

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

## SUMÁRIO

1.	<b>DESCRIÇÃO DO SISTEMA .....</b>	<b>3</b>
2.	<b>PONTOS DE VIDEOMONITORAMENTO .....</b>	<b>5</b>
2.3.	<b>Item 1: CÂMERA TIPO I - 110km/h .....</b>	<b>8</b>
2.4.	<b>Item 2: CÂMERA TIPO II – 180km/h.....</b>	<b>9</b>
2.5.	<b>Item 3: CÂMERA TIPO III – ANALÍTICO DE PESSOAS .....</b>	<b>10</b>
2.6.	<b>Item 4: INFRAESTRUTURA DOS PONTOS DE VIDEOMONITORAMENTO.....</b>	<b>11</b>
3.	<b>CIICCs (Centro Integrado de Inteligência, Comando e Controle) .....</b>	<b>13</b>
3.1.	<b>Item 10. CIICC – REGIONAL .....</b>	<b>13</b>
3.2.	<b>Item 11. CIICC - PRINCIPAL.....</b>	<b>13</b>
4.	<b>PLATAFORMA DE ANÁLISE DE VÍDEO .....</b>	<b>15</b>
4.1.	<b>Item 8. PLATAFORMA DE ANÁLISE DE VÍDEO.....</b>	<b>15</b>
4.3.2.	<b>Item 5. LICENÇA PARA ANALÍTICO DE RECONHECIMENTO FACIAL .....</b>	<b>22</b>
4.4.	<b>Item 7. INTEGRAÇÃO COM OUTROS SISTEMAS.....</b>	<b>23</b>
4.4.3.	<b>Item 6. LICENÇA PARA VISUALIZAÇÃO DE CÂMERAS DE OUTROS SISTEMAS .....</b>	<b>24</b>
5.	<b>ADMINISTRAÇÃO DO SISTEMA, SUPORTE TÉCNICO E MANUTENÇÃO .....</b>	<b>27</b>
5.19.	<b>Item 12. ADMINISTRAÇÃO DO SISTEMA.....</b>	<b>30</b>
6.	<b>TREINAMENTOS .....</b>	<b>31</b>
6.1.	<b>Item 9. TREINAMENTO DA SOLUÇÃO DE VIDEOMONITORAMENTO .....</b>	<b>31</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*).
- 1.2.** **Distribuição dos CIICCS:** A imagem abaixo apresenta a distribuição dos municípios por Centro Integrado de Inteligência, Comando e Controle (CIICC). Esta figura também detalha a quantidade de câmeras alocadas para cada CIICC, proporcionando uma visão clara e precisa da cobertura de videomonitoramento em cada região.

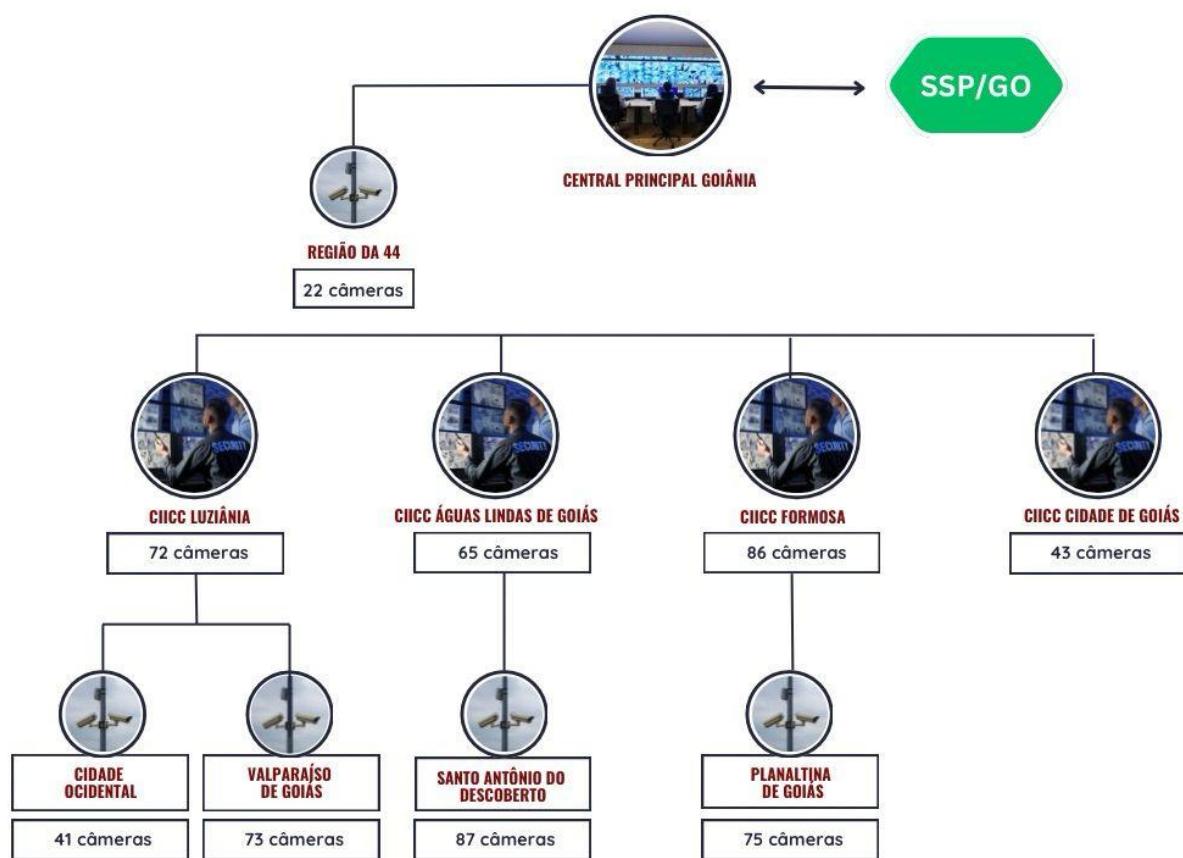


Figura 1: Distribuição dos CIICCs e seus respectivos municípios

- 1.3.** **Arquitetura do sistema de análise de vídeo:** o sistema poderá ser hospedado em nuvem privada ou pública. Os requisitos mínimos de qualidade de infraestrutura e serviço estão descritos no item **4.2. DATACENTER**.
- 1.3.1.** A CONTRATADA deve garantir que a solução em nuvem escolhida atenda integralmente aos requisitos de desempenho descritos neste caderno, bem como os requisitos de segurança e conformidade com a Lei n.º 13.709, de 14 de agosto de 2018 (Lei Geral de Proteção de Dados Pessoais), especialmente no que tange ao armazenamento e ao tratamento de dados;

- 1.3.2. A CONTRATADA deverá assegurar que todos os centros de monitoramento recebam as imagens e os analíticos sem interrupções, com baixa latência, e de acordo com os parâmetros técnicos estabelecidos neste caderno;
- 1.3.3. Todo o armazenamento e tratamento dos dados deve ocorrer em território nacional.

