4.50.1.19. Deverá possuir proteção através de filtragem de IP

4.50.1.20. Deverá possuir função para análise do tráfego de dados saintes e entrantes das interfaces de redes;

4.50.1.21. Possibilitar montagem em mesa ou bandeja de rack;

4.50.1.22. Deverá possuir ao menos os certificados FCC e CE;

4.50.1.23. Deverá permitir configuração de entrada e saída de horário de verão programada;

4.50.1.24. Deverá possuir fonte de alimentação redundante interna bivolt automático 100-240VAC, 50/60Hz; bem como seu consumo deverá ser de no máximo 25W;

4.50.1.25. Deverá possuir a menos 4 níveis de configuração de qualidade de imagem por canal;

4.50.1.26. Deverá suportar planificação de câmeras do tipo fisheye;

4.50.1.27. Possuir programação para captura e envio de alertas e fotos por e-mail;

4.50.1.28. A operação remota deverá possibilitar o monitoramento, configuração do sistema, reprodução, download de arquivos gravados e informações sobre registros;

4.50.1.29. Deverá possuir acessibilidade via web browser com o uso de no mínimo 2 navegadores diferentes.

4.51. FORNECIMENTO DE GRAVADOR DE IMAGENS NVR

4.51.1. O sistema deverá prever configurações mínimas de hardware:

4.51.1.1. O Gravador de Vídeo em Rede de Alta Definição deverá ser um hardware exclusivo concebido e dedicado para esta função, e vir pré-carregado com o firmware mais atual do fabricante;

4.51.1.2. O Gravador de Vídeo em Rede de Alta Definição deverá ser compatível com a infraestrutura de TI existente e não requerer cabeamento especial para sua inserção na rede;

4.51.1.3. O Gravador de Vídeo de Rede em Alta Definição deverá rodar em sistema operacional dedicado (firmware);

4.51.1.4. O Gravador de Vídeo de Rede de Alta Definição deverá ser escalável, ou seja, deverá permitir expansões de armazenamento;

4.51.1.5. O Gravador de Vídeo de Rede de Alta Definição deverá suportar a taxa mínima de gravação de 400Mbps de dados de imagem;

4.51.1.6. O Gravador de Vídeo de Rede de Alta Definição deverá suportar até 150 canais de câmera;

4.51.1.7. O Gravador de Vídeo de Rede de Alta Definição deverá oferecer a habilidade de troca entre fonte de energia enquanto ligados;

4.51.1.8. O Gravador de Vídeo de Rede de Alta Definição deverá possuir pelo menos 04 portas Ethernet Gigabit;

4.51.1.9. O Gravador de Vídeo de Rede de Alta Definição deverá obedecer ao padrão dos racks de servidores de 19";

4.51.1.10. Capacidade de Armazenamento mínima (efetiva) de 1.0TB, expansível até 64TB de armazenamento total.

4.51.1.11. Deverá possuir 3 anos de garantia do fabricante.

4.51.2. O Sistema de circuito fechado de televisão deverá ser uma solução de alta performance e escalonável, podendo ser utilizado em sistema de pequeno, médio e grande porte, ou até mesmo em missões críticas, suportando trabalhar 24/7/365, com alta confiabilidade podem chegando até 10.000 câmeras em um único servidor. O sistema será composto, basicamente, por câmeras de vídeo de alta tecnologia instaladas em pontos estratégicos, de modo a permitir a vigilância e o monitoramento dos ambientes em questão visando preservar o ambiente.

4.51.3. O sistema deverá estar licenciado para 32 câmeras;

4.51.4. O sistema deverá ser uma solução completa de vídeo digital IP e transmitindo essas informações aos servidores de gravação e estações de monitoramento através protocolo IP (Internet Protocol).

4.51.5. O sistema deverá permitir uma estrutura de plataforma verdadeiramente aberta e flexível sobre IP onde, que permita a utilização de câmeras IP, equipamentos de rede, servidores de gerenciamento e gravação, estações de monitoramento, analíticos, integração com sistema de gestão e subsistemas de armazenamento padrões de mercado, fornecidos por diversos fabricantes, e que facilitem a integração com as infraestruturas de TI existentes.

4.51.5.1. O Sistema deverá permitir ao operador a visualização das imagens de todas as câmeras cujo acesso é permitido, conforme níveis hierárquicos definidos no sistema, em tempo real, simultaneamente à gravação.

4.51.6. O sistema deverá fazer leitura especificas das imagens de movimentos de objetos alteração de imagens por períodos distintos, realizar movimentações automáticas das câmeras configuráveis por período distintos, analisar aglomerações em horários distintos e enviar alertas aos operadores.

4.51.7. O sistema deverá ser capaz de realizar o registro digital, de alta qualidade, das imagens de todas as câmeras, com recursos para gerenciamento de armazenamento dos arquivos resultantes através de sistema de gerenciamento de arquivos de vídeo, constituindo solução abrangente, escalonável e modular.

4.51.8. O Sistema deverá possuir uma arquitetura totalmente distribuída, de modo que quando o backbone da rede fique inoperante, os equipamentos assumam a gestão, para que o sistema continue trabalhando normalmente. E quando o backbone foi restabelecido o sistema volte funcionar normalmente com a estrutura antes configurada.

4.51.9. O sistema deverá possuir uma gestão de eventos, que possa ser redundante e escalonável podendo chegar até 60.000 eventos de entrada.

4.51.10. O Eventos do sistema deverá permitir a combinação de macros para execução de tarefas.

4.51.11. O sistema deverá possuir um sistema de gravação redundante, com recuperação automática sem a ação do operador.

4.51.12. O Sistema deverá suportar no mínimo os sistemas operacionais:

4.51.12.1. Windows 7 SP1 Professional Edition 32/64 bits

4.51.12.2. Windows 10

4.51.12.3. Windows Server 2008 R2 Enterprise Standard Edition 64 bits

4.51.12.4. Windows Server 2012 R2 Enterprise Standard Edition 64 bits

4.51.12.5. Windows Server 2016

4.51.13. O Sistema deverá possibilitar configurar a gravação no cartão SD da câmera para câmeras, que suporte gravação em cartão SD através do OnVif.

4.51.14. O Sistema deverá possuir o gerenciamento de pop-ups de vídeo na estação cliente

4.51.15. Deverá permitir a configuração independente de monitores ou matriz de vídeo para pop-ups permanentes e por alarme.

4.51.16. A Central de Segurança deve ter a possibilidade de organizar automaticamente, reordenar e reduzir o tamanho dos pop-ups de vídeo de alarme que são redirecionados para o monitor local.

4.51.17. O Sistema deverá suporta fluxos de vídeo H.265 da mesma forma que suporta o codificador H.264 para:

4.51.17.1. Transmissão ao vivo.

4.51.17.2. Gravação local e remota.

4.51.17.3. Reprodução

4.51.17.4. Autenticação de vídeo.

4.51.17.5. Extração de dados de vídeo (para evidência de CD).

4.51.18. O Sistema de gravação deverá sincronizar os gravadores primários e redundantes, para que envie as informações das falhas para as câmeras.

4.51.19. O sistema deverá possuir uma gestão de gravação com a possibilidade de registrar os seguintes eventos:

4.51.19.1. Vídeo

4.51.19.2. Áudio

4.51.19.3. Dados Externos

4.51.19.4. Metadados

4.51.19.5. Dados Analíticos

4.51.19.6. Todos sincronizados com o Vídeo

4.51.20. Toda a gravação do sistema deve possuir as seguintes formas de gravação.

4.51.20.1. Gravação contínua

4.51.20.2. Gravação de Alarme (pré/pós)

4.51.20.3. Gravação por demanda

4.51.20.4. Gravação por eventos de alarme

4.51.20.5. Gravação através de métodos via SDK

4.51.21. O sistema deverá permitir a utilização do kit de desenvolvimento de software (SDK), de modo que possa personalizar a interface do VMS e reprodução de vídeos através de dispositivos móveis.

4.51.22. O sistema deverá possuir um plug-in Kit de desenvolvimento (PDk),

4.51.23. O sistema deverá possuir dispositivos de armazenamento de Vídeo aonde o vídeo das câmeras IP é armazenado para duração específica. Os dispositivos de armazenamento poderão ser discos rígidos internos ou sistemas de armazenamento RAID diretamente conectados aos gravadores ou poderão ser sistemas de armazenamento conectado na rede (NAS) ou redes para armazenamento (SAN) gerenciadas desde os servidores de armazenamento de vídeo.

4.51.24. O Sistema deverá possuir a possibilidade de trabalhar com duas configurações:

4.51.24.1. Uma interface de usuário única;

4.51.24.2. Ou uma interface personalizada onde o usuário pode criar a sua própria interface, através do SDK, montando o seu um sistema de Gerenciamento de vídeo (VMS), o SDK deverá incluir na biblioteca de amostras de aplicação com código fonte para facilitar o desenvolvimento rápido da Interface de Usuário;

4.51.24.3. O SDK deverá permitir componentes de software orientados a objetos, e os elementos controláveis do sistema deverão ter os seguintes itens;

4.51.24.3.1. Controle completo de Gerenciamento de Eventos.

4.51.24.3.2. Controle completo de Gerenciamento de Equipamentos de Vídeo, verificação do bem-estar do sistema e gerenciamento remoto.

4.51.24.3.3. Controle completo das comunicações seriais para as câmeras PTZ.

4.51.24.3.4. Controle completo das entradas de alarme e saídas de relay.

4.51.24.3.5. Controle completo de gerenciamento de armazenamento de vídeo incluindo localização, recuperação e gerenciamento de tempo.

4.51.24.3.6. Codificação completa de vídeo, decodificação, controle de reprodução e gerenciamento.

4.51.24.3.7. Codificação completa de áudio, decodificação, controle de reprodução e gerenciamento.

4.51.25. O Sistema deverá suportar um Kit de Desenvolvimento de Plug-In (Plug-In Development Kit (PDK)) que permita a terceiras empresas de integração com o sistema do fabricante a capacidade de ligar diretamente serviços de análise de vídeo dentro da Plataforma de Vídeo Inteligente. Esses serviços poderão ser executados diretamente nos dispositivos da PLATAFORMA DE VÍDEO INTELIGENTE ou permitir interconexão direta (via IP) à PLATAFORMA DE VÍDEO INTELIGENTE para alarmes, chamado do vídeo e funções de monitoramento do sistema.

4.51.26. O Sistema deverá consistir dos seguintes componentes funcionais:

4.51.27. O Sistema Operacional de Vídeo deverá gerenciar serviços necessários para integrar todos os dispositivos do sistema em uma solução unificada de vídeo:

4.51.27.1. Serviços de Rede

4.51.27.1.1. Protocolos de Rede.

4.51.27.1.2. Tipo de Serviço.

4.51.27.1.3. Controle de Largura de Banda.

4.51.27.2. Serviços de Verificação do estado do sistema deverão disponibilizar em tempo real ao operados as seguintes informações:

4.51.27.2.1. Gerenciamento do Disco: cheio, localização, capacidade, estado;

4.51.27.2.2. Status: temperatura, velocidade do ventilador e estado, estado da entrada de vídeo (habilitada, falha, perda de vídeo);

4.51.27.2.3. Status de Rede: atividade de pacote, uso da banda, estatísticas de dispositivo de rede;

4.51.27.4. Serviços de Gerenciamento de Dispositivo deverão incluir configuração de hardware, módulos opcionais, configuração de disco rígido, configuração de entrada/saída e configuração de canal de áudio.

4.51.27.4. Cópia da configuração do dispositivo mantida tanto no dispositivo como um Serviço de Configuração Central.

4.51.27.5. Serviços de Segurança do Sistema

4.51.27.5.1. Versão do Software, Versão do firmware, Versão do driver.

4.51.27.6. Serviços de Atualização do Dispositivo.

4.51.27.6.1. Automática ou manualmente atualizar os dispositivos e sistema operacional na base da versão atual do software.

4.51.27.7. Serviços de Configuração Central deverão trabalhar conjuntamente com o sistema operacional de vídeo, permitindo as seguintes configurações:

4.51.27.7.1. Configuração remota do dispositivo desde uma ou mais estações de operador.

4.51.27.7.2. As configurações remotas deverão incluir:

4.51.27.7.2.1. Frequências de gravação por canal de vídeo individual.

4.51.27.7.2.2. Frequências de dados por canal de vídeo individual.

4.51.27.7.2.3. Tamanhos de imagem por canal de vídeo individual.

4.51.27.7.2.4. Ajustes de qualidade por canal de vídeo individual.

4.51.27.7.2.5. Localizações de armazenamento por canal de vídeo individual (aonde o vídeo para canais independentes será gravado, seja internamente na unidade ou remotamente fora da unidade).

4.51.27.7.2.6. Configurações de codificador/decodificador por canal de vídeo individual, se o dispositivo suportasse as duas capacidades por canal de vídeo.

4.51.27.7.2.7. Modos de gravação por canal de vídeo individual, os quais deverão incluir: Contínuo, Detecção de Atividade Unicamente, Evento de Alarme Unicamente e modos programáveis que combinem modos: Contínuo, Detecção de Atividade e Eventos de Alarme.

4.51.27.7.2.8. Configuração de canal de áudio e canal de vídeo associado.

4.51.27.7.2.9. Configuração de entrada de alarme de dispositivo e comportamento, incluindo ativação/desativação da entrada de alarme e períodos programados de ativação/desativação.

4.51.27.7.2.10. Configuração de saída de dispositivo (saída relay) e comportamento.

4.51.27.7.2.11. Configuração de canal de vídeo, porta de controle e protocolo PTZ para as câmeras PTZ.

4.51.27.7.2.12. Parâmetros de Classe de Serviço de Rede.

4.51.27.7.2.13. Atualização automática de um dispositivo se perder a sua configuração ou substituição de um dispositivo por um mais recente por necessidades de serviço ou reparo.

4.51.27.7.2.14. Capacidade de guardar as configurações de dispositivo separadas do dispositivo na base de dados do Serviço de Configuração Central.

4.51.27.8. Os Serviços de Gerenciamento de Alarme e Eventos deverão controlar o comportamento e processamento dos eventos de alarme no hardware e deverão permitir:

4.51.27.8.1. Mapeamento das entradas de hardware do dispositivo às saídas de hardware do dispositivo.

4.51.27.8.2. Mapeamento das entradas de hardware do dispositivo às saídas de hardware de qualquer outro dispositivo na rede.

4.51.27.8.3. Encadeamento de múltiplos eventos de entrada de hardware de um ou mais dispositivos de rede a uma ou mais saídas de hardware de qualquer dispositivo na rede.

4.51.27.8.4. Mapeamento dos eventos de software incluindo detecção de atividade, manutenção de câmera, eventos de verificação do bem-estar do sistema a uma ou mais saídas de hardware.

4.51.27.9. O Sistema deverá permitir gerar eventos de alarmes dentro da Plataforma de vídeo inteligente tais como:

4.51.27.9.1. Alarmes de Porta (porta forçada, porta bloqueada, pré-alarme)

4.51.27.9.2. Alarmes de leitora (cartão inválido, cartão perdido, cartão suspenso, cartão desconhecido, violação de antipassback, coação).

4.51.27.9.3. Alarmes de entrada digital;

4.51.27.10. O Sistema deverá permitir que os eventos possam ser agrupados, de forma que todos os alarmes de porta de uma simples porta sejam tratados como um evento único dentro do sistema.

4.51.27.11. O Sistema poderá gerar ações de respostas do sistema baseados nos eventos de alarme original tais como;

4.51.27.11.1. Ativação de saídas de hardware.

4.51.27.11.2. Chamar uma ou mais fluxos binários de câmeras ao vivo para apresentar ao operador e/ou saídas de monitores selecionados.

4.51.27.11.3. Ativar presets de câmeras em uma ou mais câmeras.

4.51.27.11.4. Gerar um evento no log de eventos do sistema.

4.51.27.11.5. Gerar um evento em tempo real para o operador na área de display da interface de usuário (GUI)

4.51.27.12. O Sistema deverá possuir um serviço de fail-over, baseado na base de dados de eventos de forma que se o lugar primário aonde são executados os Serviços de Gerenciamento de Eventos falha, até no máximo de quatro lugares adicionais poderão ser mantidos para automaticamente assumir as responsabilidades do Gerenciamento de Eventos. Se o segundo lugar falhe, as responsabilidades irão para o terceiro lugar, etc. Assim que tiver atualizações na lista de ações do Gerenciador de Eventos, todos os Gerenciadores redundantes deverão ser atualizados.

4.51.27.13. O sistema deverá possuir um serviço de relatório do sistema, onde vários sistemas de alarmes e ações dos operadores, serão armazenadas em logs, para efeitos de auditoria.

4.51.27.13.1. Os eventos que forem reportados poderão ser pesquisados por intervalo de data/hora, por operador, por tipo de evento, por modificações baseadas em tipo de evento específico entre outros.

4.51.27.13.2. Todas as atividades reportadas e recuperadas dos logs deverão incluir as seguintes informações

4.51.27.13.3. Eventos de Alarme

4.51.27.13.3.1. Entradas de hardware.

4.51.27.13.3.2. Detecção de Atividade.

4.51.27.13.3.3. Eventos de detecção de manutenção de câmera.

4.51.27.13.3.4. Dispositivos de detecção Plug-in.

4.51.27.13.4. Eventos Iniciados por Operador

4.51.27.13.4.1. Entrada ao Sistema.

4.51.27.13.4.2. Mudanças/alterações às configurações de dispositivo.

4.51.27.13.4.3. Eventos de gravação manual.

4.51.27.13.4.4. Eventos de exportação de vídeo, os quais incluem gravar clips, gravar imagens e exportar para CD/DVDs.

4.51.27.13.4.5. Backup da base de dados (configuração, alarme, operador).

4.51.27.13.5. Eventos do Sistema

4.51.27.13.5.1. Eventos do Dispositivo.

4.51.27.13.5.2. Perda de vídeo.

4.51.27.13.5.3. Câmera fora de foco.

4.51.27.13.5.4. Câmera virou.

4.51.27.13.5.5. Câmera coberta.

4.51.27.13.5.6. Unidade não gravando ou fora de linha.

4.51.27.13.5.7. Falha de Disco rígido de vídeo.

4.51.27.13.5.8. Estado de Temperatura.

4.51.27.13.5.9. Voltagem do equipamento.

4.51.27.13.5.10. Falha da Fonte de Alimentação.

4.51.27.13.5.11. Eventos de armazenamento externo desde unidades DAS conectadas aos gravadores e servidores de gravação central.

4.51.27.13.5.12. Unidade fora de linha.

4.51.27.13.5.13. Falha de Disco Rígido.

4.51.27.13.6. O sistema deverá possuir uma interface de usuário com as seguintes características mínimas;

4.51.27.13.6.1. Configuração de dispositivos.

4.51.27.13.6.2. Zonas de Câmeras, Grupos de Câmeras.

4.51.27.13.6.3. Privilégios de Acesso de Usuário.

4.51.27.13.6.4. Eventos e Gerenciamento de Eventos.

4.51.27.13.7. Base de dados de Dispositivo, Software e Configuração de Usuários;

4.51.27.13.7.1. Localização da base de dados pode ser em uma estação cliente ou em um servidor dedicado.

4.51.27.13.7.2. A base de dados deverá ser capaz de ter um backup e a reestabelecer uma base de dados antiga usando uma opção do sistema.

4.51.27.13.7.3. A configuração do dispositivo poderá ser administrada por meio do GUI com a configuração acessível usando diálogos, fichas e clicando o botão direito do mouse para acesso rápido.

4.51.27.13.7.4. O sistema deverá permitir, para um novo dispositivo, um Assistente de Configuração que automaticamente detectará os componentes do sistema instalados para o

dispositivo codificador/decodificador/gravador e perguntar para o usuário sobre os componentes mínimos necessários.

4.51.27.13.8. Base de dados do Gerenciador de Eventos

4.51.27.13.8.1. A localização da base de dados pode ser em uma estação cliente ou em um servidor dedicado.

4.51.27.13.8.2. A base de dados deverá ser capaz de ser copiada em backup e restaurar uma base de dados antiga.

4.51.27.13.9. Os elementos de Configuração do Usuário deverão incluir as seguintes características mínimas:

4.51.27.13.9.1. Até 300 diferentes operadores no sistema.

4.51.27.13.9.2. O usuário poderá estar configurado na lista de Administradores ou Operador;

4.51.27.13.9.3. Os Administradores deverão ter privilégios para todas as câmeras e opções de configuração.

4.51.27.13.9.4. Os operadores deverão estar restritos como as seguintes configurações:

4.51.27.13.9.5. Sem acesso para ajustes de configuração ou capacidade de alterar horários, acesso às câmeras ou monitorar grupos.

4.51.27.13.9.6. Somente permitidos para ver as câmeras, monitores ou alarmes que são individualmente disponíveis para eles/elas.

4.51.27.13.97. Poder gerar ou apagar ciclos de câmera e múltiplas vistas de câmeras para as câmeras as quais têm acesso. Porém, não poderá apagar vistas de câmeras múltiplas ou ciclos de câmeras criadas por um Administrador.

4.51.27.13.9.8. Funções adicionais que podem ser controladas independentemente pelo Operador incluem:

4.51.27.13.9.8.1. Controle PTZ.

4.51.27.13..9.8.2. Definir presets de câmeras PTZ.

4.51.27.13.9.8.3. Iniciar/Parar gravação sob demanda de vídeo em estações cliente, assim como a capacidade de visualizar as gravações de vídeo sob demanda.

4.51.27.13.8.4. Gravar imagens estáticas de vídeo gravado ou ao vivo.

4.51.27.13.8.5. Capacidade de visualizar o vídeo arquivado.

4.51.27.13.8.6. Capacidade de habilitar/desabilitar alarmes.

4.51.27.13.8.7. Executar uma transmissão de áudio.

4.51.27.13.8.8. Visualizar o log histórico de eventos.

4.51.27.13.9.9. Nas opções de câmeras deverão incluir as seguintes características como mínimo:

4.51.27.13.9.9.1. Suportar uma população de até 10,000 câmeras.

4.51.27.13.9.9.2. Suportar pelo menos 100 grupos de câmeras com até 100 câmeras por grupo.

4.51.27.13.9.3. Programar e executar presets de câmeras PTZ.

4.51.27.13.9.4. Capacidade de dirigir a saída direta de uma câmera para um monitor analógico segundo especificado no projeto.

4.51.27.13.9.10. Fluxo Binário Ao Vivo deverá ter as seguintes características mínimas:

4.51.27.13.9.10.1. Chamada de câmera desde mapas gráficos usando ícones de câmera.

4.51.27.13.10.2. Chamada de câmera por médio de seleção de uma câmera de uma árvore de navegação de grupo de câmeras.

4.51.27.13.9.10.3. Capacidade de chamar as câmeras por mérito de entrada rápida do número da câmera ao invés de selecioná-la da árvore de navegação.

4.51.27.13.9.10.4. As câmeras poderão ser chamadas individualmente ou em uma matriz de vídeo que permita 4, 6, 9, 16, 25 e 36 displays, dividido em 02 ou mais telas.

4.51.27.13.9.10.4.1. A matriz de vídeo permitirá também displays customizados da tela da câmera.

4.51.27.13.9.10.4.2. Vistas predefinidas de câmera poderão ser guardadas por cada operador.

4.51.27.13.9.10.4.3. A matriz de vídeo pode ser na janela principal do operador o apresentada em um segundo monitor de PC ligado na estação de trabalho do operador.

4.51.27.13.9.10.4.4. Qualquer câmera na árvore de grupo de câmeras poderá ser arrastada e solta dentro da matriz de vídeo.

4.51.27.13.9.10.4.5. Os ciclos/sequências de câmeras deverão ser ajustáveis dentro de qualquer janela da matriz de vídeo.

4.51.27.13.9.10.5. Chamada automática de câmera baseado em um evento de alarme em uma estação cliente.

4.51.27.13.9.10.6. Capacidade de aumentar a visualização da câmera na tela desde o seu tamanho original.

4.51.27.13.9.10.7. Capacidade de chamar os presets das câmeras em câmeras PTZ.

4.51.27.13.9.10.8. Capacidade de definir tours de câmera consistindo de diferentes câmeras, incluindo câmeras PTZ com presets.

4.51.27.13.9.10.9. Capacidade de controlar as câmeras PTZ usando controle do mouse direto na tela ou usando um painel de controle PTZ.

4.51.27.13.9.10.10. Capacidade de programar e gravar sequências de múltiplas câmeras em um único display de imagem.

4.51.27.13.9.10.11. As sequências de câmera poderão ser apresentadas na estação cliente ou em um monitor analógico usando decodificação de hardware, entendendo que o equipamento configurado suporta decodificação em hardware de acordo com esta especificação de projeto.

4.51.27.13.9.11. Mapas interativos de usuário que deverão incluir as seguintes características mínimas:

4.51.27.13.9.11.1. Suporte para até três níveis de mapas gráficos para cada site desejado com a capacidade de definir até 100 localidades.

4.51.27.13.9.11.2. Suportar câmeras localizadas nos mapas para com o intuito de serem chamadas para visualização ao vivo ou reprodução.

4.51.27.13.9.11.3. Suportar links nos mapas para chamar mapas adicionais e visualizações de mapas desde o mapa atual.

4.51.27.13.9.12. O display de reprodução deverá incluir uma barra de tempo gráfica para indicar os tipos de gravação contidos no período de vídeo selecionado. O controle da barra de tempo deverá incluir:

4.51.27.13.9.13. Indicação gráfica de aonde a gravação contínua o programada por tempo acontece, aonde não existe gravação e aonde tem gravação de alarme/evento. Cada tipo de gravação deverá ter um código de cor para identificar a velocidade do tipo de vídeo gravado.

4.51.27.13.10. O software da estação cliente deverá mostrar em tempo real um painel de monitoramento de alarme aonde os alarmes desde os codificadores/decodificadores/gravadores são enviados.

4.51.27.13.11. Qualquer ponto de alarme será anunciado por um sinal audível.

4.51.27.13.12. Os alarmes reportados poderão incluir:

4.51.27.13.12.1. Ativação de entradas de alarme desde um ponto de alarme de um codificador/decodificador/gravador.

4.51.27.13.12.2. Condições de falha do dispositivo como perda de vídeo, falha do equipamento ou off-line, notificação de análise de manutenção de câmera, detecção de atividade (detecção de movimento) e quaisquer outros plug-ins instalados por terceiras empresas aprovadas.

4.51.27.13.12.3. O operador pode reconhecer silenciar ou apagar o alarme do display.

4.51.27.13.12.4. O operador deverá ter a capacidade de clicar duas vezes em um evento na tela de notificação de alarme para ativar a reprodução do vídeo do evento.

4.51.27.13.12.5. O sistema deverá permitir uma contagem numérica se múltiplos alarmes do mesmo dispositivo fossem recebidos e estão na lista de pendências sem precisar abrir cada alarme separadamente para reduzir o número de registros na tela do display.

4.51.27.13.12.6. Para aprimorar a visibilidade do operador dos eventos de alarme reportados o sistema deverá permitir um meio para expandir a tela dos eventos do operador para visualizar melhor mais eventos.

4.51.27.13.12.7. Todos os eventos de alarme e ações do operador associados com um evento deverão estar gravados no log histórico.

4.51.27.14. O software cliente deverá habilitar a transmissão de mensagens audíveis para os alto falantes ligados aos canais de áudio ligados aos codificadores/decodificadores/gravadores

especificados neste projeto. As estações cliente que se espera que possam efetuar transmissões de áudio deverão ter microfones.

4.51.27.14.1. O usuário deverá ter a capacidade de selecionar para qual alto falante ou zona de autofalantes deseja transmitir uma mensagem.

4.51.27.15. O software cliente deverá ter a capacidade de monitoramento do estado dos dispositivos conectados ao sistema e deverão incluir:

4.51.27.15.1.1. O display do estado deverá estar atualizado pelo menos uma vez por segundo.

4.51.27.15.1.2. A capacidade de ler o estado da temperatura interna de todos os codificadores/decodificadores/gravadores ligados ao sistema.

4.51.27.15.1.3. Capacidade de ler a configuração dos codificadores/decodificadores/gravadores incluindo número de canais configurados de vídeo, entradas e saídas de alarme, mesmo como estado operacional dos canais de vídeo.

4.51.27.15.1.4. Visualização do estado de qualquer uma das câmeras que passam através de decodificação de hardware para os monitores.

4.51.27.15.1.5. O usuário deverá ter a capacidade de visualizar o estado de todo o armazenamento das câmeras (discos rígidos) conectado ao sistema incluindo espaço em disco, pastas e configuração para qualquer disco rígido atualmente ativo no dispositivo.

4.51.27.15.1.6. Os usuários administrativos deverão ter a permissão para visualizar logs históricos de usuário baseados em intervalos de tempo/data assim como filtros específicos de seleção do operador.

4.51.27.15.1.7. Os logs históricos poderão ser exportados em padrão .CSV para uso em programas como Microsoft Excel.

4.51.27.15.2. Análise de Conteúdo de Vídeo

4.51.27.15.2.1. O sistema deverá suportar tanto análise de conteúdo padrão embutido como plug-ins especializados de vídeo de fornecedores externos.

4.51.27.15.2.2. As Análises Padrão estarão fornecidas como segue:

4.51.27.15.2.2.1. Deverão estar embutidos dentro da PVI e completamente configurados dentro do sistema PVI.

4.51.27.15.2.2.2. Deverão ser selecionáveis para qualquer canal de vídeo do sistema.

4.51.27.15.2.2.3. Todas as análises de conteúdo deverão ser selecionáveis para todos os canais de um gravador.

4.51.27.15.2.2.4. Os eventos de Análise de Vídeo deverão ser reportados como uma alarma dentro do sistema de gerenciamento de alarmes da PVI e deverão ser configuráveis para gerar saídas de alarme e/ou respostas de operador ou qualquer outro alarme definido acima.

4.51.27.15.2.3. A detecção de atividade usada para gravação por detecção de movimento deverá ter as mínimas capacidades seguintes:

4.51.27.15.2.3.1. Detecção de atividade deverá ser selecionável para qualquer canal de vídeo do sistema.

4.51.27.15.2.3.2. Deverá ser selecionável para todos os canais dentro de um dispositivo simultaneamente sem degradar a desempenho do dispositivo (streaming, gravação, visualização, monitoração de eventos).

4.51.27.15.2.3.3. Deverá permitir detecção de atividade em tempo real para o vídeo inteiro ou permitir para o usuário a definição de um mínimo de três regiões de interesse (ROI) dentro do mesmo fluxo binário.

4.51.27.15.2.3.4. A detecção de atividade poderá ser programável para cada câmera do sistema.

4.51.27.15.2.4. Agentes de Manutenção de Câmera (CMA) deverão estar disponíveis para monitorar diferentes aspectos das câmeras instaladas no sistema e deverão incluir como mínimo os seguintes serviços:

4.51.27.15.2.4.1. Selecionáveis para qualquer canal de vídeo do sistema.

4.51.27.15.2.4.2. Deverá ser selecionável para todos os canais dentro de um dispositivo simultaneamente.

4.51.27.15.2.4.3. Câmera com Imagem Embaçada – isto detecta se o foco da câmera tem mudado baseado em uma configuração inicial do algoritmo para essa câmera.

4.51.27.15.2.4.4. Detecção de Sub/Sobre Exposição – isto detecta se a imagem da câmera virou sub/sobre exposta baseada em uma configuração inicial do algoritmo para essa câmera.

4.51.27.15.2.4.5. Detecção de Imagem Preta – isto detecta se a câmera tem sinal de vídeo mas não há imagem para mostrar.

4.51.27.15.2.4.6. Oclusão da Lente da Câmera – isto detecta se a lente da câmera foi coberta ou parcialmente coberta baseado na configuração inicial da câmera.

4.51.27.15.2.4.7. Mudança de Posicionamento da Câmera – isto detecta se o posicionamento da câmera mudou da sua posição durante a configuração inicial da câmera.

