1501, Praia de Belas, Porto Alegre, Rio Grande do Sul;

7.2.2 A implantação total, considerando a solução testada e em pleno funcionamento, do SCA deve ocorrer em até 60 (sessenta) dias após o aceite do projeto executivo;





7.2.3 A implantação total, considerando a solução testada e em pleno funcionamento, do *Digital Signage* deve ocorrer em até 60 (sessenta) dias após o aceite do projeto executivo;

7.2.4 A implantação total, considerando a solução testada e em pleno funcionamento, do CFTV deve ocorrer em até 90 (noventa) dias após o aceite do projeto executivo;

7.2.4.1 A sala de controle e suas funcionalidades deverão ser entregues após 30 dias da aprovação do projeto executivo, possibilitando assim o monitoramento das câmeras instaladas de modo escalonado ao longo do cronograma firmado entre partes;

7.2.5 Em até 90 (noventa) dias após aprovação do projeto executivo a solução integrada de segurança, objeto deste contrato, deve estar testada, com configuração de integração finalizada e em pleno funcionamento.

### **7.3 Operação assistida**

7.3.1 A Operação Assistida é composta por um conjunto de atividades que permitam o treinamento e capacitação da equipe da CONTRATANTE responsável pelas atividades de operação, além da parametrização, transferindo todo o conhecimento e experiência necessária para a operação dos produtos adquiridos (equipamentos, sistemas ou plataformas de serviços);

7.3.2 Durante o período previamente acordado, é prestado todo o suporte necessário para a operacionalidade dos produtos. Um corpo técnico formado por um ou mais especialistas é designado para o local de operação do contrato, de modo a oferecer suporte na realização de testes, análises, medidas e ajustes, assegurando que as operações diárias sejam realizadas em conformidade com os padrões pré-estabelecidos;

7.3.3 Deverá ser disponibilizado pessoal técnico qualificado e especializado das 7h às 19h durante o período de operação assistida para acompanhamento e verificação do desempenho operacional, suporte para melhoria da eficiência operacional e eliminação imediata de eventuais falhas na solução e no modo de operação. Profissionais indicados pela CONTRATADA deverão possuir certificação ou documentação que comprove de forma inequívoca a capacidade profissional nas soluções implantadas;

7.3.4 Para o caso do SCA a operação assistida iniciará após a implantação das catracas, leitores, estações de cadastramento e equipamento gerenciador do sistema. Este último instalado na sala de controle de acesso;

7.3.5 Para o caso do CFTV a operação assistida iniciará após a instalação, a configuração e o funcionamento pleno de 30% das câmeras previstas e do funcionamento completo da sala de controle;

7.3.6 Respeitado os prazos mínimos supracitados, a Operação Assistida será iniciada após a emissão de Ordem de Serviço.



## 7.4 Áreas abrangidas pela solução

Abaixo lista do escopo de cobertura das câmeras a serem instaladas.

ESCOPO DE COBERTURA CFTV	
Garagem Prédio Anexo (SEDUC)	2 entradas para carros (área interna e externa)
	2 entradas de pedestres
	Área de circulação de carros e pedestres
Térreo	Corredores das alas norte e sul
	Entradas (área interna e externa)
	Hall da escada e escada (de incêndio e principal)
	Acesso de carga e descarga
	Corredor auditório
	Auditório
	Áreas internas de trabalho
	Recepção dos órgãos
	11 Elevadores
	Corredores das alas norte e sul
	Passarela de acesso à SEDUC (área interna e externa)
2º Andar	Corredores das alas norte e sul
	Hall da escada e escada (de incêndio e principal)
	Áreas internas de trabalho
	Recepção dos órgãos
	Corredores das alas norte e sul
3º ao 21º andar	Áreas internas de trabalho
	Recepção dos órgãos
	Hall da escada e escada (de incêndio e principal)
Escolinha	Entrada (área interna e externa)
	Perímetros/cerca
Área externa	Acessos (PROCERGS, Av. Augusto de Carvalho, Av. Borges de Medeiros, R. Antonio Klinger Filho)
	Acessos ao estacionamento
	Zonas de circulação de carros e pedestres
	Rampas e escadas de acesso carga e descarga e ala norte e sul
	CAFF
	Rampa de acesso prédio SEDUC
	Entradas DMEST, UVERGS, Defesa Civil, SDR, Arquivo, Arquivo SOP e SES, Depósito, Almoxarifado e PGE
	Entrada almoxarifado
	5 acessos de estacionamento externos
	Acesso interno e externo



Prédio Anexo (SEDUC)	Hall OSPA, restaurante e academia
	Corredor externo parte de trás da SEDUC

ESCOPO CONTROLE DE ACESSO	
CAFF	Entradas das Alas Norte e Sul
Escolinha	Entrada Escola de Educação Infantil e porta traseira
Prédio Anexo (SEDUC)	Entrada prédio anexo (SEDUC)

## 8. COMPOSIÇÃO DA SOLUÇÃO

8.1 Cabe destacar que o objeto da contratação é o SERVIÇO de monitoramento e apoio à segurança, composto por sistemas integrados de circuito fechado de televisão (CFTV) e de controle de acesso (SCA), compreendendo a operação em regime de tempo integral (24x7) e demais serviços assessoriais;

8.2 Os quantitativos abaixo estabelecem as características mínimas esperadas para a solução a ser apresentada pela CONTRATADA garantindo a cobertura de todas as áreas especificadas anteriormente;

8.3 Caberá exclusivamente à CONTRATADA especificar os quantitativos de licenças, equipamentos, peças, pessoas e demais recursos para prestação dos serviços conforme Acordo de Nível de Serviço esperado.

ITEM	DESCRIÇÃO	UND.	QTD.
<b>1 - CENTRAL DE SEGURANÇA E CONTROLE</b>			
1.1	Servidor de Gerenciamento Gráfico	cj	1
1.2	Painel de VideoWall 2x1	cj	1
1.3	Estação de Trabalho de Monitoramento	cj	1
1.4	Estação de Trabalho de Cadastro com webcam	cj	7
1.5	Impressora para smartcard	un	2
<b>2 - SISTEMA DE CFTV</b>			
2.1	Servidor de videomonitoramento (VMS), incluso hardware, software e serviços necessários	cj	1
2.2	Câmera Tipo 1 – Áreas Comuns/Elevadores	un	251
2.3	Câmera Tipo 2 – Corredores	un	48
2.4	Câmera Tipo 3 – Áreas Externas/Internas Amplas	un	41
2.5	Câmera Tipo 4 – Multi-sensor	un	2
2.6	Câmera Tipo 5 – PTZ	un	1
<b>3 - SISTEMA DE CONTROLE DE ACESSO (SCA)</b>			



3.1	Servidor para Controle de Acesso, incluso hardware, software e serviços necessários	cj	1
3.2	Bloqueio Tipo 1 – Balcão	un	11
3.3	Bloqueio Tipo 2 – Balcão PNE	un	4
3.4	Kit de Acesso 1 (para portas) - Autenticação simples	un	1
3.3	Guarda corpos para acabamento nas áreas de bloqueio		*
3.4	Cartões de acesso acompanhados de cordão para crachá	un	6000
<b>4 - SISTEMA DE COMUNICAÇÃO DIGITAL (DIGITAL SIGNAGE)</b>			
4.1	Servidor para gerenciamento para Digital Signage, incluso hardware, software e serviços necessários	cj	1
4.2	Player para Digital Signage	un	44
4.3	Monitor para Digital Signage	un	44
<b>5 - SISTEMA DE ARMAZENAMENTO DE DADOS</b>			
5.1	Servidor de Armazenamento, incluso hardware, software e serviços necessários	cj	1
<b>6 - INFRAESTRUTURA LÓGICA</b>			
6.1	Switch Core 8 portas SFP+ (Núcleo)	un	4
6.2	Switch Core 24 portas UTP (Distribuição)	un	2
6.3	Switch 24 portas PoE (Borda)	un	18
<b>7 - ALIMENTAÇÃO DE RETAGUARDA E ACESSÓRIOS</b>			
7.1	Nobreak	cj	2
7.2	Rack Padrão 19" 44U - Principal	cj	2
7.3	Rack Padrão 19" 12U - p/ Distribuição	cj	5
<b>8 - SERVIÇOS ENVOLVIDOS</b>			
8.1	Fornecimento de materiais e mão de obra para remoção das câmeras existentes	un	95
8.2	Desenvolvimento do Projeto Executivo	vb	1
8.3	Fornecimento de materiais e mão de obra para implantação do sistema de videomonitoramento (CFTV)	vb	1
8.4	Fornecimento de materiais e mão de obra para implantação do SCA (SCA)	vb	1
8.5	Fornecimento de materiais e mão de obra para implantação do sistema de Digital Signage	vb	1
8.6	Fornecimento de materiais e mão de obra para implantação do sistema integrado de segurança (SIG)	vb	1
8.7	Treinamento Completo no Sistema Integrado de Segurança – SIG, incluindo Videomonitoramento, Controle de Acesso, Digital Signage Centro de Controle, para até 20 colaboradores	vb	1
8.8	Treinamento Completo no Sistema de Digital Signage, para até 8 colaboradores	vb	1
8.9	Operação Assistida de 60 dias para Sistema Integrado de Segurança – SIG	vb	1

\* Os guarda corpos deverão ser fornecidos conforme os requisitos apresentados nesse Termo de Referência, garantindo o correto acabamento das áreas de bloqueio para o Controle de Acesso.

8.4 Deverão ser considerados os seguintes aspectos para a instalação dos equipamentos:

8.4.1 Nas Alas do CAFF: 1 (uma) câmera entre pilares, a cada 2 pilares (15m);



- 8.4.2 “Entorno” são câmeras fixadas nas fachadas dos prédios;
- 8.4.3 No 2º Pavimento da SEDUC: 1 (uma) câmera na saída de cada rampa e na escada, 3 (três) câmeras distribuídas no estacionamento;
- 8.4.4 No 3º pavimento da SEDUC: câmeras distribuídas nas áreas de circulação, 1 (uma) na entrada do restaurante, 1 (uma) no hall da OSPA, 1 (uma) frente à entrada da SEDUC pela rampa, 1 (uma) em frente à entrada da SEDUC pela passarela;
- 8.4.5 Para câmeras internas e no entorno, deverá ser utilizado cabeamento metálico CAT6;
- 8.4.6 Para câmeras externas, deverá ser utilizado fibra ótica com conversor ponta a ponta (2 conversores por câmera). Cabeamento para pontos de energia serão responsabilidade da CONTRATADA;
- 8.4.7 Nas áreas externas, cada ponto de câmera deverá conter ponto elétrico para energizar conversor de fibra;
- 8.4.8 A critério da empresa, se aprovado em projeto executivo, podem ser instalados postes próprios para as câmeras externas;
- 8.4.9 Entrada principal da fibra no rack do 2º Pavimento do CAFF, previsto Splitter e DIO para distribuição das fibras entre racks;
- 8.4.10 Câmeras do tipo “bullet” deverão ser alocadas nas áreas externas;
- 8.4.11 Não será limitado o quantitativo de servidores visando a manutenção da competitividade do certamente. Desse modo, deixa-se somente o requisito de atendimento ao pleno e ininterrupto funcionamento dos sistemas e do armazenamento de informações nos prazos acordados. Mantém-se os requisitos de *failover* e *backup* para as soluções instaladas;
- 8.4.12 A demanda para catracas de controle de acesso e cartões tem como base o escopo de cobertura e o fluxo diário de 6 mil pessoas;
- 8.4.13 Para o *digital signage* foram previstos 2 (dois) monitores por andar de modo a atender as alas Norte e Sul do prédio e 2 (dois) monitores para o prédio Anexo da SEDUC;
- 8.4.14 Para o controle de acesso estão previstos 11 bloqueios do “tipo 1” e 4 bloqueios do “tipo 2” distribuídos da seguinte forma: 4 (quatro) dispositivos “tipo 1” e 1 (um) dispositivo “tipo 2” PNE para entrada norte do CAFF, 5 (cinco) dispositivos, sendo 1 (um) PNE, para entrada da ala sul do CAFF, 2 (dois) dispositivos, sendo 1 (um) PNE para entrada da ESEDI, e 3 (três) dispositivos, sendo 1 (um) PNE para entrada principal da SEDUC. Para a ESEDI, deverão ser instalados equipamentos específicos para acesso a escolas;
- 8.4.15 Para o controle de acesso está previsto um kit para portas que deverá ser instalado na ESEDI;
- 8.4.16 O quadro abaixo apresenta os arranjos de equipamentos descritos nas alíneas anteriores:



Arranjo	Equipamentos
Arranjo 1: ala norte do CAFF	<ul style="list-style-type: none"> <li>• 04 bloqueios tipo 1</li> <li>• 01 bloqueio tipo 2</li> </ul>
Arranjo 2: ala sul do CAFF	<ul style="list-style-type: none"> <li>• 04 bloqueios tipo 1</li> <li>• 01 bloqueio tipo 2</li> </ul>
Arranjo 3: entrada da SEDUC	<ul style="list-style-type: none"> <li>• 02 bloqueios tipo 1</li> <li>• 01 bloqueio tipo 2</li> </ul>
Arranjo 4: ESEDI	<ul style="list-style-type: none"> <li>• 01 bloqueio tipo 1</li> <li>• 01 bloqueio tipo 2</li> <li>• 01 kit de controle de acesso para portas</li> </ul>

8.4.17 Ainda, estão previstos a instalação de 2 (duas) centrais para cadastros, alas Norte e Sul, dotadas de 2 (dois) computadores cada com acessórios necessários para o cadastramento dos usuários, e 1 (uma) central para cadastro no prédio Anexo da SEDUC dotada de 2 (dois) computadores e acessórios necessários para o cadastramento dos usuários;

8.4.18 Guarda-corpos devem ser instalados nas áreas com implementação de equipamentos de controle de acesso com o objetivo de criar mecanismo que impossibilitem o acesso ao prédio sem identificação e validação pelo controle de acesso;

8.5 Quando da entrega dos documentos necessários para habilitação por parte da licitante vencedora do certame, deverão ser entregues junto da proposta as *datasheets* dos componentes da solução acompanhadas de planilha informando a marca e modelo de cada item.

## 9 OBRIGAÇÕES DA CONTRATADA

9.1 A CONTRATADA deve:

9.1.1 Nomear preposto para, durante o período de vigência, representá-la na execução do contrato;

9.1.2 Manter, durante a vigência do contrato, as condições de habilitação exigidas na licitação, devendo comunicar à CONTRATANTE a superveniência de fato impeditivo da manutenção dessas condições;

9.1.3 Apresentar a Anotação de Responsabilidade Técnica (ART) referente aos serviços de instalação, ou outros que sejam necessários, com indicação de responsável por qualquer peça técnica relativa a tais serviços;

9.1.3.1 Os serviços de instalação não poderão ter início sem a apresentação do registro da ART;

9.1.4 Reparar, corrigir, remover, reconstruir ou substituir, às suas expensas, no total ou em parte, o objeto do contrato em que se verificarem vícios, defeitos ou incorreções;

9.1.5 Responder pelos danos causados diretamente à CONTRATANTE ou a terceiros, decorrentes de sua culpa ou dolo na execução do contrato;

9.1.6 Respeitar as normas de controle de bens e de fluxo de pessoas nas dependências da CONTRATANTE;



9.1.12 Ter pleno conhecimento de todas as condições e peculiaridades inerentes aos serviços a serem executados não podendo invocar posteriormente desconhecimento para cobrança de serviços extras;

9.1.13 Cumprir com as normas de segurança e medicina do trabalho durante a possível permanência dos seus profissionais nas instalações da CONTRATANTE;

9.1.14 Manter seus funcionários devidamente identificados quando da execução de qualquer serviço nas dependências da CONTRATANTE referente ao objeto contratado, observando as normas de segurança interna e conduta;

9.1.15 Arcar com todas as despesas, diretas ou indiretas, encargos trabalhistas, previdenciários, fiscais e comerciais decorrentes do cumprimento das obrigações assumidas no contrato, sem qualquer ônus à CONTRATANTE;

9.2 São expressamente vedadas à CONTRATADA:

9.2.1 A veiculação de publicidade acerca deste contrato, salvo se houver prévia autorização da CONTRATANTE;

9.2.2 A subcontratação para a execução do objeto deste contrato;

9.2.3 Contratar cônjuge, companheiro ou parente em linha reta, colateral ou por afinidade, até o terceiro grau, de dirigente do órgão ou entidade contratante ou de agente público que desempenhe função na licitação ou atue na fiscalização ou na gestão do contrato durante a vigência do contrato;

## **10 OBRIGAÇÕES DA CONTRATANTE**

10.1 A CONTRATANTE deve:

10.1.1 Designar gestor do contrato para acompanhamento do mesmo durante sua vigência, bem como dos serviços prestados pela CONTRATADA;

10.1.2 Exigir o cumprimento de todas as obrigações assumidas pela CONTRATADA, de acordo com as cláusulas contratuais;

10.1.3 Proporcionar todas as condições e prestar as informações necessárias para que a CONTRATADA possa cumprir com suas obrigações,

10.1.3.1 Disponibilizar as informações e recursos necessários para que a CONTRATADA possa implantar e manter a solução de acordo com os prazos estabelecidos em contrato;

10.1.3.2 Disponibilizar aos técnicos da CONTRATADA as condições necessárias para o acesso às suas dependências, com vistas à prestação dos serviços;

10.1.4 Exercer ampla, irrestrita e permanente fiscalização de todas as obrigações e fases de execução dos serviços por parte da CONTRATADA, registrando no processo todas as ocorrências relacionadas com a execução contratual, determinando o que for necessário à regularização das faltas ou defeitos observados;

10.1.4.1 Qualquer fiscalização exercida pela CONTRATANTE será feita em seu exclusivo interesse, não implicando corresponsabilidade pela execução das atividades ajustadas e não





eximindo a CONTRATADA de suas obrigações pela fiscalização e perfeita execução dos serviços;

10.1.4.2 No exercício da fiscalização, a CONTRATANTE tem o direito de verificar a qualidade dos serviços e, se constatar que não estão sendo executados corretamente, deve exigir a correção por meio do preposto da CONTRATADA;

10.1.4.3 Constatada a não conformidade na prestação dos serviços executados, a CONTRATADA deve ser notificada formalmente pela CONTRATANTE para que, dentro dos prazos estabelecidos na seção 11 deste Termo de Referência, atenda ao pedido de correção ou justifique o não atendimento, sob pena de incorrer nos ajustes de pagamento previstos no Acordo de Nível de Serviços e/ou em sanções contratuais;

10.1.5 Efetuar o pagamento devido após a verificação de que os serviços foram prestados.

## **11 ACORDO DE NÍVEL DE SERVIÇOS**

11.1 A CONTRATADA será avaliada, mensalmente, pelo nível de prestação dos seus serviços;

11.2 A avaliação do nível de serviço da contratada será feita pelos fiscais do contrato sobre os itens previstos no presente Termo de Referência, consolidando as informações de registro de ocorrências para apresentação à gestão do contrato;

11.3 A avaliação de Nível de Serviço está relacionada aos fatos cotidianos da execução do contrato, vinculando o pagamento aos resultados alcançados, não devendo as adequações de pagamento, originadas pelo descumprimento do ANS serem interpretadas como penalidades ou multas;

11.4 O valor pago mensalmente será ajustado ao resultado da avaliação do serviço por meio do Instrumento de Medição de Resultado (IMR);

11.5 O fornecimento do objeto deste contrato será avaliado por meio de três indicadores: prazo de solução dos chamados técnicos, indicador de disponibilidade e indicador de manutenção preventiva.