#### 1.4. Disposições gerais

- 1.4.1. Todos os equipamentos fornecidos devem ser novos e sem histórico de uso anterior, não sendo aceitáveis equipamentos de origem reaproveitada ou recondicionada (*refurbished*);
- 1.4.2. A conectividade/*link* dos equipamentos até a plataforma e da plataforma até os CIICCs será de responsabilidade da CONTRATADA. Não será permitida a utilização de redes móveis (4G/LTE e demais redes de dados móveis).
- 1.4.3. Para os pontos de videomonitoramento em que não seja possível utilizar fibra óptica, poderão ser utilizados enlaces de rádio (RF). A conexão de pontos de videomonitoramento com enlaces de rádio será limitada em 30% do número total de pontos, não devendo ser ultrapassada esta quantia.
- 1.4.4. Para ambas as formas de conectividade, devem ser respeitados os parâmetros apresentados na Tabela 1 - Latência entre Câmera e Plataforma;
- 1.4.5. O custo da conectividade/*link* para transmissão das imagens das câmeras deverá ser inserido no custo mensal do item 4. **INFRAESTRUTURA DOS PONTOS DE VIDEOMONITORAMENTO**;
- 1.4.6. A latência entre a câmera e a plataforma deve estar dentro das especificações descritas na Tabela 1.
- 1.4.7. Casos em que exista limitações de infraestrutura e qualidade de conectividade a CONTRATADA poderá propor um valor maior de latência no projeto de instalação da câmera ficando a cargo da CONTRATANTE avaliar e aceitar se for de seu interesse ou remanejar o local de instalação.
- 1.4.8. Caso a latência ultrapasse o valor máximo permitido no período de um mês, por câmera, será aplicada uma glosa correspondente à Severidade Média, conforme especificado na Tabela 4 - Atendimento de Chamado

Latência entre Câmera e Plataforma					
Operação Normal		Pico de Uso		Pior Cenário	
75 % do Tempo		20% do Tempo		5% do Tempo	
65 ms	Jitter 25	85 ms	Jitter 30	180 ms	Jitter 40

Tabela 1 - Latência entre Câmera e Plataforma

- 1.4.9. O custo da conectividade/*links* dos CIICCs regionais é de responsabilidade da CONTRATADA e deve estar embutido no item **10. CIICC - REGIONAL**;
- 1.4.10. O custo da conectividade/*links* do CIICC principal é de responsabilidade da CONTRATADA e deve estar embutido no item **11. CIICC – PRINCIPAL (Goiânia)**;
- 1.4.10.1. A conexão entre cada CIICC e a internet deverá ter redundância, tendo pelo menos dois *links* de conectividade distintos, sendo cada *link* capaz de trafegar a demanda total de dados do CIICC de forma independente.
- 1.4.11. Toda conectividade/*link* deve ser dimensionada, exclusivamente, de acordo com as necessidades da solução, sem a utilização dos *links* já existentes nos locais de implantação dos CIICCs ou a utilização dos *links* deste projeto em outras atividades;

- 1.4.12.** A imagem das câmeras deve estar em *full bit rate* (nível mais alto de qualidade), garantindo a qualidade das imagens a serem analisadas e armazenadas, e as imagens em tempo real devem ter menor latência possível;
- 1.4.13.** Os preços 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;
- 1.4.14.** 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.
- 1.5.** **Projeto técnico:** abrange, mas não somente, a identificação e confirmação de viabilidade técnica 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 de vídeo
  - ✓ Armazenamento de dados
  - ✓ Dimensionamento dos links de internet e consumo do projeto
  - ✓ Integração com outros sistemas
  - ✓ Treinamento e documentação
- 1.5.1.** Surgindo a necessidade de remanejar pontos de videomonitoramento, por parte da CONTRATANTE, esta deverá comunicar formalmente a CONTRATADA, com as informações de endereços e tipos de câmera.
- 1.5.2.** Surgindo a necessidade de remanejar pontos de videomonitoramento, por parte da CONTRATADA, esta deverá comunicar formalmente a CONTRATANTE, justificando o motivo da solicitação. Apenas após a autorização expressa da CONTRATADA, o remanejamento poderá ser realizado.
- 1.5.3.** Os remanejamentos poderão ser realizados na etapa de projeto técnico. Não serão realizados remanejamento de pontos após a instalação.

## 2. PONTOS DE VIDEOMONITORAMENTO

### 2.1. Disposições gerais

- 2.1.1.** **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.
- 2.1.2.** **Analíticos:** A solução deve ser configurada para suportar os seguintes recursos analíticos:
- 2.1.2.1.** 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.

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

- ✓ Características físicas: gênero, cor de roupa e outros;
- ✓ Características da face: gênero, faixa etária e outros;
- ✓ Análise de comportamento: aglomeração, densidade populacional em determinada área e outros.

**2.1.2.3.** Analítico de veículo: permite realizar leitura de placas (*License Plate Recognition - LPR*), contagem de veículos e reconhecimento de características veiculares (cor, marca e tipo de veículo etc.). Alternativamente a contagem de veículos pode ser realizada por meio de relatórios.

- ✓ 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.

**2.1.3.** Os pontos de videomonitoramento são compostos pelos seguintes itens:

Itens
Câmera e acessórios
Poste e caixa hermética
Link de internet

**2.1.4.** 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.

**2.1.5.** **Quantidade de pontos de videomonitoramento:** A tabela abaixo permite que se verifique a quantidade de pontos de videomonitoramento por município, separados pelo tipo da câmera:

Municípios	Pontos	Câmeras				TOTAL
		TIPO I	TIPO II	TIPO III		
Águas Lindas de Goiás	24	36	12	17	65	
Santo Antônio do Descoberto	31	54	8	25	87	
Luziânia	27	46	8	18	72	
Cidade Ocidental	14	24	4	13	41	
Valparaíso de Goiás	30	28	32	13	73	
Formosa	33	46	16	24	86	
Planaltina	27	50	4	21	75	
Goiânia (Região da 44)	13	10	0	12	22	
Goiás	20	19	13	11	43	
<b>TOTAL</b>	<b>219</b>	<b>313</b>	<b>97</b>	<b>154</b>	<b>564</b>	

Tabela 2 - Quantidade de pontos de videomonitoramento

## 2.2. Requisitos obrigatórios para todas as câmeras

- 2.2.1. Rede:** Possuir interface de rede RJ-45;
- 2.2.2. Protocolos de rede:** Deve possuir no mínimo HTTP ou HTTPS, TCP, UDP, NTP e FTP;
- 2.2.3. Compressão de vídeo:** Deve possuir, no mínimo, as compressões de vídeo H.264, H.265 e MJPEG;
- 2.2.4. WDR:** Possuir alcance dinâmico estendido (WDR) de 120dB ou superior;
- 2.2.5. Infravermelho:** Deve possuir iluminador IR de 30m (podendo estar embutido na câmera ou em equipamento externo);
- 2.2.6. Fluxos (streams) simultâneos:** Deve possuir capacidade de suportar o envio de no mínimo 2 fluxos simultâneos para diferentes IPs;
- 2.2.7. 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;
- 2.2.8. Alarmes externos:** Possuir, no mínimo, 1 entrada e 1 saída de alarme;
- 2.2.9. Alimentação:** Deverá ser capaz de ser alimentada por fonte de alimentação DC 12V, AC 24V ou PoE;
- 2.2.10. Ambiente de operação:** faixa de temperatura de 0 a +60º C e umidade inferior a 90%;

- 2.2.11. 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;
  - ✓ 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 garantir a segurança na atualização de *firmwares*, aceitando apenas *firmwares* fornecidos pelo fabricante.
- 2.2.12. Compatibilidade:** Deve possuir pelo menos o protocolo ONVIF para compatibilidade entre fabricantes;
- 2.2.13.** A câmera deverá possuir função de detecção de violação de imagem (obstrução física, desfoco intencional e spray ou pichação);
- 2.2.14. 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.