4.51.27.15.2.5. Análise de Conteúdo de Vídeo deverá oferecer como segue:

4.51.27.15.2.5.1. Tipos disponíveis de Análise de Conteúdo de Vídeo, incluindo:

4.51.27.15.2.5.1.1. Objeto esquecido/Removido

4.51.27.15.2.5.1.2. Direção de Movimento / Controle de Fluxo

4.51.27.15.2.5.1.3. Detecção de Fumaça e Detecção de Fog

4.51.27.15.2.5.1.4. Gerenciamento de Multidões

4.51.27.15.2.5.1.5. Contagem de Pessoas

4.51.27.15.2.5.1.6. Controle de Tráfego

4.51.27.15.2.5.1.7. Gerenciamento de Filas de Espera

4.51.27.15.2.5.1.8. Detecção de incidentes em Interiores e Exteriores

4.51.27.15.2.5.1.9. Detecção de Escorregar e Cair

4.51.27.15.2.5.1.10. Comportamento e Seguimento

4.51.27.15.2.5.1.11. Detecção de Afogamento

4.51.27.15.2.5.1.12. Detecção de incidentes em Túneis e Trens

4.51.27.15.2.5.1.13. Os fornecedores deverão fornecer uma lista completa de todos os sistemas de análise avançado disponível e uma certificação de qualificação confirmando a integração total da Análise de Vídeo na Plataforma PVI.

4.51.27.15.2.5.1.14. O desempenho específico do sistema de análise está listado nesta especificação.

4.51.27.15.2.6. A análise de conteúdo deverá estar disponível usando terceiros fornecedores cumprindo as seguintes condições:

4.51.27.15.2.6.1. Qualificado e certificado pelo fabricante da PVI (fornecedor das unidades de codificação/decodificação/gravação) de ser totalmente integrados dentro do sistema PVI.

4.51.27.15.2.6.2. Os fornecedores deverão ter os certificados de cumprimento para qualquer análise de vídeo de acordo com esta especificação.

4.51.27.15.2.6.3. Deverão estar disponíveis em qualquer canal de vídeo baseado nos requisitos desta especificação.

4.51.27.15.2.6.4. Os eventos de Análise de Conteúdo Avançado deverão ser reportados dentro do sistema de gerenciamento de alarmes da PVI e deverão ser configuráveis para gerar saídas de alarme e/ou respostas de operador como com qualquer entrada de alarme descrita acima.

4.51.27.15.2.6.5. Os algoritmos Avançados de Análise de Conteúdo deverão estar em capacidade de ser executados nas unidades de gravação se a necessidade de hardware adicional, a não ser especificado de forma diferente dentro desta especificação.

4.51.27.15.2.6.6. Se precisar de hardware adicional, nenhuma parte dos componentes do sistema PVI será necessária para suportar a análise de conteúdo, o fornecedor deverá identificar os componentes necessários para o serviço de análise de conteúdo.

4.52. FORNECIMENTO DE PLATAFORMA DE GERENCIAMENTO UNIFICADO

4.52.1. Deverá ser fornecido um equipamento desenvolvido para uso profissional, com operação 24/7, para a operação e gerenciamento de imagens de CFTV, pré-carregada com o plataforma de software, com as seguintes características mínimas:

4.52.1.1. Acompanhada de teclado, mouse e cabo de energia;

4.52.1.2. Ser do tipo desktop;

4.52.1.3. Acompanhado de 01 (um) monitor de Led de no mínimo 22";

4.52.1.4. Sistema Operacional: Microsoft Windows 8 de 64 bits PRO ou Superior;

4.52.1.5. Processador Mínimo: Processador Intel Xeon E5-1620 ou equivalente;

4.52.1.6. Memória Mínima: 8 GB de RAM;

4.52.1.7. 01 Interface de rede RJ-45 de 1 Gigabit Ethernet (1000Base-T);

4.52.1.8. 04 (quatro) saídas de vídeo ativas com conexão VGA e HDMI;

4.52.1.9. 01 drive DVRD-RW;

4.52.1.10. Entrada de energia de 100 a 240 VAC, 50/60 Hz, auto comutável;

4.52.2. O sistema deverá ser uma solução de software de monitoramento e suportar a unificação transparente de sistemas de gerenciamento com vídeo IP com as seguintes características:

4.52.2.1. Deverá suportar a unificação transparente entre câmeras IP, gravador digital e em rede, e câmeras ligadas a DVRs, codificados nos formatos de compressão MJPEG, H.264 e H.265;

4.52.2.2. O sistema de monitoramento e gerenciamento de imagens deve possuir funcionalidade de monitoramento ao vivo de eventos, monitoramento ao vivo de imagens, reprodução de vídeos gravados e gerenciamento de alarmes;

4.52.2.3. Deverá proporcionar o gerenciamento de dispositivos com ao menos as seguintes funcionalidades: detecção de dispositivo online e adicionar dispositivos por busca automática;

4.52.2.4. Sua exibição, deverá possuir ao menos as seguintes opções: exibir endereço IP do dispositivo, exibir vídeo em tempo real, controle de PTZ, gravação manual e zoom digital;

4.52.2.5. Em relação a usuários, o sistema deverá permitir a exclusão, adição e edição de usuários, bem como definir permissões ao mesmo;

4.52.2.6. Deverá possibilitar gravação de dispositivo em borda; bem como possibilitar reprodução dos dispositivos de borda ou com armazenamento central de pelo menos 30 câmeras simultaneamente;

4.52.2.7. Deverá suportar o download das gravações ao menos nos formatos MP4 e AVI;

4.52.2.8. Deverá suportar vídeo wall com funções de gerenciar e adicionar vídeo wall; bem como suportar combinar telas em uma;

4.52.2.9. Deverá possuir função de mapa, com ao menos as seguintes facilidades: adicionar editar ou excluir ao menos 5 níveis de submapas no mapa principal;

4.52.2.10. Deverá exibir os dispositivos no sistema com opções de árvore de visualização e grupos;

4.52.2.11. O sistema necessita ser compatível com câmeras que tenham recursos de mapa de calor, reconhecimento facial, leitura automática de placas, contagem de pessoas, detecção facial, linha virtual, cerca virtual, smart-tracking e imagem térmica;

4.52.2.12. O sistema necessita ser compatível com NVRs ou DVRs que tenham recursos de reconhecimento facial, detecção facial, linha virtual, cerca virtual e geração de metadados de pessoas e veículos;

4.52.2.13. O sistema deverá ser capaz de receber informações de reconhecimento facial, com ao menos as seguintes funções: pesquisa por face semelhante, face ao vivo, pesquisa de características, relatório estruturado de gênero e idade;

4.52.2.14. Capacidade de buscar informações de reconhecimento facial no cartão SD da câmera;

4.52.2.15. Ter possibilidade de gestão de lista de pessoas (reconhecimento facial) e alarmes através do software;

4.52.2.16. Deverá possibilitar também receber informações de reconhecimento de placas de veículos com ao menos as seguintes funções: reconhecimento em tempo real, pesquisa com o histórico de reconhecimentos de placas;

4.52.2.17. Capacidade de buscar informações de leitura de placas no cartão SD da câmera;

4.52.2.18. Ter possibilidade de gestão de lista de placas permitidas e proibidas (LPR), além de alarmes, através do software;

4.52.2.19. Deverá possuir recurso de log para manutenção do sistema, com ao menos as seguintes funcionalidades: log de porta, log do gerenciador da web, log de controle do cliente;

4.52.2.20. Ainda referente a manutenção do sistema, deverá suportar funções de backup de dados do sistema, restauração de dados do sistema de arquivos local ou no servidor;

4.52.2.21. Possibilidade de ter até 1000 câmeras IPs em um único servidor, sendo, pelo menos, 64 câmeras com Leitura de Placas Embarcado e 64 câmeras com Reconhecimento facial embarcado;

4.52.2.22. Possibilidade de organizar em pelo menos 10 hierarquias com até 999 entidades por hierarquia;

4.52.2.23. Deverá ter capacidade ilimitada de usuários criados, sendo 100 usuários on-line ao mesmo tempo;

4.52.2.24. Deverá possuir ao menos 2 níveis de usuários;

4.52.2.25. Ser compatível com equipamentos via protocolo Onvif;

4.52.2.26. Deverá possuir recurso de gravação no servidor em que o software está instalado, com um armazenamento dedicado para esta função.

4.52.2.27. Possibilidade de ver status de CPU, armazenamento e consumo de banda no próprio software;

4.52.2.28. Deverá possuir possibilidade de recurso de buscas forenses, tais como: cor e tipo de roupa, chapéu, sacola, gênero, óculos, barba, idade e máscara.

4.53. FORNECIMENTO DE ESTAÇÃO DE MONITORAMENTO

4.53.1. Deverá ser fornecido um equipamento desenvolvido para uso profissional, com operação 24/7, para a operação de monitoramento de imagens de CFTV, pré-carregada com o software VMS, e com as seguintes características mínimas:

4.53.1.1. Suportar no mínimo quatro monitores de alta resolução;

4.53.1.2. Acompanhada de teclado, mouse e cabo de energia;

4.53.1.3. Ser do tipo desktop;

4.53.1.4. Acompanhado de 02 (dois) monitores de Led de no mínimo 22";

4.53.1.5. Sistema Operacional: Microsoft Windows 8 de 64 bits PRO ou Superior;

4.53.1.6. Processador Mínimo: Processador r Intel Xeon E5-1620 ou equivalente.

4.53.1.7. Memória Mínima: 8 GB de RAM;

4.53.1.8. 02 Interfaces de rede RJ-45 de 1 Gigabit Ethernet (1000Base-T);

4.53.1.9. 04 (quatro) saídas de vídeo ativas com conexão VGA e HDMI;

4.53.1.10. 01 drive DVRD-RW;

4.53.1.11. Entrada de energia de 100 a 240 VAC, 50/60 Hz, auto comutável;

4.54. FORNECIMENTO DE DISPOSITIVO DE CONTROLE TIPO I

4.54.1. Mesa controladora com tela touch screen TFT de 7" com resolução 800 × 480;

4.54.2. Deverá possuir visualização ao vivo e reprodução de vídeo na tela com resolução de até 1080p;

4.54.3. Deverá ser compatível com NVR / DVR / DVS, matriz, câmera / dome de rede, controlador de vídeo wall, etc.

4.54.4. Possuir teclas de atalho para controle de domo;

4.54.5. Deverá possuir teclas de atalho para operação de reprodução;

4.54.6. Deverá possuir suporte 3 operadores e cada usuário tem permissão para operar 1280 dispositivos;

4.54.7. Deverá possuir suporte à configuração por servidor WEB;

4.54.8. Deverá possuir controle de até 255 câmeras analógicas por conexão RS-485;

4.54.9. Deverá possuir modo de controle baseado em IP;

4.54.10. Deverá possuir interface de rede Ethernet 10M/100M/1000M;

4.54.11. Deverá possuir interface RS-232;

4.54.12. Deverá possuir interface RS-485;

4.54.13. Deverá possuir interface USB2.0;

4.54.14. Deverá possuir alimentação 12 VDC;

4.54.15. Deverá possuir consumo de energia ≤ 15W

4.54.16. Possuir Temperatura de operação entre -10 ° C a + 55 ° C (14°F a 131°F)

4.54.17. Possuir Umidade de trabalho 10% a 90%

4.54.18. Dimensões (L × P × A) 435 × 193 × 110 mm (17,1 "× 7,6" × 4,3 ")

4.54.19. Peso 2 Kg (4,4 lb)

4.55. FORNECIMENTO DE DISPOSITIVO DE CONTROLE TIPO II

4.55.1. Mesa controladora de tecnologia híbrida, compatível com sistemas de CFTV analógicos e IP, que permita sua ligação com gravadores NVR e DVR, câmeras speed dome e um monitor para visualizar as imagens;

4.55.2. Deverá possuir ao menos conexões para comunicação através de portas RJ45, RS232 e RS485;

4.55.3. Deve ainda possuir pelo menos uma porta USB;

4.55.4. Deverá suportar ao menos protocolos Pelco-P, Pelco-D e ao menos um proprietário;

4.55.5. Deve permitir configuração de acesso por perfil de usuário;

4.55.6. Deve possibilitar o controle de pelo menos 30 speed dome através da porta RS485;

4.55.7. Deve possuir ainda a função bloqueio de mesa;

4.55.8. Deve possuir um display LCD que seja com dimensões aproximadas de 75 mm x 30 mm;

4.55.9. Possuir Joystick com 3 eixos e velocidade variável com zoom que permita realizar função de PTZ;

4.55.10. Sua interface deverá possuir menus totalmente em português;

4.55.11. Deverá operar através das teclas de função do painel frontal de um gravador;

4.55.12. Sua alimentação deve ser de 12 VDC com corrente máxima de 1 A, devendo seu consumo ser menor ou igual a 5 W;

4.55.13. Deve suportar temperaturas de operação de no mínimo entre -10° C a 55° C e umidade de no máximo 90%;

4.55.14. Deverá vir acompanhado de fonte de alimentação 110/240 VAC (automática), conector para entrada RS485, cabo ethernet e cabo de comunicação RS232;

4.55.15. O equipamento deverá ser fornecido com no mínimo 1 ano de garantia pelo fabricante, juntamente com manual de usuário em português;

4.55.16. Para garantir total compatibilidade e integração com o sistema de CFTV, a mesa controladora deverá ser de mesmo fabricante que o gravador de imagens.

4.56. SERVIÇO DE MANUTENÇÃO DE CFTV

4.56.1. Contempla testes, configurações, alinhamento de câmeras, limpeza de lentes, regulagem de mecanismos, substituição e encaminhamento para a garantia do fabricante.

4.56.2. Deverá prover todos os equipamentos, materiais, mão de obra, ferramentas, para manutenção e configuração, bem como executar todas as operações necessárias para manutenção preventiva e corretiva, com o devido encaminhamento dos equipamentos e sistemas para garantia dos fabricantes, mantendo-os em operação durante o período de garantia.

4.56.3. Todos componentes da solução, como troca de qualquer equipamento que venha apresentar defeito, bem como a atualização das versões dos softwares de sistema operacional dos equipamentos e de gerenciamento dos mesmos, substituição ou encaminhamento para garantia do fabricante.

4.57. CURSO DE TREINAMENTO E TRANSFERÊNCIA DE CONHECIMENTO EM CFTV

4.57.1. Treinamento, capacitação e repasse tecnológico no modelo de operação assistida de acordo com o volume do serviço;

4.57.2. Aderido, com duração mínima de 20 horas, a ser administrada pela proponente ou o fabricante dos itens da solução de CFTV com avaliação e certificação dos profissionais do órgão contratante com pelo menos 75% de presença.

4.58. SERVIÇO DE RETIRADA DE PONTO CFTV

4.58.1. Contempla serviço de retirada de câmera fixadas em diversos locais, locação de equipamentos necessários, utilização de ferramentas necessárias, retirada de infraestrutura existente, com bota fora de material.

4.59. FORNECIMENTO DE MONITOR DE IMAGEM PROFISSIONAL 24/7 48 POLEGADAS COM INSTALAÇÃO

4.59.1. Deverá ser do tipo monitor profissional, não sendo aceitas soluções de televisores convencionais com adaptadores;

4.59.2. Possuir tamanho diagonal de 48 (quarenta e oito) polegadas ou superior;

4.59.3. Deverá apresentar relação de contraste dinâmico de 1100:1 ou superior;

4.59.4. Deverá possuir de forma intrínseca ao equipamento, as seguintes “interfaces” para entrada de vídeo: o 1 (um) conector padrão VGA;

4.59.4.1. 1 (um) conector padrão DVI-D;

4.59.2.2. (dois) conectores padrão HDMI;

4.59.2.3. (1 (um) conector padrão USB;

4.59.5. Deverá possuir uma interface para áudio;

4.59.6. Deverá suportar a resolução de 3840 x 2160 pixels (16:9 de proporção);

4.59.7. Possuir tempo de resposta de 9 (nove) ms ou inferior;

4.59.8. Possuir brilho de 500cd/m²;

4.59.9. Possuir ângulo de visão horizontal / vertical de 178:178;

4.59.10. Suportar coloração de imagem de 16,7 milhões ou superior;

4.59.11. Deverá suportar a utilização contínua de 24 horas diárias, sendo 7 dias por semana;

4.59.12. Deverá apresentar dimensões de fixação em parede de montagem de 300x300 milímetros conforme padronização VESA;

4.59.13. Possuir, no mínimo, 1 (uma) porta física constituída de conector RJ45

4.59.14. Deverá possuir fonte de alimentação elétrica com chaveamento automático (“bivolt”) para 100-240 volts e frequência de 50 a 60 (sessenta) Hz;

4.59.15. Apresentar consumo máximo de 70 (setenta) Watts;

4.59.16. Garantia dos produtos deverá ser de 01 (um) ano contra defeitos de fabricação.

4.60. FORNECIMENTO DE CONTROLADORA INTELIGENTE DE ACESSO TIPO I

4.60.1. A Controladora Inteligente do Sistema (CIS) deverá associar o sistema a todos os outros componentes de hardware de campo (leitores de cartões de acesso e módulos de controle de entrada). A Controladora Inteligente do Sistema deverá fornecer processamento distribuído completo de controle de acesso e as operações de monitoramento de alarme. Os níveis de acesso, configurações de hardware, e saídas de alarme programadas atribuída na estação de trabalho cliente de administração serão transferidos para a Controladora Inteligente do Sistema, que deve armazenar essas informações utilizando a sua função de alta velocidade, microprocessador de 32 bits local. Todas as decisões de acesso concedidas/negadas devem ser feitas na Controladora Inteligente do Sistema para fornecer respostas rápidas às operações de leitor de cartão. Uma Controladora Inteligente do Sistema totalmente configurado com até 64 leitores de cartão de acesso, deverá exigir menos de metade (0,5) de segundo para permitir acesso a um usuário de cartão de acesso, autorizado ou negar acesso a um usuário de cartão de acesso não autorizado.

4.60.2. O hardware de campo de controle de acesso do sistema deverá fornecer uma Controladora Inteligente do Sistema baseado em rede. A Controladora Inteligente do Sistema de rede é um painel de base Ethernet 10/100 MB que deverá possuir capacidade para residir em uma rede de área local (LAN) ou rede WAN, sem ligação a uma porta serial do PC. A Controladora Inteligente do Sistema deverá utilizar uma capacidade de Ethernet embarcada para oferecer essa funcionalidade sem a necessidade de componentes adicionais no sistema. As Controladoras Inteligentes do Sistema baseadas em rede devem ser capazes de se comunicar de volta com o servidor de banco de dados através de comutadores e roteadores padrão da indústria e não deve estar na mesma sub-rede.

4.60.3. A Controladora Inteligente do Sistema deve continuar a funcionar normalmente (independente) no caso em que ele perca a comunicação com o software do sistema. Enquanto neste estado off-line, a Controladora Inteligente do Sistema deve tomar as decisões de acesso concedido ou negado e manter um registro dos eventos ocorridos. Os eventos serão armazenados na memória local e, em seguida, enviados automaticamente para o banco de dados sistema após a comunicação ser restabelecida.

4.60.4. A Controladora Inteligente do Sistema deverá conter um servidor da Web incorporado para permitir a configuração de rede e parâmetros de comunicação. Por segurança, o servidor Web deve suportar comunicações SSL e permitir que nomes de usuário e senhas sejam definidos e alterados.

4.60.5. A Controladora Inteligente do Sistema deverá conter as seguintes características mínimas:

4.60.5.1. Possuir aprovações: FCC Part 15, UL 294, UL 1076, CAN/ULC 60839-11-1:2016, RoHS, CSA e CE;

4.60.5.2. Suporte para até 96 MB de memória onboard;

4.60.5.3. Comunicação através do protocolo BACNET para integração com sistemas de automação predial;

4.60.5.4. Suporte a LAN deve utilizar uma Interface Ethernet de conector RJ-45 (10/100BaseT)

4.60.5.5. Memória Flash remotamente reprogramável para atualizações de programa em tempo real e comunicações host global

4.60.5.6. Suporte para protocolo RS-485

4.60.5.7. Armazenamento de até 1.000.000 usuários de cartão de acesso/50.000 eventos dentro da memória não-volátil onboard

4.60.5.8. Deverá suportar até 64 dispositivos constituídos por módulos de interface de leitor, módulos de controle de entrada e módulos de controle de saída em qualquer combinação desejada com um máximo de 32 módulos por Controladora Inteligente do Sistema.

4.60.5.9. Suporte para várias tecnologias de cartão

4.60.5.10. Suporte para controle de elevadores

4.60.5.11. Suporte para OSDP – Open Supervised Device Protocol

4.60.5.12. Possuir suporte para comunicação criptografada AES 256bit entre a controladora inteligente e os módulos de expansão;

4.60.5.13. Possuir suporte para comunicação criptografada AES 256bit entre a controladora inteligente e o servidor do sistema de controle de acesso;

4.60.5.14. Integração com leitores de cartão de acesso de outros fabricantes

4.60.5.15. Microprocessador de 32 bits

4.60.5.16. Suporte interface biométrica

4.60.5.17. 12 VDC ou 24 VDC potência

4.60.5.18. Permitir armazenamento de PIN de até nove dígitos

4.60.5.18.1. Suporte para no mínimo 08 entradas programáveis e 04 saídas de relé programáveis por controlador

4.60.5.19. LEDs de status para o componente normal e status de comunicação

4.61. FORNECIMENTO DE CONTROLADORA INTELIGENTE DE ACESSO TIPO II

4.61.1. A Controladora Inteligente do Sistema (CIS) deverá associar o sistema a todos os outros componentes de hardware de campo (leitores de cartões de acesso e módulos de controle de entrada). A Controladora Inteligente do Sistema deverá fornecer processamento distribuído completo de controle de acesso e as operações de monitoramento de alarme. Os níveis de acesso, configurações de hardware, e saídas de alarme programadas atribuída na estação de trabalho cliente de administração serão transferidos para a Controladora Inteligente do Sistema, que deve armazenar essas informações utilizando a sua função de alta velocidade, microprocessador de 32 bits local. Todas as decisões de acesso concedidas/negadas devem ser feitas na Controladora Inteligente do Sistema para fornecer respostas rápidas às operações de leitor de cartão. Uma Controladora Inteligente do Sistema totalmente configurado com até 64 leitores de cartão de acesso, deverá exigir menos de metade (0,5) de segundo para permitir acesso a um usuário de cartão de acesso, autorizado ou negar acesso a um usuário de cartão de acesso não autorizado.

4.61.2. O hardware de campo de controle de acesso do sistema deverá fornecer uma Controladora Inteligente do Sistema baseado em rede. A Controladora Inteligente do Sistema de rede é um painel de base Ethernet 10/100 MB que deverá possuir capacidade para residir em uma rede de área local (LAN) ou rede WAN, sem ligação a uma porta serial do PC. A Controladora Inteligente do Sistema deverá utilizar uma capacidade de Ethernet embarcada para oferecer essa funcionalidade sem a necessidade de componentes adicionais no sistema. As Controladoras Inteligentes do Sistema baseadas em rede devem ser capazes de se comunicar de volta com o servidor de banco de dados através de comutadores e roteadores padrão da indústria e não deve estar na mesma sub-rede.

4.61.3. A Controladora Inteligente do Sistema deve continuar a funcionar normalmente (independente) no caso em que ele perca a comunicação com o software do sistema. Enquanto neste estado off-line, a Controladora Inteligente do Sistema deve tomar as decisões de acesso concedido ou negado e manter um registro dos eventos ocorridos. Os eventos serão armazenados na memória local e, em seguida, enviados automaticamente para o banco de dados sistema após a comunicação ser restabelecida.

4.61.4. A Controladora Inteligente do Sistema deverá conter um servidor da Web incorporado para permitir a configuração de rede e parâmetros de comunicação. Por segurança, o servidor Web deve suportar comunicações SSL e permitir que nomes de usuário e senhas sejam definidos e alterados.

4.61.5. A Controladora Inteligente do Sistema deverá conter as seguintes características mínimas:

4.61.5.1. Possuir as seguintes aprovações: FCC Part 15, RoHS, UL 294, UL 1076, CSA, e CE;

4.61.5.2. Suporte para até 6 MB de memória onboard;

4.61.5.3. Suporte a LAN deve utilizar uma Interface Ethernet de conector RJ-45 (10/100BaseT)

4.61.5.4. Memória Flash remotamente reprogramável para atualizações de programa em tempo real e comunicações host global

4.61.5.5. Suporte para protocolo RS-485

4.61.5.6. Armazenamento de até 250.000 usuários de cartão de acesso/50.000 eventos dentro da memória não-volátil onboard

4.61.5.7. Deverá suportar até 64 dispositivos constituídos por módulos de interface de leitor, módulos de controle de entrada e módulos de controle de saída em qualquer combinação desejada com um máximo de 32 módulos por Controladora Inteligente do Sistema.

4.61.5.8. Suporte para várias tecnologias de cartão

4.61.5.9. Suporte para controle de elevadores

4.61.5.10. Suporte para OSDP – Open Supervised Device Protocol

4.61.5.11. Possuir suporte para comunicação criptografada AES 256bit entre a controladora inteligente e os módulos de expansão;

4.61.5.12. Possuir suporte para comunicação criptografada AES 256bit entre a controladora inteligente e o servidor do sistema de controle de acesso;

4.61.5.13. Integração com leitores de cartão de acesso de outros fabricantes

4.61.5.14. Microprocessador de 32 bits

4.61.5.15. Suporte interface biométrica

4.61.5.16. 12 VDC ou 24 VDC potência

4.61.5.17. Permitir armazenamento de PIN de até nove dígitos

4.61.5.17.1. Suporte para no mínimo 08 entradas programáveis e 04 saídas de relé programáveis por controlador

4.61.5.18. LEDs de status para o componente normal e status de comunicação

4.62. FORNECIMENTO DE ACESSO TIPO I

O Acesso tipo 1 é composto dos seguintes itens:

01 Catraca Pedestal

01 Controladora de Acesso Tipo 1

01 Controladora de Acesso Tipo 2

01 Leitor Proximidade para Cofre

02 Leitores Biométricos

4.62.1. CATRACA DE ACESSO

4.62.1.1. Estrutura e acabamento

4.62.1.1.1. Catraca de três braços, modelo balcão com dispositivo de segurança braço que cai e motorização do giro.

4.62.1.1.2. Deve possuir acabamento externo em aço inox 304 escovado

4.62.1.1.3. É permitido o uso de plástico de alta resistência ou vidro temperado em combinação com o aço no acabamento.

4.62.1.1.4. Para evitar danos corporais ou materiais, todos os cantos e bordas externas do equipamento que podem ter contato com o usuário devem possuir raios de no mínimo 15mm.

4.62.1.1.5. O revestimento da catraca não deve possuir parafusos e nem pontos de solda aparentes

4.62.1.1.6. O equipamento deve possuir fechadura com chave para acesso aos dispositivos internos. Essa fechadura deve possuir formas arredondadas para evitar danos corporais ou materiais.

4.62.1.1.7. O equipamento deve possuir três braços, em aço inox 304 polido, com acabamento em plástico de alta resistência em sua extremidade.

4.62.1.1.8. O equipamento deve ser fixado no piso através de chumbadores adequados ao seu peso e esforço

4.62.1.1.9. Deve possuir minimamente um pictograma na parte superior para indicar acesso negado (um x vermelho) e sentido liberado (uma seta verde) indicando o sentido de giro que o mecanismo está liberado e um pictograma lateral de cada lado, para indicar a disponibilidade e/ou sentido de passagem.

4.62.1.1.10. O MCBF (médio de ciclos entre falhas) deve ser maior que 1 milhão.

4.62.1.1.11. O equipamento deve permitir o uso bidirecional, ou seja, possibilidade de travamento ou liberação nas quatro condições: 1º- Ambos sentidos livres, 2º- ambos sentidos travados, 3º- sentido de entrada travado e saída livre, 4º- sentido de entrada livre e saída travado.

4.62.1.1.1.2 Deve possuir fonte interna full range (90VAC a 240 VAC)

4.62.1.1.13. Deve permitir a instalação oculta dos leitores de entrada e saída.

4.62.1.2. Acessórios obrigatórios

4.62.1.2.1. Braço que cai

4.62.1.2.1.1. Deve possuir um dispositivo que desarme o braço que está em repouso (posição horizontal), fazendo-o passar para a posição vertical e deixando um vão livre para a passagem de pessoas em caso de emergência.

4.62.1.2.1.2. O rearme deve acontecer sem necessidade de nenhuma ferramenta ou intervenção especial, apenas com o usuário reposicionando o braço da catraca.

4.62.1.2.2. Mecanismo Motorizado

4.62.1.2.2.1. Visando a redução de manutenções e aumento da vida útil, o servo motor deverá ser do tipo “sem escovas”, também conhecido como “brush-less”.

4.62.1.2.2.2. Caso o equipamento seja dotado de Braço que cai, o rearme deve ser automático.

4.62.1.2.2.3. Deve possuir a possibilidade de configurar uma pequena movimentação no sentido para o qual o giro está liberado, “sinalizando ao usuário a liberação de acesso”

4.62.1.2.3. Urna coletora

4.62.1.2.3.1. Deve ser embutida na estrutura da catraca

4.62.1.2.3.2. Deve possuir dispositivo de recolhimento de cartões, dotado de sensor ótico para identificar o deposito de cartões que não sejam compatíveis com o leitor existente. O equipamento deve identificar que aquele é um cartão que não foi lido, permitir o recolhimento dele ao recipiente

4.62.1.2.3.3. Deve possuir urna sensorizada para coleta de cartões de visitante. O sensor deve ser independente do leitor de cartão e deve em caso de detectar o depósito de um cartão que não pode ser lido, liberar a queda dele no recipiente e não liberar o giro do braço.

4.62.1.2.3.4. Deve permitir a instalação de leitor de proximidade na urna

4.62.2. CONTROLADOR DE ACESSO TIPO 1

4.62.3. O controlador de acesso para dois leitores de cartão de acesso deverá fornecer uma interface entre a Controladora Inteligente do Sistema e leitoras de cartão de acesso. O controlador de acesso para dois leitores de cartão de acesso deverá funcionar com qualquer leitora de cartões de acesso, que produz uma saída de comunicação padrão Wiegand (Data 1/Data 0 ou Clock e Data), uma interface F/2F, ou que oferece comunicações controladas, utilizando Open Supervised Device Protocol (OSDP).

4.62.4. Um ou ambas as portas do controlador devem suportar a conexão de um dispositivo biométrico leitor de impressão digital, utilizando modelos baseados em servidor. O dispositivo de leitor biométrico de impressão digital pode ser usado no lugar de, ou em conjunto com um leitor de cartão para proporcionar maior segurança e comodidade. Quando um dispositivo leitor biométrico de impressão digital é conectado à controlador, o controlador deverá fornecer modelos biométricos para o dispositivo diretamente da Controladora Inteligente do Sistema ou IDRC, sem a exigência de um dispositivo de gateway separado biométricos.

4.62.5. O controlador deverá monitorar a posição de porta e status de pedidos para saída do dispositivo para cada uma das duas portas, e monitor de um total de 4 entradas de alarme auxiliar por controlador. Deve também controlar o sinal elétrico para cada uma das duas portas e fornecer um total de quatro saídas de relé auxiliar por controlador.

4.62.6. O controlador deverá suportar no mínimo 16 formatos de cartão único.

4.62.7. O controlador deve apoiar um leitor de cartões de acesso integrado/teclado e apoiará três modos de acesso em caso de perda de comunicação com a Controladora Inteligente do Sistema; bloqueado, desbloqueado, e código de acesso.

