

## **CADERNO DE ESPECIFICAÇÕES TÉCNICAS MINÍMAS E OBRIGATÓRIAS – OBJETO SERVIÇO**

## SUMÁRIO

<b>1. DESCRIÇÃO DO SISTEMA .....</b>	<b>3</b>
<b>2. EQUIPAMENTOS DOS PONTOS DE VIDEOMONITORAMENTO URBANO .....</b>	<b>4</b>
<b>3. COMPONENTES DE CIICC .....</b>	<b>9</b>
<b>5. SERVIDORES .....</b>	<b>13</b>
<b>6. INTEGRAÇÕES.....</b>	<b>14</b>
<b>7. SOFTWARE DE GERENCIAMENTO DE VÍDEOS (VMS).....</b>	<b>15</b>
<b>8. SEGURANÇA.....</b>	<b>22</b>
<b>9. ADMINISTRAÇÃO DO SISTEMA, SUPORTE TÉCNICO E MANUTENÇÃO .....</b>	<b>24</b>
<b>10. TREINAMENTOS.....</b>	<b>27</b>
<b>11. PADRÃO DE ENVIO DE METADADOS PARA A SSP .....</b>	<b>28</b>

## 1. DESCRIÇÃO DO SISTEMA

1.1. **TOPOLOGIA:** para otimizar o desempenho e a eficiência da solução, será adotada uma abordagem híbrida. Nessa configuração, a tecnologia e suas funcionalidades serão instaladas na camada de borda (câmeras) e/ou servidores VMS (*Video Management System*).



- ✓ O processamento de análise de reconhecimento de placas de veículos (LPR) deverá ser **obrigatoriamente** executado na camada de borda, enquanto os demais recursos analíticos poderão ser processados nas câmeras ou nos servidores VMS.

1.2. **ARQUITETURA EM FEDERAÇÃO:** O sistema deverá trabalhar numa arquitetura em federação, com uma central de videomonitoramento principal em Goiânia e com os 04 (quatro) novos centros de videomonitoramento subordinados (Águas Lindas de Goiás, Formosa, Luziânia e cidade de Goiás).

1.3. **CÂMERAS:** Todas as câmeras fornecidas deverão ser capazes de processar imagens e ter funções analíticas básicas. Não serão aceitas câmeras que apenas capturem e enviem vídeos, sem tratamentos analíticos.

1.4. A solução deve ser configurada para suportar os seguintes recursos analíticos:

1.4.1. **Reconhecimento facial:** permite identificar e rastrear pessoas específicas pelas suas características faciais e *uploads* de fotos. No contexto dessa contratação, entende-se como “Reconhecimento Facial” a funcionalidade ou recurso do sistema em identificar um indivíduo com base na comparação com outras imagens daquele indivíduo. Esse termo é diferente ao de “Detecção Facial”, que é um recurso do sistema utilizado para reconhecer a existência de uma face na imagem ou vídeo, capturar características dessa face, mas sem identificar a pessoa.

1.4.2. **Analítico de pessoas:** permite realizar a pesquisa por meio da análise de similaridade de imagens:

- a) Características físicas: gênero, cor de roupa, mochila/bolsa, chapéu e outros;
- b) Características da face: gênero, idade, óculos, máscara e outros;
- c) Análise de comportamento: aglomeração, densidade populacional em determinada área e outros.

1.4.3. **Analítico de veículo:** permite realizar leitura e contagem de placas (*License Plate Recognition - LPR*), e reconhecimento de características do veículo (cor, marca e tipo de veículo, etc.);

## 1.5. DISPOSIÇÕES GERAIS

1.5.1. Todos os equipamentos fornecidos devem ser novos e sem histórico de uso anterior, não sendo aceitáveis equipamentos de origem reaproveitada ou recondicionada (*refurbished*).

1.5.2. Todos os itens, da planilha de cotação, já devem estar embutidos o valor de instalação e manutenção dos equipamentos e infraestrutura necessária para o funcionamento da solução. Sendo tudo na forma de serviço garantindo a atualização tecnológica, manutenção e substituição quando necessário entregando uma solução completa.

1.5.3. A conectividade/*link* dos equipamentos até os CIICCs e entre CIICCs será de responsabilidade da CONTRATADA.

1.5.4. O custo da conectividade/*link* para transmissão das imagens das câmeras deverá ser inserido no custo mensal dos postes.

1.5.5. O custo da conectividade/*link* entre os CIICCs regionais deve estar embutido no item **CIICC – REGIONAL**.

1.5.6. O custo da conectividade/*link* entre os CIICCs regionais e o CIICC principal deve estar embutido no item **CIICC – PRINCIPAL**.

1.5.7. Todos os *links*/conectividade devem ser dimensionados de acordo com as necessidades da solução, deve ser considerado a transmissão das câmeras em full bit rate (Nível mais alto de qualidade) garantindo a qualidade das imagens a serem analisadas e armazenadas, não deve ser utilizado buffer no streaming com o intuito de reduzir a latência das imagens das câmeras, as imagens em tempo real devem ter menor latência possível.

1.5.8. Os preços que forem apresentados na proposta deverão cobrir todos os custos: autorizações e licenças junto aos órgãos fiscalizadores e concessionários, o fornecimento de materiais e acessórios necessários, mão de obra especializada para sua execução, leis e encargos sociais decorrentes, ferramentas e equipamentos adequados ao serviço, transportes, remoção, máquinas ou equipamentos para execução dos serviços, enfim, tudo o que for preciso para garantir a qualidade e funcionalidade do sistema, com a segurança esperada.

1.5.9. a CONTRATADA arcará com as despesas de energia elétrica geradas pelo consumo das novas unidades consumidoras (UCs) necessárias para energização e ativação das câmeras de monitoramento, durante todo o período do contrato.

1.6. **PROJETO TÉCNICO:** abrange a identificação dos locais onde as câmeras serão instaladas e os tipos de câmeras a serem utilizadas. Os elementos-chave de um projeto técnico de videomonitoramento devem incluir no mínimo:

- ✓ Localização e tipo das câmeras;
- ✓ Software de gerenciamento;
- ✓ Armazenamento de dados;
- ✓ Integração com outros sistemas;
- ✓ Treinamento e documentação.

## 2. EQUIPAMENTOS DOS PONTOS DE VIDEOMONITORAMENTO URBANO

Para atender às funcionalidades analíticas mencionadas será permitido o uso de até 03 (três) modelos de câmeras distintas, conforme descrito abaixo:

- Câmera Tipo I: para analítico de veículos em velocidade até 110km/h.
- Câmera Tipo II: para analítico de veículos em velocidade até 180km/h.
- Câmera Tipo III: para reconhecimento facial, característica de pessoas e característica de veículos.

## 2.1. REQUISITOS OBRIGATÓRIOS PARA TODAS AS CÂMERAS

2.1.1. **Rede:** Possuir interface de rede RJ-45;

2.1.2. **Protocolos de Rede:** deve possuir no mínimo HTTP ou HTTPS, TCP, UDP, NTP e FTP;

2.1.3. **Compressão de Vídeo:** Deve possuir, no mínimo, as compressões de vídeo H.264, H.265 e MJPEG

2.1.4. **WDR:** Possuir alcance dinâmico estendido (WDR) de 120dB ou superior;

2.1.5. **Infravermelho:** deve possuir iluminador IR de 30m (podendo estar embutido na câmera ou em equipamento externo);

2.1.6. **Fluxos (*streams*) simultâneos:** deve possuir capacidade de suportar o envio de no mínimo 3 fluxos simultâneos para diferentes IPs;

2.1.7. **Armazenamento:** As câmeras devem possuir capacidade para a instalação de cartões de memória, e devem ser fornecidas com cartão SD de no mínimo 128GB compatível com gravação criptografada, classe 10;

2.1.8. **Alarmes externos:** Possuir, no mínimo, 1 entrada e 1 saída de alarme;

2.1.9. **Alimentação:** Deverá ser capaz de ser alimentada por fonte de alimentação DC 12V, AC 24V ou PoE;

2.1.10. **Ambiente de operação:** faixa de temperatura de 0 a +60º C e umidade inferior a 90%;

2.1.11. **Segurança:** A câmera deverá possuir, no mínimo, os seguintes métodos de proteção contra ataques cibernéticos:

- ✓ O firmware deve ser proprietário do fabricante;
- ✓ As câmeras devem possuir proteção contra ataques de força bruta, como proteção por senha, inicialização segura e logs de acesso de usuários;
- ✓ As câmeras devem possuir proteção contra ataques de rede DDoS e Phishing;
- ✓ O dispositivo deve possuir segurança criptografada ponto a ponto, comprovada pelo fabricante;
- ✓ O dispositivo deve possuir tecnologia de checagem de dados ou filtragem de IP, disponibilizando filtros de IP (autorizados ou bloqueados);
- ✓ O dispositivo deve ser capaz de garantir a segurança na atualização de firmwares, permitindo somente a utilização de versões lançadas pelo fabricante e identificando pacotes de origem divergente ou suspeita;

2.1.12. **Compatibilidade:** Deve possuir pelo menos o protocolo ONVIF para compatibilidade entre fabricantes.

2.1.13. A câmera deverá possuir função de detecção de violação;

2.1.14. **Requisitos mínimos para instalação:**

- ✓ A câmera deve ser acompanhada de caixa de junção hermética, de modo a garantir plena conexão e vedação entre as partes, permitindo maior durabilidade e preservando, assim, a garantia; e deve ser fornecida com suporte para instalação e com todos os acessórios necessários para fixação em poste;
- ✓ No caso de fornecimento de **câmera do tipo "bullet"**, a câmera deverá ser instalada com o invólucro em alumínio com índice de proteção contra vandalismo IK10 e fator de proteção IP66 ou superior;
- ✓ No caso de fornecimento de **câmera do tipo caixa (box)**, deverá ser fornecida caixa de proteção com fator de proteção IP66 ou superior e fator de proteção contra impactos IK10; e a caixa deverá ser capaz de acoplar iluminador infravermelho e alimentá-lo.