11.5.1 A pontuação final da avaliação pode resultar em valores entre 0 (zero) e 100 (cem), correspondentes respectivamente à fornecimento do serviço desprovido de qualidade e fornecimento do serviço com qualidade elevada;

11.5.1.1 Para o caso do Indicador de Disponibilidade de Serviço (IDS) será considerado o período de pleno funcionamento da solução instalada como um todo, considerando todos os equipamentos e softwares funcionando sem falhas conjuntamente;

11.5.1.2 Para o caso do Indicador de Tempo de Solução (ITS) será considerado o tempo acima do estabelecido como parâmetro máximo para atendimento e solução do chamado técnico, considerando a contagem de tempo entre realização do chamado e finalização do atendimento ao problema, a última dada pela fiscalização do contrato, e o grau de severidade do problema estabelecido pela CONTRATANTE no momento do chamado;



11.5.1.3 Para o caso do Indicador de Manutenção Preventiva (IMP) serão considerados os dias de atraso na execução da manutenção preventiva conforme cronograma no Projeto Executivo apresentado pela CONTRATADA e aprovado pela CONTRATANTE;

11.5.2.3 Ao longo do contrato alterações nesse cronograma podem ser apresentadas pela CONTRATADA para nova aprovação da CONTRATANTE ou solicitados justificadamente pela CONTRATANTE;

11.5.3 Os quadros abaixo apresentam os indicadores que compõem o IMR:

Indicador de disponibilidade	
Item	Descrição
Finalidade	Garantir nível adequado de plena disponibilidade de funcionamento da solução contratada
Meta	Disponibilidade mínima de 97% ao mês.
Instrumento de medição	Contagem de horas mensais de plena disponibilidade da solução contratada.
Forma de acompanhamento	Pela fiscalização do contrato, por meio de registro das ocorrências de chamados mantido pela CONTRATANTE, por dados solicitados pela CONTRATANTE e fornecidos pela CONTRATADA e pelo monitoramento da execução do objeto.
Periodicidade de cálculo	Mensal
Método de cálculo	Somatório das horas disponíveis dividido pelas horas totais do mês da avaliação, multiplicado por 100 (cem) para obtenção do valor percentual.
Início da vigência	A partir do início da prestação do serviço ou prazo definido pela CONTRATANTE após início da prestação do serviço.
Faixa de ajuste de pagamento	Maior que 97% = 80 pontos
	Maior que 96% e menor ou igual a 97% = 75 pontos
	Maior que 95% e menor ou igual a 96% = 70 pontos
	Maior que 94% e menor ou igual a 95% = 60 pontos
	Maior que 90% e menor que 94% = 50 pontos
	Menor que 90% = 0 ponto

Indicador de tempo de solução	
Item	Descrição
Finalidade	Garantir que o reparo, manutenção ou assistência técnica para o correto funcionamento da solução instalada seja realizada dentro da periodicidade especificada
Meta	Retorno ao funcionamento pleno da solução contratada conforme grau de severidade:



- Severidade alta: serviço totalmente interrompido em um ou mais equipamentos	Severidade alta: - Tempo máximo: 6 horas
- Severidade moderada: serviço parcialmente interrompido ou com qualidade degradada em um ou mais equipamentos.	Severidade moderada: - Tempo máximo: 12 horas
Instrumento de medição	Contagem de tempo entre realização do chamado e finalização do atendimento, dada pela fiscalização do contrato. As horas que excederem o máximo estabelecido serão somadas ao longo do mês.
Forma de acompanhamento	Pela fiscalização do contrato, por meio de registro das ocorrências de chamados mantido pela CONTRATANTE ou fornecido pela CONTRATADA
Periodicidade de cálculo	Mensal
Método de cálculo	Média de tempo para solução de chamados:
Início da vigência	A partir do início da prestação do serviço ou prazo definido pela CONTRATANTE.
Faixa de ajuste de pagamento	Até 6 horas = 15 pontos
	Entre 6h e 1min e 8h = 13 pontos
	Entre 8h e 1 min e 10 h = 11 pontos
	Entre 10 h e 1 min e 12 h = 9 pontos
	Acima de 12h e 1 min = 0 ponto

Indicador de manutenção preventiva	
Item	Descrição
Finalidade	Garantir que a manutenção preventiva seja realizada dentro das periodicidades especificadas em Projeto Executivo.
Meta	Nenhum atraso no mês
Instrumento de medição	Constatação formal de dias de atraso
Forma de acompanhamento	Pela fiscalização do contrato, por meio de registro das ocorrências encaminhadas à CONTRATADA.
Periodicidade de cálculo	Mensal
Método de cálculo	Verificação da quantidade de dias de atraso registradas no mês de referência.



Início da vigência	A partir do início da prestação do serviço ou prazo definido pela CONTRATANTE após início da prestação do serviço.
Faixa de ajuste de pagamento	Sem ocorrências = 5 pontos
	1 a 2 dias = 4 pontos
	3 a 4 dias = 3 pontos
	5 ou mais dias = 0 ponto

11.5.4 Considerando a pontuação total a soma dos indicadores (IDS+ITS+IMP), os pagamentos devidos, relativos a cada mês de referência, devem ser ajustados pela pontuação total do serviço, conforme tabela abaixo:

Faixa de pontuação	Pagamento devido	Fator de ajuste de nível de serviço
De 90 a 100 pontos	100% do valor previsto	1,00
De 80 a 89 pontos	97% do valor previsto	0,97
De 70 a 79 pontos	95% do valor previsto	0,95
De 60 a 49 pontos	93% do valor previsto	0,93
De 50 a 59 pontos	90% do valor previsto	0,90
Abaixo de 50 pontos	90% do valor previsto	0,90 + multa contratual

11.6 A CONTRATADA poderá apresentar justificativas para a prestação dos serviços abaixo do nível de satisfação ou indisponibilidades, que poderá ser aceita pela CONTRATANTE, desde que comprovada a excepcionalidade da ocorrência, resultante exclusivamente de fatores imprevisíveis e alheios ao controle da CONTRATADA;

11.7 A critério da CONTRATANTE, garantindo ampla defesa, a CONTRATADA poderá ser penalizada com a rescisão contratual nas seguintes condições:

11.7.1 Em caso de reincidência de descontos de 10% (dez por cento) por 3 (três) vezes ou mais durante a vigência do contrato;

11.7.2 A faixa de pontuação total for inferior a 40 (quarenta) pontos por 3 (três) meses consecutivos;

11.7.3 Somatório de horas de indisponibilidade do objeto contratado no mês maior que 48 horas.

11.8 Ao final do mês de apuração, a equipe responsável pela fiscalização do contrato deve encaminhar o registro das ocorrências gerado no período para o Gestor do contrato;

11.8.1 Em caso de aceite de justificativa apresentada pela CONTRATADA para ocorrências, deverá a equipe de fiscalização apresentar por escrito ao Gestor do contrato conjuntamente ao registro de ocorrências;



11.8.2 Caso seja negado o aceite de justificativa apresentada pela CONTRATADA para ocorrências deverá a equipe de fiscalização apresentar a motivação para a decisão por escrito ao Gestor do contrato conjuntamente ao registro de ocorrências.

11.9 Cabe ao Gestor do contrato:

11.9.1 De posse dos formulários preenchidos, emitir o resultado da avaliação do nível de serviço dando ciência à CONTRATADA;

11.9.2 No caso da necessidade da aplicação de descontos, apurar o percentual de desconto a ser aplicado na fatura de período subsequente ao apurado, tomando como base o resultado da avaliação do nível de serviços, notificando a CONTRATADA previamente ao fechamento da medição e emissão da fatura do próximo período;

11.9.3 Aplicar, quando cabível, sanção à CONTRATADA e encaminhar para o conhecimento da autoridade competente;

11.9.4 Quando atribuída pontuação igual a 0 (zero) em algum dos indicadores, o Gestor deverá notificar à CONTRATADA, visando proporcionar ciência quanto ao desempenho dos trabalhos e providenciar o tratamento das falhas para a execução do contrato no período subsequente;

11.10 Caso a CONTRATADA queira solicitar prazo visando o atendimento ou correção de determinada falha de execução contratual, esta solicitação deverá ser formalizada ao Gestor do contrato, com o objetivo de análise do pedido pelo mesmo;

11.10.1 A solicitação do prazo supracitado poderá ser deferida ou indeferida conforme deliberação e justificativa do Gestor do contrato.



## **ANEXO I - Especificações técnicas dos componentes da solução**

### **1. Especificações mínimas para sistema de videomonitoramento (CFTV)**

#### **1.1 Sistema de Videomonitoramento (CFTV) - Hardware e Software (VMS)**

##### **A. HARDWARE**

- a) Suportar funcionamento ininterrupto 24x7;
- b) Deve ser compatível com o VMS ofertado;
- c) Devem estar contempladas todas as licenças necessárias ao funcionamento de sistema, assim como licenças perpétuas com direito de uso permanente, que sejam necessárias à execução das tarefas e aplicativos descritos e/ou que sejam disponibilizados pela solução ofertada;
- d) Deverá possuir gabinete tipo rack padrão 19" (dezenove polegadas), entregue com trilhos e quaisquer outros componentes necessários para instalação em rack;
- e) O equipamento deverá ser novo, estar em linha de produção no momento da licitação, sendo possível consultar o site do fabricante para verificação das especificações técnicas;
- f) Deve possuir pelo menos 8 (oito) canais de memória;
- g) Os canais de memória deverão ser preenchidos obedecendo as regras de máxima desempenho para o sistema conforme recomendação do fabricante do servidor
- h) Processador Intel Xeon Silver 4208 ou superior;
- i) Memória RAM de 16 Gigabytes ou superior;
- j) Deve possuir ao menos 2 (dois) discos rígidos padrão SSD de 200 Gigabytes cada ou superiores;
- k) Deve possuir discos e baias adequados para permitir a funcionalidade de troca a quente dos discos;
- l) Deverá possibilitar a configuração dos discos via Controladora para uso de RAID tipo 0, 1, 5, 10;

##### **B. SOFTWARE (VMS)**

- a) Deve possuir compatibilidade intrínseca, com base em biblioteca própria, para integração com mais de 10.000 dispositivos IP, entre câmeras, módulos de entrada e saída, codificadores de vídeo, entre outros, atendendo a diversos fabricantes;
- b) Deve ser do tipo multiusuário, permitindo a criação de perfis de usuários nativos do sistema sem restrições quantitativas e integração com Windows Active Directory (AD) de maneira nativa;
- c) Deve permitir a utilização de mapas estáticos;
- d) Deve suportar compatibilidade com o protocolo ONVIF nos perfis G, M, S e T sendo sua compatibilidade comprovada através da comunidade regulamentadora no website <https://onvif.org>;



- e) O sistema deve possuir plataforma aberta através de API/SDK, devendo suportar integração com hardware, analíticos ou aplicativos de terceiros, disponibilizando estas informações publicamente em website do fabricante;
- f) Deve suportar e realizar de maneira independente pelo servidor, pela câmera ou simultaneamente, a opção de detecção de movimento, independentemente do modelo de câmera, desde que o modelo de câmera esteja homologado pela solução de Gerenciamento de Imagens ofertada;
- g) Deve possuir configuração manual ou automática para detecção de movimento a ser aplicado na cena;
- h) Deve permitir, no modo ao vivo e playback, a utilização de diversas streaming de maneira adaptativa, isto é, deve permitir que a visualização das câmeras nos layouts tenha ajuste de qualidade de imagem automática, onde a resolução da câmera é alterada quando o operador passa da visualização em layout para a visualização em tela cheia, trazendo maior economia de banda e melhor qualidade de imagem quando necessário;
- i) Deve permitir que imagens de câmeras possam ser visualizadas através de um sistema central, bem como também as imagens gravadas que estejam utilizando o mesmo sistema de vídeo monitoramento, permitindo que sejam realizadas as gravações e visualizações de maneira centralizada, localmente ou até mesmo uma combinação destas duas opções;
- j) Não deve haver limitação para operação com diversos servidores de gravação, e/ou softwares clientes, etc;
- k) Deve permitir a utilização de todos os analíticos, eventos e todos os metadados de fabricantes das câmeras homologados e integrados a plataforma do VMS, sem custo adicional de licença;
- l) O Sistema deve estar de acordo com as normas de padrão internacional de certificados de módulos criptografados FIPS 140-2 (Federal Information Processing Standard Publication 140-2);
- m) O Sistema deve manter logs de registro de diversas ações tomadas por usuários, registro de eventos, alarmes, saúde do sistema, etc;
- n) Deve permitir não só o recebimento de alarmes com suas devidas descrições de ocorrência na aplicação, mas como também, permitir comentar e escalar para outros operadores se necessário;
- o) Deve permitir ao operador a criação manual de Bookmarks, com inserção de comentários nas imagens. Estes registros devem estar disponíveis posteriormente através de um processo de busca simples e intuitivo, mediante a aplicação de filtros de pesquisa;
- p) O software de operação de monitoramento deve permitir visualização ao vivo com suporte para visualizar mais de 80 câmeras em reprodução;
- q) Permitir busca inteligente por alarmes, eventos, identificação de pessoas e localização de câmera;
- r) Permitir a visualização de metadados nas imagens sendo exibidas para as câmeras que possibilitem a entrega destas informações visualmente ao cliente de monitoramento.





- s) Deve permitir interface configurável, não somente para permissões de usuários, mas também para integrações desenvolvidas por terceiros, as quais podem se tornar parte integral e funcional do cliente de monitoramento;
- t) Deve possuir aplicação Web (Cliente Web), com visualização de múltiplas imagens simultâneas de diversos servidores de gravação, visualização de imagens ao vivo, operação em modo tela cheia e suporte a áudio bidirecional;
- u) Deve ser possível realizar a ativação de eventos através da aplicação web, bem como também a ativação de saídas;
- v) Deve possuir aplicação mobile (Cliente Mobile), sem necessidade de licença adicional para dispositivos baseados em Google Android, Apple iOS;
- w) A aplicação Mobile deve permitir a visualização de imagens ao vivo, além de múltiplas imagens simultâneas dos diversos servidores de gravação, bem como também, possuir visualização otimizada para os layouts exibidos em modo retrato ou horizontal, suporte a áudio bidirecional, ativação de eventos e saídas, compartilhamento de bookmarks entre os usuários e utilização de biometria para acesso à aplicação mobile;
- x) Deve permitir a gestão de incidentes, em que a cada incidente seja possível associar diferentes trechos de vídeo, seja ao vivo ou gravados. Estas informações podem ser inseridas mediante o uso de campos personalizáveis;
- y) Deve permitir a integração com diversos fornecedores de sistemas de controle de acesso e intrusão.

## 1.2 Câmera Tipo 1 - Área comum

- a) Câmera tipo dome varifocal com infravermelho;
- b) Deve possuir sensor de imagem em estado sólido de 1/2,8", ou maior, com varredura progressiva;
- c) Possuir lente varifocal com range entre 2.8~12mm do tipo motorizada;
- d) Possuir LEDs infravermelhos com capacidade de alcance de 30m de distância;
- e) Possui filtro de corte de infravermelho removível automaticamente;
- f) Possuir resolução de 2MP (1920x1080) ou superior;
- g) Possuir sensibilidade mínima igual ou inferior, no modo colorido a 0.015 lux;
- h) Ser capaz de fornecer fluxos H.265 e H.264 de forma independente e simultânea;
- i) Permitir a transmissão em resolução máxima em até 30 frames por segundo, no fluxo principal;
- j) Suportar no mínimo 3 fluxos de vídeo configuráveis de forma independente;
- k) Permitir no mínimo 20 conexões simultâneas;
- l) Possibilitar compensação automática para tomada de imagem contra luz de fundo (BLC);
- m) Possuir Wide Dynamic Range de 120dB;
- n) Possuir ângulo de visualização horizontal de no mínimo 109°~30°;
- o) Possuir porta para conexão em rede TCP/IP com conector RJ-45 10/100BASE-T;
- p) Possuir os protocolos: HTTP, HTTPS, TCP, RTSP, RTP, SMTP, FTP, DHCP, DNS, DDNS, PPPOE, IPv6, QoS, UPnP, NTP, 802.1x, ICMP, IGMP, SNMP;
- q) Suportar qualidade de serviço (QoS) para ser capaz de priorizar o tráfego;



- r) Permitir alimentação PoE conforme padrão IEEE 802.3af/at sem uso de equipamentos adicionais;
- s) Incorporar Balanço de Branco Automático e Manual;
- t) Incorporar ajuste do controle de ganho, de forma automática;
- u) Suportar redução de ruído do tipo 3D;
- v) Possuir recurso de compensação de luz alta (HLC);
- w) Ser fornecida com capacidade embarcada para a configuração de máscaras de privacidade na própria câmera;
- x) Possuir capacidade de armazenamento local através de SD/MicroSD card, com capacidade de no mínimo 128Gb;
- y) Possuir capacidade de análise de vídeo embarcado de: cruzamento de linha, área de intrusão, remoção de objeto, objeto abandonado;
- z) A câmera deve possuir tecnologia capaz de detectar faces, extraíndo no mínimo os seguintes atributos: idade, gênero, expressão, uso de máscara, uso de óculos e barba;
- aa) Ser fornecida com capacidade inteligente embarcada, de diferenciar pessoas e veículos;
- bb) Deve ser capaz de fazer a contagem de pessoas por cruzamento de linha e em área.
- cc) Ser fornecida com capacidade embarcada para detectar movimentos;
- dd) Possuir arquitetura aberta (API) para integração com outros sistemas;
- ee) Possuir protocolo de Integração ONVIF;
- ff) Possuir, no mínimo, 1 entrada e 1 saída de alarme;
- gg) Possuir, no mínimo, 1 entrada e 1 saída de áudio;
- hh) Ser fornecida com caixa de proteção com grau de proteção IP67;
- ii) Possuir resistência a impacto com grau de proteção IK10;
- jj) Possuir formato tipo dome;
- kk) Seus acessórios devem ser do mesmo fabricante da câmera ou homologados pela mesma garantindo a qualidade da solução;
- ll) Possibilitar operação no range de temperaturas de -30°C e 55°C;
- mm) O dispositivo deve possuir segurança criptografada ponto a ponto, comprovada pelo fabricante;
- nn) O dispositivo deve possuir tecnologia de checagem pacote de dados, disponibilizando filtros como: fonte do IP, endereço de IP do alvo, tipo do protocolo, porta do alvo e da fonte;
- oo) O fabricante deve garantir que o equipamento não é vulnerável à ataques de rede DDoS e Phishing;
- pp) O dispositivo deve ser capaz de garantir a segurança na atualização de firmwares, identificando pacotes diferentes do fabricante, permitindo somente a utilização de versões de firmware lançadas pelo mesmo.