### **2.3. Item 1: CÂMERA TIPO I - 110km/h**

- 2.3.1. CÂMERA TIPO I: Analítico de veículos em velocidade até 110km/h**
- 2.3.2.** Câmera para aplicação de analítico de veículos que trafeguem a até 110km/h;
- 2.3.3.** 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;
- 2.3.4.** As câmeras devem ser instaladas em infraestruturas preparadas para a instalação às margens de ruas, avenidas e rodovias;
- 2.3.5.** As câmeras devem ser capazes de capturar, no mínimo, 2 faixas.
- 2.3.6. Características principais:**
- ✓ Sensor de imagem CMOS de 1/1.8” ou maior (é permitida a utilização de recursos como *Global Shutter*);
  - ✓ Velocidade mínima do obturador: 1/50s ou mais lento;
  - ✓ Velocidade máxima do obturador: 1/15.000s ou mais rápido;
  - ✓ Resolução igual ou superior a 2MP;

- ✓ Taxa de frames de, no mínimo, 25fps;
- ✓ Distância focal mínima: 12mm ou menor. Distância focal máxima: 32mm ou maior;
- ✓ Deve possuir balanço de branco manual e automático.

**2.3.7. 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 em movimento, combinando números e letras (ANPR), a uma velocidade de até 110 Km/h, usando tecnologia embarcada.

- 2.3.8.** Deverá trabalhar em conjunto com o VMS, enviando metadados veiculares para permitir que o *software* gerencie todas as informações necessárias;
- 2.3.9.** A comprovação do funcionamento deve ser feita através de carta do fabricante, atestando a possibilidade de integração até a data de operacionalização dos equipamentos;
- 2.3.10.** A câmera oferecida deve ter a capacidade de identificar todos os tipos de placas veiculares previstas pelo CONTRAN no Código Brasileiro de Trânsito (veículos de passeio, motocicletas, caminhões, ônibus, reboques e semirreboques etc.), independentemente da cor, categoria do veículo, de estarem revestidas ou não com a película refletiva prevista na resolução 372/2011 do CONTRAN;
- 2.3.11.** Deverá reconhecer o layout (LLL-NNNN), bem como o padrão Mercosul (LLLNLNN), sendo L = Letra e N = Número, por meio de sistema de reconhecimento ótico de caracteres (OCR – *Optical Character Recognition*);
- 2.3.12.** Deverá reconhecer veículos 24h por dia, em cenários diurnos e noturnos;
- 2.3.13.** Deverá apresentar índice de assertividade igual ou superior a 90% na Prova de Conceito (POC) e 97% em operação, nas leituras e no reconhecimento. As informações a respeito das condições de realização e requisitos a serem analisados na Prova de Conceito estarão no **Tópico 6 – Requisitos da Contratação**, do Termo de Referência.

**2.4. Item 2: CÂMERA TIPO II – 180km/h**

- 2.4.1. CÂMERA TIPO II: Analítico de veículos em velocidade até 180km/h**
- 2.4.2.** Câmera para aplicação de analítico de veículos que trafeguem a até 180km/h;
- 2.4.3.** 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;
- 2.4.4.** As câmeras devem ser instaladas em infraestruturas preparadas para a instalação às margens de ruas, avenidas e rodovias;
- 2.4.5.** As câmeras devem ser capazes de capturar, no mínimo, 2 faixas.
- 2.4.6. Características Principais:**
- ✓ Sensor de imagem CMOS de 1/1.8" ou maior (é permitida a utilização de recursos como *Global Shutter*);

- ✓ Velocidade mínima do obturador: 1/50s ou mais lento;
- ✓ Velocidade máxima do obturador: 1/15.000s ou mais rápido;
- ✓ Resolução igual ou superior a 2MP;
- ✓ Taxa de frames de, no mínimo, 30fps;
- ✓ Distância focal mínima: 12mm ou menor. Distância focal máxima: 32mm ou maior;
- ✓ Deve possuir balanço de branco manual e automático.

**2.4.7. 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 em movimento, combinando números e letras (ANPR), a uma velocidade de até 180Km/h, usando tecnologia embarcada.

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

**2.4.9.** A comprovação do funcionamento deve ser feita através de carta do fabricante, atestando a possibilidade de integração até a data de operacionalização dos equipamentos;

**2.4.10.** A câmera ofertada deve ter a capacidade de identificar todos os tipos de placas veiculares previstas pelo CONTRAN no Código Brasileiro de Trânsito (veículos de passeio, motocicletas, caminhões, ônibus, reboques e semirreboques, etc.), independentemente da cor, categoria do veículo, de estarem revestidas ou não com película refletiva prevista na resolução 372/2011 do CONTRAN;

**2.4.11.** Deverá reconhecer o layout (LLL-NNNN), bem como o padrão Mercosul (LLLNLNN), sendo L = Letra e N = Número, por meio de sistema de reconhecimento ótico de caracteres (OCR – *Optical Character Recognition*);

**2.4.12.** Deverá reconhecer veículos 24h por dia, em cenários diurnos e noturnos;

**2.4.13.** Deverá apresentar índice de assertividade igual ou superior a 90% na Prova de Conceito – POC e 97% em operação, nas leituras e no reconhecimento. As informações a respeito das condições de realização e requisitos a serem analisados na Prova de Conceito estarão no **Tópico 6 – Requisitos da Contratação**, do Termo de Referência.

**2.5. Item 3: CÂMERA TIPO III – ANALÍTICO DE PESSOAS**

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

**2.5.2.** 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;

**2.5.3. Características Principais:**

- ✓ Deverá possuir sensor de imagem CMOS de 1/2.7" ou maior (é permitida a utilização de recursos como *Global Shutter*);
- ✓ Velocidade mínima do obturador: 1/25 ou mais lento;
- ✓ Velocidade máxima do obturador: 1/10.000 ou mais rápido;

- ✓ Possuir resolução de, no mínimo, de 4MP;
- ✓ Taxa de frames de, no mínimo, 30fps;
- ✓ Distância focal mínima: 4.5mm ou menor. Distância focal máxima: 9mm ou maior;
- ✓ Deverá possuir sensibilidade mínima igual ou inferior a 0,012 lux no modo colorido, e a 0 lux no modo PB com IR ativado;
- ✓ Deverá possuir tecnologias de compensação de luz, garantindo a visibilidade da cena;
- ✓ Possuir função de Máscara de Privacidade de, no mínimo, 4 áreas.

