GOVERNO DO ESTADO
DO RIO GRANDE DO SUL

SECRETARIA
DA SEGURANÇA
PÚBLICA

PROJETO
Cercamento Eletrônico Estadual Programa Avançar

VIDEOMONITORAMENTO URBANO
CERCAMENTO ELETRÔNICO
INTELIGÊNCIA ARTIFICIAL

FASE I

TERMO DE REFERÊNCIA
CADERNOS I e II
ATUALIZADO EM ABRIL DE 2024

GOV RS
NOVAS FAÇANHAS

SUMÁRIO

PARTE I - CADERNO DE TERMO DE REFERÊNCIA

PARTE II – CADERNO DE ESPECIFICAÇÕES TÉCNICAS

CADERNO I - TERMO DE REFERÊNCIA

1 DO OBJETO

Registro de preços de bens e serviços para futura contratação de empresa especializada para implantação de solução de videomonitoramento urbano, cercamento eletrônico, inteligência artificial e meios de comunicação de dados, no projeto de cercamento eletrônico estadual do "Programa Avançar", para municípios do Estado do Rio Grande do Sul, possibilitando o monitoramento dos pontos de controle a serem implantados, com o fornecimento de equipamentos instalados, com garantia e transferência de conhecimento, de modo a atender às necessidades da Secretaria da Segurança Pública, na forma e condições constantes neste Termo de Referência.

O certame lote único contendo cinco kits.

Código GCE: 0117.0749.000021	
ITEM	DESCRIÇÃO
1	KIT 1 – Ponto completo de Cercamento Eletrônico
1.1	Ponto de Cercamento
1.2	Licença de Software Análise Comportamental
1.3	Serviços de Locação de Link de Dados – Tipo I
Código GCE: 0117.0749.000022	
2	Kit 2 – Ponto de videomonitoramento Câmera Fixa
2.1	Ponto de Videomonitoramento
2.2	Licença de Software VMS
2.3	Licença de Software Análise Forense
2.4	Licença de Software Reconhecimento Facial
2.5	Serviços de Locação de Link de Dados – Tipo I
Códigoo GCE: 0117.0749.000023	
3	KIT 3 – Ponto de Videomonitoramento Câmera Speed Dome
3.1	Ponto de Videomonitoramento – Câmeras Speed Dome Tipo II
3.2	Licença de Software VMS
3.3	Serviços de locação de Link de Dados – Tipo I
Código GCE: 0117.0736.000007	
4	KIT 4 – Manutenção e conectividade de sistema existente
4.1	Manutenção Ponto de videomonitoramento/cercamento eletrônico
4.2	Serviços de Locação de Link de Dados – Tipo I
Código GCE: 0117.0736.000006	
5	KIT 5 – Conexão de Espelhamento e manutenção do sistema
5.1	Serviços de Locação de Link de Dados – Tipo II
5.2	Manutenção em Sala de Comando e Controle (Cercamento)

2 DA FUNDAMENTAÇÃO LEGAL DA CONTRATAÇÃO

O presente Termo de Referência foi planejado e elaborado com fundamentos nos seguintes dispositivos legais:

- Lei nº 14.133, de 01 de abril de 2021, Lei de Licitações e Contratos Administrativos, que estabelece normas gerais de licitação e contratação para as Administrações Públicas diretas, autárquicas e fundacionais da União, dos Estados, do Distrito Federal e dos Municípios;

- Lei Complementar nº 123, de 14 de dezembro de 2006, que institui o Estatuto Nacional da Microempresa e da Empresa de Pequeno Porte; altera dispositivos das Leis nº 8.212 e nº 8.213, ambas de 24 de julho de 1991, da Consolidação das Leis do Trabalho - CLT, aprovada pelo Decreto-Lei nº 5.452, de 1º de maio de 1943, da Lei nº 10.189, de 14 de fevereiro de 2001, da Lei Complementar nº 63, de 11 de janeiro de 1990; e revoga as Leis nº 9.317, de 5 de dezembro de 1996, e nº 9.841, de 5 de outubro de 1999;

- Decreto-Lei nº 2.848, de 7 de dezembro de 1940, que institui o código penal Brasileiro (Redação dada pela Lei nº 7.209, de 11.7.1984);

- Lei Estadual nº 11.389, de 25 de novembro de 1999, que institui o cadastro de fornecedores impedidos de licitar e contratar com a administração pública estadual; Institui o "Cadastro de Fornecedores Impedidos de Licitar e Contratar com a Administração Pública Estadual";

- Lei Estadual nº 13.706, de 6 de abril de 2011 (atualizada até a Lei n.º 15.139, de 3 de abril de 2018), que dispõe sobre a concessão de tratamento diferenciado e simplificado para as microempresas e empresas de pequeno porte nas licitações públicas, no âmbito da Administração Pública Estadual;

- Decreto Estadual nº 42.250, de 19 de maio de 2003, que regulamenta a Lei nº 11.389, de 25 de novembro de 1999, que instituiu o Cadastro de Fornecedores Impedidos de Licitar e Contratar com a Administração Pública Estadual - CFIL/RS;

- Decreto Estadual nº 48.160, de 14 de julho de 2011 (republicado no DOE nº 137 de 18 de julho de 2011), que regulamenta o tratamento diferenciado e simplificado para as Microempresas e Empresas de Pequeno Porte nas licitações públicas de bens, serviços e obras, no âmbito da Administração Pública Estadual, estabelecido pela Lei nº 13.706, de 6 de abril de 2011, e cria o Programa Gaúcho do Uso do Poder de Compra;

- Decreto Estadual nº 55.717, de 13 de janeiro de 2021, que dispõe sobre os modelos-padrão de editais de licitações, de compras públicas em geral, de termos de contratos e de outros instrumentos complementares, no âmbito da administração pública estadual;

- Decreto Estadual nº 57.033, de 23 de maio de 2023, que regulamenta os limites para o enquadramento dos bens de consumo nas categorias comum e luxo, nos termos do § 1º do art. 20 da Lei Federal nº 14.133, de 1º de abril de 2021;

- Decreto Estadual nº 57.037, de 23 de maio de 2023, que regulamenta, no âmbito da administração pública estadual direta, autárquica e fundacional, as modalidades de licitação concorrência e pregão, de que trata a Lei Federal nº 14.133, de 1º de abril de 2021;

- Decreto Estadual nº 57.036, de 23 de maio de 2023, que regulamenta no âmbito da administração pública estadual direta, autárquica e fundacional, o sistema de registro de preços de que trata a Lei Federal nº 14.133, de 1º de abril de 2021.

3 DA JUSTIFICATIVA

A Secretaria de Estado da Segurança Pública objetiva implementar o projeto atual junto ao projeto de cercamento eletrônico estadual do Programa Avançar, para fornecimento na modalidade de locação, instalação, configuração, operação assistida, treinamento e manutenção preventiva e corretiva durante o período de garantia, com inclusão de insumos, software de gerenciamento e equipamentos de videomonitoramento urbano, cercamento eletrônico, inteligência artificial, armazenamento, para municípios do Estado do Rio Grande do Sul.

Além disso, busca-se a disponibilização dos serviços de atualização e manutenção preventiva e corretiva de projetos desenvolvidos pela Secretaria da Segurança Pública com os Municípios. Por meio do Convênio 855949, o estado do Rio Grande do Sul adquiriu 151 pontos de videomonitoramento, 187 pontos de cercamento e 30 salas de controle para atendimento dos municípios de Alvorada, Cachoeirinha, Canoas, Esteio, Gravataí, Guaíba, Sapucaia do Sul, Harmonia, Novo Hamburgo, São Leopoldo, Sapiranga, Campo Bom, Lindolfo Collor, Dois Irmãos, Rio Pardo, Pântano Grande, Encruzilhada do Sul, Candelária, Venâncio Aires, Santa Cruz do Sul, Vera Cruz, Sobradinho, Cachoeira do Sul, Santa Maria, Parobé, Quaraí, Bento Gonçalves, Vacaria, São Francisco de Paula, Nova Prata, Encantado, Espumoso, Iraí, Cruz Alta, Não-me-toque e Ibirubá. O período de garantia dos equipamentos está terminado, sendo necessária a contratação do serviço de manutenção e atualização. Além disso, vários projetos de videomonitoramento foram desenvolvidos com recursos do programa Consulta Popular, os quais também demandarão tais serviços.

O projeto de cercamento eletrônico estadual do Programa Avançar compreende o conjunto de equipamentos e softwares que deverão ser instalados nas áreas dos municípios de Alvorada, Bento Gonçalves, Cachoeirinha, Canoas, Capão da Canoa, Caxias do Sul, Cruz Alta, Esteio, Farroupilha, Gravataí, Guaíba, Ijuí, Lajeado, Novo Hamburgo, Passo Fundo, Pelotas, Porto Alegre, Rio Grande, Santa Maria, São Leopoldo, Sapucaia do Sul, Tramandaí e Viamão.

O sistema a ser instalado será dedicado ao monitoramento e gravação de imagens e passagens veiculares, efetuando a análise de vídeo inteligente, permitindo recuperação de imagens gravadas em servidores de rede, acompanhamento de alvos, identificando a origem de objeto perdido e alterações de ambiente, entre outros recursos. Interagindo com outros subsistemas, disponibilizando imagens e alarmes, em tempo real e gravados, contemplando instalação lógica e elétrica, treinamento, garantia dos equipamentos em virtude de defeitos ou quebras durante o período de contratação, bem como reparo/substituição dos equipamentos, pelo período de 24 meses (vinte e quatro).

Toda essa infraestrutura é composta por câmeras IPs, switches, nobreaks, servidores, storages, fibras ópticas, conversores de fibra, desktops, e outros itens, além de insumos para instalação, fixação e operação da solução, constantes neste Termo de Referência.

Levando-se em consideração que o rompimento de trechos da rede pode comprometer o acesso a dezenas de pontos de monitoramento, faz-se necessária a manutenção contínua dos serviços de suporte e da rede de fibra, sendo os itens a serem contratados neste Termo de Referência imprescindíveis para a operacionalização eficaz do sistema durante toda a garantia.

Deste modo, fica evidenciada a necessidade de se contratar serviços especializados para lançamento de dutos, cabos e fornecimento e a instalação das câmeras, bem como para manutenção.

O gerenciamento destes servidores, deverá ser efetuado através da criação de uma estrutura de Nuvem Privada, onde esta nuvem será alocada para uso exclusivo da SSP/RS, na sede da SSP/RS ou em local indicado por esta. Dentre os benefícios difundidos da adoção deste modelo, destacam-se: redução de custos, elasticidade no uso dos recursos, redução da ociosidade dos recursos, agilidade na implantação de novos serviços, foco nas atividades finalísticas do negócio e uso mais inteligente da equipe de TI.

Em comparação aos proveitos da computação em nuvem, o modelo tradicional de provimento de recursos de TI, adotado pela maioria dos órgãos, com o uso de salas-cofre, salas seguras, e estrutura de TI imobilizada, torna-se dispendioso, com ociosidade, perda de escala e eficiência, riscos associados aos vários processos de aquisição e a falta de sincronismo e tempestividade dos mesmos, além de apresentar grande complexidade de operação e manutenção de equipamentos.

A continuidade dos serviços é um dos atributos principais a ser levado em conta pelos gestores, tendo em vista que a interrupção da prestação dos serviços públicos causaria transtornos aos administrados. O fato é amplamente difundido na Doutrina, onde se cita o insigne doutrinador Marçal Justen Filho, discorrendo acerca do tema: *"A continuidade do serviço retrata, na verdade, a permanência da necessidade pública a ser satisfeita. Ou seja, o dispositivo abrange os serviços destinados a atender necessidade"*

A disponibilidade de mão de obra especializada na manutenção garante a continuidade e aumento da vida útil da solução.

Para que não haja interrupção no funcionamento da solução é necessária a manutenção contínua dos componentes da solução, por este motivo, se faz necessário garantia com manutenção durante os meses de contrato, on-site;

A contratação proposta está em estreita consonância com a política de TIC da SSP-RS, tendo em vista a atualização tecnológica necessária ao bom andamento dos trabalhos desta Pasta e suas aplicações de missão crítica, compreendendo os seguintes objetivos estratégicos de acordo com o projeto transversal e estruturante RS Seguro:

- Combate ao crime;
- Políticas sociais preventivas;
- Qualificação do atendimento ao cidadão;
- Resposta qualificada à criminalidade;
- Prevenção, gestão de risco e respostas às emergências e desastres.

4 DA DESCRIÇÃO DA SOLUÇÃO

O Sistema de Segurança Pública do Estado do Rio Grande do Sul, através das ações integradas das Instituições que o compõem, conjuga esforços para o enfrentamento da criminalidade, objetivando proporcionar aos cidadãos riograndenses a paz social.

Desta forma, a missão institucional da Secretaria da Segurança Pública concretiza-se mediante as ações de seu planejamento estratégico cujo objetivo primeiro é garantir a preservação da vida e a incolumidade das pessoas, por meio de políticas multissetoriais, com ênfase na prevenção e repressão à criminalidade no Estado. Neste sentido, o Governo do Estado do Rio Grande do Sul, por meio da Secretaria de Segurança Pública, lançou o RS SEGURO – Programa Transversal e Estruturante de Segurança Pública. O programa possui medidas estruturantes, orientadas pelo tripé de diretrizes: Integração + Inteligência + Investimento Qualificado. O RS SEGURO atua com foco territorial, em áreas com indicadores de maior criminalidade e vulnerabilidade socioeconômica. O uso de novas tecnologias para o enfrentamento da criminalidade é um dos caminhos adotados. Desta forma, buscam-se investimentos na utilização de equipamentos de videomonitoramento, dotados de softwares de inteligência, os quais podem auxiliar fortemente nas atividades policiais. Desta forma, a Secretaria da Segurança Pública do Estado do Rio Grande do Sul, cumprindo sua missão institucional de preservar a ordem pública, garantindo os direitos fundamentais das pessoas, visando tornar a segurança pública do Estado um modelo de referência de paz social e garantia dos direitos fundamentais da pessoa, publicou, no ano de 2018, o projeto de cercamento e monitoramento eletrônico com recursos federais, que atende a 36 municípios.

Este projeto dotou os municípios de soluções voltadas à vigilância eletrônica, fazendo uso de câmeras com alta tecnologia, as quais não só realizam o monitoramento de locais, como também fazem a leitura de placas veiculares, buscando coibir ações delituosas, através do uso de inteligência artificial.

Completamente implantado, o projeto encontra-se plenamente funcional. Porém, para que haja continuidade na prestação de serviços, faz-se necessário a ampliação deste projeto inicial, bem como a contratação de serviços de manutenção, serviços estes que visam a continuidade do funcionamento da solução adotada pelo Estado.

Assim, o Sistema de Segurança Pública do Estado do Rio Grande do Sul, através das ações integradas das Instituições que o compõem, conjuga esforços para o enfrentamento da criminalidade, objetivando proporcionar aos cidadãos riograndenses a paz social.

O acerto na escolha adequada da solução de videomonitoramento e cercamento eletrônico leva a necessidade de ampliação dos locais monitorados. Desta forma, a contratação de novos equipamentos visa suprir esta carência.

Para tanto, visando a convergência das soluções, necessário se faz o lançamento de novo projeto o que possibilitará a expansão do sistema, de acordo com as necessidades de cada município atendido, além da necessária manutenção do funcionamento sobre os equipamentos existentes. Este projeto prevê a locação de equipamentos, soluções e serviços, divididos em dois grupos distintos, com os seguintes objetivos:

- Locação de novos pontos de videomonitoramento e cercamento eletrônico; e

- Contratação de serviços de manutenção de pontos de cercamento eletrônico, pontos de vídeo monitoramento e centrais de monitoramento existentes.

Com a contratação pretendida, poderá o Estado manter a estrutura existente, ampliando-a, a medida da necessidade, sempre perseguindo sua missão institucional de promover a paz social.

Além de simplesmente locar equipamentos para a ampliação dos sistemas, a Secretaria da Segurança Pública pretende dotar cada local com ferramentas tecnológicas que agreguem inteligência ao parque instalado. Para cumprir esta tarefa, serão implantados softwares que agreguem funções como:

- Análise inteligente da malha viária urbana

A placa é a identificação do veículo e está visível e sujeita à checagem, diferentemente do chassi, por exemplo; a captura e a avaliação da placa não requerem qualquer autorização do condutor, o que facilita seu uso. O reconhecimento de placas em tempo real permite a realização de processos quase que simultaneamente, identificando o que é a placa na imagem, visto que a foto inclui o carro e o entorno, reconhecendo o número da licença. Os dados são encaminhados aos equipamentos servidores de rede e, neles, é efetuada a mineração de dados, possibilitando a detecção de veículos suspeitos, confirmando hipóteses e álibis, ou até mesmo reconhecendo os padrões de um crime, por meio da análise da cena e do entorno, construindo, desta forma, muros virtuais nos municípios.

- Reconhecimento facial avançado

O reconhecimento facial baseado em inteligência artificial e redes neurais é capaz de fornecer o mais alto nível de segurança na análise de imagens. A rede neural é treinada para identificar características faciais únicas, para que possa encontrar rostos semelhantes no banco de dados. O algoritmo funciona com bancos de dados globais de rostos, permitindo uma pesquisa em frações de segundo. A tecnologia de reconhecimento facial é capaz de detectar um número ilimitado de rostos em um quadro, tornando-o uma solução ideal para garantir segurança em áreas lotadas.

- Análise forense

A análise tradicional de vídeos demanda investimento em tempo e pessoal. A tecnologia deve suprir esta lacuna, transformando horas de vídeo em minutos de análise, fornecendo recursos e ferramentas inovadoras para análise forense de vídeo e projetos de vigilância eletrônica. O sistema é capaz de reduzir o tempo de visualização de um determinado vídeo para fins de análise investigativa. Abreviando a análise de demoradas horas de vídeo em minutos, permitindo a fácil localização de indivíduos, objetos ou cenas específicas, a solução determina agilidade, objetividade e velocidade em sua busca, através da utilização de filtros de cor, tamanho, sentido e direção, horários, entre outros.

- Plataforma integrada de gestão, tratamento e apoio a tomada de decisão

Esta plataforma integrada de gestão é uma ferramenta que utiliza técnicas de coleta, análise e cruzamento de dados para fornecer informações relevantes para a tomada de decisões em relação à segurança pública.

O sistema deverá ser capaz de coletar dados de diversas fontes, como registros policiais, informações de inteligência, dados demográficos, econômicos e sociais, entre outros. Esses dados são armazenados em um banco de dados centralizado e são analisados por algoritmos de inteligência artificial, que identificam padrões e tendências relevantes para a segurança pública.

O sistema também integra dados de câmeras de segurança, sistema de reconhecimento facial, sistemas de monitoramento de tráfego e outras tecnologias, para fornecer informações em tempo real sobre a situação de segurança em uma determinada região.

Com base nas informações coletadas e analisadas, a plataforma deve ser capaz de gerar relatórios e visualizações de dados, que suportam os gestores de segurança a entender melhor as condições de segurança em uma determinada área e sendo base nas tomadas de decisões, a serem adotadas para melhorar a atuação da segurança pública.

A licitante vencedora deverá implementar esta plataforma integrada no ambiente a ser indicado pela SSP e integrar com as informações geradas pelos softwares de análise viária e reconhecimento facial, conforme a descritivo mínimo relacionados neste Termo de Referência.

Com a implementação da segunda fase do projeto de videomonitoramento e cercamento eletrônico, a Secretaria de Segurança Pública do Estado do Rio Grande do Sul avançará, a passos largos, na consecução de suas metas e visão institucional, tornando lugares melhores para pessoas melhores, através da tecnologia e da inteligência artificial.

4.1 DO VIDEOMONITORAMENTO URBANO

Deverá ser adotada solução composta por equipamentos e programas capacitados a capturar, analisar e gerir dados oriundos de câmeras de videomonitoramento. Esta solução deverá compreender diferentes tipos de câmeras.

Os softwares envolvidos deverão oferecer suporte aos seguintes sistemas de processamento de imagens:

- Reconhecimento facial

A solução a ser fornecida deverá conter solução de análise de vídeo e solução de reconhecimento facial. Deverá ser considerada a análise de ambientes, para verificação de fatores considerados anormais, do tipo análise comportamental, mensuração e análise de grupos de pessoas, sistema de investigação forense e verificação de sinopses de vídeos.

- Análise forense

A solução deverá contemplar recursos e ferramentas para análise forense de vídeos, com capacidade para reduzir o tempo de visualização de um determinado vídeo, para análise investigativa, na proporção de horas para minutos de vídeo, permitindo a fácil localização de indivíduos, objetos ou cenas específicas, propiciando agilidade, objetividade e velocidade na pesquisa, permitindo a utilização de filtros de cor, tamanho, sentido e direção, horários, entre outros.

- Detecção automática de faces humanas em fluxos vídeo

A solução de detecção automática de faces trata-se de uma aplicação computacional dedicada e especializada à detecção automática de faces humanas em fluxo vídeo (streaming) em tempo real, imagens estáticas e dinâmicas, com algoritmos para estabelecimento de biometria facial e comparação de similaridade entre as faces capturadas e aquelas cadastradas em listas de infectados com COVID-19, listas de foragidos, desaparecidos, Interpol e demais listas, para processamento de canais de fluxo de vídeo (streaming) oriundos de câmeras de monitoramento

fixas ou do tipo PTZ, ou mesmo de outras fontes como fotos de celulares, aplicados em logradouros públicos com alta circulação de pessoas.

- Área Segura

As câmeras serão dotadas de mecanismo luminoso de identificação visual a cores, incorporado à sua estrutura, visíveis inclusive durante o dia, para identificação de condições de segurança, operando no modo de exceção de "listas brancas", com base em análise inteligente de vídeo, detectando automaticamente situações de risco e informando visualmente, pela equivalência de cores, a situação detectada. Desta forma, os transeuntes poderão identificar facilmente, através das cores emitidas pelas câmeras, as condições de segurança do local.

- Análise de Vídeo

A análise de vídeo deve se concentrar em melhorar a capacidade de um centro de controle e gerenciar de forma econômica e mensurável grandes quantidades de vídeo em tempo real.

A plataforma de análise de vídeo precisa fornecer aos operadores da CENTRAL DE MONITORAMENTO informações contextuais na forma de alertas enriquecidos com metadados que permitam definir de forma inequívoca a origem do alerta no próprio vídeo. Isso permitirá identificar possíveis ameaças à segurança, desafios e oportunidades operacionais, violações de saúde e segurança do trabalho e conformidade regulatória, além de fornecer uma consciência situacional mais profunda, tudo em um único lugar.

No centro da plataforma de análise de vídeo está a análise de comportamento anômalo, que deve ser uma licença de análise de vídeo única e abrangente que substitui dezenas de licenças baseadas em regras individuais para diferentes cenários de uso. Esta licença única criará um alerta quando forem detectadas atividades anômalas que não atendam a um padrão esperado ou normal previamente aprendido pelo algoritmo de Inteligência Artificial, de forma totalmente autônoma e não supervisionada.

A plataforma de análise de vídeo também devera classificar os alertas utilizando *Deep Learning* para, em seguida, passá-los a um motor de regras, que permitirá desencadear uma série de ações, seja por parte dos operadores ou até de forma automática.

Os recursos de detecção de ameaças da plataforma de análise de vídeo deverão adicionalmente ser capazes de monitorar grandes áreas ou perímetros, detectando objetos em movimento. A solução deve emular a visão humana, onde prestamos mais atenção aos movimentos bruscos e menos atenção aos movimentos regulares. A plataforma de análise de vídeo deve ter a capacidade de rapidamente compreender a cena, permitindo concentrar-se em alvos reais e não em fatores ambientais comuns à cena, como movimento de árvores e reflexos na água. Com as configurações corretas, deverá ser capaz de detectar alvos pequenos e em movimento rápido, bem como alvos a grandes distâncias, de até 1 km.

4.1.1 FUNCIONALIDADE DOS PONTOS DE MONITORAMENTO ELETRÔNICO

Os Pontos de Monitoramento Eletrônico serão instalados em vias urbanas, rurais e estradas dos municípios, de acordo com as necessidades estabelecidas pelos órgãos técnicos da Segurança Pública.

O principal objetivo é promover ações preventivas de combate à criminalidade, auxiliar o efetivo tático no monitoramento/vigilância e subsidiar ações estratégicas aos agentes de segurança pública, reduzindo os índices de ocorrências registradas, inclusive no trânsito, bem como garantindo segurança e bem-estar à população do município.

4.1.2 COMPOSIÇÃO BÁSICA DO PONTO DE MONITORAMENTO ELETRÔNICO

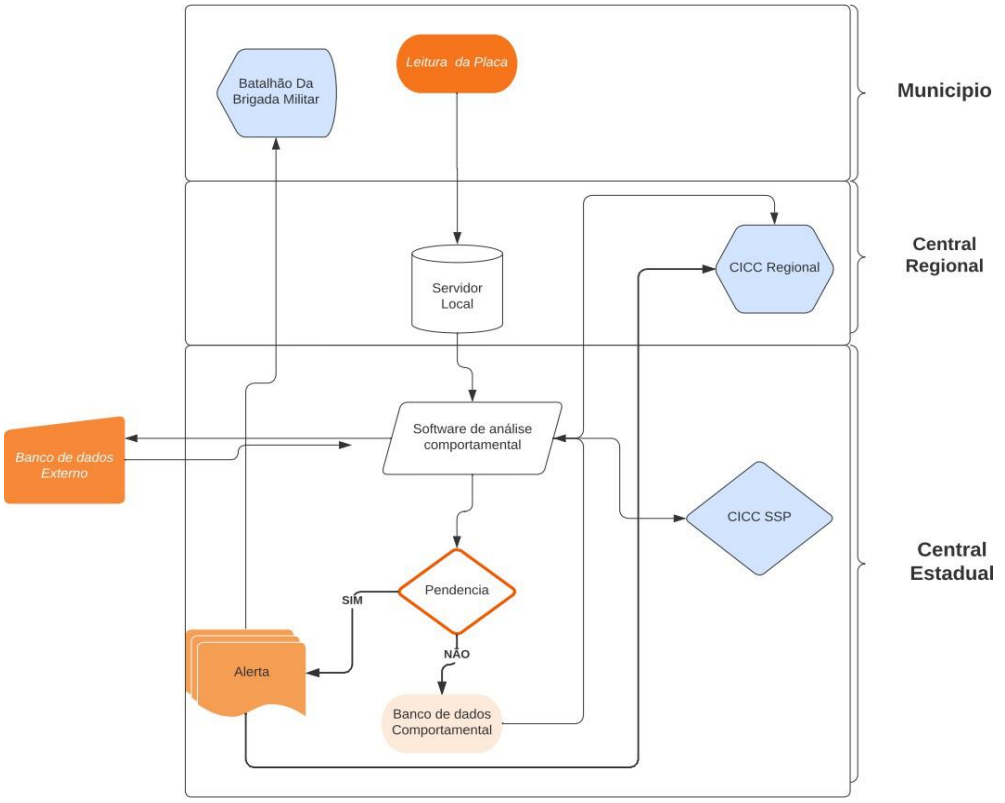
O Ponto de Monitoramento Eletrônico (PME) poderá variar de acordo com a realidade de cada local onde será instalado, sendo que estas variações não poderão implicar em aumento de custo do ponto, no entanto deverá ter, minimamente a seguinte composição:

- Uma câmera de videomonitoramento;
- Uma caixa porta equipamento;
- Um poste concreto cônico;
- Um suporte para câmera, quando for cabível;
- Um padrão para entrada de energia, que poderá variar de acordo com a concessionária local;
- Um conjunto de Nobreak, Switch/Conversor de mídia, e os respectivos cabos, dutos e conectores necessários ao perfeito funcionamento ponto de videomonitoramento;
- Um link de comunicação de dados. Esse link irá variar de local para local, mas deverá ligar o Ponto de Monitoramento Eletrônico à Central de Comando e Controle. A velocidade do link deverá ser previamente aprovada e terá com principio atender a demanda de fluxo de dados exigida pelos equipamentos e trafego de dados a ser mensurado com base nso equipamentos a serem instalados. As especificidades de cada ponto deverão constar no Projeto Executivo.
- Processamento e armazenamento – deverá estar devidamente alinhado e aprovisionado conforme as especificações previstas no item 4.2.3;

4.2 DO CERCAMENTO ELETRÔNICO

A solução deverá efetuar a leitura e reconhecimento de placas veiculares (LPR), permitindo compatibilização com o banco de dados do Estado, e os que ele tenha acesso por meio de acordo de cooperação, com a utilização do sistema ONE/CMV ou outro a ser definido pela SSP-RS, integrado à Base de Dados de Veículos Irregulares do DETRAN-RS.

Quando há a passagem de algum veículo por um dos pontos de coleta para cercamento eletrônico que serão instalados nos municípios, o sistema registra este fato, analisa a imagem, faz o reconhecimento da placa e outros metadados do veículos e envia, em tempo real, essas informações para um equipamento central, instalado na central do estado e este, por sua vez, submete a placa lida a Base de Dados de Veículos Irregulares do DETRAN, onde constam todos os veículos do Estado que não podem circular, inclusive os furtados e roubados. Uma vez constatado que se trata de um veículo irregular, o sistema enviará um alerta através do sistema para as Salas de Comando e Controle mais próximas, para que estas tomem as providências possíveis. Cada município que já possua um sistema próprio poderá integrar o sistema através de adesão ao SIM/RS.



4.2.1 SISTEMA OPERADOR NACIONAL DOS ESTADOS - ONE

Visando atender a necessidade do Fisco e contribuir com a redução do chamado “Custo Brasil”, foi concebido o projeto Brasil ID, um sistema baseado na tecnologia de identificação por radiofrequência (RFID – Radio-Frequency IDentification) que visa estabelecer um padrão único de identificação e monitoramento de produtos e documentos fiscais em circulação pelo país. O projeto conta com o apoio de diversas entidades, dentre elas a FINEP, Ministério da Ciência, Tecnologia e Inovação, Governo Federal, ENCAT e empresas parceiras.

Uma aplicação dessa tecnologia é a identificação veicular utilizando o RFID e a leitura da passagem desses veículos por antenas, ou SLD (sistema de Leitura de Dispositivo) distribuídas e operadas por parceiros credenciados como operadores do projeto Brasil ID.

Além do sistema baseado em radiofrequência, outras tecnologias se apresentam como aptas a contribuir nesse processo de identificação veicular e integração com os documentos fiscais, uma delas é a OCR (Optical Character Recognition) que permite a identificação de veículos através da imagem capturada das placas através de dispositivos instalados nas rodovias.

Uma vez identificado o veículo de carga, é possível fazer o link com o documento fiscal eletrônico responsável pela logística (MDF-e – Manifesto Eletrônico de Documentos Fiscais) e com base nessas informações munir a fiscalização de trânsito com instrumentos capazes de orientar as ações nos postos fiscais e rodovias do país.

O Operador Nacional dos Estados (ONE) surge nesse contexto como um concentrador das leituras dos SLD (participantes do projeto Brasil ID) e OCR que interessam à administração tributária.

As capturas das passagens dos veículos identificados deverão ser encaminhadas ao ONE que fará o papel de roteamento dessas informações disponibilizando para consulta aos estados e ao ambiente nacional do MDF-e.

O ambiente nacional do MDF-e usará a informação do ONE para gerar o evento de Registro de Passagem dos MDF-e abertos no momento da captura e ainda a propagação desses eventos nas Notas Fiscais Eletrônicas e Conhecimentos de Transporte Eletrônico carregadas no manifesto. Esse registro de passagem é de extrema importância para o trânsito de mercadorias uma vez que sua ocorrência impede o cancelamento do documento fiscal apontado.

Além disso, o ONE disponibilizará as leituras sobre carregamento, descarregamento ou percurso de mercadorias para que os estados relacionados no manifesto possam ter a informação do trânsito e desta forma consigam implementar ações preventivas de fiscalização ou mesmo trabalharem com um conceito de trânsito facilitado às empresas participantes do projeto, reduzindo assim, o tempo de parada nos postos fiscais e com isso reduzindo o custo operacional que esse tempo representa para empresas desse setor.

4.2.2 SISTEMA DE CONTROLE E MONITORAMENTO DE VEÍCULOS – CMV

O CMV é um sistema desenvolvido pela SEFAZ/RS (Secretaria da Fazenda) que tem por escopo permitir à Prefeitura Municipal, bem como aos Municípios integrantes do SIM/RS, o controle, em tempo real, de veículos em trânsito com irregularidades ou indicativos de envolvimento em delitos e a identificação de veículos não licenciados, possibilitando a abordagem efetiva e o cercamento eletrônico.

O projeto tem os seguintes objetivos:

- Compartilhar o uso da infraestrutura da Receita Estadual voltado ao monitoramento de veículos com a Secretaria de Segurança Pública;

- Utilizar NFes, cadastro de veículos, licenciamento, IPVA e comunicações de furto/ roubo como gatilhos para geração de alertas;

- Permitir o rastreamento de veículos de interesse da administração tributária ou segurança pública;

- Georreferenciar alertas apontados pelo sistema, criando mapeamento com os trajetos dos veículos;

- Visualizar o histórico de rastreamento das ocorrências detectadas.

- O projeto permitirá os seguintes ganhos de atuação:

- Aumento da presença do Estado por meio de recursos tecnológicos;

- Identificação e localização de veículos suspeitos;

- Redução da criminalidade e dos impactos e custos sociais;
- Controle de tráfego e melhor gestão da mobilidade urbana;

- Aumento na arrecadação através da identificação de veículos com IPVA vencido e/ou praticando infração de trânsito.

O sistema a ser fornecido pela contratada, além das demais características, deverá cobrir todas as funcionalidades do CMV utilizadas na Segurança Pública, possibilitando sua completa substituição sem prejuízo para os usuários.

4.2.3 SERVIDORES DE PROCESSAMENTO

A contratada deverá fornecer servidor/processamento equivalente, que atenda às especificações

de todos os softwares ofertados por ela durante todo o período do contrato, sendo que todos os equipamentos e softwares solicitados nos KITs deverão ser atendidos de forma plena pela solução entregue.

Para a mensuração técnica de configuração dos servidores de processamento e armazenamento deverão ser considerados as seguintes quantidades: 01 (um) Servidor para 01 (um) conjunto de 05 Kits de Pontos completos de Cercamento Eletrônico; 01 (um) Servidor para 01 (um) conjunto de 05 Kits de Pontos de videomonitoramento de Câmeras Fixas; 01 (um) servidor para 01 (um) conjunto de 05 Kits de Pontos de Videomonitoramento Câmera Speed Dome. Caso haja a contratação de mais de um serviço, ou seja, a aquisição de mais de um tipo de Kit (ex: Kit 01 + Kit 02), excetuando-se neste caso as manutenções, poderá a contratada unir os serviços de processamento e armazenamento em um só servidor, desde que suporte as demandas e funcionalidades dos softwares, garantindo um desempenho máximo e uma experiência satisfatória para os usuários.

Este requisito implica que a contratada seja responsável por disponibilizar um servidor que atenda aos requisitos mínimos estabelecidos pelos softwares oferecidos. O servidor fornecido deve ser capaz de suportar as demandas e funcionalidades dos softwares, garantindo um desempenho adequado e uma experiência satisfatória para os usuários.

É importante que a contratada forneça um serviço de servidor equivalente em termos de capacidade, poder de processamento, armazenamento e conectividade, considerando o aproveitamento de 100% (cem porcento) das especificações dos softwares oferecidos pelos fabricantes, sendo que o projeto executivo deverá propor benchmarks para análise desse ponto. Isso garantirá que os softwares funcionem corretamente e sem interrupções ao longo do período de contrato. A contratada deve prover o armazenamento de dados compatível com a necessidade para treinamento e aprendizado dos sistemas de inteligência artificial.

Além disso, a contratada deve se comprometer a manter o servidor em boas condições de funcionamento, realizar manutenções preventivas e corretivas, e garantir a disponibilidade adequada do servidor durante todo o período de contrato, bem como garantir todas as necessidades de Segurança da informação que sejam necessarias para esse ponto.

4.2.4 SISTEMA DE SEGURANÇA INTEGRADA COM OS MUNICÍPIOS - SIM

Trata-se de um sistema que interliga as estruturas de Segurança Pública já existentes no RS, criando uma doutrina única de formação de agentes de segurança, conectando as tecnologias, centralizando e racionalizando o atendimento ao cidadão como forma de aprimoramento da capacidade de resposta aos chamados de emergência.

Além disso, trabalha nas ações de reinserção de apenados na sociedade, nas ações de prevenção primária voltadas principalmente aos jovens e adolescentes, além de incentivar as parcerias público-privadas.

Esta estrutura irá contribuir para o sucesso das operações em conjunto, onde serão estabelecidos protocolos de atuação, aprimorando a capacidade de pronta resposta na realização de operações e ações rotineiras, de médio e grande porte, através de eixos de atuação: Prevenção, Operações Integradas, Inteligência, Capacitação e Treinamento, Integração de Tecnologias, Ressocialização de Apenados e Consepros.

4.2.5 FUNCIONALIDADE DOS PONTOS DE COLETA PARA CERCAMENTO ELETRÔNICO

A captura de imagens efetuada pelos pontos de coleta para cercamento eletrônico, relativas às

passagens veiculares devem atender aos seguintes requisitos:

- Detectar automaticamente as passagens veiculares por faixas de rolamento nos locais previamente definidos para a instalação de Pontos de Coleta para Cercamento Eletrônico (PCL);

- Capturar imagens que permitam a visualização da placa veicular e características do veículo, em ruas com largura de até três metros, mesmo se o veículo desloque lateralmente para qualquer um dos lados dentro dos limites das faixas sinalizadoras. Caso necessário, será adicionado um ponto a mais para atender o tamanho da via que será monitorada;

- Possibilitar a captura de imagens de veículos em aproximação (pela frente do veículo) e em afastamento (pela traseira do veículo);

- Enviar os dados coletados por meio de rede que utilize protocolo TCP/IP, tais como: placa do veículo em caracteres; características como cor, marca, modelo e tipo (sempre que possível); endereço da passagem com latitude e longitude e data e hora da passagem, referentes a cada passagem e exigidos pelo sistema de análise a ser fornecido;

- Funcionar no período noturno utilizando-se de iluminação que não ofusque os olhos e consequentemente não denunciando o local físico onde está sendo efetuada a coleta de imagens;

- As imagens enviadas ao servidor deverão ser coloridas durante o dia e pelo menos, em preto e branco durante a noite ou em períodos de baixa ou baixíssima luminosidade.

4.2.6 COMPOSIÇÃO BÁSICA DO PONTO DE COLETA PARA CERCAMENTO ELETRÔNICO

O Ponto de Coleta para Cercamento Eletrônico (PCL) poderá variar de acordo com a realidade de cada local onde será instalado, sendo que estas variações não poderão implicar em aumento de custo do ponto, no entanto deverá ter, minimamente a seguinte composição:

- Duas câmeras para captura de imagens veiculares (com lente);

- Um padrão para entrada de energia, que poderá variar de acordo com a concessionária local;

- Poste metálico projetado galvanizado a ser definido para cada local. Essas especificidades de cada ponto deverão constar do Projeto Executivo;

- Um link de comunicação de dados. Esse link irá variar de local para local, mas deverá ligar o Ponto de Monitoramento Eletrônico à Central de Comando e Controle. A velocidade do link deverá ser previamente aprovada e terá com principio atender a demanda de fluxo de dados exigida pelos equipamentos e trafego de dados a ser mensurado com base nso equipamentos a serem instalados. As especificidades de cada ponto deverão constar no Projeto Executivo.

Caberá à empresa vencedora da licitação integrar as câmeras de leitura e reconhecimento de placas veiculares fornecidas, com o Sistema Operador Nacional dos Estados – ONE / Sistema De Controle E Monitoramento De Veículos – CMV, ou outro a ser definido pela SSP-RS, o qual verifica a situação de irregularidade das placas lidas pelos Pontos de Coleta para Cercamento Eletrônico. Para tanto, será fornecido um manual de orientação para esta integração.

A empresa vencedora deverá desenvolver o Middleware (mediador) que consiste, no campo da computação distribuída, em um programa de computador que faz a mediação entre software e demais aplicações. É utilizado para mover ou transportar informações e dados entre programas de diferentes protocolos de comunicação, plataformas e dependências do sistema operacional.

A empresa vencedora deverá desenvolver o Middleware como melhor lhe aprouver, desde que a performance seja adequada. Entenda-se por performance adequada o menor tempo decorrido entre a passagem do veículo até o retorno do alerta no Sistema de Controle e Monitoramento de

Veículos, permitindo que a Central de Comando e Controle receba a informação da passagem veicular em "tempo real". Assim, quando um veículo for detectado em um Ponto de Coleta para Cercamento Eletrônico, este deverá enviar as informações ao sistema, retornando um alerta aos operadores no caso de irregularidade, permitindo assim a tomada de decisão de forma imediata.

A extração de caracteres alfanuméricos das placas veiculares deverá possuir um índice mínimo de 90% de leituras corretas, considerando-se imagens eleitas como legíveis.

As imagens eleitas como legíveis devem perfazer um índice mínimo de 95% das passagens de veículos pelo dispositivo, em todos os períodos do dia, com velocidade de até 140 km/h (cento e quarenta quilometros por hora). As imagens não eleitas como legíveis também deverão ser enviadas para o sistema, a fim de passarem por processo de Inteligência Artificial para obtenção de informações úteis referente à passagem, tais como: características do veículo, ocultação intencional ou não da placa, condições irregulares de circulação, comportamentos considerados suspeitos, entre outros possíveis.

4.3 DA INTELIGÊNCIA ARTIFICIAL

Além de simplesmente adquirir equipamentos para a ampliação dos sistemas, a Secretaria da Segurança Pública pretende dotar cada local com ferramentas tecnológicas que agreguem inteligência ao parque instalado. Para cumprir esta tarefa, serão implantados softwares que agreguem funções como:

- Análise inteligente da malha viária urbana

A placa é a identificação do veículo e está visível e sujeita à checagem, diferentemente do chassi, por exemplo; a captura e a avaliação da placa não requerem qualquer autorização do condutor, o que facilita seu uso. O reconhecimento de placas em tempo real permite a realização de processos quase que simultaneamente, identificando o que é a placa na imagem, visto que a foto inclui o carro e o entorno, reconhecendo o número da licença. Os dados são encaminhados aos equipamentos servidores de rede e, neles, é efetuada a mineração de dados, possibilitando a detecção de veículos suspeitos, confirmando hipóteses e álibis, ou até mesmo reconhecendo os padrões de um crime, por meio da análise da cena e do entorno, construindo, desta forma, muros virtuais nos municípios.

- Reconhecimento facial avançado

O reconhecimento facial baseado em inteligência artificial e redes neurais é capaz de fornecer o mais alto nível de segurança na análise de imagens. A rede neural é treinada para identificar características faciais únicas, para que possa encontrar rostos semelhantes no banco de dados. O algoritmo funciona com bancos de dados globais de rostos, permitindo uma pesquisa em frações de segundo. A tecnologia de reconhecimento facial é capaz de detectar um número ilimitado de rostos em um quadro, tornando-o uma solução ideal para garantir segurança em áreas lotadas.

- Análise forense

A análise tradicional de vídeos demanda investimento em tempo e pessoal. A tecnologia deve suprir esta lacuna, transformando horas de vídeo em minutos de análise, fornecendo recursos e ferramentas inovadoras para análise forense de vídeo e projetos de vigilância eletrônica. O sistema é capaz de reduzir o tempo de visualização de um determinado vídeo para fins de análise investigativa. Abreviando a análise de demoradas horas de vídeo em minutos, permitindo a fácil localização de indivíduos, objetos ou cenas específicas, a solução determina agilidade, objetividade e velocidade em sua busca, através da utilização de filtros de cor, tamanho, sentido e direção, horários, entre outros.

- Análise de imagens com placas não legíveis

As imagens das câmeras, tanto de videomonitoramento urbano (quando selecionadas) quanto de

cercamento eletrônico não eleitas como legíveis, deverão passar por processo de Inteligência Artificial para obtenção de informações úteis referente à passagem, tais como: características do veículo (marca, cor, modelo, tipo, adesivos ocultação intencional ou não da placa, condições irregulares de circulação, entre outros possíveis. Estas informações deverão estar disponíveis tanto para o sistema de alerta em tempo real quanto para análise posterior.

4.4 DAS LICENÇAS DE USO

A Contratada deverá entregar os softwares à Contratante, devidamente especificadas as características de licenças, contendo informações inequívocas sobre: perpetuidade das licenças, inexistência de restrições de licenciamento para uso dos softwares de qualquer natureza, como número de documentos, número de usuários, quantidade de recursos computacionais (CPU, memória, etc.) dos equipamentos onde o software será instalado.

A Contratada deverá apresentar todas as licenças de softwares, bem como todas as licenças e bancos de dados necessários para o pleno funcionamento de toda a solução ofertada.

4.5 DAS ESPECIFICAÇÕES TÉCNICAS PARA EXECUÇÃO DA INFRAESTRUTURA

Todos os materiais, salvo o disposto em contrário pelo CONTRATANTE, serão fornecidos pela CONTRATADA.