### 1.3 Câmeras Tipo 2 - Corredores

- a) Deve possuir o formato dome;
- b) Deve possuir no mínimo 2 Megapixel (1920x1080) de resolução a 30 quadros por segundo;
- c) Deve possuir no mínimo sensor de imagem de 1/2.8" Progressive Scan CMOS;



- d) Deve suportar iluminação mínima de 0.02 Lux;
- e) Deve possuir recurso WDR (Wide Dinamic Range) ou DWDR (Digital Wide Dinamic Range);
- f) Deve dispor de controle de ganho automático e manual, além de compensação para luz de fundo e luz alta;
- g) Deve possuir balanço de branco com ajuste automático e personalizável;
- h) Deve possuir campo de visão horizontal maior que 100°;
- i) Deve possuir recurso infravermelho com alcance mínimo de 30 m;
- j) Dispor de função dia e noite, acionados por filtro de corte de infravermelho automático;
- k) Deve possuir ao menos 2 (dois) fluxos diferentes configuráveis de vídeo;
- l) Deve possuir capacidade de fornecer fluxos H.265 e H.264, além de possuir um padrão de compressão de vídeo superiores e complementares a estes (HDSM, Zipstream, H.264+, H.265+ ou similares), com alta relação de compressão;
- m) Deve garantir interoperabilidade por meio dos protocolos ONVIF. Adicionalmente, o fabricante deve disponibilizar API, SDK ou plataforma aberta proprietária;
- n) Deve possuir os protocolos de comunicação e segurança TCP/IP, IPv4, IPv6, UDP, FTP, NTP, SMTP, HTTP, HTTPS, DHCP, DNS, QoS, RTP, RTSP, Multicast, 802.1x;
- o) Deve permitir configurar a taxa de bits de vídeo (bitrate);
- p) Deve possuir no mínimo 4 (quatro) áreas de região de interesse, 4 (quatro) áreas para detecção de movimento e 4 (quatro) máscaras de privacidade;
- q) Deve suportar pelo menos 6 (seis) conexões unicast simultâneas (usuários conectados);
- r) Deve possuir uma interface Ethernet RJ45 10/100 Mbps;
- s) Deve suportar alimentação via PoE 802.3af/at e fonte (DC ou AC);
- t) Deve possuir no mínimo o grau de proteção anti vandalismo IK10;
- u) Deve possuir no mínimo o grau de proteção contra água e poeira IP67;
- v) Deve suportar no mínimo a seguinte faixa de temperatura de operação -15°C a 55°C;
- w) Deve possuir segurança criptografada ponto a ponto, comprovada pelo fabricante. Esta funcionalidade pode ser ofertada utilizando appliance/servidor externo com solução de prevenção de intrusão (IPS). O appliance/servidor, bem como licenciamento e garantia deve ser fornecido pela contratada;
- x) Deve possuir tecnologia de checagem pacote de dados, disponibilizando filtros como: fonte do IP, endereço de IP do alvo, tipo do protocolo, porta do alvo e da fonte. Esta funcionalidade pode ser ofertada utilizando appliance/servidor externo com solução de controle de acesso à rede (NAC). O appliance/servidor, bem como licenciamento e garantia deve ser fornecido pela contratada;
- y) O fabricante deve garantir que o equipamento não é vulnerável à ataques de rede DDoS (ataque de negação de serviço distribuída) e Phishing (ataques de mensagens suspeitas). Esta funcionalidade pode ser ofertada utilizando appliance/servidor externo com solução de prevenção de intrusão (IPS). O appliance/servidor, bem como licenciamento e garantia deve ser fornecido pela contratada;
- z) Deve ser capaz de garantir a segurança na atualização de firmwares, identificando pacotes diferentes do fabricante, permitindo somente a utilização de versões de firmware lançadas pelo mesmo;
- aa) Deve possuir certificação CE ou UL ou FCC;



- bb) Deverá ser fornecida com eventuais acessórios para perfeita fixação, de acordo com as características de cada ambiente e superfície a ser instalada;
- cc) É obrigatório incluir na proposta técnica a marca e o modelo específico da câmera ofertada (e demais componentes ofertados) para atendimento das especificações contidas nesse documento, juntamente ao(s) catálogo(s) e/ou manual(ais) que comprovem as características requisitadas;
- dd) Possuir capacidade de armazenamento local através de SD/MicroSD card, com capacidade de no mínimo 128GB.

#### **1.4 Câmeras Tipo 3 - Áreas externas/internas amplas**

- a) Câmera em formato Bullet de 2MP, varifocal, para uso interno e externo;
- b) Deve possuir no mínimo 2 Megapixel de resolução a 30 quadros por segundo;
- c) Deve possuir no mínimo sensor de imagem de 1/2.8" ProgressiveScan CMOS;
- d) Deve suportar iluminação mínima de 0.015 Lux em cores;
- e) Deve possuir recurso WDR (Wide Dinamic Range) 120 dB;
- f) Dispor de controle de ganho automático, além de compensação para luz de fundo e luz alta;
- g) Possuir balanço de branco com ajuste automático e personalizável;
- h) Deve possuir velocidade do obturador de no mínimo 1/3s a 1/12.000s;
- i) Deve possuir lente varifocal motorizada mínimo de 2.8-12 mm;
- j) Deve permitir o estabelecimento dos seguintes ângulos de visão: 108°~30° na horizontal e 55°~17° na vertical;
- k) Deve possuir compressão de vídeo padrão H.264, MJPEG e, ao menos, um padrão de compressão de vídeo superior ao mesmo (H.265, H.264B, Zipstream, H.264+, H.264H, H.265+ ou similares), com alta relação de compressão;
- l) Deve possuir no mínimo três fluxos diferentes configuráveis de vídeo;
- m) Deve dispor ao menos uma entrada e uma saída de alarme;
- n) Deve possuir no mínimo o grau de proteção contra água e poeira IP67;
- o) Deve possuir recurso infravermelho com alcance mínimo de 50 m;
- p) Dispor de função dia e noite, acionados por filtro de corte de infravermelho automático;
- q) Deve garantir interoperabilidade por meio dos protocolos ONVIF (perfil S, G e T). Adicionalmente, o fabricante deve disponibilizar API, SDK ou plataforma aberta proprietária;
- r) Deve possuir os protocolos de comunicação e segurança TCP/IP, IPv4, IPv6, UDP, FTP, ICMP, NTP, SMTP, HTTP, HTTPS, ARP, DHCP, DNS, DDNS, QoS, RTP, RTSP, IGMP, RTCP, PPPoE, UPnP, 802.1X;
- s) Deve permitir configurar a taxa de bits de vídeo (bitrate);
- t) Deve possuir no mínimo as seguintes funcionalidades: Detecção de intrusão, Detecção de cruzamento de linha, além de detecção de movimento mediante definição de ao menos 4 áreas;
- u) Deve ser capaz de identificar e diferenciar automaticamente, através de algoritmo de Inteligência Artificial, pessoas e veículos dentro da imagem;
- v) Deve possuir uma interface Ethernet RJ45 10/100 Mbps;



- w) Deve ser PoE 802.3af dissipando potência máxima  $\leq 13\text{w}$ ;
- x) Deve suportar no mínimo a seguinte faixa de temperatura de operação  $-25^{\circ}\text{C}$  a  $60^{\circ}\text{C}$ ;
- y) Deve possuir invólucro metálico, proporcionando maior vida útil e resistência a intempéries com certificação IP67;
- z) Possuir capacidade de armazenamento local através de SD/MicroSD/SDHC/SDXC, com capacidade de no mínimo 128GB;
- aa) Deve possuir certificações FCC, CE e UL;
- bb) Deverá ser fornecida com eventuais acessórios para perfeita fixação, de acordo com as características de cada ambiente e superfície a ser instalada.

### 1.5 Câmeras Tipo 4 - “Multi-sensor”

- a) Para o modo panorâmico:
- b) Possuir sensor de imagem em estado sólido de 1/8" ou maior, com varredura progressiva;
- c) Possuir comprimento focal de 2.8mm para as lentes fixas;
- d) Possuir o mínimo 8 (oito) lentes com resolução mínima de  $1920 \times 1080$  pixels em cada uma das oito lentes;
- e) Deve possuir sensibilidade mínima igual ou inferior a 0.0005 lux no modo colorido com o F1.0 e 0.0002 lux e no modo PB;
- f) Possuir sistema de visualização em modo panorâmico possibilitando uma visualização única de todas as lentes fixas para um monitoramento mais assertivo e centralizado dos vídeos;
- g) Ser capaz de fornecer fluxos H.264, H.265 e MJPEG de forma independente e simultânea;
- h) Deve possuir compressão de vídeo padrão H.264, MJPEG e, ao menos, um padrão compressão de vídeo superior ao mesmo (H.265, H.264B, Zipstream, H.264+, H.264H, H.265+ ou similares), com alta relação de compressão;
- i) Permitir a transmissão em resolução  $1920 \times 1080$  à taxa de frames de 30 frames por segundo, no fluxo principal de vídeo;
- j) Permitir no mínimo 3 fluxos de vídeo configuráveis de forma independente;
- k) Possibilitar compensação automática para tomada de imagem contra luz de fundo (BLC);
- l) Suportar recurso para redução de ruído (3D DNR);
- m) Possuir função de Wide Dynamic Range;
- n) Possuir tempo do obturador entre 1/3s a 1/100.000 s;
- o) Possuir porta para conexão em rede TCP/IP com conector RJ-45 10/100/1000 BASE-T ou TX;
- p) Para o modo PTZ:
- q) Possuir sensor de imagem em estado sólido de 1/8" ou maior, com varredura progressiva;
- r) Possuir comprimento focal de 6mm (ou menos) até 210mm (ou mais) no modo PTZ;
- s) Possuir zoom óptico de no mínimo 38x;
- t) Possuir resolução mínima de 4 MP;



- u) Possuir sensibilidade mínima igual ou inferior a 0.001 lux no modo colorido com o F1.4 (ou superior: F1.2, F1.0, etc) e 0 lux e no modo PB (com IR ligado);
- v) Possuir iluminador IR (infravermelho) incorporado à câmera PTZ;
- w) Ser capaz de fornecer fluxos H.264, H.265 e MJPEG de forma independente e simultânea;
- x) Deve possuir compressão de vídeo padrão H.264, MJPEG e, ao menos, um padrão compressão de vídeo superior ao mesmo (H.265, H.264B, Zipstream, H.264+, H.264H, H.265+ ou similares), com alta relação de compressão;
- y) Permitir a transmissão em resolução  $2560 \times 1440$  à taxa de frames de 30 frames por segundo, no fluxo principal de vídeo;
- z) Permitir no mínimo 3 fluxos de vídeo configuráveis de forma independente;
- aa) Possibilitar compensação automática para tomada de imagem contra luz de fundo (BLC);
- bb) Suportar recurso para redução de ruído (3D DNR);
- cc) Possuir função de Wide Dynamic Range, no mínimo de 120 dB;
- dd) Possuir tempo do obturador entre 1/3s a 1/100.000 s;
- ee) Possuir porta para conexão em rede TCP/IP com conector RJ-45 10/100/1000 BASE-T ou TX;
- ff) Demais funcionalidades:
- gg) Deve possuir análise de vídeo embarcado referente cruzamento de linha e intrusão;
- hh) Possuir os protocolos: IPv4, IPv6, HTTP, TCP, UDP, RTP, RTSP, SMTP, FTP, DHCP, DNS, DDNS, QoS, UPnP, NTP, Multicast, ICMP, IGMP e PPPoE;
- ii) Permitir alimentação 24 ou 36vdc, com consumo máximo  $< 100$  w;
- jj) Incorporar Balanço de Branco;
- kk) Deve garantir interoperabilidade por meio dos protocolos ONVIF (perfil S e G). Adicionalmente, o fabricante deve disponibilizar API, SDK ou plataforma aberta proprietária;
- ll) Deve possuir arquitetura aberta para integração com outros sistemas;
- mm) Possuir ao menos uma interface de entrada e uma interface de saída para áudio;
- nn) Possuir ao menos uma interface de entrada e uma interface de saída para alarmes;
- oo) Possuir grau de proteção de acordo com padrão IP66;
- pp) Possibilitar operação no range de temperatura de  $-10^{\circ}\text{C}$  a  $+60^{\circ}\text{C}$ ;
- qq) Possuir as certificações CE ou FCC ou UL;
- rr) A câmera deve possuir garantia do fabricante de pelo menos 3 anos comprovado por declaração do fabricante incluindo informações acerca do centro de assistência técnica autorizado em território nacional. Não será aceita garantia de terceiro (distribuidor, importador ou instalador);
- ss) O dispositivo deve possuir segurança criptografada ponto a ponto, comprovada pelo fabricante;
- tt) O dispositivo deve possuir tecnologia de checagem pacote de dados, disponibilizando filtros como: fonte do IP, endereço de IP do alvo, tipo do protocolo, porta do alvo e da fonte;
- uu) O fabricante deve garantir que o equipamento não é vulnerável à ataques de rede DDoS e Phishing;





- vv) O dispositivo deve ser capaz de garantir a segurança na atualização de firmwares, identificando pacotes diferentes do fabricante, permitindo somente a utilização de versões de firmware lançadas pelo mesmo;
- ww) Possuir capacidade de armazenamento local através de SD/MicroSD card, com capacidade de no mínimo 128GB.

### 1.6 Câmera Tipo 5 - “PTZ”

- a) Deve ser do tipo speed dome com movimentação PTZ;
- b) Deve possuir sensor de imagem em estado sólido (CMOS) de 1/2.8" ou maior, com varredura progressiva;
- c) Possuir resolução de 4 MP (2560 × 1440);
- d) Deve possuir lente com zoom óptico de pelo menos 32x;
- e) A distância focal da lente deve estar entre, o valor mínimo de 3.5 mm a 5.9mm e o valor máximo de 140mm a 155mm, com suporte a foco automático e manual;
- f) Deve possuir zoom digital mínimo de 16x;
- g) O ângulo horizontal mínimo deve ser de 50° (ou mais) a 4° (ou menos);
- h) Deve possuir PAN na faixa de 360° e Tilt entre -15° e +90°;
- i) Deve possuir sensibilidade mínima igual ou inferior, no modo colorido a 0.02 lux, no modo PB a 0.002 lux e 0 lux com iluminador ligado;
- j) Deve possuir iluminador IR ou similar que atinja a distância mínima de 150m;
- k) Deve dispor de, no mínimo, 300 posições programáveis (presets);
- l) Deve permitir ronda eletrônica e varreduras múltiplas;
- m) Deve permitir operação em preset, com velocidade de PAN de no mínimo 100°/s e de TILT de no mínimo 70°/s;
- n) Deve ser capaz de fornecer fluxos MJPEG, H.264 e H265;
- o) Deve permitir a transmissão de no mínimo 3 (três) fluxos de vídeo configuráveis de forma independente no codec de compressão mais atual solicitado;
- p) Deve permitir operação na resolução máxima a 30fps em seu stream principal;
- q) Deve permitir a transmissão de vídeo por Multicast e Unicast;
- r) Deve permitir no mínimo 20 usuários;
- s) Função de Estabilização Eletrônica da Imagem (EIS) ou similar;
- t) Deve possibilitar compensação automática para tomada de imagem contraluz de fundo (BLC);
- u) Deve possuir Wide Dynamic Range (WDR), de no mínimo 120dB;
- v) Deve possuir tempo do obturador entre 1/1-1/12.000s, ou superior;
- w) Deve possuir porta para conexão em rede TCP/IP com conector RJ45 100BASE-T ou TX;
- x) Deve possuir os protocolos: RTP, RTSP, UDP, TCP, IPv4, IPv6, DHCP, HTTP, NTP, UPNP, SNMP, QoS, SMTP, DNS, DDNS e FTP;
- y) Deve possuir o protocolo de segurança HTTPS e seguir o padrão IEEE 802.1x de autenticação em rede;
- z) Deve permitir alimentação PoE+ ou através de fonte de alimentação de 24V ou 36V;
- aa) Deve incorporar Balanço de Branco Automático e Manual;





- bb) Deve possuir zonas de mascaramento de imagem programáveis embarcada na câmera de no mínimo 24 posições;
- cc) Deverá disponibilizar espaço de armazenamento mínimo de 256 GB através de cartão de memória;
- dd) Deve possuir capacidade de análise de vídeo embarcada para:
- ee) Detecção de movimento;
- ff) Detecção de sabotagem;
- gg) Detecção de intrusão em área;
- hh) Cruzamento de linha virtual;
- ii) Detecção de faces;
- jj) Deve possuir função de rastreamento automático (auto-tracking);
- kk) Deve possuir arquitetura aberta para integração com outros sistemas por meio de API ou SDK ou CGI;
- ll) Deve estar em conformidade com o Padrão ONVIF, profiles S e G;
- mm) Deve possuir 1 (uma) entrada e (uma) 1 saída de áudio, no mínimo;
- nn) Deve possuir, no mínimo, 2 (duas) entradas e 1 (uma) saída de alarme;
- oo) Deve possuir grau de proteção IP66, ou tecnologia superior que garanta a proteção à umidade e IK10 contra antivandalismo;
- pp) Possuir minimamente as certificações CE (ou UL);
- qq) Deve possibilitar operação no range de temperatura de no mínimo -30° a 55° em ambiente de 15 a 90% de umidade;
- rr) Deve acompanhar suportes e/ou acessórios para fixação em poste e parede. O suporte deverá possuir acomodação para que os cabos não fiquem expostos;
- ss) Todos os equipamentos deste tópico devem constar no portfólio de produtos do(s) fabricante(s) e com previsão de continuidade de fabricação de no mínimo um ano. Caso seja descontinuado no período mencionado deverá ser substituído. Não serão aceitos produtos descontinuados.
- tt) Deve possuir garantia do fabricante de pelo menos 3 (três) anos comprovada por carta do fabricante e ou informação constante no site do fabricante;
- uu) Deverá ser fornecida com sua respectiva fonte de alimentação ou injetor PoE compatível com o equipamento;
- vv) Deve possuir assistência técnica autorizada no Brasil;
- ww) O dispositivo deve possuir segurança criptografada ponto a ponto, comprovada pelo fabricante;
- xx) O dispositivo deve possuir tecnologia de checagem pacote de dados, disponibilizando filtros como: fonte do IP, endereço de IP do alvo, tipo do protocolo, porta do alvo e da fonte;
- yy) O fabricante deve garantir que o equipamento não é vulnerável à ataques de rede DDoS (ataque de negação de serviço distribuída) e Phishing (ataques de mensagens suspeitas);
- zz) O dispositivo deve ser capaz de garantir a segurança na atualização de firmwares, identificando pacotes diferentes do fabricante, permitindo somente a utilização de versões de firmware lançadas pelo mesmo.