## 2.2. **CÂMERA TIPO I: Analítico de veículos em velocidade até 110km/h**

2.2.1. Câmera para aplicação analítico de veículos que trafeguem a até 110km/h; A câmera para reconhecimento automático das placas veiculares (LPR) deverá operar ou de forma autônoma ou com hardware e software exclusivos, porém estes como parte integrante do custo do item, mesmo que seja proporcional à quantidade solicitada no certame;

### 2.2.2. **Características principais:**

- ✓ Sensor de imagem CMOS de 1/1.8" ou superior;
- ✓ Velocidade de obturador que atenda pelo menos aos limites de 1/25s a 1/30.000s;
- ✓ Resolução igual ou superior a 4MP;
- ✓ Taxa de frames de, no mínimo, 25fps;
- ✓ Lente varifocal de 8 a 32mm (ou superior), com ajuste automático no foco;

2.2.3. Deve possuir balanço de branco manual e automático;

### 2.2.4. **Deve possuir os seguintes analíticos:**

- ✓ Classificação por tipo de veículo, reconhecendo, no mínimo: carros, vans, caminhões, ônibus e motocicletas;
- ✓ Contagem de veículo;
- ✓ Deve reconhecer fabricantes de veículos;
- ✓ Deve reconhecer cores de veículos;
- ✓ Deve possuir a capacidade de efetuar o reconhecimento de placa de veículo (ANPR) em movimento, em velocidades de até 110km/h, usando tecnologia embarcada;

2.2.5. Deverá trabalhar em conjunto com o VMS, enviando metadados veiculares para permitir que o software gerencie todas as informações necessárias;

2.2.6. A comprovação do funcionamento deve ser feita através de carta do fabricante, tanto do VMS, quanto das câmeras, atestando a possibilidade de integração até a data de operacionalização dos equipamentos;

2.2.7. Deverá reconhecer placas padrão Brasil (conforme Resolução 231/2017 do CONTRAN e suas alterações) e do novo padrão Mercosul (conforme Resolução 729 do CONTRAN e suas alterações).

## 2.3. **CÂMERA TIPO II: Analítico de veículos em velocidade até 180 km/h.**

2.3.1. Câmera para aplicação de analítico de veículos que trafeguem a até 180km/h. A câmera deverá operar ou de forma autônoma ou com hardware e software exclusivos, porém estes como parte integrante do custo do item, mesmo que seja proporcional à quantidade solicitada no certame;

### 2.3.2. **Características Principais:**

- ✓ Sensor de imagem CMOS de 1/1.8" ou superior;
- ✓ Velocidade que atenda pelo menos aos limites de obturador de 1/25s a 1/30.000s;
- ✓ Resolução de 4MP;
- Taxa de frames mínima de 30 fps na resolução de 4MP;
- Possuir lente varifocal de 12 a 32mm (ou superior), com ajuste automático no foco;

2.3.3. Possuir Balanço do Branco manual e automático;

### 2.3.4. **Deve possuir os seguintes analíticos:**

- ✓ Classificação por tipo de veículo, reconhecendo, no mínimo: carros, vans, caminhões, ônibus e motocicletas;
- ✓ Contagem de veículo;
- ✓ Deve reconhecer fabricantes de veículos;

- ✓ Deve reconhecer cores de veículos;
- ✓ Deverá reconhecer caracteres de placas de veículos, combinando números e letras (ANPR), a uma velocidade de até 180 Km/h, possuir tecnologia embarcada;

2.3.5. Deverá trabalhar em conjunto com o VMS, enviando metadados veiculares para permitir que o software gerencie todas as informações necessárias;

2.3.6. A comprovação do funcionamento deve ser feita através de carta do fabricante, tanto do VMS, quanto das câmeras, atestando a possibilidade de integração até a data de operacionalização dos equipamentos;

2.3.7. Deverá reconhecer placas padrão Brasil (conforme Resolução 231/2017 do CONTRAN e suas alterações) e do novo padrão Mercosul (conforme Resolução 729 do CONTRAN e suas alterações).

#### 2.4. **CÂMERA TIPO III: Reconhecimento Facial e Analítico de Pessoas**

2.4.1. A Câmera para Reconhecimento Facial e Analítico de pessoas deverá operar ou de forma autônoma ou com hardware e software exclusivos, porém estes como parte integrante do custo do item, mesmo que seja proporcional à quantidade solicitada no certame;

2.4.2. Características Principais:

- ✓ Deverá possuir sensor de imagem CMOS de 1/2.7" ou superior;
- ✓ Deverá possuir velocidade do obturador de 1/3 a 1/10.000s ou superior;
- ✓ Possuir resolução de, no mínimo, de 4MP;
- ✓ Fluxo de vídeo com 30 fps, trabalhando em sua resolução máxima de 4MP. Não será aceito 60 fps em resoluções menores que a indicada;
- ✓ Permitir ajuste focal da lente entre 2.7 a 12mm ou 2.8 a 12mm;
- ✓ Deverá possuir sensibilidade mínima igual ou inferior a 0,012 lux no modo colorido, e a 0 lux no modo PB com IR ativado;

2.4.3. Deverá possuir as tecnologias HLC (Compensação de Luz Alta) e BLC (Compensação de Luz de Fundo);

2.4.4. Possuir função de Máscara de Privacidade de, no mínimo, 4 áreas;

2.4.5. Deve possuir os seguintes analíticos:

2.4.6. Possuir funções inteligentes de **Detecção de Faces**, Detecção de Cruzamento de Linha, Detecção de Intrusão, objetos deixados e objetos removidos;

- ✓ Detecção de características das pessoas, extraído no mínimo os seguintes atributos: idade, gênero, expressão, uso de máscara, uso de óculos e barba, cor de roupas, tipo de roupas (Ex: Camisa, Calça, etc) e utilização de mochila;
- ✓ Contagem de pessoas e detecção de aglomeração;
- ✓ Detecção de características de veículos, como tipo, fabricante e cor;
- ✓ Reconhecimento facial (obs.: este analítico só será necessário nos pontos indicados).

2.4.7. Nesse tipo de câmera, as funções de Reconhecimento Facial, Aglomeração, Contagem de Pessoas, Detecção de características de pessoas, Detecção de características de veículos, Contagem de veículos, Analítico para estacionamento irregular poderão opcionalmente, ser realizados pelo software VMS. Nesse caso, deverá ser incluído no fornecimento quaisquer softwares adicionais e licenças necessários para a execução desses analíticos.

2.4.8. A função de detecção facial deve ser obrigatoriamente realizada nas câmeras.

2.4.9. Todos os analíticos realizados pelas câmeras devem ocorrer simultaneamente, incluindo aqueles realizados na borda. Se optar por realizar analíticos em um servidor VMS, elas também devem ser feitas de forma simultânea.

2.4.10. A câmera deverá operar em conjunto com o VMS, enviando os metadados para que o software faça toda a gestão necessária de informações;

2.4.11. A comprovação do funcionamento deve ser feita através de carta do fabricante, tanto do VMS, quanto das câmeras, atestando a possibilidade de integração até a data de operacionalização dos equipamentos.

## 2.5. POSTE PARA CÂMERA

2.5.1. Poste metálico ou de concreto duplo T e no mínimo 150 daN, com 9 metros de comprimento;

2.5.2. Ser dimensionado para evitar trepidações provocadas por ventos de intensidade normal ou deslocamentos de ar causado pelo movimento de veículos;

2.5.3. Possuir tubulações que permitam acondicionamento de todos os cabos (ópticos, elétricos, etc.);

2.5.4. Deverá ser entregue com acessórios e fiação elétrica adequada para receber a carga elétrica dimensionada e possibilitar a instalação do medidor de energia. Essa instalação elétrica deverá estar de acordo com a norma técnica da Concessionária de energia elétrica, que dispõe sobre novas instalações elétricas em sua região de abrangência;

2.5.5. Deverá possuir base de ser engastado em profundidade mínima de 1,5 m;

2.5.6. Deverá ser fornecido com braços para alocação das câmeras;

2.5.7. Deverá ser fornecido com todo o sistema de aterramento e caixa de inspeção de acordo com as normas ABNT para atender todos os sistemas nele instalados, permitindo que todos os dispositivos tenham uma referência de terra.

2.5.8. Todos os materiais necessários para a instalação do poste serão de responsabilidade da CONTRATADA, tais como: caixas, cabos, conectores, adaptadores, disjuntores, suportes, parafusos, etc.

### 2.5.9. Quanto à instalação dos postes:

2.5.10.1. Os postes abrigarão as caixas herméticas com pontos de conexões e as câmeras;

2.5.10.2. A instalação do poste consiste na execução de todos os serviços necessários para o perfeito funcionamento do sistema, incluindo a instalação de materiais de infraestrutura utilizados na sustentação, suporte e guiamento tais como: fitas de aço inox, suportes, parafusos, braçadeiras, tubos galvanizados, cabos, conectores, caixas. Também deverá ser previsto o licenciamento para utilização do local onde o poste será instalado. Os custos para este licenciamento serão de responsabilidade da CONTRATADA;

2.5.10.3. Será de responsabilidade da empresa contratada a limpeza do local de trabalho, bem como todo e qualquer acabamento necessário;

2.5.10.4. Deverá prever a identificação física do poste e documentação técnica do material e/ ou equipamento, conforme layout projetado da solução;

2.5.10.5. Estão inclusos todos os serviços de escavação, transporte, içamento, instalação e limpeza da área de trabalho, os quais deverão seguir e estarem em completo acordo com as normas e recomendações dos organismos governamentais competentes, ainda que não especificados neste termo, nas versões vigentes quando da apresentação das propostas.

2.5.10.6. Será de responsabilidade da CONTRATADA a solicitação de energização da unidade consumidora (UC) à Concessionária de Energia Elétrica, e será de responsabilidade da CONTRATADA o pagamento das contas das unidades consumidoras (UC) geradas para alimentação das câmeras, durante o período do contrato (60 meses).

## 2.6. CAIXA HERMÉTICA

2.6.1. Deverá possuir entradas para ventilação;

2.6.2. Suportar condições de instalação externa exposta ao tempo;

2.6.3. Deverá possuir circuitos de detecção, proteção e atuação em caso de surtos elétricos. Para isso, cada caixa deverá ser entregue com os seguintes equipamentos de proteção elétrica, sendo o dimensionamento dos quantitativos de responsabilidade da CONTRATADA:

- ✓ DPS (dispositivo de proteção contra surto) Classe I 12,5/60 kA 275V;
- ✓ Disjuntor classe "C";

2.6.4. Para a interconexão dos dispositivos à rede, todo o cabeamento de rede deverá ser Cat. 5 ou superior. O fornecimento e a instalação de todo o cabeamento de rede necessário, bem como switches ou injetores PoE para alimentação das câmeras instaladas no poste, é de responsabilidade da CONTRATADA e os custos deverão já estar inclusos na proposta. Para postes que contemplarem duas ou mais câmeras por caixa, deverá ser fornecido switch.