**2.5.4. Deve possuir os seguintes analíticos:**

- ✓ Possuir funções inteligentes de detecção de faces, detecção de cruzamento de linha, detecção de intrusão, objetos deixados, objetos removidos e estacionamento irregular;
- ✓ Detecção de características das pessoas, extraíndo no mínimo os seguintes atributos: faixa etária, gênero, cor de roupas e tipo de roupas (ex: camisa, calça etc.);
- ✓ 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).

**2.5.5.** 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 e detecção de 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;

**2.5.6.** A função de detecção facial deve ser obrigatoriamente realizada nas câmeras;

**2.5.7.** É obrigatório que pelo menos os analíticos de reconhecimento facial, detecção de características de pessoas e detecção de características de veículos sejam realizados simultaneamente;

**2.5.8.** Para os demais analíticos, se não for possível a realização simultânea, a plataforma deverá permitir o agendamento dos diferentes analíticos, de forma a permitir que seu processamento seja alternado de forma automatizada (conforme agendamento);

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

**2.5.10.** A comprovação do funcionamento deve ser feita através de carta do fabricante, atestando a possibilidade de integração até a data de operacionalização dos equipamentos.

**Item 4: INFRAESTRUTURA DOS PONTOS DE VIDEOMONITORAMENTO**

**2.6. Poste para câmera**

**2.6.1.** O poste deve ser dimensionado, podendo ser metálico ou de concreto, para evitar trepidações provocadas por ventos de intensidade normal ou deslocamentos de ar causados pelo movimento de veículos. Deve-se respeitar as seguintes alturas mínimas de instalação para as câmeras:

- ✓ Para as câmeras Tipo I e II: altura mínima de 4 metros
- ✓ Para as câmeras Tipo III: altura mínima de 2,5 metros

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

**2.6.3.** 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;

- 2.6.4.** Deverá ser fornecido com braços para alocação das câmeras;
- 2.6.5.** 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;
- 2.6.6.** Todos os materiais necessários para a instalação dos postes serão de responsabilidade da CONTRATADA, tais como: caixas, cabos, conectores, adaptadores, disjuntores, suportes, parafusos etc.;
- 2.6.7.** Os postes abrigarão as caixas herméticas com pontos de conexões e as câmeras;
- 2.6.8.** 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;
- 2.6.9.** Deverá ser previsto o licenciamento para utilização do local onde o poste será instalado. Os custos para este licenciamento serão de responsabilidade da CONTRATADA;
- 2.6.10.** Será de responsabilidade da CONTRATADA a limpeza do local de trabalho, bem como todo e qualquer acabamento necessário;
- 2.6.11.** Deverá prever a identificação física do poste e documentação técnica do material e/ ou equipamento, conforme layout projetado da solução;
- 2.6.12.** 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 caderno, nas versões vigentes quando da apresentação das propostas;
- 2.6.13.** 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).

## **2.7. Caixa hermética**

- 2.7.1.** Deverá possuir entradas para ventilação;
- 2.7.2.** Suportar condições de instalação externa exposta ao tempo;
- 2.7.3.** Deverá ter um grau de proteção mínimo de IP64, garantindo proteção completa contra poeira e respingos de água de qualquer direção;
- 2.7.4.** 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"

## **2.8. Conectividade**

- 2.8.1.** A infraestrutura de conectividade deve garantir a transmissão segura, estável e contínua de dados entre os dispositivos de videomonitoramento e a central de controle. A rede deve ser

capaz de suportar o tráfego de vídeo em alta definição, garantindo baixa latência e alta disponibilidade.

- 2.8.2.** A largura de banda mínima recomendada deve ser dimensionada conforme a resolução e taxa de quadros das câmeras, garantindo a transmissão sem degradação da qualidade.
- 2.8.3.** A conectividade deve permitir integração com redes existentes, utilizando protocolos padrão de comunicação, como IPv4, IPv6 e VLANs para segmentação de tráfego.

### 3. CIICCs (Centro Integrado de Inteligência, Comando e Controle)

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. Item 10. CIICC – REGIONAL

Os itens que serão adquiridos para cada CIICC Regional estão descritos na tabela abaixo. As *workstations* para os CIICCs Regionais serão fornecidas pela CONTRATANTE e não devem ser precificados neste projeto.

Quantidade	Item
01	<i>Ledwall</i> de 5m <sup>2</sup>
01	Controladora de imagem para o <i>ledwall</i>
06	<i>Workstations</i> ( <b>fornecidas pela CONTRATANTE</b> )

#### 3.2. Item 11. CIICC - PRINCIPAL

Os itens que compõem o CIICC Principal em Goiânia, descritos na tabela abaixo, serão fornecidos pela CONTRATANTE e não devem ser precificados neste projeto.

Quantidade	Item
04	<i>Workstations</i> ( <b>fornecidas pela CONTRATANTE</b> )

Para o CIICC – Principal, o fornecedor será responsável pelo link de conectividade necessário para a operação e visualização do sistema nas *workstations* e no ledwall do CIICC, bem como pela integração deste link com as *workstations* e o ledwall. O link de conectividade deve ser dimensionado para suportar a visualização de, pelo menos, 40 câmeras.

### 3.3. 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, que serão utilizadas no apoio às atividades dos Centros Integrados de Inteligência, Comando e Controle (CIICC).

- 3.3.1.** Para orçamento, considerar as dimensões aproximadas de **3m de largura por 1.68m de altura**. As medidas reais devem ser levantadas *in loco* durante o processo de licitação;
- 3.3.2.** O painel de LED deverá atender no mínimo os seguintes parâmetros:
- 3.3.2.1. O conjunto deve apresentar resolução de 1920 x 1080;
  - 3.3.2.2. Painéis com *pitch* inferior a 1,6mm;
  - 3.3.2.3. Ângulo de visão não inferior a 140°, tanto na horizontal quanto na vertical;
  - 3.3.2.4. Possuir mínimo de 400.000 mil pixels por m<sup>2</sup> de painel;
  - 3.3.2.5. Reproduzir mais de 60 milhões de cores;
  - 3.3.2.6. Brilho: o painel deverá possuir ajuste de brilho;
  - 3.3.2.7. Temperatura de cor ajustável: 3000K - 9000k;
  - 3.3.2.8. Razão de contraste mínimo: 4000:1;
  - 3.3.2.9. Profundidade de processamento de escala de cinza (bit): 16 bit (ou superior);
  - 3.3.2.10. Ser alimentado em tensões de 110 a 220V;
  - 3.3.2.11. Possuir taxa de atualização de, no mínimo, 3.200Hz;
  - 3.3.2.12. Possuir tempo de vida útil mínima de 70.000h de uso;
  - 3.3.2.13. Operar em condição de temperatura e umidade de 0° a +40°C e 10-70% RH respectivamente;
  - 3.3.2.14. Os módulos devem permitir manutenção frontal;
  - 3.3.2.15. O sistema deverá reproduzir acima de 60000 tons de cinza;
  - 3.3.2.16. Processador de vídeo para painel de LED com SDI ou HDMI;
  - 3.3.2.17. Alternar perfeitamente entre qualquer canal;
  - 3.3.2.18. Configurações de ajuste rápido do botão;
  - 3.3.2.19. Função de detecção de sinal;
  - 3.3.2.20. Resolução de saída máxima: 1920\*1080 @ 60hz;
  - 3.3.2.21. A solução deve suportar trabalhar com codificação de cores RGB: 444. YUV: 444 e YUV:422;
  - 3.3.2.22. Deve suportar resolução de até 4K, largura de banda e vídeo de 18Gbps;
  - 3.3.2.23. Deve suportar saída de áudio através de HDMI ou display port ou interfaces próprias de áudio;
  - 3.3.2.24. O ledwall deve suportar a exibição simultânea de mais de uma fonte de vídeo, com múltiplas portas de saída e suportar longas distâncias sem perda de qualidade;
  - 3.3.2.25. Cabo RJ 45 cat6: 4 Pares 24/23 AWG Condutores Isolados (em Polietileno Especial);
  - 3.3.2.26. Constituído em PVC Retardante a Chama. Blindagem - Não Blindado (U/UTP) Conector: Rj45 Blindado Diâmetro Nominal - 6.0mm- Suporte a Gigabit Ethernet;
  - 3.3.2.27. 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);
  - 3.3.2.28. Acabamento: moldura em material de alumínio, na cor preta, cobrindo todos os vãos laterais, superiores e inferiores, fechando qualquer acesso aos módulos;
  - 3.3.2.29. 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 fornecer e instalar todos os equipamentos necessários para o seu perfeito funcionamento;