## 2. Especificações mínimas para sistema de controle de acesso (SCA)

- a) O sistema de controle de acesso tem por função identificar, permitir ou negar o acesso de pessoas, utilizando critérios pré-configurados, registrando todos os eventos relativos a esta atividade. Esta função visa prevenir os riscos que possam afetar as pessoas e as instalações inseridas no sistema;
- b) O sistema previsto utilizará a tecnologia de proximidade, QR CODE, leitor facial, catracas de acesso e controle de portas;
- c) Para os dispositivos de acesso relacionados nos itens 2.15, 2.17 e 2.18 do Anexo I, devem ser ofertadas controladoras com capacidade de gerenciar um ou vários dispositivos de forma simultânea;
- d) A controladora deve integrar os dispositivos via protocolos Wiegand e/ou OSDP e/ou TCP-IP;
- e) As controladoras podem ser dedicadas ou integradas ao dispositivo de acesso constituindo juntamente com leitor de acesso um único produto;
- f) O SCA deve prover um gerenciamento da informação e deve operar numa configuração Cliente-Servidor em computadores rodando com a plataforma Windows;
- g) A arquitetura cliente-servidor deverá ser capaz de suportar no mínimo 10 clientes até 256 clientes simultâneos, múltiplos tipos de controladoras até 20.000 dispositivos de entrada, incluindo câmeras e múltiplos tipos de leitoras de cartões;
- h) Deve operar de forma independente do banco de dados e deve suportar ao menos o Oracle standard ou SQL Server, para proteção de dados, redundância e gerenciamento;
- i) Deve ser flexível de modo a permitir que a aplicação e o banco de dados rodem no mesmo servidor e também deve permitir que a aplicação opere em servidor separado do servidor de banco de dados, ficando a critério da contratante a definição de qual modo mais conveniente será adotado;
- j) Deverá ter capacidade para até 5.000 leitoras por servidor e escalabilidade para até 40 servidores de aplicação;
- k) Deverá suportar protocolo Wiegand e/ou OSDP entre leitores de Cartão/Biometria e os controladores de acesso;
- l) A comunicação entre os controladores de acesso, servidores e gerenciadores de rede devem ser através de protocolo TCP/IP;
- m) Deverá possuir Web Client, ou software cliente que poderá ser instalado em uma estação de trabalho, permitindo gerenciar, monitorar as atividades do sistema, cadastrar e modificar dados dos portadores dos cartões – cardholders, além de permitir exibições dinâmicas;
- n) Deverá ter uma ferramenta de geração de crachás para criar e gerenciar os crachás usando uma interface gráfica e capacidade de consultas para facilitar o gerenciamento de um número grande de crachás;
- o) A solução de gerenciamento de crachás, deve ser baseada em .NET com um editor de crachás e uma interface gráfica para desenho do cartão de acesso.

### 2.1 Requisitos de Arquitetura



- a) A arquitetura padrão de rede de dados deve ser baseada em topologia TCP/IP entre os elementos de controle e comando;
- b) A proteção de dados será considerada como prioridade máxima, para tanto, o fabricante deverá atender a Lei Geral de Proteção de Dados, promulgada pela Lei nº 13.709, de 14/08/2018, respondendo as determinações da ANPD (Autoridade Nacional de Proteção de Dados). O fabricante deverá emitir declaração de que está em plena aderência (compliance) com as diretrizes do acordo de proteção de dados EU GDPR - General Data Protection Regulation ([https://ec.europa.eu/commission/priorities/justice-and-fundamental-rights/dataprotection/2018-reform-eu-data-protection-rules\\_en](https://ec.europa.eu/commission/priorities/justice-and-fundamental-rights/dataprotection/2018-reform-eu-data-protection-rules_en));
- c) Devido a criticidade do ambiente de aplicação e devido aos fluxos de dados considerados sigilosos e, alinhado ao disposto no art. 13 da Lei nº 7.170/2010 e seus incisos, é exigido que o fabricante não poderá ser de propriedade ou controlado por governo estrangeiro.
  - 1. Entende-se por propriedade a posse legal da empresa;
  - 2. Entende-se por controle o poder de controle do negócio;
  - 3. Caso o fabricante tenha participação acionária de governo estrangeiro, esta deverá ser minoritária e o fabricante deverá emitir uma declaração notificando esta condição, bem como se compromete a não fornecer qualquer dado transmitido pela rede de dados.
- d) O Sistema de Controle de Acesso deverá utilizar protocolo Wiegand e/ou OSDP entre os leitores de Cartão/Biometria/Reconhecimento Facial e os Controladores de Acesso, protocolo RS-485 entre os módulos/placas de expansão de entrada e saída;
- e) Todos os Controladores de Acesso devem operar de forma independente em caso de perda de conexão e se comunicar diretamente aos servidores sem necessidade de equipamentos intermediários através de protocolo de comunicação TCP/IP;
- f) O sistema poderá conter elementos adicionais para interoperabilidade como o servidor;
- g) Os dispositivos de acesso podem ser dedicados a uma única função, ou recurso, ou possuir capacidade de múltiplos recursos ou funções acopladas em um único dispositivo.

## 2.2 Requisitos do Cliente WEB

- a) Deve ser compatível com Microsoft ® Internet Explorer 7.0 e Mozilla Firefox ® 3.0 ou superior e permitir comunicação criptografada TLS 1.2 com o servidor;
- b) Deverá suportar autenticação do tipo “Single Sign-on” através da utilização da autenticação do Windows ou usuário e senha previamente configurados;
- c) Os privilégios do operador do SCA, deverá ser propagado para o usuário do “Web Client”, permitindo acesso apenas a objetos de segurança para qual o operador do SCA é autorizado;
- d) O “Web Client” deverá possuir recursos de Gestão de Pessoas, permitindo ao operador criar e modificar os dados das pessoas (incluindo a adição/remoção de acessos, horários e datas de vencimento);



- e) O operador deverá possuir a disponibilidade de ativar ou desativar os cartões;
- f) O operador deverá ter a capacidade de procurar, editar, adicionar e apagar os registros de pessoas do banco de dados do SCA. A função de busca deverá permitir a inclusão de nome ou sobrenome ou usuário de texto definido;
- g) Deverá permitir criar, configurar, carregar o “Web Client” além de ações manuais como: bloqueio/desbloqueio das portas, e a ativação/desativação dos eventos e salvar relatórios;
- h) Os relatórios deverão constituir-se de histórico de atividades de pessoas ou dados de auditoria;
- i) Deverá ser permitida a classificação e exibição dos dados do relatório de qualquer tela, em ordem ascendente ou descendente, sendo salvos, via “Web Client”, utilizando os seguintes formatos, não ficando limitados a: XLS, CSV, XML, TXT ou PDF;
- j) O sistema deve possuir permissão que o operador salve o relatório em um arquivo ou possa enviar via e-mail;
- k) O “Web Client” deverá possuir a capacidade de consulta de um portador de cartão ou de um grupo de portadores de cartão, de forma a permitir acessos de uma única vez, a múltiplos portadores de cartão. Uma vez finalizada a consulta, o operador deverá ter a capacidade de assegurar um acesso único ou um grupo de acessos para todos os portadores de cartão;
- l) O “Web Client” ou “cliente de aplicação” deverá possuir a capacidade de exibir relatório de atividade de uma porta, além de exibir dados como data e hora de ativação/desativação de cada cartão assegurado a um portador. O “Web Client” também deverá exibir todos os campos definidos para usuários (portadores de cartão) e detalhes de cada acesso designado a cada portador, em uma tela separada;
- m) O “Web Client” deverá possuir a capacidade de “log-off” de forma automática, baseado no período de inatividade do sistema;
- n) O SCA deve permitir que o tempo de inatividade, possa ser configurado por um administrador do sistema.

### 2.3 Requisitos de mapas gráficos

- a) O sistema deverá suportar ilimitados mapas gráficos e ícones para serem gerenciados pelo operador de forma nativa ou integrada por sistemas de terceiros;
- b) O sistema deverá suportar no mínimo os seguintes controles de mapas:
- c) Deverá visualizar planta baixa, localização para os alarmes dos dispositivos e instruções para ações pós alarmes;
- d) Deverá possuir configuração e visualização nas estações clientes de operação;
- e) Deverá permitir associação de vários mapas com diferentes áreas para criar uma hierarquia de mapas;
- f) O sistema deverá permitir operações tipo “arrastar e soltar” para adicionar qualquer ícone interativo (entradas de alarmes, saída de alarmes, eventos, mapas, relatórios, vistas dinâmicas, portas e elevadores). Estes ícones interativos deverão permitir que o operador realize tarefas e comandos relacionado ao objeto com um duplo-click no ícone;



- g) O sistema deverá permitir a adição de novas camadas ao mapa;
- h) O sistema deverá suportar no mínimo importação de mapas nos formatos AutoCAD, ou JPEG (JPG) ou PNG.

## 2.4 Requisitos da interface LDAP

- a) O sistema deverá ter a capacidade de se conectar a um serviço de diretório através do Lightweight Directory Application Protocol (LDAP);
- b) A conexão ao LDAP deverá ser configurável pelo usuário diretamente do SCA e não deverá requerer nenhum código customizado;
- c) A interface LDAP deve suportar designação automática de acessos SCA baseada nos dados contidos no registro LDAP;
- d) A funcionalidade LDAP deverá suportar as seguintes funções:
  - i. Nome do servidor LDAP e número da porta definida pelo usuário;
  - ii. Um nome único da base para a raiz de pesquisas;
  - iii. Um filtro de pesquisa LDAP para refinar as pesquisas de objetos;
  - iv. Mapeamento de atributos para os campos de pessoas;
  - v. O uso de nome único para autenticação no LDAP;
  - vi. Opção de pesquisa em todos os sub-níveis do diretório desde a base;
  - vii. Prever dados de exemplo baseados nos parâmetros de importação LDAP do SCA;
  - viii. Acessos automáticos no SCA baseados em funções de dois campos de dados;
  - ix. Importação automática das entradas do diretório do LDAP;
  - x. Autenticação via conta de usuário LDAP e SSL;
  - xi. Designação automática de acessos ao SCA.

## 2.5 Funcionalidades

- a) O sistema deve controlar o acesso a uma área designada;
- b) O sistema deve validar as credenciais do portador, através dos dados pessoais, formatos de cartão, senhas, reconhecimento facial, cadastramento biométrico e múltiplos cartões ativos. O sistema deve comparar a tentativa de entrada com as informações contidas na memória;
- c) As controladoras de acesso devem ser capazes de operar de forma independente em caso de perda de comunicação, através de registros em memória dos dados de logs de acesso de ao menos 50.000 usuários;
- d) O acesso a uma área designada será validado somente quando a credencial tiver um número válido para essa localidade e o número é válido para a data e hora corrente que a leitora for usada;
- e) O sistema deve acessar o equipamento que valida a pessoa e monitorar a segurança da localidade pelo uso de controladoras, portas, leitoras, elevadores, entradas e saídas. Quando o acesso é validado, um sinal é enviado para a leitora para permitir uma entrada na localização;



- f) O sistema deve ser configurado pelo uso da aplicação de Administração e deve prover modelos de configuração;
- g) O sistema deve permitir a configuração de lógica de acesso, intertravamentos e alarmes, possibilitando efetuar múltiplas configurações lógicas para acionamento de dispositivos de saídas;
- h) O sistema deve monitorar as atividades de controle de acesso pelo uso da estação de monitoramento;
- i) O sistema deve restringir o uso administrativo e a estação de monitoramento pelo uso de privilégios e autenticação (senha de usuário) usando a funcionalidade de senha do sistema operacional Microsoft Windows (autenticação por Windows) e através de autenticação pelo sistema (autenticação básica);
- j) O sistema deve reportar os vários aspectos do sistema pelo uso de relatórios (pré-configurados ou prontos). Relatórios deverão poder ser exportados para uma impressora ou enviados por e-mail;
- k) O sistema deve ter a capacidade de reportar condições anormais de segurança de forma audível e visual;
- l) O sistema deve controlar os equipamentos a partir da estação de monitoramento pelo uso de ações manuais, eventos e listas de causas;
- m) O sistema deve prover registro e gerenciamento de dados pelo uso do arquivo histórico (arquivamento e visualização), trilha de auditoria e procedimentos de importação e exportação manual ou automática (dados e imagens);
- n) O sistema de ter compatibilidade com o Protocolo de Dispositivo Aberto Supervisionado (OSDP) para comunicação das leitoras com a central.

## 2.6 Armazenamento

- a) Todas as informações programadas, bem como o histórico de transações, deverão ser automaticamente armazenadas no banco de dados para futura recuperação e backup. O SCA deve suportar configurações onde o banco de dados possa ser instalado: no disco do servidor do SCA, em servidor de banco de dados independente, em um servidor de banco de dados corporativo;
- b) deve ser capaz de salvar e recuperar todos os dados do sistema e histórico de transações. O servidor deve ser capaz de transferir todos os dados e históricos para discos rígidos (incluindo discos da rede);
- c) deve permitir que o histórico de atividades seja gravado num banco de dados. O sistema deve ter a capacidade de armazenar um mínimo de 50 milhões de transações;
- d) deve suportar comunicações criptografadas no mínimo do tipo SSL e/ou TLS 1.2 entre o servidor e a estação de monitoramento;
- e) deve suportar comunicações criptografadas no mínimo do tipo AES 256-bit entre o servidor e as controladoras;
- f) deve suportar o uso de redes Ethernet para a comunicação entre os servidores e as controladoras;
- g) As comunicações entre o servidor e os dispositivos de campo deverão ser encapsuladas num formato TCP/IP. O SCA deverá ter suporte a IPv4/IPv6.



### 2.6.1 Armazenamento de informação de pessoas

- a) O SCA deve prover as informações de pessoas em múltiplas abas, contendo campos pré-definidos ou campos customizados. O SCA deverá suportar a criação de diferentes tipos de campos. Os campos deverão possuir capacidade de customização por um operador ou administrador que possua tais privilégios. Cada campo definido pelo operador deverá permitir a inserção de nome, descrição ou identificação;
- b) Os campos criados pelo operador deverão ser definidos como Mandatório ou Único e deverão suportar os seguintes tipos de campo: caractere, inteiro, lógico, data/hora, data, hora, lista numerada, multilinha ou decimal;
- c) Os campos criados pelo operador deverão suportar mascaramento, de modo a fornecer consistência dos dados inseridos para todos os operadores do sistema, devendo suportar máscaras customizadas e máscaras pré-definidas;
- d) O SCA deverá fornecer a capacidade que permite ao operador atribuir/anexar até 2 (dois) documentos (tais como URL, PDF, ou arquivos TXT) para o registro de pessoal. O documento pode ser aplicado para o registro como:
  - I. Documento Compartilhado - adicionado ao SCA através do editor de documentos;
  - II. Documento Privado - importado de fora do sistema, tal como uma certidão de nascimento ou um diploma.

### 2.7 Software - Configuração

- a) O SCA deve prever a configuração de modelos. Modelos de objetos com suporte deverão ser configuráveis pelo operador para fornecer valores padrão, pré-preenchendo informações comumente usadas em campos de dados. O SCA geralmente deverá permitir qualquer objeto no sistema a ser agrupado incluindo pessoas, portas, entradas, saídas e folgas;
- b) O SCA deve manter uma distinção entre os objetos que estão sendo monitorados e objetos que estão sendo controlados, impedindo a emissão de ações manuais de objeto a objetos para os quais o operador não tem privilégios de ação. Deve haver diferentes níveis de controles dentro do sistema de privilégios de administração contra privilégios de monitoramento.
  - i. O SCA deve apoiar contas ilimitadas do operador com níveis de privilégio definível ilimitado;
  - ii. O SCA deve permitir a configuração de controladores usando navegação hierárquica baseada em árvore e menus de contexto;
  - iii. O SCA deve apoiar a capacidade para fazer o download de atualizações de firmware para os controladores;
  - iv. O SCA deve suportar os métodos de autorização e autenticação do operador em Windows logon único (SSO) ou autenticação básica de usuário com nomes de usuário definidos localmente e senhas.