## 3. COMPONENTES DE CIICC

A CONTRATANTE fornecerá sala já adequada às instalações dos CIICCs, não havendo necessidade de previsão de nenhum tipo de reforma civil pela contratada.

### 3.1. COMPONENTES DOS CIICCs REGIONAIS:

Os itens que compõe o item CIICC REGIONAL está descrito na tabela.

Quantidade	Item
01	Ledwall de 5m <sup>2</sup>
01	Controladora de imagem para o ledwall
06	Workstations
01	Gabinete para alocar os equipamentos

### 3.2. COMPONENTES DO CIICC PRINCIPAL:

Os itens que compõe o item CIICC PRINCIPAL está descrito na tabela.

Quantidade	Item
04	Workstations

### 3.3. WORKSTATION:

As workstations devem ser do tipo desktop e possuir no mínimo as seguintes configurações:

3.3.1. O equipamento deverá estar equipado com um ou dois processadores. As especificações mínimas do processador sozinho ou em conjunto devem possuir 4 núcleos de processamento e 4 threads (ou mais), para que atinja o desempenho mínimo esperado.

3.3.2. RAM: pelo menos 16 GB

3.3.3. NIC (Network Interface Card): GbE

3.3.4. No mínimo 2 placas de rede, RJ-45;

3.3.5. Uma placa de vídeo com capacidade de 4GB ou superior.

3.3.6. Tensão de entrada 110 a 220 Vac.

3.3.7. Ser fornecida com os seguintes acessórios:

- ✓ 01 (um) Teclado USB com layout QWERTY padrão ABNT;
- ✓ 01 (um) Mouse óptico USB;
- ✓ 02 (dois) Monitores LCD 24", resolução 1920 x 1080;
- ✓ Deve possuir as seguintes conexões *Display Port* ou HDMI e os respectivos cabos para a ligação dos dois monitores.

3.3.8. A estação de trabalho deverá vir equipada com sistema operacional e softwares necessários para a execução das operações de videomonitoramento.

- ✓ O sistema operacional e os softwares devem estar licenciados, com licenças definitivas (ou no mínimo até o fim do contrato).

#### 3.4. **LEDWALL (Detalhamento por metro quadrado):**

A solução deve ser composta por painéis individuais que uma vez unidos, formem a tela "LEDWALL" completa com a área mínima de 5 metros quadrados. O painel de LED deverá atender no mínimo os seguintes parâmetros:

- 3.4.1. O conjunto deve apresentar resolução de 1920 x 1080;
- 3.4.2. Painéis com Pitch inferior a 1,6mm;
- 3.4.3. Ângulo de visão não inferior a 140°, tanto na horizontal quanto na vertical;
- 3.4.4. Possuir mínimo de 400.000 mil pixels por m<sup>2</sup> de painel;
- 3.4.5. Reproduzir mais de 60 milhões de cores;
- 3.4.6. Brilho: O painel deverá possuir ajuste de brilho;
- 3.4.7. Temperatura de cor ajustável: 3000K - 9000k;
- 3.4.8. Razão de contraste mínimo: 4000:1;
- 3.4.9. Profundidade de processamento de escala de cinza (bit): 16 bit (ou superior);
- 3.4.10. Ser alimentado em tensões de 110 a 220V;
- 3.4.11. Possuir taxa de atualização de, no mínimo, 3.200Hz;
- 3.4.12. Possuir tempo de vida útil mínima de 70.000h de uso;
- 3.4.13. Operar em condição de temperatura e humidade de 0° a +40°C e 10-70% RH respectivamente;
- 3.4.14. Os módulos devem permitir manutenção frontal;
- 3.4.15. O sistema deverá reproduzir acima de 60000 tons de cinza;
- 3.4.16. Processador de vídeo para painel de LED com SDI ou HDMI. Alternar perfeitamente entre qualquer canal. Configurações de ajuste rápido do botão; Função de detecção de sinal; Resolução de saída máxima: 1920\*1080 @ 60hz;
- 3.4.17. A solução deve suportar trabalhar com codificação de cores RGB: 444. YUV: 444 e YUV:422.
- 3.4.18. Suportar longas distâncias sem perda de qualidade. Deve suportar resolução de até 4K, largura de banda e vídeo de 18Gbps, a solução deve suportar saída de áudio através de HDMI ou display port ou interfaces próprias de áudio;
- 3.4.19. O ledwall deve suportar a exibição simultânea de mais de uma fonte de vídeo, com múltiplas portas de saída, suportar longas distâncias sem perda de qualidade;
- 3.4.20. Cabo RJ 45 cat6: 4 Pares 24/23 AWG Condutores Isolados (em Polietileno Especial) Constituído em PVC Retardante a Chama. Blindagem - Não Blindado (U/UTP) Conector: Rj45 Blindado Diâmetro Nominal - 6.0mm- Suporte a Gigabit Ethernet;

3.4.21. Cabo HDMI 4k 2.0: Áudio 24bit, 192Khz, 8 canais LPCM Blu-Ray e HD DVD com resolução máxima CEC Controle de outros dispositivos DVD Áudio Super Áudio Deep Color até 48bit xvYYC Auto Lip-Sync Dolby True HD (Áudio 7.1);

3.4.22. Acabamento: moldura em material de alumínio, na cor preta, cobrindo todos os vãos laterais, superiores e inferiores, fechando qualquer acesso aos módulos;

3.4.23. A solução deverá suportar conexões de entrada tipo: Display Port ou HDMI ou DVI. Caso o fornecedor opte por usar soluções externas, estas deverão garantir a performance do projeto sem prejuízo técnico ao projeto, devendo o mesmo fornecer e instalar todos os equipamentos necessários para o seu perfeito funcionamento;

3.4.24. A solução deve ser fornecida com suporte de instalação em parede do próprio fabricante ou homologado por ele através de carta de comprovação do fabricante dos módulos de LED.

### 3.5. CONTROLADOR DE IMAGEM

3.5.1. Para cada conjunto de ledwall deve ser provida uma máquina decodificadora, com capacidade para decodificação de até 64 canais em FHD @ 10FPS;

3.5.2. A máquina decodificadora deve possuir ferramenta de videwall, que permita arranjar elementos de forma matricial em mosaicos definidos pelo usuário, bem como demonstrar dashboards e outras ferramentas que sejam convenientes à operação;

3.5.3. Para operação do ledwall, deve ser fornecido controlador com as seguintes características:

- ✓ entradas HDMI ou Display Port ou DVI;
- ✓ saídas para conexão de módulos ledwall;
- ✓ interface de controle RJ-45;

3.5.4. Deve suportar processamento de até 5MP;

3.5.5. Sistema de busca automática de sinal;

3.5.6. Deve permitir o gerenciamento de cenas;

3.5.7. Deve permitir o modo de display em tela dividida;

3.5.8. Deve possuir software-cliente para configurações e ajustes, com licenças definitivas.

### 3.6. GABINETES

3.6.1. O gabinete irá abrigar os equipamentos eletrônicos da solução, e deve apresentar os seguintes recursos:

3.6.2. Deverá ter capacidade para efetuar ajustes de parâmetros elétricos (desligar/religar uma tomada), e de climatização (alterar *setpoints* de temperatura, definir modos de operação, etc), garantindo uma visão holística da infraestrutura de missão crítica dentro do gabinete;

3.6.3. Capacidade para prover completa Infraestrutura com energia Ininterrupta, gerenciamento térmico (ar-condicionado, corredor frio e corredor quente internos ao gabinete, e ventiladores de emergência), gabinete, distribuição de energia, monitoramento ambiental e gerenciamento de infraestrutura em solução pré-projetada e testada em fábrica como Sistema, garantindo a compatibilidade entre todos os componentes do gabinete.

3.6.4. A solução deverá permitir instalação plug-and-play.

3.6.5. Deverá eliminar a necessidade de se construir sala especial e deverá melhorar a velocidade de implementação.

3.6.6. Dimensões e Aspectos Físicos: Altura 2000mm 42U, Largura de 800mm, Profundidade de 1200mm,

- 3.6.7. Deverá possuir Profundidade do corredor frio dentro do gabinete 200mm, Profundidade do corredor quente dentro do gabinete 200mm;
- 3.6.8. Deverá atender a Norma de Instalação de Equipamentos 19", EIA-310-D, Capacidade Estática 1000 kg, Cor RAL7021;
- 3.6.9. Portas de acesso:
- ✓ Deverá possuir Porta de vidro selado na frente
  - ✓ Deverá possuir Área de Acesso Frontal e traseira,
  - ✓ Todos os painéis/portas (laterais, frontal e traseiro) deverão ser removíveis;
- 3.6.10. Deverá possuir Gabinete Selado;
- 3.6.11. Deverá possuir Energia Ininterrupta UPS 6kVA / 6kW, Máxima Carga de TI conectada 3kW;
- 3.6.12. Deverá possuir Painel Elétrico de Distribuição (Entrada e Saída) com Quadro de 19" montado no rack do gabinete; Alimentação de Infra, refrigeração, ventiladores de emergência conectados ao UPS, Régua de Tomadas Gerenciáveis (Grandezas Elétricas por régua Monitoráveis Remotamente), console de Monitoramento Ambiental, iluminação tipo LED, display frontal, disjuntor reserva para expansão futura, bypass da UPS;
- 3.6.13. Deverá possuir Capacidade de Baterias Internas 10min @ 3kW de carga;
- 3.6.14. Deverá possuir Régua de Tomadas Inteligente com 16A, 24 tomadas monitoráveis remotamente (grandezas elétricas). Cada tomada deverá ser ligável/desligável via software remoto incorporado. Também deverão ter capacidade de serem ligadas/desligadas e monitoradas via Display local na parte frontal. Saídas: 18xC13; 06xC19.
- 3.6.15. Tensão de entrada e saída 220V FNT, Frequência de entrada e saída 60hz, Iluminação Em ambos os corredores internos (frio e quente) com tecnologia LED;
- 3.6.16. Deverá possuir DPS (Dispositivo de Proteção contra Surtos) 20kA (Nível C conforme IEEE Emerald Book);