- 3.3.2.30. 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.

#### **3.4. Controlador de imagem**

- 3.4.1.** Para cada conjunto de *ledwall* deve ser provida uma máquina decodificadora, com capacidade para decodificação de até 64 canais em FHD @ 10FPS;
- 3.4.2.** A máquina decodificadora deve possuir ferramenta de *videowall*, que permita arranjar elementos de forma matricial em mosaicos definidos pelo usuário, bem como demonstrar *dashboards* e outras ferramentas que sejam convenientes à operação;
- 3.4.3.** 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;
- 3.4.4.** Deve suportar processamento de até 5MP;
- 3.4.5.** Sistema de busca automática de sinal;
- 3.4.6.** Deve permitir o gerenciamento de cenas;
- 3.4.7.** Deve permitir o modo de display em tela dividida;
- 3.4.8.** Deve possuir *software-cliente* para configurações e ajustes, com licenças definitivas.

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

A plataforma de análise de vídeo é o conjunto de *hardware* (servidores, appliances, etc.), *software* (VMS, clients, etc.) e licenças necessárias para executar o videomonitoramento com inteligência artificial com eficiência.

#### **4.1. Item 8. PLATAFORMA DE ANÁLISE DE VÍDEO**

##### **4.1.1. Disposições gerais:**

- 4.1.2.** A plataforma de análise de vídeo deve ser dimensionada para suportar a totalidade dos dispositivos e analíticos previstos no projeto. Além disso, a capacidade da plataforma deve garantir a escalabilidade e permitir futuras expansões;
- 4.1.3.** A plataforma deve ser precificada com base em um valor por câmera, de modo a permitir a expansão do sistema por meio de aditivos contratuais;
- 4.1.4.** Garantia de alta capacidade de processamento (de analíticos), qualidade de transmissão e armazenamento de imagens por 30 (trinta) dias;
- 4.1.5.** Equipado com Software de Gestão de Vídeo (VMS) licenciado, permitindo a visualização, gravação, e analíticos de todos os canais de vídeo;
- 4.1.6.** Funcionalidades incluem monitoramento em tempo real, replay, analíticos e gestão de eventos.

## 4.2. DATACENTER

- 4.2.1. A proponente deverá garantir uma latência média inferior a 50ms entre o CIICC de Goiânia e o datacenter utilizado. A exigência de uma latência máxima de 50ms é justificada pela necessidade de oferecer respostas rápidas em situações de emergência, garantir um fluxo contínuo de vídeo e a qualidade do serviço e minimizar perdas de pacotes de dados. Essa especificação assegura que o sistema seja eficiente, confiável e capaz de atender às demandas críticas de segurança pública e operacional.
- 4.2.2. O armazenamento e processamento dos dados deverá ser realizado integralmente em território nacional.
- 4.2.3. O sistema deverá ser dimensionado para o armazenamento de vídeos, snapshots e metadados, cabendo à CONTRATADA garantir o armazenamento de todos os dados por um período mínimo de 30 (trinta) dias, em full HD, com as seguintes configurações mínimas: resolução de 1920 x 1080 pixels, taxa de quadros de 25 FPS e compressão H.264 ou H.265.

Distribuição de Câmeras por CIICC				
Descrição	Câmeras por CIICC	Tipo de Câmera		
		Tipo I	Tipo II	Tipo III
CIICC GOIÂNIA	22	10	0	12
CIICC GOIÁS	43	19	13	11
CIICC FORMOSA	161	96	20	45
CIICC LUZIÂNIA	186	98	44	44
CIICC ÁG. LINDAS	152	90	20	42
<b>Total</b>	<b>564</b>	<b>313</b>	<b>97</b>	<b>154</b>

Tabela 3 - Distribuição de Câmeras por CIICC

- 4.2.4. 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.

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

### 4.3.1. Características principais

- 4.3.1.1. Toda atualização de software deve ser comunicada, e as novas atualizações devem ser instaladas no prazo de até 1 (um) ano. Caso contrário, será aplicada uma multa proporcional a severidade baixa, conforme Tabela 3 - Atendimento de Chamado;
- 4.3.1.2. Deve permitir a integração de câmeras/canais de vídeo ao VMS ofertado;
- 4.3.1.3. 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;
- 4.3.1.4. 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;

- 4.3.1.5. 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;
- 4.3.1.6. 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.
- 4.3.1.7. 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 arquitetura proposta, embutindo os valores destas nos itens em que forem pertinentes.
- 4.3.1.8. 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;
- 4.3.1.9. A gravação não deverá ser limitada pelo software, e sim pela capacidade de armazenamento do hardware;
- 4.3.1.10. O sistema deve permitir diversos tipos de gravação (contínua, por detecção de movimento, por evento);
- 4.3.1.11. O sistema deve permitir a criação de mosaicos individuais ou compartilhados no cliente de monitoramento com outros usuários/grupos de usuários;
- 4.3.1.12. O sistema deverá permitir acesso de terceiros via web, autorizando conexões remotas por aplicativo/client, browser ou celular, sem a cobrança de licenças adicionais. O servidor web deverá permitir:
  - ✓ Visualização ao vivo e pesquisa de gravações;
  - ✓ Criação e edição de mosaicos;
  - ✓ Exportação de vídeos e fotos;
  - ✓ Reprodução de áudio;
  - ✓ Notificação de eventos.
- 4.3.1.13. A plataforma deve ser compatível com os principais navegadores web do mercado (exemplo: Mozilla Firefox, Microsoft Edge, Google Chrome ou Opera, etc);
- 4.3.1.14. O sistema deverá permitir conexões unicast e multicast;
- 4.3.1.15. O sistema deverá efetuar todos os registros do sistema (logs) em nível de auditoria, armazenando todas as ações dos usuários por um período de 120 (cento e vinte) dias;
- 4.3.1.16. O sistema deve permitir pelo menos 500 usuários cadastrados e 120 usuários simultâneos;
- 4.3.1.17. 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;
- 4.3.1.18. O VMS deverá servir de interface para servidores compostos por codificadores de vídeo analógicos (encoders, DVRs) e digitais, como câmeras e NVRs;
- 4.3.1.19. O VMS deverá usar dois streams independentes, um para visualização e outro para gravação;
- 4.3.1.20. O VMS deverá suportar as principais marcas de câmeras IP do mercado, além de suportar as mais recentes revisões dos padrões ONVIF;
- 4.3.1.21. 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;