Todos os materiais a serem empregados nas instalações deverão ser novos e satisfazer a todas as condições estipuladas neste Termo de Referência.

A CONTRATADA só poderá usar qualquer material depois de submetê-lo ao exame e aprovação do CONTRATANTE, a quem caberá impugnar o seu emprego, quando em desacordo com as especificações.

As amostras de materiais aprovadas pela CONTRATANTE deverão ser cuidadosamente conservadas até o fim dos trabalhos, de forma a facultar, a qualquer tempo, a verificação de sua perfeita correspondência aos materiais fornecidos ou já empregados.

Obriga-se a Contratada a retirar do recinto das obras os materiais porventura impugnados pelo CONTRATANTE , dentro de 72 horas, sendo expressamente proibido manter no recinto das obras quaisquer materiais que não satisfaçam a estas especificações.

Todos os materiais e/ou equipamentos fornecidos pela Contratada deverão atender, quando aplicáveis, às especificações, normas e recomendações da ABNT, INMETRO, e de demais normas técnicas e/ou segurança, devidamente aprovados pelo CONTRATANTE .

É vedada a utilização de materiais e/ou equipamentos improvisados e/ou usados, em substituição aos tecnicamente indicados para o fim a que se destinam, assim como não será tolerado adaptar peças, seja por corte, furo ou outro processo, de modo a utilizá-las em substituição às peças recomendadas e de dimensões adequadas.

Quando houver motivos ponderáveis para a substituição de um material e/ou equipamento especificado por outro, a Contratada, em tempo hábil, apresentará, por escrito, ao CONTRATANTE, a proposta de substituição, instruindo-a com as razões determinadas do pedido de orçamento comparativo, de acordo com o que reza o contrato entre as partes sobre a equivalência.

5 VIGÊNCIA CONTRATUAL

A vigência contratual será conforme previsão editalícia.

6 DA PLANILHA ESTIMATIVA DE CUSTOS E PROPOSTA FINANCEIRA – MODELO

Código GCE	Item	Descrição	Valor Kit Unit Mensal	Valor Total Mensal
0117.0749.000021	1	KIT - Ponto completo de Cercamento Eletrônico composto por:		
	1.1	Ponto de Cercamento	R$	R$
	1.2	Licença de Software Análise Comportamental		
	1.3	Serviços de Locação de Link de Dados - Tipo I		
	2	KIT - Ponto de Videomonitoramento Câmera Fixa composto por:		
0117.0749.000022	2.1	Ponto de Videomonitoramento - Câmera Fixa Tipo I	R$	R$
	2.2	Licença de Software de VMS		
	2.3	Licença de Software de Análise Forense		
	2.4	Licença de Software Reconhecimento Facial		
	2.5	Serviços de Locação de Link de Dados - Tipo I		
	3	KIT - Ponto de Videomonitoramento Câmera Speeddome composto por:		
0117.0749.000023	3.1	Ponto de Videomonitoramento - Câmeras SpeedDome Tipo II	R$	R$
	3.2	Licença de Software de VMS		
	3.3	Serviços de Locação de Link de Dados - Tipo I		
	4	KIT - Manutenção e conectividade de sistema existente		
0117.0736.000007	4.1	Manutenção Ponto de videomonitoramento / cercamento eletrônico	R$	R$
	4.2	Serviços de Locação de Link de Dados - Tipo I		
	5	KIT - Conexão de Espelhamento e manutenção do sistema		
0117.0736.000006	5.1	Serviços de Locação de Link de Dados - Tipo II	R$	R$
	5.2	Manutenção em Sala de Comando e Controle (Cercamento)	R$	R$
Total mensal				R$
Total Global 24 meses				R$

Para a presente contratação não será estabelecido a quantidade mínima de KIT a ser cotada, por se tratar de uma solução que embasa o projeto de cercamento eletrônico estadual do programa Avançar para os municípios elencados neste Termo de Referência, contendo interrelação entre os serviços e bens contratados com gerenciamento centralizado, onde proporcionará maior concorrência, uma vez que as licitantes que exercem suas atividades no ramo, detém todos os serviços e materiais para entrega da solução pretendida pela Administração.

Para a mensuração de valor e cálculo para o serviço a ser contratado deverão ser consideradas as seguintes quantidades: 01 (um) Servidor para 01 (um) conjunto de 05 Kits de Pontos completos de Cercamento Eletrônico; 01 (um) Servidor para 01 (um) conjunto de 05 Kits de Pontos de videomonitoramento de Câmeras Fixas; 01 (um) servidor para 01 (um) conjunto de 05 Kits de Pontos de Videomonitoramento Câmera Speed Dome. Caso haja a contratação de mais de um serviço, ou seja, a aquisição de mais de um tipo de Kit (ex: Kit 01 + Kit 02), excetuando-se neste caso as manutenções, poderá a contratada unir os serviços de processamento e armazenamento em um só servidor, desde que suporte as demandas e funcionalidades dos softwares, garantindo o desempenho máximo e uma experiência satisfatória para os usuários.

Os valores referenciais estimados foram obtidos mediante pesquisa de mercado e de preços públicos.

6.1 DA PROPOSTA FINANCEIRA

A empresa licitante, deverá fornecer sua proposta financeira, de acordo com o modelo de planilha estimativa de custos acima descritos, devendo expressamente informar, sob pena de desclassificação:

- Marca e modelo de todos os itens que compõem a solução (não sendo aceitos títulos como:

outros, vários, “conforme edital” ou outros títulos genéricos que possam gerar dúvidas.
- Estão incluídos na proposta todos os custos, diretos, indiretos, tributos, lucro, frete, e todas as despesas necessárias para a formação de seu preço;
- Validade da proposta de 60 dias após a expedição;
- Deve estar acompanhada dos prospectos técnicos, datasheet, folheto e quais quer outros documentos pertinentes a validação técnica do presente termo de referência.

7 DA GARANTIA DOS BENS E SERVIÇOS

A garantia abrangerá todos os materiais e serviços de instalação, por todo período de contrato, contados a partir da emissão do Termo de Recebimento Definitivo da solução.

A garantia dos materiais fornecidos consistirá no atendimento dos chamados técnicos da CONTRATANTE para resolução de dúvidas, panes, falhas ou não conformidade técnicas referentes ao uso, funcionamento, desempenho e à performance dos equipamentos, acessórios, periféricos e da camada lógica (softwares, microcódigos, firmware ou qualquer outro código de programa que seja parte integrante do equipamento ofertado) que integram o projeto “Segurança Pública Inteligente”.

Nos casos em que as garantias dos fabricantes forem maiores do que as exigidas no neste Termo de Referência, deverá ser considerada a garantia do fabricante.

Durante o período de garantia, a Contratada deverá atender aos chamados e realizar os serviços necessários, nos prazos definidos neste Termo de Referência, contados a partir da notificação. Para tanto, a Contratada deverá disponibilizar sistema de abertura de chamados via web, que atenda as características descritas adiante.

Nos finais de semana, feriados e fora do horário comercial, a Contratada poderá ser acionada pela CONTRATANTE , em caráter emergencial para atender demandas de manutenção corretiva em pontos de captura, que ainda se encontrem cobertos pela garantia.

8 DAS ROTINAS DE EXECUÇÃO

A Contratada deverá executar os serviços obrigatoriamente nos prazos estipulados neste Termo de Referência e indicar formalmente preposto apto a representá-la junto à CONTRATANTE , que deverá responder pela fiel execução do contrato.

A Contratada deverá fornecer projeto “As Built” das soluções entregues, refletindo as configurações dos equipamentos e sistemas instalados.

A rotina de execução deve possuir os seguintes controles que serão desenvolvidos pela Contratada, e atualizados periodicamente:

- Relatório Quinzenal de acompanhamento - RQ;
- Cronograma Detalhado de Atividades do Projeto;
- Relação de Pendências;
- Relatório Mensal de Acompanhamento.

9 DOS NÍVEIS DE SERVIÇOS

9.1 DO SUPORTE TÉCNICO AOS EQUIPAMENTOS DURANTE O PERÍODO DE GARANTIA

A Contratada deverá ofertar suporte técnico para todos os equipamentos, softwares, materiais e

serviços fornecidos, assegurando prazos de atendimentos compatíveis com a instalação, ou seja, 24 (vinte e quatro) horas por dia e 7 (sete) dias por semana (à exceção dos chamados de Severidade 5).

O atendimento aos chamados deverá obedecer à seguinte classificação quanto ao nível de severidade:

ACORDO DE NÍVEIS DE SERVIÇOS - SLA

SEVERIDADE	DESCRIÇÃO	TIPO DE ATENDIMENTO	TEMPO DE ATENDIMENTO	TEMPO DE SOLUÇÃO OU CONTORNO	OBSERVAÇÃO	PENALIDADES
1 – Crítica	Chamados referentes a situações de emergência ou problema crítico, caracterizados pela existência de ambiente paralisado.	Híbrido	No máximo 2 (duas) horas corridas após a abertura do chamado, incluindo percurso do técnico até as instalações do CONTRATANTE .	No máximo 8 (oito) horas corridas após a abertura do chamado.	O atendimento não poderá ser interrompido até o completo restabelecimento do produto envolvido, mesmo que se estenda por períodos noturnos e dias não úteis.	O não atendimento dentro do prazo estabelecido para o chamado ensejará aplicação de multa à Contratada no valor de 0,5% (cinco décimos por cento) do valor constante no contrato para o item (equipamento) correspondente, por hora ou fração de hora de atraso.
2 – Alta	Chamados associados a situações de alto impacto, incluindo os casos de degradação severa de desempenho.	Híbrido	No máximo 2(duas) horas corridas após a abertura do chamado, incluindo percurso do técnico até as instalações do CONTRATANTE .	No máximo 12 (doze) horas corridas após a abertura do chamado.	O atendimento não poderá ser interrompido até o completo restabelecimento do produto envolvido, mesmo que se estenda por períodos noturnos e dias.	O não atendimento dentro do prazo estabelecido para o chamado ensejará aplicação de multa à Contratada no valor de 0,4% (quatro décimos por cento) do valor constante no contrato para o item (equipamento) correspondente, por hora ou

						fração de hora de atraso.
3 – Média	Chamados referentes a situações de baixo impacto ou para aqueles problemas que se apresentem de forma intermitente, incluindo os casos em que haja necessidade de substituição de componente(s) que possua(m) redundância.	Híbrido	No máximo 4 (quatro) horas corridas após a abertura do chamado.	No máximo 24 (vinte e quatro) horas corridas após a abertura do chamado.	A Contratada deverá colocar à disposição do CONTRATANTE um especialista devidamente habilitado e credenciado que trabalhará o tempo que for necessário para a solução do problema, sendo que o ônus financeiro de tal providência será da Contratada.	O não atendimento dentro do prazo estabelecido para o chamado ensejará aplicação de multa à Contratada no valor de 0,2% (dois décimos por cento) do valor constante no contrato para o item (equipamento) correspondente, por hora ou fração de hora de atraso.
4 – Média	Chamados com objetivo de solicitar acompanhamento técnico presencial para o desligamento e posterior ligamento do(s) equipamento(s), em virtude de atividade programada.	Híbrido	No máximo 4 (quatro) horas corridas após a abertura do chamado.	Conforme agendamento	O atendimento deverá ser realizado conforme agendamento, mesmo que contemple períodos noturnos e dias não úteis.	O não atendimento dentro do prazo estabelecido para o chamado ensejará aplicação de multa à Contratada no valor de 0,2% (dois décimos por cento) do valor constante no contrato para o item (equipamento) correspondente, por hora ou fração de hora de atraso.
5 - Baixa	Chamados com o objetivo de sanar dúvidas quanto ao uso ou à	Híbrido	No máximo 24 (vinte e quatro) horas	No máximo 72 (setenta e duas) horas corridas após	Os chamados classificados com Severidade 5 serão atendidos	O não atendimento dentro do prazo estabelecido

	implementação do produto.		corridas após a abertura do chamado.	a abertura do chamado.	em horário comercial, ou seja, das 08:00 horas às 18:00 horas, de segunda-feira a sexta-feira, horário de Brasília.	para o chamado ensejará aplicação de multa à Contratada no valor de 0,1% (um décimo por cento) do valor constante no contrato para o item (equipamento) correspondente, por hora ou fração de hora de atraso.

Será aberto um chamado técnico para cada problema reportado, sendo iniciada a contagem do tempo de atendimento a partir da hora de acionamento.

A manutenção deverá observar os seguintes requisitos:

- Abertura de chamados:

o Os chamados deverão ser efetivados através de sistema web, fornecido pela Contratada, onde a CONTRATANTE iniciará a abertura da Ordem de Serviço (O.S);

o O sistema web abrirá automaticamente uma O.S. para a Contratada, registrando data e hora do envio, assim como o monitoramento e andamento da demanda, bem como enviará o status do serviço realizado à CONTRATANTE , atendendo ao SLA - Service Level Agreement, ajustado neste Termo de Referência.

- A execução dos serviços deverá obedecer rigorosamente:

o Às normas e especificações constantes do documento da contratação, emitido pela CONTRATANTE ;

o Às normas da Associação Brasileira de Normas Técnicas;

o Às prescrições e recomendações dos fabricantes;

o Às normas internacionais consagradas, em caso de falta de normatização da Associação Brasileira de Normas Técnicas;

o A manutenção do sistema web de Abertura de Chamados, será de inteira responsabilidade da empresa Contratada, ou seja, o funcionamento deverá ocorrer de forma ininterrupta.

Caso a Contratada não consiga solucionar o atendimento no prazo estabelecido na tabela acima, a mesma deverá justificar em relatório destinado ao Executor do Contrato, para fins de avaliação do

prazo do atendimento.

Os serviços prestados pela Contratada terão início a partir da assinatura do contrato.

9.2 DAS ROTINAS

A Contratada deverá obedecer às seguintes rotinas na prestação dos serviços:

- A execução dos serviços ocorrerá mediante aprovação de projeto executivo apresentado pela Contratada no prazo 05 (cinco) dias corridos, após recebimento da ordem de serviço;

- O prazo de início para a execução dos serviços deve ser de no máximo 30 (trinta) dias corridos, contados a partir da solicitação formal da CONTRATANTE , incluída nesse prazo a elaboração e aprovação do Projeto Executivo;

- O prazo de conclusão de entrega da solução, não deve ultrapassar 180 (cento e oitenta) dias corridos, a contar da data de recebimento da Ordem de Serviço, podendo ser prorrogado a critério da CONTRATANTE , mediante provocação.

A Contratada deverá fornecer, instalar e certificar a infraestrutura de fibras ópticas, conforme todas as especificações do Termo de Referência.

9.3 DO SOFTWARE DE ATENDIMENTO DE ACORDO DE NÍVEL DE SERVIÇO

A empresa contratada deverá disponibilizar e manter durante, a vigência do contrato, para fornecimento da solução de manutenção, um software de atendimento para acordo de níveis de serviços das ocorrências geradas pelos sistemas.

9.4 DA TRANSIÇÃO CONTRATUAL

A Transição Contratual, entendida como o processo de transferência dos conhecimentos e competências necessárias para prover a continuidade dos serviços contratados ou executados, terá início 60 (sessenta) dias antes do prazo previsto para a extinção do contrato.

Em até 45 (quarenta e cinco) dias antes do prazo previsto para a extinção do contrato, a Contratada deverá entregar à CONTRATANTE Plano de Transição Contratual detalhado, com todas as atividades e projetos necessários para esta fase, devendo conter, no mínimo:

- Identificação do ambiente de trabalho em que atua a equipe de transição, seus papéis, responsabilidades, nível de conhecimento e qualificações;

- Cronograma detalhado do Plano de Transição, identificando: as tarefas, os processos, os recursos, marcos de referência, o início, o período de tempo e a data prevista para término;

- Estruturas e atividades de gerenciamento da transição, as regras propostas de relacionamento da contratada com a CONTRATANTE e com a futura prestadora de serviços;

- Plano próprio de gerenciamento de riscos, de contingência e de acompanhamento, todos relativos ao processo de transição;

O Plano de Transição Contratual traduz a estratégia empresarial de cada contratada e deve registrar e detalhar o método de trabalho adotado na execução dos serviços desenvolvidos.

Em ocorrendo nova licitação, com mudança de fornecedor dos serviços, a Contratada deverá repassar para a vencedora do novo certame, por intermédio de eventos formais, os documentos necessários à continuidade da prestação dos serviços, bem como esclarecer dúvidas a respeito de procedimentos no relacionamento entre o CONTRATANTE e a nova contratada.

Durante o tempo requerido para desenvolver e executar o Plano de Transição, a Contratada deve se responsabilizar por qualquer recurso ou esforço adicional que necessite estar dedicado somente à tarefa de completar a transição.

Por esforço adicional entende-se: pesquisas, transferência de conhecimento (entre a Contratada e o prestador de serviços futuro), customizações do sistema, manutenções evolutivas, documentação ou qualquer outro esforço passível de cobrança vinculado à tarefa de transição.

É de responsabilidade da CONTRATANTE a disponibilidade dos recursos qualificados identificados no Plano de Transição como receptores do serviço.

10 DA POLÍTICA DE SEGURANÇA DA INFORMAÇÃO, SEGURANÇA CIBERNÉTICA, INTEGRIDADE E ÉTICA

10.1 POLÍTICAS

As Políticas de Segurança da Informação e Compliance serão definidos de forma conjunta entre CONTRATANTE e Contratada seguindo os parâmetros definidos neste Termo de Referência, a fim de garantir a segurança, integridade e disponibilidades dos dados e sistemas assim como das instalações e equipamentos utilizados na prestação dos serviços.

As Políticas de segurança da informação devem ser desenvolvidas e implantadas de forma transparente aos colaboradores da Contratada e servidores da CONTRATANTE trazendo o Compliance para a operação a fim de garantir o cumprimento das políticas de segurança e mitigar possíveis vazamentos de dados e acessos indevidos. Fica a cargo da Contratada prover todo o treinamento de pessoal necessário a implantação da Política de Segurança da Informação

A Política de Segurança da Informação deve levar em conta todas as necessidades da LGPD (13.709/2018), utilizando arquitetura Zero Knowledge e a inclusão de um sistema de firewall específico e exclusivo para bases de dados, utilizar criptografia AES 256 bits (Equivalente ou Superior) entre outras medidas que visam trazer significativo ganho de segurança sem perder desempenho ou criar limitações de acesso, trabalhando com múltiplas camadas de segurança sistêmica, utilizando criptografia de ponta a ponta em toda a plataforma e transmissão.

A política de segurança da informação, segurança cibernética e tecnologia implementada devem se adequar a qualquer alteração necessária por força de regulação, regulamentação ou alteração na legislação vigente além das já previstas no Termo de Referência.

A segurança não deve impactar o desempenho dos sistemas ou causar lentidão, delay, latência significativa que prejudique a usabilidade e experiência dos usuários, a segurança deve ser proativa contando com identificadores de intrusão e ação suspeita, toda a comunicação e acesso devem ser protegidos com criptografia a fim de impedir a interceptação dos dados, criando uma proteção de múltiplas camadas de segurança de forma a criar a segurança dos dados e sistemas mesmo quando

acessado através de redes não seguras (Redes Pública, Internet).

Deve existir uma segmentação entre o que é acessível através de redes não seguras e redes seguras, mesmo que os sistemas e dados sejam trafegados com segurança graças às múltiplas camadas de segurança é interessante a segmentação para evitar o vazamento de dados podendo ser trabalhado em conjunto com controles de acesso físicos nos locais onde existe acesso total às funções e dados dos sistemas, sendo limitadas apenas pelos níveis de acesso (permissões/privilégios) de cada usuário.

O acesso às partes da plataforma que tratam de dados sigilosos, sensíveis ou pessoais só devem ser acessíveis em locais seguros, entretanto deve ser possível alterar essa regra em caso de necessidade (Ex.: Catástrofe) para que as operações se mantenham ativas mesmo que os centros operacionais se encontrem inutilizados.

Deve ser instalado controle de acesso aos ambientes de forma a controlar o acesso físico e impedir o vazamento de dados por observação de tela (quando não é necessário copiar os arquivos é só esquecer aberto), todas as estações e equipamento que farão acesso aos sistemas e dados que compõem a plataforma devem bloquear automaticamente quando o agente de monitoramento se afastar (evitando o esquecer aberto), utilizando múltiplos sistemas (métodos) no controle de acesso.

10.2 COMPLIANCE

Devem ser definidos processos claros a serem seguidos para garantir a segurança das informações, exemplo de processos para solicitações, controle, atendimento, auditoria e recuperação de desastres (DRP).

Todos os processos e regras devem ser claros e conhecidos por todos, mostrando em detalhes como funciona, quais os limites, o que se aplica e quando, automatizando o processo e eliminando a pessoalidade do processo. A automação administrativa deve compor a base do compliance eliminando que usuários administradores utilizem seus privilégios para benefício próprio, trazendo uma análise automática e imparcial baseada em variáveis que compõem o processo.

10.3 LGPD

As Políticas de Segurança da Informação devem trazer segurança à sociedade de que seus dados estão seguros e não serão utilizados de forma irregular, mormente no que tange à Lei Geral de Proteção de Dados, não sendo compartilhado e tratado de qualquer forma, Termo de não compartilhado com terceiros e quando não trouxer qualquer benefício significativo à sociedade.

Deve evidenciar que a cooperação entre poder público e iniciativa privada é benéfica a sociedade e como pode ser feita sem ser invasiva a privacidade, trazendo ganhos a sociedade, aumentando a segurança no perímetro urbano e trazendo efeitos indiretos nos serviços oferecidos à população como a redução dos custos do seguros entre outros benefícios indiretos já conhecidos e associados a inteligência, automação, tecnologia e informação combinados na gestão pública, deixando o poder público mais proativo e eficiente com uma tomada de decisão mais assertiva e rápida levando para o passado a reatividade como normalmente se vê, sem resolver as causas.

Deve deixar claro como os dados serão capturados, tratados (quando, por quem e em que condições) e com quais objetivos, essa parte da política será complexa visto o grande número de integrações e dados que estarão na plataforma, entretanto será necessária para que possamos

passar segurança à população em relação a sua privacidade ao utilizar este grande volume de dados sensíveis.

10.4 POLÍTICA DE SEGURANÇA DA INFORMAÇÃO (PSI)

10.4.1 INTRODUÇÃO

Este documento institui a Política de Segurança da Informação e tem o compromisso com a proteção de ativos de informação visando garantir a confidencialidade, integridade e disponibilidade das informações, por meio dos padrões, procedimentos e controles instituídos neste documento, garantindo a transparência no tratamento de dados e estabelecendo as diretrizes para o tratamento de dados visando assegurar a privacidade e os demais direitos individuais previstos na LGPD.

A política de segurança da informação poderá ser alterada a cada ciclo de 6 meses durante as revisões semestrais visando melhor atender as necessidades e adequar aos novos cenários com o aperfeiçoamento contínuo dos procedimentos e processos, tendo em vista a previsão de expansão gradual desta plataforma e sua dinamicidade.

10.4.2 OBJETIVO

Este documento de Política de Segurança da Informação visa descrever regras, conceitos, estabelecer diretrizes e procedimentos para o uso de ativos da informação, a fim de garantir a confidencialidade, integridade e disponibilidade das informações visando assegurar a privacidade e os demais direitos individuais previstos na LGPD. Esta política se aplica aos seguintes ativos:

- Ativos de Informação
- Ativos de Software
- Ativos Físicos

10.4.3 ABRANGÊNCIA

A Política de Segurança da informação deve estar disponível para que seu conteúdo possa ser consultado a qualquer momento, aplicando-se a todos os funcionários, diretores, estagiários, terceirizados e qualquer outra pessoa envolvida nos processos e atividades que se aplica esta política de segurança da informação.

10.4.4 DIRETRIZES

As diretrizes da política de segurança da informação (PSI), regem a conduta e o comportamento em relação a temas de segurança, visando garantir detalhadamente a política de segurança da informação, utilizando normas e procedimentos para garantir os demais direitos individuais previstos na LGPD (Lei nº 13.709/2018), podendo ser utilizadas, como referência, medidas

adotadas em outras implementações de sistemas de tratamento de dados sensíveis que requerem segurança, integridade, disponibilidade e transparência, implementando mecanismos na infraestrutura e nos sistemas com o propósito de ampliar estas garantias.

A solução deve possuir criptografia de ponta a ponta, manter a informação armazenada segura e encriptada utilizando a Zero Knowledge e criptografia AES 265 bits (semelhante ou superior), em blocos segregados impedindo o acesso a informação não criptografada mesmo em caso de ataque/invasão da solução utilizando múltiplas camadas de segurança criando barreiras inclusive de ataque internos por equipamentos infectados, deve ainda acompanhar a atividade dos agentes e garantir que não ocorra utilização inadequada da solução dos mesmos, todos os logs da solução devem permanecer armazenados para auditoria de órgãos de controle e transparência.

Qualquer falha na segurança dos dados tratados em tecnologias de reconhecimento facial pode ter consequências graves para os titulares dos dados, como a divulgação ou o compartilhamento não-autorizado de dados pessoais (e sensíveis) que, em certas ocasiões, geram danos tão relevantes que não podem ser corrigidos.

Nesse sentido, é necessário implementar fortes medidas de segurança, tanto em nível técnico como em nível organizacional, para proteger os dados de reconhecimento facial e garantir sua integridade dentro da finalidade a que aquele tratamento correlaciona. Como tais dados são alvo constante de ataques cibernéticos variados, as entidades devem sempre tomar medidas preventivas para evitar ataques específicos e manter um plano de medidas corretivas e mitigadoras, além de contar com equipe especializada no tema.

10.4.5 TRATAMENTO DA INFORMAÇÃO

A informação deve ser protegida contra acesso de pessoas não autorizadas garantindo a autenticidade das informações, devendo ser utilizados somente recursos autorizados e de pessoas com direito de acesso para garantir a segurança quando for necessário.

10.4.6 ACESSO A INFORMAÇÃO

O controle de acesso da informação visa garantir para que cada pessoa tenha acesso somente ao que é necessário para realizar o seu trabalho garantindo sua autenticidade, deve-se possuir obrigatoriamente identificação única para todo o tipo de acesso.

10.4.7 SISTEMA E APLICATIVO

Devem ser documentados e controlados quanto às alterações e correções feitas dentro dos sistemas.

10.4.8 CLASSIFICAÇÃO DA INFORMAÇÃO

Todas as informações devem ser classificadas e protegidas com controles (Lógicos e Físicos) em todo o seu ciclo de vida.

10.4.9 SEGURANÇA FÍSICA DE EQUIPAMENTOS

O objetivo é garantir que apenas pessoas autorizadas possam ter acesso às informações para administrar e utilizar os equipamentos de forma segura visando a garantia da confidencialidade, integridade, disponibilidade e autenticidade das informações que são armazenadas e manipuladas através desses equipamentos.

10.4.10 TRANSPARÊNCIA

Disposto no inciso VI do artigo 6º da LGPD, o princípio da transparência é um dos pilares fundamentais para o tratamento de dados pessoais.

Deverá ser criado um canal de comunicação onde os usuários da plataforma poderão solicitar informações referentes ao tratamento dos seus dados pessoais e terão acessos aos controladores das informações, conforme dispõe os artigos 9º, 17º e 22º todos da Lei 13.709 de 14 de 08/2018 (LGPD).

10.4.11 PROCESSAMENTO DE DADOS

a) Finalidade específica do tratamento;

Será pública a descrição do contexto, da natureza, do escopo, da necessidade e da finalidade do tratamento das categorias de dados pessoais (art. 5º, inc. I, LGPD) e de dados pessoais sensíveis (art. 5º, inc. II, LGPD), deixando clara a forma como os dados serão captados, tratados, processados, armazenados e eliminados, com exemplos claros da utilização e simplificando o entendimento do processo e utilização da tecnologia.

O documento público de referência disponibilizado será alterado sempre que o programa integrar novos agentes, controladores e encarregados ou os processos e contextos do tratamento de dados for alterado, durante o processo de expansão e aprimoramento da plataforma, visando a transparência e compliance com a legislação vigente.

b) identificação do controlador;

No atual escopo são identificados os agentes de tratamento (arts. 37 a 40, LGPD) e o (s) encarregado (s) pela Proteção de Dados Pessoais (art. 41, LGPD) envolvidos no projeto, podendo ser alterado à medida em que o programa expande e devendo ser publicizado de forma clara sempre que for modificado.

c) Será publicado nos canais de comunicação adequados as informações de contato do Encarregado pela Proteção de Dados Pessoais;

d) Responsabilidades dos agentes que realizarão o tratamento

Os agentes responsabilizados pela realização do tratamento de dados realizarão este tratamento apenas quando necessário conforme legislação vigente, garantindo a confidencialidade, autenticidade, disponibilidade e integridade dos dados sempre garantindo ao titular dos dados o acesso a essas informações.

Os dados captados serão estritamente necessários para as atividades do sistema implantado. Apenas os agentes responsáveis terão acesso aos dados com total controle sobre mudanças e atualizações de informações, garantindo sempre a classificação dos Dados.

e) Direitos do titular de dados pessoais.

Importante destacar que a CONTRATANTE pode analisar onde em seus canais de comunicação pode manter uma comunicação CLARA e OSTENSIVA para atender a necessidade de transparência (art. 6) e de tratamento com regras claras (previsto também no artigo 23) em especial quando há compartilhamento de dados com entidades privadas (artigo 26), de maneira a que todo o fluxo de dados pessoais esteja em conformidade com a LGPD.

10.4.12 CONTROLE DE ACESSO

O gerenciamento de acessos pode ser usado para iniciar, registrar, e gerenciar as permissões de acesso às informações que os usuários poderão acessar. A partir do gerenciamento de acesso a equipe de segurança da informação poderá conceder privilégios de acesso aos usuários de acordo com a necessidade de cada um. Todos os usuários devem proteger seus respectivos login e senha para acesso ao sistema.

10.4.13 AUDITORIA

Toda a plataforma deve ser auditável. Um dos principais itens da auditoria serão os logs de acesso ao sistema e atividade na plataforma para saber quem acessou o sistema e utilizou aquela informação ou realizou determinada ação na plataforma, visando a garantia da autenticidade e confidencialidade dos dados.

10.4.14 ADERÊNCIA

A Política da Segurança da Informação (PSI), estabelece as diretrizes para proteção das informações, devendo sempre garantir a disponibilidade, integridade, autenticidade e confidencialidade das informações. As informações classificadas em qualquer grau de sigilo, sejam confidenciais ou de uso interno, devem estar disponíveis estritamente a pessoas autorizadas, devendo, portanto, ser cumprida e aplicada em todas as áreas.

10.4.15 DEFINIÇÃO E CONCEITOS

Segurança da informação é a proteção de dados para assegurar que eles estejam acessíveis somente aos responsáveis de direito, fazendo parte de um conjunto de políticas e processos que visam garantir a integridade e a proteção de dados tendo os seguintes objetivos:

- Integridade: tem como objetivo a preservação, precisão e confiabilidade dos dados durante todo o seu ciclo de vida;

- Disponibilidade: é fundamental que os dados estejam disponíveis e, para garantir esse requisito, faz-se necessário estabilidade e acesso permanente as informações, por meio de processos de manutenção rápidos, eliminação de falhas e atualizações constantes;

- Confidencialidade: garante que os dados estejam acessíveis a determinados usuários e protegidos contra pessoas não autorizadas, fator que se aplica essencialmente a dados sensíveis, a confidencialidade dos dados pessoais do usuário é um dos requisitos centrais de conformidade da LGPD;

- Autenticidade: visa confirmar a identidade do usuário antes de liberar o acesso aos sistemas e recursos, garantindo que não se passem por terceiros.

10.4.16 DESCRIÇÃO DA POLÍTICA

A Política de Segurança da Informação (PSI) é um conjunto de padrões, normas e diretrizes que tem como objetivo garantir a proteção de informações contra eventuais ameaças que possam prejudicar sua operação.

10.4.17 CLASSIFICAÇÃO DA INFORMAÇÃO E CICLO DE VIDA

A classificação da informação é uma das exigências da ISO 27001, sendo um processo focado em garantir o nível adequado de proteção de dados de acordo com sua sensibilidade, visando a garantia de que nenhum dado seja divulgado indevidamente e que apenas pessoas que têm o direito de os receber acessem as informações. O principal objetivo de classificar as informações é mitigar riscos de vazamentos.

A Contratada deverá revelar a forma pela qual protege as senhas, quando armazenadas e transmitidas dentro da infraestrutura de aplicativos da CONTRATANTE , e a forma pela qual destrói as informações, quando não tiver mais utilidade.

As informações serão geradas e avaliadas pelo gestor de informação classificando-as pelos seguintes níveis:

- Secreta: as informações secretas possuem o mais alto nível de confidencialidade e devem ser protegidas de acessos não autorizados utilizando métodos de criptografia e podendo ser acessadas apenas por determinadas pessoas, a divulgação de alguma informação secreta pode causar sérios danos;

- Confidencial: são informações que necessitam de sigilo absoluto, devem ser protegidas de alterações não autorizadas e disponíveis apenas às pessoas autorizadas a acessá-las quando for necessário. Na proteção de informações confidenciais, é necessário, além de controles de acesso, controles que garantam a integridade, e elas jamais podem ser transmitidas via internet sem o uso de criptografia e, quando descartadas, devem ser tomadas todas as medidas cabíveis para que seja destruída de forma segura e correta, sem chance de recuperação. Exemplo de Informação Confidencial: Informações que devem ser protegidas por obrigatoriedade legal, incluindo dados cadastrais (CPF, RG, etc);

- Restrita: este tipo de informação precisa ser protegida contra acessos internos e externos. Só devem ter acesso às informações restritas, pessoas que necessitam da informação para a realização de alguma atividade;

- Uso Interno: A informação deve ser classificada como interna quando não for desejável seu conhecimento por pessoas de fora da Contratada e Contratante. Não devem sair do escopo, do fluxo operacional e apenas pessoas com acesso autorizado podem utilizar essa informação. Contudo, caso haja vazamento e ela se torne de conhecimento público, em geral provoca danos em pequena ou média escala. Exemplo de Informações de uso interno: relatórios, planilhas;

- Pública: são informações divulgadas aos meios públicos, sem distinção. Exigem esforço mínimo de segurança, havendo um fluxo de processos determinados para a liberação das informações ao público. Exemplo de informações públicas: Notas de Atualizações.

Os dados permanecem disponíveis pelo tempo necessário, passam por atualizações e ao perderem sua serventia devem ser descartados adequadamente passando pelos seguintes processos:

- Armazenamento: tanto físico como lógico deve seguir os controles definidos pelo gestor da informação, com toda a proteção adequada para os dados;

- Descarte: quando a informação se torna desnecessária, a destruição e o descarte deve ser feito de forma adequada e seguir todas as diretrizes estabelecidas;

- Manuseio: Toda informação é gerada com a classificação mínima de uso até passar pela avaliação e rotulagem para o tratamento adequado a informação;

- Transporte: de acordo com a classificação atribuída a informação, deve se controlar a exposição, divulgação e destinatários;

- Procedimentos: as informações devem estar sempre disponíveis, ao acesso de usuários autorizados, possuindo segurança como controles físicos e controles lógicos;

- Controles Físicos: são barreiras que limitam fisicamente o acesso de pessoas não autorizadas às informações;

- Controles Lógicos: são mecanismos de segurança que impedem ou limitam o acesso de pessoas não autorizadas às informações diretamente da máquina, destacando-se os seguintes procedimentos de controles lógicos:

o Criptografia: é uma maneira de codificar a informação estabelecendo que somente o emissor e o receptor da informação possam decifrá-la através de uma chave que é usada tanto para criptografar e descriptografar a informação;

o Arquivos de senha: sempre será necessário para acessar algum tipo de recurso o Identificador do Usuário (ID) e a senha do usuário;

o Arquivos de Log: os arquivos de log são usados para registrar a ação do usuário. Os logs registram quem acessou o computador, aplicativos, arquivos de dados e utilitários.

O controle de acesso lógico é implantado com objetivo de garantir que apenas usuários autorizados tenham acesso aos recursos.

10.4.18 VIOLAÇÃO

As violações de segurança devem ser informadas à equipe de TI e na área de Segurança da Informação, toda violação ou desvio de informações deverá ser investigado para determinação de medidas necessárias visando a correção das falhas. O não cumprimento de algum ponto desta política pode ser submetido a sanções disciplinares, legais e contratuais.

10.4.19 VIGÊNCIA E REVISÕES

A Política de Segurança da Informação entra em vigor na data de sua publicação, tendo prazo de validade indeterminado e, portanto, sua vigência se estenderá até a edição de outro marco. Toda a plataforma passará regularmente, a cada 6 meses, por revisões, sendo analisados todos os impactos, eficiência e alinhamento com as expectativas prévias, e tendo todo o processo documentado, incluindo todos os ajustes de processos e procedimento realizados pelos agentes, além de qualquer variação de resultado, positivo ou negativo, possibilitando corrigir qualquer intercorrência que incline o programa em direção diferente definida como referência.

10.5 PLANO DE CONTINGÊNCIA

O Plano de Contingência deve apresentar uma estrutura estratégica e operativa que ajudará, sempre que necessário, a controlar uma situação de extremo impacto e risco grave, tendo o objetivo de estabelecer procedimentos de comunicação e mobilização para procedimentos de tratamento de incidentes de emergências de extremo impacto e, em caso de emergências que possam ocorrer durante as atividades na execução dos serviços, o plano deve conter todos os procedimentos necessários para a correção de falhas ou a mitigação de problemas como:

- Incidentes de segurança e ataque cibernético;
- Em caso de sequestro de dados;
- Detecção de ataque DDoS;
- Falha na infraestrutura;
- Falha na rede.

O Plano de Contingência não se limita aos exemplos de incidentes citados acima.

O plano de contingência deve assegurar que os riscos identificados sejam avaliados e classificados de acordo com o risco causado, visando a garantia da proteção das informações baseadas na LGPD, trazendo a segurança de que os dados vão estar seguros. A Contratada deverá implementar o plano de contingência juntamente com o plano de recuperação de desastres (DRP), redigindo-o conforme exigido pela LGPD. O Plano será submetido à Contratante, que poderá realizar alterações que julgar necessárias.

A Contratante pode aprovar, desaprovar, determinar novas diligências até a efetiva aprovação da versão final, devendo ser observados os requisitos estabelecidos para formulação do Plano de Contingência. A responsabilização por falhas no Plano será da licitante vencedora. Deverão ser

realizadas simulações semestrais para validação do Plano.

10.6 SEGURANÇA CIBERNÉTICA

10.6.1 INTRODUÇÃO

Este Documento institui a Política da Segurança Cibernética e tem o compromisso de assegurar a proteção de ativos, sendo a disciplina que concentra os esforços para a proteção de ativos de informações em ambiente virtual.

A crescente ameaça à segurança cibernética, somada a uma maior dependência de utilização de sistemas, faz com que a segurança da informação e a segurança cibernética sejam prioridade de primeiro nível.

10.6.2 OBJETIVO

A política de Segurança Cibernética tem como objetivo a proteção de ativos de informação. Este documento estabelece conceitos, diretrizes, normas e procedimentos visando a redução dos riscos de acessos não autorizados, redução de risco de roubo da informação e respostas contra ataques cibernéticos, visando a preservação a confidencialidade, autenticidade, disponibilidade e integridade de todas as informações, definindo regras que representam a transparência da informação conforme a LGDP (Lei nº 13.709/2018) e os princípios fundamentais para o alcance dos objetivos.

10.6.3 ABRANGÊNCIA

A Política de Segurança Cibernética deve estar disponível para que seu conteúdo possa ser consultado a qualquer momento, aplica-se a todos os funcionários, diretores, estagiários, terceirizados e qualquer outra pessoa envolvida nos processos e atividades.

10.6.4 NORMAS DE REFERÊNCIA

Para um melhor entendimento sobre segurança cibernética e segurança da informação, deve-se consultar os seguintes documentos referenciados:

- ISO 27000;
- ISO 31000;
- ISO 22301;
- Cobit 5 – DS4;
- LGPD (Lei nº 13.709/2018);

- ABNT ISO/TR nº 31004;
- ABNT NBR/IEC nº 31010;
- ABNT NBR ISO/IEC nº 27001;
- ABNT NBR ISO /IEC nº 27002;
- ABNT NBR ISO/IEC nº 27003;
- ABNT NBR ISO /IEC nº 27004;
- ABNT NBR ISO/IEC nº 27701;
- ABNT NBR ISO/IEC nº 29100;
- ABNT NBR ISO/IEC nº 29134;
- ABNT NBR ISO/IEC nº 29151.

10.6.5 DEFINIÇÃO / CONCEITOS

Segurança Cibernética é definida como um conjunto de tecnologias, processos e práticas projetados para proteger redes. Ações voltadas para segurança de operações visando que os sistemas de informações sejam capazes de resistir a eventos no espaço cibernético, definindo os seguintes conceitos:

- Risco: qualquer evento que possa ser considerado hostil a segurança da informação. Com objetivo de afetar o sistema ou conforme a ISO 31000, o efeito de incerteza nos objetivos;

- Controle: qualquer recurso ou medida que assegure formas de tratamento de riscos, incluindo a redução, eliminação ou transferência de dados;

- Ameaça: qualquer causa potencial de um incidente indesejado que possa resultar em impactos nos objetivos. Podendo ser internas ou externas;

- Informação: qualquer conjunto organizado de dados que possua algum propósito e valor para o sistema;

- Espaço Cibernético: engloba a internet, sistemas de informações, e as tecnologias digitais que dão suporte;

- Ataque Cibernético: é a exploração por parte de um agente malicioso para tirar proveito de pontos fracos como por exemplo a tentativa de roubar dados, desligar computadores;

- Ativos Tecnológicos: qualquer dispositivo físico ou digital, que suporta atividades relacionadas a informações;

- Incidente de Segurança Cibernética: todo e qualquer evento não esperado que gere algum tipo de instabilidade;

- Threat Intelligence: inteligência de ameaças cibernéticas, engloba tudo o que envolve medidas

necessárias à prevenção de ataques cibernéticos e para mitigar os efeitos causados por eles, visando a preservação da confidencialidade, integridade, disponibilidade e conformidade.

São Obrigações da Contratada:

- Indicar à Contratante procedimentos de varredura para identificação, comunicação e solução de vulnerabilidades, a exemplo, mas não se limitando, da comunicação por parte de fornecedor

de tecnologia, por instituição ou órgão especializado em tecnologia ou segurança da informação, base de dados pública ou ferramenta de busca automatizada de vulnerabilidades que seja aceita por ambas as partes;

- Adoção de mecanismo reservado de comunicação de vulnerabilidade descoberta ou que mereça contorno, de modo que somente venha a público caso já tenha solução ao caso no mínimo preventiva e, de forma definitiva quando superar totalmente o incidente;

- Enviar os logs requeridos pela Contratante e determinar qual tempo médio para atendimento das requisições;

- Deverá criptografar todos os dispositivos móveis e portáteis utilizados para prover o serviço à CONTRATANTE e que contenham dados confidenciais;

- Quando do uso de criptografia, a resistência dos algoritmos de criptografia deverá ser a mais alta possível sem afetar a usabilidade dos sistemas, aprovada pela Contratante.

10.6.6 RESPONSABILIDADES

As responsabilidades da Área de Gestão de Riscos são:

- Orientar e coordenar as ações de segurança da informação, promovendo a execução de todos os procedimentos estabelecidos;

- Definir controles para tratamento de riscos, ameaças e vulnerabilidades;

- Conduzir o processo de gestão de riscos e segurança da informação;

- Implantação e melhoria contínua das práticas de gerenciamento de riscos e controles internos.

Quanto as responsabilidades de cada ator do processo, temos:

a) Chefe da Segurança da Informação: É responsável por comunicar os incidentes cibernéticos ocorridos. São suas responsabilidades:

- Certificar-se de que a equipe interna não use indevidamente ou roube os dados;

- Gerenciar a identidade e acessos, para garantir a autenticidade;

- Investigações e perícias determinando o que deu errado em uma violação, seja interna ou externa para garantir que não ocorra novamente.

b) Chief Compliance Officer: o compliance tem atribuições mais importantes, são responsáveis por:

- Criar estratégias de gerenciamento de riscos;

- Analisar as informações e tomar as decisões cabíveis em casos de fraude;

- Implementar um programa de integridade onde vai informar sobre todos os riscos, tendo como obrigação relatar, controlar, cumprir todos os regulamentos, leis e normas.

10.6.7 PRINCÍPIOS E PROCEDIMENTOS DE SEGURANÇA DA INFORMAÇÃO

a) Quanto à informação

A informação deve ser utilizada unicamente para a finalidade para a qual foi autorizada pelo gestor da informação. Deve ser tratada de modo que seja possível realizar a proteção dos dados e do espaço cibernético contra ameaças internas e externas. É importante garantir os princípios da segurança cibernética, que são:

- Integridade: tem como objetivo a preservação, precisão e confiabilidade dos dados durante todo o seu ciclo de vida;

- Disponibilidade: é fundamental que os dados estejam disponíveis e, para garantir esse requisito, é necessário estabilidade e acesso permanente às informações, por meio de processos de manutenção rápidos, eliminação de falhas de software e atualizações constantes;

- Confidencialidade: garante que os dados estejam acessíveis a determinados usuários e protegidos contra pessoas não autorizadas, que se aplica essencialmente a dados sensíveis, a confidencialidade dos dados pessoais do usuário é um dos requisitos centrais de conformidade da LGPD.