### **Refrigeração:**

- 3.6.17. Deverá possuir Refrigeração, com capacidade de refrigeração de pelo menos 3kW, e refrigeração própria que garanta a funcionalidade dos equipamentos, com metodologia de Refrigeração expansão direta a ar;
- 3.6.18. Deverá ser instalado na parte inferior do gabinete;
- 3.6.19. Deverá possuir Sentido do Fluxo de Ar Interno Da frente (corredor frio) para traseira (corredor quente);
- 3.6.20. A Refrigeração não deverá ser alimentada pelo UPS;
- 3.6.21. Os Ventiladores de emergência para exaustão de ar quente deverá ser alimentada por UPS e gerenciável pelo sistema de monitoramento ambiental incorporado;
- 3.6.22. A tubulação entre evaporadora e condensadora deverá vir pré-configurado em fábrica para a opção de instalação de condensadora acima do Gabinete, deverá possuir Tubulação para exaustão de água de condensação;
- 3.6.23. Cabos elétricos para alimentação de Condensador deverá ser Incluso de fábrica para a opção de instalação de condensadora acima do Gabinete;
- 3.6.24. Deverá possuir Controle e Gerenciamento remotos por IP;
- 3.6.25. Deverá possuir Sensores Ambientais (Temperatura / status de porta (aberta/fechada) / detecção de líquidos), detecção de fumaça;
- 3.6.26. Deverá possuir energia e refrigeração monitoráveis, via RJ45/RS485 e slot inteligente na UPS;
- 3.6.27. Deverá possuir monitoramento de alarmes;

3.6.28. Deverá possuir Trava de Segurança na porta / controle de acesso Trava Mecânica com Chave nas portas frontal e traseira; Controle de Acesso por senha incorporado, nas portas frontal e traseira;

3.6.29. Deverá possuir Temperatura de operação aproximadamente de -5°C a +40°C.

#### **4. PLATAFORMA DE ANÁLISE DE VÍDEO**

4.1. A plataforma de análise de vídeo para 256 câmeras deve conter os seguintes itens:

- ✓ Servidores que sozinho ou em conjunto processem no máximo 256 canais de vídeo;
- ✓ Licenciados com software de VMS;
- ✓ Licenciados com sistemas operacionais específicos.

4.2. A plataforma de análise de vídeo para 64 câmeras deve conter os seguintes itens:

- ✓ Servidores que sozinho ou em conjunto processem no máximo 64 canais de vídeo;
- ✓ Licenciados com software de VMS;
- ✓ Licenciados com sistemas operacionais específicos.

#### **5. SERVIDORES**

##### **5.1. CARACTERÍSTICAS MÍNIMAS DOS SERVIDORES**

Os servidores são destinados para a plataforma de gestão, processamento e armazenamento de gravações e metadados. Devem possuir, no mínimo, as seguintes características:

5.1.1. Apenas servidores que incluam placas-mãe autênticas e oficialmente destinadas ao uso em servidores pelo fabricante serão aceitos. Placas-mãe paralelas ou de outras fontes não serão consideradas;

5.1.2. O servidor deve ser entregue com um sistema operacional próprio para servidores e compatível com todos os softwares que farão parte da plataforma. Esse sistema operacional deve ser pré-instalado, licenciado (se necessário) e configurado com todos os drivers necessários para os dispositivos especificados nesta documentação técnica;

5.1.3. O servidor deve ser equipado com duas fontes redundantes (configuração 1+1). Ambas as fontes devem ser do mesmo modelo e totalmente idênticas, incluindo potência, bem como outras características técnicas. A potência mínima requerida para cada fonte é de 750W;

5.1.4. O equipamento deve acompanhar os cabos de alimentação para cada fonte de alimentação citada;

5.1.5. Possuir Gabinete universal, de alto nível de qualidade, aplicável a gabinete tipo rack, padrão 19", (Todo e qualquer acessório necessário para fixação em rack deve ser suprido em conjunto ao servidor);

5.1.6. Serão aceitos apenas gabinetes originais fornecidos pelo fabricante do equipamento, pois eles são totalmente compatíveis com os componentes do servidor. Não serão permitidos gabinetes de terceiros ou gabinetes OEM;

5.1.7. O servidor deverá possuir pelo menos 24 núcleos de processamento e 32 threads (ou mais), para que atinja o desempenho mínimo esperado, ou qualquer outro processador que apresente ao menos 18.800 pontos desempenho, tendo como referência a base de dados Passmark CPU Mark, disponível em: [https://www.cpubenchmark.net/cpu\\_list.php](https://www.cpubenchmark.net/cpu_list.php);

5.1.8. O servidor deverá possuir placa de vídeo dedicada com capacidade de 8GB ou superior.

5.1.9. O servidor deverá possuir, pelo menos, 64 (sessenta e quatro) gigabytes de memória RAM instalada, DDR4 ou superior, com clock mínimo de 3000 Mhz;

5.1.10. Os volumes dos discos devem ser segmentados da seguinte forma:

- ✓ Volume 1 - Sistema operacional e VMS: SSD 1 TB;
- ✓ Volume 2 - Armazenamento para Gravação: com suporte a RAID 5;
- ✓ Volume 3 - Armazenamento de Metadados: com suporte a RAID 5;

5.1.11. O volume de armazenamento deve estar alocado diretamente no servidor ou ser utilizado servidor de *storage*;

5.1.12. Cada servidor deve estar equipado com um armazenamento mínimo de 16TB líquidos, com suporte a configuração RAID5, podendo serem acrescentadas unidades de armazenamento conforme necessário.

5.1.13. As baias devem ser do tipo Hot-Swap;

5.1.14. Requisitos de discos de armazenamento em Servidores:

- ✓ Deve ser de categoria Enterprise, para funcionamento em 24x7;
- ✓ Interface SATA de 6Gb/s ou superior;
- ✓ No caso de disco HDD, deve operar em velocidade de 7200 RPM ou superior;
- ✓ Cache de, pelo menos, 256MB;
- ✓ Capacidade de armazenamento de 16TB ou superior.

5.1.15. No caso de armazenamento de vídeos, snapshots, e metadados, os servidores de cada CIICC deverão ser dimensionados para suportar, no mínimo, as seguintes capacidades de armazenamento indicadas na tabela a seguir, de acordo com a região atendida. Os valores apresentados na tabela são requisitos mínimos, sendo a contratada responsável por garantir o armazenamento de todos os dados necessários pelo período de 30 dias.

Descrição	Câmeras por CIICC	Armazenamento 30 dias (TB líquidos)
CIICC GOIÂNIA	22	70
CIICC GOIÁS	43	70
CIICC FORMOSA	161	235
CIICC LUZIÂNIA	186	265
CIICC ÁG. LINDAS	152	220
<b>Total</b>	<b>564</b>	-

5.1.16. A CONTRATADA deve apresentar memória de cálculo indicando que o dimensionamento de servidores e de *storages* é suficiente para atender à demanda de armazenamento e de processamento das câmeras e dos analíticos requeridos.

5.1.17. A utilização total do processador (em todos os núcleos), nos servidores e *storages*, não devem ultrapassar o limite de 80%;

## 6. INTEGRAÇÕES

### 6.1. CAPACIDADE DE INTEGRAÇÃO COM SERVIÇOS EXTERNOS

6.1.1. A solução deverá ser possibilitar uma fácil integração com sistemas externos, utilizando as seguintes características:

6.1.2. Permitir a troca de dados utilizando APIs HTTP, possibilitando a integração de serviços web externos, abrangendo, no mínimo, os protocolos REST (Representational State Transfer);

6.1.3. Integrar-se a serviços externos da web, utilizando, no mínimo, os seguintes formatos de troca de dados: texto (.txt), JSON (JavaScript Object Notation), XML (eXtensible Markup Language) e CSV (Comma-Separated Values);

6.1.4. Utilizar recursos de integração de webhooks para viabilizar a comunicação em tempo real e a transferência de dados com sistemas ou serviços externos. Os webhooks devem constituir uma parte integral

dos recursos de integração do aplicativo, possibilitando a especificação do URL, o formato da carga útil, os métodos HTTP (por exemplo, POST, PUT) e as opções de autenticação para os webhooks de saída;

6.1.5. Permitir integração direta através de módulo integrador;

6.1.6. Permitir integração direta através de servidor de banco de dados;

6.1.7. O sistema deve incorporar mecanismos de tratamento de erros para gerenciar de maneira eficaz possíveis falhas na integração, além de fornecer notificações e registros com propósitos diagnósticos. Adicionalmente, ele deve implementar estratégias de nova tentativa para lidar com entregas de integração malsucedidas;

6.1.8. Os fornecedores devem disponibilizar documentação minuciosa abordando a configuração, a implementação e a resolução de problemas referentes à integração no aplicativo. Os detalhes sobre os recursos podem ser acessados tanto por meio da interface de usuário quanto das APIs do aplicativo;

6.1.9. Além disso, todas as informações compartilhadas com esses serviços devem ser devidamente criptografadas, utilizando o protocolo HTTPS/SSL/TLS (TLS 1.2 ou superior);

6.1.10. A integração deve ser capaz de oferecer um tempo máximo de resposta de 1 segundo e ser resiliente o suficiente para gerenciar, no mínimo, 20 solicitações simultâneas;

## 6.2. INTEGRAÇÕES COM SISTEMAS

6.2.1. O sistema deve possuir a capacidade de transmitir todos os metadados relacionados ao Analítico de Veículos para a Secretaria de Segurança Pública (SSP) de Goiás com o objetivo de armazená-los em seu próprio banco de dados;

- ✓ O sistema deve ser capaz de entregar informações para a SSPGO de acordo com o formato dos metadados indicado no Anexo deste documento.

6.2.2. O sistema deverá estar integrado (consultas) às seguintes bases de dados: DETRAN, SENATRAN, TSE, BANCO NACIONAL DE MANDADOS DE PRISÃO (BNMP) e SINESP CIDADÃO;

- ✓ A integração com esses sistemas é item essencial da aceitação das centrais de videomonitoramento, a menos que essa integração não ocorra por atrasos ou outras questões externas.