- 4.3.1.22. O VMS deve dispor de artifícios 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;
- 4.3.1.23. 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;
- 4.3.1.24. 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 a:
- ✓ Eventos de alarme;
  - ✓ Eventos de gravação (erro de partição e partição restaurada);
  - ✓ Eventos de câmeras *on-line* e *off-line*;
  - ✓ Eventos de câmera (iniciar/parar gravação, movimento iniciado/desligado, sinal perdido/recuperado, sensores de relés se acionada/desligada);
- 4.3.1.25. Deverá receber também 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.
- 4.3.1.26. 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;
- 4.3.1.27. Os eventos gerados a partir das análises poderão servir de gatilho para que o 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).
- 4.3.1.28. 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;

- 4.3.1.29. 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 automaticamente;
- 4.3.1.30. 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.
- 4.3.1.31. 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;
- 4.3.1.32. 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 ser configuradas pelos administradores do sistema;
- 4.3.1.33. Deverá permitir ao administrador ou aos usuários com direito de administração, mudar a configuração do sistema. A administração deverá ser realizada de forma descentralizada, de qualquer lugar na rede, permitindo buscar dispositivos e elementos compatíveis;
- 4.3.1.34. 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);
- 4.3.1.35. 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;
- 4.3.1.36. O sistema deverá ser capaz de gerenciar os vídeos armazenados em cartões de memória instalados nas câmeras (edge storage);
- 4.3.1.37. O sistema deverá permitir a replicação de dados entre discos, a qual deverá ser iniciada de forma automática ou manual;
- 4.3.1.38. 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;
- 4.3.1.39. Os mosaicos de câmera deverão estar disponíveis a todos os usuários no VMS, desde que, sejam compartilhados com outros grupos de usuário;
- 4.3.1.40. 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;
- 4.3.1.41. 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;
- 4.3.1.42. 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 (ativar/desativar) 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.

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

4.3.1.44. 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;

4.3.1.45. 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;

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

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

4.3.1.48. Deverá possibilitar aos operadores controlarem (pausar/play, avançar, voltar) grupos de câmeras sem afetar a possibilidade de outros operadores de ver e controlar a mesma sequência;

4.3.1.49. 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;

- ✓ 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.

4.3.1.50. O VMS deverá trabalhar com mapas online, para que seja possível identificar o posicionamento das câmeras em diversos pontos separados geograficamente;

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

- 4.3.1.52. Deverá monitorar em tempo real as condições da plataforma de análise de vídeo, indicando a utilização, carga de processamento ou falha de câmeras, por exemplo, de forma que o operador possa tomar alguma ação em caso de falhas;
- 4.3.1.53. 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;
- 4.3.1.54. Deverá permitir comunicação de áudio com a unidade de gravação. O áudio será arquivado na mesma base de dados que o vídeo;
- 4.3.1.55. 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;
- 4.3.1.56. Usuários deverão ser capazes de tirar snapshots tanto de vídeos ao vivo como gravados;
- 4.3.1.57. 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;
- 4.3.1.58. Deverá possibilitar ao operador controlar reprodução com pause, avanço e retrocesso de reprodução, avançar e voltar lentamente quadro a quadro;
- 4.3.1.59. O operador deverá ter a possibilidade de escolher quais marcadores devem ser mostrados em linha do tempo ou lista pesquisável, com o uso de filtros, como por exemplo:
- ✓ Todos os eventos
  - ✓ Tipos de alarmes
  - ✓ Alarmes não classificados
  - ✓ Fonte de alarme
  - ✓ Eventos comentados
- 4.3.1.60. Deverá prover exportação de imagem estática para os formatos JPEG com hora e data estampadas na imagem;
- 4.3.1.61. Deverá prover ferramentas para exportar sequências de vídeo em formatos padrões como EXE, AVI, MP4 ou MKV;
- 4.3.1.62. O sistema deverá possibilitar ao operador exportar gravações de vídeo através de arquivos compactados e criptografados com senha;
- 4.3.1.63. 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:
- ✓ 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
- 4.3.1.64. 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;
- 4.3.1.65. 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;

#### **4.3.2. Item 5. LICENÇA PARA ANALÍTICO DE RECONHECIMENTO FACIAL**

##### **4.3.2.1. Reconhecimento facial**

- 4.3.2.2. O sistema deve admitir a criação de múltiplos bancos de faces, para comparação e consequente reconhecimento facial;
- 4.3.2.3. O sistema de reconhecimento facial deve capturar e registrar no banco de dados as faces de todas as pessoas que passarem nos ambientes monitorados;
- 4.3.2.4. 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;
- 4.3.2.5. 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;
- 4.3.2.6. 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;
- 4.3.2.7. 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;
- 4.3.2.8. 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;
- 4.3.2.9. O sistema deve permitir a configuração da área de atuação da captura dos rostos e ajuste de sensibilidade;

##### **4.3.3. Analítico de veículos**

- 4.3.3.1. 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;
- 4.3.3.2. 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 das câmeras, atestando a possibilidade de integração até a data de operacionalização dos equipamentos.
- 4.3.3.3. 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;

- 4.3.3.4. Deve ser possível pesquisar por uma placa em mais de uma câmera simultaneamente;
- 4.3.3.5. 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.

#### **4.3.4. Analítico de pessoas**

- 4.3.4.1. 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.
- 4.3.4.2. O sistema deve permitir o rastreio de pessoas baseado em suas características físicas.
- 4.3.4.3. 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.

### **4.4. Item 7. INTEGRAÇÃO COM OUTROS SISTEMAS**

#### **4.4.1. Capacidade de integração com serviços externos**

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

- 4.4.1.1. Permitir a troca de dados utilizando APIs HTTP, possibilitando a integração de serviços web externos, abrangendo, no mínimo, os protocolos REST (Representational State Transfer);
- 4.4.1.2. Integrar-se a serviços externos da web, utilizando, no mínimo, um dos seguintes formatos de troca de dados: texto (.txt), JSON (JavaScript Object Notation), XML (eXtensible Markup Language) e CSV (Comma-Separated Values);
- 4.4.1.3. 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;
- 4.4.1.4. Permitir integração direta através de módulo integrador;
- 4.4.1.5. Permitir integração direta através de servidor de banco de dados;
- 4.4.1.6. 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;
- 4.4.1.7. 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;

- 4.4.1.8. Além disso, todas as informações compartilhadas com esses serviços devem ser devidamente criptografadas, utilizando o protocolo HTTPS/SSL/TLS (TLS 1.2 ou superior);
- 4.4.1.9. 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.