A Contratada deverá possuir e manter atualizado registro de atividades de tratamento, com inclusão dos fluxos específicos no tocante à manutenção dos serviços da plataforma.

A Contratada deverá considerar, desde a concepção dos serviços a serem criados / atualizados, as avaliações de riscos à privacidade, com a devida documentação das análises realizadas.

A Contratada deverá possuir procedimentos formalizados em relação à avaliação de riscos aos titulares de dados pessoais, mediante condução de relatórios de impacto à proteção de dados e avaliações de impacto à privacidade para considerar e resolver quaisquer preocupações de privacidade.

A Contratada deverá possuir governança sobre a gestão de acessos ao sistema e coletar assinatura de termos de confidencialidade específicos sobre o acesso às imagens do sistema a todos os funcionários que possuírem acesso às câmeras.

A Contratada deverá definir, em documentação de governança interna, os propósitos específicos para o uso de informações e procedimentos de documentos sobre como lidar com essas informações.

A Contratada deverá estabelecer um processo claro para os funcionários seguirem ao lidar com solicitações de indivíduos que desejam acessar cópias de suas próprias imagens. O processo deve ajudar a equipe a:

- Reconhecer um pedido;

- Identificar e obter as imagens solicitadas;

- Encaminhar as informações solicitadas de forma segura e aprovada à Contratante, que é a única parte que tem poderes para entregar informações a terceiros; e

- Manter os registros necessários sobre uma solicitação e a situação foi endereçada.

A Contratada deverá garantir que:

- Todos os funcionários autorizados a acessar as câmeras estão familiarizados com o sistema e entendem como revisar e extrair imagens, se necessário;

- Todos os funcionários estão familiarizados com as prováveis penalidades disciplinares por uso indevido dos sistemas da plataforma;

- Sejam atendidos e registrados padrões de quando o papel de um membro da equipe inclui explicitamente o monitoramento do sistema.

A Contratada deve dispor de meios que permitam a categorização das informações presentes no sistema, devendo ser capaz de identificar dados pessoais, dados pessoais sensíveis e informações gerais que não sejam dados pessoais. São padrões necessários:

- Autenticidade: Visa confirmar a identidade do usuário antes de liberar o acesso aos sistemas e recursos, garantindo que não se passem por terceiros;

- Irretratabilidade: Tem foco na legitimidade do autor da informação, está relacionado a garantia de impossibilidade de o emissor negar a autoria de determinada mensagem ou transação.

Deve-se ter os seguintes procedimentos para visar a garantia da segurança da informação:

- Métodos de autenticação: todos os usuários devem utilizar o método de autenticação de dois fatores, todo funcionário é responsável por todos os atos executados com seu identificador (login/senha), deve seguir os requisitos da política da Segurança da Informação e da Segurança Cibernética, impedir o uso por outras pessoas e bloqueá-lo ao se ausentar;

- Gestão e Controle de acesso: o gestor da plataforma deve autorizar o acesso a sistemas, dados e informações para a realização de qualquer atividade, podendo conceder excepcionalmente acesso temporário para execução de atividades específicas;

- Desenvolvimento Seguro e Criptografia: mecanismos de criptografia para a proteção da autenticidade dos dados, podendo ter acesso apenas às pessoas autorizadas e conforme as classificações das informações para a realização das atividades;

- Backup de Dados: ter um plano de backup de dados, uma cópia segura dos dados de um dispositivo de armazenamento ou sistema para outro ambiente, para que eles possam ser restaurados. O ciclo do Backup parcial é de 7 dias devendo ser realizado com essa periodicidade gravando as informações alteradas de forma que seja possível criar pontos de reversão em caso de falha de sistema, bloqueio de dados ou outros problemas que inviabilizam a operação da plataforma, com o armazenamento mínimo do backup por 120 dias, devem estar devidamente protegidos de ataques e armazenados em local distinto da operação da plataforma;

Teste de Penetração: É um método que avalia a segurança de um sistema ou de uma rede, simulando um ataque de uma fonte maliciosa. Envolvendo uma análise nas atividades do sistema, que buscam alguma vulnerabilidade em potencial que possa ser resultado de uma má configuração do sistema, falhas em hardwares/softwares;

- Gestão de Identidade de usuários: Os administradores de TI devem gerenciar com segurança e eficácia as identidades digitais dos usuários e os privilégios de acessos relacionados. Os administradores de TI podem configurar e modificar as funções dos usuários, rastrear e relatar as atividades do usuário visando garantir a segurança e a privacidade de dados.

b) Quanto ao registro, resposta e tratamento de incidentes de segurança cibernética

É extremamente importante registrar os incidentes de segurança cibernética e a classificação, que consiste em verificar o impacto causado pelo acidente, para o processo de tratamento de incidentes, visto que melhora a capacidade de detecção de incidentes e pode ajudar a conter danos e prejuízos. Atividades suspeitas ou incidentes identificados devem ser comunicadas ao gestor de incidentes de segurança cibernética.

Devem ser registrados eventos adversos relacionados a segurança dos sistemas ou das redes de computadores como por exemplo:

- Tentativas de invasão, com ou sem sucesso, de ganhar acesso não autorizado a um sistema ou conseguindo seus dados;
- Modificação do sistema;
- Sistema desatualizado permitindo abuso;
- Malware;
- Vírus;
- Worms.

Todos os recursos de informação que estiverem expostos na internet devem ser protegidos por um IDS / IPS que são recursos que examinam o tráfego na rede. Sempre que o IDS / IPS detectarem ou responderem a uma tentativa externa de invasão ao sistema, uma análise estruturada e procedimentos de resposta deve ser acionado para garantir a segurança dos dados. Os recursos devem possuir os seguintes procedimentos para tratar os incidentes de segurança cibernética:

- Autenticação e criptografia simétrica e assimétrica;
- Testes de invasão;
- IDS e IPS (sistemas de detecção e prevenção de ataques a redes);
- Controles de acessos (lógicos e físicos);
- Proteção contra softwares maliciosos;
- Antecipação de ataques cibernéticos;

- Manter sistemas atualizados;
- Classificar as relevâncias dos incidentes cibernéticos.

A Contratada deve possuir, também, procedimentos de varredura para identificação, comunicação e solução de vulnerabilidades, a exemplo, mas não se limitando, a comunicação por parte de fornecedor de tecnologia, por instituição ou órgão especializado em tecnologia ou segurança da informação, base de dados pública ou ferramenta de busca automatizada de vulnerabilidades que seja aceita por ambas as partes. O responsável deve comunicar e, caso seja necessário, realizar os seguintes processos:

- Plano de Recuperação de Desastre (PRD) (DRP - Disaster Recovery Plan): A comunicação para a ativação desse processo deve ser realizada em cenários sensíveis para garantir a reação apropriada a desastres ou emergência minimizando os efeitos sobre as suas atividades;

- Plano de Continuidade de Negócio (PCN): Deve ser utilizado em cenários com impacto significativo e risco grave, visando reduzir ao máximo o impacto dessas situações.

c) Quanto às violações

As violações de segurança externas ou internas devem ser informadas à equipe de TI e na área de Segurança da Informação que deverá comunicar o diretor de segurança da informação (CISO), toda violação ou desvio de informações é investigado para determinação de medidas necessárias visando a correção das falhas.

O não cumprimento de algum ponto desta política pode ser submetido a sanções disciplinares ou legais.

10.6.8 VIGÊNCIA E REVISÕES

A Política de Segurança Cibernética entra em vigor na data de assinatura do contrato, com validade indeterminada.

A Política de Segurança Cibernética deverá ser revista e atualizada a cada 6 meses, ou a qualquer tempo em caso de incidentes registrados, com objetivo a se manter em sintonia com as regras e com as melhores práticas de segurança, leis, regulamentos e procedimentos, visando melhor atender as necessidades.

10.7 INTEGRIDADE E ÉTICA

10.7.1 INTRODUÇÃO

Este documento sobre Integridade e Ética visa estabelecer orientações e diretrizes para estruturação, efetivação e melhoria das ações de integridade com incentivo à denúncia de irregularidades tendo como foco medidas anticorrupção, aplicando efetivamente os códigos de ética, conduta, política e diretrizes com a finalidade de detectar e punir desvios de condutas, práticas de corrupção (como roubos de dados internamente), fraudes e irregularidades. Esses princípios devem ser observados para atingirmos padrões éticos cada vez mais elevados.

A gestão de ética se alicerça em um conjunto de bons princípios que orientam o comportamento e as relações.

A LGPD traz, no parágrafo primeiro do artigo 20, a necessidade de fornecimento de informações claras a respeito de tratamentos automatizados. Para tanto, faz-se necessário que o agente de tratamento possua diretrizes formalizadas quanto ao tratamento automatizado de dados e quais os critérios a serem utilizados. A exemplo, o uso de tecnologia que automatize o tratamento de dados não poderá discriminar pessoas e tampouco executar desvios de finalidade no tocante à segurança dos titulares.

Para realização destes tratamentos automatizados, serão utilizadas ferramentas de inteligência artificial.

A Contratada, quando do uso de ferramentas de Inteligência Artificial, se compromete a estruturar conjuntamente com a Contratante, documentação referente à Governança em Inteligência Artificial, que poderá conter, mas não limitado à, os seguintes documentos:

- Código de Conduta para Uso de IA: que determina do ponto de vista estratégico como deve ser a interação da IA em conformidade com os interesses públicos da Contratante;

- Política de Governança de IA: que definirá as regras e restrições para definir as responsabilidades dos agentes públicos e terceiros que irão atuar diretamente com a plataforma, compreendendo aspectos táticos e operacionais referentes ao sistema inteligente;

- Procedimento para Avaliação de Impacto da IA: em conjunto com o documento para Avaliação de Impacto da IA, de forma a avaliar de maneira pormenorizada quais os riscos apresentados em sua implementação, planos de ações para supri-los, e viabilidade operacional;

- Procedimento de Auditoria: que determinará o procedimento para fiscalizar do ponto de vista técnico e ético, se o algoritmo da IA funciona corretamente, e em conformidade com as diretrizes estabelecidas pela Contratante;

A Contratada, junto à Contratante, se compromete a estruturar a criação do Comitê de Ética Algorítmica no tocante à tratamentos automatizados realizados com o uso de Inteligência Artificial, de forma que as análises não consistam em tratamentos discriminatórios ilícitos ou abusivos.

10.7.2 OBJETIVO

Ser um guia formal e institucional, para a conduta pessoal e profissional de todos os colaboradores e parceiros, padronizando os relacionamentos internos ou externos, atingindo os melhores resultados.

Os objetivos da integridade e ética são:

- Prevenir, detectar e punir desvios de conduta, roubo/furto de dados, prática de corrupção;

- Estimular um ambiente de comportamento ético e reforçar as práticas que devem ser pautadas na ética, integridade, honestidade e transparência;

- Pautar a atuação de forma social e ambientalmente responsável, evitando a ocorrência de fraude e corrupção;

- Respeito ao conjunto de valores morais que conduzem o ambiente de trabalho de forma mais respeitosa, com transparência e equidade;

- Elevar a produtividade e a qualidade.

10.7.3 ABRANGÊNCIA

A Política de Integridade e Ética deve estar disponível para que seu conteúdo possa ser consultado a qualquer momento. Aplica-se a todos os funcionários da Contratada e da Contratante envolvidos em atividades referentes ao tratado no contrato.

10.7.4 PRINCÍPIOS

Os princípios éticos são fundamentos nos quais se fundam as ações dirigidas para o bem, desse modo expressa a determinação sobre a observância aos princípios de legalidade, integridade, eficiência, transparência e respeito. Os princípios adotados, são:

- Legalidade: sempre atender à legislação vigente;

- Integridade: seguir com retidão todas as normas estabelecidas;

- Eficiência: entrega de atividades com rapidez, excelência e zelo pela economia;

- Transparência: atender a legislação vigente, sempre observando primeiramente a LGPD;

- Respeito: manter o respeito nos relacionamentos interpessoais, em qualquer circunstância.

10.7.5 DIRETRIZES

A Política de Integridade e Ética deverá estar alinhada com as seguintes diretrizes visando a garantia da integridade utilizando normas e procedimentos previstos na lei anticorrupção (LEI Nº 12.846).

a) Prevenção e combate à corrupção

A corrupção pode assumir muitas formas, mas na maioria das vezes acontece através de suborno. Não se tolera qualquer forma de corrupção. De acordo com a Lei Anticorrupção (LEI Nº 12.846), deve se seguir os seguintes procedimentos para adotar medidas anticorrupção:

- Promoção de campanhas de conscientização, com temas de integridade para público interno e externo;

- Monitoramento contínuo dessas diretrizes visando seu aperfeiçoamento na prevenção, detecção e combate à corrupção previstos no Art. 5° da Lei 12.846;

- Previsão de procedimentos que visem a pronta interrupção de irregularidades ou infrações detectadas;

- Disponibilização de canal de denúncia de irregularidades ou infrações detectadas;

- Aplicação de procedimentos específicos para prevenir fraudes e ilícitos garantindo a integridade dos dados.

10.7.6 CONDUTA ÉTICA

Diz respeito ao conjunto de valores morais que conduzem os comportamentos no ambiente de trabalho e durante o exercício das atividades. As premissas básicas podem ser definidas como sendo:

- Orientar a tomada de decisões em momentos de conflito de interesses;
- Estabelecer padrões de integridade, respeito e transparência no exercício da profissão;
- Atuar com base na legalidade, impessoalidade, moralidade, transparência e eficiência;
- Agir com dignidade e cortesia, sempre estar disposto a ouvir críticas e sugestões.

10.7.7 COMPROMISSOS

Em todos os relacionamentos devem seguir as orientações abaixo para buscar um ambiente de trabalho com mais respeito, transparência e integridade.

- Repúdio a qualquer tipo de discriminação;
- Prevenção a fraude, roubo de dados (externo ou internamente);
- Sigilo e confidencialidade das informações não públicas.
- Lisura, transparência e imparcialidade;
- Prevenção e combate à corrupção.

10.7.8 GERENCIAMENTO DISCIPLINAR

Aplicação de gerenciamento disciplinar, com o objetivo de apurar, analisar, avaliar e julgar as ocorrências sobre as quais foram cometidas onde o empregado tenha omitido, permitido ou infringido as normas legais deste documento.

10.7.9 RELACIONAMENTOS EXTERNOS

O relacionamento deverá ser efetivado de forma profissional, transparente e igualitária com o público externo. Deve-se seguir as seguintes orientações para manter um relacionamento profissional:

- Postura ética, pautada em respeito e integridade;

- Prestação de informações com transparência, integridade e veracidade;

- Manter sigilo de informações confidenciais quando recebidas em função de sua atividade profissional. Quando uma informação em caráter confidencial for solicitada deve solicitar ao gestor prévia autorização de acesso e observar as normas para cessão de tal informação.

10.7.10 GESTÃO DE RISCOS

A gestão de riscos é o conjunto de atividades coordenadas que tem o objetivo de gerenciar e controlar as ameaças investigando para a correção das falhas.

10.7.11 CONTROLE INTERNO

Gestão ou verificação de atividades, visando a garantia de conformidade com as normas e procedimentos para proteção de ativos.

10.7.12 CONFIDENCIALIDADE

Todos os níveis hierárquicos deverão manter a confidencialidade de todas as informações as quais tenham acesso em razão das suas atividades. Apenas as pessoas autorizadas poderão acessar as informações que deverão ser utilizadas exclusivamente para realizar alguma atividade. Manter rigorosamente a confidencialidade de todas as informações. São condutas a ser adotadas:

- Não enviar informações ou dados de terceiros para o ambiente externo, seja por e-mail, pen drive, ou de qualquer outra forma;

- Acompanhar a efetivação da Lei de Proteção de Dados (LGPD) e observar a privacidade e o controle de dados pessoais;

- Não compartilhar credenciais (ID, senhas e crachá) de uso individual e intransferível;

- Apenas compartilhar informações confidenciais com pessoas autorizadas e que necessitem da informação para a realização de alguma atividade.

10.7.13 COMPROMISSO COM AS NORMAS

Todos os destinatários deste documento devem considerar que as atitudes e os comportamentos são baseados no forte compromisso de fazer o melhor. Todos devem agir de acordo com as leis e normas aplicáveis, internas ou externas.

10.7.14 TRANSPARÊNCIA ATIVA

São aquelas ações/informações disponibilizadas pelos órgãos e entidades, independente de solicitação, utilizando principalmente a internet.

A divulgação de dados de forma ativa (isto é, sem a necessidade de o cidadão solicitar determinada informação) facilita o controle social da população nos investimentos e despesas públicas e reduz o número de pedidos de acesso à informação.

O Índice de Transparência Ativa (ITA) tem como principal objetivo avaliar o nível de Transparência Ativa relacionado aos portais institucionais de órgãos e entidades que compõem a Administração. A transparência ativa é função importante para subsidiar o controle social das atividades realizadas, sem que seja necessário solicitar pelo acesso às informações. O Relatório de Transparência Ativa tem o objetivo de verificar em que medida estão sendo seguidos os parâmetros previstos em Lei.

Conflito de Interesses é a situação gerada pelo conflito de interesses público e privado que possa comprometer o interesse coletivo ou influenciar, de maneira imprópria, o desempenho da função pública. A Lei Nº 12.813 de 16 de maio de 2013, define as situações que configuram conflito de interesses.

Engenharia Social é uma técnica empregada para induzir usuários desavisados a enviar dados confidenciais, infectar seus computadores com malware ou abrir links para sites infectados, conseguindo roubar seus dados pessoais. A proteção contra a engenharia social começará com treinamento. Os usuários devem ser condicionados a nunca clicar em links suspeitos, suspeitar de pessoas pedindo informações via e-mail, mensagens, etc., e sempre proteger suas credenciais de login, deverão sempre conferir a fonte sempre reservar um momento para pensar de onde vem a comunicação.

Alguns tipos de Engenharia Social:

- Phishing: Tentam se passar por instituições confiáveis, copiando layout de um e-mail corporativo, copiam informações via mensagens;

- Quid Pro Quo: Finge fornecer algo em troca da informação;

- Baiting (iscas): Essa tática de engenharia social, deixa a disposição do usuário um dispositivo infectado com malware, como pen-drives;

- Vishing: Fingem ser uma pessoa confiável e tentam, durante a conversa, obter informações da vítima, solicitando as credenciais para acessar o sistema, conseguindo informações;

- Pretexting: A pessoa inventa para extrair informações importantes do usuário, criar uma relação de amizade e utilizar essa proximidade para extrair algum dado útil para a invasão.

10.7.15 VALORES

- Visão estratégica;

- Atitude inovadora;

- Compromisso público;
- Ética e transparência;
- Integridade.

10.7.16 CANAIS DE DENÚNCIA

O e-mail é o canal de comunicação que recebe reclamações, sugestões. Faz parte das atribuições receber denúncias por fraude, corrupção. Tem por objetivo garantir o encaminhamento das demandas aos setores responsáveis, visando uma gestão eficaz e transparente.

10.7.17 VIOLAÇÃO

Qualquer tipo de violação da política de integridade e ética deve se comunicar aos superiores a fim de instaurar investigação das denúncias recebidas com responsabilidade, de maneira justa e legal.

O não cumprimento dessa política de integridade e ética será punido com sanções tanto contratuais como disciplinares/legais.

10.7.18 VIGÊNCIA E REVISÕES

O presente documento de Integridade e Ética tem validade indeterminada a partir da assinatura do contrato e sua divulgação, deverá ser revista e atualizada, ao menos a cada mês com objetivo a ser atualizada com as regras e com as melhores práticas de segurança, lei anticorrupção, regulamentos e os princípios da ética adotada.

10.8 INTEROPERABILIDADE

Será necessário realizar a interoperabilidades de sistemas trazendo funcionalidades de sistemas já existentes para a nova plataforma a fim de reduzir o trabalho de desenvolvimento e o número de contratos de mesma natureza utilizados isoladamente.

A Lei nº 14.129/2021 dispõe sobre a interoperabilidade dos sistemas de informação, entre todos os órgãos da administração pública, facilitando assim para todos os usuários, visto que será necessário fazer login apenas uma vez.

As integrações e a interoperabilidade serão implementadas gradualmente durante o período de contrato à medida que os convênios e termos de cooperação forem estabelecidos pela Contratante, ficando a Contratada obrigada a efetivar as integrações através de projeto e documentação das alterações realizadas na plataforma, incluindo método de integração utilizada. A Contratante fará as demandas de integração com prazo para conclusão/implementação de 6 meses, da mesma forma que os ciclos semestrais, ficando a critério da Contratada disponibilizar a integração com prazo inferior aos 6 meses. Fica obrigada a contratada prover meios para testar e homologar a integração antes da implementação definitiva garantindo maior estabilidade e eficiência.

O método utilizado para as integrações deve ser planejado em conjunto com a Contratante a fim de atender todos os requisitos técnicos necessários para o pleno funcionamento da aplicação.

A Contratada deverá, a partir da emissão da ordem de serviço, fazer reuniões técnicas com a Contratante para levantamento de todas as necessidades de integrações com sistemas legados, devendo, no prazo de 30 dias, apresentar cronograma de implantação para a Contratante.

A Contratada deverá prover especificamente a integração e interoperabilidades da plataforma que implantará com o GESEG, através de mecanismos que resultem em uma confiável fonte de dados, propiciando o cruzamento do sistema de alertas em um mesmo ambiente integrado.

A integração deverá ser feita nos diversos ambientes necessários, principalmente nos de homologação e produção.

A Contratada deverá realizar as seguintes atividades: identificar e entender a complexidade das interfaces necessárias entre seu sistema e os sistemas componentes do GESEG; fazer uma análise de soluções de integração; desenvolver as interfaces; validar as interfaces desenvolvidas e o processo de integração.

A Contratada, ao propor soluções para integração com os sistemas legados, deverá considerar dois cenários distintos:

- Cenário Atual: A Contratada, ao apresentar o cenário atual de integração para o sistema, deverá propor alternativas visando minimizar os reflexos da implantação do Sistema nos demais sistemas legados;

- Cenário Futuro: A Contratada deverá propor soluções para um cenário futuro considerando a melhor alternativa para que futuras integrações possam ser realizadas entre seu Sistema e os demais sistemas ou soluções do ambiente operacional da SSP/PROCERGS. O objetivo do cenário futuro é fazer uma projeção de necessidades futuras de integração, além de propor o desenvolvimento de interfaces, baseadas em alternativas técnicas melhores que as atualmente existentes.

As soluções a serem utilizadas pela Contratada para a integração nos cenários atual e futuro serão definidas pela PROCERGS em comum acordo com a Contratada, a partir das propostas apresentadas.

A Contratada deverá desenvolver as interfaces de seu sistema (para o cenário atual e futuro) de modo que a integração seja realizada automaticamente, através de scripts, rotinas, triggers, views ou procedures de banco de dados, ou utilizando abordagens e tecnologias como os Web Services, baseados em XML e API.

A Contratada deverá realizar o teste das interfaces e validação da integração seguindo os procedimentos definidos. O resultado dos testes deve ser apresentado na forma de um documento com evidências objetivas dos procedimentos executados.

Produtos a serem entregues:

- Interfaces atuais e futuras de integração com os sistemas e ambiente operacional da SSP/PROCERGS construídas;

- Sistema integrado ao ambiente da SSP/PROCERGS e em perfeito funcionamento;

- Documento Análise das Soluções de Integração, em mídia impressa e eletrônica, contendo o resultado da análise realizada, descrevendo interfaces necessárias para o sistema e a solução apresentada para os cenários atual e futuro;

- Documentação técnica detalhada das interfaces, componentes, scripts, triggers, views, procedures e qualquer outro procedimento utilizado para a integração com os sistemas legados, em mídia impressa e eletrônica;

- Casos de Teste de Integração;

- Evidências de Testes, contendo os resultados analíticos da execução de cada teste de integração definido, e que devem ser aceitas pela Contratante.

Caso a Contratante não aprove o plano de trabalho deverá apontar os pontos que não concorda para que a Contratada retifique e o submeta novamente a aprovação em até 15 dias.

A plataforma deve ser integrada a diferentes bases de dados para diversas finalidades, trazendo agilidade e otimizando processos. Deve ser possível integrar o maior número de sistemas e bases de dados pois, desta forma, será possível criar uma inteligência real e modelar processos autônomos de tomada de decisão baseados em dados e lógica, o que deve trazer maior satisfação aos cidadãos e um modelo único de eficiência, aproximando os segmentos da sociedade de forma cooperativa e permitindo ao poder público ser proativo e não mais reativo, tomando decisões com base em dados concretos e modelos que foram testados e simulados, cobrindo as possíveis variáveis e impactos da decisão com base em inteligência artificial e modelos matemáticos.

10.9 INTEGRAÇÕES

É necessário a realização de diversas integrações com sistemas e bases de dados, desta forma a inteligência da plataforma será expandida gradualmente trazendo dados, funcionalidades e interoperabilidade entre os sistemas da Contratante, reduzindo a sobreposição de recursos de mesma natureza e aumentando a cooperação no serviço público. No geral, as integrações serão realizadas através de API, entretanto, devem ser tratadas caso a caso, criando planejamento e sendo realizadas conforme os ciclos de revisão do sistema, garantido tempo hábil para o alinhamento, planejamento, homologação e entrega da integração, mitigando instabilidades, perda de dados e falhas de segurança.

10.9.1 USO DE ANALÍTICOS DE IMAGENS

O uso dos analíticos de imagens poderá ser realizado conforme determinado em lei. Todos os dados não utilizados serão descartados após período a ser determinado na Política de Segurança de Dados.

A licitante vencedora deverá realizar semestralmente um Relatório de Impacto à Proteção de Dados (Data Protection Impact Assessment), sendo essa uma documentação emitida pelo controlador, a qual contém a descrição dos processos de tratamento de dados pessoais.

Constarão do relatório as medidas, salvaguardas e mecanismos para mitigação de tais riscos, com a análise, identificação e minimização dos riscos relacionados a incidentes de segurança.

O relatório deverá indicar a viabilidade do tratamento de dados pretendidos, semestralmente. O relatório será disponibilizado para a Contratante e deverá ser encaminhado ao conselho para seu conhecimento e deliberação que julgar necessária.

A Contratante divulgará, através de seus canais de informação, campanha de aviso prévio sobre a captura de imagens, comunicando que as câmeras estarão realizando a captura de imagens nos locais indicados.

Por se tratar de uma informação restrita, a localização das câmeras não será divulgada, sendo apenas divulgada a captura das imagens. O conhecimento sobre os pontos de capturas de imagens será disponibilizado às autoridades competentes, mediante indicação do responsável pela informação e ciência do conselho.

A licitante vencedora deverá realizar parecer detalhando o grau de detalhes capturados, bem como realizar vídeo institucional para divulgação do parecer. Serão estabelecidos na política de segurança e no Relatório de Impacto à Proteção de Dados, os seguintes itens:

- As regras e registros de acesso aos dados de imagens;
- Proteção sobre o controle de armazenamento;
- Retenção de autorizações das pessoas envolvidas na operação;
- Relatório contendo acessos, consentimentos, revisões e eventuais violações a tais informações.

10.9.2 TRANSPARÊNCIA

A Política de segurança, plano de contingência e Relatório de Impacto à Proteção de Dados devem ser revistos semestralmente.

Fica a critério da licitante vencedora a contratação de consultoria especializada para elaboração dos documentos solicitados.

Todos os itens que forem de acesso público serão publicados em Diário Oficial, após a aprovação da Contratante.

Para início do uso efetivo da plataforma, após período de implantação e período de teste, deverão ser apresentados a Política de Segurança, plano de contingência e Relatório de Impacto à Proteção de Dados.

10.10 Formulário de Avaliação do Nível de Serviço (ACORDO DE NÍVEL DE SERVIÇO - SLA)

O Acordo de Nível de Serviço - SLA possui um período de 10 dias corridos a contar da assinatura do contrato para definir e implantar de forma conjunta a PSI (Política de Segurança da Informação) e DRP (recuperação de desastres).

A Contratada se compromete a prestar serviços descritos neste Termo de Referência necessários para a operação da plataforma (Operacionalização da Plataforma Inteligente), de forma estável e segura, garantindo a qualidade dos serviços prestados, realizando manutenções preventivas e

substituindo o que for necessário para garantir a operação da solução, de acordo com as descrições deste Termo de Referência, respeitando o tempo máximo de solução.

A Contratada disponibilizará todos os laudos e relatórios dos testes e auditorias realizadas à Contratante, mantendo histórico detalhado de todas as tratativas de suporte, correções de falhas, atualizações de software e qualquer outra comunicação disponível.

A Contratada deverá informar imediatamente à Contratante, sempre que houver algum tipo de comportamento anômalo que indiquem possíveis ataques ou acessos indevidos à plataforma comprometendo a segurança, possíveis vazamentos de dados, falhas de segurança, desastres ou qualquer outro incidente com o respectivo tempo de correção, deixando a Contratante sempre a par da situação.

A Contratada deve garantir a segurança, integridade e confidencialidade dos dados conforme descrito neste Termo de Referência. Os dados, metadados e informações tratados não poderão ser fornecidos a terceiros e/ou usados para fins diversos do previsto nesse Termo de Referência, sob nenhuma hipótese, sem autorização formal da Contratante, devendo cumprir a Lei Federal nº 13.709, de 14 de agosto de 2018 (Lei Geral de Proteção de Dados Pessoais) e suas alterações.

A Contratante poderá realizar testes de segurança e auditorias periódicas, através de empresa terceirizada e independente, com vistas à lisura e à transparência do procedimento.

Fica a Contratada responsável por realizar auditorias regulares de toda a solução com intervalo não superior a 6 meses, entregando os relatórios à Contratante, contendo também os resultados dos testes de segurança, devendo este procedimento ser classificado como Auditoria Interna.

Exemplo dos Relatórios que devem ser apresentados a Contratante regularmente:

- Relatório de segurança;
- Relatório de desempenho;
- Relatório de integridade de dados;
- Relatório de conformidade regulatória;
- Relatório de conformidade de segurança;
- Relatório de avaliação de ameaças e vulnerabilidades;
- Relatório de avaliação de riscos cibernéticos;
- Relatório de avaliação de continuidade de negócios;
- Relatório de avaliação de conformidade de privacidade;
- Relatório de avaliação de controles internos;
- Relatório de avaliação de segurança física;
- Relatório de gerenciamento de riscos;

- Relatório de plano de continuidade de negócios;
- Relatório de governança de TI;
- Relatório de revisão de acesso de usuário;
- Relatório de revisão de gestão de identidade;
- Relatório de revisão de segurança de rede;
- Relatório de revisão de políticas de segurança;
- Relatório de revisão de backup e recuperação de desastres;
- Relatório de revisão de gestão de incidentes de segurança;
- Relatório de revisão de gestão de incidentes;
- Relatório de revisão de gestão de riscos;
- Relatório de revisão de gestão de mudanças.

11 DA VISTORIA PRÉVIA AOS LOCAIS DE INSTALAÇÃO DA SOLUÇÃO

De acordo com o art. 67, inc. VI, da nova Lei de Licitações, a Administração exigirá na habilitação técnica declaração de que o licitante tomou conhecimento de todas as informações e das condições locais para o cumprimento das obrigações objeto da licitação.

Esta declaração, conhecida como "visita técnica" ou "vistoria técnica" tem como objetivo viabilizar ao licitante amplo conhecimento das especificidades locais, propiciando condições mais concretas para a apresentação das propostas.

A exigência está baseada nos seguintes parágrafos do art. 63 da nova Lei:

"§ 2º Quando a avaliação prévia do local de execução for imprescindível para o conhecimento pleno das condições e peculiaridades do objeto a ser contratado, o edital de licitação poderá prever, sob pena de inabilitação, a necessidade de o licitante atestar que conhece o local e as condições de realização da obra ou serviço, assegurado a ele o direito de realização de vistoria prévia.

§ 3º Para os fins previstos no § 2º deste artigo, o edital de licitação sempre deverá prever a possibilidade de substituição da vistoria por declaração formal assinada pelo responsável técnico do licitante acerca do conhecimento pleno das condições e peculiaridades da contratação.

§ 4º Para os fins previstos no § 2º deste artigo, se os licitantes optarem por realizar vistoria prévia, a Administração deverá disponibilizar data e horário diferentes para os eventuais interessados. (Grifo nosso).

As regras acima incorporaram reiteradas orientações do Tribunal de Contas da União acerca do assunto, que citamos a título de ilustração: Acórdão nº 372/2015, Acórdão nº 1.447/2015, Acórdão nº 656/2016, Acórdão nº 2.939/2018, todos do Plenário.

Desta forma, as proponentes deverão apresentar Atestado de Visita Técnica dos locais de

instalação da solução, cujo documento será expedido pela empresa com a assinatura do servidor público que acompanhou a visita, em consonância com o que dispõe a legislação.

Caso a proponente deseje participar da vistoria prévia, esta deverá ser feita com a participação do Responsável Técnico da empresa, devidamente qualificado para este fim, que poderá estar acompanhado por no máximo mais duas pessoas, todas vinculadas à empresa licitante. Tal prática visa proporcionar um melhor conhecimento do escopo dos serviços a serem desenvolvidos naquele local.

A Declaração em epígrafe terá por escopo demonstrar que a empresa vistoriou os locais de realização dos serviços e que tomou conhecimento de todos os detalhes que se farão necessários à apresentação de sua proposta e à execução dos serviços.

A vistoria deverá ser agendada com antecedência pela licitante, através do telefone (51) 3288-1926 ou do e-mail dtic@ssp.rs.gov.br. A visita deverá ocorrer após a publicação do respectivo Edital, estendendo-se o prazo até dois dias úteis anteriores à data prevista para a abertura da Sessão Pública.

A visita só será autorizada se observadas as seguintes exigências: enviar previamente relação por escrito contendo nome completo, RG e CPF de todos os funcionários que participarão da vistoria. Estes dados poderão ser analisados pela equipe de inteligência da Secretaria de Estado da Segurança Pública, para fins de controle da segurança interna dos locais.

As empresas que optarem por não participar da vistoria deverão apresentar, no momento da habilitação, Declaração Formal, assinada pelo seu Responsável Técnico e do Representante Legal da empresa, sob as penas da lei, alegando que possui pleno conhecimento das condições e peculiaridades inerentes à natureza do local, assumindo total responsabilidade por esse fato e informando que não o utilizará para quaisquer questionamentos futuros que ensejem desavenças técnicas ou financeiras com o órgão licitante.

A proponente que decidir não realizar a vistoria e, eventualmente, subestimar sua proposta, estará incorrendo em risco típico do negócio, não podendo, futuramente, opô-lo contra a Administração para eximir-se de qualquer obrigação assumida ou para rever os termos do contrato.

12. AVALIAÇÃO DAS AMOSTRAS TÉCNICAS

12.1 COMISSÃO DE AVALIAÇÃO DAS AMOSTRAS

O procedimento de avaliação das amostras de que trata o item “Das Amostras” do Termo de Referência será conduzido por comissão especialmente designada, composta por integrantes técnicos da Secretaria da Segurança Pública;

12.2 DA ENTREGA DAS AMOSTRAS

Os equipamentos solicitados para análise pelo pregoeiro deverão ser entregues para a análise em até 5 (cinco) dias uteis a contar do dia subsequente a da solicitação.

O pregoeiro responsável pelo certame conduzirá o processo de conferências dos itens entregues, juntamente com toda a documentação fornecida pela empresa.

Após análise da amostra a comissão técnica designada emitira parecer ao Pregoeiro positivo ou negativo em relação ao atendimento técnico da solução apresentada.

12.2.1 TESTE DE ACEITAÇÃO

Escopo dos testes

O Teste de Aceitação é fase fundamental para que se possa verificar a efetividade do funcionamento da solução a ser adquirida pela Contratante. Neste aspecto e, tendo em vista que o objetivo principal do projeto é a análise de dados e imagens oriundos de equipamentos eletrônicos, as quais provêm dos municípios que as originam e devem ser integradas às soluções existentes e em uso na SSP-RS, deve-se basear esta integração a plataforma integrada de gestão, para que a Contratante possa tomar decisões impulsionadas pelos dados minerados de forma adequada possibilitando uma visão abrangente dos dados, os quais poderão ser utilizados para gerar mudanças positivas, eliminando a ineficiência e adaptando-se rapidamente às mudanças nas cadeias de fornecimento de informações.

Com isto, a demonstração de adequada e efetiva integração de ferramentas manipuladoras de dados e imagens se faz fundamental para a persecução do objetivo finalístico do projeto: captura, análise, mineração, interpretação e utilização dos dados e imagens obtidos a partir das gerações ocorridas nos municípios.

Desta forma, através da adequada integração entre as soluções ofertadas e aquelas existentes na SSP-RS, a execução dos Testes de Aceitação, na prática, é um procedimento cujo objetivo é provar a viabilidade da Soução proposta e validá-lo em escala de execução.

Para comprovação das funcionalidades da aplicação será necessário a integração de ao menos dois dispositivos de captura ofertados na proposta (câmera fixa e câmera OCR) e ao menos um ponto de coleta do parque existente (Avançar I) em dois municípios do Estado do Rio Grande do Sul com a SSP-RS, demonstrando todas as soluções ofertadas de maneira centralizada, respeitando os requisitos solicitados no Termo de Referência.

12.2.2 PERÍODO DE AVALIAÇÃO

O processo de Teste de Aceitação ocorrerá em até 10 (dez) dias uteis, contados do primeiro dia útil subsequente a entrega das amostras.

O período de avaliação poderá se estender por período superior a este mediante o despacho fundamentado do Pregoeiro, por solicitação da Comissão de Avaliação.

Local e Horário

Os testes ocorrerão nas dependências na sede da SSP/RS

12.2.3 FORMAS DE MENSURAÇÃO E ANÁLISE

Os técnicos da Comissão de avaliação verificarão os requisitos técnicos selecionados dentre os requisitos exigidos no Termo de Referência de forma objetiva. Para cada item avaliado será atribuído o critério aprovado ou reprovado. Com base nos requisitos técnicos previstos no Termo de Referencia, será elaborado um Caderno De Testes que contemple os testes necessários a validação dos quesitos relacionados.

- Ordem da Avaliação

  As amostras serão analisadas uma por vez, observando a ordem dos itens selecionados.

- Inspeções

  As comprovações dos requisitos poderão ser feitas da seguinte maneira:

  - Por observação física do componente / requisito;
  - Por verificação de software, em especial para os casos dos testes de desempenho e funcionalidades.

Avaliação dos Membros da Comissão

As anotações de aprovação e reprovação dos itens será efetuada pela comissão de avaliação em escrutínio reservado. Os membros da comissão não informarão no momento da avaliação se o item foi aprovado ou reprovado.

A reprovação de um item será sempre fundamentada e deverá constar no relatório final do processo de avaliação das amostras.

Regras a Serem Observadas

Durante a reunião não será permitido ao público presente o uso de telefones celulares, estes, portanto, devem permanecer desligados ou em modo reunião.

O critério observado pela a administração para atendimento a um item poderá ser visto por qualquer um dos presentes, bastando que para isso, seja solicitada a vistas.

12.2.4 ACOMPANHAMENTO DO PROCESSO DE ANÁLISE

O processo de análise das amostras será publico, obedecidas às condições aqui estabelecidas:

Fica assegurado o direito dos membros da Comissão para peticionar tempo reservado para a discussão de temas relevantes, devendo todos os membros presentes ao local de avaliação retirar-se durante este período.

13 DA FISCALIZAÇÃO

Sujeitar-se-á a Contratada à mais ampla e irrestrita fiscalização da autoridade encarregada de acompanhar a execução do objeto desta licitação, prestando todos os esclarecimentos solicitados e atendendo às exigências formuladas dentro das prescrições legais.

A fiscalização da Contratante não eximirá, em hipótese alguma, a Contratada de quaisquer outras fiscalizações de órgãos oficiais, quanto às obrigações tributárias, fiscais, trabalhistas e demais que se fizerem necessárias.

A fiscalização não exclui nem reduz a responsabilidade da Contratada, inclusive perante terceiros, por qualquer irregularidade resultante de imperfeições técnicas, vícios redibitórios ou emprego de material inadequado ou de qualidade inferior e, na ocorrência deste, não implica corresponsabilidade da Administração Contratante ou de seus agentes e prepostos.

Quaisquer exigências da fiscalização, inerentes ao objeto do presente Edital, deverão ser prontamente atendidas pela Contratada, sem ônus para a Contratante.

Os critérios e procedimentos relativos à fiscalização do objeto estão abaixo definidos:

- O responsável pelo acompanhamento e fiscalização do contrato a ser firmado será o servidor designado pela Administração, que atuará orientando, fiscalizando e intervindo no interesse da SSP-RS, a fim de garantir o exato cumprimento das cláusulas e condições pactuadas entre as partes;

- Após a assinatura do Contrato, a SSP-RS designará formalmente, na forma do art. 117 da Lei 14.133/2021, servidor (es) com autoridade para exercer, como representante da Administração da SSP-RS, toda e qualquer ação de orientação geral, acompanhamento e fiscalização dos serviços contratados;

- A SSP-RS poderá contratar terceiros para assistir e subsidiar o(s) fiscal(is) com informações pertinentes ao acompanhamento e à fiscalização contratual;

- É direito da Fiscalização rejeitar quaisquer serviços/fornecimentos quando entender que se encontram fora das especificações técnicas definidas pelo Órgão;

- À Fiscalização compete, dentre outras atribuições:

a) encaminhar à Administração o documento que relacione as ocorrências que impliquem em multas ou outras penalidades a serem aplicadas à Contratada;

b) zelar para que o objeto da contratação seja fielmente executado conforme o ajustado no contrato;

c) anotar em documento próprio as ocorrências;

d) determinar a correção de faltas ou defeitos;

e) encaminhar à autoridade superior as providências cuja aplicação ultrapasse o seu nível de competência, etc.

- A fiscalização de que trata este item não exclui nem reduz a responsabilidade da Contratada, inclusive perante terceiros, por qualquer irregularidade, ainda que, resultante de imperfeições

técnicas, vícios redibitórios, de equipamentos inadequados ou de qualidade inferior, e, na

ocorrência desta, não implica em corresponsabilidade da Administração ou de seus agentes e prepostos, de conformidade preconiza o artigo 120 da Lei 14.133/2021.

14 DO RECEBIMENTO DO OBJETO

O objeto da licitação deverá ser entregue nos prazos e condições previstas no Termo de Referência, devidamente instalados, configurados, integrados e em plenas condições de funcionamento, nos locais determinados pela Contratante, no prazo máximo de 180 (cento e oitenta) dias, devendo a contratada apresentar no prazo de 30 (trinta) dias, após a assinatura do contrato, projeto executivo com cronograma de execução, totalizando o prazo de 210 (duzentos e dez) dias.

A execução dos serviços será acompanhada e fiscalizada por executor designado pela Contratante, que anotará em registro próprio todas as ocorrências, determinando o que for necessário a regularização das faltas ou defeitos observados, além das atribuições contidas nas Normas de Planejamento, Orçamento, Finanças, Patrimônio e Contabilidade da Contratante.

A entrega deverá ocorrer em dia de expediente da Contratante, nos horários compreendidos entre 09h00 às 17h00.

O objeto desta licitação será recebido, por servidor ou comissão designada pela autoridade competente, mediante termo circunstanciado, assinado pelas partes, da seguinte forma:

- PROVISORIAMENTE, pela Comissão, mediante termo detalhado; e

- DEFINITIVAMENTE, por comissão designada pela autoridade competente, mediante termo detalhado, assinado pelas partes, que comprove o atendimento das exigências contratuais, observado o disposto no art. 199 da Lei nº 14.133/21.

Após o recebimento definitivo do objeto, será atestada a Nota Fiscal para efeito de pagamento.

O recebimento provisório ou definitivo não exclui a responsabilidade civil pela solidez e segurança do material/equipamento, nem ético-profissional pela perfeita execução do Contrato, dentro dos limites estabelecidos pela lei ou pelo Contrato.

Se a contratada deixar de entregar a solução dentro do prazo estabelecido sem justificativa por escrito, aceita pela Administração, sujeitar-se-á às penalidades impostas na Lei Federal n° 14.133/21 e alterações subsequentes, neste Edital e no Termo de Referência.

A empresa deve efetuar a troca, às suas expensas, dos produtos que não atenderem às especificações do objeto contratado no prazo de 10 (dez) dias corridos, a contar do recebimento da solicitação, sendo que o ato de recebimento não importará aceitação.

A Contratada deverá fornecer equipamentos com certificado de homologação na ANATEL para aqueles que são exigidos. Os certificados aceitos, em caso de equipamentos cuja homologação

não seja compulsória pela ANATEL, serão aqueles emitidos por organizações designadas pela ANATEL.