## 2.8 Credenciais

- a) O SCA deve permitir um mínimo de 5 (cinco) credenciais (cartões) por registro pessoal e só contarão cartões ativos e/ou expirados para os máximos postais atribuíveis por pessoa;
- b) O SCA deve permitir a capacidade de definir o período de tempo padrão (em dias, horas ou anos) a partir da data de ativação de uma credencial até o seu término. O SCA deve apoiar uma substituição do período de tempo de expiração padrão para tipos de pessoal individuais;
- c) O SCA deve permitir credenciais temporárias. Credenciais temporárias estarão disponíveis para reuso geral sem estarem associadas aos registros de pessoal específicos. O SCA deve suportar a configuração de um número padrão de dias para credenciais temporárias de forma a permanecerem ativas depois que eles são criados;
- d) O SCA deve permitir uma configuração de todo o sistema para desativar automaticamente as credenciais de pessoal que não tenham sido utilizadas por um período de tempo especificado. O processo “Disable” por inatividade deve apoiar um usuário configurável por tempo de varredura diária.

## 2.9 Suporte a cartões e leitoras

- a) O SCA deve suportar múltiplos formatos de cartões e leitoras de cartões e deve suportar as seguintes funcionalidades para leitoras conectadas diretamente:
- b) Formatos de cartão de até 128 bits;
- c) OSDP v2.1.6 ou superior, usando criptografia OSDP Secure Channel AES128;
- d) Número ilimitado de formatos de cartões de acesso;
- e) Capacidade de suporte de até 8 formatos de cartão por leitora;
- f) Suporte a Wiegand e teclados de matriz 3x4;
- g) Cadastramento de templates dos modelos de biometria;
- h) O SCA deve suportar leitoras que geram sinais Wiegand ou OSDP incluindo:
  - i. Leitoras Multi-tecnologia;
  - ii. Leitoras Wiegand;
  - iii. Leitoras de Proximidade;
  - iv. Leitoras Biométricas;
  - v. Leitoras Smartcard;
  - vi. Leitoras Magnéticas;
  - vii. Leitoras com Teclado;
- i) O SCA deve possuir a capacidade de definir a configuração de áreas. Áreas são definidas como regiões físicas delimitadas por portas. Uma área deve consistir em uma sala, um local específico de um edifício ou de um prédio inteiro;
- j) Todas as áreas configuradas deverão ter acesso de entrada/saída das portas, permitindo a capacidade de gerar relatórios, que apresentarão todos os usuários cadastrados de cada área. Não haverá maneira de sair de uma determinada zona sem apresentação de um cartão válido a um leitor;



- k) O SCA deve permitir a criação de relatório tipo “Chamada”. A “Chamada ou Mustering” é um relatório pré-definido pelo SCA que deve listar todo o acesso de pessoal que estiverem em determinadas áreas ou grupo de áreas;
- l) O SCA deverá suportar o controle de área, de modo a fornecer a capacidade de rastreamento de pessoal. Com esta função, o operador deve obter a localização atual dos usuários dos cartões. Exibições dinâmicas e/ou relatórios podem ser gerados para mostrar cartões específicos que estão presentes em cada área definida;
- m) Os registros dos titulares dos cartões devem ser capazes de fornecer acesso fácil para visualização de localização na área, com atualização em acordo com o deslocamento de uma área para outra através do acesso por cartão ou biometria;
- n) O controlador local deve fornecer a capacidade de gerenciar e controlar as configurações de área, no caso em que ele perde a comunicação com o servidor do sistema SCA, com capacidade mínima de 100.000 portadores de cartão e 50.000 eventos;
- o) A configuração de área do SCA terá três modos de operação: Nenhuma, Antipassback e Antipassback Temporizado;
- p) O recurso Antipassback deve controlar o acesso com base na localização do titular do cartão. O SCA deve negar o acesso aos titulares que estão em violação das regras Antipassback. No caso de um usuário sair de uma área sem apresentar seu cartão ao leitor de acesso, e depois tentar entrar de novo na área, apresentando o cartão ao leitor de entrada, irá ocorrer a negação de acesso. O SCA deverá ter a capacidade de liberar os cartões que tenham violado as regras do recurso Antipassback. A opção de liberação também poderá ser aplicada em qualquer cartão de usuário;
- q) O recurso Antipassback deverá continuar a ser executado durante a falha de comunicação;
- r) Controladoras dentro de um “Cluster” que estão desconectadas do servidor e/ou controladora mestra deverão liberar todos os usuários registrados em sua memória interna através da configuração “Modo Local”. A controladora desligada deverá seguir as regras antipassback específicas para as áreas definidas na controladora. Se a controladora não reconhecer que um usuário está em uma área com recurso de violação antipassback, o acesso será concedido;
- s) O SCA deve possuir o recurso antipassback temporizado. Áreas configuradas com o antipassback temporizado devem solicitar que o portador do cartão, apresente a um leitor de saída para deixar uma área. Portadores de cartão que não saírem da área devidamente deverão aguardar um período predeterminado antes de entrar novamente na mesma área;
- t) O SCA deverá fornecer recursos de restrição de ocupação de áreas. Estas restrições deverão ser aplicadas ao portador do cartão (no campo de pessoal), ou então para um grupo de portadores. Áreas deverão ser configuráveis de modo a permitir a limitação de quantidade máxima ou mínima de acesso de pessoas, em mesmo momento ou determinado período. O SCA deve gerar alarmes ou acionar eventos, no caso da violação destas regras;
- u) Os eventos deverão ser configuráveis baseadas pelo menos nos seguintes critérios:
  - i. Status de máxima ocupação;



- ii. Status de mínima ocupação;
  - iii. Status de máxima ocupação de grupos;
  - iv. Status de mínima ocupação de grupos;
  - v. Contagem de pessoas (definido por operador);
  - vi. Status de violação (violação de entrada/saída do antipassback);
- v) O SCA deverá permitir a restrição de ocupação de áreas, tanto para o máximo quanto para o mínimo, e informar o operador em caso de violação.

## 2.10 Níveis de acesso

- a) O SCA deve suportar a configuração de um número ilimitado de níveis de acessos;
- b) As controladoras deverão suportar no mínimo 1.500 níveis de acesso e ter a capacidade mínima de até 100 níveis de acessos por pessoa;
- c) O SCA deve suportar ativação e expiração do nível acesso por data ou hora;
- d) O SCA deverá possuir a capacidade de selecionar múltiplas pessoas (portadores de cartão) através da visão dinâmica a assegurar níveis de acessos as pessoas selecionadas, como também remover os níveis de acessos as pessoas selecionadas.

## 2.11 Eventos

- a) O SCA deverá suportar configurações ilimitadas de eventos, incluindo eventos agendados e ações baseadas em disparo de eventos;
- b) O SCA deverá prover níveis de prioridade de eventos configuráveis. Deverá permitir que o operador defina cores e nomes individualmente por prioridade;
- c) O SCA deverá permitir no mínimo as seguintes configurações de eventos:
  - I. Classificação por nome do evento, data/hora, prioridade, estado e qualquer informação visualizável;
  - II. Encaminhamento para operadores por privilégios de operador, incluindo por função hora do dia;
  - III. Solicitação de reconhecimento ou não pelo operador para o evento;
  - IV. Solicitação de reconhecimento ou não para o operador limpar o evento;
  - V. Solicitar ou não que o operador deixe uma mensagem para registro do reconhecimento do evento;
  - VI. Solicitar ou não que o operador deixe uma mensagem para registro da limpeza do evento;
  - VII. Mostrar ou não uma ativação de evento;
  - VIII. Solicitar que o objeto causador da ação do evento reset após o operador reconhecer o evento;
  - IX. Exibir uma mensagem definida pelo operador no momento da ativação do evento;
  - X. Exibir uma mensagem definida pelo operador quando o evento for desativado;
  - XI. Associação com um mapa e abrir este mapa automaticamente na estação de monitoramento quando o evento é ativado;



- XII. Ativar um evento secundário quando a ativação do primeiro evento não for reconhecida por um determinado tempo;
- XIII. Ativar um evento secundário quando a ativação do primeiro evento for reconhecida, mas limpa por um determinado tempo;
- XIV. Permitir que o operador associe um arquivo de áudio a um evento;
- XV. Permitir tempo mínimo para ativação e tempo para atraso do evento;
- XVI. Permitir importação e exportação;
- XVII. Permitir emissão e remoção de relatórios com resultados;
- d) Cada evento deverá suportar incluir instruções do evento, a ser exibido na tela de detalhes do evento;
- e) O SCA deverá suportar ações de eventos e botões de eventos manuais que serão utilizados para trave, destrave, alternar e pulsar outros eventos;
- f) O SCA deve prover mecanismo de configuração de servidor SMTP, a fim de enviar e-mails após eventos ativados.

## **2.12 Critérios para importação / exportação**

- a) O SCA deve prover mecanismos para manualmente importar e exportar dados selecionados em formato XML ou texto. Esse mecanismo deve suportar a importação e exportação de qualquer classe ou tipos de dados no sistema. A validação de dados e registros de histórico são requerimentos obrigatórios;
- b) O sistema deve também suportar a importação de arquivos em formato CSV;
- c) O SCA deve prover um mecanismo de importação automática baseado em XML ou texto. Esse mecanismo deve suportar a importação de vários tipos de dados no sistema;
- d) O SCA deverá ter a capacidade de gerar importações automatizadas através de uma fonte de dados ODBC permitindo a importação de dados de pessoal, diretamente para sua base de dados.

## **2.13 Gerenciamento de visitantes**

- a) O SCA deve possuir funcionalidade de gerenciamento das visitas e visitantes, podendo ser realizado o Check-In (Entrada) e Check-Out (Saída) dos visitantes automaticamente;
- b) A funcionalidade de gerenciamento de visitas e visitantes, deverá ser do mesmo fabricante do sistema SCA, nativo, não sendo aceito software de terceiros;
- c) O SCA deve possuir funcionalidade de “baixa automática de crachá”, ou seja, quando o crachá for depositado na urna da catraca, deverá realizar a saída do visitante automaticamente na leitura do crachá, finalizando a visita, e também retornar o cartão para o estado “sem uso”, a fim de que esteja apto a ser utilizado por outro visitante sem a necessidade de realizar a desassociação do crachá manualmente.

## **2.14 Módulo de Controle de Acesso (MCA)**



- a) Deverá ser fornecido todos os hardwares necessários para a integração com os bloqueios e portas, atendendo aos seguintes requisitos mínimos:
- I. Controladora descentralizada do tipo autônoma TCP/IP com capacidade de gerenciar e controlar a porta e todos os seus dispositivos (leitoras, eletroímã, fechaduras, botoeiras, etc.). Sendo um equipamento tipo controlador de rede independente, autônomo, capaz de proporcionar controle de acesso com tomada de decisão local, para um banco de dados local de portadores de cartões, de alarme e buffer evento nas comunicações em caso de perda de comunicação, não sendo permitidos sistemas que dependem exclusivamente de um servidor central para a decisão do controle de acesso;
  - II. Os módulos de controle de acesso ethernet atuam como unidade de interface distribuídos, capazes de suportar no mínimo 16 leitoras Wiegand ou OSDP;
  - III. O MCA é interconectado diretamente aos servidores através da rede não necessitando de outros dispositivos de interface para gerenciamento dos MCAs e decisões de controle;
  - IV. Os módulos de controle de acesso devem compatíveis com os formatos de leitor/cartão: Mifare, Desfire EV1, Prox, iClass;
  - V. Os módulos de controle deverão permitir o processamento distribuído do controle de acesso, com possibilidade de funcionamento autônomo de cancelas, fechaduras eletromagnéticas, leitoras de cartão e leitores biométricos;
  - VI. Os equipamentos ofertados que serão utilizados na comunicação com os servidores da CONTRATADA deverão possuir arquitetura modular, expansível, via TCP/IP nativa com o servidor, comunicação criptografada, com uma chave criptográfica de no mínimo 256 bits, (AES – Advanced Encryption Standard);
  - VII. Os equipamentos ofertados que serão utilizados na comunicação com os servidores da CONTRATANTE deverão possuir suporte à LAN utilizando Interface Ethernet RJ-45 (10/100baseT ou velocidade superior) e suportar DHCP e endereçamento com IP fixo. Os equipamentos ofertados na solução deverão possuir capacidade para impedir que um cartão passe duas vezes, em sequência, pela mesma leitora, como também prevenir que um mesmo cartão seja usado por mais de uma pessoa, mais de uma vez, em um grupo área de acesso/portas;
  - VIII. Os equipamentos ofertados na solução deverão possuir integração para leitores de cartão de outros fabricantes, integração com os terminais de reconhecimento facial ofertados, suporte à interface biométrica e aos formatos de cartão: Magnéticos e Wiegand ou OSDP;
  - IX. Cada equipamento tipo módulo de controle deverá manter um relógio geral e um RTC (Real Time Clock) incorporado. Tanto o equipamento gerenciado quanto o RTC deverão sincronizar data e horário com o servidor central, sempre que este estiver online, em intervalos regulares pré-programados. Caso seja interrompida a comunicação entre o gerenciador e o servidor, aquele passará a sincronizar data e horário com o RTC incorporado. Quando voltar a comunicação com o servidor, ambos, o RTC e o gerenciador, passarão a



sincronizar data e horário novamente com o servidor, respeitando as diferenças que poderão acontecer devido a horário de verão ou fuso horário;

- X. Em caso de queda da rede (comunicação) ou do computador servidor (servidor de aplicação), cada equipamento gerenciado deverá continuar funcionando autonomamente com todas as últimas instruções, validando e registrando as informações de: matrícula do usuário, data do registro, hora do registro no formato dd/mm/yyyy, localidade, identificação da catraca, IP, informação/flag de entrada ou saída, inclusive contendo informação de urna, quando for o caso;
- XI. Cada módulo gerenciador deverá ser instalado em um gabinete metálico, com grau de proteção adequado ao local de instalação;
- XII. Configuração e diagnóstico via IHM local ou rede (LAN);
- XIII. Para garantir a compatibilidade e a performance da solução, a placa controladora deverá ser do mesmo fabricante do software de controle de acesso especificado neste documento.

c) Processador e Memória:

- I. O microprocessador / microcontrolador do MCA deve ter capacidade de processamento e memória para fornecer criptografia mínima de 256 bits on-board AES sem o uso de um dispositivo de criptografia externa, proporcionando decisões de acesso dentro um (01) segundo em um sistema totalmente carregado, que será utilizado para o código de inicialização e sistema operacional, e para backup de memória.
- II. O controlador deve possuir memória não volátil on-board deve ser capaz de armazenar localmente ao menos 200.000 usuários de cartão, capaz de registrar operações mesmo estando fora da rede, de verificar autorizações de acesso, controlando abertura e travamento dos dispositivos de acesso e registro dos eventos.

## **2.15 KIT CONTROLE PORTA TIPO 1 – AUTENTICAÇÃO SIMPLES**

### **2.15.1 Mola hidráulica - qtd: 1**

A mola hidráulica com as seguintes características mínimas:

- a) Dever ser do tipo universal, permitindo a instalação em portas de madeira e metal;
- b) O sistema de mola hidráulica deve para quase qualquer aplicação;
- c) Possuir proteção contra corrosão;
- d) Deve suportar portas de até 25kg.

### **2.15.2 Fechadura eletromagnética - qtd: 1**

A fechadura eletromagnética deve ter as seguintes características mínimas:

- a) Fazer a abertura e o fechamento de forma silenciosa;
- b) Deverá ser acionada por qualquer controle de acesso do mercado;
- c) Baixo consumo elétrico.



- d) Deve atender no mínimo as seguintes especificações técnicas:
  - i. Tensão: 12VCC;
  - ii. Corrente de operação: 300 a 450mA;
  - iii. Potência: 3,9 a 5,4W;
  - iv. Temperatura de operação: -5 a 50°C;
  - v. Dimensões máximas: 173 x 47 x 28 (A x L x P) mm;
  - vi. Força de Tração: 150kgf;
  - vii. Possuir sensor para sinalização do estado de abertura da porta.

#### 2.15.3 Fonte – qtd: 1

A fonte de alimentação deve ter as seguintes características mínimas:

- a) Fontes de alimentação com gabinete para acomodação de bateria para alimentação de carga;
- b) Pode abrigar internamente uma bateria de 12V;
- c) A fonte deve possuir tensão de entrada de 90 a 240 VCA e tensão de saída entre 12 e 15 VCC e corrente de saída entre 1A e 2A.
- d) Na falta de energia da rede local, a fonte continua alimentando a carga;
- e) A fonte deve indicar as seguintes sinalizações:
  - i. Sinalizar o carregamento (flutuação) da bateria;
  - ii. Sinalizar a falta de energia da rede.

#### 2.15.4 Bateria 12V – qtd: 1

A bateria 12v deve ter as seguintes características mínimas:

- a) A bateria deve ser de chumbo-ácido regulada por válvula selada VRLA recarregável, livre de manutenção e protegida contra vazamento.
- b) Deve atender as seguintes características técnicas mínimas:
  - i. Tensão: 12 Vdc;
  - ii. Capacidade: 7 Ah (C20);
  - iii. Flutuação: 13,6 a 13,8 V;
  - iv. Cíclico: 14,4 a 15,0 V;
  - v. Corrente inicial: 2,10 A.
  - vi. A bateria deve possuir vida útil de até 5 anos.

#### 2.15.5 Acionador de emergência rearmável - qtd: 1

O acionador deve ter as seguintes características mínimas:

- a) Deve ser do tipo rearmável;
- b) Deve ser do tipo sobrepor;
- c) Deve possuir sinalização sonora quando desarmado.





#### 2.15.6 Botoeira – qtd: 1

A botoeira deve ter as seguintes características mínimas:

- a) Botoeira de Acionamento interno com tecnologia infravermelho para acionamento sem contato;
- b) Deve vir fixado em espelho para instalação em caixa interna ou externa 4 x 2”;
- c) Deve possuir moldura em aço inox;
- d) Deve vir acompanhado de todos os acessórios para fixação, como parafusos, todos necessários para fixação e adequação às instalações;
- e) Deve possuir LED luminoso para indicação de estado de porta (aberto e fechado).