#### **4.4.2. Integrações com sistemas**

- 4.4.2.1. O sistema deve possuir a capacidade de transmitir todos os metadados relacionados ao analítico de veículos para a Secretaria de Estado da Segurança Pública de Goiás com o objetivo de armazená-los em seu próprio banco de dados.
  - ✓ O sistema deve ser capaz de entregar informações para a SSP/GO de acordo com o formato dos metadados indicado no item 11, deste caderno.
- 4.4.2.2. Os dados coletados pelo sistema de videomonitoramento deverão ser integrados ao Big Data Estadual sem custos adicionais, possibilitando análises estratégicas para diversos órgãos da administração pública estadual.
- 4.4.2.3. A Subsecretaria de Tecnologia da Informação deverá ser consultada para alinhar quais dados serão compartilhados, em que formato e com que frequência, assegurando aderência aos requisitos técnicos e estratégicos estabelecidos pelo Big Data Estadual.
- 4.4.2.4. O sistema deverá estar preparado para integração para consultas nas seguintes bases de dados: SSP/GO, DETRAN-GO, SENATRAN, TSE, BANCO NACIONAL DE MANDADOS DE PRISÃO (BNMP) e SINESP CIDADÃO;
  - ✓ A integração com esses sistemas será feita sob demanda da CONTRATANTE, não sendo item essencial para aceitação das centrais de videomonitoramento na entrega do projeto.
- 4.4.2.5. Para garantir a interoperabilidade e uma gestão centralizada, a solução deve permitir a visualização de imagens e consultas a outros VMS de terceiros, (podendo ser, por exemplo, via API ou SDK), desde que esses VMS suportem tais funcionalidades. As funcionalidades requeridas incluem:
  - ✓ Visualização Centralizada: Permitir que as imagens de diferentes VMSs sejam visualizadas em uma única interface;
  - ✓ Consultas Cruzadas: Habilitar consultas de dados e eventos entre a solução e os VMSs de terceiros.
- 4.4.2.6. Deverá ser prevista uma quantidade de horas para serviços de integração, conforme planilha de cotação.

#### **4.4.3. Item 6. LICENÇA PARA VISUALIZAÇÃO DE CÂMERAS DE OUTROS SISTEMAS**

##### **4.4.3.1. Visualização de outras câmeras (de terceiros ou de outros projetos)**

- 4.4.3.2. O sistema 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;

- ✓ É necessário que o sistema suporte os protocolos ONVIF (Perfis M, S, G e T). Isso garantirá a visualização de imagens e metadados das câmeras compatíveis com o protocolo ONVIF e seus respectivos perfis;
- ✓ Caso necessário, a CONTRATADA terá um prazo de 6 (seis) meses após a assinatura do contrato para adequar o sistema de forma a suportar os protocolos ONVIF (M, S, G e T). Caso esse prazo não seja respeitado sem justificativa plausível, será aplicada uma multa de 15% do pagamento do valor mensal até a regularização deste item.