Os bens poderão ser rejeitados, no todo ou em parte, quando em desacordo com as especificações constantes neste Termo de Referência, devendo ser substituídos no prazo de 10 (dez) dias corridos, a contar da notificação da Contratante, às custas da CONTRATADA, sem prejuízo da aplicação das penalidades.

A Contratante emitirá o Termo de Recebimento Provisório em até 10 (dez) dias, após o recebimento do comunicado de conclusão da solução, salvo se existirem pendências identificadas e comunicadas à Contratada, situação em que o prazo ficará sobrestado até a solução da pendência.

Os bens não utilizados imediatamente após o recebimento definitivo serão armazenados com segurança e protegidos contra a ação dos perigos mecânicos, das ameaças climáticas e de animais daninhos, conforme determina a legislação vigente.

15 DA SUBCONTRATAÇÃO

A Contratada, na execução do contrato, sem prejuízo das responsabilidades contratuais e legais, poderá subcontratar partes da obra, serviço ou fornecimento, até o limite de 30%, sempre com a anuência da Administração nos termos do artigo 122 da Lei nº 14.133/21, conforme abaixo se descreve:

> "Art. 122. Na execução do contrato e sem prejuízo das responsabilidades contratuais e legais, o contratado poderá subcontratar partes da obra, do serviço ou do fornecimento até o limite autorizado, em cada caso, pela Administração.
>
> § 1º O contratado apresentará à Administração documentação que comprove a capacidade técnica do subcontratado, que será avaliada e juntada aos autos do processo correspondente.
>
> § 2º Regulamento ou edital de licitação poderão vedar, restringir ou estabelecer condições para a subcontratação.
>
> § 3º Será vedada a subcontratação de pessoa física ou jurídica, se aquela ou os dirigentes desta mantiverem vínculo de natureza técnica, comercial, econômica, financeira, trabalhista ou civil com dirigente do órgão ou entidade contratante ou com agente público que desempenhe função na licitação ou atue na fiscalização ou na gestão do contrato, ou se deles forem cônjuge, companheiro ou parente em linha reta, colateral, ou por afinidade, até o terceiro grau, devendo essa proibição constar expressamente do edital de licitação".

A empresa vencedora da licitação deve apresentar comprovante de capacidade técnica da Subcontratada, que vai ser avaliada e juntada aos autos do processo.

A empresa vencedora da licitação não pode fazer a subcontratação de qualquer pessoa física ou jurídica com quem tenha vínculo de natureza técnica, comercial, econômica, financeira,

trabalhista ou civil com os quadros da administração pública responsáveis pela realização do certame e fiscalização dos contratos.

Será admitida a subcontratação de serviços acessórios referentes a infraestrutura, links, rede elétrica, rede lógica e seca, desde que previamente aprovada pela Contratante. Todavia, a Contratada será a única e exclusiva responsável pela execução do objeto, não tendo a Subcontratada qualquer vínculo com a Contratante.

Não poderá ser subcontratado o fornecimento dos equipamentos, materiais e softwares e os serviços de implantação da solução ofertada, além dos serviços de treinamento e suporte técnico.

16 DOS CRITÉRIOS DE SUSTENTABILIDADE

Conforme dispõe o art. 144 da Lei n. 14.133/2021, a Contratada será responsabilizada por qualquer prejuízo que venha causar à Contratante em virtude de ter suas atividades suspensas, paralisadas ou proibidas por falta de cumprimento de normas ambientais ligadas aos serviços e produtos objeto do presente Termo de Referência.

A Contratada deverá fornecer, no que for possível, e no que couber, solução que esteja de acordo com as normas atinentes à sustentabilidade.

A Contratada deverá respeitar a legislação vigente e as normas técnicas, elaboradas pela ABNT e pelo INMETRO para aferição e garantia de aplicação dos requisitos mínimos de qualidade, segurança e acessibilidade dos serviços elencados neste Termo de Referência.

17 FORMAS E CRITÉRIOS DE SELEÇÃO DO FORNECEDOR

O licitante será selecionado por meio da realização de procedimento de licitação, na modalidade de pregão eletrônico, com fundamento no art. 28, inciso I, da Lei n° 14.133, de 2021.

O critério de julgamento será o de menor preço global, devendo ser atendidas às exigências do Edital e de seus Anexos. A aceitação do objeto será feita por meio de análise comparativa entre a proposta das licitantes e o descrito no Termo de Referência e no Edital.

CADERNO II - ESPECIFICAÇÕES TÉCNICAS

DOS KITS – CERCAMENTO – MONITORAMENTO – MANUTENÇÃO

ITEM	DESCRIÇÃO	Especificações
1	**KIT 1- Pontos completos de Cercamento Eletrônico**	
1.1	**Ponto de Cercamento**	**1.1.1 CÂMERA OCR** Deverá ser fornecido 02 (dois) câmeras IP do tipo Bullet para leitura e análise de metadados de veículos, em tempo real, com as seguintes características: • Deve ser dotada de mecanismo de inteligência artificial de alto desempenho; • Deve possuir algoritmo de aprendizado que permita leitura e análise de metadados de veículos, em tempo real, com a velocidade mínima de 140 km/h; • Deve suportar o modo infravermelho (IR), à noite, para redução de poluição luminosa; • Deve possuir processar de alta performance embarcado; • Deve possuir sensor de imagem CMOS 1/3"; • Deve possuir obturador único; • Deve possuir velocidade de shutter de 1/50 s–1/100000 s, em modo automático e manual; • Deve possuir modo de exposição com íris fixa/manual/auto/P; • Deve possuir resolução de imagem mínima de 2688 x 1520; •Deve possuir resolução de vídeo de 4M(2688 x 1520), UXGA (1600 × 1200), 720P (1280 × 720), D1 (704 × 576), CIF (352 × 288); • Deve possuir taxa de quadros de vídeo: Máximo 25fps;; • Deve possuir taxa de bits de vídeo: H.264: 32kbps–32767kbps, H.265: 32kbps–32767kbps, MJPEG: 512kbps–32767kbps; • Deve possuir compressão de vídeo H.265, H.264M, H.264H, H.264B, MJPEG; • Deve possuir formato de codificação de imagem JPEG; • Deve possuir WDR de 140 dB; • Deve possuir redução de ruído 2DNR, 3DNR; • Deve possuir suporte a HLC, correção de pixel ruins, melhoria de bordas; • Deve possuir 4 mecanismos embarcados de iluminação, com LEDs infravermelho de, no mínimo, 850 nm e brilho ajustável; • Deve possuir suporte a composição de 1, 2, 3 ou 4 imagens; • Deve possuir mecanismo de disparo (trigger) por meio de detecção de vídeo ou radar/laço indutivo; • Deve possuir mecanismo de sobreposição OSD que permita, minimamente, as seguintes detecções: O Veículos motorizados: tempo, localização (localização do canal de vídeo), faixa (número, direção), placa (número e cor), velocidade, região, cor do veículo, logotipo do veículo, tipo de veículo; O Veículos não motorizados: presença/ausência de capacete, sobrecarga de passageiros; • Deve permitir armazenamento através de mecanismo FTP ou cartão TF com capacidade de até 256 Gb, classe 10; • Deve possuir alarmes para, no mínimo: armazenamento cheio, erro de armazenamento, alarme externo, sem cartão de armazenamento, lista de bloqueio de placa de veículo, acesso ilegal, desconexão de rede e conflito de endereço IP; • Deve possuir mecanismo de prevenção contra adulteração de imagens através de marca d'água e verificação de vídeo e imagens; • Deve possuir mecanismos de segurança baseados em nome de usuário e senha autorizados, ligação de endereço MAC, criptografia HTTPS e controle de acesso à rede; • Deve possuir suporte automático a linhas de detecção de desenho; • Deve possuir lente varifocal motorizada embutida de 10 mm a 40 mm; • Deve possuir suporte aos seguintes mecanismos de inteligência: o Detecção de alvo para veículos motorizados e não motorizados; o Deve permitir reconhecimento de placas (matrículas) veiculares (LPR) através do emprego de algoritmo de auto desenvolvimento para reconhecer placas de veículos combinando números e letras; o Deve possuir mecanismo que permita o reconhecimento de veículos com visualização frontal, identificando: ônibus, ônibus médio, SUV, MPV, picape, caminhão pesado, caminhão médio, carro, van e caminhão leve e, com visualização da traseira, identificando: SUV, carro, van, ônibus, picape, caminhão de carga, mini caminhão, caminhão tanque e caminhão betoneira; o Deve efetuar o reconhecimento de cores de veículos, durante o dia, identificando, minimamente: branco, rosa, preto, vermelho, amarelo, cinza, azul, verde, âmbar, roxo, marrom, cinza prateado; o Deve permitir a identificação, em relação a veículo motorizado, de: placa, tipo de veículo, cor do veículo, cor da placa, logotipo do veículo e, em relação a veículo não motorizado: tipo (duas rodas, três rodas), cor. • Deve possuir as seguintes interfaces: o Uma interface de rede RJ45 10/100/1000M; o Uma interface RS-485, para conexão a dispositivos como radar/laço indutivo; o Duas interfaces RS-232, sendo uma "G T R" para depuração serial e uma "G T1 R1" para conexão ao radar/laço indutivo; o Duas interfaces de entrada de alarme, sendo uma para relé e uma optoacopladora; o Duas interfaces de áudio, sendo uma de entrada e uma de saída. • Deve possuir alimentação 12V DC, 36V DC, PoE, com consumo ≤ 8W; • Deve operar em faixa de temperatura de −40°C a +65°C, com umidade entre 10%–90%; • Deve possuir grau de proteção IP67; • Deve possuir certificação CE, FCC, UL. 1.1.2 POSTE METÁLICO Estrutura metálica de sustentação tipo semipórtico, com as seguintes características: • Deve ser projeto para instalação de câmeras CFTV;

		• Deve possuir coluna cônica contínua reta, de seção circular; • Deve possuir braço de 2,5m de projeção horizontal; • Construção em tubo de aço estrutural, galvanizado a fogo conforme norma NBR 6323; • Deve conter altura de 6 metros; • Deve conter estrutura projetada para suportar vento de 45m/s; • Deve estar de acordo com a norma NBR6123; 1.1.3 NOBREAK TIPO 600 O equipamento deverá ser novo (sem uso) e estar na linha atual de produção do fabricante. • Possuir tensão de entrada nominal 220V; • Possuir potência de saída nominal contínua 600VA/300W; • Possuir fator de potência de 0,5; • Deve possuir tensão de saída nominal de 220V; Deve operar em frequência de saída em modo bateria 60Hz; • Possuir tomadas de acordo com a norma NBR 14136; • Deve possuir bateria do tipo VRLA; • Possuir bateria de 12v 7ah • Deve operar em faixa de temperatura de operação 0°C a 40°C. 1.1.4 SWITCH 8 PORTAS Equipamento para extensão física dos pontos de rede, com as seguintes características: Características • Deve possuir 9 (nove) portas Gigabit Ethernet 10/100/1000Base-T Conforme Padrões IEEE 802.3, IEEE 802.3u, IEEE 802.3ab; • As interfaces deverão ser Full-Duplex, auto sensing com conectores RJ45 fêmea e implementar mecanismos de autoconfiguração em todas as portas, do tipo MDI/MDI-X; • Deve possuir adicionalmente no mínimo 1 (um) porta Gigabit Ethernet Padrão IEEE 802.3z, para inserção de transceivers do tipo SFP; • As interfaces dos itens 1. e 3. devem operar de modo simultâneo; • Deve possuir leds indicativos de funcionamento; • Deve implementar os padrões IEEE 802.3at e IEEE 802.3af, em pelo menos 8 (portas); • Deve ser capaz de fornecer até 30W por porta (não simultâneo); • Deve possuir o Budget PoE de no mínimo 63W; • Deve possuir capacidade de processamento de no mínimo 20 Gbps; • Deve possuir taxa de encaminhamento de pacotes igual ou superior a 14.88 Mbps; • Sua tabela de MAC Address deve suportar no mínimo 4.000 MAC address; • Deve suportar jumbo frame de no mínimo 16KB; • O equipamento deve possuir no máximo até 1 (uma) ventoinhas internas para resfriamento; • Deve suportar temperatura de operação entre 0° e 50°; • Deve suportar operação sob umidade entre 10% e 90% RH sem condensamento; • Deve compatível com PDs compatíveis com IEEE 802.3af/at; • Deve suportar controle de fluxo EEE802.3x; • Deve suportar 802.1p/DSCP QoS; • Deve suportar IGMP Snooping; • Possuir homologação da ANATEL, de acordo com a resolução número 242 de 30/11/2000; • Possuir Certificação FCC e CE; • Deve ser RoHS (Restriction of Certain Hazardous Substances) Compliance; 1.1.5 ENTRADA ELÉTRICA • Conjunto para a conexão à rede de energia elétrica da concessionária local dentro das normas exigidas para conexão dos dispositivos à rede elétrica, além das normas da ABNT e ANEEL; • Todos os materiais e miscelâneas necessários para a instalação do padrão indicado, devem estar contemplados na proposta da licitante. • O cabeamento elétrico deverá interligar a caixa de equipamentos com o ponto/circuito de energia compatível mais próximo, após comprovada a compatibilidade do circuito; 1.1.6 CAIXA PORTA EQUIPAMENTOS Caixa metálica externa, tipo porta-equipamentos, com as seguintes características: • Deve ser fabricada em chapa de aço carbono SAE 1010/ 1100, com espessura mínima de 1,5mm; • Deve possuir dimensões externas de: (H) 600 mm, (L) 525 mm e (P) 600 mm, com tolerância de 2% nas medidas; • Deve possuir Kit de ventilação com dois ventiladores para teto; • Deve possuir abertura para ventilação forçada; • Possuir no mínimo um ventilador, padrão universal; • Deve possuir porta frontal com fechadura e chave; • Deve possuir grau de proteção IP65; • Deve possuir duas prateleiras, no interior da caixa para instalação de equipamentos, placa de montagem fabricada em chapa de aço carbono com espessura 1,5 mm; • Deve ser pintada utilizando tratamento de superfície para proteção e pintura epóxi; • Índice de Proteção (IP) – Mínimo IP 65 (selada contra poeira e protegidas contra jatos de água); • Deve permitir capacidade de carga de no mínimo 100kg; • Deve estar de acordo com a norma de antivandalismo; • Deve possuir calha elétrica.

		1.1.7 INFRAESTRUTURA • Todos os pontos deverão ser fornecidos com a infraestrutura, descrita abaixo: • Deverão ser personalizadas/detalhadas em plantas ou esquemas elétricos específicos, incluindo aterramento; • O cabeamento elétrico deverá interligar a caixa de equipamentos com o ponto/circuito de energia compatível; • O cabeamento deverá ser ligado dentro da caixa de equipamento ao disjuntor (em série com a fase) e ao varistor (em paralelo); • O dimensionamento do cabeamento deverá ser feito em função da distância e da carga, não podendo ser usada bitola de condutores com diâmetro menor que 2,5 mm²; o cabeamento usado deverá ser do tipo PP, SINTENAX ou equivalente, com três condutores encapados, envolvidos por grossa camada de borracha, de modo que seja imune a água, umidade e intempéries; • A rede elétrica de alimentação dos equipamentos será monofásica, para alimentação em 127V (cento e vinte e sete Volts). A alimentação poderá ser em 220V (duzentos e vinte Volts); • Os pontos deverão ter conectores do tipo RJ45 fêmea, para categoria 5e, com espelhos e identificação. A rede deverá ser instalada e certificada. • Os custos e execução são de inteira responsabilidade da empresa Contratada; • Deverá ser fornecido pela empresa a ser contratada, os materiais de infraestrutura necessários para instalação: • Eletrodutos de PVC; • Luvas; • Abraçadeiras • Cintas de alumínio; • Mangueira de manobra; • Parafusos e buchas; • Cabos elétricos; • Cabo UTP.
1.2	Licença de Software Análise Comportamental	1.2.1 LICENÇA DE SOFTWARE ANÁLISE COMPORTAMENTAL DA MALHA VIÁRIA LICENÇA DE SOFTWARE ANÁLISE COMPORTAMENTAL DA MALHA VIÁRIA • Possibilitar a utilização de, no mínimo, 20 estações de trabalho conectadas simultaneamente e suportando múltiplas requisições de pesquisas. • Ser capaz de receber e processar até 1500 passagens veiculares por minuto. • Suportar conexão de 400 câmeras. • Suportar conexão de 200 smartphones para uso das forças policiais • Suportar no mínimo, câmeras de 4 fabricantes diferentes, para uso em Pontos de coleta de imagens. • Apresentar todas as interfaces com o usuário em português do Brasil. • Utilizar login único para todo o sistema, permitindo deste momento em diante acessar qualquer módulo, respeitando as permissões de acesso de cada usuário, sem a necessidade de um novo login. • Suportar bloqueio por inatividade após tempo especificável em minutos, obrigando ao usuário a efetuar novo login. • Suportar mudanças obrigatórias de horário de verão (se existirem) de forma programada e automática mantendo, sem intervenção humana, todo o sistema atualizado para o período. • Permitir o cadastramento de telefones celulares para todas as interações exigidas ao longo deste Termo de Referência. • Suportar base única de cadastro de usuários e senhas, que serão utilizados para acesso a TODOS os módulos da solução proposta, que exigirem autenticação. • Suportar base única de cadastro de dados sobre veículos, que será utilizada pelos módulos da solução proposta e para autopreenchimento em cadastros, incluindo, mas não se limitando a: Marca, modelo, cor, ano de fabricação, ano do modelo, Tipo do veículo, município e estado. • Suportar base única de cadastro de dados sobre indivíduos (pessoas), que será utilizada pelos módulos da solução proposta e para autopreenchimento em cadastros. • Suportar base única de endereços que será compartilhada pelos módulos que exigirem o cadastro de endereço. • Disponibilizar módulos capazes processar as imagens recebidas dos PCLs para classificação de tipos veiculares, marca e modelo, baseando-se unicamente na capacidade de processamento da imagem, inclusive para veículos sem placas. • As classificações veiculares deverão ser no mínimo as seguintes: Carro, motocicleta, caminhão, ônibus, Van/Furgão, caminhonete, carro forte. • Disponibilizar módulo capaz realizar OCR nas imagens recebidas dos PCLs sem a leitura dos caracteres, suportando todos os formatos de placas veiculares do Brasil e do Mercosul e garantindo um índice mínimo de 90% de leituras corretas, considerando-se imagens eleitas como legíveis. • Serão consideradas imagens legíveis, aquelas que apresentam caracteres perfeitamente reconhecidos pelo olho humano, desconsiderando-se àquelas com um ou mais caracteres que suscitem dúvidas ou que sofreram interferências naturais como reflexos, efeitos glare ou flare etc. • Fornecer módulo único para gerenciar os recebimentos das imagens e dados provenientes das passagens de veículos capturadas pelos PCLs • O módulo gerenciador de recebimento deverá fornecer interface gráfica que exiba em tempo real e sem intervenção humana, as imagens recebidas dos PCLs, imediatamente após a chegada, de maneira a poder-se visualizar de forma clara e separadamente, as imagens recebidas de todas as câmeras utilizadas pela solução, em um ou mais monitores, configurada livremente pelo operador, variando de 1 a 40 câmeras por monitor • Contar com sistema gerenciador de bancos de dados. • Permitir a utilização de hardware com múltiplos volumes de armazenamento de imagens, suportando volumes de armazenamento com diferentes tamanhos. • Armazenar as imagens processadas de forma protegida, impossibilitando a visualização por outros softwares. • Permitir ao operador configurar a compactação e redimensionamento das imagens, de forma a aumentar a capacidade de dias armazenados, devendo no mínimo:

		• Permitir configurar para cada câmera, a quantidade de dias que o sistema deverá armazenar as imagens no tamanho original, antes de proceder com a compressão das imagens. • Permitir que o operador defina a qualidade e dimensões da imagem após compressão, exibindo, em tempo de configuração, as imagens lado a lado, no formato "antes e depois", permitindo a verificação visual de como ficarão as imagens após a compressão em relação às imagens originais. • Exibir, em tempo de configuração, a quantidade em KB da imagem original e quantos KB terá após a compressão. • Fornecer interface gráfica que exiba o status de funcionamento dos dispositivos ativos utilizados nos PCLs, indicando sem intervenção humana, possíveis falhas que ocorram, permitindo alertar os operadores quanto ao funcionamento do sistema. • Fornecer módulo para cadastramento de dados referentes a "fatos ocorridos", (que possuam Boletins de ocorrência) e "atos classificáveis como delituosos" (que não possuam boletins de ocorrência) e o agrupamento de informações sobre suas ENTIDADES (elementos de informações que referenciam ou identificam alguém ou algo relacionado ao fato registrado no sistema). • Este módulo, ora em diante, será referenciado apenas por "REGISTRO DOS FATOS" e deverá: • Permitir o cadastro de ENTIDADES de um FATO no mínimo para: Múltiplos indivíduos, múltiplos veículos, múltiplos objetos relacionados ao fato, múltiplos endereços eletrônicos (links) com informações relacionadas ao fato. • Possibilitar atribuir ao Fato cadastrado o intervalo de data, horas e minutos relativos ao seu início e fim, definindo assim o tempo de duração estimada de determinados fatos. • Possibilitar atribuir ao FATO cadastrado, a condição de ser privado, com acesso somente para o usuário responsável pelo cadastro. • Possibilitar atribuir ao FATO cadastrado, a permissão de acesso para outros operadores da mesma CAM devendo ser no mínimo para: • Para todos os operadores. • Para um ou mais grupos de operadores predefinidos pelo administrador. • Somente operadores autorizados pelo administrador poderão permitir compartilhamentos • Permitir, quando as Entidades forem veículos e suas respectivas placas, que estas sejam selecionadas para monitoramento com geração de alarmes, sendo obrigatório no mínimo dois tipos de monitoramento a saber: • Monitoramento Simples: Monitoramento sem exigências de identificação do operador e assinatura após os alarmes. • Monitoramento Supervisionado: Monitoramento que exigirá, após os alarmes, uma sequência de passos pelos operadores com posterior verificação por usuários de hierarquias superiores (administradores ou supervisores). • Permitir, quando as Entidades forem veículos e suas respectivas placas, que estas sejam selecionadas para monitoramento de qualquer tipo; que seja definido o nível de semelhança entre a informação cadastrada e a informação extraída da imagem e que quando esta semelhança existir, provoque um alarme. (Considerar semelhança quando os caracteres da placa veicular, extraídos da imagem, forem coincidentes com a informação cadastrada, sendo no mínimo para 6 ou 7 caracteres idênticos). • Deverá ser permitida a definição de intervalo de tempo para que o nível de semelhança definido seja considerado • Permitir, quando a Entidade for um veículo com sua respectiva placa selecionada para monitoramento, que seja definida uma periodicidade para a validade do monitoramento, podendo-se escolher em quais dias da semana, em quais intervalos de horas, quais PCLs e para quais câmeras o sistema emitirá alarmes; • Disponibilizar em tela, alerta visual e permanente, indicando quando a placa de um veículo cadastrada já estiver cadastrada em um ou mais registro(s) de fato(s), possibilitando a partir da mesma tela a exibição dos dados dos outros registros de fatos relacionados • Permitir, em tempo de cadastramento, quando a Entidade for um veículo, que seja possível a partir da tela de cadastramento, executar pesquisa das passagens registradas do veículo em questão, exibindo os resultados em ordem decrescente de tempo. • Permitir, quando a Entidade for um veículo com sua respectiva placa selecionada para monitoramento, que sejam definidos os telefones celulares previamente cadastrados para os quais, o sistema enviará os alarmes. • Quando a ENTIDADE cadastrada for uma pessoa, possibilitar a inserção de dados de qualificação, incluindo foto, que identifiquem esta pessoa, e também a anexação de múltiplos arquivos digitais de qualquer tipo. • Permitir a qualquer momento a visualização de todas as alterações nos registros dos fatos, efetuadas por qualquer operador, respeitando as devidas permissões de acesso atribuídas, com indicação de data, hora e usuário e os dados alterados em forma de histórico. • Permitir em tempo de visualização ou edição de um registro do fato, a exibição de todos os alarmes gerados e vinculados a este registro, com anexação de imagens, por tempo indeterminado. • Exibir alerta visualmente destacado ao mostrar dados de um registro de fatos que não possua número identificador de Boletim de Ocorrência quando a natureza do fato exigir o número do Boletim de ocorrência. (parametrizável). • Permitir vincular-se a um registro de fato, determinadas passagens veiculares eleitas pelo operador, com anexação de imagens, por tempo indeterminado. • Permitir em tempo de visualização de um registro do fato, a exibição de todas as passagens veiculares eleitas pelo operador e manualmente associadas a este registro, com exibição de imagens. • Permitir a visualização em lista de todos os registros de fatos com ordenação no mínimo por: Data/hora do cadastro, data/hora da última alteração, Status do registro (ativo ou encerrado), pelas placas de todos os veículos inseridas em registros, por nome do município, pelo tipo de acesso permitido (visibilidade) e por natureza do fato. • Possibilitar busca de registros por: Placa de veículos, data/hora do fato, por intervalo de data/hora e por palavra existente em qualquer campo do tipo texto. • Suportar mecanismos de busca fonética, no mínimo, nos campos destinados aos nomes de pessoas. • Permitir a filtragem no mínimo e de forma combinada: • Por data/hora do FATO, data/hora do cadastro, data/hora da última alteração. • Por registro com dados faltantes. • Pelo operador responsável pelo cadastramento. • Pela origem dos Boletins de ocorrências inseridos nos registros de fatos. • Pelo tipo de acesso permitido. • Por nome do município.

		• Pela natureza do fato. • Pelos nomes das pessoas envolvidas nos registros de fatos • Por tipo de objeto • Por registros de fatos que incluem veículos. • Por registros de fatos que incluem veículos monitorados. • Possuir módulo que possibilite a exibição e gerenciamento dos alarmes no mínimo para os monitoramentos SIMPLES e SUPERVISIONADO, anteriormente definidos, devendo: • Possibilitar que a cada alarme SIMPLES ocorrido, o operador possa visualizar na mesma tela, quais ações e procedimentos específicos foram previamente definidos para o monitoramento em questão. • Possibilitar que a cada alarme SUPERVISIONADO ocorrido, o operador possa visualizar na mesma tela, quais ações e procedimentos específicos foram previamente definidos para o monitoramento em questão e também para os PCLs. • Exibir na mesma tela de Alarme todas as imagens obtidas por ocasião da passagem veicular, inclusive as contextuais. • Permitir zoom da imagem exibida no alarme. • Emitir alarme, sonoro e visual, sempre que identificar na imagem processada, placa veicular exatamente igual àquela previamente cadastrada para monitoramento, exibindo a data, a hora, o local, e imagen(s) do veículo. • Gerar os alarmes com sons absolutamente diferentes para os monitoramentos SIMPLES E SUPERVISIONADOS. • Emitir alarmes, sonoro e visual, sempre que identificar na imagem processada, placa veicular parcialmente igual àquela cadastrada para monitoramento, respeitando o nível de semelhança definido pelo usuário, exibindo a data, a hora, o local, quais caracteres são divergentes daqueles previamente cadastrados e respectivas imagens, de forma a possibilitar alarmes de placas de veículos possivelmente adulteradas. • Possibilitar, a partir do módulo de alarmes, que os operadores com permissão para o referido registro de fato, possam acessar este registro. • Possibilitar que a cada evento de alarme, seja possível a partir da mesma tela, para os operadores com permissão de acesso, observar o perfil comportamental do veículo em questão, de forma a ajudar nas ações necessárias. • Permitir a exibição em mapa, da localização onde foi gerado o alarme. • Dispor de procedimento que silencie e reative o som do alarme. • Quando o monitoramento for SIMPLES, este módulo também deverá: • Permitir ao operador, em sua estação de trabalho, monitorar, de forma contínua e exclusiva, determinada placa veicular, suprimindo, durante este monitoramento, todos os outros alarmes de monitoramentos SIMPLES. • Permitir a filtragem por determinados períodos de data/hora com opção de especificar determinada placa do veículo gerador de alarmes. • Quando o monitoramento for SUPERVISIONADO, também deverá: • Suportar como parametrização do sistema, a supressão total da visualização do alarme pelos operadores, quando as informações e imagens sobre a passagem veicular que gerou o alarme chegarem ao servidor com atraso temporal (em minutos) maior que um limite especificável, mantendo, entretanto, a obrigatoriedade de ciência e assinatura posterior pelos supervisores. • Possuir alarme visualmente diferenciado quando a geração do mesmo ocorrer a partir de um REGISTRO DE FATO que não contiver referência a um boletim de ocorrência de forças de segurança como Guarda Municipal, Polícia Civil, Polícia Militar etc. • Emitir continuamente o som relativo aos alarmes que ainda não foram visualizados, ainda que o módulo em questão seja fechado, obrigando o operador a concluir a ação devida. • Dispor de procedimento para que determinado operador possa silenciar um alarme em todas as estações, notificando a todos os outros operadores que este tornou-se responsável pelo alarme, obrigando ao operador agora responsável, o cumprimento de todas as ações exigidas. • Gerar alarmes de exatidão ou de semelhança com sons absolutamente distintos entre si. • Exibir, a cada alarme, a relação dos alarmes ocorridos anteriormente, para os quais ainda existam procedimentos em aberto, agrupada pela placa veicular e exibindo primeiramente os alarmes mais recentes permitindo navegação pelos registros, com simultânea exibição: • Dos dados dos registros dos fatos cujas ENTIDADES acionaram os alarmes. • Das imagens dos veículos. • Das informações relativas às passagens veiculares. • Dos procedimentos previamente cadastrados nos registros dos fatos. • Impor relação de perguntas previamente cadastradas e referentes aos alarmes, que deverão ser respondidas pelo operador de forma obrigatória ou opcional, de acordo com a parametrização. • As perguntas deverão possibilitar respostas do tipo Sim ou Não ou por texto redigido quando necessário, sendo que as respostas do tipo Sim ou Não, deverão constar em relatórios estatísticos posteriores. • Permitir a finalização do alarme somente quando o operador preencher todos os campos obrigatórios. (Este deverá ser excluído da lista, permanecendo, entretanto, todos os alarmes que não tiveram os procedimentos concluídos). • Permitir a filtragem pelas placas dos veículos geradores dos alarmes. • Exibir, após login do usuário com permissão, a tela de alarme quando existir alarme(s) não finalizado(s). • Suportar como parametrização do sistema que ao soar um alarme, seja apresentado de um alerta visual, indicando que a passagem veicular que gerou o referido alarme, ocorreu há mais de um número de minutos especificável, independentemente do motivo do atraso, de maneira a evitar erros de operação. • Possuir módulo que permita a supervisão dos alarmes finalizados pelos operadores, devendo: • Permitir o acesso somente aos usuários com direitos para supervisão e checagem dos procedimentos adotados. • Possibilitar que somente os alarmes já assinados anteriormente e ainda não supervisionados, sejam apresentados de forma organizada por data/hora, sendo também exigida a navegação por estes registros com simultânea exibição dos dados dos registros dos fatos cujas ENTIDADES acionaram os alarmes, das imagens, dos dados relativos às passagens veiculares e dos procedimentos exigidos. • Exibir relação das perguntas impostas aos operadores que visualizaram os alarmes na primeira exibição e as suas respostas.

		• Exibir a mesma relação das perguntas impostas aos operadores que visualizaram os alarmes na primeira exibição permitindo respostas distintas às mesmas perguntas. • As perguntas deverão possibilitar respostas do tipo Sim ou Não ou por texto redigido quando necessário, sendo que as respostas do tipo Sim ou Não, deverão constar em relatórios estatísticos posteriores. • Permitir a finalização do alarme pelo supervisor. (Este deverá ser excluído da lista, permanecendo, entretanto, todos os alarmes já assinados anteriormente e ainda não supervisionados.) • Permitir a filtragem de alarmes ocorridos em um determinado período de data/hora, relativo às passagens veiculares que geraram os alarmes ou aos momentos exatos que os alarmes foram gerados. • Permitir a filtragem de alarmes ocorridos em um determinado período de data/hora, relativos à determinada placa veicular. • Permitir obtenção dos resultados da combinação dos 2 filtros anteriores. • Exibir algum tipo de notificação visual, quando existirem alarmes ainda não assinados pelo operador, com possibilidade de abertura do módulo relativo à esta etapa. • Permitir a partir da tela, a exibição de representação gráfica de uma linha do tempo que mostre os intervalos de tempo que o sistema levou para receber as imagens desde o ponto de coleta até a CAM, o tempo necessário para seu processamento e o tempo para disparo de evento de alarme. • Deverá ser parte integrante da solução, a disponibilização para o uso de aplicativo mobile integrado ao módulo de alarmes do SISTEMA DE GESTÃO E ANÁLISES, durante todo o período contratual, devendo no mínimo: • Receber os alarmes gerados na CAM, para os quais o número de telefone foi previamente cadastrado para este propósito, devendo no mínimo: • Gerar alerta sonoro. • Gerar notificação no formato padrão do sistema operacional do telefone em questão. • Permitir a partir da notificação, a abertura de tela que exiba o alarme gerado (com imagem), incluindo no mínimo, a placa do veículo, identificação do local, motivo e descrição do alarme. • Permitir a partir da notificação, a abertura de tela que exiba informações de data/hora e local, para no mínimo, 10 últimas passagens registradas do veículo em questão. • Permitir a exibição em lista, dos últimos alarmes recebidos (parametrizável em dias). • A solução proposta deverá suportar um módulo de pesquisas devendo: • Permitir a pesquisa no banco de dados por sequência de caracteres exatos, por sequência de caracteres contidos e por caracteres coringas. • Permitir, quando a pesquisa no banco de dados for filtrada por intervalo de data/hora, que apresente todas as imagens referentes às passagens veiculares, mesmo que por qualquer motivo não tenha sido possível extração de informações pelos sistemas automáticos. • Permitir pesquisa que exiba apenas as passagens veiculares verificadas pelos seguintes critérios, de forma única e também combinados entre si: • Por intervalo compreendido entre duas datas e horas distintas. • Por intervalo compreendido entre um único dia, entre duas horas distintas. • Em uma única câmera. • Em múltiplas câmeras selecionadas. • Por classificação de tipos de veículos, possibilitando múltipla seleção. • Por total de passagens veiculares pelos PCLs. • Por veículos inseridos como Entidades em um ou mais registro de fatos de determinadas naturezas delituosas, a critério do operador e possibilitando aplicar-se no resultado, os filtros adicionais: • Somente detecção de veículos marcados em ocorrência. • Somente de veículos cadastrados em um ou mais registro de fatos de determinadas naturezas delituosas, a critério do operador. • Permitir nos resultados de pesquisa que sejam exibidas somente a última passagem veicular de cada placa lida. • Permitir, utilizando a base única de cadastro de dados sobre veículos, pesquisas combinadas entre: Marca, modelo, cor, ano de fabricação, ano do modelo, Tipo do veículo, município e estado. • Permitir que os resultados das pesquisas sejam exibidos através de interface gráfica interativa, em múltiplos quadrantes (formato popularmente conhecido como mosaico), nos quais constem as imagens e as respectivas informações associadas a cada passagem veicular, de maneira a poder-se visualizar simultaneamente o mínimo de 8 quadrantes. • O mosaico deverá ajustar o formato de visualização da tela automaticamente, dependendo do número de quadrantes em tela e resolução do monitor igual ou acima de 768 linhas. • Possuir várias opções de mosaicos para visualizações dos resultados de pesquisas, que permitam aumentar o número de quadrantes por página. • Permitir a seleção do enquadramento desejado das imagens nos quadrantes do mosaico, que retornarão das pesquisas, no mínimo, com os seguintes enquadramentos dentro da área de visualização: • Imagem original (obtida pela câmera), contendo o veículo. • Somente do veículo cuja placa foi lida. • Somente da placa veicular lida. • Ao alternar entre os enquadramentos acima, as exibições de todas as imagens apresentadas como resultado da pesquisa, deverão passar a respeitar o enquadramento definido sem nova intervenção humana. • Permitir a exibição ou ocultação das passagens veiculares sem imagens anexadas, que possuam somente a leitura da placa. • Nos resultados das pesquisas deve ser exibido identificador visual que aponte quais imagens foram coletadas durante o horário de verão (Caso exista). • Nos resultados das pesquisas devem ser exibidos identificadores visuais que apontem quais imagens não possuem certificação de sincronização de horário da captura com o Servidor NTP da CAM. • Possuir representação gráfica de uma linha do tempo que mostre o tempo decorrido desde a captura da imagem até o armazenamento, destacando no mínimo, a data e hora de captura da imagem, data e hora de processamento e data e hora do recebimento da imagem pelo servidor.

		• Permitir zoom digital progressivo, aplicação de brilho e contraste nas imagens vinculadas aos resultados das pesquisas efetuadas utilizando-se somente do mouse e aplicando as alterações instantaneamente. • Permitir exportação de imagens relativas às passagens veiculares, passível de visualização por qualquer visualizador de imagens de mercado, suportando inserção de marca d'água e obrigatoriamente de identificadores digitais em todas as imagens, com posterior comprovação da autenticidade e integridade do arquivo exportado (não adulteração) através de ferramenta disponibilizada pela própria solução ofertada. • Permitir que, para cada veículo retornado como resultado de uma pesquisa exibida em um monitor, possa ser exibido em um segundo monitor, o perfil comportamental do veículo em questão. • Permitir a associação manual de uma determinada passagem veicular a um determinado fato registrado, inserindo a placa do veículo como uma entidade. • Permitir que a partir do mosaico de exibição dos resultados de pesquisas, possa-se proceder a correção das placas lidas pelo sistema e que tais correções possam ser auditadas, devendo no mínimo: • Suportar a inserção e correção da leitura da placa, relativa a uma passagem veicular registrada pelo sistema. • Suportar a inserção e correção das leituras das placas relativas a um lote de passagens veiculares registradas pelo sistema, para no mínimo, lote com 50 registros, apresentando ao final todas as alterações efetuadas pelo usuário e solicitando obrigatoriamente a confirmação do usuário antes de gravar definitivamente os dados inseridos e alterados. • Permitir que nos resultados das pesquisas, possa-se selecionar uma das imagens e iniciar navegação sequencial, manual ou automática, precedentes ou subsequentes, exibindo as imagens relativas à cada passagem veicular. • Permitir ao operador, quando a navegação for automática, na mesma faixa de rolagem, optar por pausar quando algum veículo exibido na navegação, estiver associado a algum REGISTRO DE FATO. • Permitir ao operador, quando a navegação for automática, por todas as imagens resultantes da pesquisa, optar por pausar quando algum veículo exibido na navegação, estiver associado a algum REGISTRO DE FATO. • Permitir que os resultados das pesquisas possam ser exportados em formato de relatório constando a descrição do motivo da exportação devendo ser do tipo texto livre, a ser preenchido pelo operador, placa do veículo, data e hora, local e sentido e imagens relativas. • Permitir, que o resultado da pesquisa possa ser georreferenciado em mapa, mostrando no mínimo as últimas 25 passagens veiculares detectadas. • Possuir interface gráfica para a administração, com acesso protegido por usuário e senha, da base única de cadastro de usuários e senhas do sistema, contendo no mínimo as seguintes funcionalidades: • Gerenciamento dos dados cadastrais dos PCLs, sendo minimamente exigidos: Nome do local, direção, faixas de rolagem, Grupo ao qual o PCL pertence e suas coordenadas geográficas. • Possuir interface gráfica com informativo sobre a capacidade de armazenamento e percentual de uso de cada volume de armazenamento das imagens, quantidade de passagens veiculares (registros) e quantidade de dias armazenados de todos os equipamentos utilizados para armazenamento dos dados na CAM e necessários para o funcionamento da solução proposta. • Possuir interface gráfica interativa, capaz de exibir os indicadores (em percentuais) das leituras de placas das imagens recebidas de cada câmera, devendo no mínimo: • Permitir filtragem por data Inicial e Final com período de horário e seleção de câmeras. • Exibir lista de todas as câmeras cadastradas, indicando para o(s) dia(s) filtrado(s), os respectivos percentuais. • Permitir o gerenciamento de usuários, grupos de usuários e políticas de permissão de acesso aos módulos do sistema e suas funcionalidades, definindo quais operadores terão acesso a quais recursos do sistema. • Suportar a aplicação de regras que controlem quais alarmes deverão ser notificados nos celulares cadastrados, sendo no mínimo pela seleção das naturezas de delitos cometidos que deverão ter seus monitoramentos notificados nos celulares. • A solução proposta deve disponibilizar uma tela (painel de informações), atualizada em tempo real, permitindo alternar a exibição no mínimo para as últimas 24 e 48 horas. • Para todas as informações e totalizações solicitadas a seguir, a solução deverá prever uma forma de diretamente do painel de informações, abrir o(s) módulo(s) específico(s) e exibir automaticamente as informações relativas às totalizações: • Quantidade de FATOS REGISTRADOS no período selecionado. • Quantidade de FATOS REGISTRADOS QUE FORAM ALTERADOS OU COMPLEMENTADOS no período selecionado. • Quantidade de FATOS REGISTRADOS QUE FORAM ENCERRADOS por usuário autorizado. • Quantidade de veículos removidos dos FATOS REGISTRADOS. • Quantidade de veículos, cujas placas foram alteradas nos FATOS REGISTRADOS • Quantidade de FATOS REGISTRADOS que necessitam de complemento de informações. • Quantidade de FATOS REGISTRADOS que receberam anotações. • Quantidade de FATOS REGISTRADOS que ainda não tem Boletim de ocorrência cadastrado. • Número de alarmes DE MONITORAMENTOS SIMPLES, ocorridos no período selecionado. • Número de alarmes DE MONITORAMENTOS SUPERVISIONADOS, ocorridos no período selecionado. • Número de alarmes DE MONITORAMENTOS SUPERVISIONADOS, que ainda não foram assinados pelo operador responsável. • Número de alarmes DE MONITORAMENTOS SUPERVISIONADOS, ainda não supervisionados e pendentes de concordância do supervisor. • O Painel de informações deverá fornecer uma área de notificações importantes, para exibição de todas as mensagens do sistema, obtidas de forma automática sendo no mínimo exigida notificação sobre PCLs com problemas, diretamente ao operador. • A solução proposta deve fornecer recurso para pesquisas rápidas sobre placas veiculares e indivíduos (pessoas) e cadastramentos mínimos necessários às ações rápidas permitindo a pesquisa sobre determinada placa veicular e retornando no mínimo: • Quantidade de registro de fatos que contém a placa, possibilitando a abertura do cadastro dos fatos, exibindo somente os registros referentes à placa. • Permitir que a partir da mesma tela, que a placa pesquisada seja cadastrada no registro de fatos, para ser monitorada, com a obrigação da inclusão da natureza do fato delituoso. • Se algum veículo com a placa em questão, possui ou não passagens registradas pelas câmeras monitoradas, possibilitando a exibição das imagens das referidas passagens veiculares.

		• Quantidade de alarmes de monitoramento SUPERVISIONADO, referente à placa em questão nas últimas 24 horas, possibilitando a exibição destes alarmes. • Permitir a pesquisa sobre determinado CPF ou NOME, retornando no mínimo a quantidade de registro de fatos que contém o CPF ou NOME, possibilitando a abertura do cadastro dos fatos com exibição somente dos registros relacionados. • Quantidade de alarmes relativos a monitoramento SIMPLES da referida placa, nas últimas 24h, possibilitando a exibição destes alarmes. • Dispor de módulos de análises de correlacionamentos: • Que identifique, veículos com registros de movimentações correlacionadas entre si, exibindo os resultados desta análise em interface gráfica interativa, distinguindo visualmente os diferentes níveis de correlação, devendo utilizar uma ou mais placas veiculares. • Que identifique, veículos com registros de movimentações correlacionadas, exibindo os resultados desta análise em interface gráfica interativa, distinguindo visualmente os diferentes níveis de correlação, devendo utilizar de forma combinada, no mínimo: • Registros de roubo, furtos ou roubos e furtos. • Uma ou mais classificações atribuídas aos veículos inseridos nos Boletins de Ocorrências ou outros delitos cadastrados nos registros de fatos, tais como: produto, recuperado, suspeito etc. • Intervalo de tempo retroativo em dias, que será considerado para a análise, devendo ser no mínimo para os últimos 7dias, 30 dias ou todo o tempo de cadastro admitido pelo sistema. • Para todos os resultados das análises de correlacionamentos, a interface gráfica interativa deverá disponibilizar a aplicação dos seguintes filtros, com alteração imediata dos níveis de correlação visualmente apresentados: • Por um ou mais tipos veiculares classificados. • Por passagens veiculares sem leitura de placa. • Por passagens veiculares registradas, ocorridas no intervalo de datas solicitado, para as quais o sistema não apontou qualquer correlação comportamental. • Por número máximo de passagens veiculares (especificável) registradas independente do dia. • Por total de passagens veiculares registradas. • Por período predominante de circulação, no mínimo para intervalos de 12h em 12h. • Por quantidade (especificável) de correlações identificadas na análise. • Para todos os resultados das análises de correlacionamentos, a interface gráfica interativa deverá exibir opcionalmente, a critério do operador, de forma visual destacada e única: • Veículos com passagens registradas a partir de determinada data (especificável), inseridos como Entidade no registro de fatos. • Veículos com passagens registradas a partir de determinada data (especificável), inseridos como Entidade monitorada no registro de fatos. • Veículos com passagens registradas a partir de determinada data (especificável) que geraram alarmes para monitoramento SIMPLES. • Veículos com passagens registradas a partir de determinada data (especificável), que geraram alarmes para monitoramentos SUPERVISIONADOS. • Para todos os resultados das análises de correlacionamentos, a interface gráfica interativa deverá exibir, indicação visual dos veículos cujas imagens não permitiram a leitura automática da placa veicular ou tiveram leitura equivocada, possibilitando a correção dos caracteres de suas placas, devendo após as correções, atualizar automaticamente o resultado da análise em questão. • Dispor de análises de correlacionamentos associativos e temporais que aponte, a partir dos dados obtidos por análises comportamentais de circulação, tempos de permanência dos veículos e dos dados existentes nos registros de fatos da solução proposta, veículos com movimentações que gerem indicativos de suspeição, devendo utilizar de forma combinada: • Uma ou mais naturezas dos Boletins de Ocorrências ou outros delitos cadastrados nos registros de fatos. • Intervalo de tempo retroativo em dias, que será considerado para a análise, devendo ser no mínimo, para os últimos 7dias, 30 dias ou todo o tempo de cadastro admitido pelo sistema. • O resultado deverá: • Ser ordenado por grau de suspeição de modo a facilitar o entendimento do motivo pelo qual cada veículo foi inserido no resultado. • Destacar visualmente os veículos constantes do resultado que estejam relacionados com algum registro de fato. • Para resultados derivados de análises obtidas sem indicação de placas veicular e ou entidades, apresentar explanação elucidativa em interface gráfica interativa, de modo que o operador do sistema tenha condições de entender o motivo pelo qual aquele veículo foi inserido no resultado. • Suportar filtro que possibilite a análise de correlacionamentos em delitos ocorridos em áreas geográficas específicas, sendo exigido no mínimo a seleção dos PCLs. • Dispor análise correlacional expansível, que aponte veículos com movimentações coincidentes com outros veículos exibindo o resultado em um gráfico interativo na forma de “rede complexa”, (Um grafo, que se representa por um conjunto de nós ligados por arestas formando uma rede que permite representar relações) que destaque visualmente o grau de coincidência da movimentação de todos os veículos do resultado, devendo utilizar de forma combinada: • Placa do veículo alvo da análise. • Número mínimo de correlações • Período em data/hora. • A tela resultante da análise deverá ser em interface gráfica interativa e permitindo no mínimo: • Expandir qualquer nó da “rede complexa” para visualizar outros veículos correlacionados ao nó expandido. • Exibir a placa, as imagens e o número de veículos correlacionados • Mover qualquer nó da “rede complexa” para facilitar a visualização quando a quantidade de itens correlacionados ocasionar sobreposição de imagens na tela. • Permitir interação com os módulos de pesquisa, perfil comportamental e exportação de imagens do sistema sem que o operador seja obrigado a fazer pesquisas complementares.

		• Que apareçam visualmente destacados na rede complexa, os nós relacionados aos “REGISTROS DOS FATOS”. • Exibir para qualquer nó, a apresentação do perfil comportamental de forma gráfica, exibindo os dados estatísticos da movimentação e apresentando no mínimo: • Número de passagens do veículo por período de tempo; • Número de passagens do veículo por PCL. • Rotas da movimentação do veículo entre PCLs, incluindo o sentido de movimentação. • Gráficos de calor que indiquem a probabilidade preventiva de presença de determinado veículo, considerando no mínimo o dia da semana e o horário. • Fornecer módulo de análise computacional, que identifique de forma automática (sem intervenção humana) possíveis veículos clonados, gerando notificações. • Dispor de análise computacional que identifique de forma automática (sem intervenção humana) passagens veiculares, com possíveis associações a um ou mais veículos, inseridos como ENTIDADES no registro de fatos permitindo a inclusão desta informação, juntamente com imagem comprobatória no referido registro de fato. • A solução proposta deverá disponibilizar módulo que permita a visualização georreferenciada dos elementos do REGISTRO DE FATOS, sendo exigido no mínimo: • A solução proposta deverá disponibilizar módulo que permita a visualização georreferenciada dos elementos do REGISTRO DE FATOS, sendo exigido no mínimo: • Capacidade de filtrar os fatos ou ocorrências por data; • Possibilidade de visualização através de múltiplas camadas; • Capacidade de selecionar os fatos por tipo; • Visualização georreferenciada dos pontos de captura de imagens; • Inclusão de novas camadas a critério do operador, tais como escolas, bancos, câmeras de CFTV, zonas, setores etc., através de interface gráfica simples e intuitiva, permitindo; • Inclusão e exclusão de novos itens dentro de cada camada a critério do operador; • Criação e edição de camadas com pontos ou camadas com áreas. • Criação e edição de camadas com pontos ou camadas com áreas. • Possibilidade de corrigir a coordenada geográfica de qualquer fato, diretamente no mapa, usando recurso de arrastar e soltar. • Possibilidade de visualização georreferenciada de mais de uma camada simultaneamente exibindo ícones distintos para cada camada; • Geração de mapa de calor, definindo áreas através de aplicação de gradiente de cores e suas temperaturas, em função da distribuição e concentração dos fatos georreferenciados; • Capacidade de, a critério do usuário, modificar a densidade do mapa de calor desejado, gerando macro ou microáreas, tendo em cada uma das microáreas definidas as concentrações de delitos cadastrados; • Possibilidade de cadastrar e visualizar áreas georreferenciadas, para demarcar regiões de interesse no mapa tais como zonas de cidades e áreas de monitoramento; • Possibilidade de visualizar as ocorrências de maneira agrupada contendo o total de registros por agrupamento; • A solução proposta deverá disponibilizar módulo que permita comparar visualmente os elementos georreferenciados do REGISTRO DE FATOS, sendo exigido no mínimo: • Possibilitar a comparação, o acompanhamento do deslocamento dos fatos e a distribuição das ocorrências em função do tempo, agrupadas por mês, com no mínimo as seguintes formas de visualização: impressa e animada. • Capacidade de filtrar os fatos ou ocorrências por intervalo de data; • Capacidade de selecionar os fatos por tipo; • Quando selecionado uma camada com determinadas áreas e outra camada com determinados pontos, o sistema deverá ser capaz de contabilizar em tempo real e de maneira automática, a quantidade de pontos contidos dentro de cada área, exibindo o resultado em forma de legenda no próprio mapa em análise. • Capacidade de exibir em mapa as ocorrências de roubo de veículos, furto de veículos e recuperação de veículos, de maneira a possibilitar a visualização e análise de onde os veículos estão sendo roubados e furtados e onde estão sendo recuperados. • Este mapa deve ser interativo e fazer uso de ferramentas gráficas com indicação animada entre os locais onde cada veículo foi furtado ou roubado e recuperado, permitindo a exibição das informações sobre o fato registrado. • A PROPONENTE deverá disponibilizar, durante todo o período contratual, todos os serviços continuados para funcionamento, manutenção e compatibilização de todos os itens do SISTEMA DE GESTÃO E ANÁLISES, que utilizam mapas, mantendo compatibilização técnica com a solução de mapas utilizada. • A solução proposta deverá suportar um módulo de informação geográfica para receber e exibir dados georreferenciados demonstrados em um sistema de mapa e deverá: • Disponibilizar mapa com no mínimo 2 tipos de representações: • Mapa padrão (Exemplo: mapa default do google ou bing) • Mapa com imagens de satélite. • Possuir opção de ativar ou desativar no mapa, as representações gráficas de malha viária e rodoviária. • Suportar a exibição dos dados georreferenciados e em tempo real para, no mínimo, os grupos: • ATENDIMENTOS • PONTOS DE COLETA DE IMAGENS • GUARNIÇÕES • CÂMERAS DE VÍDEO • ALARME PATRIMONIAL • Para todos os grupos anteriores, deverá: • Suportar a possibilidade de exibição ou ocultação dos ícones de cada grupo. • Suportar que um ou mais grupos sejam configurados para visualização dinâmica evitando poluição demasiada no mapa (por excesso de ícones), mostrando mais ícones ao aplicar zoom e menos ícones quando diminuir o zoom. • Permitir que os ícones do grupo Guarnições, sejam exibidos, de forma visualmente diferenciada entre si, no mínimo, para os seguintes status:

		• Guarnição empenhada (despachada) • Guarnição apoiando outra guarnição. • Guarnição em atividade • Guarnição com o botão de pânico ativado. • Sem conexão de internet. • Permitir que ao selecionar um ícone do grupo Guarnições, seja exibido, no mínimo, as seguintes informações: • Ação em andamento (patrulhamento, empenhada, em apoio etc.) • Percentual de carga da bateria do dispositivo móvel. • Responsável pela guarnição. • Número da linha telefônica do dispositivo móvel. • Prefixo da guarnição. • Tempo desde a última atualização. • Permitir que os ícones do grupo Pontos de Coleta de imagens, sejam exibidos, de forma visualmente diferenciada entre si, no mínimo, para os seguintes status: • OnLine • OffLine • OffLine com alerta de problema • Indicador de alarme (quando alguma câmera do ponto de coleta detectou veículo com restrição e gerou alarme) • Permitir que ao selecionar um ícone do grupo Pontos de Coleta de imagens, seja exibido, no mínimo, as seguintes informações: • Identificação do local e sentido. • Lista das câmeras do ponto de coleta. • Status de funcionamento para cada uma das câmeras. • Indicador de alarme na câmera. (quando a câmera do ponto de coleta detectou veículo com restrição e gerou alarme) • Permitir que os ícones do grupo Atendimento, sejam exibidos, de forma visualmente diferenciada entre si, no mínimo, para os seguintes status: • Em aberto. • Em atraso. • Agendado. • Em atendimento. • Guarnição com o botão de pânico ativado. • Permitir que ao selecionar um ícone do grupo Atendimento, sejam exibidas, no mínimo, as seguintes informações: • Natureza do atendimento. • Guarnição despachada para atendimento. • Tempo desde a abertura do atendimento. • Prioridade do atendimento. • Permitir que ao selecionar um ícone do grupo CFTV, seja possível, no mínimo: • Exibir a identificação do local. • Exibir o vídeo ao vivo. • Permitir que ao selecionar um ícone do grupo Alarme Patrimonial, seja exibido, no mínimo, as seguintes informações: • Identificador do local. • Setor ou local onde ocorreu o disparo de alarme. • Deverá ser parte integrante da solução, a disponibilização para o uso de aplicativo mobile integrado, durante todo o período contratual, devendo no mínimo: • Permitir ao usuário tirar uma foto de veículo com o imediato e automático envio para a CAM, incluindo, no mínimo, data/hora, coordenadas geográficas e identificação do dispositivo mobile. • Garantir que as fotos enviadas sejam somente aquelas obtidas usando o referido aplicativo. • Permitir ao usuário, a execução de blitz, apontando a câmera do celular para uma via, obtendo automaticamente uma imagem de cada veículo que passar pelo local, enviando-as automaticamente para a CAM, incluindo, no mínimo, data/hora, coordenadas geográficas e identificação do dispositivo mobile. • Detectar a presença e capturar a imagem de todos os veículos que trafeguem pelos locais previamente definidos. (Veículos com e sem placa, com placa legível ou não e com a placa oculta). • Capturar imagens, nas quais apareça a respectiva placa veicular e que permitam a identificação de características peculiares a cada automotor, tais como modelo e sinais distintivos diversos. • Para todos os casos em que no momento da captura da imagem não existir disponibilidade de conexão para envio imediato, esta deverá ser enviada a partir do momento que a conexão for restabelecida, mantendo as informações referentes ao horário da captura e não ao horário do envio. • Deverá ser fornecido com todas as licenças legalizadas de todos os softwares necessários para seu funcionamento. • Deverá ser parte integrante da solução, a disponibilização para o uso de aplicativo mobile integrado, durante todo o período contratual, devendo no mínimo: • Registrar as abordagens de indivíduos e veículos realizadas por um usuário em campo, no sistema de cercamento eletrônico. • Caso existam informações sobre o CPF da pessoa abordada ou sobre a Placa do veículo abordado, no banco de dados do cercamento eletrônico ou em bases de dados que o município possua convênios, o resultado desta consulta deverá retornar para o aplicativo em uso. • Permitir visualizar os locais e as informações das abordagens realizadas anteriormente, referentes ao mesmo indivíduo ou veículo abordado. • A Proponente deverá disponibilizar e garantir o funcionamento de um módulo de software que possibilite o recebimento e gerenciamento de solicitações de detentores de medidas protetivas e/ou medidas protetivas patrimoniais, devendo no mínimo: • Disponibilizar aplicativo de solicitações de ajuda (para celulares)

		• Possibilitar o cadastramento do usuário a partir do próprio aplicativo, contendo todas as informações necessárias à identificação do beneficiário de tais medidas, incluindo fotografia do protegido e do possível agressor. • Disponibilizar no aplicativo, um botão do tipo SOS que será acionado quando o cidadão se encontrar em situação de risco. • Permitir, por parte dos gestores do sistema, a aprovação ou reprovação deste cadastro. • Permitir que o usuário receba informações pelo próprio aplicativo celular, indicando o status de seu cadastro. • Emitir alarme ou suportar algum tipo de notificação, quando for acionado o botão SOS do aplicativo. • Disponibilizar nesta notificação as seguintes informações: • - Nome • - Cadastro • - Data/hora acionamento • - Tipo de proteção • - Localização em tempo real • - Rastreamento da localização geográfica do aplicativo • - Foto da pessoa protegida • - Foto da possível agressor. • Além do alarme ou notificação no sistema da Central de Monitoramento, deverá ser aberto automaticamente um atendimento no sistema de Gestão de operação. • Dentre os relatórios operacionais disponibilizados pela solução proposta, o mínimo exigido será: • Consulta de placas veiculares com leituras incorretas e que foram corrigidas pelos operadores, exibindo identificação do operador, placa anterior, nova placa, data e hora da correção. • Relatório de imagens relativas às passagens veiculares que foram exportadas do sistema, exibindo a identificação do operador que realizou a operação, data e hora da operação, placa do veículo relativo à passagem, data e hora da passagem e identificação do ponto de captura relativo à passagem. • Relatório de sessões de utilização do sistema, exibindo identificação do operador e data e hora das operações de abertura, autenticação e encerramento do sistema. • Relatório de pesquisas de veículos efetuadas no sistema, exibindo a identificação do operador, data e hora da pesquisa e a placa, ou parte dela, pesquisada. • Relatório de ações tomadas pelos operadores em função dos alarmes disparados pelo sistema, exibindo fotografia da passagem que gerou o alarme, dados do alarme, dados do FATO REGISTRADO relativo ao veículo monitorado e as ações tomadas pelo operador. • Relatório que permita auditoria, para verificar quais ações foram executadas pelos operadores, permitindo que o supervisor faça auditorias em suas próprias equipes de trabalho. • Relatório que permita aos operadores a checagem das informações cadastradas no REGISTRO DE FATOS, apontando a ausência de dados básicos, como por exemplo, falta de endereço ou descrição do fato ou outra exigida pela solução proposta. • Dentre os relatórios estatísticos disponibilizados pela solução proposta, o mínimo exigido será: • Relatório de dados estatísticos por tipo de FATO REGISTRADO, exibindo para um tipo de FATO REGISTRADO e um intervalo de data e hora, o mapa com itens georreferenciados em função dos endereços dos FATOS, histograma do número de ocorrências por semana, histograma do número de ocorrências por dia da semana e histograma de ocorrência por intervalos de hora de ocorrências. • Relatório de dados estatísticos para os tipos de FATOS REGISTRADOS, exibindo para os principais tipos de FATOS REGISTRADOS e um intervalo de data e hora, a distribuição do número de ocorrências por tipo de fato e os histogramas do número de ocorrências semanais para cada tipo de FATO, permitindo num único relatório acompanhar a distribuição e a evolução dos índices semanais por tipo de FATO REGISTRADO. • Relatório de veículos monitorados, exibindo o histograma de distribuição dos tipos de FATOS REGISTRADOS em função do número de monitoramentos e o histograma de modelos de veículos monitorados em função do número de monitoramentos, evidenciando quais os tipos de FATOS REGISTRADOS e modelos de veículos de maior interesse. • Relatório de dados estatísticos para os alarmes gerados, exibindo os alarmes em um intervalo de data e período do dia, os gráficos da distribuição de alarmes para o dia da semana, dia do mês, horário do alarme e PCLs. • Relatório de dados estatísticos para os FATOS REGISTRADOS, com possibilidade de filtro por tipos de FATO REGISTRADO, intervalo de data e hora, exibindo como resultado a distribuição dos tipos de FATOS REGISTRADOS em função dos períodos do dia (madrugada, manhã, tarde e noite) em gráficos, tabela e apontando os FATOS REGISTRADOS no mapa. • Relatório de dados estatísticos para a distribuição dos tipos de FATOS REGISTRADOS, com possibilidade de filtro de intervalo de data e hora, exibindo como resultado os totais de FATOS REGISTRADOS e os totais de tipos de FATOS REGISTRADOS. • Dentre os relatórios de tráfego veicular disponibilizados pela solução proposta, o mínimo exigido será: • Relatório do fluxo de passagens veiculares por local de coleta, exibindo o fluxo veicular em um intervalo de data e um determinado PCL, os gráficos da distribuição por classificação de veículo e do fluxo das passagens por hora do dia e por sentido no PCL selecionado. • Relatório de fluxo de passagens veiculares por rota, exibindo o fluxo veicular em um intervalo de data e entre dois PCLs, o gráfico com o intervalo de tempo médio para trânsito entre os locais selecionados. • PROPONENTE deverá, durante todo o período contratual, prestar todos os serviços e suportes técnicos que garantam a continuidade da compatibilidade e funcionamento dos aplicativos com os telefones celulares cadastrados, devendo: • Garantir a compatibilidade para atualizações e novas versões de sistemas operacionais. • Manter o funcionamento da validação dos telefones cadastrados, de forma a garantir a segurança das informações enviadas e recebidas. • Disponibilizar processo de revalidação em casos de troca de telefone físico, mesmo que o novo aparelho utilize o mesmo do número de telefone anterior. • Os serviços deverão garantir que somente aparelhos celulares, previamente cadastrados e autorizados sejam utilizados. • Gestão de Operação

		• A solução proposta deverá disponibilizar módulo de Gestão de Operação, que permitirá que a central de atendimento possa controlar um ou mais atendimentos simultâneos, cadastrar locais, fatos e naturezas, despachar viaturas acompanhando em tempo real todos as etapas dos atendimentos. • Este módulo deverá minimamente: • Permitir a utilização da mesma base de endereços do registro dos fatos da solução ofertada. • Permitir a autenticação dos usuários, utilizando a mesma base de usuários da solução ofertada. • Permitir o cadastramento de locais físicos referenciais, tais como praças, ginásios, bares, restaurantes, clubes, etc...., de forma que possam ser utilizados como referência durante a Gestão de operação, para identificação do local do fato que gerou o atendimento, quando o solicitante, não souber o endereço exato. • Permitir o cadastro dos meios de deslocamento (meios de transporte das guarnições) que serão utilizados na montagem do mapa força e no despacho. • Permitir a criação das guarnições, com informações sobre seus integrantes, qual o integrante responsável e quais (um ou mais) meios de deslocamento. • Atribuir um ou tipos de deslocamento a cada guarnição. • Disponibilizar interface gráfica onde seja possível visualizar em uma só tela, os atendimentos abertos, em atraso, em andamento e as prioridades de cada um dos atendimentos (conforme definidas pelo usuário), guarnições disponíveis para despacho e guarnições já empenhadas. • Exibir indicador para guarnições autodespachadas. • Obrigar o cadastramento do motivo do atendimento. • Caso o motivo seja o mesmo de algum atendimento anteriormente cadastrado, que seja possível que sejam vinculados, o atendimento em tela e quantos mais houver para o mesmo fato, de forma a designar um único despacho para vários atendimentos. • Gerar automaticamente, após o cadastramento do atendimento, um número de protocolo único. • Deve ser capaz de identificar, a partir do preenchimento dos campos exigidos para cadastro do atendimento, que o solicitante em questão, já tenha feito a mesma solicitação anteriormente ou ainda, para qualquer outra solicitação diferente, sem limite de tempo. • Caso identificado que o solicitante já tenha atendimentos registrados anteriormente, exibir na tela todos os atendimentos cadastrados permitindo ao atendente, identificar quando, onde e quais foram os protocolos dos atendimentos. • Permitir que seja informado que o atendimento foi solicitado de forma “anônima”. • Permitir o gerenciamento das guarnições, controlando no mínimo: • Quilometragem percorrida. • Horários de trabalho. • Setores patrulhados. • Composição por indivíduos. • Meios de transportes utilizados. • Permitir o acompanhamento em tempo real no mínimo dos seguintes dados de cada atendimento: • Tempo decorrido desde o início do atendimento. • Prioridade do atendimento, diferenciado por cor. • Suportar criação ilimitada dos níveis de prioridades, permitindo definir para cada nível de prioridade seu respectivo nome, cor, tempo máximo para atendimento. • Suportar a configuração do tempo máximo de atendimento aberto para o qual ainda não foi despachada nenhuma guarnição. Quando excedido este tempo máximo, um alerta de qualquer tipo (sonoro, visual etc.) deverá chamar a atenção dos operadores para este fato. • Permitir, após um cadastramento de um atendimento solicitado, visualizar-se na mesma tela, os atendimentos e as guarnições, de forma a observar-se quais as guarnições estão livres para que sejam designadas à cada atendimento. • Exibir as guarnições e seus respectivos status, identificando quais estão disponíveis e quais estão em atendimento, utilizando diferentes cores para cada status. • Permitir o vínculo de um atendimento com uma guarnição disponível, gerando um despacho numerado sequencialmente. • O numerador sequencial deverá ser reiniciado às 0h (zero hora) do dia 1º de janeiro de cada ano. • Permitir controlar a quilometragem percorrida por cada guarnição utilizada nos despachos, desde o início até o seu encerramento. • Permitir a qualquer tempo, anexar ao despacho, um ou mais documentos digitalizados que deverão permanecer anexos aos mesmos, como por exemplo: fotografias colhidas durante o procedimento do agente. • Possibilitar que sejam controlados os deslocamentos de cada guarnição por ocasião dos despachos, sendo minimamente exigidos os itens: • Local destino, data e hora de partida, quilometragens inicial e final e data e hora de chegada ao local do atendimento. • Permitir a inserção de múltiplos deslocamentos por despacho. • Permitir que durante o ciclo de vida do despacho, seja possível acrescentar mais de uma guarnição ao despacho, sendo a primeira considerada e identificada como “Responsável” ou “Principal” e as demais consideradas e identificadas como “Apoios”. • Permitir durante o ciclo de vida do despacho, que seja possível que uma guarnição considerada como “Apoio” seja designada como a nova “Responsável” ou “Principal” para continuidade do despacho, liberando a anterior para outros despachos. • Possibilitar ao finalizar o despacho, o cadastramento de qualquer narrativa (informações complementares sobre o despacho) efetuada pelo responsável pelas guarnições empenhadas. • Permitir o cadastro de boletins de ocorrência, contendo dados do local (Rua, bairro etc.), indivíduos ou veículos envolvidos, apreensões realizadas e documentos diversos através da anexação de arquivos digitais (fotos, pdf etc). • Permitir que usuários previamente definidos para tal função, aceitem os dados do boletim de ocorrência da forma como foram gerados ou devolva ao responsável para correções e/ou complementos.

		• Permitir rotina de encerramento dos despachos, suportando a inserção de dados referentes aos mesmos e liberando sequencialmente cada uma das guarnições empenhadas, em seguida, permitir rotina de encerramento do atendimento em questão, suportando a inserção de dados referentes ao mesmo. • Permitir o encerramento de um atendimento somente após os encerramentos de todos os despachos relativos ao atendimento em questão. • Armazenar todos os dados referentes aos atendimentos e despachos, pelo período mínimo de 1 (Um) ano, a fim de permitir futuras auditorias e geração de relatórios. • Deverá ser parte integrante dos serviços, a disponibilização para o uso de aplicativo mobile integrado ao módulo de Gestão de operação do SISTEMA DE GESTÃO E ANÁLISES, durante todo o período contratual, para: • Receber notificação sonora quando a guarnição e sua respectiva composição forem criadas a partir da CAM. • Registrar guarnições e suas respectivas composições com imediato envio à CAM como guarnição disponível. • Permitir a vistoria e registros da situação física da guarnição. • Permitir realizar uma abordagem e em seguida o preenchimento de um BOGMC. • Cadastrar boletins de ocorrência, contendo no mínimo os dados do local (Rua bairro etc.), de indivíduos (nome, RG etc.), de veículos envolvidos (modelo, placa etc.) e de apreensões realizadas (tipo, descrição, quantidade etc.). • Possibilitar a anexação de arquivos digitais (pdfs, fotos etc.) e permitir assinaturas digitais dos envolvidos, quando necessárias. • Permitir a leitura automática (OCR) para, no mínimo, os seguintes documentos: CNH e RG. • Permitir ao usuário, a partir dos dispositivos, visualizar seus próprios boletins de ocorrência pelo prazo mínimo de 30 dias. • Permitir que seja feito autodespacho da guarnição. • Permitir que o responsável ou supervisor de várias guarnições possa visualizar em mapa, onde estão localizadas as guarnições de sua responsabilidade e realizar um despacho. • Encerrar o despacho, tornando-se automaticamente guarnição disponível no mapa força da CAM. • Encerrar a guarnição. • Exibir botão de fácil acesso, (botão de pânico) para ser utilizado pelos integrantes da guarnição em caso de necessidade de ajuda. • Uma vez acionado o botão do pânico, o aplicativo deverá: • Permitir o cancelamento em casos de acionamento acidental. • Enviar à CAM os dados necessários para que seja exibido notificação em destaque que a guarnição está solicitando socorro. • Abrir automaticamente um atendimento no módulo de Gestão de Operação. • Deve-se possibilitar a geração de relatórios das ações cadastradas sendo no mínimo necessário: • Relatório que exiba de maneira tabular, as quantidades de atendimento por suas naturezas de classificação e também exibindo as quantidades absolutas e relativas de cada item, com possibilidade dos seguintes filtros, no mínimo: • Intervalo de data e hora • Naturezas de classificação • Relatório analítico dos atendimentos, exibindo de maneira gráfica (pizza, barra, etc.) os atendimentos abertos e encerrados, identificados como anônimos, atendimentos por período do dia, atendimentos por setores, atendimentos por canais, atendimentos por atendente, quantidade de atendimentos por dia da semana e horários com escala térmica de cor, os 20 endereços mais atendidos, os 20 bairros mais atendidos, os 20 telefones mais atendidos, com possibilidade de filtros por intervalo de data e hora. • Relatório analítico dos despachos, exibindo de maneira gráfica (pizza, barra, etc.) os despachos com ou sem atendimento, desvio de natureza, com flagrante, com ato infracional, em próprios públicos, com registro de boletim de ocorrência da própria instituição e de terceiros, apoios, quantidade de apoios, tempo de deslocamento, tempo de atendimento, quantidade de deslocamentos, tempo de primeiro atendimento, despacho por guarnição, despachos por dia da semana e horários com escala térmica de cor, os 20 endereços mais atendidos, os 20 bairros mais atendidos, os 20 telefones mais atendidos, com possibilidade de filtros por intervalo de data e hora. SERVIÇO DE GRAVAÇÃO DE VÍDEO E INTEGRAÇÃO AO REGISTRO DE FATOS • Suporte a serviço de gravação de vídeo em nuvem, para recebimento de vídeos enviados por câmeras através de internet, devendo: • Suportar a conexão de 100 câmeras IP. • Receber no mínimo, imagens (streams de vídeo) h264 e protocolo RTSP, com resolução mínima no armazenamento de 1280x720 (HD) e taxa de frames mínima de 8 fps. • Possibilidade de receber e armazenar os vídeos pelo período mínimo de 10 dias, sobrepondo após este prazo, as gravações das imagens (gravação cíclica). • Possuir visualizador para reprodução dos vídeos das câmeras. • Exibir em mapa, as localizações geográficas das câmeras de CFTV. • Possibilitar exportação de qualquer trecho de vídeo armazenado, em período definido pelo usuário. • Possuir integração com o Registro de Fatos do SISTEMA DE GESTÃO E ANÁLISES, permitindo, a partir deste, a abertura de mapa georreferenciando o local do fato cadastrado e a visualização georreferenciada, das câmeras de monitoramento existentes. • Possuir integração com o sistema de Boletins de ocorrências do SISTEMA DE GESTÃO e Análise, sendo exigido no mínimo: • Possibilitar, a partir de um registro de boletim de ocorrência, a abertura de mapa georreferenciando o local do fato cadastrado e a visualização georreferenciada, das câmeras de monitoramento existentes em um raio pré-determinado. • Permitir no mesmo mapa, a seleção de múltiplas câmeras para verificação de vídeos gravados, exibidos automaticamente, respeitando o intervalo de tempo relativo ao período de duração do Boletim de ocorrência registrado. • Permitir a seleção de determinado trecho de vídeo para importação e sua automática inserção como arquivo anexo ao Boletim de ocorrência em questão. • Permitir a partir da tela de pesquisas do sistema de gestão e análise, selecionar uma determinada passagem veicular e exibir o trecho de vídeo relativo à passagem veicular selecionada.

		• Permitir, a partir de um alarme gerado por passagem veicular monitorada, a exibição do trecho de vídeo relativo à respectiva passagem veicular que gerou o alarme. • A disponibilização do link de internet necessário acesso aos vídeos armazenados será de responsabilidade da CONTRATANTE. INTEGRAÇÃO COM OUTRAS CENTRAIS DE MONITORAMENTO • A PROPONENTE deverá disponibilizar e garantir o funcionamento de um módulo de software que possibilite a troca das informações referentes aos registros de fatos e ao disparo de alarmes, com outras Centrais de inteligência, durante todo o tempo de duração do contrato, devendo: • Manter sincronizados os dados referentes aos registros de fatos ocorridos. • Manter sincronizados os dados referentes aos disparos de alarmes comuns às CAMs. • Garantir que a replicação entre as CAMS, sejam exclusivamente dos dados que foram autorizados pelos operadores da CAM onde foram cadastrados, ou seja, o conteúdo da base de dados de uma CAM só poderá conter dados que a outra CAM autorizou. • Permitir a pesquisa de placas nas CAMs interligadas, com possibilidade de filtro por placa veicular, data e hora, obrigando o preenchimento do motivo da pesquisa e retornando o nome das CAMs, data e hora que possuem a passagem veicular dentro dos parâmetros pesquisados. • Receber como retorno a relação conciliada e ordenada por data/hora de todas as passagens veiculares relativas à placa selecionada, incluindo a possibilidade de visualização das imagens comprobatórias. • Ao solicitar a pesquisa, o operador deverá registrar o fato motivador, que deverá aparecer nas auditorias sobre pesquisas. • As imagens deverão possuir marca d'agua que indique qual usuário efetuou a pesquisa. • Garantir que a troca de dados entre as CAMs, deverá ser de maneira criptografada, fazendo uso do protocolo TLS. • A proponente deverá disponibilizar durante todo o tempo da garantia: • O Sistema de abertura e controle de chamados dispondo de atendimento telefônico para suporte técnico em até 2 horas. (segunda a sexta-feira em horário comercial); • A Intervenção técnica remota em até 2 horas. (segunda a sexta-feira em horário comercial considerado das 08:00h até as 18:00h) • A Intervenção física corretiva até o final do próximo dia útil. • A solução proposta deverá estar instalada em servidor local, alojado na central indicada. Plataforma integrada de gestão, tratamento e apoio a tomada de decisão • Solução integrada de Governança para a centralização e visualização de dados provenientes de diferentes fontes de dados, individuais ou combinados, oferecendo indicadores e métricas para tomada de decisão. Plataforma web integrada que permita a visualização de painéis e relatórios diretamente em navegador web, sem a necessidade de instalação de software ou plug-in nas máquinas dos usuários. • O software deverá atender os seguintes requisitos mínimos: • Permitir a possibilidade de se realizar leitura e integrações de fontes de dados heterogêneas sem a necessidade de hardware ou software adicional; • Possuir as funcionalidades para exportação de relatórios e painéis, integradas na mesma plataforma, com interface única; • Permitir que os dados coletados sejam visualizados sob a forma de painéis gráficos, com possibilidade interativa e associativa entre os objetos, permitindo filtros e detalhamentos; • Permitir filtrar ou disponibilizar dinamicamente pesquisa por tabela de tempo (dias, semanas, meses, trimestres, semestres e anos); • Permitir, durante a criação de novas análises, combinar colunas de um ou mais bancos de dados, através de operações como união e intersecção; • Permitir que sejam realizados detalhamentos cruzados onde a partir de um painel de indicador, o usuário seja direcionado para outro painel ou relatório contextualizado com as informações referentes ao detalhamento; • Permitir a aplicação de filtros, agrupando e classificando dados, comparando períodos, definindo metas e alertas; • Permitir conexão a uma variedade de fontes de dados, como planilhas, bancos de dados, aplicativos. API's e serviços em nuvem; • Permitir a criação de elementos visuais para monitorar e analisar dados em tempo real; • Permitir painéis incorporáveis em sites ou intranets externos; • Permitir painéis incorporáveis de sites externos; • Permitir aos usuários coletar, organizar, visualizar e analisar dados de várias fontes em um só lugar; • Permitir o compartilhamento das visualizações através de URL'S internas; • Permitir a exportação de gráficos e relatórios; • Permitir a exportação para download em PDFs, relatório de e-mail agendados e links publicados; • Permitir o acesso de usuários à plataforma, por definição de nível de acesso de usuário, com ou sem autenticação (sem autenticação através de certificado); • Possuir plataforma web integrada que permita a visualização de painéis e relatórios diretamente em navegador web, sem a necessidade de instalação de software ou plug-in nas máquinas dos usuários; • Permitir a integração com soluções de georreferenciamento, tais como Google Maps, OpenStreetMaps ou outra API de mapas existentes no mercado; • Permitir detalhamento das informações georreferenciadas através de cliques de mouse sobre uma determinada área que pode representar, uma cidade, estado ou país; • Permitir o desenvolvimento e a visualização de painéis de métricas, utilizando uma ou mais fontes de dados, trazendo funções estatísticas, como soma, média, contagem, máximo, mínimo, entre outras; • Permitir agendamento para envio automático por e-mail de objetos disponíveis na plataforma nos formatos PDF e imagem; • Permitir a atualização dos dados dos painéis em tempo real e ou em tempos de consulta parametrizados de acordo com as definições estabelecidas na etapa de análise de requisitos ou conforme disponibilidade da fonte de dados; • A solução de governança deverá ser construída a partir da leitura das bases de dados, com relações explícitas entre diversas bases, diversas tabelas e entre os conteúdos de uma mesma tabela.
		• Será de responsabilidade da contratante, a liberação de acesso à bases de dados de sistemas extras, NÃO fornecidos pela contratada, mediante assinatura de termo de responsabilidade e confidencialidade.

1.3	Serviços de Locação de Link de Dados - Tipo I	1.3.1 SERVIÇO DE LOCAÇÃO DE LINK DE DADOS – TIPO I O link de dados é responsável pela transmissão das imagens captadas pelo ponto de coleta de imagem até a sala de comando e controle. Para atender as necessidades deve-se respeitar os seguintes requisitos: O link deve ser construído em fibra óptica ou radiofrequência; Deve prover a interligação dos pontos de coleta de imagem até a sala de comando e controle; Deve possuir capacidade mínima de 10Mbps no ponto de coleta de imagem; Deverá garantir por meio de canais seguros para transmissão de dados e imagens, compostos por um canal óptico e/ou um enlace de rádio em frequência reservada à segurança pública de acordo com as disposições emanadas da Agência Nacional de Telecomunicações - ANATEL.
2	**KIT 2 - Pontos videomonitoramento Câmera Fixa**	
2.1	Ponto de Videomonitoramento - Câmera Fixa Tipo I	2.1 PONTO DE VIDEOMONITORAMENTO - CÂMERA BULLET 2.1.1 CÂMERA BULLET Deve ser fornecido 4 (quatro) câmera IP do tipo Bullet com as seguintes características: • Deve possuir resolução mínima de 4MP (2688 x 1520); • Deve possuir taxa de quadros de vídeo: o Main stream: 2688 × 1520@1–25/30 fps; o Sub Stream: 704 × 576@1–25 fps/704 × 480@1–30 fps; o Third Stream: 1280 × 720@1–25/30 fps; • Sensor de imagem CMOS 1/3" com varredura progressiva ou superior; • Suporte a compressão de vídeo no padrão H.265; H.265+, H.264; H.264+, H.264H; H.264B; • Possuir obturador na velocidade de 1/3s até 1/100.000s; • Funcionamento em baixa luminosidade com sensibilidade mínima de 0.005 Lux@F1.5 (Color, 30IRE), 0.0005 Lux@F1.5 (B/W, 30IRE), 0 Lux (iluminador ligado) (distância mínima de 60m); • Lente de 2,7mm – 13,5mm varifocal motorizada; • Ângulo de Ajuste Pan:0° - 360°, Tilt: 0° - 90°, Rotação: 0° - 360°; • Possuir função WDR real com valor mínimo de 120dB; • Função Dia & Noite com suporte auto (ICR), colorido, preto & branco; • Possuir funções inteligentes de detecção de cruzamento de linha, detecção de intrusão para veículos e seres humanos; • Deve possuir mecanismo de pesquisa inteligente para, em conjunto com o sistema de armazenamento, realizar pesquisas inteligentes refinadas, extração de eventos e mesclagem com vídeos de eventos; • Deve permitir acesso para até 20 usuários com banda total de 64 Mb; • Possuir os padrões de compatibilidades ONVIF Profile S, Profile G, Profile T, CGI, P2P; • Compatível com os protocolos de rede: IPv4/IPv6, HTTP, TCP, UDP, ARP, RTP, RTSP, RTCP, RTMP, SMTP, FTP, SFTP, DHCP, DNS, DDNS, QoS, UPnP, NTP, Multicast, ICMP, IGMP, NFS, PPPoE, SNMP; • Possuir suporte a tecnologia de armazenamento via FTP, SFTP, NAS e cartão micro SD com capacidade de até 256 Gb; • Ser apto a operações em temperaturas de -30°C a +60°C, com umidade máxima de 95%; • Possuir alimentação compatível para 12Vdc e PoE (802.3af); • Possuir grau de proteção IP67; • Deve possuir mecanismos de segurança com suporte a criptografia de vídeo/firmware/ configuração, digest; bloqueio de conta, logs de segurança, filtragem de IP/MAC, geração e importação da certificação X.509, syslog, HTTPS, 802.1x, inicialização/execução confiável; • Deve possuir compressão de áudio nos padrões G.711A, G.711Mu, G726; • Deve possuir 4 máscaras de privacidade; • Deve possuir as seguintes distâncias de detecção, observação, reconhecimento e identificação (DORI): □ Distância mínima de detecção: lente W: ≥ 60,00 m; lente T: ≥ 200,00 m; • Distância mínima de observação: lente W: ≥ 25,00 m; lente T: ≥ 80,00 m; • Distância de reconhecimento: lente W: ≥ 12,00 m; lente T: ≥ 40,0 m; • Distância de identificação: lente W: ≥ 6 m; lente T: ≥ 20,00 m. 2.1.2 SUPORTE PARA CÂMERA BULLET Suporte para instalação de câmeras externas, em poste, que permita adaptar o equipamento a diversos cenários de aplicação, com as seguintes características: • Deve possuir com comprimento de 1000 mm, parede ≥ 1,5 mm; • Deve possuir suporte para fixação ao poste; • Deve possuir pintura eletrostática (Epóxi); • Deve possuir zincagem à fogo • Deve possuir capacidade de carga mínima de 5kg. 2.1.3 NOBREAK 2000 Equipamento de rede tipo nobreak, senoidal, com as seguintes características mínimas: • Deve apresentar uma potência nominal em regime contínuo de no mínimo 2kVA; • Tensão nominal de entrada ajustável entre 120 e 220V; • Frequência nominal de operação de 60 Hz; • Tensão nominal de saída de 115V; • Deve possuir forma de onda de saída senoidal;

		• Deve possuir baterias VRLA de manutenção; • Deve possuir função de estabilizador; • Deve possuir fator de potência de 0,7; • Deve possuir proteção contra sobrecarga e curto-circuito; • Deve possuir proteção contra sub e sobretensão; • Deve possuir proteção contra descarga profunda da bateria; • Deve permitir modulo de comunicação através de SNMP; • Deve possuir proteção por bateria baixa; • Deve possuir proteção de excesso de temperatura; • Deve operar entre temperatura de 0 ~45° C; 2.1.4 SWITCH 8 PORTAS Equipamento para extensão física dos pontos de rede, com as seguintes características: Características • Deve possuir 9 (nove) portas Gigabit Ethernet 10/100/1000Base-T Conforme Padrões IEEE 802.3, IEEE 802.3u, IEEE 802.3ab; • As interfaces deverão ser Full-Duplex, auto sensing com conectores RJ45 fêmea e implementar mecanismos de autoconfiguração em todas as portas, do tipo MDI/MDI-X; • Deve possuir adicionalmente no mínimo 1 (um) porta Gigabit Ethernet Padrão IEEE 802.3z, para inserção de transceivers do tipo SFP; • As interfaces dos itens 1. e 3. devem operar de modo simultâneo; • Deve possuir leds indicativos de funcionamento; • Deve implementar os padrões IEEE 802.3at e IEEE 802.3af, em pelo menos 8 (portas); • Deve ser capaz de fornecer até 30W por porta (não simultâneo); • Deve possuir o Budget PoE de no mínimo 63W; • Deve possuir capacidade de processamento de no mínimo 20 Gbps; • Deve possuir taxa de encaminhamento de pacotes igual ou superior a 14.88 Mbps; • Sua tabela de MAC Address deve suportar no mínimo 4.000 MAC address; • Deve suportar jumbo frame de no mínimo 16KB; • O equipamento deve possuir no máximo até 1 (uma) ventoinhas internas para resfriamento; • Deve suportar temperatura de operação entre 0° e 50°; • Deve suportar operação sob umidade entre 10% e 90% RH sem condensamento; • Deve compatível com PDs compatíveis com IEEE 802.3af/at; • Deve suportar controle de fluxo EEE802.3x; • Deve suportar 802.1p/DSCP QoS; • Deve suportar IGMP Snooping; • Possuir homologação da ANATEL, de acordo com a resolução número 242 de 30/11/2000; • Possuir Certificação FCC e CE; • Deve ser RoHS (Restriction of Certain Hazardous Substances) Compliance; 2.1.5 ENTRADA ELÉTRICA • Conjunto para a conexão à rede de energia elétrica da concessionária local dentro das normas exigidas para conexão dos dispositivos à rede elétrica, além das normas da ABNT e ANEEL; • Todos os materiais e miscelâneas necessários para a instalação do padrão indicado, devem estar contemplados na proposta da licitante. • O cabeamento elétrico deverá interligar a caixa de equipamentos com o ponto/circuito de energia compatível mais próximo, após comprovada a compatibilidade do circuito; 2.1.6 POSTE DE CONCRETO Poste de concreto com as seguintes características: • Poste com estrutura circular fabricado em concreto armado; • Altura total de 9 metros; • Resistência nominal de 200 DaN; • Deverá atender todas as normas técnicas ABNT pertinentes; • Não será permitido perfurar o poste sem aprovação do fabricante; • Toda fixação de produtos e equipamentos no corpo do poste deverá ser feita através de abraçadeiras em aço galvanizado com parafusos ou outro mecanismo de fixação. 2.1.7 CAIXA PORTA EQUIPAMENTOS Caixa metálica externa, tipo porta-equipamentos, com as seguintes características: • Deve ser fabricada em chapa de aço carbono SAE 1010/ 1100, com espessura mínima de 1,5mm; • Deve possuir dimensões externas de: (H) 600 mm, (L) 525 mm e (P) 600 mm, com tolerância de 2% nas medidas; • Deve possuir Kit de ventilação com dois ventiladores para teto; • Deve possuir abertura para ventilação forçada; • Possuir no mínimo um ventilador, padrão universal; • Deve possuir porta frontal com fechadura e chave; • Deve possuir grau de proteção IP65; • Deve possuir duas prateleiras, no interior da caixa para instalação de equipamentos, placa de montagem fabricada em chapa de aço carbono com espessura 1,5 mm; • Deve ser pintada utilizando tratamento de superfície para proteção e pintura epóxi; • Índice de Proteção (IP) – Mínimo IP 65 (selada contra poeira e protegidas contra jatos de água); • Deve permitir capacidade de carga de no mínimo 100kg; • Deve estar de acordo com a norma de antivandalismo;

		• Deve possuir calha elétrica. 2.1.8 INFRAESTRUTURA • Todos os pontos deverão ser fornecidos com a infraestrutura, descrita abaixo: • Deverão ser personalizadas/detalhadas em plantas ou esquemas elétricos específicos, incluindo aterramento; • O cabeamento elétrico deverá interligar a caixa de equipamentos com o ponto/circuito de energia compatível; • O cabeamento deverá ser ligado dentro da caixa de equipamento ao disjuntor (em série com a fase) e ao varistor (em paralelo); • O dimensionamento do cabeamento deverá ser feito em função da distância e da carga, não podendo ser usada bitola de condutores com diâmetro menor que 2,5 mm²; o cabeamento usado deverá ser do tipo PP, SINTENAX ou equivalente, com três condutores encapados, envolvidos por grossa camada de borracha, de modo que seja imune a água, umidade e intempéries; • A rede elétrica de alimentação dos equipamentos será monofásica, para alimentação em 127V (cento e vinte e sete Volts). A alimentação poderá ser em 220V (duzentos e vinte Volts); • Os pontos deverão ter conectores do tipo RJ45 fêmea, para categoria 5e, com espelhos e identificação. A rede deverá ser instalada e certificada. • Os custos e execução são de inteira responsabilidade da empresa Contratada; • Deverá ser fornecido pela empresa a ser contratada, os materiais de infraestrutura necessários para instalação: • Eletrodutos de PVC; • Luvas; • Abraçadeiras • Cintas de alumínio; • Mangueira de manobra; • Parafusos e buchas; • Cabos elétricos; • Cabo UTP.
2.2	Licença de Software de VMS	2.2 LICENÇA DE SOFTWARE DE VMS A plataforma de VMS, deve ter capacidade de trabalhar com múltiplos sites independentes através da consorciação dos mesmos e os gerenciar em um único site central (SSP/RS), garantindo o monitoramento e gestão dos dispositivos de forma unificada. Deverá ser contemplada a plataforma que interconecta sistemas remotos/menores ao site central sem limite no número de dispositivos conectados a um sistema central. Não possuir banco de dados proprietário local no cliente, devendo qualquer informação inerente ao sistema ser armazenada somente no banco de dados do servidor de gerenciamento com bancos de dados de mercado, como SQL Server. Toda a comunicação e troca de informações entre os servidores devem ter a possibilidade de serem realizadas de maneira encriptada e protegida. O sistema deve permitir independência de criptografias entre câmeras e servidores de gravação e os servidores do sistema com as estações de trabalho, permitindo segregação das redes criptografadas. Deve disponibilizar funções de servidor de gerenciamento com proteção de redundância (failover), isto é, quando o servidor gestão por algum motivo vier a ficar ofline, outro servidor deve assumir suas funções até que o principal retorne a exercer suas funções normalmente. Deve disponibilizar funções de servidores de gravação com proteção de redundância sem custo adicional de licença (failover), isto é, quando o servidor/servidores de gravação por algum motivo vier a ficar ofline, outro servidor deve assumir suas funções até que o principal retorne a exercer suas funções normalmente, e as imagens gravadas no servidor de backup devem ser transmitidas ao servidor principal preenchendo a lacuna do tempo ofline. O Sistema deve permitir a função de travamento de evidência, isto é, permitir que uma evidência em específico presente no sistema seja impedida de ser apagada independente do tempo de gravação do sistema, ou seja, não seja removida mesmo após atingir o tempo de retenção de imagens estipulada no projeto. O sistema deve suportar: Visão Geral • Solução de sistema de vídeo segurança deve ser integrado, multiusuário e multi-site. Deve suportar um número ilimitado de servidor de gravação e visualização de câmeras IP, codificadores de vídeo IP; • Gerenciamento otimizado de armazenamento de vídeo: A solução deve dispor de arquivamento único, gravação de longa duração de bom desempenho, escalabilidade e custo-eficiente; • Detecção automática de modelo de câmera: Deve suportar mais de 9000 modelos de câmeras IP, codificadores de vídeo IP, e mais de 150 fornecedores diferentes, utilizando métodos como a Universal Plug and Play, Broadcast, varredura manual e varredura por faixa de IP; • Número ilimitado de servidores de gravação: Deve suporta um número ilimitados de câmeras por servidor. Gravação continua ou ativada por movimento, evento ou agendamento; • Rede e armazenamento otimizados: Deve suportar multi-streaming que otimiza a banda usando novos métodos de compressão; MPEG4, H.264, H.265 além MJPEG e MPEG4; • O Multi-live Streaming possibilita definir múltiplos fluxos de vídeo ao vivo com diferentes configurações. Ele otimiza a performance de visualização do Cliente de Monitoramento de acordo com a disponibilidade de banda (throughput) e layouts de visualização; • Deve ser capaz de armazenar conteúdo em vídeo que não são críticos em diferentes topologias e arquitetura de armazenamento; • Deve suportar a detecção de movimento, independente do modelo da câmera; seja pelo servidor ou pela câmera; ou simultaneamente;

		• Plataforma Aberta: Deve fornecer API / SDK de forma gratuita e suportar integração com hardware ou aplicativos de terceiros. • Integração nativa de todos os dispositivos compatíveis com os fóruns de compatibilidade Onvif Profile S, Q e T e PSIA. • Instalação em Windows 64 bits; • Compatível com Instalações em ambiente virtualizado VMWare e Microsoft Hyper-V; • Deve permitir exibição do alerta gerado pelos dispositivos, através do processamento dos metadados recebido das câmeras / encoders, mostrando os quadros (overlay) nos formatos e cores gerados pelos dispositivos. Tudo isto deve ser permitido através do dispositivo integrado via ONVIF. • Permitir integração com Solução de Vídeo Wall com número ilimitado de monitores; • Deve possibilitar total compatibilidade com, no mínimo, duas versões anteriores do sistema; O sistema deve conter os componentes a seguir: • Serviço de Administração • Gerenciamento centralizado: O software de administração deve oferecer um acesso único e consolidado para configuração dos servidores de gravação, mesmo em instalações multisites; • Assistentes de configuração: Guia o usuário através do processo de adição de câmeras, a configuração de vídeo e gravação, ajuste de detecção de movimento e configuração do usuário; • Detecção automática de dispositivos: permite a detecção rápida de dispositivos e câmeras usando métodos como a Universal Plug and Play, Broadcast e varredura por faixa de IP; • Opção de configuração em massa: Altera as configurações em vários dispositivos ao mesmo tempo com poucos cliques; independentemente de estarem no mesmo site ou em sites remotos; • Gerenciamento de senhas dos dispositivos diretamente na interface do software. O sistema deve permitir automação de troca periódica das senhas dos dispositivos. • Importação de dados de configuração off-line: Permite a edição off-line de dados de configuração, incluindo câmeras e as definições de dispositivos; • O sistema de backup deve permitir configurações que permita criar pontos de restauração a cada vez que uma mudança de configuração é realizada, permitindo a reversão de maneira facilitada. • Deve permitir a personalização da interface de administração de acordo com os direitos de cada usuário, concedendo permissões, restringindo funções e ocultando / desabilitando partes da interface para evitar o acesso indevido a ações restritas. • Ser nativamente compatível com Microsoft Active Directory para gestão de usuários e perfis de acesso do Windows e permitir autenticação de usuário única (SSO) • Permitir controle de acesso aos perfis de usuários: Visualização ao vivo, controle PTZ, presets PTZ, controle de saídas, Eventos, ouça o microfone, fale com a caixa de som remota, gravação manual; Reprodução, exportação AVI, exportação JPG, exportação de banco de dados, sequências, pesquisa inteligente e áudio. Bem como definir as vistas, editar vistas particulares e públicas. • Trabalhar com banco de dados centralizado de fabricantes reconhecidos de mercado como SQL Server, Oracle ou MySQL • Deve permitir acesso remoto para software de visualização e aplicativo para visualização em web browsers ou software cliente, com opção de conexão segura no acesso à câmera (HTTPS). • Ter servidor de Web embutido para download de softwares e plug-ins. • Ter histórico de provas exportadas por usuário e arquivo. • Ter histórico de atividade do usuário do cliente pelo tempo, localidade e câmeras. • Pode ser instalado em conjunto com o servidor de gravação. • Fornecer streams múltiplos de vídeo ao vivo para diferentes clientes. Serviço de Servidor Móvel O sistema deve suportar: • Acesso remoto para clientes móveis. • Realiza o login e solicitações de acesso entre clientes e o Servidor Master. • Redimensiona as imagens de vídeo vigilância para ajustar ao layout da tela dos dispositivos móveis. • Pode ser instalado em conjunto do servidor de gravação. • Deve permitir ser instalado em dispositivos com sistema operacional iOS, Android. • Deve permitir a transmissão de imagens geradas em tempo real pela câmera do dispositivo móvel para a central de monitoramento, e gravar estas imagens no sistema como se fosse um dispositivo fixo já instalado no sistema. • Deve permitir a Inclusão do geo-posicionamento através de meta dados de GPS advindos do dispositivo móvel. • Deve permitir eventos/alarmes no dispositivo móvel em tempo real; Serviço de Gestão de Eventos e Alarmes • Deve ter um motor (engine) que forneça regras para a automação de diferentes aspectos do sistema, incluindo controle da câmera, comportamento do sistema e dispositivos externos, com base em eventos ou horários. • Deve fornecer uma caixa de diálogo de configuração no estilo Microsoft Outlook, na qual eventos predefinidos e personalizados são usados nas regras para acionar ações. • Teve ter as seguintes categorias de eventos: • Hardware: dispositivos de hardware físico conectados ao sistema. • Dispositivos: certas funções e estados de dispositivos disponíveis através de dispositivos de hardware conectados. • Externo: relacionado às integrações do VMS. • Servidor de gravação: funções de arquivamento e banco de dados. • Análise: a partir de aplicativos e sistemas de análise integrados. • Definido pelo usuário: Eventos configurados de forma personalizada, permitindo que os usuários disparem

		Perfis de horário • Ter gerenciamento de evento / alarme de ponto único: gerenciamento central de todos os alarmes internos do sistema e alarmes externos de segurança. • Ter suporte à associação de alarmes a mapas. • Deve possuir um Gerenciador de Alarmes que permita: • Lista de alarmes com amplos recursos de classificação e filtragem. • Visualização instantânea de vídeo gravado de câmeras primárias e relacionadas, no momento do incidente. • Imagem em miniatura da câmera principal, no momento do incidente. • A opção de desativação de alarme deve permitir que os usuários suprimam alarmes de um determinado dispositivo por um período de tempo especificado. • Relatórios de tratamento de alarmes, fornecendo informações sobre a entrada e o desempenho do tratamento de alarmes. Serviço de Gravação e gerenciamento das gravações O sistema deve suportar: • Gravação digital simultânea de vários canais de vídeo e áudio. • Transmissão de áudio bidirecional do microfone do cliente para alto-falantes remotos. • A otimização da largura de banda devido ao multi-streaming, dividindo o fluxo de vídeo da câmera para fluxos diferenciados para ver vídeo ao vivo e gravado. • O software cliente pode solicitar a visualização ao vivo em uma taxa de quadros diferentes e em resolução mais baixa que as configurações de gravação. • Conectividade para as câmeras, codificadores de vídeo e DVRs suportando compressões como MJPEG, MPEG4, MPEG4 ASP, H.264 e MxPEG, H.265. • Detecta automaticamente os modelos de câmeras durante a instalação. • Número ilimitado de câmeras instaladas. • Tecnologia de gravação: banco de dados seguro de alta velocidade de imagens JPEG ou fluxos MPEG4 e H264 incluindo áudio. • Velocidade de gravação: Mais de 30 frames por segundo por câmera, limitado apenas pelo hardware e rede. • A qualidade da gravação depende inteiramente da câmera e do encoder: não há limitação de software. • Capacidade de gravação ilimitada, dependendo apenas da capacidade de storage. • Exportação de vídeo configurável por hora ou diária, com passagem automática opcional para unidade de rede de maior capacidade de armazenamento, com imagens disponíveis para reprodução de forma transparente para o operador. • Detecção de movimento embutida, em tempo real, com sensibilidade completamente ajustáveis e com zonas de exclusão. Permitindo ativar a gravação com velocidade de frames superior quando é detectado movimento ou quando surge um evento, notificando o alerta por e-mail. • Gravação manual com início do tempo baseada em critérios pré-definidos e privilégios de acesso. • Pan Tilt Zoom (PTZ) com presets armazenados pelo sistema, sendo em até 50 por câmera. • Ativação de presets e patterns quando acontecem determinados eventos. • Programação para ativação do pattern em períodos diferentes: isto é, diferente para dia e noite, semana, etc. • Varredura PTZ em dispositivos suportados: visualização ou gravação enquanto se move lentamente a partir de uma posição para outra. • Acione o limpador ou esguicho de água remotamente, nos modelos suportados de PTZ • Em eventos pré-definidos comandos são enviados automaticamente para exibir vídeo ao vivo em computadores remotos. • O servidor de gravação é executado como um serviço do Windows. • Gravação em multi estágios, permite configurar o sistema para gravar em locais, tempo e taxa de frames diferentes. Permitindo até a redução da taxa de frames automática para atender a demanda de tempo de configuração. • Recuperação configurável de trechos de vídeo perdidos diretamente da câmera que possui a função de gravação local (seja através de cartão de memória removível ou memória fixa embutida na câmera). • Deve suportar gravação embarcada na câmera (edge storage) em vários fabricantes e em dispositivos ONVIF nos perfis acima mencionados; • Serviços de conexão remota aos servidores de imagem. • Suportar sistemas servidores de gravação de 64 bits, em hardware e software. • Assinatura digital no banco de dados garantindo integridade do vídeo. • Monitoramento do sistema e do servidor de imagens com relatório das configurações. Redundância da gravação de vídeo • O sistema deve permitir que em caso de falha na gravação dos vídeos, outro assuma, sem a adição de licença para essa função; • A redundância poderá ser efetuada em um ou vários (N:N) storage exclusivos para essa função, ou pode ser feito nos mesmos gravadores do sistema. • Deve possibilitar mover dispositivos (câmeras ou grupo de câmeras) entre diferentes servidores de gravação; • Deve mover todos os dispositivos associados; • Deve dispensar reconfiguração de câmeras. • Observação: O serviço de gravação nos servidores de gravação não deve depender da instalação de um banco de dados local para garantir seu funcionamento. Software de Visualização de Gravação Operação O sistema deve suportar: • Visualização ao vivo e reprodução: Clients desde dispositivos móveis a computadores com suporte para visualizar até 100 câmeras de vários servidores ao mesmo tempo. • Exibições de Janelas/Layouts: Trabalha com exibições contendo até 10x10 câmeras, Hot spot, Matriz, Sequencial, imagens estáticas e ativas, vídeos ao vivo ou gravados, mapas HTML, distribuídos em todos os monitores do computador. • PTZ inteligente: controle manual, presets, macros (vá à preset quando evento), patrulhamento com esquemas múltiplos (pattern), comandos para limpador (palheta) e esguicho de água, controle por joystick e teclado/mouse. • Matriz Virtual: exibições de controle de câmara ao vivo em computadores remotos para visualização distribuída.

		• Controle de Entradas/ Saídas de Alarme: Das câmeras ou dispositivos de I/O, de forma a criar botões/eventos manuais, ou receber sinais de sistemas de intrusão ou controle de acesso. • Áudio multicanal bidirecional: Ouça áudio ao vivo/gravado com reprodução instantânea no PC cliente e transmita voz pelo microfone a alto-falantes remotos. • Permite gravação de áudio sincronizada a qualquer canal de vídeo. • Gravação manual: Baseado em privilégios de acesso definido pelo administrador, os usuários clientes podem manualmente iniciar a gravação de uma câmera por um tempo predefinido. • Dupla autenticação, exigindo com que o usuário tenha autenticação de um usuário supervisor para conseguir se autenticar no software, protegendo o sistema de acessos indevidos. • Stream de visualização adaptativo, onde a resolução da câmera é alterada automaticamente quando o operador muda a visualização do modo mosaico para modo único em tela cheia. • Capacidade de enviar vídeos ao vivo e gravado para monitores de vídeo wall dentro da própria interface. Busca, backup e dados seguros O sistema deve suportar: • Processamento de gravação: Através da busca de movimento acima do vídeo gravado, PTZ digital com suavização de imagem opcional (apenas no software visualizador). • Backup de Evidência: JPEG, AVI, WAV e formatos de dados nativos com software visualizador stand-alone, criptografia de dados e registros, notas de usuários e impressão de relatórios. • Autenticação: contas de usuário do Microsoft Active Directory e nativos. • Autorização: contas de usuário e grupos do Microsoft Active Directory e perfis de usuário nativos (do sistema), todos os privilégios de acesso e controle de ações permitidas no nível da câmera. • Histórico: Todas as ações do usuário por tempo, localizações e câmeras, e toda a operação do sistema. • Alerta: Notifica os usuários em caso de detecção de movimento ou evento por som, e-mail ou SMS. • Reprodução de gravações de vídeo e áudio localmente no servidor de gravação. • Visualização de até 16 câmeras com tempo sincronizado durante a reprodução. • Pesquisa instantânea em gravações com base na data / hora e atividade. • Pesquisa inteligente unificada, através de detecção de movimento, marcadores(bookmarks), eventos e alarmes. • Pesquisa Forense por metadados: A pesquisa deve poder utilizar eventos de metadados gerados pelas câmeras como ferramenta de busca de imagens. • Linha de tempo de atividade com recurso de lupa; possibilitando ampliar ou reduzir a faixa de tempo necessária para dar início a busca por vídeos gravados; • Pesquisa instantânea em gravações com base na data / hora e atividade / alarme (Video Motion Detection). • Provas podem ser geradas com relatório impresso, imagem em JPEG, AVI ou no formato proprietário (com visualizador incluso), ou ainda pode exportar vídeo em formato MKV padrão. • Exportação de gravações de áudio em formato WAV ou AVI. • Exportação de vídeo digital com zoom para visualizar área de interesse, e para minimizar o tamanho do arquivo exportado. • Criptografia e opção de senha de proteção para as gravações e os arquivos exportados. • Capacidade de adicionar comentários às provas exportadas, também criptografadas. • Possuir interface proprietária, desenvolvida pelo mesmo fabricante e com mesmo código fonte do servidor de gerenciamento e gravação. • Possuir mesma comunicação/ conceito visual do server side. • Não possuir banco de dados proprietário local no cliente, devendo qualquer informação inerente ao sistema ser armazenada somente no banco de dados do servidor de gerenciamento/ banco de dados SQL Server. • Opção para enviar imagens por e-mail. Aplicativo de visualização através do Web Browser O sistema deve suportar: • Visualização de vídeo ao vivo ou reprodução de gravações para 1 a 16 câmeras simultaneamente, advindos do mesmo ou diferentes servidores. • Navegação de vídeo avançadas, incluindo reprodução lenta/rápida, salto a data/hora e pesquisa de movimento no vídeo. • Exibições individuais podem ser definidas pelo usuário em vários layouts: exibição ou reprodução de imagens da câmera de vários servidores simultaneamente na mesma vista. • Vistas compartilhadas podem ser geridas centralmente, através do servidor com permissão de administrador. • Importação de mapas estáticos ou ativos para navegação rápida entre câmeras. • Controle do relé de saída de alarme. • Visão geral das sequências com movimento detectado e janela de visualização. • Visão geral de eventos / alertas. • Controle de câmeras PTZ remotamente, usando também posições pré-determinadas. • Controle remoto de PTZ por clique em ponto. • Controle remoto de zoom sinalando um retângulo. • Assumir controle manual sobre uma câmara PTZ que executa um esquema de patrulhamento; após um período de tempo sem atividade a câmera volta ao seu patrulhamento programado. • Criar arquivos AVI ou criar imagens JPEG geradas a partir de conteúdo gerado pelo software, seja estas imagens advindas de vídeo ou não; • Imprimir relatórios de incidentes com os comentários livres e pertinentes ao usuário. • Sistema de login usando nomes de usuário e senhas cadastrados no sistema proprietário ou delegado ao Microsoft Active Directory. Matriz de Vídeo O sistema deve suportar: • Matriz virtual mostrando o vídeo ao vivo diretamente de no mínimo 04 câmeras por cada tela individual a serem acionadas remotamente por comandos remotos e manuais; • Sequência de câmeras tipo FIFO (first-in-first-out)

		• Vários eventos podem controlar um monitor de matriz e eventos únicos pode controlar vários monitores. • Visualizar o vídeo na sua taxa máxima de frames em qualquer codec provido pela câmera. Cliente celular O sistema deve suportar: • Aplicativos gratuitos para dispositivos baseados em sistema operacional Android (Google), iOS (Apple) e Windows Phone 8 • Permitir a visualização de múltiplas imagens simultaneamente. • Busca e reprodução de vídeo gravado. • Toque na tela do dispositivo para zoom digital e diferentes modos de visualização da imagem. • Controle das funcionalidades PTZ das câmeras. • Salvar ou compartilhar uma foto do vídeo exibido ao vivo. • Permitir a utilização da câmera de vídeo do dispositivo móvel como um gerador de imagens para o sistema principal. Opções de Integração O sistema deve ser: • Compatível com software supervisório de alarmes e estado de dispositivos para grandes instalações. • Ter SDK gratuito para integração do vídeo em outros produtos usando a API para exibir imagens ao vivo, reprodução de atividades gravadas, mostrar imagens de determinado período de tempo, e buscar por movimento. • Criar, importação e usar páginas HTML para a navegação entre os pontos de vista ou para ativar a matriz virtual no software de visualização. • Integrado nativamente com todos os dispositivos listados nos fóruns de compatibilidade Onvif, Profile S e PSIA. • Deverá integrar a Plataforma integrada de gestão, tratamento e apoio a tomada de decisão, unificando os dados e relatórios das soluções de reconhecimento facial e análise comportamental viária ofertados, na mesma plataforma. Devendo demostrar as funcionalidades deste item no momento da análise das amostras. Licenciamento Deve estar composto por: • Licença de Sistema; • Obrigatório para a instalação do produto; • Deve abranger a instalação de um número ilimitado de servidores usando a mesma licença do software de código e a designação de servidores; • A licença contempla um número ilimitado de servidores de gravação, softwares clientes ou clientes web e aplicativos móveis; • Não tem validade e ser de propriedade do Contratante; • Todos os softwares clientes não deverão ser licenciados e podem ser instalados e utilizados em qualquer número de computadores, de forma gratuita; • Acordo de Manutenção do Produto: Esta licença garante a aquisição e uso de forma gratuita de todas as atualizações dos produtos. Deverá ser adquirida para 3 anos. Expansão do Sistema • A expansão do sistema não deve ser atrelada a quantidade atual de servidores / câmeras; • O número de servidores de gravação deve permitir ser ampliado a qualquer momento, sem necessidade de licenciamento adicional, seja local ou remoto; • O número de câmeras pode ser ampliado independentemente da quantidade de servidores de gravação e/ou estações de operação do sistema; • O número de clientes de operação e de dispositivos móveis, poderá ser ampliado a qualquer momento sem necessidade de licenciamento adicional. Plataforma integrada de gestão, tratamento e apoio a tomada de decisão • Solução integrada de Governança para a centralização e visualização de dados provenientes de diferentes fontes de dados, individuais ou combinados, oferecendo indicadores e métricas para tomada de decisão. Plataforma web integrada que permita a visualização de painéis e relatórios diretamente em navegador web, sem a necessidade de instalação de software ou plug-in nas máquinas dos usuários. • O software deverá atender os seguintes requisitos mínimos: • Permitir a possibilidade de se realizar leitura e integrações de fontes de dados heterogêneas sem a necessidade de hardware ou software adicional; • Possuir as funcionalidades para exportação de relatórios e painéis, integradas na mesma plataforma, com interface única; • Permitir que os dados coletados sejam visualizados sob a forma de painéis gráficos, com possibilidade interativa e associativa entre os objetos, permitindo filtros e detalhamentos; • Permitir filtrar ou disponibilizar dinamicamente pesquisa por tabela de tempo (dias, semanas, meses, trimestres, semestres e anos); • Permitir, durante a criação de novas análises, combinar colunas de um ou mais bancos de dados, através de operações como união e intersecção; • Permitir que sejam realizados detalhamentos cruzados onde a partir de um painel de indicador, o usuário seja direcionado para outro painel ou relatório contextualizado com as informações referentes ao detalhamento; • Permitir a aplicação de filtros, agrupando e classificando dados, comparando períodos, definindo metas e alertas; • Permitir conexão a uma variedade de fontes de dados, como planilhas, bancos de dados, aplicativos. API's e serviços em nuvem; • Permitir a criação de elementos visuais para monitorar e analisar dados em tempo real; • Permitir painéis incorporáveis em sites ou intranets externos; • Permitir painéis incorporáveis de sites externos; • Permitir aos usuários coletar, organizar, visualizar e analisar dados de várias fontes em um só lugar; • Permitir o compartilhamento das visualizações através de URL'S internas;

		• Permitir a exportação de gráficos e relatórios; • Permitir a exportação para download em PDFs, relatório de e-mail agendados e links publicados; • Permitir o acesso de usuários à plataforma, por definição de nível de acesso de usuário, com ou sem autenticação (sem autenticação através de certificado); • Possuir plataforma web integrada que permita a visualização de painéis e relatórios diretamente em navegador web, sem a necessidade de instalação de software ou plug-in nas máquinas dos usuários; • Permitir a integração com soluções de georreferenciamento, tais como Google Maps, OpenStreetMaps ou outra API de mapas existentes no mercado; • Permitir detalhamento das informações georreferenciadas através de cliques de mouse sobre uma determinada área que pode representar, uma cidade, estado ou país; • Permitir o desenvolvimento e a visualização de painéis de métricas, utilizando uma ou mais fontes de dados, trazendo funções estatísticas, como soma, média, contagem, máximo, mínimo, entre outras; • Permitir agendamento para envio automático por e-mail de objetos disponíveis na plataforma nos formatos PDF e imagem; • Permitir a atualização dos dados dos painéis em tempo real e ou em tempos de consulta parametrizados de acordo com as definições estabelecidas na etapa de análise de requisitos ou conforme disponibilidade da fonte de dados; • A solução de governança deverá ser construída a partir da leitura das bases de dados, com relações explícitas entre diversas bases, diversas tabelas e entre os conteúdos de uma mesma tabela. • Será de responsabilidade da contratante, a liberação de acesso à bases de dados de sistemas extras, NÃO fornecidos pela contratada, mediante assinatura de termo de responsabilidade e confidencialidade. Modulo de análise de vídeo A plataforma de análise de vídeo deve terá uma estrutura de processamento multicamada baseada na análise do vídeo em tempo real com um componente de autoaprendizagem de comportamento usual, que permitirá gerar alertas quando um evento incomum for detectado. Esse componente deverá ser capaz de aprender o comportamento usual a partir de uma cena de uma câmara fixa, câmera por câmera, num período não superior a uma semana. A partir de um alerta de comportamento anômalo seguir-se-á um módulo de classificação e contextualização por Deep Learning que permitirá definir qual o objeto específico que gerou o alerta. Isto visa contextualizar o alerta para facilitar sua análise por parte do motor de regras da plataforma ou mesmo do operador do centro de controle. A plataforma deverá adicionalmente conter um motor de Regras/Lógica que automaticamente interpretará os alertas classificados pelo Deep Learning e ajudará a definir as ações a tomar. A camada de análise em tempo real disparará acionadores com base nos seguintes critérios: qualquer comportamento incomum, objeto deixado ou removido, cruzamento de linha, objetos em movimento a distâncias de alguns metros a vários quilômetros (câmeras térmicas) A plataforma deve ser capaz de processar vídeo de câmeras térmicas e/ ou visíveis em formato H265, H264 com resoluções variáveis, de 352 x 288 até 1920 x 1080 ou superior. A plataforma de análise de vídeo deverá ser capaz de gerar um alarme quando for feita uma tentativa de alterar o campo de visão da câmera ou quando a qualidade da imagem se deteriorar devido a desfoque, sujeira ou ofuscamento da lente ou obscurecimento da imagem, borda embaçada detecção, etc O sistema deve permitir configurações específicas da câmera, como definição de áreas específicas, cruzamento de linha, sensibilidades, tempo máximo de um objeto em uma cena dentro de um determinado campo de visão da câmera. A plataforma de análise de vídeo funcionará como uma plataforma de Inteligência Artificial de autoaprendizagem não supervisionada, portanto não exigindo que os operadores definam regras ou condições para detectar eventos incomuns. A plataforma de análise de vídeo será capaz de escalar ou descartar alguns alertas de forma autônoma por meio de seu motor lógico, enquanto apresenta outros alertas a um operador humano para avaliação posterior. O operador deve receber uma indicação visual de quaisquer alertas gerados pela plataforma de análise de vídeo. Caixas delimitadoras com esclarecimentos de metadados devem estar visíveis no alerta enviado ao operador para contextualização adicional. A pedido do Operador, deve ser apresentado um Vídeo Clipe do Alerta, começando imediatamente antes do alerta ocorrer (pré-alarme) e terminando após o seu término (pós-alarme). A plataforma de análise de vídeo deverá ser capaz de classificar uma ampla variedade de objetos, como (mas não limitado a): pessoas, carros, bolsas, mochilas, pássaros, animais, telefones celulares, etc. A plataforma de análise de vídeo pode identificar rostos para fins de classificar ou contar pessoas. A plataforma de análise de vídeo deve ser capaz de detectar capacetes de motocicleta e capacetes de segurança do trabalho O mecanismo de regras lógicas deverá permitir a criação de regras precisas, que podem efetivamente mitigar riscos ao otimizar o fluxo de trabalho do sistema. Uma ferramenta de pesquisa forense deve estar disponível para análise pós-evento, para permitir a geração de relatórios rápidos sobre alertas/objetos específicos dentro de áreas específicas do campo de visão da câmera, para intervalos de tempo específicos A plataforma de análise de vídeo deverá oferecer funcionalidades de relatórios de Business Intelligence para fins operacionais. As informações incluirão: Volumes de alerta por câmera; estatísticas de desempenho do operador; eficiência do sistema; estatísticas de classificação. A plataforma de análise de vídeo deverá armazenar numa base de dados SQL ou similar os fotogramas das imagens associadas aos alertas gerados pelo sistema, para eventual consulta futura. Arquitetura do sistema A plataforma de análise de vídeo pode funcionar em conjunto com um VMS de mercado, um NVR ou também estar disponível numa versão autônoma (stand alone) com uma interface de usuário baseada em web. A plataforma de análise de vídeo será totalmente escalável, desde algumas câmeras a milhares de câmeras para processamento simultâneo. A plataforma de análise de vídeo deve ser eficiente em HW, com uma combinação equilibrada de uso de CPU e GPU, ou ainda OpenVino para sistemas com poucas câmeras.

		A plataforma de análise de vídeo deve poder ser implantada em arquiteturas distribuídas, permitindo uma escolha equilibrada entre uma arquitetura de HW totalmente centralizada e uma arquitetura totalmente Edge. Requisitos funcionais A plataforma de análise de vídeo deve ter monitoramento integrado que possa detectar mascaramento de câmera, ofuscamento, desfoque e reposicionamento A plataforma de análise de vídeo deve ser capaz de contar pessoas e objetos que passam pela cena A plataforma de análise de vídeo deve ser capaz de classificar o maior número possível de objetos dentro de um determinado alerta. Essa classificação deve ser exibida com uma caixa delimitadora, bem como conter uma indicação da probabilidade de classificação (0-100%). Embutido no vídeo, uma indicação visual clara deve estar disponível destacando o alerta ou evento anormal que foi detectado. O algoritmo de análise de vídeo deve empregar Deep Learning em todo o campo de visão da câmera. A plataforma de análise de vídeo deve ser capaz de classificar todos os alertas do sistema em uma lista não exaustiva de casos. A plataforma de análise de vídeo deve ser capaz de ignorar automaticamente eventos específicos para minimizar "falsos positivos" ou eventos sem risco. Esses eventos ignorados (e classificados) são geralmente, entre outros: Fatores ambientais como chuva, queda de folhas, vento, movimentação de água, animais de estimação, etc. Esses eventos ignorados devem ser explicitamente definidos pelo operador. A plataforma de análise de vídeo deve incorporar ferramentas que permitam ao pessoal de segurança e vigilância: • Revisar alertas e eventos anormais durante um período ou local definido • Relatar um alerta enriquecido com dados do Deep Learning A plataforma de análise de vídeo deve ser capaz de oferecer suporte a um conjunto de ferramentas de relatórios de incidentes, incluindo incidentes por data, incidentes por categoria e incidentes por câmera. A plataforma de análise de vídeo deve ser capaz de encaminhar alarmes para as autoridades apropriadas ou pessoal de segurança. A plataforma de análise de vídeo deve ser capaz de registrar e marcar a hora de todos os alertas, ações de regras, classificações e ações do operador para fins de treinamento, auditoria e perícia. Mecanismos de geração de alertas A plataforma de análise de vídeo aprenderá de forma adaptativa sem supervisão e, com o tempo, se ajustará automaticamente às mudanças em uma cena de câmera enquanto continua a identificar todos os eventos anormais. A plataforma de análise de vídeo deve identificar eventos anormais sem a necessidade de regras definidas pelo operador. O sistema deve detectar qualquer evento anormal sem quaisquer regras, viés ou pré-condições. A plataforma de análise de vídeo deve ser capaz de detectar vandalismo de forma autônoma A plataforma de análise de vídeo deve ser capaz de detectar de forma autônoma comportamentos agressivos, brigas etc. A plataforma de análise de vídeo deve ser capaz de detectar de forma autônoma pessoas ou objetos que estão correndo/se movendo em uma velocidade incomum, ou na direção errada A plataforma de análise de vídeo deve ser capaz de detectar de forma autônoma pessoas mandriando A plataforma de análise de vídeo deve ser capaz de detectar fumaça e fogo como pré-alarme A plataforma de análise de vídeo deve ser capaz de detectar de forma autônoma caixas registradoras que são deixadas abertas A plataforma de análise de vídeo deve ser capaz de detectar de forma autônoma pessoas ou veículos se movendo na direção errada ou em faixas erradas para carros. A plataforma de análise de vídeo deve ser capaz de detectar de forma autônoma portas que deixadas abertas A plataforma de análise de vídeo deve ser capaz de detectar de forma autônoma filas em áreas específicas da cena A plataforma de análise de vídeo deve ser capaz de detectar de forma autônoma irregularidades nas áreas reservadas para carga ou descarga de mercadorias A plataforma de análise de vídeo deve ser capaz de detectar de forma autônoma pessoas que acessam áreas proibidas em dias/horários inapropriados, /aglomeração de pessoas em áreas não autorizadas A plataforma de análise de vídeo deve ser capaz de detectar de forma autônoma vazamentos acidentais de sprinklers ou grandes derramamentos de líquidos A plataforma de análise de vídeo deve ser capaz de detectar de forma autónoma pessoas que caem - emergência médica A plataforma de análise de vídeo deve ser capaz de contar pessoas em zonas predefinidas e relatar quando uma capacidade predefinida foi excedida A plataforma de análise de vídeo deve ser capaz de detectar autonomamente pessoas caminhando na direção errada ou entrando na área restrita A plataforma de análise de vídeo deve ser capaz de detectar quando um objeto permanece em uma área especificada pelo usuário por um tempo maior do que o pré-configurado Detecção de ameaças em movimento Plataforma de análise de vídeo deve ser capaz de detectar objetos em movimento que se destacam em seu ambiente. A plataforma de análise de vídeo deve ter a capacidade de aprender a cena e focar em alvos reais e não em fatores ambientais comuns à cena. A plataforma de análise de vídeo deve ser capaz de filtrar o ruído ambiental, como, entre outros: árvores em movimento, grama em movimento, reflexos na água, etc. A plataforma de análise de vídeo deve ser capaz de detectar e identificar objetos em movimento muito rápido em distâncias curtas (<50 m) A plataforma de análise de vídeo deve ser capaz de detectar objetos em movimento a uma distância muito longa (> câmeras visíveis de +800 m ou mais de 1 km com câmeras térmicas).

		Ao usar câmeras térmicas, a plataforma de análise de vídeo deve ser capaz de detectar objetos em movimento em cenários de baixo contraste. A plataforma de análise de vídeo deve ser capaz de detectar o movimento de objetos ou pessoas mesmo quando usada em câmeras PTZ (pan tilt zoom), bem como definir zonas de exclusão individuais para cada preset do sequenciamento da câmera PTZ, de uma preset a outro. A plataforma de análise de vídeo deve ser capaz de gerar alertas direcionais relacionados a objetos que entram de uma determinada direção. Regras e mecanismo de lógica A plataforma de análise de vídeo dever ser capaz de definir um número ilimitado de regras a nível da cada câmera A plataforma de análise de vídeo deverá permitir a definição de um conjunto de regras aplicáveis ao nível da câmera A plataforma de análise de vídeo deverá permitir a priorização de alertas A plataforma de análise de vídeo deverá permitir a definição de um conjunto específico de regras para regiões específicas na visão da câmera. A plataforma de análise de vídeo deverá permitir definir regras para automaticamente descartar alertas ou escalar alertas à condição de alarme. Interface de alerta A plataforma de análise de vídeo deve ser capaz de permitir a exibição de Imagens de Alerta estáticas, enriquecidas com caixas delimitadoras de Metadados. As interfaces de gerenciamento de alertas devem permitir o gerenciamento eficaz e eficiente de grandes volumes de câmeras e alertas. As interfaces de gerenciamento de alertas deverão ser otimizadas para maximizar a eficiência do operador, ao mesmo tempo em que promovem a melhor qualidade de saída possível. As interfaces de gerenciamento de alertas incluirão funcionalidades de pesquisa e notificação, permitindo uma análise efetiva do desempenho da câmera, do sistema e do operador. Devera ser integrado ao software de reconhecimento facial ofertado, enviando os alertas gerados por incidência de indivíduos para análise do reconhecimento facial, identificando os indivíduos em cena e verificação no bando de dados. Os alertas classificados, deverão ser direcionados ao sistema de Gestão de Operação, para atendimento e despacho de viatura. Integração com o sistema de Plataforma integrada de gestão, para apoio na tomada de decisão. Pesquisa Forense O sistema suportará pesquisa/navegação de arquivos e os usuários podem filtrar o resultado da pesquisa por câmera com: a. Área específica em uma cena b. Número de objetos na área c. Tipo de objetos na área d. Tamanhos mínimo e máximo de objetos na área e. Probabilidade mínima de objetos na área f. Tipo de alerta de gatilho usado g. Intervalo de tempo de geração de alerta Modulo de detecção e mensuração de objetos Objetos Detectáveis O SOFTWARE deverá possuir a funcionalidade de carregamento de bibliotecas de detecção de objetos, onde cada biblioteca possua uma lista de objetos a serem detectados. O SOFTWARE deve possuir no mínimo quatro bibliotecas principais com os seguintes objetos disponíveis: Biblioteca Geral: pessoa, bicicleta, carro, moto, ônibus, comboio, caminhão, semáforo, hidrante, sinal de parada; Biblioteca de Crime: Capacete de moto, boné, arma pequena, arma longa, mãos ao alto, celular; Biblioteca de prevenção de incêndio: fogo e fumaça (com configuração de sensibilidade). Regras de Alarmes O SOFTWARE deverá possuir no mínimo as seguintes condições para o disparo de eventos: Objeto alvo dentro da área configurada por tempo igual ou superior ao configurado; Quantidade de objetos configurados dentro de determinada área inferior, igual ou superior a quantidade configurada; Objeto alvo parado dentro de determinada área por tempo igual ou superior ao configurado; Objeto alvo em movimento dentro de determinada área por tempo igual ou superior ao configurado; Objeto alvo não presente em determinada área; Avanço de objeto alvo em direções proibidas, configuradas através de linhas virtuais; Avanço de objeto alvo em direções proibidas, configuradas através de áreas virtuais, com análise do rastro dos objetos e quantificações da quantidade de ângulos na direção desejada; Proximidade entre objetos menor ou igual a quantidade de PIXELS configurada; Proximidade entre objetos maior ou igual a quantidade de PIXELS configurada; Proximidade entre objetos menor ou igual a quantidade de PIXELS configurada, em angulação predeterminada; Proximidade entre objetos igual a quantidade de PIXELS configurada, em angulação predeterminada; Presença de determinado objeto dentro da área de um objeto alvo; Ausência de determinado objeto dentro da área de um objeto alvo; Objeto com a incidência de cor predeterminada em porcentagem igual ou superior à configurada; Objeto sem a incidência de cor predeterminada em porcentagem igual ou superior à configurada; Falha de conexão entre o SOFTWARE e a câmera; Simplificação do cenário atual, como por exemplo falta de iluminação, pichação na lente da câmera, cena desfocada, etc...; Deteção de gesto “mãos ao alto” do objeto pessoa. • O SOFTWARE deverá possuir no mínimo as seguintes configurações para as zonas de detecções:

		Zonas de alarmes em forma de cascata de eventos, como por exemplo, disparo da zona de alarme da câmera A ser condicionado ao disparo anterior em X segundos em relação ao disparo da zona de alarme da câmera B; Zonas de exclusões de detecções; Zonas de Heatmap com exibição em tempo real da porcentagem de movimento por zona; O SOFTWARE deverá possuir no mínimo as seguintes configurações de rastreamento: Personalização da distância euclidiana mínima entre objetos por frames; Tempo de rearme para contabilização de objeto reincidente determinada linha; Tempo de busca de objetos que tenham sofrido possível oclusão. O SOFTWARE deverá permitir as seguintes configurações adicionais: Agendamento das detecções; Geração de heatmaps com armazenamento das imagens em intervalo de tempo configurável para visualização do quadro evolutivo; Tempo de busca de objetos que tenham sofrido possível oclusão.
2.3	Licença de Software de Análise Forense	2.3 LICENÇA DE SOFTWARE DE ANÁLISE FORENSE Software com capacidade de análise forense, com as seguintes características mínimas obrigatórias: • O software ofertado deverá, após gerado o resumo do vídeo, permitir ao usuário: • O software ofertado deve ser capaz de reduzir o tempo de visualização de um determinado vídeo para fins de análise forense (investigativa) – a redução pretendida é de horas para minutos de vídeo. Essa redução de tempo deverá se dar através da criação de um "resumo" do vídeo, que permita a visualização, pelo operador, de vários eventos ocorridos em momentos diferentes sendo mostrados simultaneamente. • Através deste processo de criação do resumo do vídeo, o software ofertado deverá detectar e capturar no vídeo original qualquer imagem em movimento com, pelo menos, 10 (dez) pixels de tamanho, independentemente de sua cor ou formato - cada imagem em movimento capturada deverá ser indexada e chamada de "evento" para fins desse termo de referência; • O software ofertado deverá ser capaz de indexar as imagens capturadas adicionando, às mesmas, uma marcação com pelo menos hora e minuto (no formato hh:mm) do acontecimento de cada um dos eventos, de forma tal que o usuário veja, em tempo real e durante a visualização do resumo, o momento exato do acontecimento de cada evento; • Para elaboração do "resumo" do vídeo, permitir-se-á que o software requeira um tempo de processamento prévio, não sendo exigido que o supracitado resumo seja "montado" em tempo real e durante a análise; • O software ofertado não poderá, de nenhuma forma, alterar e/ou editar o vídeo original para executar qualquer das funcionalidades exigidas nesse termo de referência - o resumo criado deverá existir independentemente do vídeo original. O vídeo original deve manter-se inalterado para que não se perca sua eficiência jurídica; • O software ofertado deverá aceitar arquivos de vídeo; • O software ofertado deverá ser capaz de exportar qualquer trecho do vídeo original, escolhido aleatoriamente pelo usuário, pelo menos no formato de arquivo AVI com a possibilidade de, na hora da exportação, incluir hora e minuto do evento referente ao trecho exportado, bem como a sua marcação (bounding box); • O software ofertado deverá ser capaz de exportar imagens congeladas retiradas do vídeo original, escolhidas aleatoriamente pelo usuário, pelo menos no formato de arquivo nativo e JPEG, com a possibilidade de, na hora da exportação, incluir hora e minuto dos eventos exibidos, bem como a marcação (bounding box) destes. Funcionalidades mínimas • Filtrar o resumo do vídeo durante sua execução, com resultado imediato e sem que seja necessário reindexar o vídeo original, com no mínimo os seguintes filtros: • COR: o usuário deve poder escolher uma ou mais cores básicas simultaneamente e, a partir do momento da escolha, o software deve apenas mostrar, em seu resumo, as imagens em movimento (eventos) que contenham traço(s) da(s) cor(es) escolhida(s); • TAMANHO: o usuário deve poder escolher numa escala comparativa se deseja ver objetos maiores ou menores e, a partir do momento da escolha, o software deve apenas mostrar, em seu resumo, as imagens em movimento(eventos) que possuam o tamanho relativo à escolha; • DIREÇÃO: o usuário deve poder escolher numa angulação de 360 graus, com intervalos de 01 (um) grau, qual a direção dos objetos em movimento que ele deseja observar - a partir desse momento, o software deve apenas mostrar, em seu resumo, as imagens em movimento (eventos) que possuam a direção relativa à escolha; • VELOCIDADE: o usuário deve poder escolher numa escala comparativa se deseja ver objetos mais rápidos ou mais lentos e, a partir do momento da escolha, o software deve apenas mostrar, em seu resumo, as imagens em movimento (eventos) que possuam a velocidade relativa à escolha; • SIMILARIDADE: o usuário deve poder escolher durante a visualização do resumo, um objeto ou pessoa em movimento e requisitar que outros objetos similares sejam mostrados- o software então deve apenas mostrar outros objetos ou pessoas em movimento (eventos) que possuam as características de formato, tamanho e velocidade do evento escolhido; • PARADA: o usuário deve poder reaquerer que o software mostre apenas objetos que estavam em movimento (eventos), pararam por um período de pelo menos10 a 60 segundos (período esse que deve poder ser escolhido pelo usuário), e voltaram a se movimentar; • TRAÇADO: o software deve permitir ao usuário desenhar um traçado (rota, caminho) com o uso do mouse e através de ferramenta do próprio software, e, a partir desse traçado, o software passe a mostrar apenas os objetos/pessoas em movimento (eventos) que percorreram aquele traçado específico (ou parte dele); • O software deverá permitir ao operador escolher se deseja ver os eventos no resumo de forma automática ou se deseja que os mesmos sejam mostrados em ordem de acontecimento (cronológica); • Em todos os casos acima, os eventos mostrados deverão conter a marcação do horário da sua ocorrência (no formato hh:mm); • Em todos os casos acima, o resultado da escolha dos filtros deve ser mostrado imediatamente, sem a necessidade de reprocessamento do vídeo original a cada filtro requisitado;

		• Durante a visualização do resumo, o usuário deverá poder, a qualquer momento e clicando sobre a imagem desejada, ver o trecho do vídeo original relativo ao ponto escolhido no resumo. O software deverá ser capaz de mostrar resumo e vídeo original lado a lado, permitindo ao usuário comparar eventos em todos os seus detalhes; • Durante a visualização do resumo, o usuário deverá poder, a qualquer momento, habilitar ou desabilitar a visualização da marcação dos eventos com a hora e minuto; • Durante a visualização do resumo, o usuário deverá poder, a qualquer momento, habilitar ou desabilitar a visualização da marcação dos eventos com "bounding boxes" (marcadores) que envolvam o objeto em movimento, permitindo assim chamar a atenção do operador para TODOS os eventos existentes no resumo; • Durante a visualização do resumo, o usuário deverá poder, a qualquer momento, alterar a densidade (quantidade) de eventos na tela, permitindo visualizar melhor eventos isolados num resumo com muitos eventos simultâneos; • Durante a visualização do resumo ou do vídeo original, o usuário deverá poder, a qualquer momento, alterar a velocidade reprodução do vídeo em pelo menos 4x, 2x, 0,5x e 0,25x; • Durante a visualização do resumo, o usuário deverá poder, a qualquer momento e clicando sobre a imagem desejada, selecionar áreas de interesse do vídeo para inclusão ou exclusão: • Na área de INCLUSÃO, o software deverá ressaltar eventos que passem por aquela área em algum momento; • Na área de EXCLUSÃO, o software deverá mostrar eventos que não passem por aquela área em momento algum; • A solução deve ser escalável em termos de SERVIDORES, CLIENTES e BANCO DE DADOS, estando apta a receber incrementos futuros sem que haja alteração na sua estrutura existente; • A solução deverá permitir criar grupos de investigação e poder associar os resumos a estes grupos; • A solução ofertada deve permitir o gerenciamento das permissões de acesso a membros do grupo de investigação; • A solução deverá permitir compartilhar os resumos com um ou mais usuários ou grupo (s) de investigação; • Os vídeos originais terão de ser processados pelo servidor e este irá gerar um resumo deste vídeo. Todos os vídeos, originais e resumos terão de ficar armazenados no servidor, sendo que os vídeos originais não podem sofrer nenhum tipo de alteração; • Deverá estar completamente integrado ao software de monitoramento ofertado neste certame.
2.4	Licença de Software Reconhecimento Facial	2.4 LICENÇA DE SOFTWARE RECONHECIMENTO FACIAL Geral: Software de sistema de reconhecimento facial, devera identificar corpos, carros e placas veiculares baseado em inteligência artificial com analíticos que funcione baseado em CPU e GPU, permitindo ainda trabalhar com múltiplas placas aceleradoras no mesmo servidor ou em múltiplos servidores com arquitetura escalável. • Detecção sem máscara com 50 pixels de largura no rosto para stream de vídeo • Deve fazer as detecções e reconhecimento com máscara, com pelo menos 80 pixels de largura no rosto para stream de vídeo Realizar carga de fotos (formatos, jpg, png) no sistema a partir de 60 pixels entre pupilas. • Necessário conseguir fazer o reconhecimento de qualquer tipo de tom de pele. Com a pessoa de lado 30 graus, com a pessoa com parte do rosto coberto também. • Deve conseguir também detectar silhuetas para fazer contagem de silhuetas e de faces criando a contagem uma única câmera ou múltiplas câmera dentro do mesmo contador. • Ser capaz de definir uma região de interesse para o contador de faces e/ou silhuetas e se necessário desenhar poligonalmente a área de interesse. • Na mesma cena, o sistema deve ser capaz de detectar/ reconhecer no mínimo 40 faces com as mínimas condições de tamanho por face. • O fabricante deve ter histórico de implementação de um projeto com ao menos 100.000 licenças de reconhecimento facial. • Deve conseguir reconhecer corpos e fazer filtragens baseada em cor da roupa na parte superior e/ou inferior • Deve ser capaz de detectar carros, realizar filtragens por tipo de carroceria, fabricante, modelo, cor e placa • A interface gráfica do sistema deve suportar o idioma português • Ser capaz de aumentar e diminuir o “full frame” do evento selecionado com zoom através do mouse • Dispor de recurso que faça círculo de contato com pessoas marcadas como potenciais infratores, em três níveis. • Necessário possuir o recurso de vivacidade (certificar-se de que é uma pessoa viva – “liveness”) para uso com stream proveniente de câmeras de CFTV • Dispor de conversor TCP/IP Wiegand para integração com sistemas de controle de acesso. O conversor recebe do sistema de reconhecimento facial o “facility code” e número do cartão da pessoa identificada, enviando essa informação através do protocolo Wiegand ao sistema de controle de acesso, para validação do acesso (ou não) da mesma. • Dispor da capacidade de integração com sistema de controle de acesso, em nível de software via API. • Possuir o recurso para postar apenas a melhor detecção, implica selecionar dentro de um conjunto de frames que formam a detecção (período de acompanhamento de uma pessoa em frente a câmera que está ativo, ou seja, enquanto a face estiver sendo detectada pelo sistema em frente a câmera sem interrupção), o melhor frame em questão de qualidade para reconhecimento e descartar os demais. • Possuir a capacidade de permitir de-duplicação de detecções e reconhecimentos de uma mesma pessoa que passe em mais de uma câmera (configurada dentro de um mesmo grupo de câmeras) para gravação de eventos únicos dentro de intervalo de tempo pré-definido, mantendo apenas o evento de melhor qualidade. • Possuir o recurso para postar múltiplas capturas durante uma detecção, implica postar todas as detecções possíveis dos frames que formam a detecção (período de acompanhamento de uma pessoa em frente a câmera que está ativo, ou seja, enquanto a face estiver sendo detectada pelo sistema em frente a câmera sem interrupção). • Possuir recurso de verificação capaz de comparar faces, corpos e carros. • Possuir recurso de agrupamento de eventos por similaridade de vetores: • sistema deve conseguir catalogar de forma única, cada indivíduo que se apresente em frente às câmeras do sistema; • À medida que o mesmo individuo apareça no vídeo das diferentes câmeras e em diferentes momentos, todos eventos devem ser agrupados dentro do mesmo catálogo do indivíduo criado inicialmente. Arquitetura: • Necessário trabalhar com arquitetura centralizada, distribuída ou híbrida.

		• Arquitetura local: Todo processamento é realizado localmente, desde a decodificação dos streams, detecção das faces e vetorizações faciais. A base de dados fica em cada servidor sendo gerenciada de forma independente. • Arquitetura centralizada: sendo todos os streams chegando a um servidor central e processados neste ambiente, onde estarão base de dados, aplicação e decodificação. • Arquitetura distribuída: podendo ter parte da aplicação na borda (decodificação de vídeo), enviando apenas as detecções com as imagens já normalizadas para um servidor de aplicação central (aplicação) e servidor de armazenamento central (base de dados). • Arquitetura híbrida: com um servidor centralizado de base de dados gerenciando as bases de dados nos servidores de borda (Servidores com base de dados, aplicação e decodificação). A interface gráfica do sistema deve ser baseada em web (“web client”), funcionando nos principais navegadores de mercado, sem requerer a instalação de nenhum programa adicional, e client servidor. • O software do sistema deverá suportar o sistema operacional Linux • O sistema deverá ter a capacidade de operar com uma base da dados de no mínimo 100 milhões de pessoas de interesse • Precisa suportar streaming de vídeos nos padrões HTTP e RTSP compressão H.264, MPEG em 25 fps e resolução 1080p com bit rate mínimo de 4Mb/s. • Deve possuir comprovadamente, capacidade técnica de integração com os principais fabricantes de câmeras do mercado, tais como intelbras, hikvision, pelco, dahua, axis. Atravéz de uma declaração formal, fornecida pelo desenvolvedor do software. Gerenciamento: • Deve permitir criar diferentes grupos de câmeras • Deve permitir criar diferentes listas de interesse (associada a cada câmera ou grupo de câmeras) • Deve permitir criar listas de interesse para desabilitar a criação de eventos de pessoas especificas • Deve permitir criar diferentes perfis de acesso/níveis de segurança, com pelo menos 3 níveis com a possibilidade de particularizar o que cada nível terá acesso • Deve possuir registro de interações dos usuários com o sistema para fins de auditória, com a possibilidade de pesquisa pela mesma interface gráfica ou API. • Deve ter funcionalidade de “video wall” permitindo criar mosaico de visualização com as diferentes câmeras configuradas no sistema, permitindo ainda a exibição do mosaico e das detecções na mesma tela Permitir o carregamento (“upload”) de grupos de fotos (formatos jpg, png) de pessoas em lote ou individualmente para dentro das listas de interesse, podendo associar a 1 (uma) ou mais listas. • Deve possuir recurso de “Iniciador”, onde seja possível escolher quais funcionalidades serão exibidas no menu de acesso rápido • Permitir armazenar de forma agregada as informações de uma mesma pessoa de interesse, em um único registro, sua face, corpo, carro e placa do veículo. • Dispor de ferramenta de software permitindo o gerenciamento da distribuição da base de dados das pessoas de interesse a partir de um servidor central em configuração mestre-escravo, com os servidores que tem base de dados autônomas instalados em cada site, tendo a opção de definição de horário de sincronização entre os servidores ou que as bases de dados possam ser gerenciadas entre servidores de forma individual 1:1 ou em grupo 1:N. • Deve ter a funcionalidade de alertar sobre a tentativa de cadastro de pessoa de interesse duplicado, caso a pessoa que esteja sendo inserida já exista na base de dados Ter a possibilidade de fazer filtragem simultânea dos seguintes fatores: por pessoa específica, de pessoas com e sem máscara, com e sem barba, com e sem óculos de grau, com e sem óculos de sol, por emoções, por câmera, por grupo de câmeras, por lista de interesse, por dia do evento. • Possuir recurso de extração de relatórios a partir de filtros de pesquisas aplicados a faces, como: • Por pessoa de interesse; • Por Lista de interesse; • Por detecções ou reconhecimentos; • Por eventos reconhecidos pelo operador; • Por grupo de câmeras; • Por Câmera; • Por intervalo de tempo (data); • Por ID de evento; • Por idade ou intervalo de idade; • Por atributos faciais: • Barba; • Emoções (Nervoso, Nojo, Feliz, Triste, Medo, Surpreso, Neutro); • Por gênero (homem, mulher); • Por óculos (De grau, de sol); • Por vivacidade (liveness); • Por máscara facial (utilizando, não utilizando ou com uso impróprio); • Por seleção de múltiplos filtros citados acima. • Possuir recurso de extração de relatórios a partir de filtros de pesquisas aplicados a Corpos, como: • Cor da parte superior da roupa • Cor da parte inferior da roupa • Possuir recurso de extração de relatórios a partir de filtros de pesquisas aplicados a Carros, como: • Tipo de carroceria (Convertible, Coupe, Crossover, Limousine, Minivan, Pickup, Sedan, Shooting brake, Suv, Van) • Cor do carro • Placa • Fabricante • Modelo • Permitir ajustes finos separados para cada um dos analíticos (face, corpo e carro)

		• Permitir ajustar a orientação do vídeo da câmera com um clique Recursos para Proteção de Dados: • Necessário compatibilidade com a LGPD (Lei Geral de Proteção de Dados) dispondo pelo menos das seguintes funcionalidades: • Deve possuir a opção de borrar rostos de pessoas que por circunstância compõe a imagem no ato do reconhecimento, mas que são alheias a pessoa de interesse cadastrada; • Deve possuir a opção de salvar detecções apenas das pessoas que estão cadastradas na base quando detectadas. • SEGURANÇA: Deve possuir recurso de monitoramento de sessão por re-autenticação do operador Analíticos: • Necessário trabalhar com vídeos de câmeras que não estão integradas à plataforma de reconhecimento facial (vídeo “ofline”) e que estejam nos formatos de vídeo MP4, FLV, codec de vídeo H.264, sendo assim possível realizar buscas forenses, como por exemplo, vídeos oriundos de VMS, telefones celulares ou câmeras corporais (“body cam”). • Ter analíticos, que identificam gênero, uso de barba, uso de óculos de grau ou de sol. • Ter analíticos, que identificam cor da parte superior e inferior da roupa em um corpo • Ter analíticos, que identificam tipo de carroceira, fabricante, modelo, cor e placa de um carro • Ter analíticos que identificam fluxo de pessoas informando número de visitantes, quantos visitantes novos e quantos visitantes recorrentes, idade média dos visitantes e gênero deles, para um determinado período. • Ter os analíticos que identificam as seguintes emoções: bravo, medo, nojo, alegria, surpresa, tristeza e neutro. Integração: • Disponibilizar API (“application programming interface”) aberta para integração com outros sistemas, sendo possuído diferentes métodos para chamada nos eventos de faces, corpos e carros • Possuir recurso de disparo de “Webhooks” para eventos relacionados a faces, corpos, carros e contadores • Dispositivo Móvel Celular (“smart phone”): • Aplicativo telefones celulares com sistema operacional Android dispondo dos seguintes recursos: • Recebimento de detecções em tempo real, face e “full frame”; • Recebimentos de alertas sobre Pessoas de Interesse reconhecidas, nome, nível de similaridade, câmera, hora do evento, face reconhecida, full frame e foto de cadastro Cadastramento de Pessoas de interesse no servidor central via mobile, por foto (formatos jpg, png) armazenada ou utilizando a câmera em tempo real. • Visualização da base de dados de pessoas de interesse Recurso de pesquisa por face, corpo ou carro na base de dados de pessoas de interesse ou em todos os eventos com carregamento de foto (formatos jpg, png) de comparação via arquivo ou câmera. Plataforma integrada de gestão, tratamento e apoio a tomada de decisão Solução integrada de Governança para a centralização e visualização de dados provenientes de diferentes fontes de dados, individuais ou combinados, oferecendo indicadores e métricas para tomada de decisão. Plataforma web integrada que permita a visualização de painéis e relatórios diretamente em navegador web, sem a necessidade de instalação de software ou plug-in nas máquinas dos usuários. • O software deverá atender os seguintes requisitos mínimos: • Permitir a possibilidade de se realizar leitura e integrações de fontes de dados heterogêneas sem a necessidade de hardware ou software adicional; • Possuir as funcionalidades para exportação de relatórios e painéis, integradas na mesma plataforma, com interface única; • Permitir que os dados coletados sejam visualizados sob a forma de painéis gráficos, com possibilidade interativa e associativa entre os objetos, permitindo filtros e detalhamentos; • Permitir filtrar ou disponibilizar dinamicamente pesquisa por tabela de tempo (dias, semanas, meses, trimestres, semestres e anos); • Permitir, durante a criação de novas análises, combinar colunas de um ou mais bancos de dados, através de operações como união e intersecção; • Permitir que sejam realizados detalhamentos cruzados onde a partir de um painel de indicador, o usuário seja direcionado para outro painel ou relatório contextualizado com as informações referentes ao detalhamento; • Permitir a aplicação de filtros, agrupando e classificando dados, comparando períodos, definindo metas e alertas; • Permitir conexão a uma variedade de fontes de dados, como planilhas, bancos de dados, aplicativos. API’s e serviços em nuvem; • Permitir a criação de elementos visuais para monitorar e analisar dados em tempo real; • Permitir painéis incorporáveis em sites ou intranets externos; • Permitir painéis incorporáveis de sites externos; • Permitir aos usuários coletar, organizar, visualizar e analisar dados de várias fontes em um só lugar; • Permitir o compartilhamento das visualizações através de URL’S internas; • Permitir a exportação de gráficos e relatórios; • Permitir a exportação para download em PDFs, relatório de e-mail agendados e links publicados; • Permitir o acesso de usuários à plataforma, por definição de nível de acesso de usuário, com ou sem autenticação (sem autenticação através de certificado); • Possuir plataforma web integrada que permita a visualização de painéis e relatórios diretamente em navegador web, sem a necessidade de instalação de software ou plug-in nas máquinas dos usuários; • Permitir a integração com soluções de georreferenciamento, tais como Google Maps, OpenStreetMaps ou outra API de mapas existentes no mercado; • Permitir detalhamento das informações georreferenciadas através de cliques de mouse sobre uma determinada área que pode representar, uma cidade, estado ou país; • Permitir o desenvolvimento e a visualização de painéis de métricas, utilizando uma ou mais fontes de dados, trazendo funções estatísticas, como soma, média, contagem, máximo, mínimo, entre outras; • Permitir agendamento para envio automático por e-mail de objetos disponíveis na plataforma nos formatos PDF e imagem;
		• Permitir a atualização dos dados dos painéis em tempo real e ou em tempos de consulta parametrizados de acordo com as definições estabelecidas na etapa de análise de requisitos ou conforme disponibilidade da fonte de dados; • A solução de governança deverá ser construída a partir da leitura das bases de dados, com relações explícitas entre diversas bases, diversas tabelas e entre os conteúdos de uma mesma tabela. • Será de responsabilidade da contratante, a liberação de acesso à bases de dados de sistemas extras, NÃO fornecidos pela contratada, mediante assinatura de termo de responsabilidade e confidencialidade.

2.5	Serviços de Locação de Link de Dados - Tipo I	2.5 SERVIÇO DE LOCAÇÃO DE LINK DE DADOS – TIPO I O link de dados é responsável pela transmissão das imagens captadas pelo ponto de coleta de imagem até a sala de comando e controle. Para atender as necessidades deve-se respeitar os seguintes requisitos: O link deve ser construído em fibra óptica ou radiofrequência; Deve prover a interligação dos pontos de coleta de imagem até a sala de comando e controle; Deve possuir capacidade mínima de 10Mbps no ponto de coleta de imagem; Deverá garantir por meio de canais seguros para transmissão de dados e imagens, compostos por um canal óptico e/ou um enlace de rádio em frequência reservada à segurança pública de acordo com as disposições emanadas da Agência Nacional de Telecomunicações - ANATEL.
3	**KIT 3- Pontos Videomonitoramento Câmera Speeddome**	
3.1	Ponto de Videomonitoramento -Câmeras Speeddome Tipo II	3.1 PONTO DE VIDEOMONITORAMENTO - CÂMERA SPEEDDOME 3.1.1 CÂMERA SPEEDDOME Câmera IP do tipo PTZ, com funções de análise e reconhecimento facial embarcadas, com as seguintes características: • Deverá ser instalada uma câmera por ponto de monitoramento; • Sensor do tipo CMOS com varredura progressiva de tamanho 1/1.8 polegadas ou superior; • Resolução de 2 Megapixels; • Resolução máxima de 1920 x 1080 pixels; • Velocidade de shutter ente 1s e 1/30.000s ou superior; • Deve possuir iluminação mínima em modo colorido de 0,001 Lux@F1.4, em modo Preto e Branco de 0,0001 Lux Lux@F1.4 e, com o IR ligado, em 0 Lux Lux@F1.4; • Distância de Infravermelho de até 500m; • Distância focal entre 5,6 e 223mm ou superior; • Zoom ótico de 40x e digital de 16x; • Controle manual e automático de foco; • Distância de detecção de até 2.340 m; • Distância de reconhecimento de até 460 m; • Distância de identificação de até 230 m; • Foco motorizado e manual; • Pan de 0 a 360 graus sem fim e tilt de -30 até 90 graus com auto flip de 180º; • Velocidade em modo manual para Pan de 0,1 até 240°/s e para Tilt de 0,1 até 100°/s; • Velocidade de preset para Pan de no mínimo, 240°/s e para Tilt de 120°/s; • Modo PTZ com 5 padrões e 8 patrulhas e panoramização automática; • Recuperação de contexto, ou seja, a câmera deve restaurar automaticamente o PTZ anterior e o status da lente após falha de energia; • Mecanismos de proteção de perímetro: Suporta o acionamento de alarmes por tipos de alvos (humanos e veículo) filtrando falsos alarmes causados por animais, farfalhar de folhas, luzes brilhantes, etc.; • Suporte a análises de vídeo: detecção de movimento, violação de vídeo, mudança de cena, desconexão de rede, conflito de endereço IP, acesso ilegal, anomalia de armazenamento, objeto perdido/abandonado; • Deve possuir mecanismo interno de reconhecimento facial com suporte ao armazenamento de até 10.000 faces; • Suporte as seguintes codificações de vídeo: H.265+, H.265, H.264+, H.264, MJPEG (Sub Stream); • Suporte a 3 fluxos de vídeo; • Modos de bitrate CBR e VBR; • Possuir filtro de corte infravermelho; • Possuir tecnologias de melhoramento de imagem BLC, HLC e WDR com ganho de 120dB ou superior; • Possuir tecnologia de redução de ruído Ultra DNR (2D/3D); • Suporte as funções: Região de Interesse, Estabilização eletrônica de imagem e antinevoeiro (defog); • Suporte para, no mínimo, 24 máscaras de privacidade; • Suporte a compressão de áudio G.711a, G.711mu, PCM, G.726, AAC, G722.1, G.729, MPEG2-Layer2; • Deve possuir interface Fast Ethernet com suporte ao padrão IEEE 802.1x • Deve possuir suporte aos protocolos de rede IPv4/IPv6, HTTP, HTTPS, SSL, TCP/IP, UDP, UPnP, ICMP, IGMP, SNMPv1/v2c/v3(MIB-2), ARP, RTCP, RTSP, RTP, SMTP, NTP, DHCP, DNS, PPPOE, DDNS, FTP, IP Filter, QoS, Bonjour; Deve permitir acesso para até 20 usuários; • Deve permitir métodos de transmissão Multicast e Unicast; • Deve possuir certificações CE: EN55032/EN55024/EN50130-4 e FCC: Part15 subpartB, ANSI C63.4-2014; • Possuir 1 entrada e 1 saída de áudio; • Alimentação 24VAC e Hi-PoE com consumo máximo de 26W; • Operar entre as temperaturas de -40°C e +70°C e humidade relativa do ar abaixo de 95%; • Deve possuir resistência a líquidos e sólidos IP67; • A câmera deverá possuir, incorporada à sua estrutura, mecanismo luminoso de identificação visual a cores, visíveis inclusive durante o dia, para identificação de condições de segurança de local, operando no modo de exceção de “listas brancas”, com base em análise inteligente de vídeo, detectando automaticamente situações de risco e informando visualmente, pela equivalência de cores, a situação detectada.

		3.1.2 SUPORTE PARA CÂMERA SPEED DOME Suporte para instalação de câmeras externas, em paredes ou poste, que permita adaptar o equipamento a diversos cenários de aplicação, com as seguintes características: • Deve possuir comprimento de 1500 mm, parede ≥ 1,5 mm; • Deve possuir suporte para encaixe/fixação da câmera; • Deve possuir suporte para fixação ao poste; • Deve possuir zincagem à fogo; • Possuir pintura eletrostática; • Deve possuir capacidade de carga mínima de 10 kg. 3.1.3 FONTE DE ALIMENTAÇÃO Fonte de alimentação tipo colmeia, com as seguintes características: • Deve possuir alimentação bivolt 110/220VAC, selecionável por chave; • Deve possuir saída de 24VAC; • Deve possuir corrente mínima de 3A; • Deve possuir potência mínima de 50W; • Deve possuir filtros contra interferência na imagem e proteção contra curto-circuito na saída. 3.1.4 NOBREAK 2000 Equipamento de rede tipo nobreak, senoidal, com as seguintes características mínimas: • Deve apresentar uma potência nominal em regime contínuo de no mínimo 2kVA; • Tensão nominal de entrada ajustável entre 120 e 220V; • Frequência nominal de operação de 60 Hz; • Tensão nominal de saída de 115V; • Deve possuir forma de onda de saída senoidal; • Deve possuir baterias VRLA de manutenção; • Deve possuir função de estabilizador; • Deve possuir fator de potência de 0,7; • Deve possuir proteção contra sobrecarga e curto-circuito; • Deve possuir proteção contra sub e sobretensão; • Deve possuir proteção contra descarga profunda da bateria; • Deve permitir modulo de comunicação através de SNMP; • Deve possuir proteção por bateria baixa; • Deve possuir proteção de excesso de temperatura; • Deve operar entre temperatura de 0 ~45° C; 3.1.5 SWITCH 8 PORTAS Equipamento para extensão física dos pontos de rede, com as seguintes características: Características • Deve possuir 9 (nove) portas Gigabit Ethernet 10/100/1000Base-T Conforme Padrões IEEE 802.3, IEEE 802.3u, IEEE 802.3ab; • As interfaces deverão ser Full-Duplex, auto sensing com conectores RJ45 fêmea e implementar mecanismos de autoconfiguração em todas as portas, do tipo MDI/MDI-X; • Deve possuir adicionalmente no mínimo 1 (um) porta Gigabit Ethernet Padrão IEEE 802.3z, para inserção de transceivers do tipo SFP; • As interfaces dos itens 1. e 3. devem operar de modo simultâneo; • Deve possuir leds indicativos de funcionamento; • Deve implementar os padrões IEEE 802.3at e IEEE 802.3af, em pelo menos 8 (portas); • Deve ser capaz de fornecer até 30W por porta (não simultâneo); • Deve possuir o Budget PoE de no mínimo 63W; • Deve possuir capacidade de processamento de no mínimo 20 Gbps; • Deve possuir taxa de encaminhamento de pacotes igual ou superior a 14.88 Mbps; • Sua tabela de MAC Address deve suportar no mínimo 4.000 MAC address; • Deve suportar jumbo frame de no mínimo 16KB; • O equipamento deve possuir no máximo até 1 (uma) ventoinhas internas para resfriamento; • Deve suportar temperatura de operação entre 0° e 50°; • Deve suportar operação sob umidade entre 10% e 90% RH sem condensamento; • Deve compatível com PDs compatíveis com IEEE 802.3af/at; • Deve suportar controle de fluxo EEE802.3x; • Deve suportar 802.1p/DSCP QoS; • Deve suportar IGMP Snooping; • Possuir homologação da ANATEL, de acordo com a resolução número 242 de 30/11/2000; • Possuir Certificação FCC e CE; • Deve ser RoHS (Restriction of Certain Hazardous Substances) Compliance; 3.1.6 ENTRADA ELÉTRICA • Conjunto para a conexão à rede de energia elétrica da concessionária local dentro das normas exigidas para conexão dos dispositivos à rede elétrica, além das normas da ABNT e ANEEL; • Todos os materiais e miscelâneas necessários para a instalação do padrão indicado, devem estar contemplados na proposta da licitante. • O cabeamento elétrico deverá interligar a caixa de equipamentos com o ponto/circuito de energia compatível mais próximo, após comprovada a compatibilidade do circuito;

		3.1.7 POSTE DE CONCRETO Poste de concreto com as seguintes características: • Poste com estrutura circular fabricado em concreto armado; • Altura total de 9 metros; • Resistência nominal de 200 DaN; • Deverá atender todas as normas técnicas ABNT pertinentes; • Não será permitido perfurar o poste sem aprovação do fabricante; • Toda fixação de produtos e equipamentos no corpo do poste deverá ser feita através de abraçadeiras em aço galvanizado com parafusos ou outro mecanismo de fixação. 3.1.8 CAIXA PORTA EQUIPAMENTOS Caixa metálica externa, tipo porta-equipamentos, com as seguintes características: • Deve ser fabricada em chapa de aço carbono SAE 1010/ 1100, com espessura mínima de 1,5mm; • Deve possuir dimensões externas de: (H) 600 mm, (L) 525 mm e (P) 600 mm, com tolerância de 2% nas medidas; • Deve possuir Kit de ventilação com dois ventiladores para teto; • Deve possuir abertura para ventilação forçada; • Possuir no mínimo um ventilador, padrão universal; • Deve possuir porta frontal com fechadura e chave; • Deve possuir grau de proteção IP65; • Deve possuir duas prateleiras, no interior da caixa para instalação de equipamentos, placa de montagem fabricada em chapa de aço carbono com espessura 1,5 mm; • Deve ser pintada utilizando tratamento de superfície para proteção e pintura epóxi; • Índice de Proteção (IP) – Mínimo IP 65 (selada contra poeira e protegidas contra jatos de água); • Deve permitir capacidade de carga de no mínimo 100kg; • Deve estar de acordo com a norma de antivandalismo; • Deve possuir calha elétrica. 3.1.9 INFRAESTRUTURA • Todos os pontos deverão ser fornecidos com a infraestrutura, descrita abaixo: • Deverão ser personalizadas/detalhadas em plantas ou esquemas elétricos específicos, incluindo aterramento; • O cabeamento elétrico deverá interligar a caixa de equipamentos com o ponto/circuito de energia compatível; • O cabeamento deverá ser ligado dentro da caixa de equipamento ao disjuntor (em série com a fase) e ao varistor (em paralelo); • O dimensionamento do cabeamento deverá ser feito em função da distância e da carga, não podendo ser usada bitola de condutores com diâmetro menor que 2,5 mm^2; o cabeamento usado deverá ser do tipo PP, SINTENAX ou equivalente, com três condutores encapados, envolvidos por grossa camada de borracha, de modo que seja imune a água, umidade e intempéries; • A rede elétrica de alimentação dos equipamentos será monofásica, para alimentação em 127V (cento e vinte e sete Volts). A alimentação poderá ser em 220V (duzentos e vinte Volts); • Os pontos deverão ter conectores do tipo RJ45 fêmea, para categoria 5e, com espelhos e identificação. A rede deverá ser instalada e certificada. • Os custos e execução são de inteira responsabilidade da empresa Contratada; • Deverá ser fornecido pela empresa a ser contratada, os materiais de infraestrutura necessários para instalação: • Eletrodutos de PVC; • Luvas; • Abraçadeiras • Cintas de alumínio; • Mangueira de manobra; • Parafusos e buchas; • Cabos elétricos; • Cabo UTP.
3.2	Licença de Software de VMS	3.2 LICENÇA DE SOFTWARE DE VMS A plataforma de VMS, deve ter capacidade de trabalhar com múltiplos sites independentes através da consorciação dos mesmos e os gerenciar em um único site central (SSP/RS), garantindo o monitoramento e gestão dos dispositivos de forma unificada. Deverá ser contemplada a plataforma que interconecta sistemas remotos/menores ao site central sem limite no número de dispositivos conectados a um sistema central. Não possuir banco de dados proprietário local no cliente, devendo qualquer informação inerente ao sistema ser armazenada somente no banco de dados do servidor de gerenciamento com bancos de dados de mercado, como SQL Server. Toda a comunicação e troca de informações entre os servidores devem ter a possibilidade de serem realizadas de maneira encriptada e protegida. O sistema deve permitir independência de criptografias entre câmeras e servidores de gravação e os servidores do sistema com as estações de trabalho, permitindo segregação das redes criptografadas. Deve disponibilizar funções de servidor de gerenciamento com proteção de redundância (failover), isto é, quando o servidor gestão por algum motivo vier a ficar ofline, outro servidor deve assumir suas funções até que o principal retorne a exercer suas funções normalmente. Deve disponibilizar funções de servidores de gravação com proteção de redundância sem custo adicional de licença (failover), isto é, quando o servidor/servidores de gravação por algum motivo vier a ficar ofline, outro servidor deve assumir suas

		funções até que o principal retorne a exercer suas funções normalmente, e as imagens gravadas no servidor de backup devem ser transmitidas ao servidor principal preenchendo a lacuna do tempo ofline. O Sistema deve permitir a função de travamento de evidência, isto é, permitir que uma evidência em específico presente no sistema seja impedida de ser apagada independente do tempo de gravação do sistema, ou seja, não seja removida mesmo após atingir o tempo de retenção de imagens estipulada no projeto. O sistema deve suportar: Visão Geral • Solução de sistema de vídeo segurança deve ser integrado, multiusuário e multi-site. Deve suportar um número ilimitado de servidor de gravação e visualização de câmeras IP, codificadores de vídeo IP; • Gerenciamento otimizado de armazenamento de vídeo: A solução deve dispor de arquivamento único, gravação de longa duração de bom desempenho, escalabilidade e custo-eficiente; • Detecção automática de modelo de câmera: Deve suportar mais de 9000 modelos de câmeras IP, codificadores de vídeo IP, e mais de 150 fornecedores diferentes, utilizando métodos como a Universal Plug and Play, Broadcast, varredura manual e varredura por faixa de IP; • Número ilimitado de servidores de gravação: Deve suporta um número ilimitados de câmeras por servidor. Gravação continua ou ativada por movimento, evento ou agendamento; • Rede e armazenamento otimizados: Deve suportar multi-streaming que otimiza a banda usando novos métodos de compressão; MPEG4, H.264, H.265 além MJPEG e MPEG4; • O Multi-live Streaming possibilita definir múltiplos fluxos de vídeo ao vivo com diferentes configurações. Ele otimiza a performance de visualização do Cliente de Monitoramento de acordo com a disponibilidade de banda (throughput) e layouts de visualização; • Deve ser capaz de armazenar conteúdo em vídeo que não são críticos em diferentes topologias e arquitetura de armazenamento; • Deve suportar a detecção de movimento, independente do modelo da câmera; seja pelo servidor ou pela câmera; ou simultaneamente; • Plataforma Aberta: Deve fornecer API / SDK de forma gratuita e suportar integração com hardware ou aplicativos de terceiros. • Integração nativa de todos os dispositivos compatíveis com os fóruns de compatibilidade Onvif Profile S, Q e T e PSIA. • Instalação em Windows 64 bits; • Compatível com Instalações em ambiente virtualizado VMWare e Microsoft Hyper-V; • Deve permitir exibição do alerta gerado pelos dispositivos, através do processamento dos metadados recebido das câmeras / encoders, mostrando os quadros (overlay) nos formatos e cores gerados pelos dispositivos. Tudo isto deve ser permitido através do dispositivo integrado via ONVIF.0011000000 • Permitir integração com Solução de Vídeo Wall com número ilimitado de monitores; • Deve possibilitar total compatibilidade com, no mínimo, duas versões anteriores do sistema; O sistema deve conter os componentes a seguir: • Serviço de Administração • Gerenciamento centralizado: O software de administração deve oferecer um acesso único e consolidado para configuração dos servidores de gravação, mesmo em instalações multisites; • Assistentes de configuração: Guia o usuário através do processo de adição de câmeras, a configuração de vídeo e gravação, ajuste de detecção de movimento e configuração do usuário; • Detecção automática de dispositivos: permite a detecção rápida de dispositivos e câmeras usando métodos como a Universal Plug and Play, Broadcast e varredura por faixa de IP; • Opção de configuração em massa: Altera as configurações em vários dispositivos ao mesmo tempo com poucos cliques; independentemente de estarem no mesmo site ou em sites remotos; • Gerenciamento de senhas dos dispositivos diretamente na interface do software. O sistema deve permitir automação de troca periódica das senhas dos dispositivos. • Importação de dados de configuração off-line: Permite a edição off-line de dados de configuração, incluindo câmeras e as definições de dispositivos; • Sistema automático de pontos de restauração: um ponto de restauração é criado a cada vez que uma mudança de configuração é feita. Permite a reversão fácil de pontos de configuração previamente definidos e permite o cancelamento de mudanças de configuração indesejados e a restauração de configurações anteriores válidas; • Deve permitir a personalização da interface de administração de acordo com os direitos de cada usuário, concedendo permissões, restringindo funções e ocultando / desabilitando partes da interface para evitar o acesso indevido a ações restritas. • Ser nativamente compatível com Microsoft Active Directory para gestão de usuários e perfis de acesso do Windows e permitir autenticação de usuário única (SSO) • Permitir controle de acesso aos perfis de usuários: Visualização ao vivo, controle PTZ, presets PTZ, controle de saídas, Eventos, ouça o microfone, fale com a caixa de som remota, gravação manual; Reprodução, exportação AVI, exportação JPG, exportação de banco de dados, sequências, pesquisa inteligente e áudio. Bem como definir as vistas, editar vistas particulares e públicas. • Trabalhar com banco de dados centralizado de fabricantes reconhecidos de mercado como SQL Server, Oracle ou MySQL • Deve permitir acesso remoto para o software de visualização e aplicativo para visualização em web browsers ou software client com opção de conexão segura no acesso à câmera (HTTPS) • Ter servidor de Web embutido para download de softwares e plug-ins. • Ter histórico de provas exportadas por usuário e arquivo. • Ter histórico de atividade do usuário do cliente pelo tempo, localidade e câmeras. • Pode ser instalado em conjunto com o servidor de gravação. • Fornecer streams múltiplos de vídeo ao vivo para diferentes clientes. Serviço de Servidor Móvel O sistema deve suportar:

		• Acesso remoto para clientes móveis. • Realiza o login e solicitações de acesso entre clientes e o Servidor Master. • Redimensiona as imagens de vídeo vigilância para ajustar ao layout da tela dos dispositivos móveis. • Pode ser instalado em conjunto do servidor de gravação. • Deve permitir ser instalado em dispositivos com sistema operacional iOS, Android e Windows Phone • Deve permitir a transmissão de imagens geradas em tempo real pela câmera do dispositivo móvel para a central de monitoramento, e gravar estas imagens no sistema como se fosse um dispositivo fixo já instalado no sistema. • Deve permitir a Inclusão do geo-posicionamento através de meta dados de GPS advindos do dispositivo móvel no do app. • Deve permitir eventos/alarmes no dispositivo móvel em tempo real; Serviço de Gestão de Eventos e Alarmes • Deve ter um motor (engine) que forneça regras para a automação de diferentes aspectos do sistema, incluindo controle da câmera, comportamento do sistema e dispositivos externos, com base em eventos ou horários. • Deve fornecer uma caixa de diálogo de configuração no estilo Microsoft Outlook, na qual eventos predefinidos e personalizados são usados nas regras para acionar ações. • Teve ter as seguintes categorias de eventos: • Hardware: dispositivos de hardware físico conectados ao sistema. • Dispositivos: certas funções e estados de dispositivos disponíveis através de dispositivos de hardware conectados. • Externo: relacionado às integrações do VMS. • Servidor de gravação: funções de arquivamento e banco de dados. • Análise: a partir de aplicativos e sistemas de análise integrados. • Definido pelo usuário: Eventos configurados de forma personalizada, permitindo que os usuários disparem. Perfis de horário • Ter gerenciamento de evento / alarme de ponto único: gerenciamento central de todos os alarmes internos do sistema e alarmes externos de segurança. • Ter suporte à associação de alarmes a mapas. • Deve possuir um Gerenciador de Alarmes que permita: • Lista de alarmes com amplos recursos de classificação e filtragem. • Visualização instantânea de vídeo gravado de câmeras primárias e relacionadas, no momento do incidente. • Imagem em miniatura da câmera principal, no momento do incidente. • A opção de desativação de alarme deve permitir que os usuários suprimam alarmes de um determinado dispositivo por um período de tempo especificado. • Relatórios de tratamento de alarmes, fornecendo informações sobre a entrada e o desempenho do tratamento de alarmes. Serviço de Gravação e gerenciamento das gravações O sistema deve suportar: • Gravação digital simultânea de vários canais de vídeo e áudio. • Transmissão de áudio bidirecional do microfone do cliente para alto-falantes remotos. • A otimização da largura de banda devido ao multi-streaming, dividindo o fluxo de vídeo da câmera para fluxos diferenciados para ver vídeo ao vivo e gravado. • O software cliente pode solicitar a visualização ao vivo em uma taxa de quadros diferentes e em resolução mais baixa que as configurações de gravação. • Conectividade para as câmeras, codificadores de vídeo e DVRs suportando compressões como MJPEG, MPEG4, MPEG4 ASP, H.264 e MxPEG, H.265. • Detecta automaticamente os modelos de câmeras durante a instalação. • Número ilimitado de câmeras instaladas. • Tecnologia de gravação: banco de dados seguro de alta velocidade de imagens JPEG ou fluxos MPEG4 e H264 incluindo áudio. • Velocidade de gravação: Mais de 30 frames por segundo por câmera, limitado apenas pelo hardware e rede. • A qualidade da gravação depende inteiramente da câmera e do encoder: não há limitação de software. • Capacidade de gravação ilimitada, dependendo apenas da capacidade de storage. • Exportação de vídeo configurável por hora ou diária, com passagem automática opcional para unidade de rede de maior capacidade de armazenamento, com imagens disponíveis para reprodução de forma transparente para o operador. • Detecção de movimento embutida, em tempo real, com sensibilidade completamente ajustáveis e com zonas de exclusão. Permitindo ativar a gravação com velocidade de frames superior quando é detectado movimento ou quando surge um evento, notificando o alerta por e-mail. • Gravação manual com início do tempo baseada em critérios pré-definidos e privilégios de acesso. • Pan Tilt Zoom (PTZ) com presets armazenados pelo sistema, sendo em até 50 por câmera. • Ativação de presets e patterns quando acontecem determinados eventos. • Programação para ativação do pattern em períodos diferentes: isto é, diferente para dia e noite, semana, etc. • Varredura PTZ em dispositivos suportados: visualização ou gravação enquanto se move lentamente a partir de uma posição para outra. • Acione o limpador ou esguicho de água remotamente, nos modelos suportados de PTZ • Em eventos pré-definidos comandos são enviados automaticamente para exibir vídeo ao vivo em computadores remotos. • O servidor de gravação é executado como um serviço do Windows. • Gravação em multi estágios, permite configurar o sistema para gravar em locais, tempo e taxa de frames diferentes. Permitindo até a redução da taxa de frames automática para atender a demanda de tempo de configuração. • Recuperação configurável de trechos de vídeo perdidos diretamente da câmera que possui a função de gravação local (seja através de cartão de memória removível ou memória fixa embutida na câmera). • Deve suportar gravação embarcada na câmera (edge storage) em vários fabricantes e em dispositivos ONVIF nos perfis acima mencionados; • Serviços de conexão remota aos servidores de imagem. • Suportar sistemas servidores de gravação de 64 bits, em hardware e software.

		• Assinatura digital no banco de dados garantindo integridade do vídeo. • Monitoramento do sistema e do servidor de imagens com relatório das configurações. Redundância da gravação de vídeo • O sistema deve permitir que em caso de falha na gravação dos vídeos, outro assuma, sem a adição de licença para essa função; • A redundância poderá ser efetuada em um ou vários (N:N) storage exclusivos para essa função, ou pode ser feito nos mesmos gravadores do sistema. • Deve possibilitar mover dispositivos (câmeras ou grupo de câmeras) entre diferentes servidores de gravação; • Deve mover todos os dispositivos associados; • Deve dispensar reconfiguração de cFâmeras. • Observação: O serviço de gravação nos servidores de gravação não deve depender da instalação de um banco de dados local para garantir seu funcionamento. Software De Visualização De Gravação Operação O sistema deve suportar: • Visualização ao vivo e reprodução: Clients desde dispositivos móveis a computadores com suporte para visualizar até 100 câmeras de vários servidores ao mesmo tempo. • Exibições de Janelas/Layouts: Trabalha com exibições contendo no mínimo 8x8 câmeras, Hot spot, Matriz, Sequencial, imagens estáticas e ativas, vídeos ao vivo ou gravados, mapas HTML, distribuídos em todos os monitores do computador. • PTZ inteligente: controle manual, presets, macros (vá à preset quando evento), patrulhamento com esquemas múltiplos (pattern), comandos para limpador (palheta) e esguicho de água, controle por joystick e teclado/mouse. • Matriz Virtual: exibições de controle de câmara ao vivo em computadores remotos para visualização distribuída. • Áudio multicanal bidirecional: Ouça áudio ao vivo/gravado com reprodução instantânea no PC cliente e transmita voz pelo microfone a alto-falantes remotos. • Permite gravação de áudio sincronizada a qualquer canal de vídeo. • Gravação manual: Baseado em privilégios de acesso definido pelo administrador, os usuários clientes podem manualmente iniciar a gravação de uma câmera por um tempo predefinido. • O software deve possuir um sistema de gerenciamento de usuários que exija permissão do administrador para criar, resetar ou alterar as de aceso de outros usuários. • Stream de visualização adaptativo, onde a resolução da câmera é alterada automaticamente quando o operador muda a visualização do modo mosaico para modo único em tela cheia. • Capacidade de enviar vídeos ao vivo e gravado para monitores de vídeo wall dentro da própria interface. Busca, backup e dados seguros O sistema deve suportar: • Processamento de gravação: Através da busca de movimento acima do vídeo gravado, PTZ digital com suavização de imagem opcional (apenas no software visualizador). • Backup de Evidência: JPEG, AVI, WAV e formatos de dados nativos com software visualizador stand-alone, criptografia de dados e registros, notas de usuários e impressão de relatórios. • Autenticação: contas de usuário do Microsoft Active Directory e nativos. • Autorização: contas de usuário e grupos do Microsoft Active Directory e perfis de usuário nativos (do sistema), todos os privilégios de acesso e controle de ações permitidas no nível da câmera. • Histórico: Todas as ações do usuário por tempo, localizações e câmeras, e toda a operação do sistema. • Alerta: Notifica os usuários em caso de detecção de movimento ou evento por som, e-mail ou SMS. • Reprodução de gravações de vídeo e áudio localmente no servidor de gravação. • Visualização de até 16 câmeras com tempo sincronizado durante a reprodução. • Pesquisa instantânea em gravações com base na data / hora e atividade. • Pesquisa inteligente unificada, através de detecção de movimento, marcadores(bookmarks), eventos e alarmes. • Pesquisa Forense por metadados: A pesquisa deve poder utilizar eventos de metadados gerados pelas câmeras como ferramenta de busca de imagens. • Linha de tempo de atividade com recurso de lupa; possibilitando ampliar ou reduzir a faixa de tempo necessária para dar início a busca por vídeos gravados; • Pesquisa instantânea em gravações com base na data / hora e atividade / alarme (Video Motion Detection). • Provas podem ser geradas com relatório impresso, imagem em JPEG, AVI ou no formato proprietário (com visualizador incluso), ou ainda pode exportar vídeo em formato MKV padrão. • Exportação de gravações de áudio em formato WAV ou AVI. • Exportação de vídeo digital com zoom para visualizar área de interesse, e para minimizar o tamanho do arquivo exportado. • Criptografia e opção de senha de proteção para as gravações e os arquivos exportados. • Capacidade de adicionar comentários às provas exportadas, também criptografadas. • Possuir interface proprietária, desenvolvida pelo mesmo fabricante e com mesmo código fonte do servidor de gerenciamento e gravação. • Não possuir banco de dados proprietário local no cliente, devendo qualquer informação inerente ao sistema ser armazenada somente no banco de dados do servidor de gerenciamento/ banco de dados SQL Server. • Opção para enviar imagens por e-mail. Aplicativo de visualização através do Web Browser O sistema deve suportar: • Visualização de vídeo ao vivo ou reprodução de gravações para 1 a 16 câmeras simultaneamente, advindos do mesmo ou diferentes servidores.

		• Exibições individuais podem ser definidas pelo usuário em vários layouts: exibição ou reprodução de imagens da câmera de vários servidores simultaneamente na mesma vista. • Vistas compartilhadas podem ser geridas centralmente, através do servidor com permissão de administrador. • Importação de mapas estáticos ou ativos para navegação rápida entre câmeras. • Controle do relé de saída de alarme. • Visão geral das sequências com movimento detectado e janela de visualização. • Visão geral de eventos / alertas. • Controle de câmeras PTZ remotamente, usando também posições pré-determinadas. • Controle remoto de PTZ por clique em ponto. • Controle remoto de zoom sinalando um retângulo. • Assumir controle manual sobre uma câmara PTZ que executa um esquema de patrulhamento; após um período de tempo sem atividade a câmera volta ao seu patrulhamento programado. • Criar arquivos AVI ou criar imagens JPEG geradas a partir de conteúdo gerado pelo software, seja estas imagens advindas de vídeo ou não; • Imprimir relatórios de incidentes com os comentários livres e pertinentes ao usuário. • Sistema de login usando nomes de usuário e senhas cadastrados no sistema proprietário ou delegado ao Microsoft Active Directory. Matriz de Vídeo O sistema deve suportar: • Matriz virtual mostrando o vídeo ao vivo diretamente de no mínimo 04 câmeras por cada tela individual a serem acionadas remotamente por comandos remotos e manuais; • Sequência de câmeras tipo FIFO (first-in-first-out) • Vários eventos podem controlar um monitor de matriz e eventos únicos pode controlar vários monitores. • Visualizar o vídeo na sua taxa máxima de frames em qualquer codec provido pela câmera. Cliente celular O sistema deve suportar: • Aplicativos gratuitos para dispositivos baseados em sistema operacional Android (Google), iOS (Apple). • Permitir a visualização de múltiplas imagens simultaneamente. • Busca e reprodução de vídeo gravado. • Toque na tela do dispositivo para zoom digital e diferentes modos de visualização da imagem. • Controle das funcionalidades PTZ das câmeras. • Salvar ou compartilhar uma foto do vídeo exibido ao vivo. • Permitir a utilização da câmera de vídeo do dispositivo móvel como um gerador de imagens para o sistema principal. Opções de Integração O sistema deve ser: • Compatível com software supervisório de alarmes e estado de dispositivos para grandes instalações.. • Ter SDK gratuito para integração do vídeo em outros produtos usando a API para exibir imagens ao vivo, reprodução de atividades gravadas, mostrar imagens de determinado período de tempo, e buscar por movimento. • Criar, importação e usar páginas HTML para a navegação entre os pontos de vista ou para ativar a matriz virtual no software de visualização. • Integrado nativamente com todos os dispositivos listados nos fóruns de compatibilidade Onvif, Profile S e PSIA. • Deverá integrar a Plataforma integrada de gestão, tratamento e apoio a tomada de decisão, unificando os dados e relatórios das soluções de reconhecimento facial e análise comportamental viária ofertados, na mesma plataforma. Devendo demostrar as funcionalidades deste item no momento da análise das amostras. Licenciamento Deve estar composto por: • Licença de Sistema; • Obrigatório para a instalação do produto; • A licença contempla um número ilimitado de servidores de gravação, softwares clientes, clientes web e aplicativos móveis; • Todos os softwares clientes não deverão ser licenciados e podem ser instalados e utilizados em qualquer número de computadores, de forma gratuita; • Acordo de Manutenção do Produto: Esta licença garante a aquisição e uso de forma gratuita de todas as atualizações dos produtos. Deverá ser adquirida para 3 anos. Expansão do Sistema • A expansão do sistema não deve ser atrelada a quantidade atual de servidores / câmeras; • O número de servidores de gravação deve permitir ser ampliado a qualquer momento, sem necessidade de licenciamento adicional, seja local ou remoto; • O número de câmeras pode ser ampliado independentemente da quantidade de servidores de gravação e/ou estações de operação do sistema; • O número de clientes de operação e de dispositivos móveis, poderá ser ampliado a qualquer momento sem necessidade de licenciamento adicional. Plataforma integrada de gestão, tratamento e apoio a tomada de decisão • Solução integrada de Governança para a centralização e visualização de dados provenientes de diferentes fontes de dados, individuais ou combinados, oferecendo indicadores e métricas para tomada de decisão. Plataforma web integrada que permita a visualização de painéis e relatórios diretamente em navegador web, sem a necessidade de instalação de software ou plug-in nas máquinas dos usuários. • O software deverá atender os seguintes requisitos mínimos: • Permitir a possibilidade de se realizar leitura e integrações de fontes de dados heterogêneas sem a necessidade de hardware ou software adicional; • Possuir as funcionalidades para exportação de relatórios e painéis, integradas na mesma plataforma, com interface única;

		• Permitir que os dados coletados sejam visualizados sob a forma de painéis gráficos, com possibilidade interativa e associativa entre os objetos, permitindo filtros e detalhamentos; • Permitir filtrar ou disponibilizar dinamicamente pesquisa por tabela de tempo (dias, semanas, meses, trimestres, semestres e anos); • Permitir, durante a criação de novas análises, combinar colunas de um ou mais bancos de dados, através de operações como união e intersecção; • Permitir que sejam realizados detalhamentos cruzados onde a partir de um painel de indicador, o usuário seja direcionado para outro painel ou relatório contextualizado com as informações referentes ao detalhamento; • Permitir a aplicação de filtros, agrupando e classificando dados, comparando períodos, definindo metas e alertas; • Permitir conexão a uma variedade de fontes de dados, como planilhas, bancos de dados, aplicativos. API's e serviços em nuvem; • Permitir a criação de elementos visuais para monitorar e analisar dados em tempo real; • Permitir painéis incorporáveis em sites ou intranets externos; • Permitir painéis incorporáveis de sites externos; • Permitir aos usuários coletar, organizar, visualizar e analisar dados de várias fontes em um só lugar; • Permitir o compartilhamento das visualizações através de URL'S internas; • Permitir a exportação de gráficos e relatórios; • Permitir a exportação para download em PDFs, relatório de e-mail agendados e links publicados; • Permitir o acesso de usuários à plataforma, por definição de nível de acesso de usuário, com ou sem autenticação (sem autenticação através de certificado); • Possuir plataforma web integrada que permita a visualização de painéis e relatórios diretamente em navegador web, sem a necessidade de instalação de software ou plug-in nas máquinas dos usuários; • Permitir a integração com soluções de georreferenciamento, tais como Google Maps, OpenStreetMaps ou outra API de mapas existentes no mercado; • Permitir detalhamento das informações georreferenciadas através de cliques de mouse sobre uma determinada área que pode representar, uma cidade, estado ou país; • Permitir o desenvolvimento e a visualização de painéis de métricas, utilizando uma ou mais fontes de dados, trazendo funções estatísticas, como soma, média, contagem, máximo, mínimo, entre outras; • Permitir agendamento para envio automático por e-mail de objetos disponíveis na plataforma nos formatos PDF e imagem; • Permitir a atualização dos dados dos painéis em tempo real e ou em tempos de consulta parametrizados de acordo com as definições estabelecidas na etapa de análise de requisitos ou conforme disponibilidade da fonte de dados; • A solução de governança deverá ser construída a partir da leitura das bases de dados, com relações explícitas entre diversas bases, diversas tabelas e entre os conteúdos de uma mesma tabela. • Será de responsabilidade da contratante, a liberação de acesso à bases de dados de sistemas extras, NÃO fornecidos pela contratada, mediante assinatura de termo de responsabilidade e confidencialidade. Modulo de análise de vídeo A plataforma de análise de vídeo deve terá uma estrutura de processamento multicamada baseada na análise do vídeo em tempo real com um componente de autoaprendizagem de comportamento usual, que permitirá gerar alertas quando um evento incomum for detectado. Esse componente deverá ser capaz de aprender o comportamento usual a partir de uma cena de uma câmara fixa, câmera por câmera, num período não superior a uma semana. A partir de um alerta de comportamento anômalo seguir-se-á um módulo de classificação e contextualização por Deep Learning que permitirá definir qual o objeto específico que gerou o alerta. Isto visa contextualizar o alerta para facilitar sua análise por parte do motor de regras da plataforma ou mesmo do operador do centro de controle. A plataforma deverá adicionalmente conter um motor de Regras/Lógica que automaticamente interpretará os alertas classificados pelo Deep Learning e ajudará a definir as ações a tomar. A camada de análise em tempo real disparará acionadores com base nos seguintes critérios: qualquer comportamento incomum, objeto deixado ou removido, cruzamento de linha, objetos em movimento a distâncias de alguns metros a vários quilômetros (câmeras térmicas) A plataforma deve ser capaz de processar vídeo de câmeras térmicas e/ ou visíveis em formato H265, H264 com resoluções variáveis, de 352 x 288 até 1920 x 1080 ou superior. A plataforma de análise de vídeo deverá ser capaz de gerar um alarme quando for feita uma tentativa de alterar o campo de visão da câmera ou quando a qualidade da imagem se deteriorar devido a desfoque, sujeira ou ofuscamento da lente ou obscurecimento da imagem, borda embaçada detecção, etc O sistema deve permitir configurações específicas da câmera, como definição de áreas específicas, cruzamento de linha, sensibilidades, tempo máximo de um objeto em uma cena dentro de um determinado campo de visão da câmera. A plataforma de análise de vídeo funcionará como uma plataforma de Inteligência Artificial de autoaprendizagem não supervisionada, portanto não exigindo que os operadores definam regras ou condições para detectar eventos incomuns. A plataforma de análise de vídeo será capaz de escalar ou descartar alguns alertas de forma autônoma por meio de seu motor lógico, enquanto apresenta outros alertas a um operador humano para avaliação posterior. O operador deve receber uma indicação visual de quaisquer alertas gerados pela plataforma de análise de vídeo. Caixas delimitadoras com esclarecimentos de metadados devem estar visíveis no alerta enviado ao operador para contextualização adicional. A pedido do Operador, deve ser apresentado um Vídeo Clipe do Alerta, começando imediatamente antes do alerta ocorrer (pré-alarme) e terminando após o seu término (pós-alarme). A plataforma de análise de vídeo deverá ser capaz de classificar uma ampla variedade de objetos, como (mas não limitado a): pessoas, carros, bolsas, mochilas, pássaros, animais, telefones celulares, etc. A plataforma de análise de vídeo pode identificar rostos para fins de classificar ou contar pessoas. A plataforma de análise de vídeo deve ser capaz de detectar capacetes de motocicleta e capacetes de segurança do trabalho

		O mecanismo de regras lógicas deverá permitir a criação de regras precisas, que podem efetivamente mitigar riscos ao otimizar o fluxo de trabalho do sistema. Uma ferramenta de pesquisa forense deve estar disponível para análise pós-evento, para permitir a geração de relatórios rápidos sobre alertas/objetos específicos dentro de áreas específicas do campo de visão da câmera, para intervalos de tempo específicos A plataforma de análise de vídeo deverá oferecer funcionalidades de relatórios de Business Intelligence para fins operacionais. As informações incluirão: Volumes de alerta por câmera; estatísticas de desempenho do operador; eficiência do sistema; estatísticas de classificação. A plataforma de análise de vídeo deverá armazenar numa base de dados SQL ou similar os fotogramas das imagens associadas aos alertas gerados pelo sistema, para eventual consulta futura. Arquitetura do sistema A plataforma de análise de vídeo pode funcionar em conjunto com um VMS de mercado, um NVR ou também estar disponível numa versão autônoma (stand alone) com uma interface de usuário baseada em web. A plataforma de análise de vídeo será totalmente escalável, desde algumas câmeras a milhares de câmeras para processamento simultâneo. A plataforma de análise de vídeo deve ser eficiente em HW, com uma combinação equilibrada de uso de CPU e GPU, ou ainda OpenVino para sistemas com poucas câmeras. A plataforma de análise de vídeo deve poder ser implantada em arquiteturas distribuídas, permitindo uma escolha equilibrada entre uma arquitetura de HW totalmente centralizada e uma arquitetura totalmente Edge. Requisitos funcionais A plataforma de análise de vídeo deve ter monitoramento integrado que possa detectar mascaramento de câmera, ofuscamento, desfoque e reposicionamento A plataforma de análise de vídeo deve ser capaz de contar pessoas e objetos que passam pela cena A plataforma de análise de vídeo deve ser capaz de classificar o maior número possível de objetos dentro de um determinado alerta. Essa classificação deve ser exibida com uma caixa delimitadora, bem como conter uma indicação da probabilidade de classificação (0-100%). Embutido no vídeo, uma indicação visual clara deve estar disponível destacando o alerta ou evento anormal que foi detectado. O algoritmo de análise de vídeo deve empregar Deep Learning em todo o campo de visão da câmera. A plataforma de análise de vídeo deve ser capaz de classificar todos os alertas do sistema em uma lista não exaustiva de casos. A plataforma de análise de vídeo deve ser capaz de ignorar automaticamente eventos específicos para minimizar "falsos positivos" ou eventos sem risco. Esses eventos ignorados (e classificados) são geralmente, entre outros: Fatores ambientais como chuva, queda de folhas, vento, movimentação de água, animais de estimação, etc. Esses eventos ignorados devem ser explicitamente definidos pelo operador. A plataforma de análise de vídeo deve incorporar ferramentas que permitam ao pessoal de segurança e vigilância: • Revisar alertas e eventos anormais durante um período ou local definido • Relatar um alerta enriquecido com dados do Deep Learning A plataforma de análise de vídeo deve ser capaz de oferecer suporte a um conjunto de ferramentas de relatórios de incidentes, incluindo incidentes por data, incidentes por categoria e incidentes por câmera. A plataforma de análise de vídeo deve ser capaz de encaminhar alarmes para as autoridades apropriadas ou pessoal de segurança. A plataforma de análise de vídeo deve ser capaz de registrar e marcar a hora de todos os alertas, ações de regras, classificações e ações do operador para fins de treinamento, auditoria e perícia. Mecanismos de geração de alertas A plataforma de análise de vídeo aprenderá de forma adaptativa sem supervisão e, com o tempo, se ajustará automaticamente às mudanças em uma cena de câmera enquanto continua a identificar todos os eventos anormais. A plataforma de análise de vídeo deve identificar eventos anormais sem a necessidade de regras definidas pelo operador. O sistema deve detectar qualquer evento anormal sem quaisquer regras, viés ou pré-condições. A plataforma de análise de vídeo deve ser capaz de detectar vandalismo de forma autônoma A plataforma de análise de vídeo deve ser capaz de detectar de forma autônoma comportamentos agressivos, brigas etc. A plataforma de análise de vídeo deve ser capaz de detectar de forma autônoma pessoas ou objetos que estão correndo/se movendo em uma velocidade incomum, ou na direção errada A plataforma de análise de vídeo deve ser capaz de detectar de forma autônoma pessoas mandriando A plataforma de análise de vídeo deve ser capaz de detectar fumaça e fogo como pré-alarme A plataforma de análise de vídeo deve ser capaz de detectar de forma autônoma caixas registradoras que são deixadas abertas A plataforma de análise de vídeo deve ser capaz de detectar de forma autônoma pessoas ou veículos se movendo na direção errada ou em faixas erradas para carros. A plataforma de análise de vídeo deve ser capaz de detectar de forma autônoma portas que deixadas abertas A plataforma de análise de vídeo deve ser capaz de detectar de forma autônoma filas em áreas específicas da cena A plataforma de análise de vídeo deve ser capaz de detectar de forma autônoma irregularidades nas áreas reservadas para carga ou descarga de mercadorias A plataforma de análise de vídeo deve ser capaz de detectar de forma autônoma pessoas que acessam áreas proibidas em dias/horários inapropriados, /aglomeração de pessoas em áreas não autorizadas A plataforma de análise de vídeo deve ser capaz de detectar de forma autônoma vazamentos acidentais de sprinklers ou grandes derramamentos de líquidos A plataforma de análise de vídeo deve ser capaz de detectar de forma autónoma pessoas que caem - emergência médica

		A plataforma de análise de vídeo deve ser capaz de contar pessoas em zonas predefinidas e relatar quando uma capacidade predefinida foi excedida A plataforma de análise de vídeo deve ser capaz de detectar autonomamente pessoas caminhando na direção errada ou entrando na área restrita A plataforma de análise de vídeo deve ser capaz de detectar quando um objeto permanece em uma área especificada pelo usuário por um tempo maior do que o pré-configurado Detecção de ameaças em movimento Plataforma de análise de vídeo deve ser capaz de detectar objetos em movimento que se destacam em seu ambiente. A plataforma de análise de vídeo deve ter a capacidade de aprender a cena e focar em alvos reais e não em fatores ambientais comuns à cena. A plataforma de análise de vídeo deve ser capaz de filtrar o ruído ambiental, como, entre outros: árvores em movimento, grama em movimento, reflexos na água, etc. A plataforma de análise de vídeo deve ser capaz de detectar e identificar objetos em movimento muito rápido em distâncias curtas (<50 m) A plataforma de análise de vídeo deve ser capaz de detectar objetos em movimento a uma distância muito longa (> câmeras visíveis de +800 m ou mais de 1 km com câmeras térmicas). Ao usar câmeras térmicas, a plataforma de análise de vídeo deve ser capaz de detectar objetos em movimento em cenários de baixo contraste. A plataforma de análise de vídeo deve ser capaz de detectar o movimento de objetos ou pessoas mesmo quando usada em câmeras PTZ (pan tilt zoom), bem como definir zonas de exclusão individuais para cada preset do sequenciamento da câmera PTZ, de uma preset a outro. A plataforma de análise de vídeo deve ser capaz de gerar alertas direcionais relacionados a objetos que entram de uma determinada direção. Regras e mecanismo de lógica A plataforma de análise de vídeo dever ser capaz de definir um número ilimitado de regras a nível da cada câmera A plataforma de análise de vídeo deverá permitir a definição de um conjunto de regras aplicáveis ao nível da câmera A plataforma de análise de vídeo deverá permitir a priorização de alertas A plataforma de análise de vídeo deverá permitir a definição de um conjunto específico de regras para regiões específicas na visão da câmera. A plataforma de análise de vídeo deverá permitir definir regras para automaticamente descartar alertas ou escalar alertas à condição de alarme. Interface de alerta A plataforma de análise de vídeo deve ser capaz de permitir a exibição de Imagens de Alerta estáticas, enriquecidas com caixas delimitadoras de Metadados. As interfaces de gerenciamento de alertas devem permitir o gerenciamento eficaz e eficiente de grandes volumes de câmeras e alertas. As interfaces de gerenciamento de alertas deverão ser otimizadas para maximizar a eficiência do operador, ao mesmo tempo em que promovem a melhor qualidade de saída possível. As interfaces de gerenciamento de alertas incluirão funcionalidades de pesquisa e notificação, permitindo uma análise efetiva do desempenho da câmera, do sistema e do operador. Devera ser integrado ao software de reconhecimento facial ofertado, enviando os alertas gerados por incidência de indivíduos para análise do reconhecimento facial, identificando os indivíduos em cena e verificação no bando de dados. Os alertas classificados, deverão ser direcionados ao sistema de Gestão de Operação, para atendimento e despacho de viatura. Integração com o sistema de Plataforma integrada de gestão, para apoio na tomada de decisão. Pesquisa Forense O sistema suportará pesquisa/navegação de arquivos e os usuários podem filtrar o resultado da pesquisa por câmera com: a. Área específica em uma cena b. Número de objetos na área c. Tipo de objetos na área d. Tamanhos mínimo e máximo de objetos na área e. Probabilidade mínima de objetos na área f. Tipo de alerta de gatilho usado g. Intervalo de tempo de geração de alerta Modulo de detecção e mensuração de objetos Objetos Detectáveis O SOFTWARE deverá possuir a funcionalidade de carregamento de bibliotecas de detecção de objetos, onde cada biblioteca possua uma lista de objetos a serem detectados. O SOFTWARE deve possuir no mínimo quatro bibliotecas principais com os seguintes objetos disponíveis: Biblioteca Geral: pessoa, bicicleta, carro, moto, ônibus, comboio, caminhão, semáforo, hidrante, sinal de parada; Biblioteca de Crime: Capacete de moto, boné, arma pequena, arma longa, mãos ao alto, celular; Biblioteca de prevenção de incêndio: fogo e fumaça (com configuração de sensibilidade). Regras de Alarmes O SOFTWARE deverá possuir no mínimo as seguintes condições para o disparo de eventos: Objeto alvo dentro da área configurada por tempo igual ou superior ao configurado; Quantidade de objetos configurados dentro de determinada área inferior, igual ou superior a quantidade configurada; Objeto alvo parado dentro de determinada área por tempo igual ou superior ao configurado; Objeto alvo em movimento dentro de determinada área por tempo igual ou superior ao configurado;

		Objeto alvo não presente em determinada área; Avanço de objeto alvo em direções proibidas, configuradas através de linhas virtuais; Avanço de objeto alvo em direções proibidas, configuradas através de áreas virtuais, com análise do rastro dos objetos e quantificações da quantidade de ângulos na direção desejada; Proximidade entre objetos menor ou igual a quantidade de PIXELS configurada; Proximidade entre objetos maior ou igual a quantidade de PIXELS configurada; Proximidade entre objetos menor ou igual a quantidade de PIXELS configurada, em angulação predeterminada; Proximidade entre objetos igual a quantidade de PIXELS configurada, em angulação predeterminada; Presença de determinado objeto dentro da área de um objeto alvo; Ausência de determinado objeto dentro da área de um objeto alvo; Objeto com a incidência de cor predeterminada em porcentagem igual ou superior à configurada; Objeto sem a incidência de cor predeterminada em porcentagem igual ou superior à configurada; Falha de conexão entre o SOFTWARE e a câmera; Simplificação do cenário atual, como por exemplo falta de iluminação, pichação na lente da câmera, cena desfocada, etc...; Deteção de gesto "mãos ao alto" do objeto pessoa. • O SOFTWARE deverá possuir no mínimo as seguintes configurações para as zonas de detecções: Zonas de alarmes em forma de cascata de eventos, como por exemplo, disparo da zona de alarme da câmera A ser condicionado ao disparo anterior em X segundos em relação ao disparo da zona de alarme da câmera B; Zonas de exclusões de detecções; Zonas de Heatmap com exibição em tempo real da porcentagem de movimento por zona; O SOFTWARE deverá possuir no mínimo as seguintes configurações de rastreamento: Personalização da distância euclidiana mínima entre objetos por frames; Tempo de rearme para contabilização de objeto reincidente determinada linha; Tempo de busca de objetos que tenham sofrido possível oclusão. O SOFTWARE deverá permitir as seguintes configurações adicionais: Agendamento das detecções; Geração de heatmaps com armazenamento das imagens em intervalo de tempo configurável para visualização do quadro evolutivo; Tempo de busca de objetos que tenham sofrido possível oclusão.
3.3	Serviços de Locação de Link de Dados - Tipo I	3.3 SERVIÇO DE LOCAÇÃO DE LINK DE DADOS – TIPO I O link de dados é responsável pela transmissão das imagens captadas pelo ponto de coleta de imagem até a sala de comando e controle. Para atender as necessidades deve-se respeitar os seguintes requisitos: O link deve ser construído em fibra óptica ou radiofrequência; Deve prover a interligação dos pontos de coleta de imagem até a sala de comando e controle; Deve possuir capacidade mínima de 10Mbps no ponto de coleta de imagem; Deverá garantir por meio de canais seguros para transmissão de dados e imagens, compostos por um canal óptico e/ou um enlace de rádio em frequência reservada à segurança pública de acordo com as disposições emanadas da Agência Nacional de Telecomunicações - ANATEL.
4	KIT 4- Manutenção **e conectividade de sistema existente**	
4.1	Manutenção Ponto de Videomonitoramento	4.1 MANUTENÇÃO DE SISTEMA DE MONITORAMENTO ELETRONICO • Pretende-se a contratação de serviços de manutenção do Sistema de Cercamento e Monitoramento Eletrônico, implantado com recursos do Convênio nº 855949/2017. A contratação se deu, a partir da Ata de Registro de Preços nº 720/2018, decorrente do Pregão Eletrônico nº 409/2018, cujo Termo de Referência descreve a composição dos kits ponto de cercamento, ponto de videomonitoramento, sala de comando e controle (monitoramento) e sala de comando e controle (cercamento). • O prazo de garantia dos equipamentos e serviços adquiridos é de 2 anos. Não só o Governo do Estado contratou a partir da referida Ata, outros entes também o fizeram. • Neste sentido, se faz necessária a contratação da manutenção, com vistas à continuidade dos serviços. • A Manutenção Preventiva, cujo objetivo é diminuir as possibilidades de paralisações, contempla os serviços efetuados para manter os equipamentos funcionando em condições normais e compreende: manutenção do bom estado de conservação, substituição de componentes que comprometam o bom funcionamento, modificações necessárias com objetivo de atualização dos aparelhos, limpeza, regulagem, inspeção e simulação de testes mecânicos e eletroeletrônicos em todo o sistema interno e externo, entre outras ações que garantam a operacionalização dos equipamentos. • A manutenção preventiva do sistema deverá ser realizada de forma periódica, em quantidade de horas suficientes para cumprir, no mínimo, as tarefas listadas a seguir: • Verificar as identificações das câmeras, cabos, etc. e refazê-las se necessário; • Limpeza da parte externa\internas das caixas metálicas; • Limpeza da lente e visor das câmeras; • Ajuste de foco das lentes; • Verificação das tensões de alimentação; • Verificação da instalação física (suporte e fiação); • Verificação das imagens quanto a interferências, ajuste de foco, contraste, cores, enquadramento, etc.; • Monitores: limpeza, verificação das conexões e ajustes de tela; • Os procedimentos a serem executados com relação as câmeras que são externas, em razão do local onde encontram-se instaladas, poderá ser necessária a adoção de procedimentos especiais de segurança para execução das tarefas listadas. As propostas de preços das licitantes deverão prever esses serviços, os quais não poderão ser alegados como motivo para majoração dos valores contratuais.

		• Entende-se por manutenção corretiva, aquela destinada a rever instalações, remover os defeitos de funcionamento de qualquer natureza apresentados pelos materiais, equipamentos e instalações. Deverá ser realizada por técnico(s) especializado(s) da Contratada, quando solicitado pela Fiscalização. • A Contratada deverá realizar a assistência técnica corretiva nos equipamentos sempre que solicitado pela Fiscalização no prazo estabelecido neste termo de referência, contado da data de cada solicitação. • Os serviços de manutenção preventiva\corretiva serão prestados com o fornecimento, pela Contratada, de todos os acessórios necessários para a execução dos serviços. • A manutenção preventiva\corretiva em sala de comando e controle consiste nos seguintes equipamentos: rack's, bastidores, switches, monitores, TV's profissionais, concentradores, conversores ópticos, servidores storages, nobreaks, DIO's, conversores, patch cords, alimentação elétrica dos sistemas, terminais de computadores, cabeamento estruturado, conectores e jacks RJ45,e demais componentes dos sistemas, consiste em todas as ações necessárias para manter o bom funcionamento e acabamento de todos os componentes, sendo constituído os seguintes procedimentos: • Efetuar testes de funcionalidade; • Verificar o estado geral das instalações; • Efetuar manutenção preventiva\corretiva nos dispositivos de conexão (patch pannel, blocos de conexão rápida, tomadas e similares); • Verificar alimentação elétrica do sistema canaletas e eletrodutos (sistemas e similares); • Realizar a conservação e limpeza de todos os equipamentos e dispositivos de imagens e dados; • Refazer e adequar a identificação de cabos, patch cords, rack's, DIO's, caixas de emendas ópticas, pigtails, caixas de passagem e equipamentos e demais componentes do sistema; • Verificar e corrigir a arrumação de cabos metálicos e rack's; • Demais procedimentos necessários para a correção e prevenção de possíveis defeitos; • Instalação\atualização de sistema operacional e software de monitoramento. 4.1.1 Manutenção de Kit Ponto de Monitoramento Eletrônico O ponto é composto pelos seguintes itens: • 01 câmera speed dome com zoom óptico; • 01 caixa porta equipamento; • 01 poste de concreto cônico (mínimo 9m); • 01 suporte para câmera; • 01 entrada de energia elétrica; • 01 nobreak; • 02 switches/conversores de mídia; • 01 link de fibra óptica ou de radiofrequência. 4.1.2 Manutenção de Kit Sala de Comando e Controle - Cercamento A sala é composta pelos seguintes itens: • 02 estações de trabalho c/2 monitores; • 01 servidor e storage; • 01 nobreak; • 01 rack piso; • 01 switch 24 portas; • 02 mesas; • 02 cadeiras; • 01 condicionador de ar 12000 BTUs; • 01 armário. 4.2 MONITORAMENTO REMOTO 4.2.1 MONITORAMENTO DE ATIVOS • O software de gerenciamento de rede deve garantir a disponibilidade e informações dos componentes de rede e medidas de tráfego e uso; • Deverá abranger todos os aspectos da rede, com monitoramento de up e downtime, monitoramento do tráfego e uso, SNMP, NetFlow e status dos equipamentos; • Deve possuir suporte para, no mínimo, 40 tipos de sensores de controle, incluindo PING, HTTP, WMI, SNMP, SMTP, POP3, FTP, RDP, DNS; • Deve possuir capacidade de análise de tráfego e comportamento de rede; • Deve possuir detecção automática de rede e configuração do sensor; • Deve possuir capacidade de integração de sensores personalizados; • Deve possuir interface baseada em WEB; • Deve possuir suporte a diversos layouts de painel, permitindo, no mínimo, visão geral e rápida; • Deve fornecer resultados de monitoramento visíveis através de várias opções de perspectiva; • Deve possuir visão hierárquica de grupos, dispositivos, sensores, canais; • Deve possuir listagem de sensores - alfabética, mais rápida, mais lenta, por tag, por tipo, entre outras; • Deve fornecer relatórios e arquivos de log, com registros detalhados de todas as atividades e resultados; • Deve possuir gráficos para sensores, dispositivos e grupos que mostrem o monitoramento das últimas 2 horas, últimas 48 horas, últimos 60 dias e últimos 365 dias; • Deve possuir "Mapas" customizáveis que reúnam monitoramento de estações, gráficos e tabelas, usando layouts personalizáveis; • Deve possuir alertas de acordo com critérios configurados individualmente; • Deve fornecer relatórios periódicos em formato HTML e PDF; • Deve possuir mecanismos de notificação, tais como: via e-mail, SMS, solicitação HTTP, syslog, entre outros;

		• Deve ser compatível com Windows Server. 2.2 MONITORAMENTO DE SLA • Deve permitir que o usuário possa iniciar um chamado de atendimento para determinado equipamento pelo próprio painel de visualização; • Deverá ter cadastro de tipos de equipamento; • Deverá ter cadastro de equipamentos, com IP, nome, tipo, grupo e grau de importância; • Deve permitir cadastro de responsáveis pelo atendimento dos chamados, com possibilidade de determinar equipamentos ou grupos de equipamentos de sua responsabilidade; • Deve permitir cadastrar tipos de SLA por equipamentos ou grupos específicos, com tempos determinados de atendimento, conforme seu grau de importância; • Deve estar integrado com aplicativo móvel, permitindo, por exemplo, determinar quais técnicos poderão atender aos chamados, podendo esses receber informações sobre os equipamentos, agendas de manutenção preventiva ou corretiva; • O aplicativo móvel deverá permitir que o início do tratamento do chamado técnico seja efetuado se o atendente estiver no mesmo geoposicionamento dos equipamentos com problema; • O atendente deve ter opção de registrar o atendimento e criar um fluxo de trabalho de atendimentos, podendo direcionar para outro atendente, finalizar ou outras ações pré-determinadas; • O sistema deverá apresentar, na central de monitoramento, todo fluxo de trabalho de tratamento dos atendimentos, com uma linha do tempo das ações e com possibilidade de inserção de comentários em cada fase de atendimento; • O sistema deverá acusar se algum chamado se apresenta em atraso e determinar em qual fase o mesmo se encontra.
4.2	Serviços de Locação de Link de Dados - Tipo I	4.2 SERVIÇO DE LOCAÇÃO DE LINK DE DADOS – TIPO I O link de dados é responsável pela transmissão das imagens captadas pelo ponto de coleta de imagem até a sala de comando e controle. Para atender as necessidades deve-se respeitar os seguintes requisitos: O link deve ser construído em fibra óptica ou radiofrequência; Deve prover a interligação dos pontos de coleta de imagem até a sala de comando e controle; Deve possuir capacidade mínima de 10Mbps no ponto de coleta de imagem; Deverá garantir por meio de canais seguros para transmissão de dados e imagens, compostos por um canal óptico e/ou um enlace de rádio em frequência reservada à segurança pública de acordo com as disposições emanadas da Agência Nacional de Telecomunicações - ANATEL.
5	**KIT - 5 Conexão de Espelhamento e manutenção do sistema**	
5.1	Serviços de Locação de Link de Dados - Tipo II	5.1 SERVIÇO DE LOCAÇÃO DE LINK DE DADOS – TIPO II O link de dados tipo II será responsável pela transmissão das imagens captadas nos municípios, devendo as imagens serem transmitidas da sala de comando e controle e integradas ao CICC-R de Porto Alegre. O link de integração da Sala de Comando e Controle no município com o CICC-R de Porto alegre será de responsabilidade da contratada. O link de comunicação deverá ter largura de banda suficiente para trafegar dados oriundo das imagens obtidas através de todas as câmeras do município, tráfego este considerado entre a sala de comando e controle do município e o CICC-R instalado na sede da SSP-RS, em Porto Alegre.
5.2	Manutenção em Sala de Comando e Controle (Cercamento)	5.2 MANUTENÇÃO DE SISTEMA DE MONITORAMENTO ELETRONICO • Pretende-se a contratação de serviços de manutenção do Sistema de Cercamento e Monitoramento Eletrônico, implantado com recursos do Convênio nº 855949/2017. A contratação se deu, a partir da Ata de Registro de Preços nº 720/2018, decorrente do Pregão Eletrônico nº 409/2018, cujo Termo de Referência descreve a composição dos kits ponto de cercamento, ponto de videomonitoramento, sala de comando e controle (monitoramento) e sala de comando e controle (cercamento). • O prazo de garantia dos equipamentos e serviços adquiridos é de 2 anos. Não só o Governo do Estado contratou a partir da referida Ata, outros entes também o fizeram. • Neste sentido, se faz necessária a contratação da manutenção, com vistas à continuidade dos serviços. • A Manutenção Preventiva, cujo objetivo é diminuir as possibilidades de paralisações, contempla os serviços efetuados para manter os equipamentos funcionando em condições normais e compreende: manutenção do bom estado de conservação, substituição de componentes que comprometam o bom funcionamento, modificações necessárias com objetivo de atualização dos aparelhos, limpeza, regulagem, inspeção e simulação de testes mecânicos e eletroeletrônicos em todo o sistema interno e externo, entre outras ações que garantam a operacionalização dos equipamentos. • A manutenção preventiva do sistema deverá ser realizada de forma periódica, em quantidade de horas suficientes para cumprir, no mínimo, as tarefas listadas a seguir: • Verificar as identificações das câmeras, cabos, etc. e refazê-las se necessário; • Limpeza da parte externa\internas das caixas metálicas; • Limpeza da lente e visor das câmeras; • Ajuste de foco das lentes; • Verificação das tensões de alimentação; • Verificação da instalação física (suporte e fiação); • Verificação das imagens quanto a interferências, ajuste de foco, contraste, cores, enquadramento, etc.; • Monitores: limpeza, verificação das conexões e ajustes de tela; • Os procedimentos a serem executados com relação as câmeras que são externas, em razão do local onde encontram-se instaladas, poderá ser necessária a adoção de procedimentos especiais de segurança para execução das tarefas listadas. As propostas de preços das licitantes deverão prever esses serviços, os quais não poderão ser alegados como motivo para majoração dos valores contratuais.

		• Entende-se por manutenção corretiva, aquela destinada a rever instalações, remover os defeitos de funcionamento de qualquer natureza apresentados pelos materiais, equipamentos e instalações. Deverá ser realizada por técnico(s) especializado(s) da Contratada, quando solicitado pela Fiscalização. • A Contratada deverá realizar a assistência técnica corretiva nos equipamentos sempre que solicitado pela Fiscalização no prazo estabelecido neste termo de referência, contado da data de cada solicitação. • Os serviços de manutenção preventiva\corretiva serão prestados com o fornecimento, pela Contratada, de todos os acessórios necessários para a execução dos serviços. • A manutenção preventiva\corretiva em sala de comando e controle consiste nos seguintes equipamentos: rack's,bastidores, switches, monitores, TV's profissionais, concentradores, conversores ópticos, servidores storages, nobreaks, DIO's, conversores, patch cords, alimentação elétrica dos sistemas, terminais de computadores, cabeamento estruturado, conectores e jacks RJ45,e demais componentes dos sistemas, consiste em todas as ações necessárias para manter o bom funcionamento e acabamento de todos os componentes, sendo constituído os seguintes procedimentos: • Efetuar testes de funcionalidade; • Verificar o estado geral das instalações; • Efetuar manutenção preventiva\corretiva nos dispositivos de conexão (patch pannel, blocos de conexãorápida, tomadas e similares); • Verificar alimentação elétrica do sistema canaletas e eletrodutos (sistemas e similares); • Realizar a conservação e limpeza de todos os equipamentos e dispositivos de imagens e dados; • Refazer e adequar a identificação de cabos, patch cords, rack's, DIO's, caixas de emendas ópticas,pigtails, caixas de passagem e equipamentos e demais componentes do sistema; • Verificar e corrigir a arrumação de cabos metálicos e rack's; • Demais procedimentos necessários para a correção e prevenção de possíveis defeitos; • Instalação\atualização de sistema operacional e software de monitoramento. 5.2.1 Manutenção de Kit Ponto de Monitoramento Eletrônico O ponto é composto pelos seguintes itens: • 01 câmera speed dome com zoom óptico; • 01 caixa porta equipamento; • 01 poste de concreto cônico (mínimo 9m); • 01 suporte para câmera; • 01 entrada de energia elétrica; • 01 nobreak; • 02 switches/conversores de mídia; • 01 link de fibra óptica ou de radiofrequência. 5.2.2 Manutenção de Kit Sala de Comando e Controle - Cercamento A sala é composta pelos seguintes itens: • 02 estações de trabalho c/2 monitores; • 01 servidor e storage; • 01 nobreak; • 01 rack piso; • 01 switch 24 portas; • 02 mesas; • 02 cadeiras; • 01 condicionador de ar 12000 BTUs; • 01 armário. 5.3 MONITORAMENTO REMOTO 5.3.1 MONITORAMENTO DE ATIVOS • O software de gerenciamento de rede deve garantir a disponibilidade e informações dos componentes de rede e medidas de tráfego e uso; • Deverá abranger todos os aspectos da rede, com monitoramento de up e downtime, monitoramento do tráfego e uso, SNMP, NetFlow e status dos equipamentos; • Deve possuir suporte para, no mínimo, 40 tipos de sensores de controle, incluindo PING, HTTP, WMI, SNMP, SMTP, POP3, FTP, RDP, DNS; • Deve possuir capacidade de análise de tráfego e comportamento de rede; • Deve possuir detecção automática de rede e configuração do sensor; • Deve possuir capacidade de integração de sensores personalizados; • Deve possuir interface baseada em WEB; • Deve possuir suporte a diversos layouts de painel, permitindo, no mínimo, visão geral e rápida; • Deve fornecer resultados de monitoramento visíveis através de várias opções de perspectiva; • Deve possuir visão hierárquica de grupos, dispositivos, sensores, canais; • Deve possuir listagem de sensores - alfabética, mais rápida, mais lenta, por tag, por tipo, entre outras; • Deve fornecer relatórios e arquivos de log, com registros detalhados de todas as atividades e resultados; • Deve possuir gráficos para sensores, dispositivos e grupos que mostrem o monitoramento das últimas 2 horas, últimas 48 horas, últimos 60 dias e últimos 365 dias; • Deve possuir"Mapas" customizáveis que reúnam monitoramento de estações, gráficos e tabelas, usando layouts personalizáveis; • Deve possuir alertas de acordo com critérios configurados individualmente; • Deve fornecer relatórios periódicos em formato HTML e PDF; • Deve possuir mecanismos de notificação, tais como: via e-mail, SMS, solicitação HTTP, syslog, entre outros; • Deve ser compatível com Windows Server. 5.3.1 MONITORAMENTO DE SLA • Deve permitir que o usuário possa iniciar um chamado de atendimento para determinado equipamento pelo próprio painel de visualização; • Deverá ter cadastro de tipos de equipamento; • Deverá ter cadastro de equipamentos, com IP, nome, tipo, grupo e grau de importância; • Deve permitir cadastro de responsáveis pelo atendimento dos chamados, com possibilidade de determinar equipamentos ou grupos de equipamentos de sua responsabilidade; • Deve permitir cadastrar tipos de SLA por equipamentos ou grupos específicos, com tempos determinados de atendimento, conforme seu grau de importância;

		• Deve estar integrado com aplicativo móvel, permitindo, por exemplo, determinar quais técnicos poderão atender aos chamados, podendo esses receber informações sobre os equipamentos, agendas de manutenção preventiva ou corretiva; • O aplicativo móvel deverá permitir que o início do tratamento do chamado técnico seja efetuado se o atendente estiver no mesmo geoposicionamento dos equipamentos com problema; • O atendente deve ter opção de registrar o atendimento e criar um fluxo de trabalho de atendimentos, podendo direcionar para outro atendente, finalizar ou outras ações pré-determinadas; • O sistema deverá apresentar, na central de monitoramento, todo fluxo de trabalho de tratamento dos atendimentos, com uma linha do tempo das ações e com possibilidade de inserção de comentários em cada fase de atendimento; • O sistema deverá acusar se algum chamado se apresenta em atraso e determinar em qual fase o mesmo se encontra.