4.62.8. O controlador deverá oferecer as seguintes características mínimas:

UL 294, ULC, e CE certificado

4.62.8.1.1. Com no mínimo uma porta serial padrão RS485;

4.62.8.1.2. Suporte para OSDP – Open Supervised Device Protocol

4.62.8.1.3. Possuir suporte para comunicação criptografada AES 256bit entre a controladora inteligente e os módulos de expansão;

4.62.8.1.4. Suporte para controle de elevadores

4.62.8.1.5. Alimentação de entrada 12VDC ou 24VDC

4.62.8.1.6. Suporte para até 16 formatos de cartão magnético e Wiegand

4.62.8.1.7. Suporte para Comunicações de Clock/Data, Data1/Data0 Wiegand, F/2F;

4.62.8.1.8. Suporte para no mínimo 08 entradas programáveis e 06 saídas de relé programáveis por controlador

4.62.9. CONTROLADOR DE ACESSO TIPO 2

4.62.9.1. O controlador de acesso para uma leitora de controle de acesso deverá fornecer uma interface entre a Controladora Inteligente do Sistema e leitores de cartão de acesso. O controlador de acesso para uma leitora de acesso deverá funcionar com qualquer leitora de cartões de acesso que produz uma saída de comunicação padrão Wiegand (Data 1/Data 0 ou Clock e Data) e interface F/2F, ou que oferece comunicações controladas, utilizando Open Device Supervisionado Protocol (OSDP).

4.62.9.2. O controlador deverá suportar a conexão de um dispositivo biométrico de leitor de impressão digital, utilizando modelos baseados em servidor. O dispositivo de leitor biométrico de impressão digital pode ser usado no lugar de, ou em conjunto com um leitora de cartão de acesso para proporcionar maior segurança e comodidade. Quando um dispositivo leitor biométrico de impressão digital é conectado à controladora, a controladora deverá fornecer modelos biométricos para o dispositivo diretamente da Controladora Inteligente do Sistema ou IDRC, sem a exigência de um dispositivo de gateway separado biométricos.

4.62.9.3. A controladora deverá acompanhar por porta e posição de situação do dispositivo por solicitação de saída. Deverá também controlar o sinal elétrico e fornecer uma saída de relé auxiliar.

4.62.9.4. A controladora deverá suportar no mínimo 16 formatos de cartão único.

4.62.9.5. A controladora deverá apoiar uma leitora de cartões de acesso integrado/teclado e apoiará três modos de acesso em caso de perda de comunicação com a Controladora Inteligente do Sistema; bloqueado, desbloqueado, e código de acesso.

4.62.9.6. A controladora deverá oferecer as seguintes características mínimas:

4.62.9.6.1. UL 294, ULC, e CE certificado

4.62.9.6.2. Com no mínimo uma porta serial padrão RS485;

4.62.9.6.3. Suporte para OSDP – Open Supervised Device Protocol

4.62.9.6.4. Possuir suporte para comunicação criptografada AES 256bit entre a controladora inteligente e os módulos de expansão;

4.62.9.6.5. Suporte para controle de elevadores

4.62.9.6.6. Alimentação de entrada 12VDC ou 24VDC

4.62.9.6.7. Suporte para até 16 formatos de cartão magnético e Wiegand

4.62.9.6.8. Suporte para Comunicações de Clock/Data, Data1/Data0 Wiegand, F/2F;

4.62.9.6.9. Suporte para no mínimo 02 entradas programáveis e 01 saídas de relé programáveis por controlador

4.62.10. LEITOR DE PROXIMIDADE

4.62.10.1. Permite o acesso seguro com um dispositivo móvel que potencializa as tecnologias de comunicação padrão que funcionam com ambos sistemas operacionais iOS® e Android™.

4.62.10.2. Suporta IDs Móveis novas e grupos de cartões existentes para migração sem interrupções para um padrão mais seguro.

4.62.10.3. Configurações de leitura ajustáveis que permitem controlar a operação geral e o alcance de leitura dos IDs móveis, possibilitando a flexibilidade em distâncias menores.

4.62.10.4. Deve possuir capacidade para leitura de smartcards contacless e smartphones;

4.62.10.5. Deve suportar frequências de operação de 13,56MHz e de 2,4GHz simultaneamente;

4.62.10.6. Deve possuir capacidade de leitura para distâncias de até 7,1 cm entre smartcards contactless e a leitora;

4.62.10.7. Deve possuir capacidade de leitura para distâncias de até 2 metros entre o smartphone e a leitora;

Deve suportar alimentação elétrica de 5 a 16VDC;

4.62.10.8. Deve possuir criptografia com uso de algoritmo seguro para transmissão de RF entre a leitora e o cartão;

4.62.10.9. Deve possuir autenticação mútua entre o cartão e a leitora;

4.62.10.10. Deve possuir compatibilidade com a tecnologia de cartões de acordo com as normas ISO 15693, ISO 14443A e ISO 14443B;

4.62.10.11. Deve suportar simultaneamente, sem a necessidade de qualquer de troca ou modificação de hardware, no mínimo a leitura das seguintes tecnologias: Mifare, Desfire, NFC (Near Field Communication), Bluetooth e iClass;

4.62.10.12. Deve suportar upgrade de firmware em campo através de cartão on site, sem a necessidade de remover a leitora para laboratório;

4.62.10.13. Deve suportar instalação em áreas interna e/ou externa abrigada, além de possuir o padrão de proteção no mínimo de IP55;

4.62.10.14. Deve possuir encapsulamento em policarbonato resistente, de acordo com o padrão UL94;

4.62.10.15. Deve possuir opção de instalação de cabo ou terminal de conectores;

4.62.10.16. Deve suportar instalação segundo os padrões Wiegand e Clock-and-Data com no mínimo 150mts de cabo de 22AWG;

4.62.10.17. Deve suportar temperatura de operação de no mínimo -25 a 65ºC;

4.62.10.18. Deve suportar operação com umidade de 5 a 95%, não condensada, no mínimo.

4.62.11. LEITOR BIOMETRICO

4.62.11.1. Sensor biométrico do tipo óptico com resolução mínima de 500 dpi;

4.62.11.2. Possuir memória básica para até 500 usuários com capacidade de expansão para até 10.000 usuários;

4.62.11.3. Permitir o cadastro de até 3 dedos por usuário, sendo 2 para uso normal e 1 para coação;

4.62.11.4. Possuir display 2.8” WVGA touchsreen;

4.62.11.5. Capacidade de operação no modo 1:1 ou 1:N;

4.62.11.6. Possibilitar a identificação de usuários no modo 1:N de até 10.000 usuários em menos de 1 segundo;

4.62.11.7. Permitir o armazenamento de log de até 1.000.000 de eventos no próprio leitor;

4.62.11.8. Possuir leitor Smartcard HID Iclass interno de 13.56MHz;

4.62.11.9. Somente Biometria 1:N

4.62.11.9.1. Biometria + Cartão

4.62.11.9.2. Somente Cartão

4.62.11.10. Flexibilidade de operação permitindo a definição do modo de autenticação por usuário, à saber:

4.62.11.10.1. Somente Biometria 1:N

4.62.11.10.2. Biometria + Senha

4.62.11.10.3. Somente Senha

4.62.11.10.4. Biometria + Cartão

4.62.11.10.5. Biometria + Cartão + Senha

4.62.11.10.6. Somente Cartão

4.62.11.11. Possibilidade de armazenamento e leitura de templates gravados na memória do cartão inteligente Iclass;

4.62.11.12. O leitor biométrico deverá possuir algoritmo de software capaz de identificar tentativas de fraudes utilizando dedos falsos (FFD – Fake Finger Detection);

4.62.11.13. O sensor biométrico deverá possuir certificação FBI PIV IQS;

4.62.11.14. Capacidade de ser alimentado através de Switches POE e também por fonte DC externa 12 ou 24 volts;

4.62.11.15. Possuir saída Wiegand para conexão à uma controladora de acesso padrão de mercado;

4.62.11.16. Suporte para OSDP – Open Supervised Device Protocol

4.62.11.17. Possibilitar o controle direto do bloqueio físico sem a necessidade de controladora de acesso através de suas entradas e saídas digitas;

4.62.11.18. Possuir uma entrada padrão Wiegand para conexão de um leitor externo;

4.62.11.19. Possuir no mínimo um relê de saída para acionamento de bloqueios físicos e ainda 2 entradas e 2 saídas digitais para controle e acionamentos diversos;

4.62.11.20. Comunicação Ethernet para gerenciamento do leitor e distribuição dos templates;

4.62.11.21. Grau de proteção contra intemperes: IP65;

4.62.11.22. Grau de proteção contra vandalismo: IK08;

4.62.11.23. Possuir tamper switch para monitoramento de tentativas de violação;

4.62.11.24. Certificações: CE, CB, FCC e RoHS.

4.63. FORNECIMENTO DE ACESSO TIPO II

O Acesso tipo 2 é composto dos seguintes itens:

01 Catraca de Acesso

01 Controladora de Acesso

01 Leitor Biométrico

4.63.1. CATRACA DE ACESSO

4.63.1.1. Estrutura e acabamento

4.63.1.1.1. Catraca com braço do tipo “clip”, com vão de passagem adequado a norma ABNT 5010 e acionamento motorizado;

4.63.1.1.2. Deve possuir acabamento externo em aço inox 304 escovado;

4.63.1.1.3. É permitido o uso de plástico de alta resistência em combinação com o aço no acabamento;

4.63.1.1.4. Para evitar danos corporais ou materiais, todos os cantos e bordas externas do equipamento que podem ter contato com o usuário devem possuir raios de no mínimo 15 mm;

4.63.1.1.5. O revestimento da catraca não deve possuir parafusos e nem pontos de solda aparentes;

4.63.1.1.6. O equipamento deve possuir fechadura com chave para acesso aos dispositivos internos. Essa fechadura deve possuir formas arredondadas para evitar danos corporais ou materiais;

4.63.1.1.7. O equipamento deve ser fixado no piso através de chumbadores adequados ao seu peso e esforço

4.63.1.1.8. Deve possuir minimamente um pictograma na parte superior para indicar acesso negado (um x vermelho) e sentido liberado (uma seta verde indicando o sentido de giro que o mecanismo está liberado e um pictograma lateral de cada lado, para indicar a disponibilidade e/ou sentido de passagem.

4.63.1.1.9. O MCBF (médio de ciclos entre falhas) deve ser maior que 1 milhão.

4.63.1.1.10. O equipamento deve permitir o uso bidirecional, ou seja, possibilidade de travamento ou liberação nas quatro condições: 1º- Ambos sentidos livres, 2º- ambos sentidos travados, 3º- sentido de entrada travado e saída livre, 4º- sentido de entrada livre e saída travado.

4.63.1.1.11. Deve possuir fonte interna full range (90VAC a 240 VAC)

4.63.1.2. Acessórios obrigatórios

4.63.1.2.1. Mecanismo Motorizado

4.63.1.2.1.1. Visando a redução de manutenções e aumento da vida útil, o servo motor deverá ser do tipo “sem escovas”, também conhecido como “brush-less”.

4.63.1.2.1.2. Deve possuir precisão de posicionamento menor que 0,360°

4.63.1.2.1.3. Caso o equipamento seja dotado de braço que cai, o rearme deve ser automático.

4.63.1.2.1.4. Deve possuir a possibilidade de configurar uma pequena movimentação no sentido para o qual o giro está liberado, “sinalizando ao usuário a liberação de acesso”

4.63.1.2.2. Urna coletora

4.63.1.2.2.1. Deve ser embutida na estrutura da catraca

4.63.1.2.2.2. Deve possuir dispositivo de recolhimento de cartões, dotado de sensor ótico para identificar o deposito de cartões que não sejam compatíveis com o leitor existente. O equipamento deve identificar que aquele é um cartão que não foi lido, permitir o recolhimento dele ao recipiente

4.63.1.2.2.3. Deve possuir urna sensorizada para coleta de cartões de visitante. O sensor deve ser independente do leitor de cartão e deve em caso de detectar o depósito de um cartão que não pode ser lido, liberar a queda dele no recipiente e não liberar o giro do braço.

4.63.1.2.2.4. Deve permitir a instalação de leitor de proximidade na urna

4.63.2. CONTROLADOR DE ACESSO

4.63.2.1. O controlador de acesso para dois leitores de cartão de acesso deverá fornecer uma interface entre a Controladora Inteligente do Sistema e leitoras de cartão de acesso. O controlador de acesso para dois leitores de cartão de acesso deverá funcionar com qualquer leitora de cartões de acesso, que produz uma saída de comunicação padrão Wiegand (Data 1/Data 0 ou Clock e Data), uma interface F/2F, ou que oferece comunicações controladas, utilizando Open Supervised Device Protocol (OSDP).

4.63.2.2. Um ou ambas as portas do controlador devem suportar a conexão de um dispositivo biométrico leitor de impressão digital, utilizando modelos baseados em servidor. O dispositivo de leitor biométrico de impressão digital pode ser usado no lugar de, ou em conjunto com um leitor de cartão para proporcionar maior segurança e comodidade. Quando um dispositivo leitor biométrico de impressão digital é conectado à controlador, o controlador deverá fornecer modelos biométricos para o dispositivo diretamente da Controladora Inteligente do Sistema ou IDRC, sem a exigência de um dispositivo de gateway separado biométricos.

4.63.2.3. O controlador deverá monitorar a posição de porta e status de pedidos para saída do dispositivo para cada uma das duas portas, e monitor de um total de 4 entradas de alarme auxiliar por controlador. Deve também controlar o sinal elétrico para cada uma das duas portas e fornecer um total de quatro saídas de relé auxiliar por controlador.

4.63.2.4. O controlador deverá suportar no mínimo 16 formatos de cartão único.

4.63.2.5. O controlador deve apoiar um leitor de cartões de acesso integrado/teclado e apoiará três modos de acesso em caso de perda de comunicação com a Controladora Inteligente do Sistema; bloqueado, desbloqueado, e código de acesso.

4.63.2.6. O controlador deverá oferecer as seguintes características mínimas:

4.63.2.6.1. UL 294, ULC, e CE certificado

4.63.2.6.2. Com no mínimo uma porta serial padrão RS485;

4.63.2.6.3. Suporte para OSDP – Open Supervised Device Protocol

4.63.2.6.4. Possuir suporte para comunicação criptografada AES 256bit entre a controladora inteligente e os módulos de expansão;

4.63.2.6.5. Suporte para controle de elevadores

4.63.2.6.6. Alimentação de entrada 12VDC ou 24VDC

4.63.2.6.7. Suporte para até 16 formatos de cartão magnético e Wiegand

4.63.2.6.8. Suporte para Comunicações de Clock/Data, Data1/Data0 Wiegand, F/2F;

4.63.2.6.9. Suporte para no mínimo 08 entradas programáveis e 06 saídas de relé programáveis por controlador

463.3. LEITOR BIOMETRICO

4.63.3.1. Sensor biométrico do tipo óptico com resolução mínima de 500 dpi;

4.63.3.2. Possuir memória básica para até 500 usuários com capacidade de expansão para até 10.000 usuários;

4.63.3.3. Permitir o cadastro de até 3 dedos por usuário, sendo 2 para uso normal e 1 para coação;

4.63.3.4. Possuir display 2.8” WVGA touchsreen;

4.63.3.5. Capacidade de operação no modo 1:1 ou 1:N;

4.63.3.6. Possibilitar a identificação de usuários no modo 1:N de até 10.000 usuários em menos de 1 segundo;

4.63.3.7. Permitir o armazenamento de log de até 1.000.000 de eventos no próprio leitor;

4.63.3.8. Possuir leitor Smartcard HID Iclass interno de 13.56MHz;

4.63.3.9. Somente Biometria 1:N

4.63.3.9.1. Biometria + Cartão

4.63.3.9.2. Somente Cartão

4.63.3.10. Flexibilidade de operação permitindo a definição do modo de autenticação por usuário, à saber:

4.63.3.10.1. Somente Biometria 1:N

4.63.3.10.2. Biometria + Senha

4.63.3.10.3. Somente Senha

4.63.3.10.4. Biometria + Cartão

4.63.3.10.5. Biometria + Cartão + Senha

4.63.3.10.6. Somente Cartão

4.63.3.11. Possibilidade de armazenamento e leitura de templates gravados na memória do cartão inteligente Iclass;

4.63.3.12. O leitor biométrico deverá possuir algoritmo de software capaz de identificar tentativas de fraudes utilizando dedos falsos (FFD – Fake Finger Detection);

4.63.3.13. O sensor biométrico deverá possuir certificação FBI PIV IQS;

4.63.3.14. Capacidade de ser alimentado através de Switches POE e também por fonte DC externa 12 ou 24 volts;

4.63.3.15. Possuir saída Wiegand para conexão à uma controladora de acesso padrão de mercado;

4.63.3.16. Suporte para OSDP – Open Supervised Device Protocol

4.63.3.17. Possibilitar o controle direto do bloqueio físico sem a necessidade de controladora de acesso através de suas entradas e saídas digitas;

4.63.3.18. Possuir uma entrada padrão Wiegand para conexão de um leitor externo;

4.63.3.19. Possuir no mínimo um relê de saída para acionamento de bloqueios físicos e ainda 2 entradas e 2 saídas digitais para controle e acionamentos diversos;

4.63.3.20. Comunicação Ethernet para gerenciamento do leitor e distribuição dos templates;

4.63.3.21. Grau de proteção contra intemperes: IP65;

4.63.3.22. Grau de proteção contra vandalismo: IK08;

4.63.3.23. Possuir tamper switch para monitoramento de tentativas de violação;

4.63.3.24. Certificações: CE, CB, FCC e RoHS.

4.64. FORNECIMENTO DE ACESSO TIPO III

O Acesso tipo 3 é composto dos seguintes itens:

01 controlador IP

01 leitor de cartões e biometria

01 fechadura eletromagnética

01 mola hidráulica

01 botoeira

01 botoeira de emergência

01 fonte de 1AH com caixa

O kit deve ser totalmente gerenciável e as placas controladoras deverão ser homologadas para trabalhar com o software da Unidade de Processamento e Armazenamento de Controle de Acesso, devendo ser fornecido com todos os acessórios e licenças necessárias para a integração ao sistema de controle de acesso.

4.64.1. CARACTERÍSTICAS DO CONTROLADOR DE ACESSO IP

A controladora deverá fornecer uma solução cartão única com interface de dois leitores para controle de uma porta. A controladora deve fornecer controle de acesso completo do Fabricante com um dispositivo que pode ser instalado na borda do perímetro seguro. A controladora deverá ser compacta e uma opção para alimentação via PoE ou 12 VDC. A controladora deve ter processamento robusto e memória on-board que deve permitir que milhares de usuários de cartão de acesso que possam ser armazenados localmente por tolerância de falhas. A controladora deve suportar a maioria dos recursos de controle de acesso padrão do sistema de gestão de segurança. A controlada deverá permitir alterar a sua configuração para que possa gerenciar até oito (08) módulos de expansão via RS-485.

4.64.2. A Controladora de acesso IP deverá conter as seguintes características mínimas:

4.64.2.1. Porta Primária: 10/100 Ethernet;

4.64.2.2. Duas portas para leitoras: Fita magnética, Wiegand;

4.64.2.3. Duas entradas fixas para contato de porta e pedido de saída (REX);

4.64.2.4. Duas saídas, uma para parada de porta e uma para uso geral;

4.64.2.5. Firmware armazenado em memória flash, download em segundo plano das atualizações de firmware suportadas;

4.64.2.6. Suportar até 200.000 portadores de cartão, 50.000 transações de evento buffer;

4.64.2.7. Suportar no mínimo 128 níveis de acesso por usuário do cartão;

4.64.2.8. Datas e horários de ativação e desativação de crachás programáveis;

4.64.2.9. Dezesseis formatos de cartão por controladora inteligente para uma porta;

4.64.2.10. Suporte de modelo biométrico Proximity, iCLASS, multiClass, MIFARE, e DESFIRE;

4.64.2.11. Suporte máximo número PIN de nove dígitos;

4.64.2.12. Suporte para controle de elevadores

4.64.2.13. Suporte para OSDP – Open Supervised Device Protocol

4.64.2.14. Capacidades anti-dupla passagem melhoradas Controles aninhados anti-dupla passagem global rígida, e flexível controle anti-dupla passagem por tempo, controle de duas pessoas, controle de uma ou de duas pessoas designadas, controle de carona, e limite de ocupação;

4.64.2.15. Suporte para download seletivo;

4.64.2.16. Suporte de catraca;

4.64.2.17. Nove LEDs de status;

4.64.2.18. Entrada dedicada para violação de “tamper” e falha de alimentação elétrica;

4.64.2.19. Possuir suporte para comunicação criptografada AES 256bit entre a controladora inteligente e os módulos de expansão;

4.64.2.20. Possuir suporte para comunicação criptografada AES 256bit entre a controladora inteligente e o servidor do sistema de controle de acesso;

4.64.2.21. 6 MB de memória flash on-board disponível para banco de dados de ativos e portadores de cartão;

4.64.2.22. Suportar memória de 50,000 eventos respaldada por bateria para registro de eventos

4.64.2.23. Bateria recarregável on-board com até duas semanas de suporte;

4.64.2.24. Suporte máximo para dois leitores por barreira física (porta);

4.64.2.25. Alimentação 12 VDC ou PoE;

4.64.2.26. Componente reconhecido UL294, em conformidade com CE, ROHS, FCC Parte 15 Classe A, criptografia certificada pelo NIST.

4.64.3. CARACTERÍSTICAS DA LEITOR DE CARTÕES E BIOMETRIA:

4.64.3.1. Sensor biométrico do tipo óptico com resolução mínima de 500 dpi;

4.64.3.2. Possuir memória básica para até 500 usuários com capacidade de expansão para até 10.000 usuários;

4.64.3.3. Permitir o cadastro de até 3 dedos por usuário, sendo 2 para uso normal e 1 para coação;

4.64.3.4. Possuir display 2.8” WVGA touchsreen;

4.64.3.5. Capacidade de operação no modo 1:1 ou 1:N;

4.64.3.6. Possibilitar a identificação de usuários no modo 1:N de até 10.000 usuários em menos de 1 segundo;

4.64.3.7. Permitir o armazenamento de log de até 1.000.000 de eventos no próprio leitor;

4.64.3.8. Possuir leitor Smartcard HID Iclass interno de 13.56MHz;

4.64.3.9. Somente Biometria 1:N

4.64.3.9.1. Biometria + Cartão

4.64.3.9.2. Somente Cartão

4.64.3.10. Flexibilidade de operação permitindo a definição do modo de autenticação por usuário, à saber:

4.64.3.10.1. Somente Biometria 1:N

4.64.3.10.2. Biometria + Senha

4.64.3.10.3. Somente Senha

4.64.3.10.4. Biometria + Cartão

4.64.3.10.5. Biometria + Cartão + Senha

4.64.3.10.6. Somente Cartão

4.64.3.11. Possibilidade de armazenamento e leitura de templates gravados na memória do cartão inteligente Iclass;

4.64.3.12. O leitor biométrico deverá possuir algoritmo de software capaz de identificar tentativas de fraudes utilizando dedos falsos (FFD – Fake Finger Detection);

4.64.3.13. O sensor biométrico deverá possuir certificação FBI PIV IQS;

4.64.3.14. Capacidade de ser alimentado através de Switches POE e também por fonte DC externa 12 ou 24 volts;

4.64.3.15. Possuir saída Wiegand para conexão à uma controladora de acesso padrão de mercado;

4.64.3.16. Suporte para OSDP – Open Supervised Device Protocol

4.64.3.17. Possibilitar o controle direto do bloqueio físico sem a necessidade de controladora de acesso através de suas entradas e saídas digitas;

4.64.3.18. Possuir uma entrada padrão Wiegand para conexão de um leitor externo;

4.64.3.19. Possuir no mínimo um relê de saída para acionamento de bloqueios físicos e ainda 2 entradas e 2 saídas digitais para controle e acionamentos diversos;

4.64.3.20. Comunicação Ethernet para gerenciamento do leitor e distribuição dos templates;

4.64.3.21. Grau de proteção contra intemperes: IP65;

4.64.3.22. Grau de proteção contra vandalismo: IK08;

4.64.3.23. Possuir tamper switch para monitoramento de tentativas de violação;

4.64.3.24. Certificações: CE, CB, FCC e RoHS.

4.64.4. CARACTERÍSTICAS DA LEITOR DE CARTÕES E BIOMETRIA:

4.64.4.1. Sensor biométrico do tipo óptico com resolução mínima de 500 dpi;

4.64.4.2. Possuir memória básica para até 500 usuários com capacidade de expansão para até 10.000 usuários;

4.64.4.3. Permitir o cadastro de até 3 dedos por usuário, sendo 2 para uso normal e 1 para coação;

4.64.4.4. Possuir display 2.8” WVGA touchsreen;

4.64.4.5. Capacidade de operação no modo 1:1 ou 1:N;

4.64.4.6. Possibilitar a identificação de usuários no modo 1:N de até 10.000 usuários em menos de 1 segundo;

4.64.4.7. Permitir o armazenamento de log de até 1.000.000 de eventos no próprio leitor;

4.64.4.8. Possuir leitor Smartcard HID Iclass interno de 13.56MHz;

4.64.4.9. Somente Biometria 1:N

4.64.4.9.1. Biometria + Cartão

4.64.4.9.2. Somente Cartão

4.64.4.10. Flexibilidade de operação permitindo a definição do modo de autenticação por usuário, à saber:

4.64.4.10.1. Somente Biometria 1:N

4.64.4.10.2. Biometria + Senha

4.64.4.10.3. Somente Senha

4.64.4.10..4. Biometria + Cartão

4.64.4.10.5. Biometria + Cartão + Senha

4.64.4.10.6. Somente Cartão

4.64.4.11.Possibilidade de armazenamento e leitura de templates gravados na memória do cartão inteligente Iclass;

4.64.4.12. O leitor biométrico deverá possuir algoritmo de software capaz de identificar tentativas de fraudes utilizando dedos falsos (FFD – Fake Finger Detection);

4.64.4.13. O sensor biométrico deverá possuir certificação FBI PIV IQS;

4.64.4.14. Capacidade de ser alimentado através de Switches POE e também por fonte DC externa 12 ou 24 volts;

4.64.4.15. Possuir saída Wiegand para conexão à uma controladora de acesso padrão de mercado;

4.64.4.16. Possibilitar o controle direto do bloqueio físico sem a necessidade de controladora de acesso através de suas entradas e saídas digitas;

4.64.4.17. Possuir uma entrada padrão Wiegand para conexão de um leitor externo;

4.64.4.18. Possuir no mínimo um relê de saída para acionamento de bloqueios físicos e ainda 2 entradas e 2 saídas digitais para controle e acionamentos diversos;

4.64.4.19. Comunicação Ethernet para gerenciamento do leitor e distribuição dos templates;

4.64.4.20. Grau de proteção contra intemperes: IP65;

4.64.4.21. Grau de proteção contra vandalismo: IK08;

4.64.4.22. Possuir tamper switch para monitoramento de tentativas de violação;

4.64.4.23. Certificações: CE, CB, FCC e RoHS.

4.64.5. CARACTERÍSTICAS DA FECHADURA ELETROMAGNÉTICA:

4.64.5.1. Deve possuir acessórios para fixação em portas de madeiras e de vidro e vir acompanhada de todos os acessórios, como placas de fixação, parafusos e tudo o que for necessário para fixação e adequação às instalações;

4.64.5.2. Deve suportar no mínimo 150kg de carga quando instalada;

4.64.5.3. Deve consumir no máximo 350ma quando alimentada em 12VDC;

4.64.5.4. Deve possuir sensor que informe ao sistema se a porta encontra-se aberta ou fechada.

4.64.5.5. Acabamento em alumínio anodizado.

4.64.6. CARACTERÍSTICAS DA MOLA HIDRÁULICA:

4.64.6.1. Mola hidráulica aérea para o controle de portas, com o sistema pinhão e cremalheira ou equivalente, para que a porta feche sozinha, suavemente e sem ruídos;

4.64.6.2. Tamanho compacto, permitindo controle hidráulico total a partir de 180°

4.64.6.3. (Ângulo de abertura da porta), com harmonia e compatibilidade com o ambiente arquitetônico;

4.64.6.4. Na cor cinza;

4.64.6.5. Possuir braço de parada que permita manter a porta aberta em qualquer ângulo de 0° a 105º durante o tempo que for necessário, sem necessidade de outro complemento ou acessório;

4.64.6.6. Tamanho único para as três potências;

4.64.6.7. Reversível para portas direita ou esquerda;

4.64.6.8. Não necessitar de ferramentas especiais p/ instalação e substituição;

4.64.6.9. Originalmente já possa ser instalada na porta ou no batente;

4.64.6.10. Não deve exigir manutenção;

6.64.6.11. Indicada para qualquer tipo de porta ou portão;

6.64.6.12. Revestimento em esmalte sintético (poliuretano), aplicado de forma a assegurar proteção, beleza e durabilidade.

4.64.7. CARACTERÍSTICAS DA BOTOEIRA:

4.64.7.1. Botoeira de acionamento interno (botoeira-push button) para abertura de porta (saída) via equipamentos de controle acesso para abertura de portas

4.64.7.2. Deve vir fixado em espelho para instalação em caixa interna ou externa 4 x 2”;

4.64.7.3. Deve funcionar em modo passivo, sendo que deverá ter alternativa de funcionamento em sistema NF e na (normalmente aberto e normal fechado)

4.64.7.4. Deve vir acompanhado de todos os acessórios para fixação, como parafusos e tudo o que for necessário para fixação e adequação às instalações;

4.64.7.5. Deve possuir chave push button e ser retrátil após usa utilização;

4.64.7.6. Acabamento da placa e do botão em material aço inoxidável;

4.64.8. CARACTERÍSTICAS DA BOTOEIRA DE EMERGÊNCIA:

4.64.8.1. Botoeiras de acionamento interno de emergência (botoeira - push button) para abertura de porta;

4.64.8.2. Botão de acionamento interno (botoeira- push button) para abertura de porta (saída), via equipamentos de controle acesso para abertura de portas;

4.64.8.3. Utilizado para liberar a porta controlada em caso de incêndio ou pânico, fazendo com que o acesso esteja garantido em situações de risco. É do tipo “quebre o vidro” na cor verde conforme leis e normas vigentes.

4.64.8.4. Deve ser ligado em série com a alimentação das fechaduras eletroímãs, cortando-a mecanicamente em caso de sinistro.

4.64.8.5. Deve funcionar em modo passivo, sendo que deverá ter alternativa de funcionamento em sistema NF e na (normalmente aberto e normal fechado)

4.64.8.6. Deve vir acompanhado de todos os acessórios para fixação, como parafusos e tudo o que for necessário para fixação e adequação às instalações;

4.64.8.7. Deve possuir chave push button e ser retrátil após usa utilização;

4.64.9. CARACTERÍSTICAS DA FONTE DE 1 AH COM CAIXA:

4.64.9.1. Deve trabalhar em conjunto com a bateria para garantir a alimentação da carga mesmo na falta de energia

4.64.9.2. Deve possuir gabinete metálico com capacidade para abrigar uma bateria de 7AH, a fonte e a placa controladora (VER TAMANHO DA PLACA)

4.64.9.3. Deve sinalizar flutuação de bateria

4.64.9.4. Deve sinalizar falta de energia na rede

4.64.9.5. Deve sinalizar rompimento de fusível

4.64.9.6. Especificações elétricas:

4.64.9.7. Tensão de entrada: 220/127 VCA - Tensão de saída 12,7 VCC - Corrente de saída 1A

4.65. FORNECIMENTO DE ACESSO TIPO IV

O Kit cancela é composto dos seguintes itens:

01 cancela veicular automática com laço magnético;

01 controladora

01 leitor UHF

O kit deve ser totalmente gerenciável e homologado para trabalhar com o software da Unidade de Processamento e Armazenamento de Controle de Acesso, devendo ser fornecido com todos os acessórios e licenças necessárias para a integração ao sistema de controle de acesso.