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

#### 4.4.4. Padrão de envio de metadados para a SSP-GO

4.4.4.1. Os metadados das câmeras de videomonitoramento devem ser enviados para a SSP/GO:

- ✓ 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"  
     }  
   }  
   ...  
 }]
```

### 4.5. SEGURANÇA

#### 4.5.1. Solução de segurança cibernética

4.5.1.1. A plataforma deverá possuir pelo menos as seguintes funcionalidades de segurança, devendo ser capaz de suportar toda a demanda necessária para a operação do sistema (ex.: throughput, sessões, etc):

- 4.5.1.2. A solução de firewall deve consistir em sistema de proteção de rede baseada em appliance físico ou virtual, não sendo permitidas soluções open source (produto montado);
- 4.5.1.3. Possuir hardware de alta capacidade, permitindo capacidades em alta escalabilidade, e ser otimizada para análise de conteúdo de aplicações em camada 7;
- 4.5.1.4. O gerenciamento da solução deve suportar acesso via SSH, cliente ou WEB (HTTPS) e API aberta;
- 4.5.1.5. Os dispositivos de proteção de rede devem possuir suporte a roteamento multicast (PIM-SM e PIM-DM);
- 4.5.1.6. Deve suportar BGP, OSPF, RIP e roteamento estático;
- 4.5.1.7. Os dispositivos de proteção de rede devem possuir suporte a DHCP Relay e DHCP Server;
- 4.5.1.8. Deve suportar ao menos 30 tabelas independentes de roteamento, por contexto de firewall;
- 4.5.1.9. 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;
- 4.5.1.10. Deve implementar Network Prefix Translation (NPTv6) ou NAT66, prevenindo problemas de roteamento assimétrico;
- 4.5.1.11. Deve suportar NAT64;
- 4.5.1.12. Deve permitir monitorar via SNMP o uso de CPU, memória, espaço em disco, VPN, situação do cluster e violações de segurança;
- 4.5.1.13. Proteção anti-spoofing;
- 4.5.1.14. Deve suportar Modo Camada – 3 (L3), para inspeção de dados em linha e visibilidade do tráfego;
- 4.5.1.15. Não serão aceitas soluções baseadas em PCs de uso geral.
- 4.5.1.16. A solução de firewall deve possuir conectores nativos para integração com nuvens privadas, pelo menos: VMware ESXI, Cisco ACI e Kubernetes;
- 4.5.1.17. 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;
- 4.5.1.18. Controle de políticas por usuários, grupos de usuários, IPs, redes e zonas de segurança;
- 4.5.1.19. Controle, inspeção e descriptografia de SSL por política para tráfego de saída (Outbound);
- 4.5.1.20. Deve descriptografar tráfego outbound em conexões negociadas com TLS 1.2 ou superior;
- 4.5.1.21. 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.

#### **4.5.2. Prevenção de ameaças**

- 4.5.2.1. Para proteção do ambiente contra-ataques, os dispositivos de proteção devem possuir módulo de IPS, Antivírus e Anti-Spyware;
- 4.5.2.2. Deve incluir assinaturas de bloqueio de arquivos maliciosos (Antivírus e Anti-Spyware). A ferramenta precisa de uma assinatura válida e ativa para receber atualizações e suportes contínuos do fornecedor. Isso assegura que o software esteja sempre atualizado com as últimas definições de segurança. O software de antivírus e anti-spyware deve ser configurado para receber atualizações diárias de definições de ameaças, garantindo que o sistema esteja sempre protegido contra as ameaças mais recentes, e o sistema deve ser capaz de verificar se as atualizações diárias estão sendo aplicadas corretamente e reportar falhas, caso não ocorra a atualização;
- 4.5.2.3. Deve ser possível a criação de políticas por usuários, grupos de usuários, IPs, redes ou zonas de segurança;

- 4.5.2.4. Detectar e bloquear a origem de portscans;
- 4.5.2.5. Bloquear ataques efetuados por worms conhecidos;
- 4.5.2.6. Permitir o bloqueio de vírus e spywares em, pelo menos, os seguintes protocolos: HTTP, FTP, SMB, SMTP e POP3;
- 4.5.2.7. Identificar e bloquear comunicação com botnets;
- 4.5.2.8. Registrar no 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;
- 4.5.2.9. Os eventos devem identificar o país de onde partiu a ameaça;
- 4.5.2.10. Deve incluir proteção contra vírus em conteúdo HTML e javascript, software espião (spyware) e worms;
- 4.5.2.11. Possuir proteção contra downloads involuntários usando HTTP de arquivos executáveis e maliciosos;
- 4.5.2.12. A solução deve analisar o comportamento de arquivos suspeitos em um ambiente controlado;
- 4.5.2.13. O sistema deve possuir proteção contra-ataques de rede DDoS e Phishing.

#### **4.5.3. Múltiplo Fator de Autenticação (MFA)**

- 4.5.3.1. Deve fazer parte da contratação, solução avançada de Múltiplo Fator de Autenticação (MFA) projetada para oferecer uma camada adicional de segurança no processo de autenticação de usuários, tornando mais difícil para invasores obterem acesso não autorizado a sistemas, aplicativos e dados sensíveis.

### **5. ADMINISTRAÇÃO DO SISTEMA, SUPORTE TÉCNICO E MANUTENÇÃO**

- 5.1.** 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.
- 5.1.1.** Todos os itens, da planilha de cotação, já devem conter, embutido, o valor de instalação e manutenção dos equipamentos e infraestrutura necessária para o funcionamento da solução.
- 5.1.2.** Por se tratar de prestação de serviço, a especificação de cada item deve conter também quaisquer custos de atualização tecnológica, manutenções e substituições (quando necessário), bem como quaisquer custos adicionais de licenças e acessórios necessários para o funcionamento do equipamento ou software.
- 5.2.** A CONTRATADA deverá disponibilizar SERVIÇO DE ATENDIMENTO composto por equipe com conhecimentos sólidos no funcionamento e operação dos serviços.
- 5.2.1.** Após a instalação dos equipamentos no CIICC de Goiânia, a CONTRATADA deverá disponibilizar um residente para atuar *on site* no CIICC de Goiânia, em horário comercial, por um período de um mês.

- 5.2.2.** O residente deverá iniciar as atividades após a conclusão do treinamento da solução e da operação assistida.
- 5.3.** Os serviços de “manutenção” incluirão:
- 5.3.1.** Solução de falhas ou defeitos no funcionamento, incluindo a instalação de arquivos para correção dos erros;
- 5.3.2.** Esclarecimento de dúvidas sobre o funcionamento e operação da solução;
- 5.3.3.** Instalação de novas versões ou atualizações e *patches* de todos os equipamentos fornecidos.
- 5.4.** Patches de segurança deverão ser instalados em até 30 dias após a disponibilização pelo fabricante.
- 5.5.** 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.
- 5.5.1.** Para os chamados de severidade crítica, conforme especificado na Tabela 3 - Atendimento de Chamado, devem ser considerados o SERVIÇO DE ATENDIMENTO DE 24X7, podendo ser em modo de sobreaviso.
- 5.6.** A manutenção técnica corretiva será realizada sempre que solicitada pelo CONTRATANTE por meio da abertura de chamado técnico diretamente à empresa CONTRATADA.
- 5.7.** 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.
- 5.8.** 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.
- 5.9.** No atendimento aos chamados técnicos abertos deverá ser disponibilizado suporte personalizado por um analista designado.
- 5.10.** 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.
- 5.11.** 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.
- 5.12.** A severidade de atendimento aos chamados será definida conforme avaliação do problema frente a Tabela 3 - Atendimento de Chamado.

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 a qualquer falha que comprometa toda a solução, como conexão, Firewall, Plataformas de Gerenciamento, Servidores, Gravação de Vídeo e Sistema em Nuvem.	Não se aplica
Média	90% das ocorrências em até 12h e 100% das ocorrências em até 18h	Se aplica a conectividade, disponibilidade e latência 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

Tabela 4 - Atendimento de Chamado

- 5.12.1. **Severidade Crítica:** Se aplica a qualquer falha que comprometa toda a solução, como conexão, *firewall*, plataformas de gerenciamento, servidores, gravação de vídeo e sistema em nuvem (dependendo da solução utilizada);
- 5.12.2. **Severidade Média:** Se aplica a conectividade, disponibilidade e latência de dispositivos de codificação e aos produtos que estejam apenas parcialmente inoperantes ou que sua inoperância não comprometa toda a solução;
- 5.12.3. **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.
- 5.13. Na abertura de chamados técnicos, serão fornecidas informações, como anormalidade observada, nome do responsável pela solicitação do serviço e severidade do chamado.
- 5.14. Chamados relativos ao *firewall*: 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.
- 5.15. Inclusão dos incidentes ocorridos e suas correções, além das vulnerabilidades identificadas com suas soluções.
- 5.16. Incidentes resolvidos fora do prazo e vulnerabilidades sem soluções identificadas serão considerados como incidentes de severidade crítica e sofrerão a respectiva glosa.
- 5.17. Todas as solicitações feitas pelo CONTRATANTE deverão ser registradas pela CONTRATADA para acompanhamento e controle da execução dos serviços e ainda:

- 5.17.1.** 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;
- 5.17.2.** O tempo do início efetivo de atendimento ao chamado técnico deverá ser de acordo com a Tabela 3 - Atendimento de Chamado, contado a partir da abertura do mesmo;
- 5.17.3.** Após o início do atendimento, o tempo de solução do problema deverá ser de acordo com a Tabela 3 - Atendimento de Chamado, não devendo ultrapassar os prazos estabelecidos para as respectivas severidades.

**5.18. Indicadores**

- 5.18.1.** 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 3 - 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.
- 5.18.2.** Paradas programadas, comunicadas e acordadas com antecedência mínima de 10 (dez) dias corridos, não serão contabilizadas na avaliação dos indicadores de desempenho.

**5.19. Item 12. ADMINISTRAÇÃO DO SISTEMA**

- 5.19.1. 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).
- 5.19.2. 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.

- 5.19.3.** Revisões trimestrais de:
- ✓ Revisão da lista de usuários;
  - ✓ Revisão de regras de firewall;
  - ✓ Inventários (de equipamentos, de software, de câmeras, etc);
- 5.19.4.** Controle de acesso: criação / bloqueio de usuários;
- 5.19.5.** Controle de mudanças.

## 6. TREINAMENTOS

### 6.1. Item 9. TREINAMENTO DA SOLUÇÃO DE VIDEO MONITORAMENTO

- 6.1.1.** 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;
- 6.1.2.** 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;
- 6.1.3.** A carga horária do treinamento não deve ultrapassar 8h por dia;
- 6.1.4.** O treinamento deve ter duração máxima de 40 horas, sendo 24 horas de treinamento teórico e 16 horas de operação assistida;
- 6.1.5.** Os serviços de operação assistida deverão ser realizados nas dependências dos CIICCs;
- 6.1.6.** 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;
- 6.1.7.** 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;
- 6.1.8.** O treinamento deve contemplar até 10 (dez) alunos, por turma, selecionados pela CONTRATANTE;
- 6.1.9.** 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;
- 6.1.10.** O treinamento deve ser presencial, em Goiânia ou no Entorno, com todas as despesas de transporte e estadia dos instrutores custeadas pela CONTRATADA;
- 6.1.11.** 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;
- 6.1.12.** O material didático utilizado no treinamento deve ser o material oficial do fabricante dos equipamentos/solução;
- 6.1.13.** 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.