6.2.3. O sistema deve possibilitar consultas a outros VMSs de terceiros, que possuam capacidade de integração como as listadas nessa sessão.

6.2.4. Deverá ser prevista uma quantidade de horas para serviços de integração, conforme planilha de cotação.

## 6.3. VISUALIZAÇÃO DE OUTRAS CÂMERAS (de terceiros ou de outros projetos)

6.3.1. A plataforma deve garantir a interoperabilidade com dispositivos de fabricantes que estejam em conformidade com o protocolo ONVIF, possibilitando a visualização de câmeras de outros fabricantes ou sistemas;

- ✓ Para essa integração, devem ser suportados os protocolos ONVIF (Profile S, G e T) e pelo menos mais um protocolo de API aberta assim como ISAPI, VAPIX, SUNAPI, PS-API entre outros.

6.3.2. Devem ser previstas licenças para a visualização de câmeras de outros projetos, conforme planilha de cotação.

## 7. SOFTWARE DE GERENCIAMENTO DE VÍDEOS (VMS)

### 7.1. CARACTERÍSTICAS PRINCIPAIS

7.1.1. Deve permitir a integração de câmeras/canais de vídeo ao VMS ofertado;

- 7.1.2. Os *softwares* e aplicativos que constituirão a plataforma devem admitir a livre utilização de recursos de hardware padrões de mercado, de modo a não configurar vínculos de exclusividade, seguindo veementemente os padrões de arquitetura aberta.
- 7.1.3. O VMS deverá oferecer uma completa solução de vigilância de vídeo. Ela precisa ser facilmente escalável, de forma a serem adicionadas novas câmeras (individualmente ou em lote), serviços ou capacidade de armazenamento e de processamento;
- 7.1.4. Licenciamento do VMS: O licenciamento do VMS poderá ser feito para uma licença base e também para licenças de acordo com a quantidade de câmeras/canais de vídeo gerenciadas.
- 7.1.5. Licenciamento dos analíticos: Caso sejam necessárias licenças adicionais e que não estejam cobertas nos preços das câmeras, devem ser precificadas três tipos de licenças, uma para cada analítico previsto:
- ✓ Reconhecimento facial;
  - ✓ Analítico de pessoas;
  - ✓ Analítico de veículos.
- 7.1.6. O sistema deve possibilitar a análise dos seguintes itens, sem custo adicional:
- ✓ Contagem de veículos, para câmeras de LPR;
  - ✓ Estacionamento irregular (*Irregular parking*), deve ser considerado para as câmeras que não são LPR.
- 7.1.7. Caso necessite de outras licenças além das consideradas na planilha de cotação, essas deverão ser fornecidas pela CONTRATADA em quantidade suficiente para a funcionalidade do seu *software* e de acordo com a quantidade de servidores propostos, com valores diluídos nas licenças de canal de vídeo do VMS;
- 7.1.8. Deverá ser apresentado relatório do fabricante do Software de VMS comprovando que os servidores previstos são suficientes para rodar todos os analíticos previstos de maneira simultânea;
- 7.1.9. A gravação não deverá ser limitada pelo software, e sim pela capacidade de armazenamento do hardware;
- 7.1.10. O sistema deve permitir diversos tipos de gravação (contínua, por detecção de movimento, por evento);
- 7.1.11. O sistema deve permitir a criação de mosaicos individuais ou compartilhados no cliente de monitoramento com outros usuários/grupos de usuários;
- 7.1.12. O sistema deverá permitir acesso web, permitindo conexões remotas não só pelo aplicativo cliente como pelo browser e celular. O servidor web deverá permitir:
- ✓ Visualização ao vivo e pesquisa de gravações;
  - ✓ Criação e edição de mosaicos;
  - ✓ Movimentação de câmeras móveis e *fish eyes* em tempo real;
  - ✓ Exportação de vídeos e fotos;
  - ✓ Reprodução de áudio;
  - ✓ Notificação de eventos.
- 7.1.13. A plataforma deve ser compatível com os principais navegadores web do mercado (Exemplo: Mozilla Firefox, Microsoft Edge, Google Chrome ou Opera, etc);
- 7.1.14. O sistema deverá permitir conexões unicast e multicast;
- 7.1.15. O sistema deverá efetuar todos os registros do sistema (logs) em nível de auditoria, armazenando todas as ações dos usuários;
- 7.1.16. Todos os streams de vídeos fornecidos por câmeras analógicas ou câmeras IP serão codificados em formatos de compressão H.265 e/ou H.264 e suas derivações, MPEG-4, M-JPEG, e gravados simultaneamente em tempo real.
- 7.1.17. O VMS deverá servir de interface para servidores compostos por codificadores de vídeo analógicos (encoders, DVRs) e digitais, como câmeras e NVRs;

7.1.18. O VMS deverá usar dois *streams* independentes, um para visualização e outro para gravação; O VMS deverá suportar as principais marcas de câmeras IP do mercado, além de suportar as mais recentes revisões dos padrões ONVIF.

7.1.19. O VMS deverá possuir no mínimo as seguintes funções: visualização ao vivo de imagens, player de arquivos para consultar as imagens gravadas, interface de operação do sistema, ferramentas de configuração, funcionalidades de análise de vídeo, análise forense de arquivos e ferramenta de visualização de logs;

7.1.20. O VMS deve dispor de artifícios de controle e manutenção que permitam verificar a qualidade do *stream* de imagem entregue pelas câmeras ao núcleo de processamento, apresentando dados estatísticos para os canais que estiverem em conformidade com os níveis de qualidade de vídeo definidos ao sistema.

7.1.21. Em caso de perda de sinal de uma das câmeras, o VMS deverá detectar a perda de vídeo e deverá ter a possibilidade de alertar o administrador do sistema;

7.1.22. O servidor deverá receber todos os eventos no sistema e tomar as ações apropriadas baseado em relações evento/ação definidas pelo usuário. Os eventos mencionados podem corresponder à:

- ✓ Eventos de alarme;
- ✓ Eventos de gravação (erro de partição e partição restaurada);
- ✓ Eventos de câmera (iniciar/parar gravação, movimento iniciado/desligado, sinal perdido/recuperado, sensores de relés se acionada/desligada);
- ✓ Eventos de análise de vídeo, como:
- ✓ Objetos abandonados;
- ✓ Reconhecimento Facial;
- ✓ Cruzamento de limite em alguma direção;
- ✓ Contagem de pessoas;
- ✓ Detecção de aglomeração;
- ✓ Buscas múltiplas (por cor de roupa, características físicas, óculos e etc.);
- ✓ Mapa de calor;
- ✓ Medição de filas;
- ✓ Movimento na área de interesse;
- ✓ Mudança no plano de fundo da cena;
- ✓ Perda de qualidade de vídeo (perda de foco, sujeira, ofuscamento ou obscurecimento da imagem);
- ✓ Parada na área de interesse (podendo ser automóveis ou pessoas);
- ✓ Permanência na área (podendo ser automóveis ou pessoas);
- ✓ Entrada e saída na área (podendo ser automóveis ou pessoas);
- ✓ Detecção de ociosidade (*loitering*), podendo ser objetos, pessoas e automóveis;
- ✓ Análise de vídeo embarcada de câmeras IP;
- ✓ Eventos de análise de áudio (detecção de ruído, detecção de ausência total de som), com configuração do limite de áudio aceitável;

7.1.23. Caso o sistema não possua algum recurso de análise de vídeo e áudio de forma nativa, serão aceitas integrações com outros sistemas para alcançar o recurso, desde que seja comprovada a integração pelo fabricante;

7.1.24. Os eventos gerados a partir das análises poderão servir de gatilho para que sistema seja capaz de executar as seguintes ações:

- ✓ Ações de gravação (por exemplo iniciar e parar gravação);
- ✓ Ações de monitoramento (visualizar uma câmera ou mosaico);
- ✓ Ações de notificação (enviar alerta de som, enviar e-mail);
- ✓ Ações de saída de alarme (ativar ou desativar uma saída de alarme).

7.1.25. O sistema deverá suportar múltiplas conexões com servidores e gerenciá-los através de uma mesma interface, permitindo ações nos servidores que compõem o sistema, como por exemplo: configuração de câmeras, usuários, analíticos e discos de gravação;

7.1.26. O VMS deverá permitir, através de uma mesma interface, a possibilidade de integrar ilimitados sites distribuídos e operá-los como um único sistema de gerenciamento de vídeo, permitindo que configurações de câmeras, usuários, analíticos e volume de gravação que compõem todo o sistema, e consultas as listas de observações em tempo real de faces e placas veiculares cadastradas no sistema sejam sincronizadas em todos os servidores de automaticamente;

7.1.27. O VMS deverá possuir a funcionalidade de armazenamento de streams de vídeo e áudio baseado em eventos disparadores como:

- ✓ Detecção de movimento;
- ✓ Reconhecimento Facial;
- ✓ Ativação de entrada digital;
- ✓ Eventos de análise de vídeo.

7.1.28. O VMS deverá autenticar usuários e dar acesso ao sistema baseado em direitos de acesso predefinidos; através de credenciais de acesso criadas antecipadamente por um usuário administrador ou com privilégios para tal. Cada usuário terá o acesso aos recursos, canais e funções mediante seus privilégios de acesso;

7.1.29. Após tentativas de acesso com senha incorreta, a plataforma deverá bloquear o acesso do usuário por um tempo pré-definido. As quantidades de tentativas e tempo de bloqueio devem configuradas pelos administradores do sistema;

7.1.30. Deverá permitir ao administrador ou aos usuários com direito de acesso a mudar a configuração do sistema. A administração deverá ser descentralizada do sistema de qualquer lugar na rede, permitindo buscar todos os dispositivos e servidores compatíveis na rede;

7.1.31. O VMS deverá permitir múltiplos agendamentos de gravação sendo designados a uma única câmera. Cada agendamento deverá permitir configurações de modo de gravação (contínuo, por evento), configuração de hora e data (diário, semanal, contínuo);

7.1.32. O VMS deverá suportar gestão avançada de alarme, como por exemplo, permitir que um determinado grupo de usuário possa programar alarmes e visualizar histórico de eventos e que possa inserir comentários sobre o evento no tratamento e classificação de um alarme.