4.65.1. CARACTERÍSTICAS DA CANCELA VEICULAR AUTOMÁTICA COM LAÇO MAGNÉTICO:

4.65.1.1. Ter garantia de fábrica de no mínimo 10 (onze) milhões de ciclos de abertura limitados a 2 anos.

4.65.1.2.Tempo médio entre as manutenções de 2 anos (dado estatístico).

4.65.1.3. Placa eletrônica embutida com no mínimo as seguintes funções programáveis: controle de semáforo, amarelo piscante, fechamento retardado, contagem sequencial de passagem de veículos, entre outros.

4.65.1.4. Dispositivo anti-esmagamento com laço indutivo e fechamento automático

4.65.1.5. Braço em alumínio escamoteável.

4.65.1.6. Na falta de energia a cancela deverá permitir a operação de forma manual.

4.65.1.7. Deverá possuir pintura eletroestática a pó em poliéster de no mínimo 70 microns resistente a UV, ou equivalente que tenha igual ou superior resistência.

4.65.1.8. Tempo de abertura de no máximo 2 segundos.

4.65.1.9. Ser de fácil instalação e manutenção.

4.65.1.10. Possuir no mínimo 4 entradas digitais de controle.

4.65.1.11. Deverá trabalhar com voltagem de 220v ou bivolt.

4.65.1.12. Tempo de fechamento de no máximo 3 segundos.

4.65.1.13. Comprimento do braço de 4 metros ou similar.

4.65.1.14. O laço magnético veicular deverá possuir as seguintes características:

4.65.1.14.1. Deve detectar motocicleta, veículos de passeio ou caminhões;

4.65.1.14.2. Deve possuir tempo de resposta a partir de 2ms;

4.65.1.14.3. Deve permitir a seleção de pelo menos 4 frequências de trabalho;

4.65.1.14.4. Deve operar em modo de presença na entrada do laço indutivo;

4.65.1.14.5. Deve operar em modo pulso de 0,1s na entrada do laço indutivo;

4.65.1.14.6. Deve possuir sintonia automática;

4.65.1.14.7. Deve possuir consumo máximo de 70ma;

4.65.1.14.8. Deve possuir led de indicação de detecção de veículo;

4.65.1.14.9. Deve possuir led de sinalização de falha de laço indutivo aberto;

4.65.1.14.10. Deve possuir pelo menos 7 níveis de sensibilidade;

4.65.1.14.11. Deve possuir led de indicação de detecção de veículo;

4.65.14.12. Deve possuir chave de reset manual;

4.65.14.13. Deve possuir saída de sinal de detecção com contato de relê normalmente aberto ou fechado;

4.65.14.14. Deve operar a temperaturas de pelo menos -20ºc até 50ºc;

4.65.14.15. Deve possuir instalação em trilho din;

4.65.14.16. Deve possuir proteção contra surtos na entrada do laço indutivo;

4.65.14.17. Deve possuir alimentação 24VDC ou 12VDC;

4.65.14.18. Deve possuir proteção contra inversão de polaridade na entrada de alimentação;

4.65.14.19. Deve possuir um laço indutivo pré-fabricado para detecção de motocicletas, veículos de passeio ou caminhões.

4.65.2. CARACTERÍSTICAS DO CONTROLADOR DE ACESSO IP

A controladora deverá fornecer uma solução cartão única com interface de dois leitores para controle de uma porta. A controladora deve fornecer controle de acesso completo do Fabricante

com um dispositivo que pode ser instalado na borda do perímetro seguro. A controladora deverá ser compacta e uma opção para alimentação via PoE ou 12 VDC. A controladora deve ter processamento robusto e memória on-board que deve permitir que milhares de usuários de cartão de acesso que possam ser armazenados localmente por tolerância de falhas. A controladora deve suportar a maioria dos recursos de controle de acesso padrão do sistema de gestão de segurança. A controlada deverá permitir alterar a sua configuração para que possa gerenciar até oito (08) módulos de expansão via RS-485.

4.65.2.1. A Controladora de acesso IP deverá conter as seguintes características mínimas:

4.65.2.1.1. Porta Primária: 10/100 Ethernet;

4.65.2.1.2. Duas portas para leitoras: Fita magnética, Wiegand;

4.65.2.1.3. Duas entradas fixas para contato de porta e pedido de saída (REX);

4.65.2.1.4. Duas saídas, uma para parada de porta e uma para uso geral;

4.65.2.1.5. Firmware armazenado em memória flash, download em segundo plano das atualizações de firmware suportadas;

4.65.2.1.6. Suportar até 200.000 portadores de cartão, 50.000 transações de evento buffer;

4.65.2.1.7. Suportar no mínimo 128 níveis de acesso por usuário do cartão;

4.65.2.1.8. Datas e horários de ativação e desativação de crachás programáveis;

4.65.2.1.9. Dezesseis formatos de cartão por controladora inteligente para uma porta;

4.65.2.1.10. Suporte de modelo biométrico Proximity, iCLASS, multiClass, MIFARE, e DESFIRE;

4.65.2.1.11. Suporte máximo número PIN de nove dígitos;

4.65.2.1.12. Suporte para controle de elevadores

4.65.2.1.13. Suporte para OSDP – Open Supervised Device Protocol

4.65.2.1.14. Capacidades anti-dupla passagem melhoradas Controles aninhados anti-dupla passagem global rígida, e flexível controle anti-dupla passagem por tempo, controle de duas pessoas, controle de uma ou de duas pessoas designadas, controle de carona, e limite de ocupação;

4.65.2.1.15. Suporte para download seletivo;

4.65.2.1.16. Suporte de catraca;

4.65.2.1.17. Nove LEDs de status;

4.65.2.1.18. Entrada dedicada para violação de “tamper” e falha de alimentação elétrica;

4.65.2.1.19. Possuir suporte para comunicação criptografada AES 256bit entre a controladora inteligente e os módulos de expansão;

4.65.2.1.20. Possuir suporte para comunicação criptografada AES 256bit entre a controladora inteligente e o servidor do sistema de controle de acesso;

4.65.2.1.21. 6 MB de memória flash on-board disponível para banco de dados de ativos e portadores de cartão;

4.65.2.1.22. Suportar memória de 50,000 eventos respaldada por bateria para registro de eventos

4.65.2.1.23. Bateria recarregável on-board com até duas semanas de suporte;

4.65.2.1.24. Suporte máximo para dois leitores por barreira física (porta);

4.65.2.1.25. Alimentação 12 VDC ou PoE;

4.65.2.1.26. Componente reconhecido UL294, em conformidade com CE, ROHS, FCC Parte 15 Classe A, criptografia certificada pelo NIST.

4.65.3. CARACTERÍSTICAS DA LEITOR DE CARTÕES E BIOMETRIA:

4.65.3.1. Sensor biométrico do tipo óptico com resolução mínima de 500 dpi;

4.65.3.2. Possuir memória básica para até 500 usuários com capacidade de expansão para até 10.000 usuários;

4.65.3.3. Permitir o cadastro de até 3 dedos por usuário, sendo 2 para uso normal e 1 para coação;

4.65.3.4. Possuir display 2.8” WVGA touchsreen;

4.65.3.5. Capacidade de operação no modo 1:1 ou 1:N;

4.65.3.6. Possibilitar a identificação de usuários no modo 1:N de até 10.000 usuários em menos de 1 segundo;

4.65.3.7. Permitir o armazenamento de log de até 1.000.000 de eventos no próprio leitor;

4.65.3.8. Possuir leitor Smartcard HID Iclass interno de 13.56MHz;

4.65.3.9. Somente Biometria 1:N

4.65.3.9.1. Biometria + Cartão

4.65.3.9.2. Somente Cartão

4.65.3.10. Flexibilidade de operação permitindo a definição do modo de autenticação por usuário, à saber:

4.65.3.10.1. Somente Biometria 1:N

4.65.3.10.2. Biometria + Senha

4.65.3.10.3. Somente Senha

4.65.3.10.4. Biometria + Cartão

4.65.3.10.5. Biometria + Cartão + Senha

4.65.3.10.6. Somente Cartão

4.65.3.11. Possibilidade de armazenamento e leitura de templates gravados na memória do cartão inteligente Iclass;

4.65.3.12. O leitor biométrico deverá possuir algoritmo de software capaz de identificar tentativas de fraudes utilizando dedos falsos (FFD – Fake Finger Detection);

4.65.3.13. O sensor biométrico deverá possuir certificação FBI PIV IQS;

4.65.3.14. Capacidade de ser alimentado através de Switches POE e também por fonte DC externa 12 ou 24 volts;

4.65.3.15. Possuir saída Wiegand para conexão à uma controladora de acesso padrão de mercado;

4.65.3.16. Suporte para OSDP – Open Supervised Device Protocol

4.65.3.17. Possibilitar o controle direto do bloqueio físico sem a necessidade de controladora de acesso através de suas entradas e saídas digitas;

4.65.3.18. Possuir uma entrada padrão Wiegand para conexão de um leitor externo;

4.65.3.19. Possuir no mínimo um relê de saída para acionamento de bloqueios físicos e ainda 2 entradas e 2 saídas digitais para controle e acionamentos diversos;

4.65.3.20. Comunicação Ethernet para gerenciamento do leitor e distribuição dos templates;

4.65.3.21. Grau de proteção contra intemperes: IP65;

4.65.3.22. Grau de proteção contra vandalismo: IK08;

4.65.3.23. Possuir tamper switch para monitoramento de tentativas de violação;

4.65.3.24. Certificações: CE, CB, FCC e RoHS.

4.65.4. CARACTERÍSTICAS DO LEITOR UHF

4.65.4.1. As leitoras de TAG UHF deverão ser fornecidas com as seguintes características:

4.65.4.1.1. Suportar padrão de comunicação OSDP e Wiegand

4.65.4.1.2. Deve possuir interface de usuário configurável em campo através de uma porta ethernet para facilitar a manutenção.

4.65.4.1.3. Deve possuir fácil configuração com a interface da web incorporado suporta credenciais compatíveis com padrão isso 18000-6c.

4.65.4.1.4 Garante autenticidade dos dados e privacidade dos dados através de criptografia AES 128 bits

4.65.4.1.5. Inibe a clonagem de dados pela associação de um objeto a uma credencial frequência de transmissão 902-928 MHZ

4.65.4.1.6. Range de leitura de 3 a 5 metros

4.65.4.1.7. Tensão de entrada (VDC) 12 VDC ou 24 VDC

4.65.4.1.8. Deve possuir no mínimo as seguintes certificações: UL294 / CUL (EUA E CANADÁ), CB SCHEME, CERTIFICAÇÃO FCC (EUA), IC (CANADÁ), CE(UE), IFETEL (MÉXICO), ANATEL

4.65.4.1.9. (Brasil)

4.65.4.1.10. Compatibilidade com cartões de UHF EPC classe 1 GEN 2, GEN 18000-6C

4.65.4.1.11. Hardware de elemento seguro certificado por eal5+ - fornece proteção à prova de violação de chaves/operações criptográficas

4.65.4.1.12. Deve ser uma caixa de policarbonato resistente, projetada para ambientes rigorosos e suportar intempéries;

4.65.4.1.13. Deve possuir encapsulamento em policarbonato resistente, de acordo com o padrão UL94;

4.65.4.1.14. Grau de proteção IP65

4.65.4.1.15. Deve possuir terminal de conectores para ligação de cabos;

4.65.4.1.16. Deve suportar instalação segundo os padrões Wiegand com no mínimo 150 mts de cabo de 18AWG;

4.65.4.1.17. Deve suportar temperatura de operação de no mínimo -35 a 65ºc;

4.65.4.1.18. Deve suportar operação com umidade de 5 a 95%, não condensada, no mínimo;

4.65.4.1.19. Deve possuir um ano de garantia.

4.66. FORNECIMENTO DE CREDENCIAL TIPO I

4.66.1. O chip HF do cartão com dupla tecnologia deve apresentar as seguintes características:

4.66.1.1. Deve suportar a frequência de operação de 13,56Mhz;

4.66.1.2. Deve possuir segurança de transmissão de RF entre a leitora e o cartão deve ser criptografado através de algoritmo seguro;

4.66.1.3. Deve suportar área de aplicação protegidas por código de 64bits de leitura/gravação;

4.66.1.4. Deve suportar a comunicação entre o cartão e a leitora de no máximo 100ms;

4.66.1.5. Deve possuir design passivo e funcionar sem a necessidade de bateria e suportar no mínimo 100.000 leituras e gravação;

4.66.1.6. Deve possuir memória de no mínimo 16k;

4.66.1.7. Deve suportar no mínimo os padrões ISO/IEC 15693 e 14443B;

4.66.1.8. Deve suportar retenção de dados de no mínimo 10 anos;

4.66.1.9. Deve suportar a distância de até 10 centímetros;

4.66.2. O chip UHF deve apresentar as seguintes características:

4.66.2.1. Range de leitura de 3 até 5 metros

4.66.2.2. Tag passivo sem bateria;

4.66.2.3. Frequência de transmissão entre 860 a 960 MHz

4.66.2.4. Cartão de memória com capacidade de retenção de 50 anos e 100.000 ciclos

4.66.2.5. Usa proteção de lógica (senha de acesso) para evitar não autorizado acesso à memória.

4.66.2.6. Alcance típico de leitura de até 5 metros

4.66.2.7. Frequência de operação 860-960 MHz

4.66.2.8. Interface de RF Conforme sugerido por ISO18000-6C e EPC Class-1 Gen-2

4.66.3. O material do cartão deve apresentar as seguintes características:

4.66.3.1. Cartão Construção Composição 40% Poliéster / 60% PVC

4.66.3.2. Dimensões 5,40 x 8,57 x 0,084 centímetros

4.66.3.3. Temperatura Operacional -40 ° C a 70 ° C

4.66.3.4. Umidade de operação 5 - 95% sem condensação

4.67. FORNECIMENTO DE CREDENCIAL TIPO II

4.67.1. Deve suportar a frequência de operação de 13,56 Mhz;

4.67.2. Memória de no mínimo 8 Kbit, para instalação de aplicações internas no cartão;

4.67.3. A transmissão de RF entre a leitora e o cartão deve ser criptografada através de algoritmo seguro, suportando também criptografia padrão AES;

4.67.4. Deve suportar área de aplicação protegidas por código de 128 bits de leitura/gravação;

4.67.5. Deve suportar a realização de autenticação mútua entre cartão e leitor baseado na ISO/IEC 24727-3 2008;

4.67.6. Deve suportar a comunicação entre o cartão e a leitora de no máximo 100 ms;

4.67.7. Deve possuir design passivo e funcionar sem a necessidade de bateria e suportar no mínimo 500.000 leituras e gravação;

4.67.8. Deve possuir numeração externa do cartão, que poderá ser gravado com jato de tinta ou laser;

4.67.9. Deve possuir garantia vitalícia comprovada no site do fabricante;

4.67.10. Deve suportar no mínimo o padrão ISO/IED 7810, 7816 e 14443A;

4.67.11. Deve suportar retenção de dados de no mínimo 20 anos;

4.67.12. Deve suportar a distância de leitura quando apresentada à leitora de de 6 até 33 cm dependendo do leitor;

4.67.13. Deve possuir no máximo 0,09 cm de espessura, ser construído em PVC laminado flexível tipo ISO CR80;

4.67.14. Deve suportar a temperatura operacional na faixa mínima de -40° a 70° C;

4.67.15. Deve suportar umidade operacional na faixa mínima de 5 a 95% não condensado.

4.67.16. Suportar One Time Password;

4.68. FORNECIMENTO DE CREDENCIAL TIPO III

4.68.1. As identidades digitais devem garantir privacidade, segurança e integridade dos dados e serem fácil de administrar através de um gerenciamento completo do ciclo de vida das credenciais digitais (criação, distribuição e cancelamento).

4.68.2. A identidade digital deve habilitar os telefones celulares para uso na corporação inteira como um cartão ou outra forma de identificação, para aumentar a produtividade do funcionário. A Identidade celular móvel deve oferecer um modelo de preservação de privacidade para proteger dados de identificação pessoal contra acessos não autorizados.

4.68.3. As IDs móveis devem ser baseadas em objetos de dados protegidos por criptografia com os mais avançados protocolos e algoritmos criptográficos. Esses objetos de dados portáteis são distribuídos de dispositivo a dispositivo utilizando um protocolo seguro para garantir a proteção de ponta a ponta entre o dispositivo e a leitora, independente do padrão de comunicações subjacente.

4.68.4. As Identidades Digitais devem ter capacidade de vinculação de dados com o MAC do dispositivo do usuário. Ser armazenado em área segura do chip do smartphone. Além disso devem ser agnóstica, ou seja, portátil para qualquer dispositivo capaz de executar o aplicativo da Identidade Digital. A Identidade Digital deve estar contida em um Objeto de dados protegidos por criptografia que maximiza o modelo de dados e a segurança da informação

4.68.5. As transações entre o smartphone e o leitor deve ser baseados em padrões internacionais de mensagens seguras, a autenticação forte e confidencialidade dos dados. Padrões de segurança usados: NIST e NSA Suite B criptografia, AES-128 e SHA-256

4.68.6. Toda transação com a Identidade Digital deve ser única e não pode ser clonada (gravado e reproduzido). Deve suportar ataques de reflexão, ataques replay, supressão mensagem, mensagem de reordenamento, modificação mensagem, mensagem de concatenação e inserção de mensagens

4.68.7. O aplicativo da Identidade Digital deve usar um protocolo de mensagens segura e é usado para proteger a comunicação over-the-air entre o telefone eo leitor, independentemente se NFC ou Bluetooth inteligente é usado. O Seos não dependem da segurança da tecnologia de transporte

4.68.8. As Identidades Digitais móveis devem ser armazenadas na área sensível do aparelho, no mesmo local que as outras senhas de aplicativos e informações sensíveis são armazenadas.

4.68.9. As Identidades Digitais devem ser armazenadas com criptografia AES-128 e a transmissão no ar deve ser criptografada usando AES-128 / CMAC96. E o O aplicativo seguro das Identidades Digitais.

4.68.10. O aplicativo de Identidade Digital deve estar disponível no App Store da Apple e Google Play. E este aplicativo deve ser capaz de gerenciar múltiplas Identidades Digitais. E também possuir compatibilidade com Android 4.3 e 4.4 ou superior e também com IOS 7.0 ou superior.

4.68.11. Deverá possuir Portal de Identidades Digitais Seguras para Controle de Acesso:

4.68.11.1. O Portal de Identidades Digitais Seguras usada para o Controle de Acesso deve ser capaz de gerenciar o ciclo de vida completo das Identidades Digitais Móveis (criação, distribuição e cancelamento)

4.68.11.2. Plataforma baseada em nuvem, aplicações web seguras e tecnologias de dispositivos móveis padrão para criar uma solução que é fácil de implementar e simples de gerenciar. Deve suportar uma população crescente de dispositivos Android e iPhone.

4.68.11.3. Deve ser uma aplicação web intuitiva que aumenta a eficiência operacional, gestão da matrícula e provisionamento de Identidades Digitais. Nenhum físicas de codificação, impressão, ou retornos são necessárias.

4.69. FORNECIMENTO DE SISTEMA DE GESTÃO DE SEGURANÇA

As especificações técnicas apresentadas abaixo visam estabelecer os requisitos mínimos para o fornecimento de equipamentos para atender a solução do GAP-DF maximizando o nível de segurança na unidade supracitada com o uso do sistema de gestão de segurança, aplicando o módulo de controle de acesso e visitantes.

O sistema de controle de acesso deverá ter com principal característica permitir ou negar o acesso de pessoas nas cancelas, catracas e portas de acesso ou qualquer barreira física para controle das mesmas, baseado na leitura de cartões de alta tecnologia sem contato ou com a leitura biométrica, ou qualquer outro dispositivo de identificação de usuário, bem como nas informações constantes na base de dados, a partir de cadastramento previamente executado.

Serão utilizados níveis de segurança de acordo com as características da edificação e em consonância com os padrões mundiais de segurança, que terão flexibilidade para serem alterados a qualquer momento, visto que o sistema será modular, expansível não exigindo a instalação de um novo ou diferente sistema de gestão de segurança, e apto a realizar diferentes programações, em função das necessidades apresentadas.

Deverá ser do mesmo fabricante das controladoras de acesso ou homologados entre si desde que comprovado em ambos os sites web.

4.69.1. Módulo de Controle de Acesso:

4.69.1.1. Todo o Módulo de Controle de Acesso de pessoas e veículos deverá ser realizado através leitura de cartões de alta tecnologia, e/ou biométricos de impressão digital, ou em conjunto leitura de cartões de alta tecnologia sem contato, ou leitura de cartões de alta tecnologia sem contato com ou sem teclado integrado, todos estes associados a portas, a catracas, e as cancelas e etc.

4.69.2. Características do Módulo de Controle de Acesso:

4.69.2.1. O Módulo de Controle de Acesso deverá ser composto por equipamentos baseados em hardware e software, com capacidade de integrar múltiplas funções de segurança, incluindo gerenciamento, controle de monitoramento de cartões, alarmes, produção de cartões com foto, interface com os subsistemas de vigilância de vídeos ou subsistemas de banco de dados;

4.69.2.2. O Módulo de Controle de Acesso deverá ser compatível com o protocolo de comunicação de rede padrão TCP/IP entre a aplicação/usuários, estações de trabalho do operador, controladoras e os subsistemas de base de dados, usando conectividade do Ethernet 10/100MB sobre topologias de rede LAN/WAN;

4.69.2.3. O Módulo de Controle de Acesso deverá ser escalável em aplicação cliente/servidor e web Server para integração das operações de segurança integrada de modo a incluir gerenciamento e administração da configuração do sistema, comando e controle, e monitoramento em tempo real, gerenciamento de alarmes, vídeo, credenciamento de visitantes, e interface com subsistemas e aplicações de bancos de dados;

4.69.2.4. O Módulo de Controle de Acesso deverá usar uma arquitetura aberta;

4.69.2.5. O Módulo de Controle de Acesso deverá ser desenvolvido de forma a que todos os módulos do sistema (controle de acesso, alarme, monitoramento administração de ID, administração de visitantes, gerenciamento de ativos e vídeo digital) sejam entregues ao cliente uma aplicação com um código forte capaz de rodar em máquinas 64bits;

4.69.2.6. O Módulo de Controle de Acesso deverá permitir que em uma única interface de usuário possa trabalhar com diversos idiomas tais como: árabe (ARA), Croata (VFC), Checa (JEC), holandês (NID), inglês (ENU), finlandês (FIN), francês (FRA), alemão (DEU), Hebraico (HEB), italiano (ITA), polonês (PLK), Português Brasil (PTB), russo (RUS), espanhol (SPA), Sueco (SVE) entre outras;

4.69.2.7. O Módulo de Controle de Acesso deverá exigir apenas uma única licença, presente no servidor físico ou ambiente virtual VMware para que o sistema opere normalmente. O Sistema de gestão de segurança deverá permitir que o usuário tenha capacidade de ativar, excluir ou reparar a licença sem a intervenção do fabricante;

4.69.2.8. O Módulo de Controle de Acesso deverá possuir à capacidade de logon único (single sign-on) dos administradores e operadores do sistema, autenticando no sistema utilizando a mesma conta do domínio Windows (AD);

4.69.2.9. No processo de logon único o sistema deverá permitir que os administradores ou operadores rodem os aplicativos interativos sem a necessidade de digitar o nome ou senha, com isso irá facilitar a administração e manutenção do sistema, deverá permitir também a autenticação via API de scripts, executando os scripts usando a conta do Windows, permitindo assim um logon mais seguro e restringindo as ações do usuário;

4.69.2.10. O Módulo de Controle de Acesso deverá monitorar e integrar perfeitamente com sistemas inteligentes, painéis de alarme, interfones, painéis de incêndios, entres outros sistemas;

4.69.2.11. O Módulo de Controle de Acesso deverá permitir comunicação com suas controladoras de sistema inteligente, através de RS-485, RS-232, Ethernet TCP/IP (IPV4 e IPV6) ou se necessário a utilização de modens:

4.69.2.11.1. Microsoft SQL Server 2008 SP2 e SP3, Microsoft SQL Server 2008 R2 SP1 e SP2, Microsoft SQL Server SP1 2012 e Express, Microsoft SQL Server 2014 e Express, Oracle 11g R1 e

R2 Server e Oracle Server 12 c R1. Dados Oracle podem residir em plataformas Windows ou UNIX.

4.69.2.12. O Módulo de Controle de Acesso deverá suportar servidores Microsoft Windows Clustering, Hot Standby e servidores tolerantes a falhas de hot Standby e tolerante;

4.69.2.13. O Módulo de Controle de Acesso deverá suportar no mínimo 32 leitoras para controle de acesso e 5 clientes e um número ilimitado de entradas ou saídas de alarme, e podendo ser expansível até um número ilimitado de leitoras para controle de acesso, de clientes e entradas e saídas de alarme;

4.69.2.14. O Módulo de Controle de Acesso deverá fornecer manuais e ferramentas funcionais como descrição e especificações gerais do sistema, procedimento e instalação do Módulo de Controle de Acesso, modelos dos diagramas dos componentes e esquemas do sistema;

4.69.2.15. O Módulo de Controle de Acesso deverá suportar diversos modelos de leituras de cartões de alta tecnologia simultaneamente no sistema, podendo assim suportar cartões de várias tecnologias;

4.69.2.16. O Módulo de Controle de Acesso deverá possuir um sistema de circuito fechado de televisão nativo, ou deverá possuir recursos para integrações com sistemas de circuito fechado de televisão de terceiros;

4.69.2.17. O Módulo de Controle de Acesso deverá suportar um número ilimitado de leitoras de cartões de alta tecnologia, câmeras de vídeos, pontos de entrada e saídas de relés, pontos de detecção de intrusão e pontos de detecção e alarme de incêndio.

4.69.3. Componentes do Módulo de Controle de Acesso:

4.69.3.1. O Módulo de Controle de Acesso deverá possuir ou ter a possibilidade dos seguintes recursos:

4.69.3.1.1. Controle de acesso: ser capaz de conceder ou negar o acesso dos usuários, permitir configuração de níveis de acesso, determinar entradas e saídas de alarme, permitir gerenciar e monitorar áreas de monitoramento, como controle de pessoas e antipassback, segmentação e controle de fuso horário;

4.69.3.1.2. Monitoramento de alarme: deverá fornecer informações sobre o tempo e o local do alarme em conjunto com a sua prioridade, classificar os alarmes pendentes ou inserir novos alarmes com base em qualquer um dos seguintes atributos;

4.69.3.1.2.1. Prioridade, data e hora do alarme;

4.69.3.1.2.2. Descrição do alarme:

4.69.3.1.2.2.1. Leitor;

4.69.3.1.2.2.2. Gerenciamento;

4.69.3.1.2.2.3. Entrada e Saída de acesso;

4.69.3.1.2.2.4. Nome do usuário.

4.69.3.1.3. Permitir que dependendo do tipo de alarme de emergência, o Módulo de Controle de Acesso possa enviar mensagens alfanuméricas ou e-mails, e mostrar em tempo real na tela do operador um número limitado de alarmes especificados pelo operador;

4.69.3.1.4.O Módulo de Controle de Acesso deverá possuir um mecanismo de limpeza automático (FIFO), dos alarmes carregados, quando atingir o limite estabelecido pelo operador;

4.69.3.1.5. Administração de credenciais: deverá possuir um módulo de gestão integrada e transparente das credenciais, onde terá como principal funcionalidade o gerenciamento dos usuários dos cartões, como captura das imagens, das biometrias quando necessárias, e bem como também a importação e exportação de dados de funcionários e permitir modificar os direitos de acesso dos usuários do cartão;

4.69.3.1.6. Gerenciamento de Vídeo Digital: deverá permitir a visualização do vídeo, em tempo real para cada alarme associado, e ou a criação de um segmento de vídeo gravado especificando a duração de um pré-alarme e um pós-alarme;

4.69.3.1.7. Deve permitir gravadores digitais de múltiplo fabricantes do mercado, e possuir suporte a câmeras IP e codificadores de vídeo de vários fabricantes;

4.69.3.1.8. Administração de detecção de intrusão: deverá permitir a integração de maneira transparente, com painéis de detecção de intrusão e painéis de detecção avançados, de diversos fabricantes tais como BOSCH e Honeywell, entre outros;

4.69.3.1.9. Deve permitir que dentro do Módulo de Controle de Acesso, o operador possa realizar o monitoramento e gerenciamento dos recursos de detecção de intrusão, tais como armar ou desarmar uma área, monitorar o status do dispositivo e ativar funções globais, como auditoria;

4.69.3.1.10. Gestão de Ativos: deverá permitir a administração e o acompanhamento em tempo real de todos os ativos do cliente. A gestão de ativos deverá possuir um gerenciamento centralizado, para que o administrador do sistema possa gerar relatórios de atribuições atuais, bem como o histórico da alocação do ativo para cada usuário do cartão. O Módulo de Controle de Acesso deverá ser capaz de restringir a passagem de um ativo por pontos de controle não autorizado para o usuário;

4.69.3.1.11. Gestão de visitantes: deverá possuir um módulo de visitantes, baseado em um aplicativo web, para que o cliente possa registrar e acompanhar os visitantes nas dependências da empresa. A gestão de visitante deverá permitir que o operador possa registrar um visitante, marcar a entrada e a saída do visitante, capturar uma foto ou outros tipos de identificações tais como documento pessoal ou passaporte, ou até mesmo verificar visitas pré-agendadas;

4.69.3.1.12. Gerenciamento remoto de níveis de acesso: deverá permitir que os operadores ou administradores do sistema possam remotamente atribuir ou remover um nível de acesso aos

usuários de cartão. Todas as transações relacionadas com a atribuição ou cancelamento dos níveis de acesso devem ser completamente registradas com data e hora e o operador que realizou esta operação;

4.69.3.1.13. Interface com terceiros: O Módulo de Controle de Acesso deverá possuir integração com hardware e software, fornecendo um servidor OPC padrão da indústria para permitir a exportação de todo e qualquer alarme e eventos para clientes OPC, tais como automação de edifícios e/ou sistemas de controle de processo. A interface de terceiros deverá permitir integração com sistema de alarme de incêndios, sistemas de segurança pessoal, sistemas de intercomunicação, sistemas de recursos humanos;

4.69.3.1.14. Administração do Sistema: deverá permitir a criação de estações de controle, definições de permissão de acesso no sistema, grupos de acessos, relatórios, mapas e etc;

4.69.3.1.15. Soluções mobile: deverá suportar uma arquitetura mobile, para os clientes com necessidade de computação móvel;

4.69.3.1.16. Criação de Cartões: deverá possuir um módulo que permita a criação e design dos layouts de cartões que podem ser impressos no cartão;

4.69.3.1.17. Criação de formulários e telas: deverá possuir a possibilidade de criação e edição de campos personalizados no sistema, tais como RG, CPF entre outros;

4.69.3.1.18. Criação de Mapas Gráficos: deverá permitir a criação e edição de mapas gráficos que permitirá que os operadores do sistema possam operar as portas ou qualquer elemento do sistema via o mapa;

4.69.3.1.19. Interfaces de aplicações programáveis: deverá permitir um conjunto de interfaces programáveis de aplicativo (API), para integração de hardware de terceiros ou soluções de softwares baseado em arquiteturas aberta;

4.69.3.1.20. Importação de dados: deverá permitir que o cliente possa importar as informações de usuários dos cartões no banco de dados, criando novos registros;

4.69.3.1.21. Troca Bidirecional de dados: deverá suportar a transferência de dados bidirecional em tempo real de banco de dados de terceiros, tais como sistemas de recursos humanos, entre outros;

4.69.3.1.22. Servidores redundantes: deverá possuir uma arquitetura de servidor de banco de dados redundantes e tolerantes a falha.