#### 2.15.7 Leitor Facial – qtd: 1

O leitor facial deve ter as seguintes características mínimas:

- a) O terminal leitor de reconhecimento facial deve ser integrado ao software de controle de acesso ofertado, podendo também atuar autonomamente (stand alone) em caso de desconexão e para fins de controle da catraca ou porta em que se encontra;
- b) A integração deve possibilitar o cadastramento de faces em uma interface unificada, não sendo permitido o uso de um software distinto para cadastramento de faces e outro para cadastramento de visitantes;
- c) Ser equipado com tela LED com dimensão maior ou igual a 7", com resolução mínima 1024 x 600 pixels, equipada com função touch screen para acesso ao menu de funções e interação com a interface do equipamento;
- d) Deve possibilitar a leitura de faces dos usuários entre 1.2 e 2 metros de altura;
- e) Deve possibilitar a leitura QR Code e cartão de proximidade do tipo Mifare (13,56MHz) compatíveis com o software de controle de acesso ofertado;
- f) Possuir câmera dupla no painel frontal;
- g) Deve dispor de recurso WDR ou DWDR para tratamento dos níveis de contraste na imagem;
- h) Deve possibilitar que a velocidade de leitura menor ou igual a um segundo para reconhecimento facial;
- i) Deve ser capaz de armazenar ao menos 5.000 faces na memória interna;
- j) Deve ser capaz de armazenar em seu histórico ao menos 100.000 eventos/gravações diversas;
- k) Deve possuir índice de precisão superior a 99% para reconhecimento facial;
- l) Deve possuir tecnologia antifraude que permita a detecção de face viva, impedindo o acesso por fotos ou vídeos;
- m) Possuir ao menos 1 porta de integração para cada uma das seguintes tecnologias/serviços:
  - i. RS-485
  - ii. Wiegand
  - iii. Ethernet - 10/100 mbps
  - iv. Botão de requisição de saída



v.Fechadura eletrônica/eletromagnética  
vi.Entrada de alarme

- n) Deve possuir interface de configuração via rede;
- o) Deve suportar os protocolos OSDP ou Wiegand;
- p) Deve possuir capacidade de combinar informações do reconhecimento de face, com senha para liberar/negar acesso de modo combinado;
- q) Deve possuir arquitetura aberta para integração com outros sistemas por meio de API ou SDK ou CGI;
- r) O equipamento deverá ser fornecido com sua respectiva fonte de alimentação compatível com as características elétricas da região de instalação;
- s) Deve possibilitar operação no range de temperatura de no mínimo -10° a 45° em ambiente de 10 a 80% de umidade;
- t) Deve acompanhar suportes e/ou acessórios para fixação parede. O suporte deverá possuir acomodação para que os cabos não fiquem expostos.

## **2.16 Servidor para Sistema de Controle de Acesso**

- a) Possuir processamento Intel Xeon E-2136 última geração com pontuação de CPU em ferramentas de benchmark acima dos 13500 ou superior;
- b) Vir acompanhado de sistema operacional Windows Server 2019 (ou superior) ou Windows 10 Embedded IoT Enterprise (ou superior), instalado e devidamente configurado;
- c) Controladora de disco com suporte a RAID1;
- d) Possuir pelo menos 4Tb de armazenamento em disco (bruto);
- e) Possuir altura máxima de 2U e formato nativo padrão ao rack padrão 19", não sendo aceitos equipamentos que necessitem de bandejas;
- f) Possuir memória de 16GB DDR4 ou superior;
- g) Possuir pelo menos duas portas de rede gigabit RJ45;
- h) Deverá ser fornecido com teclado com fio em português (Brasil) e mouse laser com fio;
- i) Os cabos de alimentação deverão atender ao padrão brasileiro (NBR 14136) e em número suficiente para atender ao número de fontes que acompanham o equipamento (neste caso, no mínimo dois cabos);
- j) Possuir fonte de alimentação redundante de 100 a 240V, 50/60Hz, de 500 W ou superior, cada.

## **2.17 Bloqueio Tipo I - Balcão**

Catraca tipo balcão tipo gabinete em aço inox AISI 304 escovado, devendo possuir as seguintes características mínimas:

- a) Deve possuir pictogramas tricolores de operação com leds de alto brilho;
- b) Deve possuir porta pivotante motorizada de acionamento suave e silencioso;
- c) Deve sistema de liberação em caso de emergência;



- d) Deve possuir abertura e capacidade de passagem para usuários pedestres, com largura de vão de 600mm;
- e) Deve suportar folhas em policarbonato ou vidros temperados incolor de 10mm ou 12mm. Deve ser entregue com duas folhas para fechamento eficiente do bloqueio, em largura suficiente para usuários;
- f) Deverá possuir no mínimo de 5.000.000 (cinco milhões) de ciclos de acionamentos entre falhas (MCBF);
- g) Deverá ser projetada para uso contínuo, em regime de 24 horas;
- h) Deverá permitir taxa de passagem de pelo menos 35 pessoas por minuto;
- i) Deverá funcionar de forma suave e sem ruídos;
- j) O corpo do gabinete externo deverá ser confeccionado em aço inoxidável AISI 304 ou superior com chapa de no mínimo 1,5mm;
- k) Sua fixação deverá ser realizada diretamente ao chão através da base do gabinete;
- l) Sua estrutura deverá ser resistente de modo a garantir a segurança em caso de vandalismo e/ou má utilização por parte dos usuários;
- m) Seu gabinete deverá comportar a adição de componentes de acesso, como fontes, placas, e módulos controladores bem como leitoras e validadores de acesso diversos respeitando seu espaço interno;
- n) Deverá permitir passagens unidirecionais e bidirecionais, funcionando de acordo com a configuração do ambiente, com os pictogramas atuando de forma ao controle definido;
- o) No ato de acesso, o bloqueio deverá possuir capacidade de emissão de feedbacks sonoros como acesso liberado e negado;
- p) Deverá ser entregue com espaço montado em acrílico com suporte para leitoras, pictogramas, monitores de acesso, entre outros dispositivos de integração e controle;
- q) O equipamento deve possuir sensor de identificação de passagem, evitando que a porta feche acidentalmente no usuário;
- r) Os pictogramas devem ser confeccionados em LED de alto brilho e um dispositivo de feedback sonoro (buzzer);
- s) A catraca deverá possuir uma proteção mínima IP44 contra poeira, areia e jatos de água;
- t) Dever ser compatível com o sistema de controle de acesso e leitores faciais ofertados, permitindo a instalação de até dois leitores faciais por gabinete (entrada e saída).
- u) Devem ser fornecidos 2 (dois) leitores faciais, integrados e compatíveis com os gabinetes, em conformidade com as exigências mínimas definidas no item 2.15.7, acompanhados dos seus respectivos suportes para catraca.

## **2.18 Bloqueio Tipo 2 - Balcão PNE**

Catraca tipo balcão tipo gabinete em aço inox AISI 304, devendo possuir as seguintes características mínimas:

- a) Deve possuir pictogramas tricolores de operação com leds de alto brilho.
- b) Deve possuir porta pivotante motorizada de acionamento suave e silencioso;
- c) Deve sistema de liberação em caso de emergência;



- d) Deve possuir abertura e capacidade de passagem para usuários pedestres e para usuários de cadeira de rodas de acordo com a ABNT NBR 9050, com largura de vão de 900mm;
- e) Deve suportar folhas em policarbonato ou vidros temperados incolor de 10mm ou 12mm. Deve ser entregue com duas folhas para fechamento eficiente do bloqueio, em largura suficiente para usuários pedestres ou usuários de cadeira de rodas conforme normas aplicáveis;
- f) Deverá possuir no mínimo de 5.000.000 (cinco milhões) de ciclos de acionamentos entre falhas (MCBF);
- g) Deverá ser projetada para uso contínuo, em regime de 24 horas;
- h) Deverá permitir taxa de passagem de pelo menos 35 pessoas por minuto;
- i) Deverá possibilitar tempo de destrave de até 0,2s;
- j) Deverá funcionar de forma suave e sem ruídos;
- k) O corpo do gabinete externo deverá ser confeccionado em aço inoxidável AISI 304 ou superior com chapa de no mínimo 1,5 mm;
- l) Sua fixação deverá ser realizada diretamente ao chão através da base do gabinete;
- m) Sua estrutura deverá ser resistente de modo a garantir a segurança em caso de vandalismo e/ou má utilização por parte dos usuários;
- n) Seu gabinete deverá comportar a adição de componentes de acesso, como fontes, placas, e módulos controladores bem como leitoras e validadores de acesso diversos respeitando seu espaço interno;
- o) Deverá permitir passagens unidirecionais e bidirecionais, funcionando de acordo com a configuração do ambiente, com os pictogramas atuando de forma ao controle definido;
- p) No ato de acesso, o bloqueio deverá possuir capacidade de emissão de feedbacks sonoros como acesso liberado e negado;
- q) Deverá ser entregue com espaço montado em acrílico com suporte para leitoras, pictogramas, monitores de acesso, entre outros dispositivos de integração e controle;
- r) O equipamento deve possuir sensor de identificação de passagem, evitando que a porta feche acidentalmente no usuário;
- s) Os pictogramas devem ser confeccionados em LED de alto brilho e um dispositivo de feedback sonoro (buzzer);
- t) A catraca deverá possuir uma proteção mínima IP44 contra poeira, areia e jatos de água;
- u) Dever ser compatível com o sistema de controle de acesso e leitores faciais ofertados, permitindo a instalação de até dois leitores faciais por gabinete (entrada e saída).
- v) Devem ser fornecidos 2 (dois) leitores faciais, integrados e compatíveis com os gabinetes, em conformidade com as exigências mínimas definidas no item 2.15.7, acompanhados dos seus respectivos suportes para catraca.

## **2.19 Cartões de acesso acompanhados de cordão para crachá**

- a) Cartão no formato crachá, com funcionamento por proximidade, tipo Mifare (13,56MHz) padrão ISO 14.443, acompanhado de cordão para crachá;
- b) Os cartões devem ser compatíveis com os leitores de reconhecimento facial e software de controle de acesso ofertados;



- c) O cartão deverá ser confeccionado em PVC, com acabamento overlay laminado, na cor branca;
- d) O cartão deverá possuir no mínimo 54mm de largura, 86mm de comprimento e 0,75mm de espessura;
- e) O cartão deverá possuir perfuração compatível com acabamento do tipo argola e jacaré;
- f) O cartão deverá possuir impressão em ambas as faces no padrão 4X4 cores;
- g) O cordão deverá ser confeccionado em poliéster acetinado, em cor a ser definida pela CONTRATANTE, personalizado com impressão por sublimação ou serigrafia;
- h) O cordão deverá possuir fixador de tipo argola e jacaré;
- i) O cordão deverá possuir no mínimo 20mm de largura, 800mm de comprimento;
- j) A arte que será impressa no cartão de acesso e no cordão para crachá será definida pela CONTRATANTE;
- k) Os cartões e cordões deverão ser produzidos conforme demanda da CONTRATANTE.

### **3. Especificações *Digital Signage***

#### **3.1 Monitores**

- a) Monitor profissional do tipo LFD, atendendo os seguintes requisitos mínimos:
- b) Tempo de operação: 24 x 7 (24 horas por dia, 07 dias por semana);
- c) Tamanho: 50 polegadas;
- d) Resolução: 3840 x 2160;
- e) Orientação: retrato e paisagem;
- f) Formato de tela: 16:9;
- g) Tempo de resposta máximo de 12 ms;
- h) Ângulo de visão de 178° (horizontal e vertical)
- i) Conectividade: *Wi-Fi*, Ethernet (LAN), ao menos 01 (uma) entrada HDMI e 01 (uma) entrada USB;
- j) Controle remoto;
- k) Fonte de alimentação 100~240VAC;
- l) Suporte para fixação em parede compatível com padrão VESA.

#### **3.2 Player para *Digital Signage***

- a) NUC, ou dispositivo similar para funcionalidade de sinalização digital, atendendo os seguintes requisitos mínimos:
  - I) Processador Intel Core i3 ou similar, 6M cache, até 4.10 GHz em frequência turbo;
  - II) Memória RAM de, no mínimo, 4GB DDR4;
  - III) Armazenamento de, no mínimo, 256GB SSD ou HDD 2.5”;
  - IV) Suporte para, no mínimo, Windows 10 ou Linux OS;
  - V) Duas saídas de vídeo, sendo que pelo menos uma deve ser HDMI;



- VI) Interfaces USB 2.0 e 3.0;
  - VII) Interface LAN RJ45 10/100/1000 Mbps;
  - VIII) Alimentação AC-DC 100-240VAC;
  - IX) Suporte de fixação VESA;
  - X) O player deverá ser compatível com o software para *digital signage* e os formatos informados no ponto 3.3;
- b) No caso de comprovado atendimento dos requisitos por telas com as funcionalidades descritas *built-in*, ainda que não atendam aos sistemas operacionais mencionados, não será necessário o fornecimento de NUC ou dispositivos acessórios.

### 3.3 Software para *Digital Signage*

- a) *Software* de gerenciamento para sinalização digital, versão Server, atendendo os seguintes requisitos mínimos:
- I) Compatível com Windows ou Linux;
  - II) Exibir conteúdo na disposição horizontal e vertical;
  - III) Aceitar os formatos de vídeo: AVI, MOV, MP4, MPEG1, MPEG2, MPEG4, JPEG, WMV, FLV, DIVX;
  - IV) Aceitar os formatos de áudio: MPEG, MP3, AAC;
  - V) Permitir a criação e uso de *playlists*;
  - VI) Execução de conteúdos sincronizados entre 02 (duas) ou mais telas;
  - VII) Funcionar em qualquer sistema operacional;
  - VIII) Ser compatível com software de exibição de conteúdo;
  - IX) Permitir *upload* das seguintes mídias: vídeo, imagem, áudio, HTML5;
  - X) Permitir a segmentação do conteúdo a ser exibido por tela;
  - XI) Permitir o agendamento por: intervalo de datas, intervalo de horários, dias da semana.

### 3.4 Servidor para gerenciamento de *Digital Signage*

- a) Microcomputador padrão workstation;
- b) Processador Intel i7 com 12 núcleos e 20 threads;
- c) Memória RAM: 16GB DDR4;
- d) Armazenamento: 512GB SSD;
- e) Placa gráfica off-board com pelo menos 4GB DDR5
- f) Teclado e mouse com fio do mesmo fabricante do equipamento;
- g) Sistema operacional Windows 11 Pro Português;
- h) Deve possuir placa mãe com BIOS desenvolvida pelo próprio fabricante do equipamento.



#### **4. Demais componentes da solução**

##### **4.1 Sistema de armazenamento**

- a) O servidor deve possibilitar a gravação de vídeo em rede de alto desempenho e armazenamento, suportando funcionamento ininterrupto (24x7);
- b) Deve ser compatível com o VMS ofertado;
- c) Devem estar contempladas todas as licenças necessárias ao funcionamento de sistema, assim como licenças perpétuas com direito de uso permanente, que sejam necessárias à execução das tarefas e aplicativos descritos e/ou que sejam disponibilizados pela solução ofertada;
- d) Deverá possuir gabinete tipo rack padrão 19" (dezenove polegadas), entregue com trilhos e quaisquer outros componentes necessários para instalação em rack;
- e) Não serão aceitos equipamentos com discos rígidos de uso comum para computadores, não fabricados e com características específicas para videomonitoramento, conforme informação do fabricante dos HDDs;
- f) Servidor deverá vir equipado com HDD's suficientes para prover gravação de todas as câmeras por 20 dias, 24 horas por dia a 20FPS com ciclo de movimento de 50%, resolução de 1920×1080, compressão em H.265, em RAID 5;
- g) Deverá ser baseado em plataforma para suportar pelo menos 2 (dois processadores);
- h) O equipamento deverá ser novo, estar em linha de produção no momento da licitação, sendo possível consultar o site do fabricante para verificação das especificações técnicas;
- i) Deve possuir pelo menos 8 (oito) canais de memória;
- j) Os canais de memória deverão ser preenchidos obedecendo as regras de máxima desempenho para o sistema conforme recomendação do fabricante do servidor;
- k) Processador Intel Xeon Silver 4208 ou superior;
- l) Memória RAM de 32 Gigabytes ou superior;
- m) Deve possuir ao menos 2 (dois) discos rígidos padrão SSD de 200 Gigabytes cada ou superiores;
- n) Deve possuir discos e baias adequados para permitir a funcionalidade de troca a quente dos discos;
- o) Deverá possibilitar a configuração dos discos via Controladora para uso de RAID tipo 0, 1, 5, 10;

##### **4.2 Impressora de cartões de identificação**

- a) Impressão de um lado ou frente e verso;
- b) Impressão por transferência térmica de sublimação de tinta colorida ou monocromática;
- c) Resolução de impressão de 300dpi/11,8 pontos por milímetro;
- d) Velocidade de impressão monocromática de um lado de 1100 cartões /hora ou superior;
- e) Impressão em cores:
  - I) Um lado (YMCKO): 210 cartões/hora ou superior;
  - II) Frente e verso (YMCKOK) - 185 cartões/hora ou superior;
  - III) Um lado (YMCKO) com laminação - 195 cartões/hora ou superior;
- f) Interface: USB 2.0 (plug-and-play) / Ethernet 10/100 / 802.11 b/g wireless;
- g) Tamanho de cartão padrão aceito: CR-80, formato ISO 7810, tipo ID-1;





- h) Tipos de cartão aceitos: PVC e composto, cartões ABS, PET, PET-G, Papel sintético de alto desempenho, adesivo, campo para assinatura, transparentes com bloqueadores de IR;
- i) Área de impressão: de borda a borda em cartões CR-80;
- j) Capacidade de entrada de cartões: 125 cartões ou superior;
- k) Capacidade de saída de cartões: até 100 cartões ou superior;
- l) Capacidade de alimentação de cartão único;
- m) Codificação:
  - I) Cartão inteligente (Smart Card) de contato / sem contato;
  - II) Codificadora de tarja magnética: AAMVA e ISO 7811;
  - III) Estação de contato de smart card ISO 7816 para codificadores de contato externos de terceiros;
  - IV) Codificadora sem contato MIFARE ISO 14443 A e B (13,56 MHz) e codificadora de contato ISO 7816 com certificação de EMV nível 1 e conformidade com PC/SC;
  - V) Codificadora RFID UHF Gen 2.

#### **4.3 Webcam para recepção**

- a) Captura de fotos para utilização pelo sistema de controle de acesso;
- b) Resolução mínima de 1,3 megapixels;
- c) Vídeos em alta definição;
- d) Compatível com estações de cadastramento.

#### **4.4 Estações de cadastramento**

- a) Deverá ser um equipamento desenvolvido especificamente para operação no modo workstation;
- b) Gabinete formato torre;
- c) O equipamento cotado deverá ser novo, estar em linha de produção no momento da licitação, sendo possível consultar o site do fabricante para verificação das especificações técnicas;
- d) Deverá possuir pelo menos 1 (um) processador com frequência baseada em processador de pelo menos 3,5 GHz, frequência turbo máx. de pelo menos 4,2 GHz, no mínimo 4 núcleos, no mínimo 6 threads, cache de pelo menos 6 MB e pelo menos 16 linhas PCI Express;
- e) Deve possuir processamento gráfico integrado com frequência de base gráfica de pelo menos 320 MHz;
- f) Chipset do mesmo fabricante do(s) processador(es) com suporte a PCI Express 3.0 ou superior com suporte a pelo menos 2 (dois) DIMMs por canal;
- g) Possuir, pelo menos, memória instalada de 8GB DDR4 SDRAM, disposta em 1 (um) pente de 8 GB com capacidade de chegar à pelo menos 64 GB;
- h) Deve possuir pelo menos 2 (dois) canais de memória;
- i) Os canais de memória deverão ser preenchidos obedecendo as regras de máxima desempenho para o sistema conforme recomendação do fabricante do servidor;
- j) Possuir 04 slots DIMM, suporte para módulos de memória DDR4 até pelo menos 2.933MHz;
- k) Possuir pelo menos 4 (quatro) conectores SATA 6 Gb/s interfaces integradas;



- l) Motherboard deve possuir nativamente pelo menos dois conectores M.2 não sendo aceitos adaptadores (ex.: PCI) para tal funcionalidade por reduzir a taxa de comunicação efetiva;
- m) Deverá possuir 1 (uma) unidade de estado sólido (SSD) com capacidade de, no mínimo, 120 GB SSD onde deverá ser instalado o sistema operacional e o(s) aplicativo(s);
- n) Deve possuir pelo menos 1 (uma) interface gráfica integrada Display Port com resolução mínima de 1920x1080 e pelo menos 1 (uma) porta HDMI com resolução de pelo menos 4096x2160;
- o) Deve possuir pelo menos 3 (três) portas USB 3.1;
- p) Deve possuir pelo menos uma porta Ethernet RJ-45 com velocidades de pelo menos 1 Gbps;
- q) Deverá possuir pelo menos 1 (um) disco rígido HDD 3,5 polegadas apropriado para sistemas de segurança e vigilância de, no mínimo, 1 TB, cache de pelo menos 58 MB, pronto para operação 24x7, interface SATA 6 Gb/s taxa de transferência sustentada de pico de pelo menos 170 MB/s, potência média de trabalho de no máximo 6 W preparado para operar no mínimo 8600 horas por ano, mantendo alta AFR de <1%, os discos rígidos. Deverão ser designados para carga de trabalho de videovigilância e operação de gravação em tempo integral;
- r) Não serão aceitos equipamentos com discos rígidos de uso comum para computadores, não fabricados e com características específicas para videomonitoramento, conforme informação do fabricante dos HDDs;
- s) Ventilação apropriada à configuração, com fonte de alimentação de, no mínimo, 500W reais com fator de correção ativo, bivolt;
- t) A fonte de alimentação deverá possuir faixa de tensão de entrada de 100 a 240V (automático) à 60Hz, interna ao equipamento (não serão aceitos equipamentos que operem em tensão de entrada em 12Vdc ou 24Vdc);
- u) O equipamento deverá possuir ventiladores internos originais do equipamento, necessários para a perfeita refrigeração do sistema interno do servidor na sua configuração máxima;
- v) Deverá suportar pelo menos 2 (duas) baias de 3,5" e pelo menos 2 (duas) SSDs de 2,5";
- w) A temperatura de operação deverá ser de pelo menos 0° a 60°C;
- x) Deve possuir pelo menos um slot PCI Express executando x16;
- y) Equipamento não será aceito caso sejam utilizados discos em gabinetes externos ao servidor;
- z) Deverá possuir sistema operacional Windows Enterprise 10 IoT ou superior, já gravado e totalmente compatível com o equipamento;
- aa) O sistema operacional deverá possuir os recursos (e os eventuais softwares adicionais se necessários) para implementar:
  - a. funcionalidade para bloqueio ao instalar novos app's;
  - b. criptografia dos discos;
  - c. boot seguro;
  - d. suportar geração de consulta de integridade de dispositivos gerenciados;
  - e. autenticação de múltiplos fatores ao fazer logon no servidor;
  - f. controle de atualização do Windows de forma remota e com horário agendado em modo avançado;
  - g. modo leitura de pastas e arquivos somente, sem permitir escrita, modificação, ou deletar arquivos;
  - h. sistema operacional deverá sempre carregar aplicativos padrão autorizados ao logon, controlado pelo administrador de rede;



- bb) A CONTRATADA deverá fornecer a respectiva licença de uso definitiva do software de sistema operacional;
- cc) Deverão ser fornecidos teclado e mouse;
- dd) Deverá ser fornecida leitora/gravadora de cartão USB, compatível com o cartão e software de controle de acesso ofertados;
- ee) A estação de cadastramento deverá vir acompanhada de 1 (um) monitor do tipo LED, com tela de 23 polegadas e ao menos as seguintes características: resolução 1920x1080, brilho de 250cd/m<sup>2</sup>, contraste de 1000:1, tempo de resposta de 8ms, ângulo de visão de 175°/175°, portas HDMI e Display Port. Deverá operar em 100 a 230 VAC, 60Hz;
- ff) O fabricante deverá possuir página de suporte técnico na Internet com disponibilidade das últimas versões de drivers, firmwares;
- gg) Garantia de total de 1 (um) ano on-site, disponibilizada pelo fabricante. Anexar declaração específica para este Pregão, comprovando este prazo e informando os dados da empresa autorizada para a prestação dos serviços em garantia comprovando este prazo e informando;
- hh) Os equipamentos deverão, comprovadamente, estar em fase normal de produção/fabricação, no portfólio de produtos do(s) fabricante(s), não sendo aceitos equipamentos descontinuados pelo(s) fabricante(s);
- ii) Equipamentos com previsão de continuidade de fabricação de no mínimo um ano. Caso seja descontinuado no período mencionado deverá ser substituído;
- jj) Anexar documentação técnica detalhada oficial do fabricante contemplado todos os requisitos solicitados;

#### **4.5 Estação de monitoramento de imagens**

- a) Deverá ser um equipamento desenvolvido especificamente para a função de estação tipo cliente (estação de trabalho) que permita monitoramento de CFTV de alta definição (não serão aceitos equipamentos adaptados ou desenvolvidos para outras finalidades);
- b) Gabinete formato torre;
- c) O equipamento cotado deverá ser novo, estar em linha de produção no momento da licitação, sendo possível consultar o site do fabricante para verificação das especificações técnicas;
- d) Deverá possuir pelo menos 1 (um) processador com frequência baseada em processador de pelo menos 2,9 GHz, frequência turbo máx. de pelo menos 4,5 GHz, no mínimo 8 núcleos, no mínimo 12 threads, cache de pelo menos 14,5 MB e pelo menos 16 linhas PCI Express;
- e) Deve possuir processamento gráfico integrado com frequência de base gráfica de pelo menos 320 MHz;
- f) Chipset do mesmo fabricante do(s) processador(es) com suporte a PCI Express 3.0 ou superior com suporte a pelo menos 2 (dois) DIMMs por canal;
- g) Possuir, pelo menos, memória instalada de 16GB DDR4 SDRAM, disposta em 1 (um) pente de 16 GB com capacidade de chegar à pelo menos 64 GB;
- h) Deve possuir pelo menos 2 (dois) canais de memória;
- i) Os canais de memória deverão ser preenchidos obedecendo as regras de máximo desempenho para o sistema conforme recomendação do fabricante do servidor;
- j) Possuir 04 slots DIMM, suporte para módulos de memória DDR4 até pelo menos 2.933 MHz;
- k) Possuir pelo menos 4 (quatro) conectores SATA 6 Gb/s interfaces integradas;



- l) Motherboard deve possuir nativamente pelo menos dois conectores M.2 não sendo aceitos adaptadores (ex.: PCI) para tal funcionalidade por reduzir a taxa de comunicação efetiva;
- m) Deverá possuir 1 (uma) unidade de estado sólido (SSD) com capacidade de, no mínimo, 480 GB SSD onde deverá ser instalado o sistema operacional e o(s) aplicativo(s);
- n) Deverá possuir HD tipo SATA com capacidade de 4TB para armazenamento de dados;
- o) Deverá vir acompanhada de placa de vídeo offboard com memória de 8GB GDDR6, ao menos 2.500 núcleos CUDA, ao menos 2 (duas) portas Display Port e 1 (uma) porta HDMI;
- p) Deve possuir pelo menos 3 (três) portas USB 3.1;
- q) Deve possuir pelo menos uma porta Ethernet RJ-45 com velocidades de pelo menos 1 Gbps;
- r) Não serão aceitos equipamentos com discos rígidos de uso comum para computadores, não fabricados e com características específicas para videomonitoramento, conforme informação do fabricante dos HDDs;
- s) Ventilação apropriada à configuração, com fonte de alimentação de, no mínimo, 500 W reais com fator de correção ativo, bivolt;
- t) A fonte de alimentação deverá possuir faixa de tensão de entrada de 100 a 240V (automático) à 60Hz, interna ao equipamento (não serão aceitos equipamentos que operem em tensão de entrada em 12Vdc ou 24Vdc);
- u) O equipamento deverá possuir ventiladores internos originais do equipamento, necessários para a perfeita refrigeração do sistema interno do servidor na sua configuração máxima;
- v) Deverá suportar pelo menos 2 (duas) baías de 3,5" e pelo menos 2 (duas) SSDs de 2,5";
- w) A temperatura de operação deverá ser de pelo menos 0° a 60°C;
- x) Deve possuir pelo menos um slot PCI Express executando x16;
- y) Equipamento não será aceito caso sejam utilizados discos em gabinetes externos ao servidor;
- z) Deverá possuir sistema operacional Windows Enterprise 10 IoT ou superior, já gravado e totalmente compatível com o equipamento;
- aa) O sistema operacional deverá possuir os recursos (e os eventuais softwares adicionais se necessários) para implementar:
  - a. funcionalidade para bloqueio ao instalar novos app's;
  - b. criptografia dos discos;
  - c. boot seguro;
  - d. suportar geração de consulta de integridade de dispositivos gerenciados;
  - e. autenticação de múltiplos fatores ao fazer logon no servidor;
  - f. controle de atualização do Windows de forma remota e com horário agendado em modo avançado;
  - g. modo leitura de pastas e arquivos somente, sem permitir escrita, modificação, ou deletar arquivos;
  - h. sistema operacional deverá sempre carregar aplicativos padrão autorizados ao logon, controlado pelo administrador de rede;
- bb) A CONTRATADA deverá fornecer a respectiva licença de uso definitiva do software de sistema operacional;
- cc) Deverão ser fornecidos teclado e mouse;
- dd) O fabricante deverá possuir página de suporte técnico na Internet com disponibilidade das últimas versões de drivers, firmwares;
- ee) Garantia de total de 1 (um) ano on-site, disponibilizada pelo fabricante. Anexar declaração específica para este Pregão, comprovando este prazo e informando os dados



da empresa autorizada para a prestação dos serviços em garantia comprovando este prazo e informando os dados da empresa autorizada para a prestação dos serviços em garantia;

- ff) Os equipamentos deverão, comprovadamente, estar em fase normal de produção/fabricação, no portfólio de produtos do(s) fabricante(s), não sendo aceitos equipamentos descontinuados pelo(s) fabricante(s);
- gg) Equipamentos com previsão de continuidade de fabricação de no mínimo um ano. Caso seja descontinuado no período mencionado deverá ser substituído;
- hh) Anexar documentação técnica detalhada oficial do fabricante contemplado todos os requisitos solicitados;

#### **4.6 Nobreak – 6kVA/230V**

- a) Capacidade de potência de saída: 6KVA / 5,4KW;
- b) Tensão nominal de saída: 230V;
- c) Tensão nominal de entrada: 230V (F-N-T);
- d) Tecnologia de conversão online;
- e) Forma de onda senoidal;
- f) Distorção na saída menor que 5%;
- g) Painel LCD para status e controle;
- h) Formato Rack com 4U de altura.

#### **4.7 Switch Core 24 portas UTP**

- a) Deverá ser homologado pela ANATEL;
- b) Deve ser instalado em rack padrão EIA (19”) e possuir kits completos para instalação;
- c) Deve possuir altura máxima de 1 RU;
- d) Deve possuir, no mínimo, 24 (vinte e quatro) portas, 10/100/1000 BaseT full-duplex ativas simultaneamente, autosense com conectores RJ-45 diretamente conectada ao chassi, sem conversores externos, com MDI/MDIX automático;
- e) Deve possuir no mínimo de 4 (quatro) Slots SFP+ (Small Form-factor Pluggable Plus), não populados, para uplink 10 Gigabit Ethernet;
- f) Deve implementar os padrões Ethernet: IEEE 802.3 (Ethernet), 802.3u (Fast Ethernet) e 802.3z, 802.3ab (Gigabit Ethernet), 802.3ae (10 Gigabit Ethernet), IEEE 802.3x (Flow Control), IEEE 802.1ab (LLDP) e LLDP-MED;
- g) Deve Possuir porta console RS-232 com conectores DB9 ou RJ-45;
- h) Deve possuir fonte de alimentação primária interna ao equipamento, que opere com tensões de entrada entre 110 e 220 VAC e suporte frequência entre 50/60hz;
- i) Deve possuir capacidade de encaminhamento no mínimo 120 (cento e vinte) Mpps;
- j) Deve possuir capacidade encaminhamento de tráfego de no mínimo 160 (cento e sessenta) Gbps;
- k) Deve Implementar tabela de endereçamento para, no mínimo, 16000 (dezesesseis mil) endereços MAC;
- l) Deve Implementar no mínimo 4000 (quatro mil) VLANs;
- m) Deve suportar RIPng (RFC 2080) para IPv6
- n) Deve suportar rotas estáticas em IPv4;
- o) Deve suportar rotas RIP em IPv4;
- p) Deve suportar rotas estáticas em IPv6;
- q) Deve suportar rotas RIP em IPv6;



- r) Deve suportar no mínimo 256 rotas IPv4 e 128 rotas IPv6;
- s) Suporte a OSPFv2
- t) Deve implementar IEEE 802.3ad;
- u) Deve implementar IGMP v1, v2, v3 e snooping;
- v) Deve implementar spanning tree, RSTP e MSTP;
- w) Deve implementar DHCP Snooping, DHCP client , DHCP Relay e DHCP server;
- x) Deve implementar Jumbo Frame 9K;
- y) Deve implementar MVRP segundo o padrão IEEE 802.1q;
- z) Deve implementar VRRP (Virtual Router Redundancy Protocol) para prover alta disponibilidade;
- aa) Deve permitir empilhamento;
- bb) Deve Implementar IEEE 802.1p;
- cc) Deve Implementar Rate Limiting;
- dd) Deve implementar gerenciamento de banda de entrada (ingress) e saída (egress);
- ee) Deve possuir algoritmo de enfileiramento: Weighted Round Robin (WRR);
- ff) Suportar Auto QoS para gerenciamento do switch e telefones IP;
- gg) Deve implementar controle fluxo para broadcast, multicast e fluxo desconhecido permitindo fixar o limite por porta.
- hh) Deve permitir o controle de acesso a rede baseado no endereço MAC;
- ii) Deve implementar IEEE 802.1X Port-Based Network Access Control;
- jj) Deve implementar autenticação via portal de visitante nativo do switch;
- kk) Deve Implementar ACL ou outra funcionalidade de filtragem de tráfego por porta TCP/UDP de origem/destino, por endereço MAC de origem/destino, por endereço IP de origem/destino e por valor do campo ToS;
- ll) Deve implementar funcionalidade de Arp Spoof protection;
- mm) Deve implementar recurso de DHCP Server;
- nn) Deve Implementar SSH;
- oo) Deve Implementar SNMP v1, v2c e v3;
- pp) Deve Implementar NTP ou SNTP;
- qq) Deve Implementar Syslog;
- rr) Deve Implementar Radius e TACACS+;
- ss) Deve Implementar espelhamento de tráfego, inclusive entre portas de switches distintos da pilha. Deve permitir espelhar simultaneamente os frames recebidos e transmitidos;
- tt) Deve Implementar Telnet;
- uu) Deve Implementar TFTP ou FTP;
- vv) Deve Implementar configuração via CLI e WEB;
- ww) Deve implementar Sflow ou Netflow v5 ou Netflow v9;
- xx) Deve Implementar RMON;
- yy) Deve Implementar gerenciamento por HTTPS através de acesso direto ao equipamento por web browser padrão;
- zz) Deve suportar, no mínimo, 02 (duas) Imagens do sistema operacional e 2 (dois) arquivos de configuração;
- aaa) Deve ser empilhável com o “Switch Core 8 portas SFP+” e ser fornecido com 1 (um) cabo de empilhamento com velocidade de 10G ou superior, compatível com ambos dos tipos de switch core.

#### **4.8 Switch Core 8 portas SFP+**

- a) Deverá ser homologado pela ANATEL;
- b) Deve ser instalado em rack padrão EIA (19”) e possuir kits completos para instalação;





- c) Deve possuir altura máxima de 1 RU;
- d) Deve possuir no mínimo de 8 (oito) Slots SFP+ (Small Form-factor Pluggable Plus), não populados, para uplink 10 Gigabit Ethernet;
- e) Deve implementar os padrões Ethernet: IEEE 802.3 (Ethernet), 802.3u (Fast Ethernet) e 802.3z, 802.3ab (Gigabit Ethernet), 802.3ae (10 Gigabit Ethernet), IEEE 802.3x (Flow Control), IEEE 802.1ab (LLDP) e LLDP-MED;
- f) Deve Possuir porta console RS-232 com conectores DB9 ou RJ-45;
- g) Deve possuir fonte de alimentação primária interna ao equipamento, que opere com tensões de entrada entre 110 e 220 VAC e suporte frequência entre 50/60hz;
- h) Deve possuir capacidade de encaminhamento no mínimo 120 (cento e vinte) Mpps;
- i) Deve possuir capacidade encaminhamento de tráfego de no mínimo 160 (cento e sessenta) Gbps;
- j) Deve Implementar tabela de endereçamento para, no mínimo, 16000 (dezesesseis mil) endereços MAC;
- k) Deve Implementar no mínimo 4000 (quatro mil) VLANs;
- l) Deve suportar RIPng (RFC 2080) para IPv6
- m) Deve suportar rotas estáticas em IPv4;
- n) Deve suportar rotas RIP em IPv4;
- o) Deve suportar rotas estáticas em IPv6;
- p) Deve suportar rotas RIP em IPv6;
- q) Deve suportar no mínimo 256 rotas IPv4 e 128 rotas IPv6;
- r) Suporte a OSPFv2
- s) Deve implementar IEEE 802.3ad;
- t) Deve implementar IGMP v1, v2, v3 e snooping;
- u) Deve implementar spanning tree, RSTP e MSTP;
- v) Deve implementar DHCP Snooping, DHCP client, DHCP Relay e DHCP server;
- w) Deve implementar Jumbo Frame 9K;
- x) Deve implementar MVRP segundo o padrão IEEE 802.1q;
- y) Deve implementar VRRP (Virtual Router Redundancy Protocol) para prover alta disponibilidade;
- z) Deve permitir empilhamento;
- aa) Deve Implementar IEEE 802.1p;
- bb) Deve Implementar Rate Limiting;
- cc) Deve implementar gerenciamento de banda de entrada (ingress) e saída (egress);
- dd) Deve possuir algoritmo de enfileiramento: Weighted Round Robin (WRR);
- ee) Suportar Auto QoS para gerenciamento do switch e telefones IP;
- ff) Deve implementar controle fluxo para broadcast, multicast e fluxo desconhecido permitindo fixar o limite por porta.
- gg) Deve permitir o controle de acesso a rede baseado no endereço MAC;
- hh) Deve implementar IEEE 802.1X Port-Based Network Access Control;
- ii) Deve implementar autenticação via portal de visitante nativo do switch;
- jj) Deve Implementar ACL ou outra funcionalidade de filtragem de tráfego por porta TCP/UDP de origem/destino, por endereço MAC de origem/destino, por endereço IP de origem/destino e por valor do campo ToS;
- kk) Deve implementar funcionalidade de Arp Spoof protection;
- ll) Deve implementar recurso de DHCP Server;
- mm) Deve Implementar SSH;
- nn) Deve Implementar SNMP v1, v2c e v3;
- oo) Deve Implementar NTP ou SNTP;
- pp) Deve Implementar Syslog;





- qq) Deve Implementar Radius e TACACS+;
- rr) Deve Implementar espelhamento de tráfego, inclusive entre portas de switches distintos da pilha. Deve permitir espelhar simultaneamente os frames recebidos e transmitidos;
- ss) Deve Implementar Telnet;
- tt) Deve Implementar TFTP ou FTP;
- uu) Deve Implementar configuração via CLI e WEB;
- vv) Deve implementar Sflow ou Netflow v5 ou Netflow v9;
- ww) Deve Implementar RMON;
- xx) Deve Implementar gerenciamento por HTTPS através de acesso direto ao equipamento por web browser padrão;
- yy) Deve suportar, no mínimo, 02 (duas) Imagens do sistema operacional e 2 (dois) arquivos de configuração;
- zz) Deve ser fornecido com 16 (seis) mini gbics com velocidade 10Giga para fibras monomodo, para uso nos switches centrais e de borda;
- aaa) Deve ser empilhável com o “Switch Core 24 portas UTP” e ser fornecido com 1 (um) cabo de empilhamento com velocidade de 10G ou superior, compatível com ambos dos tipos de switch core.

#### **4.9 Switch 24 portas PoE**

- a) Deverá ser Homologados pela ANATEL;
- b) Deve ser instalado em rack padrão EIA (19”) e possuir kits completos para instalação;
- c) Deve possuir altura máxima de 1 RU;
- d) Deve possuir, no mínimo, 24 (vinte e quatro) portas, PoE, 10/100/1000 Base T full-duplex ativas simultaneamente, autosense com conectores RJ-45 diretamente conectada ao chassi, sem conversores externos, com MDI/MDIX automático;
- e) Deve possuir no mínimo de 2 (dois) Slots SFP (Small Form-factor Pluggable), não populados, para uplink Gigabit Ethernet;
- f) Deve possuir no mínimo de 2 (dois) Slots SFP+ (Small Form-factor Pluggable Plus), não populados, para uplink 10 Gigabit Ethernet;
- g) Deve ser compatível com o padrão IEEE 802.3af e IEEE 802.3at;
- h) Deve fornecer pelo menos 180 Watts de potência para as portas PoE;
- i) Deve implementar os padrões Ethernet: IEEE 802.3 (Ethernet), 802.3u (Fast Ethernet) e 802.3z, 802.3ab (Gigabit Ethernet), 802.3ae (10 Gigabit Ethernet), IEEE 802.3x (Flow Control), IEEE 802.1ab (LLDP) e LLDP-MED;
- j) Deve Possuir porta console RS-232 com conectores DB9 ou RJ-45;
- k) Deve possuir fonte de alimentação primária interna ao equipamento, que opere com tensões de entrada entre 110 e 220 VAC e suporte frequência entre 50/60hz.

#### **4.10 Cabo UTP 4 pares categoria 6**

- a) Sistemas de Cabeamento Estruturado para tráfego de voz, dados e imagens, segundo requisitos da norma ANSI/TIA-568 Categoria 6, para cabeamento primário e secundário entre os painéis de distribuição (Patch Panels) ou conectores nas áreas de trabalho, em sistemas que requeiram grande margem de segurança sobre as especificações normalizadas para garantia de suporte às aplicações futuras.
- b) Possuir certificado de performance elétrica (VERIFIED) pela UL ou ETL, conforme especificações da norma ANSI/TIA-568 CATEGORIA 6;
- c) O cabo utilizado deverá possuir certificação Anatel;



- d) Possuir impresso na capa externa nome do fabricante, marca do produto, e sistema de rastreabilidade que permita identificar a data de fabricação dos cabos.
- e) Possuir certificação de canal para 6 conexões por laboratório de 3ª. Parte;
- f) Deve atender ao código de cores especificado abaixo:
  - a. par 1: azul-branco, com uma faixa azul (stripe) no condutor branco;
  - b. par 2: laranja-branco, com uma faixa laranja (stripe) no condutor branco;
  - c. par 3: verde-branco, com uma faixa verde (stripe) no condutor branco;
  - d. par 4: marrom-branco, com uma faixa marrom (stripe) no condutor branco.
- g) Capa externa em composto antichamas, com baixo nível de emissão de fumaça (LSZH);
- h) Deverá ser apresentado através de catálogos ou proposta técnica de produto do fabricante, testes das principais características elétricas em transmissões de altas velocidades (valores típicos) de ATENUAÇÃO (dB/100m), NEXT (dB), PSNEXT (dB), RL (dB), ACRF (dB), para frequências de 250Mhz.

#### **4.11 Patch cord CAT.6 RJ45/RJ45**

- a) Sistemas de Cabeamento Estruturado para tráfego de voz, dados e imagens, segundo requisitos da norma ANSI/TIA/EIA-568 Categoria 6. Previstos para cabeamento horizontal ou secundário, uso interno, em ponto de acesso à área de trabalho para interligação do hardware de comunicação do usuário às tomadas de conexão da rede e também nas salas de telecomunicações, para manobras entre os painéis de distribuição (Patch panels) e os equipamentos ativos da rede (hubs, switches, etc.);
- b) Patch Cord para interligação entre a “tomada lógica” e “equipamento” ou para manobra na Sala de Telecomunicações;
- c) Possui Certificação UL ou ETL LISTED;
- d) Deve ter duas certificações Anatel conforme regulamento da entidade: a do cabo flexível conforme classe de flamabilidade e do cordão de manobra;
- e) Deve cumprir com os requisitos quanto à taxa máxima de compostos que não agridam ao meio ambiente conforme a diretiva RoHS;
- f) Deverão ser montados e testados em fábrica, com garantia de performance;
- g) O acessório deve ser confeccionado em cabo par trançado, U/UTP Categoria 6 (Unshielded Twisted Pair), 24 AWG x 4 pares, composto por condutores de cobre flexível, multifilar, isolamento e capa externa em material não propagante à chama tipo LSZH, conectorizados à RJ-45 macho Categoria 6 nas duas extremidades, estes conectores (RJ-45 macho), devem atender às especificações contidas na norma ANSI/TIA/EIA-568 Categoria 6, ter corpo em material termoplástico de alto impacto não propagante à chama, que atenda a norma UL 94 V-0 (flamabilidade), possuir vias de contato produzidas em bronze fosforoso com camadas de 2,54 µm de níquel e 1,27 µm de ouro, para a proteção contra oxidação, garras duplas para garantia de vinculação elétrica com as veias do cabo;
- h) O Cabo utilizado deve apresentar Certificação ETL em conformidade com a norma ANSI/TIA/EIA-568 CATEGORIA 6 (stranded cable);

#### **4.12 Patch panel**

- a) Sistemas de cabeamento estruturado, uso interno, para cabeamento horizontal ou secundário, em salas de telecomunicações (cross-connect) onde permite a montagem de conectores/adaptadores para UTP, fibra, coaxial e aplicações multimídia (áudio e vídeo).
- b) Patch panel descarregado;
- c) Apresentar uma capacidade de 24 portas em 1 unidade de rack;



- d) Painel frontal em aço com local para inserção de porta etiquetas de identificação em acrílico para proteção;
- e) Acabamento em pintura epóxi de alta resistência a riscos na cor preta resistente e protegido contra corrosão;
- f) Apresenta largura de 19", conforme requisitos da norma ANSI/TIA/EIA- 310E;
- g) Deverá ser fornecido com conectores RJ-45 (Fêmea) Categorias 6;
- h) Deve possuir identificação do fabricante no corpo do produto;
- i) Deve possuir identificação dos conectores na parte frontal do patch panel (facilitando manutenção e instalação);
- j) Possuir local para aplicação de ícones de identificação (para codificação), conforme requisitos da norma ANSI/TIA/EIA-606-A;
- k) Fornecido de fábrica com ícones de identificação (nas cores azul e vermelha).

#### **4.13 Distribuidor Interno Óptico (DIO) até 12 Fibras**

- a) Distribuidor óptico para até 12 fibras de parede ou prateleira;
- b) Indicado para uso interno;
- c) Deve ter capacidade de gerenciar até 12 fibras ópticas;
- d) Deve permitir utilizar conectores LC ou SC e em acordo com os demais componentes da solução;
- e) Deve atender ao padrão de conectores utilizados nos demais componentes da solução;
- f) Deve suportar cabos ópticos de construção tight ou loose;
- g) Deve acompanhar o distribuidor óptico, sistema de bandeja de emenda, protetor de emenda, extensões ópticas, adaptadores e braçadeiras plásticas;
- h) Fabricado em plástico de alta resistência a impactos;
- i) Possuir compartimento interno para acomodar e proteger o storage de pigtails.

#### **4.14 Cabo Óptico "Tight Buffer" Multimodo 10 gigabit até 320m**

- a) Sistemas de Cabeamento Estruturado para tráfego de voz, dados e imagens em interligações ópticas internas, em backbones de interligações verticais entre armários de distribuição principal e de andares ou para atendimento às áreas de trabalho em sistemas FTTD (Fiber To The Desk).
- b) Permitir aplicação em ambiente interno, com construção do tipo "tight", composto por fibras ópticas multimodo especiais para aplicações 10 gigabit com revestimento primário em acrilato e revestimento secundário em material polimérico colorido (900 µm), reunidas e revestidas por fibras sintéticas dielétricas para suporte mecânico (resistência à tração) e cobertas por uma capa externa em polímero especial para uso interno;
- c) Composto por no mínimo 4 fibras;
- d) Permitir aplicações 10 gigabit em até 320 metros (OM3);
- e) Apresentar Certificação UL;
- f) Apresentar Certificação ANATEL;
- g) Este cabo deverá ser constituído por fibras multimodo 50/125 µm;
- h) Ser totalmente dielétrico, garantindo a proteção dos equipamentos ativos de transmissão contra propagação de descargas elétricas atmosféricas;
- i) Possuir raio mínimo de curvatura de 40 mm após a instalação e de 100mm durante a instalação;
- j) Temperatura de operação de 10 a 40 graus;
- k) Possuir impresso na capa externa nome do fabricante, marca do produto, data de fabricação, gravação sequencial métrica (em sistema de medida internacional SI);



- l) Aplicação em sistemas de cabeamento intrabuilding, segundo as normas ANSI EIA/TIA 568.

#### **4.15 Cordão Óptico Multimodo 50.0µm OM3**

- a) Sistemas de cabeamento estruturado para tráfego de voz, dados e imagens, segundo requisitos da norma ANSI/TIA/EIA-568-B.3 uso interno para cabeamento vertical ou primário em salas ou armários de distribuição principal, ou para cabeamento horizontal ou secundário em salas de telecomunicações (cross-connect) na função de interligação de distribuidores e bloqueios ópticos com os equipamentos de rede;
- b) Este cordão deverá ser constituído por um par (duplex) de fibras ópticas multimodo 50/125µm OM3, tipo “tight”;
- c) Utilizar padrão “zip-cord” de reunião das fibras para diâmetro de 2mm;
- d) A fibra óptica deste cordão deverá possuir revestimento primário em acrilato e revestimento secundário em PVC;
- e) Sobre o revestimento secundário deverão existir elementos de tração e capa em PVC não propagante à chama;
- f) As extremidades deste cordão óptico duplo devem vir devidamente conectorizadas e testadas de fábrica;
- g) Possuir impresso na capa externa nome do fabricante, identificação do produto e data de fabricação;
- h) Ser disponibilizado nas opções de terminações com conectores LC ou SC e em acordo com os demais componentes da solução;
- i) O cabo (cordão) óptico deverá possuir certificação ANATEL.

#### **4.16 Rack piso 44U**

- a) Rack padrão 19”;
- b) Altura de 44Us;
- c) Profundidade de 700 a 900mm;
- d) Possuir sistema de ventilação;
- e) Possuir planos frontais e traseiros, perfurados para utilização de porca gaiola;
- f) Possuir porta frontal em vidro temperado ou acrílico, com fechadura tipo cilindro;
- g) Possuir tampas laterais em aço com fecho rápido;
- h) Ser fornecido com pés niveladores para alinhamento de piso;
- i) Possuir a possibilidade de instalação de rodízios giratórios, facilitando a movimentação do rack;
- j) Possuir grau de proteção IP20;
- k) Possuir acabamento feito com pintura epóxi-pó micro-texturizada preta;
- l) Fornecido com 1 régua com 8 tomadas 1U 19”.

#### **4.17 Rack parede 12U**

- a) Altura de 12Us;
- b) Profundidade de 570 a 670mm;
- c) Possuir sistema de ventilação;
- d) Possuir planos frontais e traseiros, perfurados para utilização de porca gaiola;
- e) Possuir porta frontal em vidro temperado ou acrílico, com fechadura tipo cilindro;
- f) Possuir tampas laterais em aço com fecho rápido;
- g) Possuir grau de proteção IP20;



- h) Possuir acabamento feito com pintura epóxi-pó micro-texturizada preta;
- i) Fornecido com 1 régua com 8 tomadas 1U 19".

#### 4.18 Servidor de Gerenciamento Gráfico

- a) Microcomputador padrão estação de trabalho;
- b) Processador deverá ser ao menos Intel i7 com 12 núcleos e 20 threads, ou equivalente;
- c) Requisitos mínimos de memória RAM: 16GB DDR4;
- d) Requisitos mínimos para capacidade de armazenamento: 512GB SSD;
- e) Placa gráfica off-board com ao menos 4GB DDR5;
- f) Teclado e mouse com fio do mesmo fabricante do equipamento;
- g) Sistema Operacional Windows 11 Pro, versão em língua portuguesa;
- h) Deve possuir placa mãe com BIOS desenvolvida pelo próprio fabricante do equipamento.

#### 4.19 Monitor para videowall

- a) O equipamento deverá ser novo, de primeiro uso, e ser compatível com as características mínimas abaixo descritas;
- b) Monitor profissional, apropriado ao uso em *videowall*, com molduras pretas e com tela LED colorido, *full HD*, com tratamento anti-reflexivo;
- c) Tamanho da tela deverá ser de 55" (diagonal visual aproximada);
- d) O formato da tela deverá ser 16:9 (*widescreen*);
- e) Deve possuir ângulos de visão mínimo de 178° (horizontal e vertical);
- f) Deve possuir resolução de no mínimo 1920X1080;
- g) Deve possuir brilho de, no mínimo, 500 cd/m<sup>2</sup>;
- h) Deve possuir contraste mínimo de 1.000 por 1 ou superior;
- i) Tempo de resposta máximo de 12 ms;
- j) Conexões de entrada: no mínimo, 02 HDMI, 01 DVI-D, 01 RJ45 e 01 RS232C;
- k) Conexões de saída: no mínimo, 01 DVI ou *Display Port* e 01 RS232C ou 01 RJ45;
- l) Deverão possuir fonte interna de alimentação/energia com seleção automática de tensão 100~240VAC, com frequência de 50/60 Hz;
- m) Deve possuir borda com no máximo 1,8mm na junção, tanto na horizontal quanto na vertical, medida de pixel a pixel;
- n) A carenagem do monitor deve ter estrutura reforçada e adequada para suportar a instalação no suporte do *videowall* no padrão VESA;
- o) Deve ser capaz de operar em temperatura ambiente entre 0°C e 40°C, e em umidade relativa do ar de 10% a 80%;
- p) Deve permitir modo de operação 24X7 (vinte e quatro horas por dia / sete dias por semana);
- q) Deve permitir a instalação e funcionamento, em *videowall*, na posição horizontal e/ou vertical;
- r) Deve possuir sensor de temperatura;
- s) Deve ser fornecido com, no mínimo, cabo de alimentação e controle remoto com pilhas, em quantidade suficiente para seu funcionamento e manual de instruções;
- t) Deverão ser fornecidos todos os cabos necessários para conexão com o equipamento controlador de *videowall* fornecido;



23130000020951

- u) Todo monitor deve ser fornecido com módulo de suporte pantográfico que permita a manutenção frontal e a extração individual do monitor. O suporte deve permitir o ajuste nos três eixos;
- v) Cada suporte deverá suportar ao menos 50kg de carga.