7.1.33. O sistema deverá ser capaz de gerenciar os vídeos armazenados em cartões de memória instalados nas câmeras (edge storage);

7.1.34. O sistema deverá permitir a replicação de dados entre discos, a qual deverá ser iniciada de forma automática ou manual;

7.1.35. Os usuários administradores deverão ter a possibilidade de criar diversos discos no sistema, atribuindo câmeras específicas para determinados discos e com diferentes parâmetros de gravação, sem afetar a performance do sistema, eficiência de gravação e a funcionalidade geral das câmeras;

7.1.36. Os mosaicos de câmera deverão estar disponíveis a todos os usuários no VMS, desde que, sejam compartilhados com outros grupos de usuário;

7.1.37. Deverá ter a capacidade de definir acesso e direitos por grupo de usuários, bem como limitar acessos a determinados grupos de usuário no acesso web;

7.1.38. Deverá suportar funcionalidades “wizards” para descobrimento automático de dispositivos IP (câmeras e codificadores) dentro da rede e a possibilidade de adicioná-los automaticamente à configuração de qualquer servidor dentro de um grupo de servidores;

7.1.39. Possuir a capacidade de estabelecer o modo de gravação para cada câmera baseado em detecção de movimento, entrada de alarme, eventos de análise de vídeo, agendado ou continuamente;

7.1.40. Possibilitar a criação de uma lista complexa de ações que poderão ser ativadas em eventualidades. Os administradores podem escolher ações específicas de uma variedade de comandos comuns e complexos:

- ✓ Gravar câmera visualizada com áudio (caso a câmera possua o recurso);
- ✓ Enviar alerta sonoro;
- ✓ Enviar e-mail para um ou mais endereços pré-configurados;
- ✓ Enviar um sinal para acionar um relé de um dispositivo;
- ✓ Abrir mosaicos para câmera específica ou qualquer outro mosaico pré-configurado;
- ✓ Ativar um alarme;
- ✓ Armar/desarmar uma câmera de vídeo;
- ✓ Executar aplicações externas;
- ✓ Exportar automaticamente snapshots ou vídeos;
- ✓ Enviar consultas HTTP/HTTPS do tipo GET ou POST para um servidor específico através da API.

7.1.41. Deverá suportar criação de inúmeros agendamentos de gravação e designação de qualquer câmera a qualquer agendamento;

7.1.42. Usuários deverão ter a possibilidade de configurar diferentes tipos de análise de vídeo com a possibilidade de calibrar cada característica de análise de vídeo dependendo de tamanho do objeto, velocidade do movimento e/ou contraste com o plano de fundo;

7.1.43. O sistema dever ter a possibilidade de criar grupos de câmeras definidos pelo usuário. Os grupos de câmera deverão ser disponibilizados na interface de visualização para facilitar navegação por diferentes mosaicos de grupos de câmeras combinadas;

7.1.44. Deverá possibilitar monitoramento ao vivo de vários streams de vídeo simultaneamente no mesmo monitor, ou em um computador que suporte múltiplos monitores;

7.1.45. Deverá mostrar todas as câmeras e grupos de câmeras conectadas ao sistema;

7.1.46. Deverá possibilitar aos operadores controlar (Pausar/Play, avançar, voltar) grupos de câmeras sem afetar a possibilidade de outros operadores de ver e controlar a mesma sequência;

7.1.47. Deverá suportar a funcionalidade de Mapeamento, onde mapas digitais ou plantas baixas são usadas para representar a localização física de câmeras e outros dispositivos do sistema de vigilância;

- ✓ Mapas terão a possibilidade de conter hyperlinks com o objetivo de criar uma hierarquia de mapas interligados;
- ✓ A funcionalidade de mapeamento deverá ter a possibilidade de importar mapas de qualquer software gráfico que suporte pelo menos os formatos de imagem BMP, JPEG e/ou GIF;
- ✓ O sistema deverá ter todas as câmeras georreferenciadas, seja através de informações de localização (coordenadas) na câmera, ou de cadastro da localização de cada câmera no VMS;
- ✓ O sistema deverá permitir ao operador visualizar uma câmera ao vivo através do mapa, e a interface do mapa deverá prover informação sobre o status de certos objetos (alarmes, ativados por detectores) e visualizará área de visão da câmera no mapa;
- ✓ O sistema deve permitir a definição de eventos que gerem alarmes a partir da identificação dos atributos de veículo de interesse. Quando o evento for gerado, o sistema deve referenciar no mapa o dispositivo de captura que originou o alarme, permitindo identificar o local onde o evento ocorreu;
- ✓ O sistema deverá permitir que usuário realize seleções a partir de um mapa, permitindo identificar com maior precisão os locais por onde o veículo transitou e exibindo graficamente o trajeto realizado por ele.

7.1.48. O VMS deverá trabalhar com mapas online, para que seja possível identificar o posicionamento das câmeras em diversos pontos separados geograficamente. Para que esta função seja incorporada será necessário o licenciamento correspondente ao projeto com o desenvolvedor da plataforma de mapas online;

7.1.49. Deverá permitir o Monitoramento de Eventos em tempo real, com a possibilidade de configurar filtros de eventos específicos para cada exibição;

7.1.50. Deverá monitorar em tempo real as condições de cada servidor do sistema, indicando a utilização de disco, carga de CPU, falha de câmeras, de forma que o operador possa tomar alguma ação em caso de falhas;

7.1.51. Deverá suportar zoom digital no stream de vídeo ao vivo e gravado. O zoom digital para câmeras fixas deverá possibilitar ao operador designar área de interesse na visão da câmera e o VMS irá automaticamente dar zoom na área designada;

7.1.52. Deverá permitir comunicação de áudio com a unidade de gravação. O áudio será arquivado na mesma base de dados que o vídeo;

7.1.53. Deverá fornecer ao operador informações sobre o alarme ativado, com a possibilidade de entrar no gerenciamento deste alarme clicando na janela de preview do alarme;

7.1.54. Usuários deverão ser capazes de tirar snapshots tanto de vídeos ao vivo como gravados;

7.1.55. O sistema deverá possuir a capacidade reprodução de arquivos de áudio e vídeo gravados, suportar a reprodução de qualquer intervalo de tempo e possibilitar ao operador selecionar reprodução sincronizada de todos os streams de vídeo;

7.1.56. Deverá possibilitar ao operador controlar reprodução com pause, avanço e retrocesso de reprodução, avançar e voltar lentamente quadro a quadro;

7.1.57. O operador deverá ter a possibilidade de escolher quais marcadores devem ser mostrados na linha do tempo com o uso de filtros, como por exemplo:

- ✓ Todos os eventos;
- ✓ Tipos de alarmes;
- ✓ Alarmes não classificados;
- ✓ Fonte de alarme;
- ✓ Eventos comentados.

7.1.58. Deverá prover exportação de imagem estática para os formatos JPEG e PDF com hora e data estampadas na imagem;

7.1.59. Deverá prover ferramentas para exportar sequências de vídeo em formatos padrões como EXE, AVI, MP4 ou MKV;

7.1.60. O sistema deverá possibilitar ao operador exportar gravações de vídeo através de arquivos compactados e criptografados com senha;

7.1.61. Deverá possibilitar que os usuários visualizem as imagens utilizando a função dewarp (modo imersivo) em vídeos exportados provenientes de câmeras com lente do tipo *fish eye* (olho de peixe);

7.1.62. O sistema deverá permitir ferramenta de busca do tipo análise forense que permita ao operador realizar a procura por um determinado acontecimento com base em filtros sem a necessidade de pré-configurar as características de análise de vídeo da(s) câmera(s). Esta análise poderá ser feita em qualquer câmera no sistema configurada com esta análise, minimamente, com as seguintes opções de filtros primários:

- ✓ Movimento na área de interesse;
- ✓ Cruzamento de limite em alguma direção;
- ✓ Múltiplos objetos movimentando-se simultaneamente na mesma área;
- ✓ Permanência na área;
- ✓ Passagem de uma área para a outra.

7.1.63. Ainda sobre a ferramenta de busca, a partir de uma busca iniciada pelos filtros primários citados acima, deverá ser possível suplementar a busca com o uso de filtros secundários como por exemplo:

- ✓ Direção de Movimento;
- ✓ Detecção de aglomeração;
- ✓ Contagem de pessoas;

- ✓ Busca múltipla (características físicas, cor de roupa, etc.);
- ✓ Realizar buscas a partir de upload de fotos;
- ✓ Cor do objeto;
- ✓ Tipo do objeto;
- ✓ Entrada e saída na área de interesse.

7.1.64. O sistema deverá permitir ferramentas de inteligência artificial para detectar apenas humanos, ignorando todo falso alarme que possa ocorrer com outros objetos (ex: galhos de árvores, veículos, animais etc.). Caso não exista de forma nativa, serão aceitos softwares de terceiros desde que estejam completamente integrados ao sistema;

7.1.65. O sistema deve permitir ferramentas de inteligência artificial para detectar pessoas em posição de uso de armas de fogo e/ou rendidas na cena, alertando de forma proativa potenciais situações de risco. Caso o software não possua o recurso de forma nativa, serão aceitas integrações com outros sistemas para alcançar o recurso desde que seja comprovada a integração pelo fabricante;

## 7.2. RECONHECIMENTO FACIAL

7.2.1. O sistema deve admitir a criação de múltiplos bancos de face, para comparação e consequente reconhecimento facial;

7.2.2. O sistema de reconhecimento facial deve capturar e registrar no banco de dados as faces de todas as pessoas que passarem nos ambientes monitorados.

7.2.3. Para consulta no banco de dados, o operador deve ter a possibilidade de inserir uma foto para pesquisa no banco de dados, e verificar se uma determinada pessoa esteve presente no local, consultando todo o histórico de imagens armazenados nos servidores.