4.69.4. Funcionalidades do Módulo de Controle de Acesso.

4.69.4.1. O Módulo de Controle de Acesso deverá ter as seguintes funcionalidades mínimas relativas à capacidades do sistema:

4.69.4.1.1. Deverá permitir a criação e armazenamento de no mínimo de 255 zonas de tempo, onde para cada fuso horário deverá ter no mínimo 6 intervalos de tempo;

4.69.4.1.2. Deverá permitir que cada usuário do cartão de acesso, tenha no mínimo 128 níveis de acesso, totalizando assim 32.000 níveis de acesso. Este níveis de acesso serão compostos de uma combinação de leitoras de cartão de acesso e zonas de tempo;

4.69.4.1.3. Deverá permitir comandos de usuário através de teclado;

4.69.4.1.4. Deverá permitir níveis de acesso temporários com datas de início e datas de fim no acesso;

4.69.4.1.5. Deverá permitir grupos de acesso com no mínimo 6 níveis de acesso, chegando até 32 níveis de acesso por grupo;

4.69.4.1.6. O Módulo de Controle de Acesso deverá permitir a configuração de liberação de acesso lento, através de um comando de fuso horário padrão até que seja apresentado cartões de acesso válidos para conceder acesso;

4.69.4.1.7. Deverá permitir segmentação do banco de dados, para qual cada segmento possa ter seu próximo grupo de titulares de cartão, hardware e parâmetros do sistema, e etc;

4.69.4.1.8. Deverá permitir no mínimo de 8 características de controle de áreas como Antipassback, global obrigatório, controle de antipassback, controle de duas pessoas, e limite de ocupação;

4.69.4.1.9. Deverá suportar link de eventos de entradas ou saídas de alarme global, onde a qualquer entrada ou saída de alarme ou evento possa ser vinculado a qualquer outra entrada ou saída de alarme do sistema, podendo assim permitir a criação de listas de funções baseadas nos alarmes, ou até mesmo funções que mude automaticamente o modo de operação das leitoras de controle de acesso (liberado ou bloqueado), ou fechamento de áreas. O Módulo de Controle de Acesso deverá suportar até 6 ações por lista de funções;

4.69.4.1.10. O Módulo de Controle de Acesso deverá suportar vários recursos de utilização nos cartões de acesso tais como:

4.69.4.1.10.1. Controle de acesso através de acompanhamento do usuário do cartão de acesso por uma pessoa responsável;

4.69.4.1.10.2. Limitar a quantidade de acessos do usuário do cartão de acesso, em determinados locais como restaurantes;

4.69.4.1.10.3. Suportar que o sistema não alarme, quando o usuário do cartão de acesso possua alguma necessidade especial, e precise que a porta fique mantida a porta por um tempo maior;

4.69.4.1.10.4. Suportar nativamente um recurso de ronda de guarda, onde o usuário de cartão de acesso, passe por pontos pré-definidos e o sistema possa controlar o tempo e o local por onde o usuário está passando para verificação do ambiente.

4.69.1.11. O Módulo de Controle de Acesso deverá suportar múltiplos tipos de formatos de cartão de acesso, onde a controladora ira possuir no seus registros até 8 tipos de formatos, podendo assim

o trabalhar simultaneamente com vários modelos de leitoras de controle de acesso, não precisando se desfazer de leitoras de acesso já instaladas;

4.69.1.12. O Módulo de Controle de Acesso deverá permitir que o operador, possa monitorar todos os alarmes na área de monitoramento designado, onde poderão estabelecer controles de permissões e dos seguintes modos:

4.69.1.12.1. Modos de acesso;

4.69.1.12.2. Portas abertas;

4.69.1.12.3. Saídas de relé e leitora de cartão de acesso;

4.69.1.12.4. Mascaramento\Desmascaramento de alarme;

4.69.1.12.5. Executar lista de funções.

4.69.4.1.13. O Módulo de Controle de Acesso deverá possuir um módulo de captura de imagem do usuário do cartão de acesso, compatíveis com câmeras de vídeo com iluminação de RGB flash, e câmeras de entrada composta com fontes de entrada s-video e USB, com resolução mínima resolução 1024x968;

4.69.4.1.14. Deverá permitir a importação de imagens dos usuários dos cartões de acesso, em diversos formatos tais como:

4.69.4.1.14.1. Bitmaps (.bmp, .DIB);

4.69.4.1.14.2. JPEG (.jpg);

4.69.4.1.14.3. JIFF (.jif);

4.69.4.1.14.4. ZSoft PCX ou DCX (.PCX, .dcx);

4.69.4.1.14.5. Adobe Photoshop (.PSD);

4.69.4.1.14.6. CALS Raster (.cal);

4.69.4.1.14.7. GEM ou Ventura IMG (.img);

4.69.4.1.14.8. POLIA de IBM (.ica);

4.69.4.1.14.9. Raster do WordPerfect (.wpg);

4.69.4.1.14.10. Macintosh PICT (PCT);

4.69.4.1.14.11. Portable Network Graphics;

4.69.4.1.14.12. TIFF (.tif);

4.69.4.1.14.13. Metarquivo do Windows (. WMF, EMF);

4.69.4.1.14.14. Targa (TGA);

4.69.4.1.14.15. Kodak Photo CD (PCD);

4.69.4.1.14.16. Kodak Flashpix (.fpx);

4.69.4.1.14.17. Encap Post Script (. EPS);

4.69.4.1.15. Deverá possuir um módulo de verificação de dados biométricos, onde a verificação dos dados estará disponível para o operador, com uma perfeita integração da biometria com o Módulo

de Controle de Acesso, não sendo necessário o uso de softwares de terceiros, e muito menos a captura dos dados biométricos separados do Módulo de Controle de Acesso;

4.69.4.1.16. O Módulo de Controle de Acesso deverá permitir que o operador possa fazer uma verificação on-line do usuário de cartão de acesso, através de uma foto, quando o tiver passando em um ponto de controle;

4.69.4.1.17. O Módulo de Controle de Acesso deverá possuir um portal WEB, para todos os usuários de cartão de acesso ou para os designados ver as portas que tenha recusado o acesso recentemente, e permitir que o operador possa ver a lista de portas configuráveis disponíveis para enviar uma solicitação de autorização de acesso, para os aprovadores responsáveis pela aquela área;

4.69.4.1.18. O Módulo de Controle de Acesso deverá possuir integração com sistemas de chamada antecipadas para diversos fabricantes de elevadores;

4.69.4.1.19. O Módulo de Controle de Acesso deverá possuir um rastreamento de quaisquer dispositivos (leitoras de controle de acesso, cartões de acesso, entre outros) que esteja cadastrado no sistema;

4.69.4.1.20. O Módulo de Controle de Acesso deverá permitir ou negar o acesso de um usuário através de um pop-up;

4.69.4.1.21. O Módulo de Controle de Acesso deverá fornecer respostas da base de dados on-line sem degradar a performance do sistema;

4.69.4.1.22. O Módulo de Controle de Acesso deverá possuir uma gestão de vídeo digital, disponível com uma solução totalmente integrada com o monitoramento do controle de acesso, onde deverá permitir um gerenciamento de todos os ativos, alarmes e etc;

4.69.4.1.23. A gestão de vídeo digital, deverá fornecer uma arquitetura completamente modular, oferecendo atualizações dos equipamentos, e permitir a visualização ao vivo ou vídeo gravado de todas as imagens do sistema;

4.69.4.1.24. A gestão de vídeo digital deverá possuir recursos de buscas de vídeos inteligentes, exportação de vídeo;

4.69.4.1.25. O Módulo de Controle de Acesso deverá possuir um gama muito grande de relatórios de todos os recursos e dispositivos do sistema;

4.69.4.1.26. O Módulo de Controle de Acesso deverá fornecer alguns relatórios pré-programados tais como:

4.69.4.1.26.1. Proprietário do cartão;

4.69.4.1.26.2. Administração do sistema e configurações do equipamento;

4.69.4.1.26.3. Programações do sistema e eventos;

4.69.4.1.26.4. Acesso a leitora;

4.69.4.1.26.5. Acesso a andares;

4.69.4.1.26.6. Tempo e frequência;

4.69.4.1.26.7. Histórico de alarmes;

4.69.4.1.26.8 Histórico de cartões;

4.69.4.1.26.9. Histórico do operador.

4.69.4.1.27. O Módulo de Controle de Acesso deverá permitir os operadores executar a configuração da página, pré-visão de relatório on-line, imprimir e exportar relatórios em múltiplos formatos de arquivos de destinos tais como:

4.69.4.1.27.1. Crystal Reports;

4.69.4.1.27.2. Data Interchange Format;

4.69.4.1.27.3. Excel;

4.69.4.1.27.4. HTML;

4.69.4.1.27.5. Lotus;

4.69.4.1.27.6. ODBC;

4.69.4.1.27.7. Texto não formatado.

4.69.4.1.28. O Módulo de Controle de Acesso deverá suportar conectividade direta a base de dados de modo a facilitar geração de relatórios através de aplicações externas na base de dados de terceiros através de SQL Server, Microsoft Access e Crystal Reports.

4.69.5. Especificações mínimas dos servidores e estações de trabalho:

4.69.5.1. O Sistema de gestão de segurança deverá integrar todo o Módulo de Controle de Acesso, gerenciamento de credenciais, gestão de vídeo digital, gestão de detecção de intrusão, gerenciamento de ativos e gerenciamento visitantes entre outros. O sistema gestão de segurança deverá permitir a incorporação e integração dos servidores, estações de trabalhos cliente do Módulo de Controle de Acesso.

4.69.5.2. As operações administrativas do sistema de gestão de segurança deverão estar disponíveis a partir de qualquer estação de trabalho cliente no sistema.

4.69.5.3. Servidor de Bando de Dados:

4.69.5.3.1. Todos os dados do sistema deverão residir no servidor de banco de dados. Além disso, todos os bancos de dados e processamento de consulta devem acontecer no servidor. O servidor de banco de dados também poderá ser utilizados como estação de trabalho com completa capacidade monitoramento de alarme, processamento de imagens, exibição, edição e recursos administrativos. As Controladoras Inteligentes do Sistema também podem ser conectadas ao servidor de banco de dados.

4.69.5.4. Especificações mínimas de Servidor:

4.69.5.4.1. Intel® ® Xeon E5-1603, Quad Core, 2.8 GHz Turbo, 10 MB, ou superior;

4.69.5.4.2. Fonte de alimentação 635 W;

4.69.5.4.3. Memoria 8 GB (4 por 2 GB) 1600 MHz, DDR3 ou superior;

4.69.5.4.4. 8x DVD + RW, ou superior;

4.69.5.4.5. 1 TB 3.5 polegadas Serial ATA (7200RPM) disco rígido, ou superior;

4.69.5.4.6. 1GB NVIDIA® Quadro® K600 (1 DP & 1 DVI-eu) (1 DP-DVI e 1 adaptador DVI-VGA);

4.69.5.4.7. Porta Ethernet RJ45 10/100MB, ou superior;

4.69.5.4.8. Alto-falantes do chassi interno, ou superior;

4.69.5.4.9. (6) portas USB 2.0, (4) portas USB 3.0, ou superior;

4.69.5.4.10. (1) porta serial, ou superior;

4.69.5.4.11. Teclado / mouse USB, ou superior.

4.70. FORNECIMENTO DE ESTAÇÃO DE CADASTRO DE FUNCIONÁRIO

4.70.1. As estações de cadastro de funcionários devem ser fornecidas para todos os sistemas que exigem estações de trabalho adicionais. A estação de trabalho cliente deve ser utilizada como estação de trabalho para monitoramento de alarmes, e/ou administração, gestão de credenciais, gestão de visitantes, gestão de vídeo digital e/ou gestão de ativos.

4.70.2. Deverá vir acompanhada com mesmo software de gerenciamento de controle de acesso (Client).

4.70.3. v

4.70.3.1. Intel Xeon E5-2603, Quad Core, 1,8 GHz, 10 MB, 6,4 GT, ou superior;

4.70.3.2. 4GB (2 x 2GB) 1600MHz DDR3 RDIMM CEE, ou superior;

4.70.3.3. 8 x Slimline DVD + /-RW, ou superior;

4.70.3.4. 500 GB 2,5 polegadas SATA 3.0 Gb/s - 7200RPM, ou superior;

4.70.3.5. 1 GB NVIDIA Quadro K600 (DP de saída 1 & 1 DVI), ou superior;

4.70.3.6. Windows 7 Professional 64 bit, ou superior;

4.70.4. Leitor Biométrico de mesa

4.70.4.1. Deverá ser totalmente compatível com o software e com os leitores de biometria ofertados.

4.71. FORNECIMENTO DE SISTEMA DE GESTÃO DE VISITANTES

4.71.1. Deverá ser fornecido software para gerenciamento de visitantes;

4.71.2. Deverá ser do mesmo fabricante do software de gerenciamento de controle de acesso.

4.72. FORNECIMENTO LICENÇA ADICIONAL 64 LEITORES

4.72.1. Deverá ser fornecido licença adicional de 64 leitores;

4.72.2. Deverá ser do mesmo fabricante do software de gerenciamento de controle de acesso.

4.73. FORNECIMENTO DE ESTAÇÃO DE CADASTRO DE VISITANTES

4.73.1. As estações de cadastro de visitantes devem ser fornecidas para todos os sistemas que exigem estações de trabalho adicionais. A estação de trabalho cliente deve ser utilizada como estação de trabalho para monitoramento de alarmes, e/ou administração, gestão de credenciais, gestão de visitantes, gestão de vídeo digital e/ou gestão de ativos.

4.73.2. Deverá vir acompanhada com mesmo software de gerenciamento de controle de acesso (Client).

4.73.3. Especificações mínimas da estação de trabalho cliente:

4.73.3.1. Intel Xeon E5-2603, Quad Core, 1,8 GHz, 10 MB, 6,4 GT, ou superior;

4.73.4.2. 4GB (2 x 2GB) 1600MHz DDR3 RDIMM CEE, ou superior;

4.73.4.3. 8 x Slimline DVD + /-RW, ou superior;

4.73.4.4. 500 GB 2,5 polegadas SATA 3.0 Gb/s - 7200RPM, ou superior;

4.73.4.5. 1 GB NVIDIA Quadro K600 (DP de saída 1 & 1 DVI), ou superior;

4.73.4.6. Windows 7 Professional 64 bit, ou superior;

4.73.5. Leitor de Cartão de mesa

4.73.5.1. Deverá ser totalmente compatível com o software ofertado.

4.74. SERVIÇO DE MANUTENÇÃO DE CONTROLE DE ACESSO

4.74.1. Contempla testes, configurações, limpeza dos kits de catracas, cancelas e portas, regulagem de mecanismos, substituição e encaminhamento para a garantia do fabricante.

4.74.2. Deverá prover todos os equipamentos, materiais, mão de obra, ferramentas, para manutenção e configuração, bem como executar todas as operações necessárias para manutenção preventiva e corretiva, com o devido encaminhamento dos equipamentos e sistemas para garantia dos fabricantes, mantendo-os em operação durante o período de garantia.

4.74.3. Todos componentes da solução, como troca de qualquer equipamento que venha apresentar defeito, bem como a atualização das versões dos softwares de sistema operacional dos equipamentos e de gerenciamento dos mesmos, substituição ou encaminhamento para garantia do fabricante.

4.75. SERVIÇO DE RETIRADA DE PONTO CONTROLE DE ACESSO

4.75.1. Contempla serviço de retirada de pontos de controle de acesso em diversos locais como catracas, leitores, kit portas, cancelas, etc. Locação de equipamentos necessários, utilização de ferramentas necessárias, retirada de infraestrutura existente, com bota fora de material.

4.76. CURSO DE TREINAMENTO E TRANSFERÊNCIA DE CONHECIMENTO EM CONTROLE DE ACESSO

4.76.1. Treinamento, capacitação e repasse tecnológico no modelo de operação assistida de acordo com o volume do serviço.

4.76.2. Aderido, com duração mínima de 20 horas, a ser administrada pelo proponente ou pelo fabricante dos itens da solução de CA (controle de acesso) com certificação dos profissionais do órgão contratante com pelo menos 75% de presença.

4.77. FORNECIMENTO DE SWITCH CORE TIPO I COM INSTALAÇÃO E CONFIGURAÇÃO

4.77.1. O equipamento deverá ser novo (sem uso) e estarem na linha atual de produção do fabricante;

4.77.2. Deverá acompanhar os kits de fixação para instalação em rack de 19";

4.77.3. Deverá possuir fonte interna de alimentação com operação em 110/220VAC, 60Hz, com chaveamento automático de tensão;

4.77.4. Deverá possuir fonte redundante interna no equipamento.

4.77.5. Possuir capacidade de empilhamento com o mínimo de 4 (duas) unidades. A velocidade de empilhamento deve ser de mínimo de 10 Gbps;

4.77.6. Quando empilhados, todos os switches deverão ser gerenciados por um único endereço IP, não sendo permitido clustering ou individualização de endereços IP em cada switch. A configuração de empilhamento não deve exigir que sejam adicionados endereços IP para cada switch da pilha, diminuindo a complexidade de administração e configuração;

4.77.7. O equipamento deverá vir acompanhado de todo hardware, softwares e conectividades necessários para o empilhamento incluindo cabos para conexão simples (entre dois switchs) de no mínimo 0,50m.

4.77.8. Possuir, no mínimo, 24 (vinte e quatro) interfaces 1GbE SFP

4.77.9. Deve possuir no mínimo 4 portas 1GbE SFP. Estas portas poderão ser do tipo Combo (RJ45/SFP).

4.77.10. Deve possuir no mínimo 4 portas 10GbE SFP+. Essas portas devem operar de forma independente das outras, totalizando 32(trinta e duas) portas ativas simultaneamente;

4.77.11. Deve possuir capacidade de switching de no mínimo 136 Gbps para switches com arquitetura empilhável;

4.77.12. Deve possuir a capacidade de encaminhamento de pacotes de no mínimo 101Mpps (medidos com pacotes de 64 bytes).

4.77.13. Deve permitir a configuração de rotas estáticas em IPv4, para hosts ou redes;

4.77.14. Deve suportar, no mínimo, 64 rotas estáticas IPv4;

4.77.15. Deve implementar Policy Based Routing;

4.77.16. Deve implementar o mínimo de 4000 Vlans de acordo com o padrão IEEE 802.1Q;

4.77.17. Suportar jumbo frames - 9KB;

4.77.18. Deve suportar o gerenciamento de 24 switches através de uma mesma interface;

4.77.19. Permitir a configuração de Private VLAN;

4.77.20. Deve implementar reconhecimento de telefones IP e a associação automática de seu tráfego em VLAN específica (Voice VLAN).

4.77.21. Deve implementar os seguintes padrões IEEE:

4.77.21.1. IEEE 802.1D MAC Bridges;

4.77.21.2. IEEE 802.1p Priority;

4.77.21.3. IEEE 802.1Q VLANs;

4.77.21.4. IEEE 802.1s (MSTP);

4.77.21.5. IEEE 802.1w Rapid Reconfiguration of Spanning Tree;

4.77.21.6. IEEE 802.1AB Link Layer Discovery Protocol (LLDP);

4.77.21.7. IEEE 802.1P (CoS);

4.77.21.8. IEEE 802.1X Port Based Network Access Control;

4.77.21.9. IEEE 802.3 Type 10BASE-T;

4.77.21.10. IEEE 802.3ab 1000BASE-T;

4.77.21.11. IEEE 802.3ad Link Aggregation Control Protocol (LACP);

4.77.21.12. IEEE 802.3i 10BASE-T;

4.77.21.13. IEEE 802.3x Flow Control;

4.77.21.14. IEEE 802.3z 1000BASE-X;

4.77.21.15. IEEE 802.1D, Spanning Tree Protocol (STP);

4.77.21.16. IEEE 802.1w, Rapid Spanning Tree Protocol (RSTP);

4.77.21.17. IEEE 802.1s, Multiple Spanning Tree Protocol (MSTP);

4.77.21.18. Devem permitir a criação mínima de 08 instâncias de MSTP;

4.77.21.19. Deve implementar a funcionalidade Root Guard;

4.70.22. Permitir a implementação de mecanismos de proteção contra ataques de negação de serviço;

4.77.23. Permitir o gerenciamento através de navegador WEB padrão, com capacidade de visualizar o status de cada porta e configurar, pelo menos, VLANs, STP e parâmetros de velocidade das portas;

4.77.24. Deve permitir a configuração total do equipamento via CLI (Command Line Interface);

4.77.25. Deve possibilitar a priorização de frames através da implementação de IEEE 802.1p;

4.77.26. Deve implementar mecanismo de escalonamento de fila StrictPriority (SP queueing) e WRR;

4.77.27. Deve implementar mecanismos de limitação de banda com granularidade mínima de 64Kb;

4.77.28. Deve permitir a execução de scripts baseado em eventos;

4.77.29. Deve implementar cliente de atualização de data e hora por meio do emprego do protocolo SNTP ou NTP;

4.77.30. Deve implementar cliente de atualização de data e hora por meio do emprego do protocolo SNTv6;

4.77.31. Deve implementar os protocolos SNMP v2 e SNMP v3;

4.77.32. Deve possuir a capacidade de enviar SNMP Traps em caso de falhas no sistema de ventilação, alimentação elétrica ou em caso de operação em alta temperatura;

4.77.33. Deve suportar os seguintes grupos RMON: Statistics, History, Alarms e Events;

4.77.34. Deve implementar o protocolo TELNET;

4.77.35. Deve implementar o protocolo TFTP ou o protocolo SFTP;

4.77.36. Deve implementar o protocolo SSHv2;

4.77.37. Deve implementar controle de acesso por meio do protocolo IEEE 802.1x, PortBased Network Access Control com os seguintes recursos, no mínimo:

4.77.38. Múltiplos suplicantes por porta;

4.77.39. Associação dinâmica de VLANs;

4.77.40. Deve implementar VLAN de convidados (Guest VLAN);

4.77.41. Deverá implementar autenticação baseada em MAC Address;

4.77.42. Deve implementar associação automática de VLAN de acordo com usuário autenticado;

4.77.43. Deve possibilitar a criação de ACLs baseadas em informações da camada de enlace (endereços MAC), da camada de rede (endereços IP) e de informações da camada de transporte (portas UDP e TCP) para controle de tráfego;

4.77.44. Deve permitir a aplicação de QoS baseado em critérios estabelecidos por meio de Listas de Controle de Acesso;

4.77.45. Deve implementar mecanismo de controle de tráfego do tipo broadcast;

4.77.46. Deve possibilitar o espelhamento do tráfego de rede (portmirroring/monitor), para fins de análise, de no mínimo uma porta de origem para uma porta de destino.

4.77.47. Deve ser Dual Stack, ou seja, possuir suporte a IPv6 e IPv4;

4.77.48. Deve implementar MLD snooping, tanto v1 quanto v2;

4.77.49. Deve suportar RADIUS Accounting conforme RFC 2866;

4.77.50. Deve implementar DHCP Client;

4.77.51. Deve implementar DHCP Relay;

4.77.52. Deve suportar LLDP;

4.77.53. O switch deve possuir mecanismo de proteção contra ataques do tipo negação de serviço;

4.77.54. Deve suportar Protocolo Telnet sobre transporte IPv6 (Telnet over IPv6 transport);

4.77.55. Ping sobre transporte IPv6 (Ping over IPv6 transport);

4.77.56. Traceroute sobre transporte IPv6 (Traceroute over IPv6 transport);

4.77.57. Deve suportar NTPv6;

4.77.58. Deve suportar tunelamento 6-to-4;

4.77.59. Deve suportar resolução do nomes DNS sobre IPv6;

4.77.60. Deve possuir DHCP Snooping, suportando também inspeção dinâmica de ARP;

4.77.61. Deve permitir implementar configurações de scripts automaticamente conforme eventos e de acordo com horários pré-estabelecidos;

4.77.62. Implementar IGMP Snooping (v1, v2 e v3). O comutador deve ser capaz de fazer "snooping" de pacotes IGMPv1, IGMPv2 e IGMPv3.

4.77.63. Suportar OSPFv2 ou OSPFv3

4.77.64. Suportar RIPv1 ou RIPv2

4.77.65. Possuir DHCP Server e DHCP Relay

4.77.66. Suportar DVMRP

4.77.67. Suportar VRRP

4.77.68. Suportar ECMP

4.77.69. Deve estar em conformidade com as RFC's: 950, 932, 1191, 4541, 2246, 2865, 2866 e 2868;

4.77.70. Deve estar em conformidade com a RFC 768;

4.77.71. Deve estar em conformidade com a RFC 791;

4.77.72. Deve estar em conformidade com a RFC 793;

4.77.73. Deve possuir a capacidade de aprendizagem automática de no mínimo 16.000 endereços MAC;

4.77.74. O hardware deverá possuir no mínimo 1Gb de memória RAM

4.77.75. Deverá possuir dois slots virtuais para armazenamento de firmware

4.77.76. Deve vir acompanhado dos cabos de ligação elétrica necessários à instalação e ao seu perfeito funcionamento;

4.77.77. Deve ter porta console RS-232 e vir acompanhado do cabo de comunicação;

4.77.78. Módulos, portas, cabos ou qualquer outro acessório fundamental para o correto funcionamento do empilhamento deverão ser fornecidos;

4.77.79. Possuir garantia de 12 (doze) meses.

4.77.80. Deve ser fornecido com todas as licenças de software necessárias para o funcionamento integral de todas as funcionalidades disponíveis para o equipamento;

4.77.81. O equipamento ofertado deve possuir certificado de homologação na Anatel, de acordo com a resolução n° 242;

4.78. FORNECIMENTO DE SWITCH DE ACESSO COM PORTAS GIGABIT E POE COM INSTALAÇÃO E CONFIGURAÇÃO

4.78.1. O equipamento deverá ser novo (sem uso) e estarem na linha atual de produção do fabricante;

4.78.2. Deverá acompanhar os kits de fixação para instalação em rack de 19";

4.78.3. Deverá possuir fonte interna de alimentação com operação em 110/220VAC, 60Hz, com chaveamento automático de tensão;

4.78.4. Possuir, no mínimo, 24 (vinte e quatro) interfaces 10/100/1000BASE-T PoE com conectores RJ45, não sendo permitido o fornecimento de conectores RJ21, RJ.5, harmônicos ou similares;

4.78.5. Deve possuir 4 portas 1GbE SFP. Essas portas devem operar de forma independente das outras, totalizando 28(vinte e oito) portas ativas simultaneamente;

4.78.6. Deve suportar IEEE 802.3af e 802.3at em todas as portas 10/100/1000BaseT ofertadas;

4.78.7. A capacidade da fonte para alimentar dispositivos sem PoE, sem considerar o consumo do switch, deve ser pelo menos 375W.

4.78.8. Deve possuir capacidade de switching de no mínimo 56 Gbps.

4.78.9. Deve possuir a capacidade de encaminhamento de pacotes de no mínimo 41Mpps (medidos com pacotes de 64 bytes).

4.78.10. Deve implementar o mínimo de 4000 Vlans de acordo com o padrão IEEE 802.1Q;

4.78.11. Suportar jumbo frames - 10KB;

4.78.12. Deve suportar o gerenciamento de 32 switches através de uma mesma interface;

4.78.13. Permitir a configuração de Private VLAN;

4.78.14. Deve implementar reconhecimento de telefones IP e a associação automática de seu tráfego em VLAN específica (Voice VLAN).

4.78.15. Deve implementar os seguintes padrões IEEE:

4.78.15.1. IEEE 802.1D MAC Bridges;

4.78.15.2. IEEE 802.1p Priority;

4.78.15.3. IEEE 802.1Q VLANs;

4.78.15.4. IEEE 802.1s (MSTP);

4.78.25.5. IEEE 802.1w Rapid Reconfiguration of Spanning Tree;

4.78.25.6. IEEE 802.1AB Link Layer Discovery Protocol (LLDP);

4.78.25.7. IEEE 802.1P (CoS);

4.78.25.8. IEEE 802.1X Port Based Network Access Control;

4.78.25.9. IEEE 802.3ab 1000BASE-T;

4.78.25.10. IEEE 802.3ad Link Aggregation Control Protocol (LACP);

4.78.25.11. IEEE 802.3i 10BASE-T;

4.78.25.12. IEEE 802.3x Flow Control;

4.78.25.13. IEEE 802.3z 1000BASE-X;

4.78.25.14. IEEE 802.1D, Spanning Tree Protocol (STP);

4.78.25.15. IEEE 802.1w, Rapid Spanning Tree Protocol (RSTP);

4.78.25.16. IEEE 802.1s, Multiple Spanning Tree Protocol (MSTP);

4.78.25.17. Deve permitir a criação mínima de 08 instâncias de MSTP;

4.78.16. Deve implementar a funcionalidade Root Guard;

4.78.17. Permitir a implementação de mecanismos de proteção contra ataques de negação de serviço;

4.78.18. Permitir o gerenciamento através de navegador WEB padrão, com capacidade de visualizar o status de cada porta e configurar, pelo menos, VLANs, STP e parâmetros de velocidade das portas;

4.78.19. Deve permitir a configuração total do equipamento via CLI (Command Line Interface);

4.78.20. Deve possibilitar a priorização de frames através da implementação de IEEE 802.1p;

4.78.21. Deve implementar mecanismo de escalonamento de fila StrictPriority (SP queueing) e WRR;

4.78.22. Deve implementar mecanismos de limitação de banda com granularidade mínima de 64Kb;

4.78.23. Deve permitir a execução de scripts baseado em eventos;

4.78.24. Deve implementar cliente de atualização de data e hora por meio do emprego do protocolo SNTP ou NTP;

4.78.25. Deve implementar cliente de atualização de data e hora por meio do emprego do protocolo SNTv6;

4.78.26. Deve implementar os protocolos SNMP v2 e SNMP v3;

4.78.27. Deve possuir a capacidade de enviar SNMP Traps em caso de falhas no sistema de ventilação, alimentação elétrica ou em caso de operação em alta temperatura;

4.78.28. Deve suportar os seguintes grupos RMON: Statistics, History, Alarms e Events;

4.78.29. Deve implementar o protocolo TELNET;

4.78.30. Deve implementar o protocolo TFTP ou o protocolo SFTP;

4.78.31. Deve implementar o protocolo SSHv2;

4.78.32. Deve implementar controle de acesso por meio do protocolo IEEE 802.1x, PortBased Network Access Control com os seguintes recursos, no mínimo:

4.78.33. Múltiplos suplicantes por porta;

4.78.34. Associação dinâmica de VLANs;

4.78.35. Deve implementar VLAN de convidados (Guest VLAN);

4.78.36. Deverá implementar autenticação baseada em MAC Address;

4.78.37. Deve implementar associação automática de VLAN de acordo com usuário autenticado;

4.78.38. Deve possibilitar a criação de ACLs baseadas em informações da camada de enlace (endereços MAC), da camada de rede (endereços IP) e de informações da camada de transporte (portas UDP e TCP) para controle de tráfego;

4.78.39. Deve permitir a aplicação de QoS baseado em critérios estabelecidos por meio de Listas de Controle de Acesso;

4.78.40. Deve implementar mecanismo de controle de tráfego do tipo broadcast;

4.78.41. Deve possibilitar o espelhamento do tráfego de rede (portmirroring/monitor), para fins de análise, de no mínimo uma porta de origem para uma porta de destino.

4.78.42. Deve ser Dual Stack, ou seja possuir suporte a IPv6 e IPv4;

4.78.43. Deve implementar MLD snooping, tanto v1 quanto v2;

4.78.44. Deve suportar RADIUS Accounting conforme RFC 2866;

4.78.45. Deve implementar DHCP Client;

4.78.46. Deve implementar DHCP Relay;

4.78.47. Deve suportar LLDP;

4.78.48. O switch deve possuir mecanismo de proteção contra ataques do tipo negação de serviço;

4.78.49. Deve suportar Protocolo Telnet sobre transporte IPv6 (Telnet over IPv6 transport);

4.78.50. Ping sobre transporte IPv6 (Ping over IPv6 transport);

4.78.51. Traceroute sobre transporte IPv6 (Traceroute over IPv6 transport);

4.78.52. Deve suportar NTPv6;

4.78.53. Deve suportar tunelamento 6-to-4;

4.78.54. Deve suportar resolução do nomes DNS sobre IPv6;

4.78.55. Deve possuir DHCP Snooping, suportando também inspeção dinâmica de ARP;

4.78.56. Deve permitir implementar configurações de scripts automaticamente conforme eventos e de acordo com horários pré-estabelecidos;

4.78.57. Deve estar em conformidade com as RFC’s: 950, 932, 1191, 4541, 2246, 2865, 2866 e 2868;

4.78.58. Deve estar em conformidade com a RFC 768;

4.78.59. Deve estar em conformidade com a RFC 791;

4.78.60. Deve estar em conformidade com a RFC 793;

4.78.61. Deve possuir a capacidade de aprendizagem automática de no mínimo 16.000 endereços MAC;

4.78.62. Deve vir acompanhado dos cabos de ligação elétrica necessários à instalação e ao seu perfeito funcionamento;

4.78.63. Deve ter porta console RS-232 e vir acompanhado do cabo de comunicação;

4.78.64. Módulos, portas, cabos ou qualquer outro acessório fundamental para o correto funcionamento do empilhamento deverão ser fornecidos;

4.78.65. Possuir garantia de 12 (doze) meses.

4.78.66. Deve ser fornecido com todas as licenças de software necessárias para o funcionamento integral de todas as funcionalidades disponíveis para o equipamento;

4.78.67. O equipamento ofertado deve possuir certificado de homologação na Anatel, de acordo com a resolução n° 242;

4.79. FORNECIMENTO DE INTERFACES SFP TIPO I – COM INSTALAÇÃO

4.79.1. Módulos SFP/Mini-GBIC 1000BASE-SX LC para fibra multi-modo 50 micron OM3, para todos os switches gerenciáveis:

4.79.1.1. Compatibilidade total com os switches gerenciáveis deste edital, e com o padrão SFP MSA, assegurado pelo fabricante do switch.

4.79.1.2. Devem possuir capacidade de detecção de ausência/presença de sinal no enlace 1000BASE-X.

4.79.1.3. Módulos ópticos devem possuir conector LC para fibra óptica.

4.79.1.4. Os módulos devem possuir velocidade de 1Gbps por canal unidirecional (SFP MSA), permitindo transmissão full-duplex em wire-speed (mínimo de 1Gbps úteis reais por canal unidirecional, 2Gbps úteis full-duplex, utilizando os dois canais).

4.80. FORNECIMENTO DE INTERFACES SFP TIPO II – COM INSTALAÇÃO

4.80.1. Módulos SFP/Mini-GBIC 1000BASE-LX LC para fibra mono-modo, para todos os switches gerenciáveis;

4.80.1.1. Compatibilidade total com os switches gerenciáveis deste edital, e com o padrão SFP MSA, assegurado pelo fabricante do switch.

4.80.1.2. Devem possuir capacidade de detecção de ausência/presença de sinal no enlace 1000BASE-X

4.80.1.3. Módulos ópticos devem possuir conector LC para fibra óptica

4.80.1.4. Os módulos devem possuir velocidade de 1Gbps por canal unidirecional (SFP MSA), permitindo transmissão full-duplex em wire-speed (mínimo de 1Gbps úteis reais por canal unidirecional, 2Gbps úteis full-duplex, utilizando os dois canais).

4.81. FORNECIMENTO DE INTERFACES SFP TIPO III – COM INSTALAÇÃO

4.81.1. Módulos SFP+/Mini-GBIC 10G-SR LC para fibra multi-modo 850nm, para todos os switches gerenciáveis:

4.81.1.1. Compatibilidade total com os switches gerenciáveis deste edital, e com o padrão SFP+ MSA, assegurado pelo fabricante do switch.

4.81.1.2. Devem possuir capacidade de detecção de ausência/presença de sinal no enlace 10G-SR.

4.81.1.3. Módulos ópticos devem possuir conector LC para fibra óptica.

4.81.1.4. Os módulos devem possuir velocidade de 10Gbps por canal unidirecional (SFP+ MSA), permitindo transmissão full-duplex em wire-speed (mínimo de 10Gbps úteis reais por canal unidirecional, 20Gbps úteis full-duplex, utilizando os dois canais).

4.82. RÁDIO PROFISSIONAL

4.82.1. Todos os equipamentos ofertados na proposta do licitante no sistema de rádio deverão obrigatoriamente ser apresentados com a certificação da Anatel vigente. A licitante que não apresentar o certificado vigente da “Anatel” no dia da abertura da licitação será desclassificada.

4.82.2. Características de RF do rádio:

4.82.2.1. Operar nas faixas de 4.9GHz a 5.8GHz, de acordo com os requisitos da resolução da ANATEL.

4.82.2.2. Permitir operação em situações de LOS, NLOS e nLOS.

4.82.2.3. Possuir antena integrada com ganho mínimo de 23 dBi.

4.82.2.4. Utilizar modulação adaptativa e OFDM (Orthogonal Frequency Division Multiplexing).

4.82.2.5. Operar em modo MIMO, MISO e SISO.

4.82.2.6. Operar com protocolo aéreo proprietário, não sendo permitida a oferta de produtos que usem protocolo padrão Wi-Fi (IEEE 802.11a, IEEE 802.11b, IEEE 802.11g, IEEE 802.11n e 802.11ac).

4.82.2.7. Suportar as larguras de canais de 40MHz, 20MHz, 10MHz e 5MHz.

4.82.2.8. Suportar modulação BPSK, QPSK,16QAM e 64QAM.

4.82.2.9. Ter potência transmissão de, pelo menos, 24 dBm.

4.82.2.10. Ter a sensibilidade do receptor entre -69dBm e -94dBm.

4.82.2.11. Ter analisador de espectro integrado.

4.82.2.12. Possuir mecanismo/ferramenta de alinhamento de antena integrado ao equipamento, de forma a garantir o melhor apontamento de antena e consequentemente melhor performance do sistema.

4.82.3. Características de rede:

4.82.3.1. Possuir interface de rede que opere em 10/100Mbps ou mais.

4.82.3.2. Implementar priorização de tráfego baseada em IEEE 802.1p, IP ToS, DSCP, tags de VLAN, IP e MAC address.

4.82.3.3. Possuir, pelo menos, 8 filas de priorização de tráfego (QoS).

4.82.3.4. Possuir a funcionalidade de servidor DHCP, cliente DHCP e DHCP relay.

4.82.3.5. Ter a capacidade de ser configurado em modo L2 (Bridge puro) e L3 (com funções de roteamento).

4.82.3.6. Fazer NAT, suportar roteamento L3, OSPFv2, RIPv2 e capacidade de rota estática, caso o equipamento não possua esta funcionalidade, será aceito um equipamento externo para esta função, desde que o mesmo faça parte da solução.

4.82.3.7. Ter proteção automática contra loop na parte de bridge.

4.82.3.8. Suportar filtros de ARP, Proxy MAC e filtro de IP.

4.82.3.9. Possuir suporte a STP/rSTP e IGMP Snooping, caso o equipamento não possua esta funcionalidade, será aceito um equipamento externo para esta função, desde que o mesmo faça parte da solução.

4.82.3.10. Ser transparente para todo tráfego ethernet, incluindo MPLS.

4.82.3.11. Suportar VLAN Q-in-Q, caso o equipamento não possua esta funcionalidade, será aceito um equipamento externo para esta função, desde que o mesmo faça parte da solução.

4.82.4. Características de gerenciamento:

4.82.4.1. Suportar SNMPv1 e SNMPv3.

4.82.4.2. Ter opção de gerenciamento por SSH, telnet e interface web.

4.82.4.3. Permitir reset para retornar à configuração de fábrica.

4.82.5. Capacidade (throughput) do rádio:

4.82.5.1. Ter capacidade mínima de throughput de 8 Mbps, com capacidade de expansão até 180Mbps agregados sem a necessidade de troca do hardware.

4.82.5.2. Ter capacidade de processamento de pacotes por segundo (pps) de no mínimo 90.000 pps.

4.82.6. Características Elétricas do rádio:

4.82.6.1. Ter consumo máximo de até 17 W.

4.82.6.2. Ter proteção contra descargas de raios.

4.82.7. Características Ambientais:

4.82.7.1. Ser imune à chuva, neblina e poluição com nível de proteção IP67.

4.82.7.2. O componente externo do rádio deve trabalhar dentro da seguinte faixa de temperatura: -40° C a +60° C.

4.83. SERVIÇO COM FORNECIMENTO DE UPGRADE DE VELOCIDADE PARA RÁDIO PROFISSIONAL

4.83.1. Características Gerais

4.83.1.1. Fornecimento, instalação e configuração de licença de upgrade de velocidade e compatível com o rádio profissional para aumento de velocidade de conexão para 100Mbps.

4.84. SERVIÇO DE CONFIGURAÇÃO DA SOLUÇÃO DE RÁDIO

4.84.1. Características Gerais

4.84.1.1. Serviço de configuração, ajustes, fixação, alinhamento para utilização de elementos do sistema de CFTV e Controle de Acesso prevendo a customização para o local de implantação do sistema, configuração do software, configuração e ativação entre outras funções para utilização plena dos recursos contratados.

4.84.1.2. Este serviço inclui a operação assistida por 3 dias úteis juntamente com a equipe da Contratante.

4.85. PONTO DE INTERCONEXÃO COM DISPOSITIVOS MÓVEIS

4.85.1. Características Gerais

4.85.1.1. Fornecimento, instalação e configuração de dispositivo de interconexão com dispositivos móveis.

4.85.1.2. Deve possibilitar a conexão do sistema de CFTV e Controle de Acesso com o dispositivo móvel de monitoramento (DMM) especificado neste termo de referência.

4.85.1.3. Deve possuir ferramenta de gerência que permita personalização e total gerenciamento da conexão de rede.

4.85.2. Características Específicas

4.85.2.1. Access Point corporativo, com possibilidade de gerenciamento de forma standalone por interface WEB ou aplicativo, ou centralizada através de software proprietário ou software terceiro compatibilizado com o produto;

4.85.2.2. Deve possuir modo de operação Access Point, Roteador e Repetidor;

4.85.2.3. Deve suportar uma capacidade de 500 usuários conectados simultaneamente;

4.85.2.4. Deve possuir funcionalidade que possibilite a demonstração de status com informações gerais, lista de clientes, gráfico de throughput da rede e gráfico de PPS;

4.85.2.5. Deve utilizar os protocolos de proteção wireless WPA (AES/TKIP), WPA2 (AES/TKIP), WPAPSK AES/TKIP), WPA2-PSK (AES/TKIP), Captive portal embarcado ou na utilização do software de gerenciamento. Além disso, o produto deve possuir compatibilidade com Captive portal externo com Radius no modo de operação roteador;

4.85.2.6. Deve permitir funções de wireless avançada como a utilização de pelo menos 16 SSIDs (8 por frequência), WACL (controle de acesso), SSID oculto, isolação de SSID, isolação de clientes e de rede (somente internet), máximo de clientes conectados por SSID, modulação automática adaptativa, canal automático e VLAN por SSID;

4.85.2.7. Deve possuir funcionalidade que possibilite a utilização de QoS nos modos Roteador e Access Point através de WMM, limite e garantia de banda por SSID;

4.85.2.8. Deve possuir funcionalidade de Roaming;

4.85.2.9. Em modo Roteador, deve permitir conexão com rede WAN com IP estático, dinâmico e PPPoE, e é compatível com técnicas de roteamento NAT e estáticas;

4.85.2.10. Em modo Access Point, deve permitir conexão na rede LAN com IP estático, dinâmico e Fallback;

4.85.2.11. Deve permitir gerenciamento, com timeout de sessão, através de HTTP, HTTPS, SSH;

4.85.2.12. Deve possuir configuração de VLAN de gerenciamento;

4.85.2.13. Deve ser compatível com serviços de Discovery LLDP, CDP e Proprietário, servidor DHCP, SNMP, cliente NTP e log remoto (Syslog);

4.85.2.14. Em modo Roteador, deve permitir funções como ping WAN, UPnP, controle por IP, por rede e por MAC, DMZ e redirecionamento de portas;

4.85.2.15. Deve possuir ferramentas de site Survey e nível de sinal;

4.85.2.16. O equipamento deve possuir botão de reset para reiniciar o dispositivo e retornar as configurações padrão de fábrica;

4.85.2.17. O equipamento deve possuir LED, na qual demonstra o status de funcionamento do produto;

4.85.2.18. O produto deve permitir controle sobre o LED, definir se ficará ligado ou desligado, com função de agendamento. Além disso, possui função de busca pelo LED;

4.85.2.19. Deve possuir 2 portas Ethernet (10/100/1000Mbps);

4.85.2.20. O produto deve ser dualband, com tecnologia MiMo, compatível com as frequências de 2,4 GHz e 5GHz simultaneamente, com potência de transmissão de 24dBm em 2.4GHz e 24dBm em 5GHz, no padrão IEEE 802.11 a/b/g/n/ac e velocidade de 450 Mbps em 2.4GHz e 1300 Mbps em 5GHz;

4.85.2.21. O produto deve oferecer área de cobertura Wi-Fi de até 350 m²;

4.85.2.22. Na frequência 5Ghz, deve suportar os canais que exigem algoritmos de DFS (Dinamic Frequency Selection);

4.85.2.23. Sua estrutura interna deve possuir 3 antenas de 4dBi em 2.4GHz e 3 antenas de 5dBi em 5GHz

4.85.2.24. Deve possuir memória flash de 16 MB e memória RAM de 128 MB;

4.85.2.25. Deve possuir o chipset QCA 9563 + QCA 9982 + AR8337;

4.85.2.26. Sua alimentação deve ser através de POE passivo de 48V ou padrão 802.3af;

4.85.2.27. O dispositivo deve ser fornecido com fonte de alimentação (injetor PoE passivo) com entrada de 100 a 240 VAC com corrente máxima de 1 A e deve possuir saída de 48 VDC com corrente máxima de 0,5 A;

4.85.2.28. Deve possuir e ser entregue licença de software de gerenciamento do access point do mesmo fabricante do equipamento;

4.85.2.29. O equipamento já deve ser homologado e certificado com a Anatel sem nenhuma pendência. Não serão aceitos equipamentos que não estejam 100% homologados e divulgados no portal da Agência;

4.85.2.30. Deve permitir que seja instalado tanto em teto ou parede e todos os acessórios para estas instalações devem ser entregues;

4.86. SERVIÇO COM FORNECIMENTO DE LICENÇA DE GERENCIAMENTO DE PONTOS DE INTERCONEXÃO COM DISPOSITIVOS MÓVEIS

4.86.1.1. Serviço com fornecimento de licença, instalação e configuração de software para gerência de 01 ponto de interconexão com dispositivos móveis.

4.86.1.2. Deve ser homologado e totalmente compatível com o ponto de interconexão com dispositivos móveis descritos neste termo de referência.

4.86.1.3. Deve permitir a configuração de redes distribuídas em multisite com número ilimitado de locais para gerenciar de forma remota e centralizada, sem a necessidade de concentradores ou gateways físicos instalados na rede local.

4.86.1.4. Deve ser entregue licença de software que permita a realização das seguintes funcionalidades:

4.86.1.5. Totalmente homologado e compatível com o ponto de interconexão com dispositivos móveis descrito neste termo de referência, atestado por declaração do software e do fabricante do ponto de interconexão.

4.86.1.6. Deve permitir a configuração de múltiplas redes por site;

4.86.1.7. Deve permitir o posicionamento e monitoramento dos APs via mapa digital compatível com o Google Maps;

4.86.1.8. Deve permitir o monitoramento dos clientes conectados em tempo real e consumo de dados por AP, disponibilidade do AP (online/off-line), consumo de dados em tempo real;

4.86.1.9. Capacidade de Rogue APs Detection, Identificação de SSIDs vizinhos com o mesmo SSID configurado na rede;

4.86.1.10. Deve possuir pelo menos os protocolos de proteção wireless Wireless Segurança Aberta, WEP, WPA2-PSK, Captive Portal, Captive Portal Externo com Radius (AAA Radius) e Captive Portal Externo sem Radius;

4.86.1.11. Possuir configuração de wireless Avançado com configuração de até 8 redes Wi-Fi por Site e SSID Oculto e Isolação de Clientes, Limite de clientes conectados por SSID, Walled Garden, WACL, VLAN;

4.86.1.12. Deve permitir configurar Wireless QoS, controle de Banda por SSID e controle de Banda por cliente;

4.86.1.13. Em modo Access Point deve permitir a configuração de Nome (netname), configuração de TimeZone, configuração de modo IEEE, configuração de canal, configuração de potência, SSH, configuração de Nat por SSID (obrigatório para SSID com captive portal, configuração de IP (DHCP e Fixo), Syslog;

4.86.1.14. Deve permitir atualização remota de firmware, sem necessidade de baixar firmware;

4.86.1.15. Deve possuir autorollback para testar configurações antes de aplica-las de forma definitiva;

4.86.1.16. Possibilidade de retornar o equipamento para o sistema operacional original de fábrica;

4.86.1.17. Deve permitir o agendamento automático de reinicialização;

4.86.1.18. Possuir Captive Portal avançado com possibilidade de criar páginas de captive portal totalmente customizada, permitindo utilizar variados tipos de autenticação no mesmo captive portal como Login Social com as plataformas Facebook, Instagram, Google, Linkedin, Twitter, VC, Windows Live;

4.86.1.19. Possuir captive portal integrado com o Facebook para liberar acesso à internet mediante check-in e/ou like na página configurada;

4.86.1.20. Possuir captive portal mediante autenticação com métodos de e-mail, telefone, e-mail e telefone, click, código, cupom, SMS Token, formulário customizado;

4.86.1.21. Possuir captive portal mediante cupom com possibilidade de criar cupons com perfis customizados para acesso, e monitoramento em tempo real sobre a utilização dos cupons (cupons utilizados, expirados, consumo atual do cupom, tempo restante para utilização, etc)

4.86.1.22. Deve possuir ferramenta integrada a plataforma para a composição e modificação de captive portals;

4.86.1.23. Deve possuir Dashboard Social com um portal com relatórios e gráficos dos dados de clientes autenticados na rede Wi-Fi com possibilidade de filtro por período;

4.86.1.24. Deve possuir Registro de Conexões com relatório com conexões dos usuários em cada Access Points com o tipo de autenticação utilizada.

4.86.1.25. Deve permitir fazer customização de tela e divulgação de avisos ou de comunicação de marketing através da função Splash Page, para inserir anúncio e propagandas de vídeos e imagens para liberação da rede WiFi. Pode ser usada em conjunto com captive portal.

4.87. DISPOSITIVO MÓVEL DE MONITORAMENTO

4.87.1. Fornecimento, instalação e configuração de dispositivo móvel de monitoramento (DMM).

4.87.2. Deve permitir a verificação das imagens do sistema de CFTV e o acompanhamento dos dados do sistema de controle de acesso, com design robusto e apto para deslocamento pela área da contratante.

4.87.3. Deve permitir e vir licenciado para uso da câmera acoplada no DMM como câmera de monitoramento do sistema.

4.87.4. Deve possuir e vir licenciado com software de gestão para segurança, correto uso do equipamento e gestão de instalações de aplicações.

4.87.5. Deve vir equipado com alça rígida de transporte do mesmo fabricante do equipamento.

4.87.5.1. Dispositivo de monitoramento móvel, do tipo tablet corporativo e robusto, com as seguintes características mínimas:

4.87.5.2. Deve possuir processador com velocidade de clock (mínima): 2,2 GHz, 8 núcleos e 8GB de memória RAM.

4.87.5.3. Deve possuir armazenamento interno com SSD de 128 GB ou superior;

4.87.5.4. Deve possuir memória de armazenamento tipo Flash de estado sólido;

4.87.5.5. Deve possuir suporte a cartão de memória tipo micro SD, podendo suportar até 256GB, sendo acessível pela parte externa. Deve ser entregue cartão de memória de 32GB.

4.87.5.6. Deve possuir conectividade:

4.87.5.6.1. WiFi padrão IEEE 802.11 ac 2.4GHz + 5.0GHz

4.87.5.6.2. Bluetooth 4.0 (mínimo);

4.87.5.6.3. Suporte de Rede de dados 4G (quarta geração);

4.87.5.6.4. Possuir tecnologia: NFC;

4.87.5.6.5. Possuir tecnologia: GPS;

4.87.5.7. Deve operar em modo autônomo e concorrente

4.87.5.8. Deve possuir interface micro USB 3.0 Tipo B ou Tipo C;

4.87.5.9. Deve possuir slot para cartão de memória: Micro SD (SD ou SDHC ou SDXC);

4.87.5.10. Deve possuir microfone Embutido;

4.87.5.11. Deve possuir conector (saída) para fone de ouvido: Padrão P2 de 3,5mm;

4.87.5.12. Deve possuir interface de contato para carga da bateria;

4.87.5.13. Deve possuir slot Dual Nano SIM;

4.87.5.14. Deve possuir porta ethernet RJ-45.

4.87.5.15. Deve possuir tela de no mínimo 8", e (máximo) 10.1" polegadas, sem incluir bordas ou molduras, do tipo multitoque capacitiva sensível ao toque, com tecnologia LCD, com resolução mínima de 1920 x 1200 pixels;

4.87.5.16. A tela deve ser produzida em Corning Gorilla Glass 3;

4.87.5.17. Deve possuir sensor automático para toque feito por mãos, luvas e molhado;

4.87.5.18. Deve possuir película protetora contra arranhões.

4.87.5.19. Deve possuir câmera frontal de no mínimo 2MP

4.87.5.20. Deve possuir câmera traseira com no mínimo 12MP e flash;

4.87.5.21. Deve possuir bateria padrão de, no mínimo, 36Wh com carregamento rápido, composta de Lítio-ion ou polímero de lítio, de fácil acesso e substituível.

4.87.5.22. Deve ser capaz de trabalhar com bateria extendida de pelo menos 98Wh;

4.87.5.23. Deve permitir troca de bateria à quente (hot swap);

4.87.5.24. Deve possuir como opcional adaptador para carregamento veicular (do mesmo fabricante);

4.87.5.25. Deve ser entregue com duas baterias, a do aparelho e mais uma (bateria estendida).

4.87.5.26. O gabinete não poderá apresentar saliências, pontas ou estruturas externas perfurantes ou cortantes;

4.87.5.27. Deve possuir teclas para controle de volume do som;

4.87.5.28. Deve possuir no máximo peso de 1,5Kg;

4.87.5.29. Deve possuir microfone e alto-falante integrados a estrutura do dispositivo.

4.87.5.30. Deve possuir compatibilidade com o padrão MIL-STD-810G, comprovada por certificação;

4.87.5.31. Deve possuir resistência a poeira e água, com classificação IP65 ou superior.

4.87.5.32. Deve possuir sistema operacional Android;

4.87.5.33. Deve possuir idioma em português do Brasil;

4.87.5.34. Deve ser entregue com cabo de dados USB Tipo A para Micro USB 3.0 Tipo B ou Tipo C (de acordo com a entrada do dispositivo);

4.87.5.35. Deve ser entregue com carregador bivolt 110/220, do tipo carregamento rápido, com seleção automática de voltagem e plugue padrão ABNT;

4.87.5.36. Deve ser entregue com dispositivo de escrita (caneta) com tecnologia integrada ao display do tablet para uso de aplicação de escrita;

4.87.5.37. Deve ser entregue com capa protetora, específica para o tablet fornecido em relação ao tamanho (largura, espessura e comprimento), do mesmo fabricante ou homologada para o mesmo. A capa deverá manter a acessibilidade aos botões e recursos do tablet e deve possuir alça de transporte.

4.87.5.38. Deve possuir como opções de segurança leitor de smart card ou leitor biométrico integrado ao equipamento:

4.87.5.39. O tablet deve ser fornecido com dispositivo de escrita, software de utilização de escrita e integrado ao sistema operacional do tablet:

4.87.5.40. O tablet deve possuir e vir licenciado com tecnologia que permita a gestão remota através de uma solução de EMM (Enterprise Mobile Management), e que possua APIs para aplicação das seguintes políticas de TI:

4.87.5.40.1. Aplicação remota de formato e modo quiosque;

4.87.5.40.2. Localização do tablet;

4.87.5.40.3. Comando para impedir a desativação do GPS;

4.87.5.40.4. Comando remoto para apagar todos os dados do tablet;

4.87.5.40.5. Comando remoto para bloqueio do tablet;

4.87.5.40.6. Comando para bloqueio de instalação de aplicativos.

4.87.5.40.7. Comando para Habilitar/Desabilitar as seguintes funções do tablet:

4.87.5.40.8. 8 - Câmera, Modo de desenvolvimento, Debugging de USB.

4.87.5.41. A solução de EMM deve ser uma solução em nuvem e não necessitar de instalação adicional de servidores pelo órgão;

4.87.5.42. Deve possuir interface de administrador de TI com opção para português.

4.87.5.43. Deve possuir 36 meses de garantia.

4.88. PÓRTICO PARA CÂMERAS

4.88.1.1. Fornecimento de material de pórtico para pontos de captação de imagem, envolvendo transporte, montagem, instalação de pontos de captação de imagem, de equipamentos de rádio, de equipamentos de proteção elétrica, de equipamentos de alimentação e interligação lógica (switches POE), instalação de pontos de rede elétrica e lógica, ativação, configuração, limpeza e fechamento seguro do pórtico.

4.88.1.2. Este pórtico será utilizado para hospedagem de pontos de captação de imagem, com resistência física contra corrosão, condução elétrica, vandalismo físico e queima, com identidade visual da Contratante.

4.88.1.3. O produto deverá ser de linha de produção, possuir datasheet do fabricante, e já ter sido comprovadamente utilizado em outros clientes ou projetos.

4.88.1.4. Os serviços de ativação, fixação, conectorização ou qualquer outro serviço que se fizer necessário para o pleno funcionamento da solução deverá estar incluso no fornecimento desta solução pela LICITANTE.

4.88.1.5. Garantia mínima do fabricante de 25 (vinte e cinco) anos comprovada por carta de fabricante e/ou informação constante no site do fabricante.

4.88.1.6. O Pórtico deverá ser produzido em material não propagante à chama, não condutor de energia elétrica e totalmente resistente à maresia e a ações de vandalismo.

4.88.1.7. Deverá ser entregue com altura de 6 metros, a partir do nível do chão.

4.88.1.8. Deverá ser fornecido com identificação visual do Contratante, com aplicação de marca de fácil identificação e prevendo resistência a intempéries e exposição a condições climáticas adversas.

4.88.1.9. Deverá ser fornecido com condições de abrigar, com garantia de segurança e funcionalidade, em seu interior, os equipamentos que compõe a solução de conectividade de rede, incluindo switch PoE, nobreak e fonte dos rádios.

4.88.1.10. Deverá possuir capacidade de hospedar equipamento de rádio PTP, conforme especificado neste Termo de Referência, permitindo o ajuste rotacional do rádio para alinhamento com outro rádio PTP ou rádio base. O local de instalação do rádio deverá preservá-lo de pousos de pássaros no equipamento, a fim de preservar o alinhamento e não causar paradas de transmissão.

4.88.1.11. Deverá ser resistente a intempéries, garantindo a segurança dos equipamentos instalados.

4.88.1.12. Deverá possuir interface para instalação de, no mínimo, os seguintes equipamentos de monitoramento:

4.88.1.12.1. 01 (uma) câmera PTZ, conforme especificação deste Termo de Referência;

4.88.1.12.2. 02 (duas) câmeras fixas bullet, conforme especificação deste Termo de Referência.

4.88.1.13. Deverá ser entregue com quantidade suficiente de pontos de energia elétrica estabilizada para alimentar switches PoE e fonte do rádio a serem instalados na estrutura do Poste.

4.88.1.14. Deverá ser entregue com quantidade suficiente de pontos de rede com alimentação PoE para interligação e alimentação dos equipamentos instalados.

4.88.1.15. A instalação do switch POE e a chegada de rede ótica ou metálica deverá ser feita em trilho din. A terminação de ponto ótico ou metálico deve ser realizado em suporte para fixação em trilho DIN EN 50002 e para trilhos com 35mm conforme norma DIN 43880, com fixação para 1 tomada RJ45 ou 1 adaptador tipo LC Duplex ou 1 adaptador SC/RJ ou 1 adaptador E2000, com suporte para etiqueta impressa do mesmo fabricante do cabo UTP.

4.88.1.16. Deverá ser entregue com base de sustentação sólida para fixação em piso, com capacidade de suportar todo o peso de sua estrutura e dos equipamentos previstos.

5. RESPONSABILIDADE DAS PARTES

5.1. DEVERES E RESPONSABILIDADES DA CONTRATANTE

5.1.1. Acompanhar, fiscalizar e conferir o objeto contratual;

5.1.2. Proporcionar todas as facilidades para que a CONTRATADA possa efetuar os serviços dentro das normas estabelecidas no contrato;

5.1.3. Permitir livre acesso dos funcionários da CONTRATADA aos equipamentos que integram os serviços, objeto deste TERMO DE REFERÊNCIA, para execução dos serviços de instalação, manutenção e assistência técnica;

5.1.4. Receber os serviços e equipamentos que integram os serviços pela CONTRATADA, desde que estejam em conformidade com o objeto contratado;

5.1.5. Prestar informações e esclarecimentos que venham a ser solicitados pela CONTRATADA;

5.1.6. Comunicar a CONTRATADA as irregularidades observadas na execução do Contrato;

5.1.7. Não consentir que terceiro sem autorização execute os serviços de manutenção e reparo dos equipamentos que integram os serviços;

5.1.8. Fornecer instalação elétrica e física, indispensável ao assentamento dos equipamentos que integram os serviços e adequadas ao perfeito funcionamento dos mesmos;

5.1.9. Assegurar aos técnicos credenciados pela CONTRATADA o acesso aos equipamentos que integram os serviços para efetuarem as manutenções preventivas e corretivas, resguardadas todas as necessidades de sigilo e segurança, bem como dependerá de autorização da CONTRATADA toda e qualquer intervenção nos equipamentos que integram os serviços;

5.1.10. Não remover os equipamentos que integram os serviços do local instalado ou reinstalado, sem prévio e expresso consentimento da CONTRATADA;

5.1.11. Solicitar a substituição dos equipamentos defeituosos que integram os serviços;

5.1.12. Notificar à CONTRATADA sobre imperfeições, falhas ou irregularidades constatadas na prestação dos serviços, para que sejam adotadas as medidas necessárias;

5.1.13. Atestar a nota fiscal emitida pela CONTRATADO e efetivar o pagamento se a nota estiver de acordo com todas as normas legais.