7.2.4. O sistema deve permitir a definição do nível de similaridade utilizado na comparação entre a foto inserida no banco de dados e o registro de imagens capturadas pelas câmeras;

7.2.5. Caso o software não possua o recurso de forma nativa, serão aceitas integrações com outros sistemas para alcançar o recurso desde que seja comprovada a integração pelo fabricante;

7.2.6. O software deve possuir ferramenta de reconhecimento facial para alertas em tempo real (configuráveis pelo Administrador do sistema) caso uma pessoa cadastrada como suspeita seja reconhecida. Caso o software não possua o recurso de forma nativa, serão aceitas integrações com outros sistemas para alcançar o recurso desde que seja comprovada a integração pelo fabricante;

7.2.7. O sistema deve permitir que as capturas de face e alertas/eventos sejam representadas em mapa eletrônico, indicando a localização do dispositivo que capturou a imagem, permitindo identificar o local onde indivíduo esteve e, possivelmente, o trajeto realizado;

7.2.8. O sistema deve permitir a configuração da área de atuação da captura dos rostos e ajuste de sensibilidade.

7.2.9. Deve ser possível pesquisar por um rosto em mais de um CIICC simultaneamente;

## 7.3. ANALÍTICO DE VEÍCULOS

7.3.1. O sistema deve receber e registrar no banco de dados a placa de todos os veículos que passarem nos ambientes monitorados. O operador deve ter a possibilidade de consultar as placas de veículos no banco de dados, seja inserindo toda a numeração ou parte dela.

- ✓ Caso o sistema não possua o recurso de forma nativa, serão aceitas integrações com outros sistemas para alcançar o recurso desde que seja comprovada a integração pelo fabricante;

7.3.2. Deve permitir integração com as câmeras de LPR fornecidas, permitindo a busca de metadados veiculares, como cor, tipo e placa, com comprovação atestada através de carta do fabricante tanto do VMS quanto das câmeras, atestando a possibilidade de integração até a data de operacionalização dos equipamentos.

7.3.3. O sistema de leitura de placas deverá também possuir ferramenta para alertas em tempo real (configuráveis pelo administrador do sistema) caso uma placa cadastrada como suspeita seja reconhecida.

- ✓ Caso o software não possua o recurso de forma nativa, serão aceitas integrações com outros sistemas para alcançar o recurso desde que seja comprovada a integração pelo fabricante;

7.3.4. Deve ser possível pesquisar por uma placa em mais de uma câmera simultaneamente;

7.3.5. O sistema deve permitir a leitura parcial de placas e a realização de buscas por similaridade e com uma combinação de outros atributos do veículo.

## 7.4. ANALÍTICO DE PESSOAS

7.4.1. Contagem de Pessoas e Aglomeração

- ✓ O sistema deve permitir a contagem de pessoas em zonas determinadas na cena;
- ✓ O sistema deve permitir a configuração da zona, como demarcação, quantidade de pessoas permitidas e somatório de pessoas do local.
- ✓ Em caso de violação de uma regra, o sistema deve ser capaz de emitir alertas;
- ✓ Os alertas devem ficar marcados na linha temporal ou em log, permitindo que o evento seja rastreado na busca.

7.4.2. O sistema deve permitir o rastreamento de pessoas baseado em suas características físicas.

7.4.3. Serão aceitos metadados corporais, como cor e tipo de roupa, uso de óculos, barba e bigode; também serão aceitas soluções que permitam a busca por similaridade, de modo que a partir de uma imagem, o sistema consiga encontrar pessoas com características similares de vestimenta e postura, por exemplo, chegando ao mesmo resultado.

## 8. SEGURANÇA

8.1. SOLUÇÃO DE SEGURANÇA CIBERNÉTICA

8.1.1. A solução deve consistir em sistema de proteção de rede baseada em appliance físico, não sendo permitido appliances virtuais ou solução open source (produto montado);

8.1.2. A CONTRATADA deverá dimensionar as características de throughput e de quantidades de sessões necessárias para o atendimento à cada central de monitoramento;

8.1.3. Possuir hardware de alta capacidade, permitindo capacidades em alta escalabilidade, e ser otimizada para análise de conteúdo de aplicações em camada 7;

8.1.4. O gerenciamento da solução deve suportar acesso via SSH, cliente ou WEB (HTTPS) e API aberta;

8.1.5. Os dispositivos de proteção de rede devem possuir suporte a roteamento multicast (PIM-SM e PIM-DM);

8.1.6. Deve suportar BGP, OSPF, RIP e roteamento estático;

8.1.7. Os dispositivos de proteção de rede devem possuir suporte a DHCP Relay e DHCP Server;

8.1.8. Deve suportar ao menos 30 tabelas independentes de roteamento, por contexto de firewall;

- 8.1.9. Deve suportar NAT dinâmico (Many-to-Many), NAT estático (1-to-1), NAT estático bidirecional 1-to-1, Tradução de porta (PAT), NAT de Origem e NAT de Destino simultaneamente;
- 8.1.10. Deve implementar Network Prefix Translation (NPTv6) ou NAT66, prevenindo problemas de roteamento assimétrico;
- 8.1.11. Deve suportar NAT64;
- 8.1.12. Deve permitir monitorar via SNMP o uso de CPU, memória, espaço em disco, VPN, situação do cluster e violações de segurança;
- 8.1.13. Proteção anti-spoofing;
- 8.1.14. Deve suportar Modo Camada – 3 (L3), para inspeção de dados em linha e visibilidade do tráfego;
- 8.1.15. Não serão aceitas soluções baseadas em PCs de uso geral.
- 8.1.16. A solução de firewall deve possuir conectores nativos para integração com nuvens privadas, pelo menos: VMware ESXI, Cisco ACI e Kubernetes;
- 8.1.17. Deve suportar a execução de scripts, envio de e-mails, e APIs mediante hosts comprometidos, agendamentos, mudanças de configuração e ocorrência de eventos de rede e segurança pré-definidos;
- 8.1.18. Controle de políticas por usuários, grupos de usuários, IPs, redes e zonas de segurança;
- 8.1.19. Controle, inspeção e descryptografia de SSL por política para tráfego de saída (Outbound);
- 8.1.20. Deve descryptografar tráfego outbound em conexões negociadas com TLS 1.2 ou superior;
- 8.1.21. Deve permitir o bloqueio de arquivo por sua extensão e possibilitar a correta identificação do arquivo por seu tipo mesmo quando sua extensão for renomeada.

## 8.2. PREVENÇÃO DE AMEAÇAS

- 8.2.1. Para proteção do ambiente contra-ataques, os dispositivos de proteção devem possuir módulo de IPS, Antivírus e Anti-Spyware;
- 8.2.2. Deve incluir assinaturas de bloqueio de arquivos maliciosos (Antivírus e Anti-Spyware);
- 8.2.3. Deve ser possível a criação de políticas por usuários, grupos de usuários, IPs, redes ou zonas de segurança;
- 8.2.4. Detectar e bloquear a origem de portscans;
- 8.2.5. Bloquear ataques efetuados por worms conhecidos;
- 8.2.6. Permitir o bloqueio de vírus e spywares em, pelo menos, os seguintes protocolos: HTTP, FTP, SMB, SMTP e POP3;
- 8.2.7. Identificar e bloquear comunicação com botnets;
- 8.2.8. Registrar na console de monitoração as seguintes informações sobre ameaças identificadas: o nome da assinatura ou do ataque, aplicação, usuário, origem e o destino da comunicação, além da ação tomada pelo dispositivo;
- 8.2.9. Os eventos devem identificar o país de onde partiu a ameaça;
- 8.2.10. Deve incluir proteção contra vírus em conteúdo HTML e javascript, software espião (spyware) e worms;
- 8.2.11. Possuir proteção contra downloads involuntários usando HTTP de arquivos executáveis e maliciosos;
- 8.2.12. A solução deve analisar o comportamento de arquivos suspeitos em um ambiente controlado;

## 9. ADMINISTRAÇÃO DO SISTEMA, SUPORTE TÉCNICO E MANUTENÇÃO

9.1. Tendo em vista se tratar de uma contratação de prestação de serviço, conforme definido no OBJETO, toda e qualquer reposição e manutenção de equipamentos ficará a cargo da CONTRATADA. Esta será obrigada a realizar a manutenção e substituição de todos itens e componentes utilizados na execução contratual, como câmeras, *switch*, poste, estação de trabalho, etc, sempre que necessário, independente da causa (problemas elétricos, infraestrutura, roubo, furto, vandalismo, causas naturais (raios/enchentes), etc). Levando em consideração essa necessidade e os serviços que serão suportados pela CONTRATADA, estes devem estar inclusos no preço formulado.

9.2. A CONTRATADA deverá disponibilizar SERVIÇO DE ATENDIMENTO composto por equipe com conhecimentos sólidos no funcionamento e operação dos serviços;

9.3. Os serviços de “manutenção” incluirão:

9.3.1. Solução de falhas ou defeitos no funcionamento, incluindo a instalação de arquivos para correção dos erros;

9.3.2. Esclarecimento de dúvidas sobre o funcionamento e operação da solução;

9.3.3. Instalação de novas versões ou atualizações e patches de todos os equipamentos fornecidos;

9.4. Patches de segurança deverão ser instalados em até 30 dias após a disponibilização pelo fabricante.

9.5. A CONTRATADA deve disponibilizar o SERVIÇO DE ATENDIMENTO 8X7 (oito horas por dia, sete dias da semana, de domingo a domingo) e equipe com conhecimentos sólidos no funcionamento e operação da solução de gestão;

9.6. A manutenção técnica corretiva será realizada sempre que solicitada pelo CONTRATANTE por meio da abertura de chamado técnico diretamente à empresa CONTRATADA;

9.7. A manutenção técnica corretiva deverá ser realizada, também, quando alguma falha ou mau funcionamento forem detectados pela CONTRATADA, sem a obrigatoriedade de abertura de chamado por parte da CONTRATANTE em situações como esta;

9.8. As aberturas dos chamados podem ser por telefone (com número do tipo "0800" ou DDD 62), por e-mail (disponibilizado e-mail oficial da CONTRATADA) ou plataforma oficial de aberturas de chamados;

9.9. No atendimento aos chamados técnicos abertos deverá ser disponibilizado suporte personalizado por um analista designado;

9.10. Um chamado técnico somente poderá ser fechado após a confirmação do responsável do CONTRATANTE e o término de atendimento dar-se-á com a disponibilidade do recurso para uso em perfeitas condições de funcionamento;

9.11. A abertura do chamado começará a contar a partir do momento em que for detectado a falha no sistema ou quando houver o contato via telefone/e-mail/plataforma;

9.12. A severidade de atendimento aos chamados será definida conforme avaliação do problema frente a TABELA DE ATENDIMENTO DE CHAMADO:

TABELA DE ATENDIMENTO DE CHAMADO			
SEVERIDADE	TEMPO MÁXIMO PARA SOLUÇÃO	CIICC	CÂMERA
Crítica	90% das ocorrências em até 6h e 100% das ocorrências em até 9h	Se aplica aos produtos que sua inoperância comprometa toda a solução - conexão, Firewall, Plataformas de Gerenciamento, Gravação de Vídeo.	Não se aplica
Média	90% das ocorrências em até 12h e 100% das ocorrências em até 18h	Se aplica a conectividade de dispositivos de codificação e aos produtos que estejam apenas parcialmente inoperantes ou que sua inoperância não comprometa toda a solução.	Unidade
Baixa	90% das ocorrências em até 48h e 100% das ocorrências em até 96h	Se aplica aos casos de consulta técnica para dúvidas em geral, tais como: configuração de analíticos, operação do sistema "cliente", configuração de eventos, monitoramento e outros cuja relevância não afeta o funcionamento do sistema como um todo.	Unidade

9.12.1. **Severidade Crítica:** Se aplica aos produtos que sua inoperância comprometa toda a solução - Firewall, Plataformas de Gerenciamento, Gravação de Vídeo;

9.12.2. **Severidade Média:** Se aplica a conectividade de dispositivos de codificação e aos produtos que estejam apenas parcialmente inoperantes ou que sua inoperância não comprometa toda a solução;

9.12.3. **Severidade Baixa:** Se aplica aos casos de consulta técnica para dúvidas em geral, tais como: configuração de analíticos, operação do sistema "cliente", configuração de eventos, monitoramento e outros cuja relevância não afeta o funcionamento do sistema como um todo;

Na abertura de chamados técnicos, serão fornecidas informações, como anormalidade observada, nome do responsável pela solicitação do serviço e severidade do chamado;

#### 9.13. Chamados relativos ao Firewall:

9.13.1. Para o ideal monitoramento do sistema de segurança, a CONTRATADA deverá apresentar quinzenalmente relatório com os seguintes itens:

- ✓ Análise do sistema e mapeamento de vulnerabilidades, com suas medidas corretivas;
- ✓ Inclusão dos incidentes ocorridos e suas correções, além das vulnerabilidades identificadas com suas soluções.

9.13.2. Incidentes resolvidos fora do prazo e vulnerabilidades sem soluções identificadas serão considerados como incidentes de severidade crítica e sofrerão a respectiva glosa.

9.14. Todas as solicitações feitas pelo CONTRATANTE deverão ser registradas pela CONTRATADA para acompanhamento e controle da execução dos serviços e ainda:

9.14.1. A CONTRATADA, após a realização dos serviços de manutenção corretiva, deverá apresentar um Relatório de Visita, contendo identificação do chamado, data e hora de abertura do chamado, data e hora do início e término do atendimento, identificação do defeito, técnico responsável pela solução, às providências adotadas e outras informações pertinentes. Este relatório deverá ser homologado pelo gestor do contrato;

9.14.2. O tempo do início efetivo de atendimento ao chamado técnico deverá ser de acordo com a Tabela de Atendimento de Chamado, abaixo, contado a partir da abertura do mesmo;

9.14.3. Após o início do atendimento, o tempo de solução do problema deverá ser de acordo com a Tabela de Atendimento de Chamado, abaixo, não devendo ultrapassar os prazos estabelecidos para as respectivas severidades.

## 9.15. INDICADORES

9.15.1. O indicador deverá, portanto, avaliar mensalmente se os chamados abertos tiveram o seu “TEMPO MÁXIMO PARA SOLUÇÃO” cumpridos conforme percentuais de atingimento indicados na Tabela de Atendimento de Chamado. Dessa forma, o indicador mensura a quantidade de solicitações que foram atendidas dentro do prazo e do período de medição (30 dias) separadamente por suas severidades. Para cada severidade deverão ser avaliados os indicadores de 90% e no de 100%, ou seja, para cada severidade serão 2 indicadores a serem avaliados.

9.15.2. NOTA: Paradas programadas, comunicadas e acordadas com antecedência mínima de 10 (dez) dias corridos, não serão contabilizadas na avaliação dos indicadores de desempenho;

## 9.16. SUPORTE À ADMINISTRAÇÃO DO SISTEMA

### 9.16.1. Relatórios do Projeto

- ✓ Relatórios semanais de acompanhamento (status geral, gantt, atividades da semana);
- ✓ Relatórios financeiros mensais;
- ✓ Relatórios mensais de suporte (quantidade de atendimentos, tempo de cada atendimento, etc);
- ✓ Relatórios sobre os eventos gerados pelo sistema (como quantidade de veículos, faces detectadas, e demais eventos gerados pelos analíticos).

### 9.16.2. Gestão da base de dados

- ✓ Relatórios mensais de utilização, integridade e desempenho das bases de dados (BD);
- ✓ Planejamento da BD: avaliação da capacidade de armazenamento necessária com base na quantidade de câmeras, qualidade de vídeo e retenção de dados desejada;
- ✓ Gestão de backups de configuração do sistema;
- ✓ Gerenciamento de Retenção: verificação e ajustes nas políticas de retenção de dados;
- ✓ Segurança dos Dados: configuração de medidas de segurança para proteger os dados contra acesso não autorizado, a nível de BD;
- ✓ Monitoramento de Desempenho da BD, incluindo a verificação do espaço em disco, da integridade dos arquivos e da capacidade de processamento;
- ✓ Manutenção Preventiva de hardware e software para garantir que o sistema esteja sempre funcionando de forma otimizada.

### 9.16.3. Revisões trimestrais de:

- ✓ Revisão da lista de usuários;
- ✓ Revisão de regras de firewall;
- ✓ Relatório de patches instalados e disponibilizados pelos fabricantes (câmeras, servidores, storage, softwares, firewall);
- ✓ Inventários (de equipamentos, de software, de câmeras, etc);

### 9.16.4. Controle de acesso: criação / bloqueio de usuários;

### 9.16.5. Controle de mudanças.

## **10. TREINAMENTOS**

### **10.1. TREINAMENTO E OPERAÇÃO ASSISTIDA DA SOLUÇÃO DE VIDEOMONITORAMENTO**

10.1.1. Depois de implantado cada CIICC a solução, e com pelo menos 10 câmeras em operação em cada CIICC, a CONTRATADA deverá ministrar o treinamento e repasse de conhecimento de todos os equipamentos e softwares envolvidos na solução. O treinamento deverá ser planejado pela CONTRATADA e levado à aprovação da CONTRATANTE.

10.1.2. O treinamento deverá contemplar a operação do hardware fornecido, bem como abranger toda a solução de software ofertada (câmeras, softwares analíticos, servidores, controladora do ledwall), preferencialmente ministrado, no caso dos softwares, por instrutor com certificação válida do fabricante;

10.1.3. A carga horária do treinamento não deve ultrapassar 8h por dia;

10.1.4. O treinamento deve ter duração máxima de 40 horas, sendo 24 horas de treinamento teórico e 16 horas de operação assistida;

10.1.5. Os serviços de operação assistida deverão ser realizados nas dependências dos CIICCs;

10.1.6. A operação assistida deverá ser iniciada após a conclusão dos procedimentos de configuração completa do sistema, de modo a não haver concomitância de períodos ou conflito entre os prazos necessários para configuração e os prazos para a operação assistida;

10.1.7. Caso o período de operação assistida não transcorrer conforme o esperado, com o sistema apresentando graves falhas de desempenho, a fiscalização poderá interrompê-lo, exigindo a solução destas falhas antes da retomada ou reinício do prazo estipulado para esta atividade;

10.1.8. O treinamento deve contemplar até 10 alunos, por turma, selecionados pela CONTRATANTE;

10.1.9. Os treinamentos serão realizados em estrutura da contratante, porém, quaisquer custos com instrutores, refeições, equipamentos e outros necessários à perfeita execução do treinamento são de responsabilidade da CONTRATADA;

10.1.10. O treinamento deve ser presencial, em Goiânia ou no Entorno, com todas as despesas de transporte e estadia dos instrutores custeadas pela CONTRATADA;

10.1.11. O material didático utilizado no treinamento deve ser fornecido de forma individual e deverá ser preferencialmente impresso, salvo em caso de impossibilidade devidamente justificada e aceita pela CONTRATANTE;

10.1.12. O material didático utilizado no treinamento deve ser o material oficial do fabricante dos equipamentos/solução;

10.1.13. Ao final do treinamento, em um prazo máximo de até 07 (sete) dias úteis, a CONTRATADA deverá emitir certificado de participação para os participantes que concluírem no mínimo 70% da carga horária ministrada.

### **10.2. TREINAMENTO DO SISTEMA DE SEGURANÇA**

10.2.1. A CONTRATADA deverá ministrar os treinamentos e repasse de conhecimento acerca das soluções adquiridas e implementadas com, no mínimo, as seguintes características:

10.2.2. Deve ser prevista uma turma com até 10 participantes e carga horária total de 16h;

10.2.3. Os treinamentos deverão ser ministrados em Goiânia, por profissionais capacitados e certificados pela fabricante dos equipamentos envolvidos;

10.2.4. Os treinamentos deverão ser realizados através de materiais / manuais oficiais do fabricante ou apostilas técnicas desenvolvidas pela CONTRATADA.

## 11. PADRÃO DE ENVIO DE METADADOS PARA A SSP

Os metadados das câmeras de videomonitoramento devem ser enviados para a SSPGO:

Serviço que recebe os sinais de passagem de veículos no padrão RESTFull em protocolo HTTPS;

Enviado em um arquivo texto em multipart/form-data, contendo o JSON dos sinais, tamanho máximo de 100MB;

Arquivo a ser enviado deve conter os parâmetros abaixo:

```
[
  {
    {
      "placa": "XXX9999",
      "dataHoraTz": "2020-03-02T13:16:04-03:00",
      "empresa": "XXX", "YYY", "...",
      "camera": {
        "numero": "numeração do equipamento",
        "latitude": "-18.167009903836323",
        "longitude": "-47.93628019466483",
        "endereco": "endereço do equipamento"
      },
      "tipoVeiculo": "tipo do veículo",
      "marca": "marca do veículo",
      "cor": "cor do veículo",
      "imagem": {
        "imgVeiculo": "imagem em Base64"
      }
    }
  }
  ...
]
```