5.2. DEVERES E RESPONSABILIDADES DA CONTRATADA

5.2.1. Manter durante toda a contratação as condições de habilitação, assim como os critérios que a levou a sagrar-se vencedora do certame;

5.2.2. Cumprir fielmente as obrigações assumidas no Contrato, de forma que os serviços sejam realizados com esmero e perfeição;

5.2.3. Os equipamentos que integram os serviços disponibilizados ao CONTRATANTE deverão ser novos e de primeiro uso, ser mantidos em perfeito estado de funcionamento, devendo a CONTRATADA proceder às manutenções preventivas e corretivas, sem ônus para o CONTRATANTE, observando as recomendações técnicas do fabricante, sem que isso ocasione qualquer prejuízo à execução dos serviços;

5.2.4. Assegurar a manutenção, suporte técnico e operacional necessários ao pleno e perfeito funcionamento dos equipamentos que integram os serviços, efetuando os ajustes, reparos ou a substituição parcial ou total dos equipamentos, peças e partes sem qualquer ônus para o CONTRATANTE;

5.2.5. Providenciar junto ao DER/DF a identificação dos seus empregados;

5.2.6. Assumir todos os gastos e despesas que se fizerem necessários para o cumprimento do Contrato;

5.2.7. Obter prévia autorização da CONTRATANTE antes de realizar toda e qualquer interversão no objeto contratado;

5.2.8. A CONTRATADA deverá comprovar, sempre que requerido pela Administração, por meio de cópias de notas fiscais, a procedência das peças, partes de peças e componentes, bem como de outros materiais necessários à prestação dos serviços;

5.2.9. Toda e qualquer adaptação das instalações elétricas e lógicas que se façam necessárias à execução dos serviços será de responsabilidade da Contratada e somente poderá ser efetuada na presença de servidor designado pelo DER/DF, previamente agendado e autorizado. Quando forem necessárias modificações, de qualquer natureza, deverá ser fornecido diagrama das instalações para a prévia aprovação;

5.2.10. Responder por todos os encargos trabalhistas, previdenciários, fiscais e comerciais, resultantes da execução do objeto contratado;

5.2.11. Não transferir a terceiro, por qualquer forma, nem mesmo parcialmente, o contrato, nem subcontratar qualquer das prestações a que está obrigada, sem prévio consentimento por escrito do CONTRATANTE;

5.2.12. Caso a execução dos serviços de manutenção seja efetivada pela rede de assistência técnica autorizada do fabricante dos equipamentos que integram os serviços, a Contratada deverá supervisionar os serviços prestados, permanecendo como única responsável contratual frente à CONTRATANTE, não sendo admitida, em nenhuma hipótese, a transferência da responsabilidade contratual da CONTRATADA para quaisquer terceiros;

5.2.13. Atender as solicitações para reinstalação do(s) equipamentos(s) que integram os serviços decorrente de sua transferência de local no prazo máximo de 30 (trinta) dias úteis, podendo este prazo ser prorrogado por igual período, uma única vez, desde que justificada a necessidade,

cabendo à equipe técnica da CONTRATENTE julgar o pedido. Caso haja necessidade de mudança de local de instalação dos equipamentos, esta ocorrerá por conta da Contratada, e será limitada à área geográfica do Distrito Federal.

5.2.14. A empresa contratada deverá assegurar transferência de todas as obrigações contratuais ao sucessor em caso de venda da empresa contratada ou incorporação por novos controladores.

6. MODELO DE EXECUÇÃO DO CONTRATO

A entrega de todo o serviço deverá ocorrer em até 30 (trinta) dias corridos após a emissão da ordem de serviço para início da execução do contrato, podendo este prazo ser prorrogado por igual período, uma única vez, desde que justificada a necessidade, cabendo à equipe técnica da CONTRATENTE julgar o pedido;

Os serviços deverão ser entregues de acordo com os prazos acordados, nas condições e especificações estipuladas;

A contratada deverá encaminhar relatório (minutos utilizados) mensalmente juntamente com a fatura;

A contratada deverá comunicar toda e qualquer impossibilidade de execução e/ou entrega dos serviços no prazo estipulado, com antecedência mínima de 10 (dez) dias, justificando seu motivo.

Os serviços só poderão ser executados mediante a emissão de Ordens de Serviço.

A contagem dos prazos se iniciará no dia seguinte à data da OS (Ordem de Serviços) com a definição dos serviços a serem realizados, os prazos estipulados poderão ser negociados conforme complexidade e demanda do DER.

O pagamento será efetuado no prazo de até 30 (trinta) dias corridos após a emissão da nota fiscal e atesto do executor, mediante depósito em conta bancária indicada pela empresa vencedora, de acordo com a legislação vigente.

A CONTRATADA instalará, por sua exclusiva conta e responsabilidade, equipamentos novos (de primeiro uso), em linha de produção do fabricante, em perfeitas condições de funcionamento e produtividade e que assim os manterá durante toda a vigência do contrato caso seja necessário.

6.1. PRAZO DE ENTREGA E ESPECIFICAÇÕES DOS SERVIÇOS DE INSTALAÇÃO DO SISTEMA ELETRONICO

6.1.1. A CONTRATADA deverá instalar o sistema eletrônico, em horário a ser acordado com a CONTRATANTE, de acordo com as quantidades previstas neste Termo de Referência.

6.1.2. A CONTRATADA deverá instalar o sistema eletrônico no prazo máximo de 30 (trinta) dias corridos após emissão da ordem de serviço expedida pela CONTATANTE, podendo este prazo ser

prorrogado por igual período, uma única vez, desde que justificada a necessidade, cabendo à equipe técnica da CONTRATENTE julgar o pedido;

6.2. CRONOGRAMA DE EXECUÇÃO

A CONTRATADA deverá obedecer ao seguinte cronograma de atividades:

CRONOGRAMA DE ATIVIDADES			
ITEM	Ação	Responsável	Prazo Máximo
1	Convocar a CONTRATADA para reunião de alinhamento	DER-DF	D+2 dias
2	Reunião de alinhamento para definição dos prazos e assinaturas de documentos	DER-DF e CONTRATADA	D+4 dias
3	Encaminhamento do cronograma detalhado dos serviços a serem realizados na fase de implantação	CONTRATADA	D+6 dias
4	Aprovação do cronograma	DER-DF	D+8 dias
5	Execução do cronograma aprovado	CONTRATADA	D+10 dias
6	Aceite definitivo da Fase de Implantação	DER-DF	D+30 dias

Onde “D” é a data de publicação do extrato do contrato no Diário Oficial do Distrito Federal.

7. MODELO DE GESTÃO DO CONTRATO

As requisições decorrentes da presente licitação serão formalizadas, de acordo com a necessidade do DER-DF, por termo de contrato, a ser celebrado pelo DER-DF, que será denominada de CONTRATANTE, e a licitante vencedora, que será denominada de CONTRATADA, as quais observarão todas as normas legais e regulamentares, além das previstas neste TERMO DE REFERÊNCIA e seus Anexos.

Será nomeado executor e suplente pelo DER-DF para acompanhamento e gestão do contrato.

A execução somente será iniciada depois de aprovada a instalação da solução de TI. Para tanto, a contratada terá o prazo de até 30 dias, após a publicação do extrato do contrato no D.O.D.F., para implantar a infraestrutura necessária, assim como para efetuar os serviços correlatos de acordo com a demanda, podendo este prazo ser prorrogado por igual período, uma única vez, desde que justificada a necessidade, cabendo à equipe técnica da CONTRATENTE julgar o pedido.

A entrega dos serviços deverá ocorrer após a emissão da ordem de serviço para início da execução do contrato, conforme cronograma de execução.

7.1. DO PAGAMENTO

7.1.1. O pagamento será efetuado mensalmente, mediante a apresentação pela CONTRATADA da Nota Fiscal, detalhamento da minutagem consumida e documentos fiscais/certidões, por meio de ordem bancária, em moeda corrente, creditada na conta corrente da CONTRATADA, contados da data de aceitação dos serviços, pelo Setor Competente do CONTRATANTE.

7.1.2. O primeiro faturamento, para fins de ajuste, deverá ocorrer aos dias correspondentes ao mês de entrega dos serviços contratos, e os seguintes deverão ser faturados considerando o mês integral.

7.1.3. Caso haja incorreção no faturamento, os documentos de cobrança serão devolvidos para regularização, não cabendo atualização financeira sob hipótese alguma;

7.1.4. A Fatura deverá ser emitida pela própria CONTRATADA, obrigatoriamente, com o número de inscrição do CNPJ apresentado nos documentos de habilitação e da proposta e no Contrato, sendo também admitindo Faturas emitidas em CNPJs filiais da matriz;

7.1.5. Serão retidos na fonte os tributos e contribuições sobre os pagamentos efetuados, utilizando-se as alíquotas previstas para o objeto do contrato;

7.1.6. Ocorrendo atraso no pagamento, desde que a CONTRATADA não tenha concorrido de alguma forma para o atraso, o valor devido deverá ser atualizado financeiramente desde a data final do período de adimplemento de cada parcela, até a data do efetivo pagamento. A atualização será feita tendo como base a avaliação do IPCA, ou outro indicador que venha substituí-lo, proporcionalmente aos dias de atraso.

7.2. DA FISCALIZAÇÃO

7.2.1. A fiscalização da prestação dos serviços será exercida por representante do CONTRATANTE, neste ato denominado Executor, devidamente credenciado, ao qual competirá dirimir as dúvidas que surgirem no curso da execução, dando ciência de tudo à CONTRATADA, Art. 67 da Lei n.º 8.666/93, com suas alterações.

7.2.1. A fiscalização que trata esta Cláusula não exclui nem reduz a responsabilidade da CONTRATADA, até mesmo perante terceiro, por qualquer irregularidade, inclusive resultante de imperfeições técnicas, emprego de material inadequado ou de qualidade inferior e, na ocorrência desta, não implica corresponsabilidade do CONTRATANTE ou de seus agentes e prepostos, Art. 70 da Lei n.º 8.666/93, com suas alterações.

8. ESTIMATIVA DE CUSTOS

O valor estimado para o período de 12 (doze) meses da contratação será de R$ 7.445.534,41 (sete milhões, quatrocentos e quarenta e cinco mil, quinhentos e trinta e quatro reais e quarenta e um centavos).

8.1. METODOLOGIA PARA OBTENÇÃO DE VALORES ESTIMADOS

A metodologia aplicada para obtenção das estimativas de preços consiste em enviar, ou e-mail, às empresas especializadas disponíveis no mercado de livre comércio brasileiro, documento oficial onde consta a descrição sumária e o quantitativo dos itens a serem adquiridos, ressaltando a idoneidade da aceitação por meio de papel timbrado pelas empresas, onde constam: Razão Social, CNPJ, telefones e endereços.

Procedimento de pesquisa de preço é realizado em obediência às decisões nº 5465, de 20 de outubro de 2005; nº 6183, de 22 de setembro de 2009, do TCDF – Tribunal de Contas do Distrito Federal; e decreto nº 36.220, art. 3º, de 30 de Dezembro de 2014.

Empresas	Valor Global(R$)
NMeios	7.445.534,41
Quality	8.198.692,10
GETTEC	7.197.329,14
Preço Médio	7.613.851,88
Preço Mediano	7.445.534,41

Tendo em vista as peculiaridades do DER-DF, composto por 5 Distritos Rodoviários e a Sede, em diferentes localidades e diferentes estruturas prediais, não foi possível encontrar preço público, com as características e singularidades do DER-DF.

Fez se o levantamento em cada Distrito Rodoviário e Sede, conforme planilha em anexo, das necessidades dos quantitativos das câmaras e localidade, e as empresas realizaram visitas aos locais e fizeram seus respectivos orçamentos.

9. ADEQUAÇÃO ORÇAMENTÁRIA E CRONOGRAMA FÍSICO-FINANCEIRO

A despesa com a contratação objeto deste Estudo Técnico Preliminar terá suporte orçamentário em Natureza de Despesa 3.3.90.39 - Outros Serviços de Terceiros, serão utilizadas as fontes dos recursos de Multas (237), Tesouro (100) e/ou Faixa de Domínio (220).

10. CRITÉRIOS PARA SELEÇÃO DO FORNECEDOR

10.1. PROPOSTA DE PREÇOS

A proposta da licitante deverá conter:

10.1.1. Preço, contemplando os valores unitário e total, em moeda nacional, em algarismo por extenso (havendo discordância entre os preços unitário e total, prevalecerá o primeiro, e entre os valores expressos em algarismos e por extenso, serão considerados estes últimos, devendo o

Pregoeiro proceder às correções necessárias), já considerando todas as despesas com tributos, fretes e demais despesas que incidam direta ou indiretamente sobre os serviços, mesmo que não estejam registrados nestes documentos;

10.1.2. Prazo de validade, não inferior a 60 (sessenta) dias corridos, a contar da data de sua apresentação. Na ausência de indicação expressa do prazo de validade, considerar-se-á tacitamente indicado o prazo de 60 dias;

10.1.3. As propostas deverão apresentar preços compatíveis com os preços correntes de mercado, conforme estabelece o art. 43, inciso IV da Lei 8.666/93 e alterações posteriores;

10.1.4. Todas as declarações e documentações emitidas pela empresa licitante, incluindo sua proposta de preços, deverão ser assinadas por seu representante legal, sob pena de desclassificação/inabilitação.

10.2. CRITÉRIO DE JULGAMENTO

10.2.1. A particularidade relacionada à presente contratação é a necessidade de se adotar o critério de julgamento, tomando-se por base o MENOR PREÇO GLOBAL, diante da impossibilidade de parcelamento do objeto, senão vejamos:

10.2.2. A contratação global permitirá a apresentação de melhores condições financeiras na ocasião da licitação, principalmente se considerada os percentuais de descontos que as licitantes poderão obter dos fabricantes de equipamentos, decorrentes da compra de maior volume e diversidade de equipamentos (economia de escala).

10.2.3. Além disso, o fracionamento da contratação em itens distintos poderá resultar no fracasso da presente contratação, especialmente devido aos seguintes motivos:

10.2.3.1. Risco do menor preço para soluções que integram os serviços a serem apresentados por licitante diverso.

10.2.3.2. Possibilidade de contratação de valores distintos para o mesmo tipo de serviço;

10.2.3.3. Dificuldade da administração dos contratos, em virtude do aumento da variedade dos softwares de gerenciamento dos serviços de comunicação;

10.2.3.4. Aumento dos custos operacionais administrativos relacionados à gestão de maior quantidade de empresas contratadas, para a execução do mesmo objeto, em uma mesma localidade, ferindo o Princípio da Padronização;

10.2.3.5. Acréscimo dos encargos do CONTRATANTE, no que se refere à disponibilização de maior quantidade de espaço físico, os quais serão destinados à manutenção das estruturas de suporte técnico das futuras contratadas.

10.3. DA DOCUMENTAÇÃO

10.3.1. Diante da alta complexidade do objeto a ser contratado, o qual é imprescindível para a Autarquia possibilitar sua comunicação com o público interno e externo, atendendo às necessidades do exercício da sua missão institucional, é indispensável exigir, como critério de HABILITAÇÃO, a apresentação das seguintes documentações, além das exigências administrativas e legais especificadas no Edital, sob pena de inabilitação:

10.3.2. O Termo de Vistoria ou Termo de não Vistoria, assinado pela licitante, declarando ter conhecimento dos locais de realização dos serviços, instalações de infraestrutura e condições ambientais;

10.3.3. Declaração da LICITANTE de que instalará, por sua exclusiva conta e responsabilidade, equipamentos novos (de primeiro uso), em linha de produção do fabricante, em perfeitas condições de funcionamento e produtividade e que assim os manterá durante toda a vigência do contrato;

10.3.4. A validade da documentação apresentada é de responsabilidade da empresa, podendo o DER-DF promover as diligências que entender necessárias junto à entidade profissional competente.

10.3.5. Todas as declarações e documentações emitidas pela empresa licitante, incluindo sua proposta de preços, deverão ser assinadas pelo seu representante legal, sob pena de desclassificação/inabilitação.

10.3.6. Equívocos, omissões e/ou inexatidões, bem como a falta de competência para assinar os documentos acima referidos poderão resultar em aplicação de sanções e penalidades à empresa, de acordo com o previsto neste instrumento, bem como nas legislações que regulam o exercício ilegal de profissão e ainda no Código Penal Brasileiro.

10.3.7. O DER/DF quer assegurar qualidade por meio de uma descrição detalhada do objeto, bem como pela exigência de certos requisitos de qualificação técnica, como condição de habilitação dos licitantes. Em se tratando de licitações do tipo menor preço, é comum que se sagrem vencedores os participantes que formalmente preenchem todos os requisitos de habilitação técnica, e/ou não conseguem executar o contrato de modo eficiente, o que provoca graves prejuízos à administração.

11. VISTORIA

11.1. Quando da vistoria ao local, a CONTRATADA deverá inteirar-se de todos os aspectos referentes à execução dos serviços.

11.2. As LICITANTES poderão realizar vistoria técnica nas instalações do DER/DF de segunda-feira à sexta-feira, das 8:00h às 17:00h:

11.3. A vistoria técnica deverá ser realizada em até, no máximo, 24 (vinte e quatro) horas da abertura do processo licitatório.

11.4. Quanto a vistoria ao local do serviço, as licitantes devem se inteirar de todos os aspectos referentes à execução do fornecimento do serviço;

11.5. Para a realização de vistoria, será exigido da licitante assinatura de Termo de confidencialidade, Anexo IV, no qual a licitante se compromete a não divulgar as informações confidenciais sobre a infraestrutura do DER/DF;

11.6. Para todos os efeitos, considerar-se-á que a Licitante tem pleno conhecimento da natureza e do escopo dos serviços, não se admitindo, posteriormente, qualquer alegação de desconhecimento dos mesmos;

11.7. Efetuada a vistoria será lavrada, por representante da empresa, termo de vistoria, conforme Anexo II.

11.8. A Não-Vistoria conforme Anexo III, o qual deverá ser preenchido e assinado pelo interessado em participar da licitação, anexando-o, oportunamente, à sua proposta e habilitação técnica, caso a contratada não tenha realizado a vistoria.

11.9. É responsabilidade da empresa pelo dimensionamento de sua proposta, de modo a não incorrer em omissões, as quais não poderão ser alegadas em favor de eventuais alterações no valor do objeto licitado/contratado.

12. PRAZO DE EXECUÇÃO

12.1. A vigência do Contrato será de 12 (doze) meses, contados a partir da data de sua assinatura, podendo, no interesse do DER-DF, ser prorrogado conforme inciso II e § 4º do Artigo 57 da Lei nº 8.666/93.

12.2. O contrato durante sua execução poderá ser reajustado de acordo com o Índice Nacional de Preços ao Consumidor Amplo – IPCA, conforme Decreto nº 36.246, DE 02 DE JANEIRO DE 2015, após a execução dos primeiros 12 meses.

13. SANÇÕES

13.1. ESPÉCIES

13.1.1. As licitantes e/ou contratadas que não cumprirem integralmente as obrigações assumidas, garantida a prévia defesa, estão sujeitas às seguintes sanções em conformidade com o Decreto nº 26.851, de 30/05/2006, publicado no DODF nº 103, de 31/05/2006, pg. 05/07, alterado pelos Decretos nºs 26.993/2006, de 12/07/2006 e 27.069/2006, de 14/08/2006 e 36.974/2015:

13.1.2. I - Advertência;

13.1.3. II - Multa; e

13.1.4. III - Suspensão temporária de participação em licitação, e impedimento de contratar com a Administração do Distrito Federal, por prazo não superior a 2 (dois) anos, e dosada segundo a natureza e a gravidade da falta cometida.

13.1.5. para a licitante e/ou contratada que, convocada dentro do prazo de validade de sua proposta, não celebrar o contrato, deixar de entregar ou apresentar documentação falsa exigida para o certame, ensejar o retardamento da execução do seu objeto, comportar-se de modo inidôneo ou cometer fraude fiscal; a penalidade será aplicada por prazo não superior a 5 (cinco) anos, e a licitante e/ou contratada será descredenciada do Sistema de Cadastro de Fornecedores, sem prejuízo das multas previstas em edital e no contrato e das demais cominações legais, aplicadas e dosadas segundo a natureza e a gravidade da falta cometida;

13.1.6. IV - Declaração de inidoneidade para licitar ou contratar com a Administração Pública enquanto perdurarem os motivos determinantes da punição ou até que seja promovida a reabilitação perante a própria autoridade que aplicou a penalidade, que será concedida sempre que a contratada ressarcir a Administração pelos prejuízos resultantes e após decorrido o prazo da sanção aplicada com base no inciso anterior.

13.1.7. As sanções previstas nos incisos I, III e IV do subitem anterior poderão ser aplicadas juntamente com a do inciso II, facultada a defesa prévia do interessado, no respectivo processo, no prazo de 5 (cinco) dias úteis.

13.2. ADVERTÊNCIA

13.2.1. A advertência é o aviso por escrito, emitido quando a licitante e/ou contratada descumprir qualquer obrigação, seja quando o descumprimento da obrigação ocorrer durante o procedimento licitatório ou na fase de execução contratual, entendida desde a recusa em retirar a nota de empenho ou assinar o contrato.

13.3. MULTA

13.3.1. A multa é a sanção pecuniária que será imposta à contratada pelo ordenador de despesas do DER-DF, por atraso injustificado na entrega ou execução do contrato, e será aplicada nos seguintes percentuais:

I - 0,33% (trinta e três centésimos por cento) por dia de atraso, na entrega de material ou execução de serviços, calculado sobre o valor correspondente à parte inadimplente, até o limite de 9,9%, que corresponde a até 30 (trinta) dias de atraso;

II - 0,66 % (sessenta e seis centésimos por cento) por dia de atraso, na entrega de material ou execução de serviços, calculado, desde o primeiro dia de atraso, sobre o valor correspondente à

parte inadimplente, em caráter excepcional, e a critério do órgão contratante, quando o atraso ultrapassar 30 (trinta) dias;

III - 5% (cinco por cento) sobre o valor total do contrato/nota de empenho, por descumprimento do prazo de entrega, sem prejuízo da aplicação do disposto nos incisos I e II deste subitem;

IV - 15% (quinze por cento) em caso de recusa injustificada do adjudicatário em assinar o contrato ou retirar o instrumento equivalente, dentro do prazo estabelecido pela Administração, recusa parcial ou total na entrega do material, recusa na conclusão do serviço, ou rescisão do contrato/ nota de empenho, calculado sobre a parte inadimplente; e

V - 20% (vinte por cento) sobre o valor do contrato/nota de empenho, pelo descumprimento de qualquer cláusula do contrato, exceto prazo de entrega.

A multa será formalizada por simples apostilamento contratual, na forma do art. 65, § 8º, da Lei nº 8.666/93 e será executada após regular processo administrativo, oferecido à contratada a oportunidade de defesa prévia, no prazo de 05 (cinco) dias úteis, a contar do recebimento da notificação, nos termos do § 3o do art. 86 da Lei nº 8.666/93, observada a seguinte ordem:

I - mediante desconto no valor da garantia depositada do respectivo contrato;

II - mediante desconto no valor das parcelas devidas à contratada; e

III - mediante procedimento administrativo ou judicial de execução.

13.3.2. Se a multa aplicada for superior ao valor da garantia prestada, além da perda desta, responderá à contratada pela sua diferença, devidamente atualizada pelo Índice Geral de Preços - Mercado (IGP-M) ou equivalente, que será descontada dos pagamentos eventualmente devidos pela Administração ou cobrados judicialmente.

13.3.3. O atraso, para efeito de cálculo de multa, será contado em dias corridos, a partir do dia seguinte ao do vencimento do prazo de entrega ou execução do contrato, se dia de expediente normal na repartição interessada, ou no primeiro dia útil seguinte.

Em despacho, com fundamentação sumária, poderá ser relevado:

I - o atraso não superior a 05 (cinco) dias; e

II - a execução de multa cujo montante seja inferior ao dos respectivos custos de cobrança.

13.3.4. A multa poderá ser aplicada cumulativamente com outras sanções, segundo a natureza e a gravidade da falta cometida, observado o princípio da proporcionalidade.

13.3.5. Decorridos 30 (trinta) dias de atraso, a nota de empenho e/ou contrato deverão ser cancelados e/ou rescindidos, exceto se houver justificado interesse da unidade contratante em admitir atraso superior a 30 (trinta) dias, que será penalizado na forma do inciso II do subitem 11.3.1.

A sanção pecuniária prevista no inciso IV do subitem 11.3.1 não se aplica nas hipóteses de rescisão contratual que não ensejam penalidades.

13.4. SUSPENSÃO

13.4.1. A suspensão é a sanção que impede temporariamente o fornecedor de participar de licitação e de contratar com a Administração, e, se aplicada em decorrência de licitação na modalidade pregão, ainda suspende o registro cadastral da licitante e/ou contratada no Cadastro de Fornecedores do Distrito Federal, instituído pelo Decreto nº 25.966, de 23 de junho de 2005, e no Sistema de Cadastramento Unificado de Fornecedores – SICAF, de acordo com os prazos a seguir:

I - por até 30 (trinta) dias, quando, vencido o prazo de advertência, emitida pelo DER-DF, a licitante e/ou contratada permanecer inadimplente;

II - por até 90 (noventa) dias, quando a licitante deixar de entregar, no prazo estabelecido no edital, os documentos e anexos exigidos, quer por via fax ou internet, de forma provisória, ou, em original ou cópia autenticada, de forma definitiva;

III - por até 12 (doze) meses, quando a licitante, na modalidade pregão, convocada dentro do prazo de validade de sua proposta, não celebrar o contrato, ensejar o retardamento na execução do seu objeto, falhar ou fraudar na execução do contrato; e

IV - por até 24 (vinte e quatro) meses, quando a licitante:

apresentar documentos fraudulentos, adulterados ou falsificados nas licitações, objetivando obter, para si ou para outrem, vantagem decorrente da adjudicação do objeto da licitação;

tenha praticado atos ilícitos visando a frustrar os objetivos da licitação;

receber qualquer das multas previstas no subitem anterior e não efetuar o pagamento;

13.4.2. A penalidade de suspensão será aplicada pelo Diretor Geral do DER-DF e será publicada no Diário Oficial do Distrito Federal.

13.4.3. O prazo previsto no inciso IV poderá ser aumentado para até 05 (cinco) anos, quando as condutas ali previstas forem praticadas no âmbito dos procedimentos derivados dos pregões.

13.5. DECLARAÇÃO DE INIDONEIDADE

13.5.1. A declaração de inidoneidade será aplicada pelo DER-DF, à vista dos motivos informados na instrução processual.

13.5.2. A declaração de inidoneidade prevista neste item 11.5 permanecerá em vigor enquanto perdurarem os motivos que determinaram a punição ou até que seja promovida a reabilitação perante a própria autoridade que a aplicou, e será concedida sempre que a contratada ressarcir a Administração pelos prejuízos resultantes de sua conduta e após decorrido o prazo da sanção.

13.5.3. A declaração de inidoneidade e/ou sua extinção será publicada no Diário Oficial do Distrito Federal, e seus efeitos serão extensivos a todos os órgãos/entidades subordinados ou vinculados ao

Poder Executivo do Distrito Federal, e à Administração Pública, consoante disposto no art. 87, IV da Lei nº 8.666/1993.

13.6. ASSENTAMENTO EM REGISTROS

13.6.1. Toda sanção aplicada será anotada no histórico cadastral da empresa.

13.6.2. As penalidades terão seus registros cancelados após o decurso do prazo do ato que as aplicou.

13.7. SUJEIÇÃO A PERDAS E DANOS

13.7.1. Independentemente das sanções legais cabíveis, regulamentadas pelo Decreto nº 26.851/06 e suas alterações, previstas neste edital, a licitante e/ou contratada ficará sujeita, ainda, à composição das perdas e danos causados à Administração pelo descumprimento das obrigações licitatórias e/ou contratuais, conforme:

13.7.1.1. Art. 70. O contratado é responsável pelos danos causados diretamente à Administração ou a terceiros, decorrentes de sua culpa ou dolo na execução do contrato, não excluindo ou reduzindo essa responsabilidade a fiscalização ou o acompanhamento pelo órgão interessado. (Artigo 70, Lei 8.666/1993).

13.8. DA FUNDAMENTAÇÃO LEGAL

13.8.1. Em relação à legalidade, o presente certame deverá submeter-se aos ditames da Lei nº 8.666/93, Lei nº 10.520/2010, Decreto nº 3.555/2000, Resoluções nºs 218/73 e 1.025/2009 do Conselho Federal de Engenharia e Agronomia, Lei nº 12.305/2010, Decreto nº 7.404/2010, Lei Distrital nº 5.610/2016, Decreto Distrital nº 37.568/2016 e suas atualizações, bem como demais disposições legais correlatas, assim como a Portaria 20/2016 do Ministério do Planejamento, Orçamento e Gestão –MPOG, devidamente adequada ao caso específico do DER-DF.

13.8.2. O Art. 6º, inc. VIII, alíneas “a” a “e”, da Lei 8.666/93, estabelece que o Regime de Execução Indireta é uma das exigências legais para a celebração dos contratos administrativos. O Regime de Execução Indireta consiste na forma pela qual a Administração Pública contrata com terceiros a realização de uma obra, serviço ou fornecimento.

PLANILHA

Item	Descrição	Unidade	1º Distrito	2º Distrito	3º Distrito	4º Distrito	5º Distrito	Sede	QTD
1	SERVIÇO COM FORNECIMENTO DE	PEÇA	11	9	11	11	11	1	54

	MATERIAL DE INSTALAÇÃO DE NOBREAK TIPO I								
2	SERVIÇO COM FORNECIMENTO DE MATERIAL DE INSTALAÇÃO DE NOBREAK TIPO II	PEÇA	1	1	1	1	1	1	6
3	SERVIÇO DE REMANEJAMENTO OU RETIRADA DE PONTO ELÉTRICO	PONTO	5	5	5	5	5	5	30
4	SERVIÇO COM FORNECIMENTO DE MATERIAL DE INSTALAÇÃO DE PONTOS DE ENERGIA ELÉTRICA	PONTO	5	5	5	5	5	5	30
5	SERVIÇO COM FORNECIMENTO DE MATERIAL DE INSTALAÇÃO DE QUADRO DE DISTRIBUIÇÃO ELÉTRICO	UNIDADE	1	1	1	1	1	1	6
6	SERVIÇO COM FORNECIMENTO DE MATERIAL DE INSTALAÇÃO DE ATERRAMENTO BÁSICO PARA PROTEÇÃO DE QUADROS ELÉTRICOS,	UNIDADE	1	1	1	1	1	1	6

	ELETROCALHAS E RACK'S								
7	SERVIÇO DE LANÇAMENTO DE FIBRA OPTICA EM POSTE OU SUBTERRANEO	METROS	150	150	1000	300	600	0	2200
8	SERVIÇO COM FORNECIMENTO DE MATERIAL DE INSTALAÇÃO DE PIGTAIL ÓPTICO MONOFIBRA MM OM2 MONTADO	UNIDADE	32	32	32	32	44		172
9	SERVIÇO DE EMENDA E FUSÃO DE FIBRA ÓTICA	UNIDADE	32	32	32	32	44		172
10	SERVIÇO DE CERTIFICAÇÃO DE FIBRA ÓPTICA	UNIDADE	32	32	32	32	44		172
11	SERVIÇO COM FORNECIMENTO DE MATERIAL DE INSTALAÇÃO DE DISTRIBUIDOR INTERNO ÓTICO “DIO” PARA ATÉ 48 FIBRAS	PEÇA	3	6	3	3	3	1	19
12	SERVIÇO COM FORNECIMENTO DE RACK PADRÃO 19” TIPO I	PEÇA	10	8	10	10	9	1	48
13	SERVIÇO COM FORNECIMENTO DE	PEÇA	1	1	1	1	1	0	5

	RACK PADRÃO 19” TIPO II								
14	SERVIÇO COM FORNECIMENTO DE RACK PADRÃO 19” TIPO III	PEÇA						1	1
15	SERVIÇO COM FORNECIMENTO DE MATERIAL DE PONTO DE REDE CAT 6	PONTO	47	90	52	11			200
16	SERVIÇO COM FORNECIMENTO DE MATERIAL DE PONTO DE REDE CAT 6 C/ CP	PONTO	3	3	3	25	45	21	100
17	SERVIÇO COM FORNECIMENTO DE MATERIAL DE INSTALAÇÃO DE PATCH CORD UTP CAT 6 DE 1,5 A 2,5 MT	PEÇA	100	186	110	72	90	42	600
18	SERVIÇO DE REMANEJAMENTO OU RETIRADA DE PONTO DE REDE DE DADOS	PEÇA	10	10	10	10	10		50
19	SERVIÇO DE ABERTURA E FECHAMENTO DE VALA ATRAVÉS DE MÉTODO DESTRUTIVO (MD)	METRO	300	300	1000	300	300		2200

	EM SOLO BRUTO								
20	SERVIÇO DE RECONSTRUÇÃO DE ASFALTO	METRO		30					30
21	SERVIÇO DE ABERTURA E FECHAMENTO DE RASGO EM ALVENARIA	METRO	100	100	110	80	110		500
22	SERVIÇO DE EXECUÇÃO E/OU RECOMPOSIÇÃO DE FORRO E/ OU DIVISÓRIA DE GESSO ACARTONADO MONOLÍTICO	M²	20	20	20	20	20		100
23	SERVIÇO DE PINTURA E/OU REPINTURA DE PAREDE OU FORRO DE GESSO EM MASSA PVA E COR BRANCA	M²	20	20	20	20	20		100
24	SERVIÇO DE REMOÇÃO E/OU RETIRADA DE CANALETAS	SERV	20	20	20	20	20		100
25	SERVIÇO COM FORNECIMENTO DE MATERIAL DE INFRAESTRUTURA TIPO I	METRO	50	100	50	50	50	60	360
26	SERVIÇO COM	METRO	10	20	10	10	10	10	70

	FORNECIMENTO DE MATERIAL DE INFRAESTRUTURA TIPO II								
27	SERVIÇO COM FORNECIMENTO DE MATERIAL DE INFRAESTRUTURA TIPO III	METRO	600	1000	600	500	800	500	4000
28	SERVIÇO COM FORNECIMENTO DE MATERIAL DE INFRAESTRUTURA TIPO IV	METRO	30	50	30	30	30	30	200
29	SERVIÇO COM FORNECIMENTO DE MATERIAL DE INFRAESTRUTURA TIPO V	METRO	60	60	80	40	40	41	321
30	SERVIÇO COM FORNECIMENTO DE MATERIAL DE INFRAESTRUTURA TIPO VI	METRO	5	5	5	5	5	5	30
31	SERVIÇO COM FORNECIMENTO DE MATERIAL DE INFRAESTRUTURA TIPO VII	METRO	12	14	6	6	6	6	50
32	SERVIÇO COM FORNECIMENTO DE MATERIAL DE INFRAESTRUTURA TIPO VIII	PEÇA	37	60	60	60	30	30	277

33	SERVIÇO COM FORNECIMENTO DE MATERIAL DE INFRAESTRUTURA TIPO IX	METRO	100	200	200	100	100	100	800
34	SERVIÇO COM FORNECIMENTO DE MATERIAL DE INFRAESTRUTURA TIPO X	PEÇA	1	1	1	1	1	1	6
35	SERVIÇO COM FORNECIMENTO DE MATERIAL DE INFRAESTRUTURA TIPO XI	M²	39	60	80	40	40	41	300
36	SERVIÇO COM FORNECIMENTO DE MATERIAL DE INFRAESTRUTURA TIPO XII	PEÇA	5	5	5	5	5	5	30
37	FORNECIMENTO, INSTALAÇÃO E MANUTENÇÃO POR 36 MESES DE SIAED – SISTEMA DE INFRAESTRUTURA DE ALTA EFICIÊNCIA E DISPONIBILIDADE	UND		1					1
38	FORNECIMENTO DE PONTO MONITORADO INTELIGENTE TIPO I	UNIDADE	19	56	28	13	8	9	133
39	FORNECIMENTO DE	UNIDADE	2	2	2	2	2		10

	PONTO MONITORADO INTELIGENTE TIPO II								
40	FORNECIMENTO DE PONTO MONITORADO INTELIGENTE TIPO III	UNIDADE	4	4	4	4	4		20
41	FORNECIMENTO DE PONTO MONITORADO INTELIGENTE TIPO IV	UNIDADE	19	19	14	9	7	12	80
42	FORNECIMENTO DE PONTO MONITORADO INTELIGENTE TIPO V	UNIDADE	1	1	1	1	1	1	6
43	FORNECIMENTO DE PONTO MONITORADO INTELIGENTE TIPO VI	UNIDADE	1	1	1	1	1	1	6
44	FORNECIMENTO DE PONTO MONITORADO INTELIGENTE TIPO VII	UNIDADE	2	2	2			2	8
45	FORNECIMENTO DE PONTO MONITORADO INTELIGENTE TIPO VIII	UNIDADE	3				2	2	7

46	FORNECIMENTO DE PONTO MONITORADO INTELIGENTE TIPO IX	UNIDADE		1	4	2			7
47	FORNECIMENTO DE PONTO MONITORADO INTELIGENTE TIPO X	UNIDADE		7					7
48	FORNECIMENTO DE UNIDADE DE PROCESSAMENTO E GRAVAÇÃO TIPO I	UNIDADE					2		2
49	FORNECIMENTO DE UNIDADE DE PROCESSAMENTO E GRAVAÇÃO TIPO II	UNIDADE	2		2	1			5
50	FORNECIMENTO DE UNIDADE DE PROCESSAMENTO E GRAVAÇÃO TIPO III	UNIDADE		1					1
51	FORNECIMENTO DE GRAVADOR DE IMAGENS NVR	UNIDADE						1	1
52	FORNECIMENTO DE PLATAFORMA DE GERENCIAMENTO UNIFICADO	UNIDADE						1	1
53	FORNECIMENTO DE ESTAÇÃO DE MONITORAMENTO	UNIDADE	1	1	1	1	1	1	6
54	FORNECIMENTO DE	UNIDADE						1	1

	DISPOSITIVO DE CONTROLE TIPO I								
55	FORNECIMENTO DE DISPOSITIVO DE CONTROLE TIPO II	UNIDADE	1	1	1	1	1		5
56	SERVIÇO DE MANUTENÇÃO DE CFTV	UNIDADE	2	2	2	2	2	2	12
57	CURSO DE TREINAMENTO E TRANSFERÊNCIA DE CONHECIMENTO EM CFTV	UNIDADE	1	1	1	1	1	1	6
58	SERVIÇO DE RETIRADA DE PONTO CFTV	UNIDADE	4	4	4	4			16
59	FORNECIMENTO DE MONITOR DE IMAGEM PROFISSIONAL 24/7 48 POLEGADAS COM INSTALAÇÃO	UNIDADE	2	2	2	2	2	2	12
60	FORNECIMENTO DE CONTROLADORA INTELIGENTE DE ACESSO TIPO I	UNIDADE		1					1
61	FORNECIMENTO DE CONTROLADORA INTELIGENTE DE ACESSO TIPO II	UNIDADE			1				1
62	FORNECIMENTO DE ACESSO TIPO I	UNIDADE	1	1	1	1	1		5
63	FORNECIMENTO DE	UNIDADE		1					1

	ACESSO TIPO II								
64	FORNECIMENTO DE ACESSO TIPO III	UNIDADE	1	1	1	1	1		5
65	FORNECIMENTO DE ACESSO TIPO IV	UNIDADE	1	1	1			1	4
66	FORNECIMENTO DE CREDENCIAL TIPO I	UNIDADE	25	25	25			25	100
67	FORNECIMENTO DE CREDENCIAL TIPO II	UNIDADE	25	25	25			25	100
68	FORNECIMENTO DE CREDENCIAL TIPO III	UNIDADE	25	25	25			25	100
69	FORNECIMENTO DE SISTEMA DE GESTÃO DE SEGURANÇA	UNIDADE						1	1
70	FORNECIMENTO DE ESTAÇÃO DE CADASTRO DE FUNCIONÁRIO	UNIDADE	1	1	1			1	4
71	FORNECIMENTO DE SISTEMA DE GESTÃO DE VISITANTES	UNIDADE						1	1
72	FORNECIMENTO LICENÇA ADICIONAL 64 LEITORES	UNIDADE						1	1
73	FORNECIMENTO DE ESTAÇÃO DE CADASTRO DE VISITANTES	UNIDADE	1	1	1	1	1	1	6

74	SERVIÇO DE MANUTENÇÃO DE CONTROLE DE ACESSO	UNIDADE	1	1	1	1	1	1	6
75	SERVIÇO DE RETIRADA DE PONTO CONTROLE DE ACESSO	UNIDADE	1	1	1	1	1	1	6
76	CURSO DE TREINAMENTO E TRANSFERÊNCIA DE CONHECIMENTO EM CONTROLE DE ACESSO	UNIDADE	1	1	1	1	1	1	6
77	FORNECIMENTO DE SWITCH CORE TIPO I COM INSTALAÇÃO E CONFIGURAÇÃO	UNIDADE		1					1
78	FORNECIMENTO DE SWITCH DE ACESSO COM PORTAS GIGABIT E POE COM INSTALAÇÃO E CONFIGURAÇÃO	UNIDADE	11	9	11	11	11	1	54
79	FORNECIMENTO DE INTERFACES SFP TIPO I – COM INSTALAÇÃO	UNIDADE	11	10	11	11	11	1	55
80	FORNECIMENTO DE INTERFACES SFP TIPO II – COM INSTALAÇÃO	UNIDADE		1					1
81	FORNECIMENTO DE INTERFACES SFP	UNIDADE		1					1

	TIPO III – COM INSTALAÇÃO								
82	RÁDIO PROFISSIONAL	UNIDADE		1					1
83	SERVIÇO COM FORNECIMENTO DE UPGRADE DE VELOCIDADE PARA RÁDIO PROFISSIONAL	UNIDADE		1					1
84	SERVIÇO DE CONFIGURAÇÃO DA SOLUÇÃO DE RÁDIO	UNIDADE		1					1
85	PONTO DE INTERCONEXÃO COM DISPOSITIVOS MÓVEIS	UNIDADE		1					1
86	SERVIÇO COM FORNECIMENTO DE LICENÇA DE GERENCIAMENTO DE PONTOS DE INTERCONEXÃO COM DISPOSITIVOS MÓVEIS	UNIDADE		1					1
87	DISPOSITIVO MÓVEL DE MONITORAMENTO	UNIDADE		1					1
88	PORTICO PARA CÂMERAS	UNIDADE	2	2			1	1	6

DER DF

ANEXO II

MODELO “A”: EMPREGADOR PESSOA JURÍDICA

D E C L A R A Ç Ã O

Ref.: (identificação da licitação)

....., inscrito no CNPJ nº....., por intermédio de seu representante legal o(a) Sr(a)....., portador(a) da Carteira de Identidade nº..... e do CPF nº ....., DECLARA, para fins do disposto no inciso V do art. 27 da Lei nº 8.666, de 21 de junho de 1993, acrescido pela Lei nº 9.854, de 27 de outubro de 1999, que não emprega menor de dezoito anos em trabalho noturno, perigoso ou insalubre e não emprega menor de dezesseis anos.

Ressalva: emprega menor, a partir de quatorze anos, na condição de aprendiz ( ).

.....

(data)

.....

(representante)

(Observação: em caso afirmativo, assinalar a ressalva acima)

DER DF

ANEXO III

M O D E L O - DECLARAÇÃO DE CIÊNCIA E TERMO DE RESPONSABILIDADE

A empresa _____, inscrita no CNPJ sob o nº _____, sediada no endereço _____, telefone/fax nº _____, por intermédio do seu representante legal Sr(a). _____ _____, portador(a) da Carteira de Identidade nº _____ e do CPF nº _____, DECLARA que atende a todos os requisitos de habilitação para participação em procedimentos licitatórios, bem como RESPONSABILIZA-SE pelas transações efetuadas em seu nome, assumindo como firmes e verdadeiras suas propostas e lances, inclusive os atos praticados diretamente ou por seu representante, nos termos do Decreto Federal nº 10.024, de 20/09/2019, adotado no âmbito do DF através do Decreto nº 25.966, de 23/06/2005.

Compromete-se, ainda, o encaminhamento da presente Declaração/Termo, devidamente assinado, à Comissão Julgadora Permanente do DER-DF, no prazo de 03 (três) dias úteis, juntamente com a documentação necessária, no endereço: Setor de Administração Municipal, Bloco "C", Ed. Sede do DER-DF, Brasília-DF.

Brasília-DF, ___ de _____ de _____.

_____

Representante Legal

Observações: Preferencialmente preencher em papel timbrado da empresa e apresentar, caso não cadastrado no SICAF, toda a documentação necessária ao cadastramento no "licitações-e", tais como aquelas relativas à:

I) habilitação jurídica, quando for o caso;

II) qualificação técnica;

III) qualificação econômico-financeira, quando for o caso;

IV) regularidade fiscal com a Fazenda Nacional, o sistema de seguridade social e o Fundo de Garantia de Tempo de Serviço – FGTS;

V) regularidade fiscal perante s Fazendas Estaduais e Municipais; e

VI) ao cumprimento do disposto no inciso XXXIII do art. 7º da Constituição e no inciso XVIII do art. 78 da Lei nº 8.666, de 1993.

DER DF

ANEXO IV

MODELO DE DECLARAÇÃO PARA MICROEMPRESA E EMPRESA DE PEQUENO PORTE

....., inscrita no CNPJ nº....., por intermédio de seu representante legal o(a) Sr. (a)....., portador(a) da Carteira de Identidade nº.....e o CPF nº....., DECLARA, para fins legais, sob as penas da lei, de que cumpre os requisitos legais para a qualificação como microempresa ou empresa de pequeno porte nas condições do Estatuto Nacional da Microempresa e da Empresa de Pequeno Porte, instituído pela Lei Complementar nº. 123, de 14 de dezembro de 2006, em especial quanto ao seu art. 3º, e que está apta a usufruir do tratamento favorecido estabelecido nos art. 42 a 49 da referida Lei Complementar, e que não se enquadra nas situações relacionadas no §4º do art. 3º da citada Lei Complementar.

_____

Representante Legal

DER DF

ANEXO V

Declaro de que atendo aos requisitos previstos no artigo 2º da Lei Distrital nº 4.770, de 22 de fevereiro de 2012.

_____

Representante Legal

DER DF

ANEXO VI

DECLARAÇÃO PARA OS FINS DO DECRETO Nº 39.860, DE 30 DE MAIO DE 2019

ÓRGÃO/ENTIDADE
PROCESSO
MODALIDADE DE LICITAÇÃO
NÚMERO DA LICITAÇÃO
L I C I TA N T E
CNPJ/CPF
INSCRIÇÃO ESTADUAL/DISTRITAL
REPRESENTANTE LEGAL
CPF

A pessoa física ou jurídica acima identificada, por intermédio de seu representante legal, declara que não incorre nas vedações previstas no art. 9º da Lei nº 8.666, de 21 de junho de 1993, e no art. 1º do Decreto nº 39.860, de 30 de maio de 2019. Essa declaração é a expressão da verdade, sob as penas da lei.

Brasília, _____, de _____ de _____.

_____

Assinatura

ANEXO VII – MINUTA DA ATA DE REGISTRO DE PREÇOS

ATA DE REGISTRO DE PREÇOS nº: _____/20____

PROCESSO nº: _____

PREGÃO nº: _____

O DISTRITO FEDERAL, por intermédio do DEPARTAMENTO DE ESTRADAS DE RODAGEM DO DISTRITO FEDERAL – DER/DF, com sede nesta Capital, no Setor de Administração Municipal – Bloco "C" - Edifício Sede do DER/DF, inscrito no CNPJ/MF nº 00.070.532/0001-03, neste ato representado na forma do seu Regimento Interno, instituído pelo Decreto nº 37.949, de 12 de janeiro de 2017, nos termos da Lei nº 8.666, de 21 de junho de 1993, da Lei nº 10.520, de 17 de julho de 2002, e do Decreto Federal nº 7.892, de 23 de janeiro de 2013, no que couberem, do Decreto Distrital nº 39.103, de 6 de junho de 2018, do Decreto Federal nº 10.024, de 20 de setembro de 2019, e das demais normas legais aplicáveis, em face da classificação das propostas apresentadas no Pregão Eletrônico SRP nº ____/_____, RESOLVE registrar os preços ofertados pelo Fornecedor Beneficiário (licitante vencedor), _____, localizado _____, inscrito no CNPJ sob o nº _____, representado pelo _____ conforme quadro abaixo:

Item	Qtd. Total Registrada	Unid.	Especificação do Objeto	Valor Unitário (R$)	Valor Total (R$)

CONDIÇÕES GERAIS:

1.1. Os prazos, as quantidades e as condições de entrega obedecerão aos critérios estabelecidos no Edital do Pregão Eletrônico SRP nº _____/_____ (Processo SEI/GDF nº _____).

1.2. O pedido mínimo para efeito de contratação corresponderá a 1 (uma) unidade dos itens constantes no Termo de Referência.

1.3. A existência de preços registrados não obriga o DER/DF a firmar as contratações que deles poderão advir, facultando-se a realização de licitação específica para a aquisição pretendida, sendo assegurado ao fornecedor beneficiário do registro preferência de fornecimento em igualdade de

condições, nos termos do art. 15, §4º da Lei nº 8.666/1993 c/c art. 16 do Decreto Distrital nº 39.103/2018.

1.4. O teor do Edital do Pregão Eletrônico SRP nº _____/_____, seus anexos e as propostas do fornecedor beneficiário, bem como dos licitantes que aceitaram cotar os bens ou os serviços com preços iguais ao do licitante vencedor, são partes integrantes desta Ata.

1.5. Este Registro de Preços tem vigência de 12 (doze) meses, contados da data de sua assinatura, sendo seu extrato publicado no Diário Oficial do Distrito Federal, às expensas do DER/DF.

1.6. A presente Ata, após lida e achada conforme, é assinada pelos representantes legais do Departamento de Estradas de Rodagem do Distrito Federal e do Fornecedor Beneficiário.

1.7. Fica eleito o Foro da Justiça Comum do Distrito Federal para dirimir eventuais controvérsias relativas à presente Ata de Registro de Preços.

Brasília/DF, _____ de _____ de _____.

DEPARTAMENTO DE ESTRADAS DE RODAGEM DO DISTRITO FEDERAL
[autoridade do DER/DF competente para assinar a Ata de Registro de Preços]

FORNECEDOR BENEFICIÁRIO (LICITANTE VENCEDOR):

[Razão social da empresa]
Representante legal: [nome completo]
CI: [número e órgão emissor]
CPF: [número]
Instrumento de outorga de poderes: [procuração/contrato social/estatuto social]
[procuração/contrato social/estatuto social]

ANEXO À ATA DE REGISTRO DE PREÇOS Nº _____

Para efeitos do disposto no art. 11 do Decreto Distrital nº 39.103, de 6 de junho de 2018, fica incluído na ATA DE REGISTRO DE PREÇOS Nº _____, na forma do presente Anexo, o registro dos licitantes que aceitaram cotar os produtos com preços iguais ao do licitante vencedor, na sequência da classificação do certame, da seguinte forma:

Licitante classificado em _____, empresa _____, localizado _____, inscrito no CNPJ sob o nº _____, representado neste ato por _____

Brasília/DF, _____ de _____ de _____.

DEPARTAMENTO DE ESTRADAS DE RODAGEM DO DISTRITO FEDERAL

[autoridade do DER/DF competente para assinar a Ata de Registro de Preços]

DEMAIS LICITANTE(S) REGISTRADO(S):

[Razão social da empresa]

Representante legal: [nome completo]

CI: [número e órgão emissor]

CPF: [número]

Instrumento de outorga de poderes: [procuração/contrato social/estatuto social]

[procuração/contrato social/estatuto social]

ANEXO VIII – MINUTA DE CONTRATO

PROCESSO Nº

CONTRATO Nº /20___

CONTRATO QUE ENTRE SI FAZEM O DEPARTAMENTO DE ESTRADAS DE RODAGEM DO DISTRITO FEDERAL - DER/DF E _____, OBJETIVANDO A PRESTAÇÃO DE SERVIÇOS, _____, NA FORMA ABAIXO.

O DEPARTAMENTO DE ESTRADAS DE RODAGEM DO DISTRITO FEDERAL - DER/DF, sediado no SAM Bloco "C" Edifício Sede do DER/DF, Setor Complementares – BRASÍLIA/DF, inscrito no CNPJ sob o nº 00.070.532/0001-03, doravante denominado DER/DF, neste ato representado por seu Diretor Geral, Engº _____, e o Superintendente de _____, o _____, , e a empresa _____, com sede no _____, inscrita no CNPJ sob o _____, doravante denominada CONTRATADA, neste ato representada por _____, RG nº _____ e CPF nº _____, conforme poderes apresentados e arquivados, resolvem firmar o presente contrato sob a regência da Lei n.º 8.666 de 21 de junho de 1993, mediante as seguintes cláusulas:

CLÁUSULA PRIMEIRA - DA FUNDAMENTAÇÃO

O presente instrumento tem por fundamento legal o Edital de Pregão Eletrônico nº ____/_____-DMASE/SUAFIN/DER-DF, devidamente homologado, SEI _____.

CLÁUSULA SEGUNDA - DO OBJETO

Constitui objeto do presente contrato a prestação de serviços, sob demanda, de tudo conforme especificações nos anexos do Edital de Pregão Eletrônico nº ____/_____, e a proposta da Contratada, SEI _____

CLÁUSULA TERCEIRA – DA FORMA E REGIME DE EXECUÇÃO

O Contrato será executado de forma indireta, sob o regime de empreitada unitário, segundo o disposto nos artigos 6º e 10º da Lei n. 8.666/93.

CLÁUSULA QUARTA - DAS ESPECIFICAÇÕES

Na execução dos serviços, objeto do presente Contrato, deverão ser observadas as especificações constantes do Edital e seus anexos, e as Normas Técnicas vigentes no DER/DF, independentemente de transcrição.

CLÁUSULA QUINTA - DAS OBRIGAÇÕES

5.1. Fica a Contratada responsável pelas obrigações relacionadas no Edital de Pregão Eletrônico nº _____/_____, e na proposta aceita pelo DER-DF (SEI _____) e por quaisquer danos pessoais ou materiais causados por seus empregados a terceiros, bem como o pagamento de salários, encargos sociais e trabalhistas, tributos e demais despesas eventuais, decorrentes da prestação de serviços.

5.2. Integra o presente Contrato o Edital de Pregão Eletrônico nº ___/____, Anexos e Especificações, bem como a proposta da Contratada, independentemente de transcrição.

5.3. Os serviços, objeto do presente Contrato, serão executados de conformidade com a legislação vigente, Normas Técnicas ABNT e Código de Edificações do Distrito Federal.

5.4. DAS OBRIGAÇÕES DA CONTRATADA:

5.4.1. Manter, durante toda a execução do contrato, em compatibilidade com as obrigações assumidas, todas as condições de habilitação e qualificação exigidas no ato convocatório;

5.4.2. Responsabilizar-se por quaisquer danos pessoais e/ ou materiais, causados por técnicos (empregados) e acidentes causados por terceiros, bem como pelo pagamento de salários, encargos sociais e trabalhistas, tributos e demais despesas eventuais, decorrentes da prestação dos serviços;

5.4.3. Responsabilizar-se das eventuais despesas para execução do serviço solicitado, qualquer que seja o valor, e cumprir todas as obrigações constantes do(s) Anexo(s) deste Ato Convocatório;

5.4.4. Comprovar, mês a mês, o efetivo recolhimento dos encargos sociais incidentes sobre a folha de pagamento dos empregados destinados para a prestação dos serviços;

5.4.5. Constitui obrigação da contratada o disposto no Termo de Referência (Anexo I) do presente edital.

5.5. DAS OBRIGAÇÕES DO DER-DF:

5.5.1. Indicar o executor interno do Contrato, conforme Art. 67 da Lei 8.666/93 e Dec. 32.598/2010;

5.5.2. Cumprir os compromissos financeiros assumidos com a Contratada;

5.5.3. Fornecer e colocar à disposição da Contratada, todos os elementos e informações que se fizerem necessários à execução dos serviços;

5.5.4. Notificar, formal e tempestivamente, a contratada sobre as irregularidades observadas no serviço;

5.5.5. Notificar a Contratada, por escrito e com antecedência sobre multas, penalidades quaisquer débitos de sua responsabilidade, bem como fiscalizar a execução do Objeto Contratado.

CLÁUSULA SEXTA - DO VALOR

O valor estimativo total do presente Contrato, sob demanda, é de R$ _____ (por extenso), procedentes do Orçamento do DER/DF para o corrente exercício, nos termos da correspondente Lei Orçamentária Anual.

CLÁUSULA SÉTIMA - DA DOTAÇÃO

A despesa correrá à conta da seguinte Dotação Orçamentária:

I – Unidade Orçamentária: 26.205;

II – Programa de Trabalho:

III – Natureza da Despesa: 4; e

IV – Fonte de Recursos: 0.

7.2. Foi emitida a Nota de Empenho nº ____, datada de ___/___/____, no valor de R$ _____(por extenso), na modalidade _____.

CLÁUSULA OITAVA – DO REAJUSTE

8.1. O contrato poderá ser reajustado após transcorrido 1 (um) ano de sua vigência, em conformidade com a legislação pertinente.

CLÁUSULA NONA - DA GARANTIA

A garantia de ___% (_____ por cento) do valor deste Contrato, ora efetivada conforme previsão constante no Ato convocatório, será ao final do contrato restituída em até 30 (trinta) dias, após requerida ao Diretor Geral do DER/DF.

9.1. Não serão devolvidos a garantia inicial, respectivos reforços e multas, no caso de rescisão do Contrato por culpa exclusiva da Contratada.

CLÁUSULA DÉCIMA - DO PAGAMENTO

10.1. Para efeito de pagamento, a CONTRATADA deverá apresentar os documentos abaixo relacionados:

I – Certidão Negativa de Débitos Relativos às Contribuições Previdenciárias e às de Terceiros, expedida pela Secretaria da Receita Federal do Brasil (Anexo XI da Portaria Conjunta PGFN/RFB nº 3, de 2.5.2007), observado o disposto no art. 4º do Decreto nº 6.106, de 30.4.2007;

II – Certificado de Regularidade do Fundo de Garantia por Tempo de Serviço – FGTS, fornecido pela CEF – Caixa Econômica Federal, devidamente atualizado (Lei n.º 8.036/90);

III – Prova de regularidade para com a Fazenda Federal mediante apresentação de Certidão Conjunta Negativa de Débitos relativos a Tributos Federais e à Dívida da União, expedida pela Procuradoria Geral da Fazenda Nacional – PGFN ou pela Secretaria da Receita Federal do Brasil, em plena validade;

IV – a empresa sediada, domiciliada ou com filial no Distrito Federal, deverá apresenta, também, prova de quitação com a Fazenda do Distrito Federal (Certidão de Regularidade com a Fazenda do Distrito Federal);

V – Certidão Negativa de Débitos Trabalhistas (CNDT), emitida pelo Tribunal Superior do Trabalho, nos termos da Lei 12.440/2011, em plena validade.

10.2. O pagamento será efetuado até 30 (trinta) dias, contados a partir da data de apresentação da Nota Fiscal, desde que o documento de cobrança esteja em condições de liquidação de pagamento.

10.3. Nenhum pagamento será efetuado à licitante enquanto pendente de liquidação, qualquer obrigação que lhe for imposta, em virtude de penalidade ou inadimplência, sem que isso gere direito ao pleito de reajustamento de preços ou correção monetária (quando for o caso).

10.4. Caso haja multa por inadimplemento contratual, será adotado o seguinte procedimento:

I – Se o valor da multa for superior ao valor da garantia prestada, além da perda desta, responderá a contratada pela sua diferença, a qual será descontada dos pagamentos eventualmente devidos pela Administração ou ainda, quando for o caso, cobrada judicialmente.

10.5**.** Para as empresas com sede ou domicílio no Distrito Federal, com créditos de valores iguais ou superiores a R$ 5.000,00 (cinco mil reais), os pagamentos serão feitos exclusivamente, mediante crédito em conta corrente, em nome do beneficiário junto ao Banco de Brasília S/A – BRB. Para tanto deverão apresentar o número da conta corrente e agência onde deseja receber seus créditos, de acordo com o Decreto n.º 32.767 de 17/02/2011, publicado no DODF nº 35, pág.3, de 18/02/2011.

CLÁUSULA DÉCIMA PRIMEIRA - DOS PRAZOS

11.1. O prazo de vigência do contrato será de 48 (quarenta e oito) meses, a contar da data de sua assinatura, podendo ser prorrogado, com base no inciso II, artigo 57 da Lei nº 8.666/93, desde que não haja denúncia de quaisquer das partes e, terá o seu extrato publicado na Imprensa oficial, que é condição indispensável para sua eficácia.

11.1.1**.** A prorrogação do contrato será precedida de pesquisa para verificar se as condições oferecidas pela licitante contratada continuam mais vantajosas para o DER-DF.

CLÁUSULA DÉCIMA SEGUNDA – DA ALTERAÇÃO CONTRATUAL

Toda e qualquer alteração contratual deverá ser processada mediante celebração de Termo Aditivo, com amparo no art. 65 da Lei n. 8.666/93, vedada a modificação do objeto.

CLÁUSULA DÉCIMA TERCEIRA – DA RESPONSABILIDADE DO DER/DF

O DER/DF responderá pelos danos que seus agentes, nessa qualidade, causarem a terceiros, assegurado o direito de regresso contra o responsável nos casos de dolo e de culpa.

CLÁUSULA DÉCIMA QUARTA - DAS PENALIDADES

Em caso de inexecução parcial ou total da execução dos serviços, de qualquer outra inadimplência, a Contratada estará sujeita, sem prejuízo da responsabilidade civil e criminal, no que couber, garantida prévia defesa, às penalidades previstas no Artigo 87, Incisos I a IV da Lei nº 8.666 de 21 de junho de 1993.

15.1. No caso de multas, observar-se-á o disposto no Artigo 86 da Lei nº 8.666/1993.

15.2. Se a multa aplicada for superior ao valor da garantia prestada, além da perda desta, responderá a Contratada pela sua diferença, que poderá ser descontada de pagamentos eventualmente devidos pelo DER/DF, ou cobrada judicialmente.

CLÁUSULA DÉCIMA QUINTA – DA DISSOLUÇÃO

O Contrato poderá ser dissolvido de comum acordo, bastando, para tanto, manifestação escrita de uma das partes, com antecedência mínima de 60 (sessenta) dias, sem interrupção do curso normal da execução do Contrato.

CLÁUSULA DÉCIMA SEXTA - DA RESCISÃO

Operar-se-á de pleno direito a rescisão do Contrato, independentemente de interpelação judicial ou extrajudicial, sem prejuízo das penalidades previstas na Cláusula Décima Quinta, quando ocorrerem as hipóteses enumeradas nos Incisos I a XVII, do Artigo 78, da Lei n.º 8.666, de 21 de junho de 1993.

17.1. Na hipótese da rescisão prevista no Artigo 79, Inciso I, fica o DER/DF autorizado a adotar as providências elencadas no Artigo 80, da Lei de regência.

CLÁUSULA DÉCIMA SÉTIMA - DOS RECURSOS ADMINISTRATIVOS

Dos atos do DER/DF, decorrentes do presente ajuste, caberá recurso na forma do disposto no Artigo 109, da Lei n.º 8.666, de 21 de junho de 1993.

CLÁUSULA DÉCIMA OITAVA – DOS DÉBITOS PARA COM A FAZENDA PÚBLICA

Os débitos da Contratada para com o DER/DF, decorrentes ou não do ajuste, serão cobrados na forma da legislação pertinente, podendo, quando for o caso, ensejar a rescisão unilateral do Contrato.

CLÁUSULA DÉCIMA NONA – DO EXECUTOR

O Diretor Geral do DER/DF, por meio de Instrução de Serviço, designará um Executor para o Contrato, que desempenhará as atribuições previstas nas Normas de Execução Orçamentária, Financeira e Contábil.

CLÁUSULA VIGÉSIMA – DA PUBLICAÇÃO E DO REGISTRO

A eficácia do Contrato fica condicionada à publicação resumida do instrumento pelo DER/DF, na Imprensa Oficial, até o quinto dia útil do mês seguinte ao de sua assinatura, par ocorrer no prazo de vinte dias daquela data, após o que deverá ser providenciado o registro do instrumento pela Procuradoria Jurídica do DER/DF.

CLÁUSULA VIGÉSIMA PRIMEIRA - DO FORO

Para as questões decorrentes deste contrato fica eleito o Foro da Capital da República.

E, por estarem assim justas e de acordo, para a firmeza e validade do que ficou estipulado, lavrou-se o presente, que lido e achado conforme, é assinado pelas partes.

Brasília, de de 20....

Pelo DER/DF:

Pela SU.....:

Pela CONTRATADA: