PREFEITURA MUNICIPAL DE SÃO JOSÉ DO RIO PRETO

CONCESSÃO ADMINISTRATIVA PARA IMPLANTAÇÃO, MANUTENÇÃOE OPERAÇÃO DE SISTEMAS DE CIDADE INTELIGENTE NO MUNICÍPIO - "SMART RIO PRETO"

ANEXO II.2 – CADERNO DE ENCARGOS – SISTEMA DE VIDEOMONITORAMENTO

CONCORRÊNCIA PÚBLICA – PRESENCIAL Nº 01/2025

SECRETARIA MUNICIPAL DE ADMINISTRAÇÃO
DIRETORIA DE CONTRATAÇÕES PÚBLICAS
Avenida: Alberto Andaló, 3030 (2º andar) - Centro – CEP: 15015-000 - São José do Rio Preto - SP
Telefone: (17) 3203-1135 / 3203-1239 / 3203.1347 – www.riopreto.sp.gov.br

PREFEITURA DE
RIO PRETO

SUMÁRIO

ESPECIFICAÇÃO TÉCNICA DE MATERIAIS, SISTEMAS E SERVIÇOS DE IMPLANTAÇÃO, MODERNIZAÇÃO, MANUTENÇÃO E OPERAÇÃO DO SISTEMA DE MONITORAMENTO PÚBLICO DO MUNICÍPIO DE SÃO JOSÉ DO RIO PRETO

1. SOLUÇÃO

A solução deve ser composta por uma Plataforma de Sistema de Monitoramento (referida como Plataforma ou Plataforma *Smart* Rio Preto), serviços de desenvolvimento e implantação de *software*, implantação de infraestrutura, conectividade, elaboração de projeto técnico e instalação de equipamentos e mobiliário, ficando a cargo da CONTRATADA prover todo o material e serviços necessários à implementação da solução. Será de responsabilidade da CONTRATADA realizar todo o licenciamento necessário à execução do serviço, seja de componentes da solução como *hardware* e *software*, como também licenças para uso do solo e de postes para a instalação de equipamentos.

A Plataforma tem por principal função ser um concentrador / integrador dos diversos sistemas de monitoramento da Administração Municipal, otimizando os serviços, que passarão a ser operados de forma cooperativa e integrada entre os órgãos, resultando no melhor atendimento aos munícipes e aproveitamento dos recursos disponíveis na Administração Pública. A Plataforma também deve receber dados provenientes de sistemas de empresas da iniciativa privada, facilitando a cooperação com a sociedade. Esta nova Plataforma substituirá outras Plataformas que têm como missão a cooperação com a sociedade, permitindo maior interação da sociedade com o Poder Público.

A Plataforma *Smart* Rio Preto deve funcionar de maneira que as imagens das câmeras de videomonitoramento da cidade de SÃO JOSÉ DO RIO PRETO sejam concentradas em uma única Plataforma *Web* (Rede Mundial de Computadores). Assim, serão atendidas as necessidades do novo centro integrado de soluções em segurança dos cidadãos da cidade. Importante destacar que todas as entregas deverão ser feitas na forma de *SaaS* dentro da Plataforma.

A CONTRATADA será responsável por elaborar o projeto de implantação da solução *Smart* Rio Preto, tendo em vista a necessidade de evolução desta solução, seja pelas mudanças tecnológicas, seja por necessidade da Administração Pública, ante a dinâmica da própria cidade. A solução deve ser tão dinâmica quanto as necessidades da cidade, trazendo agilidade para a Administração Pública. Os projetos apresentados, conforme as fases definidas, devem ser analisados e aprovados pela CONTRATANTE antes de sua execução pela CONTRATADA.

A Plataforma *Smart* Rio Preto deve ser toda construída de forma a ser acessível através da *Web*, permitindo utilização em diversos dispositivos (multiplataforma), de acordo com as tecnologias mais recentes e atualizadas, sendo acessível por *desktops* e dispositivos móveis, independente do sistema operacional desde que este possua um navegador (*browser*) atual e compatível com a solução (por exemplo: *chrome*, *opera* e *firefox*).

A aplicação *Web* (designada Plataforma) será utilizada para o gerenciamento de todo conteúdo, incluindo a própria Plataforma. Será através dela que serão feitos o planejamento, análise de dados, atividades de videomonitoramento, atendimento / rádio despacho. Também deve ser possível a construção de aplicações por fluxo e utilizando *No Code* e/ou *Low Code*, além de diversas integrações. Esta Plataforma concentradora realizará as integrações entre os vários sistemas, permitindo a cooperação e integração entre diversos órgãos e serviços. É o item mais importante na implementação da Plataforma Inteligente, permitindo a troca de informações rápida e a interoperabilidade entre sistemas, o que aumenta a cooperação, reduz o tempo de reação a incidentes e traz maior eficiência às ações preventivas, otimizando a utilização de recursos com um planejamento unificado e escalonado para cobrir as variáveis identificadas, tendo contingência e pronta resposta ao maior número de situações possível.

Entende-se como Plataforma (Plataforma *Web*, Plataforma *Smart* Rio Preto): conjunto de sistemas e subsistemas integrados e interoperáveis, com funcionalidades agrupadas por módulos, com *interfaces* personalizadas e controle de acesso unificado, trazendo a ideia (experiência) ao usuário de que se trata de um único sistema, não sendo necessário realizar *login* múltiplas vezes (sempre que acessar outra ferramenta ou sistema). Todos os sistemas e subsistemas que compõem a Plataforma devem ser executados em *cloud computing* e possuir *interface* de acesso em arquitetura *Web* (acessível através de *browser*), além de serem disponibilizados como *SaaS*. Independente da linguagem utilizada para construção dos sistemas / serviços (*back end*) e das *interfaces* (*front end*), estas devem funcionar nos principais navegadores (*browser*: *chrome*, *opera* e *firefox*) do mercado, a fim de garantir maior compatibilidade da Plataforma com múltiplos

sistemas (*Cross Platform*) a um custo reduzido, sem a necessidade de instalar aplicação-cliente, além do próprio navegador (*browser*).

A Plataforma / solução deve ser escalável, permitindo sua expansão gradual, e o CORE (Núcleo da Plataforma) deve ser *IaaS Multi Cloud*, em que todos os sistemas e subsistemas que compõem a Plataforma devem ser alocados.

Além da infraestrutura *IaaS* utilizada pela CONTRATADA, para prover a Plataforma / solução à CONTRATANTE, o sistema de gerenciamento *multi cloud* deve permitir à CONTRATANTE acoplar / incluir *IaaS* proveniente de OUTROS CONTRATOS, caso entenda necessário, para viabilizar integrações entre sistemas ou dar maior escalabilidade à Plataforma.

A solução de gerenciamento de *IaaS multi cloud* utilizada pela CONTRATADA deve permitir a migração e movimentação de processos / serviços entre diferentes *IaaS*, simplificando a transferência dos dados e a continuidade dos serviços ao término do contrato.

1.1. Escalabilidade

A escalabilidade da Plataforma tem como principal função garantir a disponibilidade de acesso à Plataforma, em situações fora da normalidade de operação da Plataforma.

A escalabilidade também deve permitir a expansão gradual da Plataforma à medida que é implantada e novos componentes, funcionalidades, módulos e integrações forem incluídos e disponibilizados conforme descrito neste termo de referência e em seus anexos, e deve ser considerada, também, a possibilidade de aditamento do contrato conforme legislação vigente.

1.2. Disponibilidade e Segurança

A solução deve contar com todas as ferramentas necessárias a garantir a segurança da Plataforma de ponta a ponta, criando um modelo de múltiplas camadas de segurança como forma de mitigar ataques, violações, vazamentos e garantir a confidencialidade, disponibilidade e integridade, contando com criptografia para todo o tráfego, bases de dados, dados e arquivos armazenados, utilização de SSL/TLS, *firewall* (UTM, NGFW), WAF (*Web Application Firewall*), CDN, VPN e outras tecnologias para garantir a comunicação segura através de redes, e deve possuir *interface* para definição de regras de acesso, priorização, bloqueio

e ação baseada em variáveis, *interfaces* de gerenciamento da infraestrutura e de redes com monitoramento, segregação (ex.: Vlan) e outras ferramentas de controle disponíveis nas camadas de rede.

As Partes devem trabalhar em conjunto para definir as necessidades de segurança de acordo com a conectividade / *Link*s propostos pela contratante para a Plataforma / solução e também para elaboração de Plano de Recuperação de Desastres (DRP) e Plano de Contingência.

As informações de todos os equipamentos, sistemas e ferramentas utilizados na Plataforma / solução devem estar disponíveis em tempo real à CONTRATANTE através de painel vinculado ao Módulo de Gestão conforme descrito, permitindo, assim, a análise e acompanhamento da operação da Plataforma e tempo de reação reduzido sempre que anomalias forem detectadas e que precisem de correção (ex.: *Link* rompido do ponto #4598) ou mitigação a ataques (em que o tempo de resposta pode ser a diferença entre um ataque mal sucedido e o vazamento de dados), e estas informações devem servir como ferramenta de diagnóstico das falhas e como fiscalização da qualidade dos serviços que compõem a Plataforma.

A solução deve possuir registro e alerta para ajudar a detectar qualquer atividade não autorizada, incluindo uma segunda linha de defesa com a detecção e resposta de *endpoint* gerenciado, para complementar a segurança da Plataforma.

1.3. Legado dos Programas Anteriores

Os programas legados terão continuidade em nível conceitual, mantendo os pontos positivos que estes programas possuíam e dando continuidade às iniciativas, incluindo uma nova perspectiva com revisões e aprimoramento dinâmico, utilizando revisões periódicas em curtos períodos de tempo para avaliar a necessidades de alteração no programa, garantindo a melhoria contínua dos serviços oferecidos à população.

Apenas dados serão migrados de sistemas legados para a nova Plataforma e devem passar pelo processo de reestruturação, análise e descarte de dados irrelevantes ou sem propósito, conforme legislação vigente, visando as garantias individuais e a privacidade.

Todas as integrações à nova Plataforma *Smart* Rio Preto, com parceiros, devem passar por prévio processo de homologação, a fim de garantir a qualidade e segurança da solução como um todo. As integrações deste

tipo serão realizadas através de API (Interfaces de Programação de Aplicações) aberta e serão realizadas pelo parceiro em sua própria Plataforma.

Será obrigatória a adequação aos padrões da Plataforma, bem como a aceitação dos termos da LGPD (Lei Geral de Proteção de Dados) para o compartilhamento das imagens com a Prefeitura de SÃO JOSÉ DO RIO PRETO, tendo que assinar TERMO DE CONSENTIMENTO da cessão e uso das imagens, assim como novo processo de homologação das empresas que poderão fazer as integrações e oferecer este serviço com o armazenamento em nuvem aos munícipes.

1.5. Programas Legados de Monitoramento

Todos serão substituídos pela parte da Plataforma responsável pelo videomonitoramento, e tratativa de alertas, em se tratando de câmeras próprias, terão armazenamento, e o período de armazenamento será passível de administração, bem como de outras características.

1.6. Programas Legados de Cooperação com a Sociedade

Todos serão substituídos em diversos módulos, nas funções de análise de dados, estatística, planejamento e simulação, para a Plataforma, permitindo que estas funções estejam disponíveis a todos e desta forma gerar relatórios e gráficos utilizando dados em tempo real, comparando dados conforme parâmetros definidos e sua flutuação. A Plataforma *Smart* Rio Preto deve, ainda, permitir maior interação com usuários, através de um componente de acompanhamento de demandas da sociedade.

1.7. Implantação da Solução

A vigência do contrato será de 30 anos, prazo no qual deverá a CONTRATADA amortizar o seu investimento. Não haverá transferência de patrimônio da CONTRATANTE para a CONTRATADA ao final da vigência contratual.

Os *software*s e equipamentos serão substituídos sempre que não cumpram a sua função ou tragam riscos à segurança. A substituição de equipamentos pela CONTRATADA será exigida apenas caso comprometam a qualidade do serviço, inclusive no que tange à segurança. As características dos equipamentos a serem instalados, que não estejam delineadas neste Termo de Referência, inclusive no que tange a serem novos ou usados, devem ser definidas pela CONTRATADA, que deve, contudo, sempre cumprir com os parâmetros de qualidade do serviço definidos neste Termo de Referência.

A implementação da solução proposta é fundamental para atender às necessidades da Administração Pública de maneira eficiente e inovadora. É importante ressaltar que a tecnologia avança rapidamente, e é crucial que a Plataforma / solução seja moldada para acompanhar essas mudanças, permitindo a incorporação de novas funcionalidades e tecnologias emergentes.

Mediante contrato de 30 anos, a solução proposta tem o tempo necessário para ser implementada e aprimorada, com atualizações tecnológicas sempre que necessárias ou definidas durante as revisões semestrais. É importante destacar que a definição das tecnologias a serem utilizadas na Plataforma / solução ficará a cargo da CONTRATADA, validada pela Administração Pública.

Serão realizados testes de homologação antes da implementação definitiva, para garantir que a solução proposta esteja de acordo com as exigências do Edital.

A solução proposta deve permitir a modernização e otimização dos processos administrativos, possibilitando uma gestão mais eficiente e transparente, com a utilização de tecnologias inovadoras e integradas.

A CONTRATADA deve prover ferramenta de Gestão de Projetos como forma sistêmica e informatizada de acompanhar o cronograma de implantação da Plataforma / solução, disponibilizando acesso, à CONTRATANTE, a todos os processos, desde a elaboração da solução, implementação de novos recursos e tudo que compõe a solução, que devem ser documentados, e esta documentação subsidiará a tomada de decisão para continuidade da Plataforma *Smart* Rio Preto.

A solução poderá ser hospedada no Brasil ou exterior desde que os provedores de serviços estejam sujeitos às melhores práticas internacionais e seja respeitada a LGPD.

Para efeitos de auditoria, a CONTRATADA deve apresentar toda a documentação dos equipamentos, sistemas, adequações / personalizações e suas atualizações de todos os projetos desenvolvidos.

2. INSTALAÇÃO DAS CÂMERAS

A CONTRATADA deverá previamente documentar a forma de instalação das câmeras, conforme necessidade da CONTRATANTE, respeitando as normas técnicas para a realização dos serviços e levando em conta todas as necessidades da instalação, como *modem*, roteador, *switch*, *nobreak*, cabo de rede, caixa

/ armário / *rack* / *shelter*, tipo de cabo, eletroduto, poste e braço para fixação das câmeras, entre outros aqui não especificados devido à grande variação de necessidades de cada local de instalação e tecnologia utilizada na solução.

A documentação relativa a cada câmera deverá ser aprovada pela CONTRATANTE, devendo conter o detalhamento técnico dos equipamentos utilizados, bem como sua adequação ao cronograma.

Todo poste metálico deve possuir isolante elétrico aplicado em sua superfície, iniciando no nível do solo até a altura de 3,30 metros, como forma de mitigar o risco de choque elétrico (o isolante deve cobrir todas as superfícies metálicas, incluindo base e parafusos), podendo ser utilizado isolante líquido desde que previamente aplicado ao poste antes da instalação no local, garantindo, assim, a efetividade do isolamento.

A solução a ser fornecida deverá ser composta por uma Plataforma *Web* modular de Atendimento e Despacho (doravante denominada "Plataforma"), acompanhada dos respectivos serviços de desenvolvimento, implantação de *software*, cibersegurança, elaboração de projeto técnico e instalação de equipamentos. Caberá integralmente à CONTRATADA o fornecimento de todos os materiais, licenças, componentes e serviços necessários à implementação e plena operação da solução.

Será também de responsabilidade da CONTRATADA a obtenção de todas as licenças e autorizações necessárias, tanto para o funcionamento dos componentes da solução quanto para a instalação dos equipamentos em campo, observando integralmente à legislação vigente e às normas técnicas aplicáveis.

A Plataforma *Web* deverá ser implantada inicialmente em ambiente de nuvem, garantindo alta disponibilidade, escalabilidade e segurança. Ao término do contrato, a CONTRATADA deverá realizar a migração integral da solução para o ambiente *on-premisse* da CONTRATANTE, incluindo customizações realizadas no período, banco de dados, histórico de registros, licenças perpétuas e toda a documentação técnica, garantindo à CONTRATANTE a aquisição plena e definitiva da Plataforma, sem dependência de terceiros.

A Plataforma tem por principal função ser um concentrador / integrador dos diversos serviços voltados para área de segurança pública, que passarão a ser operados de forma cooperativa e integrada pela Secretaria de Municipal de Segurança, resultando no melhor atendimento aos munícipes e aproveitamento dos recursos disponíveis na Administração Pública.

A Plataforma deve funcionar de maneira que as imagens das câmeras de videomonitoramento sejam concentradas em uma única Plataforma *Web* de Atendimento e Despacho. Assim, serão atendidas as necessidades do centro integrado de soluções em segurança dos cidadãos.

Fica a CONTRATADA responsável por elaborar o projeto de implantação da Plataforma / solução, tendo em vista a necessidade de evolução desta solução, seja pelas mudanças tecnológicas, seja por necessidade da Administração Pública, ante a dinâmica da própria cidade. A solução deve ser tão dinâmica quanto as necessidades da cidade, trazendo agilidade para a Administração Pública. Os projetos, apresentados conforme as fases definidas, devem ser analisados e aprovados pela CONTRATANTE antes de sua execução pela CONTRATADA.

A Plataforma será utilizada para o gerenciamento de todos os serviços de Atendimento e Despacho da Secretaria Municipal de Segurança Pública. Através dela é que serão feitos o planejamento, análise de dados, atividades de Videomonitoramento, atendimento, radio e despacho. Esta Plataforma concentradora realizará as integrações entre os vários sistemas, permitindo a cooperação e integração de diversos serviços.

Deverá ter sistema de níveis de acesso, que dá diferentes permissões de acordo com as configurações de *login* que os usuários detêm, e caberá ao administrador da CONTRATANTE criar acessos limitados para os usuários conforme sua necessidade.

Deverá ser possível processar e analisar imagens em tempo real e as imagens gravadas, implementando-se conforme a necessidade analítica, simultaneamente para análise delas, otimizando-se o processo de análise, e os algoritmos de análise devem ser executados de forma paralela (execução simultaneamente sem fila de processos).

Entende-se, por análise dinâmica, *software* que permite selecionar objetos predeterminados (ex.: carro, camiseta e motocicleta) e executar pesquisa a partir de horário estabelecido nos vídeos de câmeras de segurança, disponibilizando resultados de acordo com os requisitos especificados.

Deverá realizar análise dinâmica de vídeo em nuvem baseada em *cloud computing*, com capacidade de controlar e visualizar imagens de câmeras IP conectadas à internet ou de câmeras analógicas quando conectadas a equipamentos IP e estes à internet.

- Deter *interface* amigável baseada em HTML5;

- Permitir que o acesso aos *logins* de eventos seja feito somente pelo administrador do sistema ou por quem o administrador liberar;
- Possuir limite de acessos simultâneos de um mesmo usuário. Este recurso deve existir para limitar a quantidade de *logins* simultâneos, automáticos ou não, que um determinado usuário ou grupo de usuário pode realizar no sistema com a mesma conta;
- Imagens ao vivo e gravadas devem continuar disponíveis mesmo em situação de processamento de dados;
- Possuir campo para adicionar ou remover novas câmeras na pesquisa;
- Deter campo para informar solicitações, como, por exemplo, “homem com camisa azul e calça jeans”;
- Possuir filtro de data e hora do início e final de pesquisas;
- Disponibilizar a gravação dos momentos exatos em que o objeto pesquisado passou pela câmera pelo período de gravação vigente;
- Possibilitar o *download* da imagem de pesquisa; e
- Deter um sistema de histórico de registro de eventos, para gravar pesquisas realizadas.

O histórico deve contar com, no mínimo, os seguintes itens:

- ID da solicitação;
- *Status*;
- Câmaras analisadas;
- Solicitante;
- Data;
- Hora; e
- Campo de detalhamento.

No campo de detalhamento, deve informar, minimamente, os seguintes itens:

- Status;
- Data da solicitação;
- Hora da solicitação;
- Período analisado;

- Solicitação;
- Dados da câmera (nome das câmeras, endereço, tipo de câmera e número de série);
- Dados do responsável pela pesquisa (nome, e-mail, matrícula e telefone);
- Resultado da análise com os horários destacados; e
- *Player* do vídeo com possibilidade de *download*, de aumentar ou diminuir a velocidade de reprodução, e *picture-in-picture*.

2.1. Câmera Facial

Reconhecimento simultâneo de várias faces em um fluxo de vídeo. As imagens dos rostos são salvas com data, hora e local de acesso.

Detecção de face coberta (óculos, barbas e diferentes tipos de cabelo etc.).

Possuir aba em lista com registro de todos os eventos de captura facial ao vivo, assim que as leituras forem feitas, detendo dos seguintes dados:

- Captura (com imagem borrada);
- Referência;
- Informações;
- Localização com data, local e nome da câmera que fez a captura. Além disso deve deter aba para alertas ao vivo de possíveis identificações positivas no reconhecimento; e
- Confiança de leitura em percentual (%).

Ao clicar na captura, o usuário deve ser levado para outra aba que descreva os seguintes dados:

- Foto da captura feita;
- Referência;
- *Tag* de motivo da captura;
- CPF;
- RG;
- Cadastrado em dd/mm/aaaa;
- Localização com data, local georreferenciado em mapa e nome da câmera que fez a captura;

- Mandado de prisão;
- Situação;
- Nº do mandado de prisão;
- Data de expedição;
- Data de validade;
- Processo número;
- Espécie de prisão;
- Magistrado;
- Órgão expedidor; e
- País.

Deve ter aba de busca personalizada, com filtros que facilitem a pesquisa do mesmo, minimamente da seguinte forma:

- Data e hora de início da pesquisa;
- Data e hora de término;
- Função para selecionar se imagens são apenas com referências;
- Categorias (*Tags* personalizadas para cada tipo de pesquisa);
- Câmeras;
- Pessoa (possibilidade de colocar o nome do procurado); e
- Confiança.

Também tem que disponibilizar campo de novos cadastros de faces procuradas, com, minimamente, os seguintes itens:

- Campo para adição de faces;
- Nome;
- Função de seleção se cadastro está ativo;
- Apelido;
- CPF;
- RG;

- Estado;
- Cidade;
- Marcar como (*Tags* personalizáveis já mencionadas);
- Mandados de prisão;
- Situação;
- Espécie de prisão;
- Nº do mandado de prisão;
- Magistrado;
- Data de expedição;
- Órgão expedidor;
- Data de validade;
- País;
- Número de processo; e
- Comentários adicionais.

Deve deter campo de busca por nome do registro feito, bem como possuir busca de registro por foto, para situações em que não haja a possibilidade de realizar busca pelo nome.

Além disso, as câmeras devem possibilitar a criação de filtros de pesquisa na busca com, no mínimo, os seguintes itens:

- Buscar por nome;
- Seleção se cadastro está ativo; e
- Categoria.

A criação de categoria deve deter campo para descrição do nome da categoria e possibilidade de excluir categorias criadas.

Deve ser possível atualizar o analítico conforme necessário, para aperfeiçoar a Plataforma e as capacidades de reconhecimento.

2.1.1. Busca Inteligente por Face

Analítico capaz de fazer varredura em imagens, com capacidade de reconhecimento facial a partir de arquivo disponibilizado pelo usuário, tendo a capacidade de trazer os resultados ao mesmo passo que continua a pesquisa.

Entregar campo para *upload* de face procurada.

Limite de nível de confiança da leitura, para procuras mais precisas ou mais genéricas, dependendo do caso de uso.

2.2. Câmera de Leitura de Placa

Funcionalidade de identificação de placas dos veículos em *cloud computing*, com base em leitura dos *frames* das imagens de câmeras específicas e habilitadas para essa função.

Reconhecimento e registro de caracteres de placas em movimento e consulta em tempo real a banco de dados de veículos, em casos necessários.

Ter sistema de eventos ao vivo, para acompanhamento simultâneo, podendo separar por câmeras disponíveis a visualização do mesmo.

São necessários, na área de evento, os seguintes itens:

- Placa e caracteres descritos da leitura feita;
- Recorte da captura da placa;
- Informações relacionadas à leitura feita; e
- Localização.

Ao clicar na captura desejada, é necessário que a aplicação crie nova aba com informações mais detalhadas, com imagem da captura, recorte da placa e mapa com a georreferência do local com capacidade de ampliação ou diminuição de área para pesquisa de possíveis rotas, e possibilidade de *download* da imagem.

Ao encontrar número ou letra não condizente, deve ser possível editar o resultado da leitura manualmente, possibilitando novas verificações do elemento (número/letra).

Possibilidade de integração com banco de dados de veículos, para trazer informações como:

- Marca;

- Modelo;
- Cor;
- Carroceria;
- Cidade; e
- Ano.

Trazer histórico dos registros das detecções de placa do veículo dos últimos 30 dias.

É necessário campo de detecções que traga o histórico de todas as detecções feitas da placa selecionada.

No mesmo devem-se ter, minimamente, os seguintes itens:

- ID da detecção;
- Foto do recorte da placa detectada;
- Localização da detecção;
- Nome da câmera;
- Data e hora; e
- Caixa de seleção para criação de possível rota.

Também é necessária aba de rotas, para visualizar, através de imagem de mapa, possível percurso feito pela placa detectada.

Deve possuir aba de alertas ao vivo, para possível ocorrência com placa registrada, e trazendo as informações de placa, informações adicionais e localização.

O sistema deve possuir capacidade de leitura das antigas placas nacionais de identificação veicular, de acordo com as regras da Resolução nº 31/2007-CONTRAN (Conselho Nacional de Trânsito), bem como das novas placas nacionais de identificação veicular, de acordo com as regras da Resolução nº 780/2019-MI/CNT, do Conselho Nacional de Trânsito - CONTRAN

O registro das placas capturadas deve ser feito em servidor em nuvem, por, pelo menos, o tempo de gravação da placa, em lista contendo informações relativas, de dados à transcrição da placa, como identificação da câmera pelo qual o veículo passou, horário e data que houve o registro, bem como o nível de confiança da leitura para todas as placas lidas por todas as câmeras que tenha a funcionalidade habilitada.

É necessário que o sistema tenha aba de busca, para localizar possíveis registros de captura importantes para a contratante. São necessários, minimamente, os seguintes campos:

- Câmeras;
- Placa;
- Início em (data e hora);
- Término em (data e hora);
- Campo de seleção com filtro de situação irregular; e
- Campo de seleção de apenas motos.

Além disso, o sistema de busca deve disponibilizar recorte da imagem da placa, caracteres descritos da leitura feita, informações relacionadas e localização.

Deverá permitir o cadastro de lista de placas em modo de lista, para notificações de placas com algum tipo de restrição, de forma que haja o imediato envio de notificação à central de controle e a aplicativos *mobile*, caso seja identificada alguma placa da lista.

Igualmente, deverá permitir integração, através de *Application Programming Interface* (API), com *software*s de órgãos de segurança do governo do estado e do governo federal.

Tempo de resposta de *delay* de visualização de, no máximo, 60 (sessenta) segundos, considerando uma conexão de dados mínima de 5 MB de *upload* de internet exclusiva, para acesso à Plataforma.

A Plataforma deve estar de acordo com o novo sistema de placas de identificação veicular da Resolução nº 780, de 26 de junho de 2019, do Conselho Nacional de Trânsito - CONTRAN.

A Plataforma ainda deve contar com o sistema de registro de veículos suspeitos, em que o usuário poderá:

- Registrar o veículo na lista, contando com as informações da placa e descrição pelo qual o veículo está cadastrado;
- Dispor de campo de descrição; e
- Dispor de campo para ativar ou desativar o alerta dessa captura também deve ter a possibilidade de excluir registros feitos.

A Plataforma deve possibilitar um sistema de notificação sobre as placas registradas na lista de placas, sendo que o alerta sobre o veículo identificado deverá ocorrer em sistema *Web* e aplicativo *Android*, com informações de nome da câmera, placa do veículo, foto e descrição.

Os registros das placas capturadas permanecem armazenados em um período mínimo de 6 meses.

Deve permitir a criação de relatórios que possibilitem filtrar e facilitar a pesquisa de determinadas detecções. Nos relatórios, são necessários os seguintes campos:

- Nome do relatório;
- Usuário solicitante;
- *Token*;
- *Status*;
- Filtro utilizado;
- Data de criação; e
- Botão de *download* do relatório.

Os filtros de pesquisa mínimos são:

- Nome do relatório;
- Placa procurada;
- Data e hora do início;
- Data e hora do término; e
- Câmeras a serem pesquisadas.

A leitura de placas veiculares deverá possibilitar a coleta de informações e dados do trânsito nas vias públicas, tais como contagem de veículos (carros de passageiros, caminhões e motos), identificação de veículo imobilizado / quebrado etc. Por meio destas informações, é possível a geração de dados estatísticos, de modo a auxiliar na gestão do trânsito do Município, através da *interface* com os sistemas utilizados para análise criminalística.

Este sistema, para identificação instantânea, via imagem, dos caracteres da placa de identificação do veículo, deverá dispor de recursos que possibilitem a detecção e identificação automática das placas e porte

dos veículos (pequenos, médios, grandes e motocicletas) que transitarem no ponto da via na qual esteja em operação.

O sistema deverá possibilitar a captura e reconhecimento de todos os tipos de placas veiculares brasileiras.

O sistema deverá distinguir, de maneira automática, o tipo de fundo da placa veicular lida, sendo ela com fundo branco ou não. Também deverá distinguir se a placa é do modelo normal ou de moto.

Deverá ser possível o armazenamento do banco de dados, contendo informações gerais para consulta cadastral dos veículos, e capturar as placas dos veículos que trafegam na via.

O sistema deverá permitir a forma de operação automática, ou seja, ser acionado e a imagem de cada veículo ser reconhecida automaticamente, sem a interferência do operador.

Deverá perceber as variações de iluminação ambiente e, automaticamente, realizar os ajustes necessários para captação otimizada das imagens.

O sistema deverá possibilitar fazer o cadastro de um veículo que se está monitorando ou importar uma lista de placas de veículos que se tem interesse em monitorar o comportamento.

O sistema deve permitir que o usuário faça o cadastro manual de placas que são consideradas alvos ou que pertencem a veículos que têm histórico de serem utilizados para fins ilícitos. Nesse cadastro manual, o usuário pode preencher características que são importantes desse alvo, classificar qual o tipo de monitoramento, configurar em quais equipamentos essa placa deve ser monitorada e quais grupos ou usuários precisam ser notificados caso essa placa tenha sido detectada em algum dos pontos de captura. A notificação de veículos monitorados pode ser enviada para um usuário específico ou para um grupo de usuários.

Um trecho monitorado é composto por pelo menos dois pontos de captura. Com base no ponto inicial e final do trecho, a solução calcula o comprimento do trecho e consulta, em bases globais, uma velocidade média de referência. Com base nessas informações, a Plataforma utiliza todas as passagens de veículos através dos dois pontos de captura para levantar estatísticas importantes sobre o fluxo de veículos desse trecho.

Algumas características são:

- Velocidade média dos veículos que estão circulando pela via;

- Veículos que passam com maior velocidade média no trecho; e
- Tempo médio que os veículos utilizam para fazer o trecho etc.

O sistema deverá possuir mapa de calor dos pontos de captura, indicando quais pontos possuem uma maior incidência de identificação de veículos que estão sendo monitorados.

Além do mapa de calor, são apresentadas outras estatísticas coletadas da base de alertas de veículos monitorados, como, por exemplo, horários, dias da semana e dias do mês que possuem uma maior incidência de veículos com restrição.

O objetivo é trazer buscas e correlações de dados de forma a prover, de maneira rápida e intuitiva, para os agentes de Segurança Pública, os pontos de captura pelos quais mais passam veículos monitorados, quais os dias da semana em que mais circulam os veículos com restrição e quais os horários do dia em que mais ocorrem eventos de veículos monitorados, e, com base nessas informações, auxiliar a montar operações policiais de maneira mais assertiva.

O sistema deverá possuir integração com os principais Sistemas de Segurança Pública brasileiros. A integração com os órgãos de Segurança Pública é ativada por convênios que poderão ser firmados com sistemas responsáveis.

O sistema deverá possibilitar o recebimento de imagens e textos dos equipamentos instalados na via, tais como radares (fixos e móveis) e câmeras de monitoramento (pública / privada).

O sistema deverá possibilitar o *link* entre as câmeras de captura de placa (LPR – *"License Plate Recognition"*) e câmeras de monitoramento, através de relacionamento entre os equipamentos, possibilitando a abertura de mosaico de visualização das imagens ao vivo da câmera responsável pela captura da placa, bem como das câmeras de monitoramento próximas à respectiva câmera.

O sistema deverá, de forma automática, exibir os dados relativos ao veículo cuja placa foi lida e identificada como alarme.

O sistema deverá, de forma automática, exibir a correlação entre os veículos, ou seja, possibilitar que, ao selecionar uma passagem, os veículos identificados anteriormente e posteriormente sejam exibidos sem necessidade de seleção, respeitando-se um intervalo de tempo predeterminado por equipamentos.

O sistema deverá possibilitar a seleção de passagens anteriores e exibir a correlação entre veículos, ou seja, possibilitar que ao selecionar uma passagem e sua respectiva placa em um determinado equipamento, identifique quais equipamentos a referida placa capturada, bem como os veículos identificados anteriormente e posteriormente sejam exibidos sem a necessidade de seleção, respeitando-se um intervalo de tempo predeterminado por equipamento.

O sistema deve possibilitar, quando do processamento de imagens (imagens recebidas e processadas diretamente na Plataforma), a identificação da cor do veículo e tipos, tais como: carro, moto, caminhão, ônibus etc.

O sistema deverá possibilitar a seleção de passagens por tipo de veículo, através de seleção de data, horário e equipamento, mesmo que a placa do veículo não tenha sido extraída (falha de leitura), possibilitando, dessa forma, a filtragem dos veículos de interesse.

O sistema deverá armazenar todas as passagens recebidas, mesmo aquelas cujas placas não foram extraídas.

O sistema deverá possibilitar a extração destacada da placa da imagem principal, para averiguação de adulteração ou identificação de má conservação da placa, possibilitando a aplicação de *zoom*, brilho e contraste para melhor visualização.

3. ATENDIMENTOS E DESPACHOS

A Solução de Atendimentos e Despachos deve ser totalmente *Web*, assim como os demais módulos da Plataforma, e fica a CONTRATADA responsável por adequar / personalizar a solução conforme as necessidades da CONTRATANTE ao longo de todo o contrato, realizando ajustes e otimizações na solução.

A CONTRATADA deverá prover os sistemas gerenciais necessários ao bom funcionamento da solução, migrando os dados e substituindo os sistemas legados da CONTRATANTE para esta nova solução, garantindo, assim, segurança, estabilidade e eficiência à operação regular da CONTRATADA e a instrumentação da gestão de recursos e pessoal.

A CONTRATADA deve elaborar projeto de adequação da solução, que deve ser aprovado pela CONTRATANTE antes da implantação da solução, levando em consideração todas as necessidades

descritas no termo de referência, utilizando sistemas de controle de acesso único, multifator e com a gestão centralizada; sendo assim, após *login* no portal, todos os módulos e sistemas devem utilizar esta autenticação para liberar o acesso às suas funcionalidades, da mesma forma como ocorre em soluções corporativas de *login* único (exemplo: *Google* e *Microsoft*, entre outros que possibilitam a utilização de diversos sistemas e ferramentas após realizar o *login* uma única vez).

A Plataforma tecnológica deve ser baseada em ambiente *cloud*, tendo todo o CORE da solução localizado na nuvem, permitindo o acesso do cliente via *interfaces Web* e via aplicativos para *smartphones*, e ainda permitindo sua integração com outras soluções localizadas fisicamente na central de comando e controle. Esta Plataforma deverá ser capaz de:

- Gerenciar forças de campo, podendo identificar, de maneira simples e fácil, a disponibilidade de todas as forças de campo de todas as localidades, por 24h por dia, 7 dias por semana;
- Possuir *interface desktop Web*, garantindo ao operador a capacidade de receber demandas, podendo registrar todos os dados necessários e, ainda, possibilitar gerenciar e despachar forças de campo;
- Possuir aplicativos para *smartphone*, permitindo que as forças de campo possam gerar demandas para a central, bem como ser destacadas para atendimento; e
- Configurar regras pré-programadas para definir o despacho de forças de campo específicas para cada tipo diferente de demanda, agilizando, assim, o processo de atendimento às necessidades.

A solução de gestão de forças e despacho deverá possuir, pelo menos, as seguintes características:

3.1. Arquitetura da Solução

- As *interfaces Web* e de aplicativo do sistema devem utilizar encriptação SSL/TLS; e
- O sistema deve definir um ID único para cada dispositivo móvel conectado.

3.2. Gerenciamento de Usuários

- O sistema deve permitir que os usuários sejam associados a um ou mais grupos;
- O sistema deve permitir que os usuários sejam associados a uma ou mais capacidades;
- O sistema deve permitir que um ou mais equipamentos sejam associados aos usuários;
- O sistema deve permitir que os usuários sejam associados a uma determinada área geográfica;
- O sistema deve permitir que os usuários sejam associados a um ou mais centros de comando / agências;

- O sistema deve permitir que os usuários dos aplicativos móveis possam ter o acesso definido a diferentes módulos e funções, permitindo uma customização variada à *interface* acessada; e
- O sistema deve permitir que os usuários sejam exibidos ou buscados com base em múltiplos atributos.

3.3. Configuração de Grupos

- O sistema deve permitir a associação de grupos a centros de controle / agências, de maneira a permitir que os centros de controle / agências possam visualizar, gerenciar e realizar ações para cada grupo.

3.4. Gerenciamento de Unidades

- O sistema deve permitir que múltiplos usuários de aplicativos móveis sejam associados a uma unidade física, como a um veículo, por exemplo;
- O sistema deve permitir a criação de unidades;
- O sistema deve permitir a adição de detalhes, como código da unidade e tipo de unidade para cada unidade criada; e
- O sistema deve permitir a associação de usuários a unidades.

3.5. Gerenciamento de Mapas

- O sistema deve permitir que sejam criados pontos de interesse nos mapas;
- O sistema deve permitir que sejam criadas cercas virtuais nos mapas; e
- Alarmes devem ser gerados com base em usuários definidos entrando ou saindo de cercas virtuais configuradas.

3.6. Incidentes

- O sistema deve permitir a configuração de diferentes tipos de incidentes que serão gerenciados a partir dele;
- Para cada tipo de incidente, deve ser possível a definição de diferentes níveis de SLA ("*Service Level Agreement*", em português Acordo de Nível de Serviço);
- Cada tipo de incidente pode ter um ou mais formulários configurados para inserção de dados; e
- Os formulários devem possuir livre configuração por parte dos usuários, não necessitando de customizações por parte do fabricante da solução.

3.7. Configurações de Regras de Despacho

- O sistema deve permitir que sejam configuradas regras de despacho automáticas para cada tipo de incidente;
- As regras devem permitir que um determinado número de usuários seja despachado automaticamente para cada tipo de incidente;
- As regras devem permitir que usuários de determinado grupo sejam despachados automaticamente para cada tipo de incidente;
- As regras devem permitir que usuários com determinada capacidade sejam despachados automaticamente para cada tipo de incidente;
- As regras devem permitir que usuários que possuam determinado tipo de equipamento sejam despachados automaticamente para cada tipo de incidente;
- As regras devem permitir que usuários em determinado tipo de unidade sejam despachados para cada tipo de incidente; e
- Cada regra de despacho deve possuir um limite predeterminado de tempo estimado de chegada para atendimento, para definição de usuários despachados.

3.8. Mensageria

- O sistema deve permitir que mensagens sejam enviadas para os usuários;
- As mensagens podem ser de texto simples, em formato de questão ou em formato de pesquisa, com múltiplas respostas possíveis;
- As mensagens podem solicitar que os usuários que a recebam possam confirmar sua localização;
- O sistema deve permitir que sejam anexados arquivos às mensagens encaminhadas;
- Referência das funcionalidades que devem estar presentes no CAD: Atendimento - Responsável pelo Atendimento; e
- Através desse módulo é possível prestar o atendimento ao cidadão, registrar e encaminhar uma ocorrência.

3.9. Das Funcionalidades Atendimento – Função Atendente

- Selecionar regiões;
- Registrar ocorrência;
- Entrar em parada administrativa;
- Sincronizar dados;

- Habilitar / Desabilitar mapa;
- Habilitar / Desabilitar sons; e
- Visualizar notificações.

3.10. Despacho – Função Despachador

- Selecionar regiões;
- Atualizar painel de incidentes;
- Atualizar painel de recursos;
- Editar registro de incidente;
- Empenhar registro de incidente;
- Redefinir registro de incidente;
- Transferir incidente;
- Solicitar apoio;
- Finalizar registro de incidente;
- Pesquisar registro de incidente;
- Definir alerta geral;
- Entrar em parada administrativa;
- Sincronizar dados;
- Habilitar / Desabilitar mapa;
- Habilitar / Desabilitar sons; e
- Visualizar notificações.

3.11. Supervisão – Função Supervisor

- Supervisionar incidentes;
- Detalhar incidente na supervisão;
- Definir região de atuação do incidente;
- Notificar operador para atuar em nova região;
- Finalizar incidente sem operador ativo;

- Pesquisar incidentes;
- Transferir incidentes;
- Atualizar painéis;
- Sincronizar dados; e
- Emitir relatórios.

3.12. Gerenciador – Função Administrador

- Manter agência;
- Manter Centros de Captação das Ocorrências; e
- Manter *Tag* de naturezas.

3.13. Administrador de Agência

- Definir nível de integração da agência;
- Manter regiões de atuação da agência; e
- Manter câmeras de região de atuação.

3.14. Administrador de CCO

- Administrar Centro de Captação de Ocorrências;
- Manter regiões de captação de ocorrências;
- Manter usuários do Centro de Captação de Ocorrências;
- Gerir incidentes por período;
- Gerir incidentes em tempo real; e
- Relatórios de despacho;

3.15. Operador de Recursos

- Manter cargos;
- Manter pessoas;
- Manter funções;

- Manter equipamentos;
- Manter equipes; e
- Gerar relatórios.

3.16. Formulário de Atendimento

- O registro de ocorrências é apresentado em janela modal, ou seja, permanece em primeiro plano obrigatório em relação às demais até que seja fechada. O sistema bloqueia as ações de fechar a janela através do comando na barra de título ou atalho de teclado, devendo o usuário, necessariamente, utilizar os comandos disponíveis.

3.17. Classificação da Chamada

- Dados do solicitante: nome, telefone e data/hora atualizados pelo sistema no momento da abertura;
- Localização da ocorrência: informar o endereço da ocorrência, lista com todas as unidades municipais previamente cadastradas, complemento, ponto de referência e tudo isto integrado com *Google Maps*;
- Dados da ocorrência: permitir a busca fonética de naturezas de incidente e busca rápida para uma palavra-chave que pertence à natureza que tipifica o incidente. Após iniciar a digitação, será exibida uma lista com as naturezas relacionadas, e dentro da lista de natureza deve ter a tipificação da ocorrência (ex.: furto se é simples ou qualificado); partes e objetos envolvidos: campo para inserir objetos como armas, veículos e pessoas, conformidade com o Banco Nacional de Mandados de Prisão, o SINARM (Sistema Nacional de Armas) e o DENATRAN (Departamento Nacional de Trânsito);
- Narrativa: a seção “Narrativa” é destinada ao registro livre das informações que não puderam ser registradas nos campos das naturezas selecionadas;
- Ocorrências semelhantes: permitir o acúmulo de mais ocorrências para o mesmo local para não gerar duplicidade;
- Observação: durante o preenchimento do registro de ocorrência, é possível executar as ações: Finalizar; Edição; Encaminhar e Continuar Edição, ou Encaminhar e Finalizar Edição dependendo da classificação à chamada;
- Ao selecionar a ação Finalizar Edição, o registro de ocorrência é finalizado e o atendente retorna ao painel de pré-atendimento. No caso do operador que acumula o perfil de atendente, a aplicação retorna para o painel de incidentes;

- Ao selecionar a ação Encaminhar e Continuar Edição, a versão corrente do registro de ocorrência é encaminhada para despacho e o registro continua aberto disponível para edição; e
- Ao selecionar a ação Encaminhar e Finalizar Edição, o registro de ocorrência é encaminhado para despacho e fechado. Então o atendente retorna ao painel de pré-atendimento. No caso do operador que acumula o perfil do atendente, a aplicação retorna para o painel de incidentes.

3.18. Empenho

- Permitir o empenho de um recurso no atendimento local a um incidente, designado a pelo menos uma região de atuação; e
- O Painel de Recursos está dividido em recursos disponíveis e contempla a lista das equipes disponíveis para empenho, com as informações de cada equipe e material disponível.

3.19. Pausa Operacional

- Permitir que equipes sejam colocadas em *status* administrativos, refeição, manutenção e outras atividades que impossibilitem de serem despachadas uma ocorrência naquele momento.

3.20. *Status* das Equipes

- Permitir que, através de um painel, visualizem-se os recursos disponíveis do painel de recursos, e monitorar o *status* atual de uma equipe posicionando o cursor do *mouse* sobre ela.

3.21. Alterar *Status* de Empenho

- Permitir a alteração manualmente do *status* de um empenho, no caso, a chegada em locais de atendimento de ocorrência, como hospital, escola, delegacia, IML etc.;
- Transferir ocorrência para outras equipes de empenho ou região de atuação;
- Solicitar apoio para empenho com mais de uma equipe por ocorrência;
- Finalizar ocorrência e redirecionar ocorrência para atualização de informações;
- Definir alerta geral; e
- Permitir ao despachador definir um registro de incidente como alerta geral.

3.22. Janela do Mapa

Exibir informações georreferenciadas sobre incidente, equipamentos e câmeras de monitoramento integradas ao *Google Maps*, habilitar e desabilitar camadas de visualização de incidentes, como equipes

disponíveis, câmeras disponíveis, equipes em atendimento, ocorrências pendentes, regiões de atuações, unidades municipais e, entre outras, informações de interesse da administração.

3.23. Escalabilidade da Plataforma

A escalabilidade tem como principal função garantir a disponibilidade de acesso à Plataforma, em situações fora da normalidade de operação da Plataforma.

A escalabilidade também deve permitir a expansão gradual da Plataforma à medida que são implantados novos componentes, funcionalidades, módulos e integrações, que forem incluídos e disponibilizados conforme descrito neste termo de referência e em seus anexos, e deve ser considerada, também, a possibilidade de aditamento do contrato conforme legislação vigente.

A Plataforma deve ser entregue com capacidade de conectar câmeras de videomonitoramento e gravação em nuvem, baseada em *cloud computing*, com capacidade de controlar e visualizar imagens de câmeras IP conectadas à internet ou câmeras analógicas conectadas a equipamentos IP e estes à internet.

Compatível com qualquer equipamento que possua RTSP ("*Real Time Streaming Protocol*") e Codec H.264 implementado.

Sistema 100% *cloud* e possuir suporte a protocolos IPv4 e IPv6.

Possuir *interface* amigável baseada em HTML5 e traduzida para, no mínimo, o Português, e com capacidade para expandir para Espanhol e Inglês.

Permitir operações simultâneas, como gravação, reprodução de vídeo, configuração do sistema, videomonitoramento ao vivo e pesquisa de imagens, sem que a execução de uma tarefa prejudique a execução da outra.

A Plataforma deve trabalhar com resoluções desde QCIF até Megapixel, porém a qualidade de imagem deve depender somente da configuração da taxa de *upload* da rede em que a câmera estiver instalada. Quanto melhor a qualidade de conexão, melhor pode ser a qualidade da imagem configurada na câmera. A velocidade de *upload* vai definir quantas câmeras poderão ser instaladas na mesma rede.

Suportar velocidade de gravação e visualização ao vivo de, no mínimo, 30 FPS por câmera, dependendo exclusivamente do *hardware* e internet.

O videomonitoramento ao vivo deve ser ilimitado, podendo monitorar câmeras em um ou mais monitores e com diversos mosaicos de tela.

Possuir mosaico automatizado, de modo que o sistema ajustará o formato da visualização da tela automaticamente, de acordo com formatos predeterminados.

Possibilitar a criação de diversos mosaicos de videomonitoramento, cada qual com configuração independente de posicionamento de câmeras.

Suportar dois ou mais monitores de vídeo selecionáveis por estação-cliente para o videomonitoramento ao vivo, permitindo monitores *touchscreen*.

Imagens ao vivo e gravadas deverão ser disponibilizadas simultaneamente para, no mínimo, 50 usuários em monitores diversos e independentes.

O sistema de reprodução de imagens deve ser baseado em recuperação utilizando faixa de data e hora (calendário), especificados pelo usuário.

Possuir linha de tempo das imagens gravadas, que deve mostrar os pontos onde existem gravação, bem como permitir a seleção do horário corrente através da linha.

O sistema deve permitir a reprodução de vídeo arquivado através do *player* de vídeo.

APIs de integração para dados e informações das câmeras.

Exportação, para meio removível, de vídeos salvos manualmente, no formato MP4.

Permitir ao usuário a execução de pesquisas em suas câmeras, por nome ou localização em mapa geográfico da região.

4. NÍVEIS DE ACESSO AO SISTEMA DE VIDEOMONITORAMENTO

Ter sistema de níveis de acesso, que dá diferentes permissões de acordo com as configurações de *login* que os usuários detêm. Caberá ao administrador da CONTRATANTE criar acessos limitados para os usuários conforme sua necessidade.

Contar com sistema de criação de grupo de usuários, com acessos a determinadas câmeras que o administrador determina, acessos para emitir alertas de emergência, ver a linha do tempo e fazer *download* de vídeos.

Possuir módulo de controle de usuário e senha com direitos diferenciados para cada usuário ou grupo de usuário, para acesso às facilidades do sistema e câmeras.

Um usuário poderá fazer parte de um ou mais grupos, recebendo as permissões referentes a todos os grupos a que pertencer.

Uma vez logado, o usuário deverá ter acesso em qualquer local do mundo, desde que não exista bloqueio de redes, sem necessidade de novo *login* ou mudança de endereçamento.

A Plataforma deverá deter um sistema de registro de eventos, para registrar todas as atividades de todos os usuários, bem como as atividades do próprio sistema.

O sistema deve permitir que o acesso aos *logins* de eventos seja feito somente pelo administrador do sistema ou por quem o administrador liberar.

Possuir limite de acessos simultâneos de um mesmo usuário. Este recurso deve existir para limitar a quantidade de *logins* simultâneos, automáticos ou não, que um determinado usuário ou grupo de usuário pode realizar no sistema com a mesma conta.

Enviar notificações e alertas de eventos para *software* de terceiros específicos e autorizados.

Possibilidade de bloquear contas de usuários do sistema; reprodução e acelerar o vídeo em: 2x, 4x, 8x.

Trabalhar com fuso horário.

5. VISUALIZAÇÃO DO SISTEMA DE VIDEOMONITORAMENTO

Possuir de mapa com, minimamente, os seguintes filtros:

a. Filtro por tipo de câmeras (LPR, PTZ, Fixa e Panorâmica);

b. Filtro por câmeras, abrindo um buscador pelo nome das câmeras;

c. Filtro por localização, abrindo buscador que possa colocar os endereços para verificar a disponibilidade de câmeras no local;

d. Filtro por sistema de *Tags*, para filtrar possíveis interesses colocados através de *Tag*; e

e. Filtro personalizado por pontos de interesses feitos por operador. Deter botão de câmeras *online* e *offline* para facilitar a busca nas câmeras.

Possibilitar criação de subcategorias de mapas, com, minimamente, a possibilidade de se destacar, no mapa, sub-regiões.

Disponibilizar lista das câmeras com, minimamente, os seguintes dados:

a. Título da câmera;

b. Número de série;

c. Tipo de câmera;

d. Integração;

e. *Status*;

f. *Tags*;

g. Data de cadastro; e

h. Função de edição de câmeras.

Deve permitir alterar as seguintes configurações na função de edição de câmeras:

a. Título da câmera;

b. Endereço;

c. Latitude;

d. Longitude; e

e. *Tags.*

Possibilitar a criação de *Tags* e a associação das *Tags* a câmeras criadas.

Dispor de criação de *Tags* para agrupar *download*s e agrupar o número de *download*s relacionados a cada *Tag*, bem como permitir a criação de novas *Tags* de *downloads*.

Ter histórico dos *download*s feitos, com, minimamente, os seguintes dados:

a. Nome do arquivo;

b. Usuário;

c. Câmera;

d. Status do *download*;

e. Criado em;

f. *Tags*; e

g. Botão para *download* do vídeo salvo.

Possibilidade de criar grupos personalizados de alerta para notificações, relacionando câmeras com usuários determinados pelo gerenciador do contrato, devendo deter seguintes dados:

a. Nome do grupo;

b. Descrição;

c. Câmeras; e

d. Configuração para silenciar notificações.

6. ACESSO INICIAL NA PÁGINA *WEB*

Equivalente à página inicial do *Google*, *Microsoft*, *Yahoo, AOL*, *GMX* e outros portais, com alguns *banners* e informações com *design* simples.

"*Login*": área de *login* com autenticação de dois fatores;

Assim que o usuário fizer *login*, ele é direcionado ao módulo a que ele pertence e, no caso de usuário com acesso a mais de um módulo, as opções de acesso aos módulos ficarão disponíveis na tela conforme suas permissões, no *app menu*.

"Cadastro": página de cadastro com validação de CEP, CPF e registro de funcionário público, e todos os cadastros devem vir do *login* único do município ou da conta .gov, bem como os dados não constantes no *login* único devem ser preenchidos para que sejam incluídos ao cadastro de usuário, criando a base de dados temática conforme legislação vigente.

6.1. Cadastro de Funcionário Público

a. Número de registro de funcionário público;

b. Entidade da Administração Pública;

c. Secretaria / Ministério;

d. Nome;

e. CPF;

f. E-mail;

g. Telefone;

h. CEP com função de buscar e completar o endereço;

i. Número do logradouro;

j. Complemento do endereço;

k. Li e aceito Termo de Uso e Política de Privacidade;

l. Li e aceito Termo de Adesão; e

m. Li e aceito Termo de Confidencialidade.

Após preencher os dados, eles devem ser validados junto à base de dados de funcionários públicos e os demais dados do registro serão preenchidos automaticamente. Caso não seja possível fazer a validação, deverá surgir um *pop up* com a seguinte informação:

"*Desculpe, servidor não encontrado. Entre em contato com seu superior e solicite o cadastro de sua equipe*".

6.2. Cadastro de Empresa

CNPJ: após validação do CNPJ, alguns dados serão preenchidos automaticamente, como nome da empresa, responsável pela empresa, telefone, e-mail e endereço da empresa.

Serão solicitados os seguintes dados:

a. CPF do funcionário (neste caso, o *id* do funcionário deve ser vinculado ao CNPJ da empresa para que o módulo integrador fique disponível ao usuário para realizar as integrações);

b. Termo de adesão da empresa integradora;

c. Quantidade de câmeras compartilhadas; e

d. Ramo de atuação da empresa.

"Sobre o Programa": destinado a explicar como funciona a Plataforma, como aderir ao programa e como solicitar imagens; abriga também o "*newsletter*";

"Denunciar Abuso": area reservada para informar mau uso da Plataforma e outros abusos.

No núcleo de acessos, todos os elementos relacionados aos acessos deve ser adicionado, criando uma aba chamada "Usuários".

6.3. Usuários

É necessário que o administrador crie ou edite as informações de um usuário, alterando os dados cadastrais, os níveis de permissão ou os grupos associados ao usuário.

Ao cadastrar um usuário, o sistema deve entregar o seguinte nível de detalhamento:

a. Nome;

b. E-mail;

c. CPF;

d. Matrícula;

e. Telefone;

f. Órgão;

g. Unidade;

h. Cargo;

i. *Tags*;

j. Apelido e

k. Patente.

Além desses itens, deve entregar a possibilidade de associar esse cadastro a um grupo de câmeras, níveis de permissão e habilidades.

Também é necessária a possibilidade de excluir usuários, para os níveis permitidos.

Deve ser possível criar e excluir *Tags* para relacionar com usuário.

7. NÍVEIS DE PERMISSÃO

Se faz necessária a criação de níveis de permissão, permitindo que o administrador edite os níveis de permissão, removendo ou acrescentando permissões:

- Permitir que o administrador crie um novo nível de permissão, adicionando usuários;
- Permitir que o administrador exclua ou desabilite um nível de permissão previamente criado;
- Permitir que o administrador controle os usuários cadastrados na Plataforma, podendo desabilitar ou excluir um usuário previamente criado;
- Permitir que o administrador crie ou edite as informações de um grupo, alterando os níveis de permissão e alertas a serem recebidos, modo de visualização às câmeras, funcionalidades disponíveis ao grupo de usuários e observação sobre o grupo;
- Desenvolver a possibilidade de o administrador criar ou editar as informações de um nível de permissão, a fim de predefinir o perfil de acesso ao sistema. Ex.: nível de permissão Administrador, Forças Policiais, Usuário, Técnico / Instalador. Tal função estabelecerá o formato de acesso ao sistema e ferramentas disponíveis para consulta;
- Permitir que o usuário tenha acesso às leituras de placas quando o nível de permissão correspondente estiver habilitado;
- Permitir ao usuário visualizar detalhes de uma placa capturada, como imagens do veículo e da placa, a câmera responsável, a data e o horário da captura e o nível de confiança da captura, quando o nível de permissão correspondente estiver habilitado;
- Permitir ao usuário visualizar detalhes adicionais de uma placa capturada, como a marca do veículo, o modelo, a cor, o tipo e a cidade de registro. Essas informações estarão disponíveis apenas para veículos incluídos no banco de dados;
- Permitir ao usuário realizar o *download* do evento de captura de placa;

- Permitir ao usuário visualizar a transmissão ao vivo da câmera que capturou a placa de um veículo;
- Permitir ao usuário visualizar uma miniatura de mapa, mostrando a localização da câmera que capturou a placa de um veículo, com a opção de dar *zoom* no mapa para reconhecimento do local; e
- Permitir ao usuário buscar por placa ou período de captura, com a opção de filtrar por câmeras, placas ou segmentar apenas por lista de placas procuradas, usando critérios como data e horário.

Nos níveis de permissão, devem-se ter, minimamente, as seguintes permissões:

7.1. Módulo Facial

- Acesso total ao módulo.

7.2. Módulo Despacho

- Acesso total ao módulo;
- Reabrir ocorrências;
- Transferir ocorrências;
- Gerenciar *Tags* de ocorrência;
- Gerenciar *Tags* de relatório;
- Gerenciar equipes da mesma unidade;
- Gerenciar equipes do mesmo órgão;
- Gerenciar órgão das ocorrências;
- Gerenciar órgão nos tipos de ocorrências;
- Gerenciar órgão nas *Tags* de ocorrências;
- Gerenciar órgão nos relatórios;
- Gerenciar órgão nas *Tags* de relatórios;
- Gerenciar equipamentos;
- Gerenciar órgão nos equipamentos;
- Gerenciar habilidades;

- Gerenciar órgão nas habilidades;
- Gerenciar funções;
- Gerenciar órgão nas funções;
- Gerenciar relações de veículo;
- Gerenciar órgão nas relações de veículo;
- Gerenciar relações de pessoa;
- Gerenciar órgão nas relações de pessoa;
- Gerenciar categorias de objetos;
- Gerenciar órgão nas categorias de objeto;
- Gerenciar nomes de equipes;
- Gerenciar órgão nos nomes de equipes;
- Gerar relatório de ocorrências;
- Baixar relatório de ocorrências;
- Gerenciar categorias de finalização;
- Gerenciar órgão nas categorias de finalização; e
- Gerenciar pausa de equipes.

7.3. Módulo Leitura de Placas

- Acesso total ao módulo;
- Editar placa de detecções;
- Módulo câmera;
- Gerenciar câmeras;
- Salvar gravações;
- Fazer *download* de gravações;

- Fazer *download* do relatório;
- Gerenciar pontos de interesse;
- Gerenciar *Tags* de câmeras;
- Gerenciar *Tags* de *download*;
- Criar requisição de manutenção;
- Criar requisição de manutenção emergencial;
- Gerenciar grupos de alerta;
- Gerar análise de vídeo; e
- Assistir análise de vídeo.

7.4. Módulo Acessos

- Gerenciar usuários;
- Gerenciar *Tags* do usuário;
- Gerenciar níveis de permissão;
- Gerenciar grupos de câmeras;
- Gerenciar acessos a catracas; e
- Editar ajustes da Plataforma.

7.5. Módulo *Dashboard*

- Acesso total ao módulo; e
- Acesso ao módulo de busca inteligente.

7.6. Módulo *Logs*

- Acesso total ao módulo;
- Módulo CRM ("*Customer Relationship Management*");
-

- Consultar senha das câmeras;
- Módulo *APP* Agente;
- Buscar pessoas por foto; e
- Receber ocorrências.

7.7. Módulo Eventos

- Acesso total ao módulo.

7.8. Grupos

Também se faz necessário atrelar usuários a grupos, que vão partilhar acessos a determinadas câmeras, selecionadas pelo administrador do grupo, e determinar permissões, dentre as quais as seguintes são obrigatórias:

- Assistir ao vivo;
- Assistir gravações;
- Mover PTZ ("*Pan-Tilt-Zoom*"), para movimentos horizontais, verticais e de aproximação;
- Visualizar detecção facial; e
- Visualizar detecções de leitura de placas.

7.9. Órgãos Municipais

Deve existir aba para cadastro de órgãos municipais e os usuários criados devem ter os seguintes dados:

a. Nome;

b. Descrição;

c. Cargos;

d. Comandos; e

e. Unidades.

7.10. Prioridade de PTZ

Sistema deve ter aba para priorizar o uso de PTZ, entregando níveis diferentes de prioridade para cada usuário, conforme controle do administrador do contrato.

8. AJUSTES DE PLATAFORMA

Também se faz necessária a criação de aba com Ajustes da Plataforma, onde os termos de uso podem ser editados, pelo administrador do contrato ou por quem ele assim permitir, e que deve contar com sistema para limitar as sessões de uso do sistema, considerando duração da sessão em minutos e limite de sessões abertas simultaneamente. Os Ajustes de Plataforma deverão ser divididos para versão de computador e versão de celular.

8.1. CRM (“*Customer Relationship Management*”)

O CRM ficará responsável pela gestão dos equipamentos ligados ao sistema, de seus *status* e condições. A seguir constam os itens imprescindíveis de serem monitorados:

8.2. Câmeras

A lista de todas as câmeras conectadas ao sistema, com, no mínimo, os seguintes itens:

a. Título;

b. Tipo de instalação (4G, Fibra, Rádio etc.);

c. Número de série;

d. Tipo (Fixa, LPR, Panorâmica etc.);

e. Integração;

f. *Status* (*Online*, *Offline*);

g. Data de cadastro;

h. Função de edição dos dados das câmeras; e

i. Função para desligar a câmera.

8.3. Central de Alarme

A lista de todas as centrais de alarme conectadas ao sistema, com, no mínimo, os seguintes itens:

a. Título;

b. Tipo de internet;

c. Número de série;

d. Data de cadastro;

e. Endereço;

f. Latitude;

g. Longitude; e

h. Tipo de rede.

8.4. Eventos de Desconexões

Deter sistema para registro e tratamento de eventos de desconexão de câmeras, em estilo *Kanban*, com, minimamente, 3 fases (Pendente, Em andamento e Concluído).

Os eventos em fase Pendente devem deter data de início e nenhum usuário atrelado ao evento.

Assim que o evento é clicado por algum agente, automaticamente o agente se torna o proprietário do evento.

Os eventos concluídos só poderão ser salvos com motivo e observações devidamente preenchidos.

Ter *status* de câmeras para câmeras *offline* e também para recepção de eventos de análise de imagem.

8.5. *LOGS*

Os registros de todas as movimentações feitas devem ser devidamente realizados e salvos, podendo ser consultados através de relatórios tanto em PDF quanto em XLSX pela administradora do contrato.

É necessário que os seguintes itens estejam disponíveis:

- Aceito os Termos de Uso;
- Adicionou foto a uma pessoa;
- Agente mudou de equipe;
- Agente se ativou na equipe;
- Assistiu mosaico;

- Atualizou a foto do usuário;
- Atualizou a placa da detecção;
- Atualizou nome de equipe;
- Atualizou Termos de Uso;
- Atualizou uma categoria no módulo facial;
- Atualizou uma pessoa no módulo facial;
- Baixou relatório de câmeras;
- Baixou vídeo;
- Buscou câmera;
- Buscou eventos (facial por foto);
- Buscou pessoas (facial por foto);
- Buscou *timeline*;
- Cadastrou categoria de finalização;
- Cadastrou nome de equipe;
- Cadastrou uma pessoa no módulo facial;
- Criou alerta no grupo;
- Criou grupo de permissão de facial;
- Criou câmera;
- Criou categoria de objeto;
- Criou central de alarme;
- Criou envolvimento com pessoa;
- Criou envolvimento com veículo;
- Criou equipamento;

- Criou equipe;
- Criou função;
- Criou grupo;
- Criou habilidade;
- Criou mosaico;
- Criou nível de permissão;
- Criou placa;
- Criou ponto de interesse;
- Criou relatório de despacho;
- Criou relatório de detecções de LPR;
- Criou relatório de *logs*;
- Criou *Tag*;
- Criou tipo de ocorrência;
- Criou uma categoria no módulo facial;
- Criou usuário;
- Deletou categoria de objeto;
- Deletou central de alarme;
- Deletou envolvimento com pessoa;
- Deletou envolvimento com veículo;
- Deletou equipe;
- Deletou subcategoria de finalização;
- Desabilitou câmera;
- Editou câmera;

- Editou categoria de finalização;
- Editou categoria de objeto;
- Editou central de alarme;
- Editou configuração de sessão;
- Editou envolvimento com pessoa;
- Editou envolvimento com veículo;
- Editou equipamento;
- Editou equipe;
- Editou função;
- Editou grupo;
- Editou habilidade;
- Editou mosaico;
- Editou nível de permissão;
- Editou órgão;
- Editou ponto de interesse;
- Editou *Tag*;
- Editou tipo de ocorrência;
- Editou usuário;
- Editou viatura;
- Equipe ativada;
- Equipe despachada;
- Equipe finalizada;
- Finalizou ocorrência;

- Gerou *download*;
- Gerou uma análise de vídeo;
- Habilitou câmera;
- *Login*;
- *Logout*;
- Mudou função do agente na equipe;
- Criou ocorrência;
- Criou título na ocorrência;
- Criou objeto na ocorrência;
- Criou pessoa na ocorrência;
- Criou veículo na ocorrência;
- Ocorrência assumida;
- Ocorrência transferida;
- Alterou título na ocorrência;
- Ocorrência criada;
- Pausou unidade;
- Removeu câmera;
- Removeu equipamento;
- Removeu foto de uma pessoa;
- Removeu grupo;
- Removeu habilidade;
- Removeu mosaico;
- Removeu nível de permissão;

- Removeu nome de equipe;
- Removeu órgão;
- Removeu *Tag*;
- Removeu tipo de ocorrência;
- Removeu uma categoria no módulo facial;
- Removeu uma pessoa no módulo facial;
- Removeu usuário;
- Reabriu ocorrência;
- Reativou time;
- Veículo ativado; e
- Veículo desativado.

8.6. *DASHBOARD*

Parte do sistema para, de maneira personalizável, ter a geração de relatórios personalizados, gráficos, rastreio de atividades e monitoramento de desempenho da Plataforma em tempo real.

8.7. Ocorrências

- Sistema deve disponibilizar mapa com mancha de calor baseado nos números de eventos gerados;
- Disponibilizar equipes totais, disponíveis e indisponíveis para duas rodas, quatro rodas e a pé, georreferenciadas no mapa;
- Também deve trazer painel com ocorrências pendentes, em atendimento, em andamento e concluídas; e
- Deve permitir filtros personalizáveis por data de criação, tipo, prioridade, *status*, tipo de ocorrência, equipes, *Tags*, órgãos, comando, assumido por, transferido por, recebido por e finalizado por.

8.8. Agentes

- Deve ter painel mostrando a quantidade de agentes *online*, *offline* e total;
- Tabela com o nome, telefone e última atualização, priorizando os *on-line*;

- Deve mostrar, no mapa, a geolocalização dos agentes; e
- Deve permitir filtros personalizáveis por usuário, telefone, órgão e unidade.

9. USO

O uso da Plataforma deve ser simples, intuitivo e trazer a função de assistente virtual para auxiliar na utilização da Plataforma, visto o grande número de funcionalidades e a constante expansão da solução, reduzindo a necessidade de repetidos treinamentos e requalificações dos usuários para operação da Plataforma, funcionando o assistente como tutorial de uso, FAQ ("*Frequently Asked Questions*" ou perguntas frequentes) e suporte, trazendo agilidade e mantendo as funções de suporte sempre à mão dos usuários.

9.1. Integrações

É desejável a realização de diversas integrações com sistemas e bases de dados, de forma que a inteligência da Plataforma será expandida gradualmente, trazendo dados, funcionalidades e interoperabilidade entre os serviços da Secretaria Municipal de Segurança Pública, 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.

9.2. *APPs*

Complementam a Plataforma, trazendo ferramentas de pesquisa, comunicação, formulários, despacho e GPS aos agentes em campo, *interface* de comunicação com agências de apoio aos serviços de urgência e emergência, ferramenta de consulta e edição de dados aos servidores 24h / 7 dias da semana e botão de pânico para pessoas em programas de proteção.

9.3. Sistemas

Deve ser possível desenvolver (moldar e implantar) sistemas (aplicações) nativamente integrados à solução (Plataforma), utilizando fluxos e blocos sem a necessidade de codificação (*No Code - Low Code*) que serão hospedados na própria solução, suprindo as necessidades de sistemas informáticos da CONTRATANTE de forma rápida, simples e flexível, possibilitando a substituição de antigos sistemas legados, trazendo

atualização, otimização e automação aos processos internos suportados pela Secretaria Municipal de Segurança Pública.

A forma de desenvolver as funcionalidades desejadas das aplicações deve ser simples, tal como a partir da utilização de um *Business Process Management* (BPM) para modelagem dos fluxos.

9.4. *Low Code* / *No Code*

A Plataforma de *NO CODE*/*LOW CODE* deverá ser utilizada para o desenvolvimento de módulos ou funcionalidades, possibilitando a absorção de processos, que atualmente são realizados manualmente ou por outros sistemas diversos utilizados pela Secretaria Municipal de Segurança Pública. Promove-se, assim, a automação de processos e fluxos internos dentro da municipalidade.

9.5. Câmeras

Serão utilizados vários modelos de câmeras, que deverão ter seus analíticos processados na Plataforma, bem como também deverão ser integrados seus analíticos existentes, para necessidades específicas da CONTRATANTE.

Deve ter relatório sobre as câmeras instaladas, por dia, total, *online*, *offline* e em quantos locais.

As câmeras devem ser separadas por tipo, entre elas Fixa, LPR, PTZ, Panorâmica ou outros modelos, todas com suas respectivas quantidades, *online* e *offline*, em números totais e em percentual, além de entregar lista das últimas câmeras instaladas, com número de série, título da câmera, *status*, tipo e data e hora do cadastro.

9.6. Programas Legados de Monitoramento

Todos os dispositivos serão integrados pela Plataforma. No caso de câmeras-legados, a responsabilidade pelo armazenamento, conectividade e manutenção pelo período de retenção das imagens será da CONTRATANTE, conforme contratos já existentes. É prevista a integração de 490 câmeras-legados.

9.7. Bases de Dados

Os dados dos usuários deverão permanecer armazenados na Plataforma até o término do contrato e devem ser transferidos, conforme indicado pela CONTRATANTE, ao término do contrato.

Os dados de operação deverão permanecer armazenados na Plataforma até o término do contrato e devem ser transferidos, conforme indicado pela CONTRATANTE, ao término do contrato.

9.7.1. Idioma: a Plataforma, toda a comunicação e o suporte devem ser em Português Brasileiro (Pt-Br) como idioma principal e, como idiomas secundários, Inglês (En-US) e Espanhol.

9.7.2. Manual: deve possuir manual de uso para a Plataforma no idioma Português Brasileiro (Pt-Br) e este deve ser atualizado sempre que houver alterações na Plataforma.

Deve possuir guia de uso rápido (*quick guide*) para operador (não relacionado à LGPD) no idioma Português Brasileiro (Pt-Br) e este deve ser atualizado sempre que houver alterações na Plataforma.

Deve possuir *tour* na Plataforma (tutorial de primeiro uso) mostrando as principais funções e mudanças que ocorram em atualizações.

10. DOCUMENTAÇÃO

Deve possuir documentação ampla da Plataforma, com histórico de atualizações e correções implementadas.

Deve ser mantida documentação detalhada e atualizada de toda a solução da Plataforma, com todos os serviços, chamados, manutenções, correções, ordens de serviço, solicitação, projetos de implantação, licenciamento e outras atividades necessárias à implantação da solução.

11. ADMINISTRAÇÃO E TRANSPARÊNCIA

A estrutura organizacional administrativa da Plataforma será regulamentada posteriormente, sendo formada pelo Conselho e Equipe Gestora da Plataforma. O Conselho ficará responsável pela tomada de decisão que gera impacto significativo na operação da Plataforma, analíticos de imagem, processamento de dados, privacidade e outros temas sensíveis e que precisam de maior atenção.

A Equipe Gestora da Plataforma será responsável pela gestão regular (administração) da Plataforma diariamente, garantindo a operação da Plataforma e o cumprimento das deliberações do Conselho.

A equipe deve, também, monitorar a Plataforma através das ferramentas destinadas a este fim, disponíveis no Módulo Gestor e através de quaisquer outras ferramentas que julgue necessárias à fiscalização e monitoramento da Plataforma e seus serviços.

12. 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 CONTRATADA deverá realizar, trimestralmente, um Relatório de Impacto à Proteção de Dados (*Data Protection Impact Assessment*), sendo 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 riscos de invasão de dados, com a análise, identificação e minimização dos riscos relacionados a incidentes de segurança.

O Relatório deverá indicar a viabilidade do tratamento de dados pretendido pela empresa, semestralmente.

A municipalidade divulgará, através de seus canais de informação, campanha de aviso prévio sobre a captura de imagens, comunicando que as câmeras realizarão a captura de imagens pela cidade.

Por se tratar de uma informação restrita, a localização das câmeras não será divulgada, tendo apenas a divulgação da captura das imagens pela cidade.

Conhecimento sobre os pontos de capturas de imagens será disponibilizado às autoridades competentes, mediante indicação do responsável pela informação e ciência do Conselho.

A CONTRATADA deverá realizar parecer detalhando o grau de detalhes capturados, bem como realizar vídeo institucional para divulgação do parecer.

Serão estabelecidos, na Política de Segurança de Dados 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; e
- Relatório contendo acessos, consentimentos, revisões e eventuais violações a tais informações.

13. TRANSPARÊNCIA

A Política de Segurança de Dados, 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 do-Órgão Colegiado.

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

Estimativa do número de usuários simultâneos da Plataforma:

MÓDULO COMPONENTE DA PLATAFORMA	QUANTIDADE DE USUÁRIOS SIMULTÂNEOS
Gestão da Plataforma	500
Operação	500
Administrativo de Operação	500
APP Agente de Campo	1.000
Web APP (PWA) Operacional Complementar	1.000
Web APP (PWA) Consulta	1.000
Veículos Monitorados (Telemetria, GPS)	1.000

PWA: "*Progressive Web App*"

14. GESTÃO DA PLATAFORMA

Representa o número máximo de usuários simultâneos do Módulo de Gestão.

14.1. Operação

Representa o número máximo de usuários simultâneos do Módulo de Operação.

14.2. Administrativo de Operação

Representa o número máximo de usuários simultâneos do Módulo Administrativo de Operação.

14.3. *APP* Agente Campo

Representa o número de agentes utilizando o *APP* Agente de Campo simultaneamente durante o trabalho.

14.4. *Web APP* Consulta

Representa o número estimado de agentes utilizando simultaneamente o *Web APP* (*site*/portal) durante o pico de uso. Durante a utilização regular, este volume não deve passar dos 10% de usuários simultâneos.

Exemplos de utilização: consulta de escala de trabalho, marcar DEAC, consultar suas informações pessoais relacionadas ao serviço ou realizar outra atividade necessária a suas atividades diárias fora do horário de serviço.

14.5. *Web APP* Operacional Complementar

Representa um grupo de usuários de suporte operacional, não necessariamente ligados à administração que opera a Plataforma, mas que possuem relação direta com a operação da agência.

Exemplo:

- Hospitais, que podem ser municipais, estaduais, federais ou privados; e
- Os agentes da PM que conduzem suspeitos à DP.

Este componente deve servir como um sistema de aviso/notificação entre a administração e os demais órgãos estaduais, federais ou outros que, através da Plataforma, possam ter destinos para conclusão dos serviços.

14.6. Veículos Monitorados (Telemetria, GPS)

Representa o número de veículos que devem ser rastreados através da Plataforma, trazendo os dados de telemetria de forma que possam ser utilizados em formulários operacionais regulares, resultando em automação e controle aos processos e possibilitando auditorias assertivas e a correção de eventuais desvios de qualquer natureza.

15. *APP* AGENTE DE CAMPO

Sobre:

Este *app* visa otimizar os processos, simplificar os trabalhos e otimizar as atividades diárias.

Com esta nova Plataforma, será possível melhorar ainda mais os trabalhos, automatizando processos e trazendo maior volume de informações de forma automática, expandindo as possibilidades de utilização do aplicativo, não só para substituir os antigos formulários, mas para suportar novas formas de Atendimento e Despacho, recebendo informações dos agentes em campo. Exemplo: GPS, fotos, vídeos e áudios.

Necessidades:

- Substituir os formulários em papel;
- Permitir a comunicação bilateral entre a central e o agente;
- Realizar a captura de imagens (fotos e vídeos) e enviar à central;
- Receber os despachos do CAD direcionados ao agente;
- Receber imagens e *streaming* de câmeras próximas à ocorrência;
- Receber rota GPS/*Waze* para a ocorrência;
- Capturar a posição GPS dos terminais;
- Identificar Agente / Equipe e recurso disponível;
- Realizar pesquisas nas bases de dados (exemplo: procurados, desaparecidos e veículos);
- Abertura e encerramento de talonário eletrônico;
- Reconhecimento facial de suspeitos através do *Smartphone*;
- Busca de placa por imagem – situação do veículo;
- Grupos de comunicação simultânea com agentes de uma agência (grupo de atendimento);

- Grupos de comunicação simultânea com agentes de múltiplas agências (grupo de atendimento); e
- Comunicação segura via *chat* com criptografia.

15.1. VoIP com Criptografia

Conseguir identificar o dispositivo (*hardware* e número de telefone) onde o usuário se autenticou.

Permitir aos agentes realizar consultas a bibliotecas, manuais, procedimentos e processos (documentos internos do Serviço Público, de acesso restrito aos servidores disponíveis na gestão de documentos).

Realizar pesquisa de boletins de ocorrência.

Buscar / validar documentos de pessoas, veículos etc.

Visualizar dispositivos próximos (exemplo: câmeras e visualizar as imagens) indicados pela central.

Buscar prontuário / histórico médico (atender às necessidades do SAMU – Serviço de Atendimento Móvel de Urgência).

15.2. Funcionalidades

A partir das necessidades apresentadas, a CONTRATADA deve desenvolver o aplicativo para *Android* e/ou *IOS* que atenda às necessidades apresentadas, de forma que novas funcionalidades possam ser incluídas quando necessário, aprimorando o aplicativo ao longo do contrato.

Deve ser possível criar novos formulários dentro do *app* através de um sistema *low code* ou *no code* a partir do qual, além da criação dos novos formulários, seja possível editar os existentes, por exemplo: criar um formulário para autuação de trânsito ou cadastro de ocorrência específica, como prontuário de atendimento médico.

Visão Geral:

O App Agente de Campo é a ferramenta móvel para a GCM realizar, em campo, a comunicação e consultas sincronizadas com a Plataforma de Atendimento e Despacho, dentre outras operações cotidianas.

O aplicativo móvel deve possibilitar a customização de quais opções e funções estarão disponíveis, com base nos direitos do usuário.

Se possuir os direitos para tal, o usuário deve poder visualizar todos os outros usuários disponíveis em um mapa, visualizar todos os incidentes, preencher formulários, trocar mensagens de texto e voz com outros usuários e enviar mensagens via o módulo de mensageria.

Usuários com direitos para tal poderão responder a despachos, sendo destacadas em formato próprio, com capacidade de atualizar a aplicação de acordo com cada passo ou ação tomada.

Usuários com direito para tal poderão reportar situações ou gerar demandas de SOS para a central de controle.

Recebimento de ocorrências e notificações da Plataforma de Atendimento e Despacho.

Registro e finalização de ocorrências.

Consultas de pessoas e veículos às bases de dados.

Consulta de ocorrência na base nacional através da integração com o SINESP – Sistema Nacional de Informaçãoes de Segurança Pública;.

Visualização, no mapa, de ocorrências em andamento e demais aplicativos *mobile* que estejam atuando na mesma região de atuação, através dos registros na Plataforma de Atendimento e Despacho.

Preencher formulários eletrônicos e preencher formulários com informação proveniente da leitura de *QR Code* e NFC ("*Near Field Communication*").

Proposta de rota traçada até o local da ocorrência, através da integração com *Waze*.

Ler *QR Code* para consulta e validação de documentos.

15.3. Controle de Acesso

O controle de acesso deve ser unificado com a Plataforma (autenticação e gestão de usuários). Validação de usuário por reconhecimento facial, deve ser possível utilizado o mesmo app para as múltiplas agencias diferenciando o que é acessado somente pelas permissões e privilégios de cada usuário sendo direcionado para direcionado para sua respectiva área (agência e funcionalidades) após o *login*.

15.4. Execução

Fica a CONTRATADA encarregada de elaborar o projeto executivo para o desenvolvimento e implantação do novo *app*, que deve ser aprovado pela CONTRATADA antes da execução, podendo existir exigências

de ajustes de *design, layout,* funcionalidade ou funcionamento, garantindo que esta solução atenderá às necessidades da CONTRATANTE.

15.4.1. Dos Analíticos e Inteligência Artificial

- **Analíticos de Detecção de Movimento Perímetro / Cerca Virtual:**

Ativar gravação e emitir alerta ao agente do monitoramento, sempre que identificar se houve algum movimento suspeito ou invasão de perímetro dentro da zona de vigilância, incluindo velocidade, tamanho ou direção do objeto, dentro da área predeterminada, a qualquer momento pelos agentes do monitoramento.

- **Analíticos de Reconhecimento Facial:**

Reconhecimento simultâneo de várias faces em um fluxo de vídeo. As imagens dos rostos são salvas com data, hora e local de acesso. Detecção de face coberta (óculos, barbas e diferentes tipos de cabelo etc.). Deve ser possível atualizar o analítico conforme necessário para aperfeiçoar a Plataforma e as capacidades de reconhecimento, conforme definido nas revisões semestrais e em outras necessidades de ajuste levantadas, que exijam ajuste ou novo treinamento do algoritmo visando conformidade, isonomia e transparência na análise das imagens.

Exemplo de utilização: cruzamento dos dados do judiciário e SSP (Secretaria de Segurança Pública) de procurados, foragidos e desaparecidos, para identificação, que deve passar pela validação de um agente em caso positivo e encaminhado ao órgão competente para que tome as medidas cabíveis.

- **Analíticos de Leitura Automática de Placas / Fluxo de Veículos:**

Reconhecimento e registro de número de placas em movimento e consulta em tempo real a banco de dados de veículos furtados / roubados através de *interface* com os sistemas utilizados para análise criminalística.

A leitura de placas veiculares deverá possibilitar a coleta de informações e dados do trânsito nas vias públicas, tais como contagem de veículos (carros de passageiros, caminhões e motos), identificação de veículo imobilizado / quebrado etc. Por meio destas informações, é possível a geração de dados estatísticos, de modo a auxiliar na gestão do trânsito do Município, através da *interface* com os sistemas utilizados para análise criminalística.

Este sistema, para identificação instantânea, via imagem, dos caracteres da placa de identificação do veículo, deverá dispor de recursos que possibilitem a detecção e identificação automática das placas e porte dos veículos (pequenos, médios, grandes e motocicletas) que transitarem no ponto da via na qual esteja em operação. O sistema deverá possibilitar a captura e reconhecimento de todos os tipos de placas veiculares brasileiras. O sistema deverá distinguir, de maneira automática, o tipo de fundo da placa veicular lida, sendo ela com fundo branco ou não. Também deverá distinguir se a placa é do modelo normal ou de moto. Deverá ser possível o armazenamento do banco de dados, contendo informações gerais para consulta cadastral dos veículos, e capturar as placas dos veículos que trafegam na via, registrando, no mínimo, os seguintes dados: data, horário, local e placa reconhecida.

O sistema deverá permitir a forma de operação automática, ou seja, ser acionado e a margem de cada veículo ser reconhecida automaticamente, sem a interferência do agente do monitoramento. Deverá perceber as variações de iluminação ambiente e, automaticamente, realizar os ajustes necessários para captação otimizada das imagens.

O sistema deverá possibilitar fazer cadastro de um veículo que se está monitorando ou importar uma lista de placas de veículos de que se tem interesse em monitorar o comportamento.

O sistema deve permitir que o usuário faça o cadastro manual de placas que são consideradas alvos ou que pertencem a veículos que têm histórico de serem utilizados para crimes. Nesse cadastro manual, o usuário pode preencher características que são importantes desse alvo, classificar qual o tipo de monitoramento, configurar em quais equipamentos essa placa deve ser monitorada e quais grupos ou usuários precisam ser notificados caso essa placa tenha sido detectada em algum dos pontos de captura. A notificação de veículos monitorados pode ser enviada para um usuário específico ou para um grupo de usuários.

Um trecho monitorado é composto por pelo menos dois pontos de captura. Com base no ponto inicial e final do trecho, a solução calcula o comprimento do trecho e consulta, em bases globais, uma velocidade média de referência. Com base nessas informações, a Plataforma utiliza todas as passagens de veículos através dos dois pontos de captura, para levantar estatísticas importantes sobre o fluxo de veículos desse trecho.

Algumas características são: a velocidade média dos veículos que estão circulando pela via, veículos que passam com maior velocidade média no trecho, tempo médio que os veículos utilizam para fazer o trecho etc.

O sistema deverá possuir mapa de calor dos pontos de captura, indicando quais pontos possuem uma maior incidência de identificação de veículos que estão sendo monitorados. Além do mapa de calor, são apresentadas outras estatísticas coletadas da base de alertas de veículos monitorados, como, por exemplo, horários, dias da semana e dias do mês que possuem uma maior incidência de veículos com restrição.

O objetivo é trazer buscas e correlações de dados de forma a prover, de maneira rápida e intuitiva, para os agentes de Segurança Pública, os pontos de captura pelos quais mais passam veículos monitorados, quais os dias da semana que mais circulam os veículos com restrição, quais os horários do dia que mais ocorrem eventos de veículos monitorados etc. E, com base nessas informações, auxiliar a montar operações policiais de maneira mais assertiva.

O sistema deverá possuir integração com os principais sistemas de Segurança Pública brasileiros. A integração com os órgãos de Segurança Pública é ativada pela SECRETARIA MUNICIPAL DE SEGURANÇA PÚBLICA mediante convênios que poderão ser firmados com sistemas, como Muralha Paulista, Cortex (Receita Federal) e SPIA-PRF (Sistema de Inteligência da PRF).

O sistema deverá possibilitar o recebimento de imagens e textos dos equipamentos instalados na via, tais como radares (fixos e móveis) e câmeras de monitoramento (publica / privada).

O sistema deverá possibilitar o *link* entre as câmeras de captura de placa (LPR/OCR) e câmeras de monitoramento através de relacionamento entre os equipamentos, possibilitando a abertura de mosaico de visualização das imagens ao vivo da câmera responsável pela captura da placa, bem como das câmeras de monitoramento próximas à respectiva câmera.

O sistema deverá, de forma automática, exibir os dados relativos ao veículo cuja placa foi lida e identificada como alarme.

O sistema deverá, de forma automática, exibir a possível rota de deslocamento feita pelo veículo, identificado os pontos de passagem, quantidade de passagens, data e horário das passagens.

O sistema deverá, de forma automática, exibir a correlação entre os veículos, ou seja, possibilitar que, ao selecionar uma passagem, os veículos identificados anteriormente e posteriormente sejam exibidos sem necessidade de seleção, respeitando-se um intervalo de tempo predeterminado por equipamentos.

O sistema deverá possibilitar a seleção de passagens anteriores e exibir a correlação entre veículos, ou seja, possibilitar que, ao selecionar uma passagem e sua respectiva placa em um determinado equipamento, identifique em quais equipamentos a referida placa foi capturada, bem como permitir que os veículos identificados anteriormente e posteriormente sejam exibidos sem a necessidade de seleção, respeitando-se um intervalo de tempo predeterminado por equipamento.
O sistema deve possibilitar, quando do processamento de imagens (imagens recebidas e processadas diretamente na Plataforma), a identificação da cor do veículo e tipos, tais como carro, moto, caminhão, ônibus etc.

O sistema deverá possibilitar a seleção de passagens por tipo de veículo, através de seleção de data, horário e equipamento, mesmo que a placa do veículo não tenha sido extraída (falha de leitura), possibilitando, dessa forma, a filtragem dos veículos de interesse.

O sistema deverá armazenar todas as passagens recebidas, mesmo aquelas cujas placas não foram extraídas.
O sistema deverá possibilitar a extração destacada da placa da imagem principal para averiguação de adulteração ou identificação de má conservação da placa, possibilitando a aplicação de *zoom*, brilho e contraste para melhor visualização dela.

15.4.2. Analíticos de Estacionamento Ilegal / Irregular

Possibilita detectar a ocupação de vagas em estacionamento ou vias públicas.

15.4.3. Analíticos de Detecção de Densidade / Concentração de Pessoas

Detectar a concentração de pessoas dentro de uma área determinada quando exceder limites predefinidos.

15.4.4. Analítico Dinâmico Baseado em Aprendizagem de Máquina:

Deverá ser possível processar e analisar imagens em tempo real e as imagens gravadas, implementando, conforme a necessidade, múltiplos analíticos simultaneamente para análise delas, otimizando o processo de análise. Os algoritmos de análise devem ser executados de forma paralela (execução simultaneamente sem fila de processos).

15.5. Desenvolvimento e Atualização:

Deverá ser possível treinar novos analíticos de imagem dotados de inteligência artificial e autoaprendizagem, de forma que sejam criados novos padrões de análise de acordo com a necessidade da contratante de analisar imagens.

15.6. Utilização dos Analíticos de Imagem:

A utilização dos analíticos visa otimizar o atendimento dos serviços de monitoramento de forma confiável, rápida e transparente, possibilitando o acionamento de diferentes órgãos para o atendimento à população, levando em conta o contexto que gerou o alerta no processo de validação realizado pelos agentes, possibilitando acionar, inclusive, a assistência social, atendimento médico, policial e zeladoria, entre outros serviços a depender do contexto analisado. Os analíticos devem passar por revisões semestrais e avaliações, com o intuito de garantir a isonomia e a análise confiável, sendo ajustados sempre que alguma inconsistência ou problema for identificado, estando sujeito a auditorias de funcionamento do analítico, com garantia à LGPD e à transparência no uso da tecnologia e nos processos que são suportados por ela. A utilização da tecnologia não substitui o processo humano de análise, planejamento e tomada de decisão, apenas possibilita a criação processos mais eficientes e transparentes.

16. INTEGRAÇÕES E INTEROPERABILIDADE

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. Fica a CONTRATADA obrigada a realizar as integrações, realizando projeto e documentação das alterações

efetuadas 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. Fica a critério da CONTRATADA disponibilizar a integração com prazo inferior aos 6 meses e fica obrigada a CONTRATADA a 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 a 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 da Prefeitura Municipal de SÃO JOSÉ DO RIO PRETO, e deverá, no prazo de 30 dias, apresentar cronograma de implantação para a CONTRATANTE. Caso a CONTRATANTE não aprove o cronograma, deverá apontar os pontos que não concorda para que a CONTRATADA retifique e o submeta novamente à aprovação em até 15 dias.

A Plataforma deve ser integrada a diferentes bases de dados, para diversas finalidades conforme "*o Sistema Único de Segurança Pública, instituído pela Lei Federal nº 13,675 no dia 11 de junho de 2018*". Serão integrados órgãos municipais, estaduais e federais, trazendo agilidade e otimizando processos.

Deve ser possível integrar o maior número de sistemas e bases de dados possíveis, 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 no território nacional. Isto deve aproximar os segmentos da sociedade de forma cooperativa e permitir 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.

16.1. Bases de Dados

- Bases de Dados das Secretarias;

- Bases de Dados RH Município;
- Bases de Dados Criminal Procurados;
- Bases de Dados Desaparecidos;
- Bases de Dados Boletins de Ocorrência;
- Bases de Dados Detran; e
- Bases de Dados Carros Roubados.

Exemplo das bases que deverão ser integradas à Plataforma para seres utilizadas na validação de usuário do tipo Servidor Público:

- RH para validação de registro funcional; e
- RH para validação do local, atividade e onde está lotado.

16.2. Sistema Único de Segurança Pública (SUSP)

Conforme a Lei Federal nº 13.675, de 11 de junho de 2018, que institui o SUSP, deve ser realizada a integração com diversos órgãos, de forma a viabilizar a cooperação ágil e desburocratizar os processos de troca de informações entre os entes.

A Plataforma *Smart* Rio Preto deve estar integrada a todos os sistemas do ecossistema do Sistema Único de Segurança Pública (SUSP) e do Sistema Nacional de Informações de Segurança Pública (Sinesp), à medida que forem implantados e se tornarem disponíveis para integração através de convênios e acordos de cooperação. A seguir estão comentados alguns dos sistemas que devem estar integrados desde o início à Plataforma *Smart* Rio Preto.

- SINESP (todos os sistemas e bases de dados disponíveis)
- CORTEX

HUB de Integração: módulo que visa simplificar os processos de integração entre sistemas e a cooperação com a sociedade.

O Módulo de Integração / Hub de Integração deve ser formado por uma API aberta com sistema de gerenciamento, ferramenta para automatizar o fluxo de dados entre sistemas de *software* e plataforma de gerenciamento de fluxo de trabalho, para *pipelines* de engenharia de dados, e deve possuir sistema de controle de acesso e gestão das integrações, criando, assim, um robusto sistema de integração autogerenciada.

O Hub de Integração é uma infraestrutura centralizada que deve atuar como um ponto de conexão para integrar sistemas, aplicativos e dados de diferentes fontes.

Ele fornece uma plataforma para permitir a comunicação, a troca de informações e o compartilhamento de recursos entre vários sistemas, aplicativos ou serviços.

O Hub de Integração deve ser considerado como uma camada intermediária entre diferentes sistemas, que permite que eles se comuniquem sem ter que se preocupar com os detalhes técnicos da integração. Ele deve facilitar a integração entre sistemas que utilizam diferentes protocolos de comunicação, formatos de dados e tecnologias de transporte.

Os principais benefícios de um Hub de Integração devem ser a capacidade de fornecer uma visão holística de todos os sistemas e processos envolvidos em uma operação, permitir gerenciar e monitorar a integração de dados em tempo real, identificar problemas rapidamente e otimizar a eficiência dos processos de negócios.

O Hub de Integração pode ser configurado para suportar diferentes padrões de integração, como mensagens assíncronas, mensagens síncronas, APIs, APIs *RESTful*, *Web Socket* e serviços da *Web*. Ele deve ser projetado para permitir diferentes níveis de interação entre os sistemas, desde a troca de informações básicas até a integração completa dos processos de negócios.

O Hub de Integração deve reduzir o tempo e o custo de desenvolvimento de soluções de integração personalizadas. Ele deve oferecer uma solução flexível e escalável para integrar novos sistemas ou serviços, bem como para atualizar ou substituir sistemas existentes.

O Hub de Integração deve fornecer recursos para gerenciar as credenciais e chaves utilizadas nas integrações. Isso deve incluir a capacidade de armazenar e gerenciar as chaves criptográficas e certificados utilizados para a autenticação e criptografia de dados.

O Hub de Integração deve fornecer recursos para gerenciar, de forma segura, as credenciais e chaves utilizadas nas integrações, garantindo a autenticação e autorização correta entre sistemas e a segurança da troca de informações. Isso deve incluir recursos para gerenciar as permissões de acesso, a criptografia de dados e a auditoria de acesso aos recursos de credenciais e chaves.

16.3. Secretarias do Município

Deve ser possível integrar todas as secretarias, autarquias e estatais do Município para absorção dos dados dos diversos órgãos, de forma a gerar uma inteligência de gestão unificada, com o máximo de dados e desempenho possível.

16.4. Integração com Drones

Deve ser possível a integração com drones e receber todas as informações transmitidas por eles, por exemplo: localização (georreferenciada), *streaming* de vídeo, imagem de câmera térmica, altitude, velocidade e qualquer outra informação disponível e que possa ser aproveitada na Plataforma.

Desta forma, se torna necessário que a Plataforma seja compatível com o protocolo RTMP ("*Real-Time Messaging Protocol*") para receber o *streaming* de vídeo de forma simples, podendo ser utilizada por outros tipos de câmeras além dos drones.

16.5. Câmeras Veiculares

Deve ser possível integrar as câmeras embarcadas nos veículos e dispositivos secundários (exemplo: radar de velocidade), receber o *streaming* de vídeo e qualquer outro dado, e utilizar as imagens e dados na Plataforma (exemplo: analisar se um dos carros à frente é roubado ou tem alguma outra pendência e notificar os agentes em caso de positivo).

16.6. Controle de Barreiras Automáticas

Deve ser possível integrar sistemas de controle de barreiras automáticas de diversos tipos, por exemplo: barreira pivotante (utilizada em acessos a pontes e avenidas que têm horários com reversão de fluxo ou restrição de horário), barreira – bloqueio de estrada *Kerbs* de elevação hidráulica (barreira que bloqueia toda a passagem, impedindo carros, e que resiste a colisões de veículos), barreira de elevação hidráulica – pino retrátil (utilizada em locais onde o acesso a veículos é restrito e liberado a pedestres, como no centro velho da cidade de SÃO JOSÉ DO RIO PRETO) e barreira para furar pneu (utilizada para forçar a parada de veículos ao furar os pneus).

16.7. Sinalização Inteligente de Trânsito

Deve ser possível a integração com as placas de sinalização de trânsito eletrônicas (letreiros) e semáforos inteligentes.

16.8. Rastreadores GPS

Deve ser possível integrar com os diversos sistemas de rastreadores GPS utilizados no mercado por locadoras de veículos e outras empresas que têm o objetivo de disponibilizar veículos a terceiros. Deve, também, ser integrado com os sistemas de Rastreadores GPS utilizados pela CONTRATANTE.

16.9. Sensores de Solo

Deve ser integrado a sensores de solo, exemplo: sensores de umidade, deslocamento, vibração, pressão e outros sensores de solo.

O uso destes sensores visa prevenir catástrofes, como as de deslizamentos em áreas de risco, permitindo a detecção antecipada e evacuação de áreas, reduzindo significativamente o número de possíveis vítimas.

16.10. Sensores de Disparo

Deve ser integrado a sensores de disparo, permitindo a detecção de disparo de armas de fogo.

16.11. Sensores Hídricos

Deve ser integrado a diversos tipos de sensores hídricos, exemplo: nível, fluxo, vazão e velocidade (mede a velocidade da água/correnteza).

16.12. Sensores de Incêndio (Fumaça e Chama)

Deve ser integrado aos sistemas de detectores de incêndio, permitindo a atuação rápida e reduzindo o número de possíveis vítimas e outros transtornos.

16.13. Radares

Deve ser possível a integração com os diversos tipos de sistemas de radar disponíveis no mercado, com o objetivo de se absorver os sistemas já instalados, trazer a informação para a operação da Plataforma e trabalhar preventivamente, detectando objetos no ar e em solo em diversas regiões e situações, por exemplo: detectando o uso não autorizado de drones que possam causar um acidente ou a invasão de privacidade.

16.14. Dispositivos *IoT*

Deve ser possível a integração de qualquer dispositivo *IoT* pelos protocolos abertos destinados a este fim, largamente utilizados no mercado, garantido compatibilidade e a expansão da Plataforma com novos dispositivos.

16.15. Estações Climáticas

Deve ser possível a integração com as estações climáticas, trazendo as informações em tempo real para a Plataforma, de forma que será possível trabalhar com a informação mais atualizada e cruzar os dados com os provenientes dos diversos sensores e trazer uma atuação mais proativa e presente do Poder Público. Exemplo: reduzindo os transtornos no período de chuvas, cruzando os dados de "previsão x estações x sensores", será possível identificar os locais de chuva rapidamente, identificar possíveis pontos de alagamento e fazer o acionamento de bombas de drenagem, ou trabalhar de outra forma, tomando as medidas necessárias para mitigar transtornos à população.

16.16. Instituto Nacional de Meteorologia (INMET)

Deve estar integrado ao Instituto Nacional de Meteorologia e trazer os dados em tempo real para a Plataforma, para serem utilizados para o cruzamento de dados e tomada de decisão.

16.17. Concessionárias de Serviços Públicos

Deve estar integrado ao sistemas da concessionária hídrica do Município e trazer as informações em tempo real, permitindo a análise e cruzamento de dados, de forma que deve ser possível analisar os problemas

hídricos e resolvê-los o mais rápido possível de maneira conjunta e, quando necessário, trazer uma solução atenuadora do problema a fim de mitigar o sofrimento da população. Por exemplo: cruzar "reclamações x Ordem de Serviço x andamento). Desta forma, será possível atenuar o sofrimento da população por falta dos serviços, trazendo alternativa ao abastecimento tradicional ou tomando outra contra medida, garantindo que seja realizado no menor prazo possível.

A integração deve ser de mão dupla e permitir o envio de dados para o sistema da concessionária, por exemplo: quando é necessário o desligamento da rede de elétrica por um acidente – quando for necessário o desligamento, ele poderá ser solicitado através da Plataforma e enviado a um agente da concessionária, o que reduzirá significativamente o tempo de reação, mantendo a comunicação ativa entre todas as partes envolvidas e aumentando a eficiência dos atendimentos. A integração também deve permitir a detecção de falhas nas redes de serviço da concessionária.

16.18. Outras Cidades

Deve ser possível a integração com uma Plataforma de mesma natureza através de uma API aberta, que possibilite a integração segura e transparente entre os sistemas, permitindo maior cooperação e inteligência na tomada de decisões.

17. INICIATIVA PRIVADA

A seguir constam alguns exemplos de possibilidades de integração a ser implantada no âmbito da concessão, com segmentos da iniciativa privada, o que trará a desburocratização e proatividade no atendimento à sociedade. Com a cooperação entre o Poder Público e iniciativa privada, será possível trazer agilidade e dinamismo a processos normalmente lentos e de pouca eficiência.
Seguem algumas das categorias de empresa com as quais se pretende realizar integração e cooperação:

- GPS – *Maps*/*Waze*;
- Empresas de Tecnologia;
- Seguradoras;

- Locadoras de Veículos;
- Transporte de Passageiros por *App*;
- Transportadoras – Logística;
- Segurança Patrimonial;
- Transporte de Valores; e
- Outras empresas que tenham interesse em compartilhar dados.

17.1. Rádio

Deve estar integrado e interoperar com as soluções de rádio-despacho existentes, recebendo todos os dados de ocorrência.

17.2. Despacho

Deve ser integrado a soluções legadas de outros órgãos/agências, sendo possível redirecionar (enviar e receber) ocorrências através da integração a outra agência, e também deve receber informações da localização da viatura, efetivo e recursos disponíveis (catálogo de recursos).

17.3. 153/156

Deve estar integrado e interoperar com a solução do 153/156 sistema SIGRC (Sistema Integrado de Gestão do Relacionamento com o Cidadão), e deve também permitir o acompanhamento em tempo real dos atendimentos em andamento.

17.4. *VoIP*/PABX

Deve estar integrado com a soluções dos diferentes órgãos, permitindo o encaminhamento entre as diferentes soluções utilizando o *VoIP* como novo padrão, e deve ser possível realizar ligações através de *softphones*, *IP phone*, estar integrado à solução de rádio-despacho e possuir a função siga-me através de *softphone*. No caso de não atendimento ou da não conexão do *softphone*, a ligação deverá ser encaminhada para um número de telefone móvel (celular).

17.5. Mapas

Deve ser interoperável com os sistemas de mapas QGIS ("Quantum GIS" - Software de Sistema de Informações Geográficas) utilizados pela Administração Pública, para criação de mapas temáticos, trazendo estas informações para a nova Plataforma, onde deve ser possível trabalhar com múltiplas camadas nos mapas e aplicar diversos filtros conforme a necessidade.

Exemplo 1: Mapa de Força (Mapa Operacional), Mapa de Risco (Áreas de Risco), Mapas Sinóticos, Mapas Geográficos, Mapas Geológicos, Mapas Topográficos e Mapas de Infraestrutura, entre outros mapas).
As informações provenientes de outras integrações também devem ser exibidas nos mapas.
Exemplo 2: Localização Semafórica, *status* e controles, localização de sensores de solo e *status*, sensores de nível e *status*, bombas e *status* e controle (bombas de água), sensores de fluxo, sensores de pressão e sensores de vazão, entre outros sensores e dispositivos necessários à administração automatizada e centralizada.

Desta forma, deve ser possível criar mapas inteligentes e dinâmicos com a informação em tempo real, o que torna a atuação dos órgãos muito mais preventiva que reativa. Isso permitirá criar planejamento de contingência e testar os modelos no simulador, que deve utilizar inteligência artificial e os dados reais provenientes da Plataforma, para avaliação dos modelos.

17.6. Detecção por Sistema Embarcado (Analítico)

Deve ser integrado aos sistemas embarcados das câmeras, sistemas de radar (incluindo velocidade veicular) e de outros dispositivos, com *Artificial Intelligence* (AI).

17.7. Segurança Privada

Deve ser possível integrar e receber dados de empresas de segurança privada, seguradoras e empresas de transporte por aplicativo, simplificando o processo de acionamento/notificação das autoridades.

17.8. Comunicação Automática de Detecção

Deve ser possível criar regras para notificação automática da unidade mais próxima de uma ocorrência, através da Plataforma, por exemplo: um carro roubado é detectado por um radar / câmera de trânsito que automaticamente envia a notificação para a viatura mais próxima e para a central.

18. ESPECIFICAÇÃO DAS CÂMERAS E POSTES

18.1. Câmeras

A.1. Todas as câmeras devem ser compatíveis com interoperabilidade ONVIF, por exemplo: ONVIF ("*Open Network Video Interface Forum*") Profile S, ONVIF Profile G, ONVIF Profile M, ONVIF Profile T, dependendo do tipo de câmera e das necessidades operacionais da CONTRATANTE, ou possuírem fluxo de vídeo RTSP para integração com a solução solicitada. Deverá haver também API, *Webhook* ou SDK aberta para integração com outras soluções.

A.2. Todas as câmeras devem possuir suporte à comunicação segura, com criptografia (TLS1.1/1.2), e suportar os protocolos (TCP/IP, UDP, ICMP, DHCP, DNS, DDNS, QoS, RTP, RTSP, RTCP, NTP, IGMP, IPv6, IPv4, HTTP e HTTPS) e compressão (H.264 e H.265), e o acesso por autenticação deve possuir controle centralizado na Plataforma. Toda a comunicação entre as câmeras e a Plataforma deve ser criptografada.

A.3. Todas as câmeras devem possuir tecnologia de checagem de pacote de dados, disponibilizando filtros como: fonte do IP, endereço de IP do alvo, tipo do protocolo, porta do alvo e da fonte.

A.4. Todas as câmeras devem ser fornecidas com suportes para poste, parede ou teto, a definir o local pela Contratante.

A.5. Todas as câmeras devem ser fornecidas com cartão SD de memória interna com pelo menos 256 GB. Esse cartão deve ser homologado pelo fabricante da câmera.

A.6. Todas as câmeras devem garantir que o equipamento não seja vulnerável à ataques de rede DDoS e *Phishing*, pelo fabricante.

A.7. Todas as câmeras devem ser capazes de garantir a segurança na atualização de *firmwares*, identificando pacotes diferentes do fabricante, permitindo somente a utilização de versões de *firmware* lançadas pelo mesmo fabricante.

A.8. Todas as câmeras devem possuir, pelo fabricante, certificação ISO 27001 válida, garantindo a integridade e segurança dos dados coletados pelos dispositivos do mesmo.

A.9. Caso o recurso de análise de vídeo descrito neste documento não esteja embarcado na câmera, deverá ser fornecida solução totalmente licenciada, com GPU ("*Graphics Processing Unit*") e processamentos necessários apresentando as mesmas características e *performance* para realizar as análises de vídeo desejadas, de modo que o operador possa obter alarmes e realizar notificações em tempo real.

A.10. As câmeras também devem possuir API aberta para integração de *software*.

Os modelos de câmeras a seguir elencados são exemplos das especificações técnicas necessárias ao desempenho das atividades da Plataforma *Smart* Rio Preto.

18.2. CÂMERA FIXA PARA FACIAL

- Imagens de alta qualidade com resolução de 4 MP;
- Tecnologia para melhoria de performance em ambientes com baixa iluminação;
- Tecnologia de compressão H.264 e ou H.265;
- Imagens nítidas contra luz de fundo forte devido à tecnologia WDR real de 140 dB;
- Resistente a água e poeira (IP67);
- Tecnologia infravermelha avançada com longo alcance de infravermelho, mínimo de 50 m;
- Compatível com 4 *streams* de vídeo;
- 30 FPS;
- Distância focal e FOV:
  - 2,8 mm, FOV horizontal 100°, FOV vertical 50º a 58°, FOV diagonal 131° a 139°; ou
  - 4 mm ou 3,6 mm, FOV horizontal 80°, FOV vertical 50º a 58°, FOV diagonal 100° a 104°; ou
  - 6 mm, FOV horizontal 60°, FOV vertical 30° a 37°, FOV diagonal 60º a 69°.
- Navegador da *Web*: *Chrome*, *Firefox*;

- Configurações de imagem: saturação, brilho, contraste, nitidez, AGC e balanço de branco ajustável pelo *software* cliente ou pelo navegador da *Web*;
- *Interface* Ethernet: 1 porta *Ethernet* RJ45 10 mbps /100 mbps;
- *Interface* de alarme: 1 entrada e 1 saída;
- Função geral: espelho, proteção por senha, máscara de privacidade, marca d'água e filtro de endereço IP;
- Consumo de energia e corrente: VDC, PoE – 36 V a 57 V;
- Fonte de alimentação: VCC (Volts de Corrente Contínua), PoE;
- Consumo de energia máximo 9 W;
- Análise de Inteligência Artificial embarcada ou externa:

  - Objeto abandonado;

  - Detecção facial minimamente com:
    - Seleção automática de *Snapshot* (define por IA o melhor *Snapshot* para análise);
    - Aprimoramento de *Snapshot*; e
    - Pelo menos 5 atributos faciais.

  - Metadados humanos minimamente com:
    - Cor de roupa superior e inferior;
    - Gênero;
    - Chapéu ou capacete; e
    - Bolsa ou mochila.

18.3. CÂMERA MÓVEL PTZ

- Imagens de alta qualidade com resolução de 4 MP;
- 45x *Zoom* óptico;
- Digital *Zoom*: 16x;
- IR: 250 m;
- Tecnologia para melhoria de *performance* em ambientes com baixa iluminação;
- Configurações de imagem: saturação, brilho, contraste, nitidez, AGC e balanço de branco ajustável pelo *software* cliente ou pelo navegador da *Web*;
- *Interface* Ethernet: 1 porta Ethernet RJ45 10 mbps /100 mbps;
- *Interface* de alarme: 5 entradas e 2 saídas;

- Função geral: espelho, proteção por senha, máscara de privacidade, marca d'água e filtro de endereço IP;
- Tecnologia de compressão H.264 e ou H.265;
- *Interface* Ethernet: 1 porta Ethernet RJ45 10 mbps /100 mbps;
- 30 FPS;
- Lente Motorizada de 4 – 175 mm;
- Distância focal e FOV:
    - Horizontal 2° a 70°, vertical 1º a 35°, FOV diagonal 3° a 68°.
- 3 *streams* de vídeo;
- Fonte de alimentação 24 VDC, 2.5 A (± 25%);
- Imagens nítidas contra luz de fundo forte devido à tecnologia WDR real de 120 dB;
- Resistente a:
    - Água e poeira (IP67);
    - Antivandalismo (IK10); e
    - Prova de raios (TVS 6000 V).
- Proteção contra surtos;
- Proteção contra transientes de tensão;
- Navegador da *Web*: *Chrome*, *Firefox*;
- Consumo de energia máximo de 30 W;
- *Shutter* Eletrônico de 1/1 s - 1/30.000 s;
- Até 300 *presets*;
- Pelo menos 8 *Tours* com até 30 *presets*;
- Análise de Inteligência Artificial embarcada ou externa:

  - Objeto abandonado; e

  - Detecção facial minimamente com:
    - Seleção automática de *Snapshot* (define por IA o melhor *Snapshot* para análise);
    - Aprimoramento de *Snapshot*; e
    - Pelo menos 5 atributos faciais.
- Metadados humanos minimamente com:
    - Cor de roupa superior e inferior;

- Gênero;
- Chapéu ou capacete; e
- Bolsa ou mochila.

18.4. CÂMERA FIXA PARA LEITURA DE PLACA

- Imagens de alta qualidade com resolução de 4 MP;
- Tecnologia para melhoria de performance em ambientes com baixa iluminação;
- Tecnologia de compressão H.264 e ou H.265;
- Imagens nítidas contra luz de fundo forte devido à tecnologia WDR real de 140 dB;
- Resistente a água e poeira (IP67), antivandalismo (IK10);
- Tecnologia infravermelha avançada com longo alcance de infravermelho, mínimo de 25 m;
- Compatível com 4 *streams* de *vídeo*;
- 30 FPS;
- Lente Motorizada de 10 – 50 mm;
- Distância focal e FOV: horizontal 9° a 40°, vertical 5º a 22°, FOV diagonal 10° a 46°;
- Navegador da *Web*: *Chrome*, *Firefox*;
- Configurações de imagem: saturação, brilho, contraste, nitidez, AGC e balanço de branco ajustável pelo *software* cliente ou pelo navegador da *Web*;
- *Interface* Ethernet: 1 porta Ethernet RJ45 10 mbps /100 mbps;
- *Interface* de alarme: 2 entradas e 2 saídas;
- Função geral: espelho, proteção por senha, máscara de privacidade, marca d'água e filtro de endereço IP;
- Consumo de energia e corrente: 15-36 VDC;
- Fonte de alimentação: VCC, PoE;
- Consumo de energia máximo 15 W;
- Detectar até duas faixas;
- Detectar veículos até 180 km/h;
- Análise de Inteligência Artificial embarcada ou externa:
  - Classificação de tipo de veículo, minimamente:
    - Moto;

- Carro;
- Ônibus; e
- Caminhão.

o Classificação de cor do veículo;

o Classificação de marca do veículo minimamente:

- Audi;
- Mercedes;
- BMW;
- Citroen;
- Chevrolet;
- Honda;
- Hyundai;
- Jeep;
- BYD;
- Peugeot;
- Renault;
- Scania; e
- Volkswagen.

o Classificação de irregularidades, minimamente:

- Excesso de velocidade;
- Contramão;
- Mudança ilegal de faixa; e
- Sem capacete.

o Classificação de estatísticas, minimamente:

- Fluxo de veículos;
- Velocidade média;
- Tipo de veículo; e
- Comprimento de filas.

18.5. Postes

Os postes a serem utilizados para a instalação das câmeras deverão seguir a especificação descrita no subtópico a seguir. Os modelos de postes a seguir relacionados são exemplos das especificações técnicas necessárias ao desempenho das atividades da Plataforma *Smart* Rio Preto.

18.6. Especificação Técnica de Infraestrutura de Instalação de Câmera em Campo

Esta especificação destina-se a orientar as linhas gerais para o fornecimento de equipamentos. Devido às especificidades de cada central e de cada aplicação, todos os itens desta especificação estão sujeitos a revisões, que podem implicar alterações, acréscimos ou exclusões. Portanto, a aplicação desta especificação não deverá ser automática, devendo sempre ser submetida à análise das áreas envolvidas antes da efetivação do fornecimento.

O ponto de câmera (PTZ ou Fixa) deverá ser instalado em coluna de aço de 8 metros, ou aproveitado um dos tipos de estrutura previstos a seguir:

- Coluna de aço de 15 metros;
- Torre de aço de 30 metros;
- Parede ou teto de imóvel ou túnel;
- Coluna ou torre existente; e
- Pórtico ou semipórtico de PMV existente.

No caso de montagem em parede de túnel, em coluna existente ou suporte de PMV, deverão ser fornecidos os suportes de fixação de câmera e armário na estrutura existente.

Os pontos de câmera poderão ter câmeras PTZ, fixas ou ambas, em quantidades e alturas variáveis para cada ponto. A quantidade e a altura destas câmeras serão previamente informadas pelo Centro Administrativo da *Smart* Rio Preto.

Toda a fiação nas estruturas de fixação (coluna, torre etc.) deverá ser interna, com derivação para a câmera e para o armário de equipamentos.

Para evitar a infiltração de água, os suportes deverão ter todos os seus orifícios devidamente tapados e vedados.

Para as câmeras em interior de túnel ou sob viadutos, a fixação será na parede (ou pilar) ou teto.

O conjunto da câmera PTZ deverá ser projetado para instalação, preferencialmente, em topo de coluna / torre, podendo, também ser instalado na lateral de coluna / torre ou em parede / teto de túnel através de simples troca de suporte.

A instalação de câmera fixa em coluna / torre ou parede / teto deverá ser na lateral da estrutura. Para instalação em suporte de PMV, a fixação deverá ser na estrutura do pórtico ou semipórtico.

Deverão ser fornecidos os conjuntos de suportes de fixação de acordo, em topo ou lateral de coluna, com braços extensores onde se fizerem necessários.

Deverá ser considerada, durante as fases de projeto e instalação, a eventual existência de interferências nos locais definidos pelo Centro Administrativo da *Smart* Rio Preto.

Deverá ser realizada a prospecção do subsolo para a localização de eventuais interferências.

O projeto de fundação dos suportes deverá ser desenvolvido levando-se em conta, para cada caso, as cargas previstas e o tipo de terreno existente no local, previamente constatados por ensaios de solo.

O projeto de fixação dos equipamentos, bem como de sua estrutura de sustentação, deverá ser à prova de folga por trepidação causada pelo tráfego, utilizando-se de expedientes tais como grampos, porcas duplas, arruelas de pressão ou travamento químico.

Deverão ser fornecidos os projetos de instalação dos equipamentos, que deverão conter, no mínimo, as seguintes informações:

- *Layout*, com a localização dos equipamentos;
- Localização exata do ponto de fixação e instalação dos equipamentos;

●Encaminhamento dos dutos da rede de comunicação;
●Encaminhamento dos dutos de rede de alimentação elétrica;
●O projeto da fundação deverá ser realizado de forma integrada com a rede de duto de alimentação elétrica e com a rede de duto de fibra óptica; e
●Cada equipamento deverá estar interligado, através de rede subterrânea de um duto de PVC de 100 mm de diâmetro, com a rede de dutos principal da RTDI, exceto nos casos de instalação em obra de arte, onde o duto deverá ser de ferro galvanizado de 50 mm de diâmetro.

Deverá ser executada a interligação entre o ponto de câmera (coluna, torre etc.) à caixa de RTD mais próxima, por meio de duto subterrâneo.

A construção deste duto deverá obedecer às mesmas especificações técnicas do Centro Administrativo da *Smart* Rio Preto, aplicáveis à construção civil de dutos, com a exigência de uma caixa subterrânea junto ao equipamento.

Sempre que a instalação do ponto de câmera causar dano ao pavimento, deverá ser executada a recomposição do piso com as mesmas características do piso original.

19. LOCAIS DE INSTALAÇÃO DAS CÂMERAS

19.1. Instalação das Câmeras

A CONTRATANTE indicará os locais a serem instaladas as câmeras, conforme seu interesse de segurança pública para cada região.
Os locais de instalação poderão ser alterados até antes da instalação.
Poderão ser utilizados os postes legados, postes das concessionárias, prédios públicos e privados, túnel e demais locais que forneçam condições para a instalação com segurança das câmeras.
A CONTRATADA providenciará a autorização do responsável do local, para a instalação.

19.2. Custo de Movimentação das Câmeras Instaladas

Deverá ser previsto um custo unitário para a alteração do local de instalação das câmeras. Esse custo deverá englobar toda a mão de obra para remoção e posterior instalação da câmera no novo local a ser indicado pela CONTRATANTE.

Só será considerada a movimentação da câmera após a sua integração na Plataforma, com transmissão de imagens e georreferenciamento do novo local.

A CONTRATANTE poderá solicitar mensalmente a alteração de local de até 50 câmeras instaladas na Plataforma.

19.3. Quantitativo de Câmeras e Cronograma de Implantação

O projeto de instalação das câmeras fica a cargo da Concessionária, que deve levar em conta os seguintes marcos:

Ano da Concessão	Percentual mínimo de implantação das câmeras
Ano 1	30%
Ano 2	60%
Ano 3	100%

19.4. Câmeras Fixas

Serão instaladas 2.000 câmeras fixas, conforme descritivo referência 1 das especificações da câmeras e postes deste Termo de Referência.

Essas câmeras serão instaladas em frente dos equipamentos públicos no local de entrada, com maior volume de trânsito de pessoas.

O local de instalação poderá ser indicado pela chefia do equipamento e aprovado pelo Centro Administrativo da *Smart* Rio Preto.

Nas coordenadas das câmeras do tipo fixas, deverão ser instaladas 2 (duas) câmeras, por ponto, onde cada câmera deverá estar direcionada para sentidos opostos, em um ângulo de 180°.

Nas coordenadas das câmeras do tipo fixas de praças e parques, deverão ser instaladas 4 (quatro) câmeras por ponto, alinhadas com os pontos cardeais, em um angulo de 90°.

19.5. Câmeras PTZ

Serão instaladas 500 câmeras PTZ, conforme descritivo das especificações da câmeras e postes deste Termo de Referência.

Essas câmeras serão instaladas nos postes previstos, referência B das especificações da câmeras e postes deste Termo de Referência, mas poderão ser dispostas em postes já instalados, postes das concessionárias e imóveis, mediante autorização do local.

19.6. Câmeras LPR/OCR

Serão instaladas 500 câmeras LPR/OCR, conforme descritivo das especificações da câmeras e postes deste Termo de Referência.

Essas câmeras serão instaladas com direcionamento para as vias, sendo posicionadas para ler, no mínimo, 2 faixas da via.

19.7. Localização das Câmeras

A localização das câmeras integrantes da *Smart* Rio Preto deverá ser decorrente de projeto a ser elaborado pela CONTRATADA, a ser aprovado pela CONTRATANTE, e deverá ser mantido cadastro atualizado com as coordenadas de cada câmera.

19.8. Pontos de Fixação e Postes

A CONTRATANTE deverá utilizar pontos da estrutura já existentes sempre que cabível, tais como torres, postes, suportes e paredes, conforme projeto de instalação da câmera.

Todas as outras câmeras poderão usar a estrutura existente conforme projeto de instalação das câmeras, definido pela CONTRATANTE

Nos processos de mudança de local das câmeras, no projeto poderá se acrescentar ou suprimir o uso dos postes, conforme a necessidade do local.

A prioridade é que se instalem câmeras utilizando a estrutura existente. Só será instalado um poste quando não existir outra estrutura que viabilize a visada para a captura das imagens pretendidas.

20. CENTRO DE CONTROLE OPERACIONAL

20.1. Unidade a Ser Implantada

Toda a estrutura edificada, incluindo mobiliário, equipamentos e infraestrutura do local descrita neste anexo, são de responsabilidade da CONTRATADA.

Deverá ser apresentado um projeto antes da execução, para análise e aprovação da CONTRATANTE.

A CONTRATANTE poderá indicar áreas alternativas para a escolha do Centro de Controle Operacional, sendo que a CONTRATADA deverá elaborar projeto com *design* funcional, amplo, moderno e confortável, de acordo com as melhores técnicas, mantendo o Centro Operacional sempre atualizado tecnologicamente e atendendo às necessidades em constante mudança de uma cidade inteligente.

Todas as estações de trabalho e monitoramento devem ser entregues completas, com todos os acessórios, periféricos e *software*s necessários devidamente licenciados. As estações devem vir completas com todos os sistemas/*suite* de escritório. Por exemplo: sistema operacional, *Office*, *mouse*, *mousepad*, teclado e *headset.*

O mobiliário será todo de responsabilidade da CONTRATADA, devendo apresentar projeto antes da execução.

20.2. Ambientes

20.2.1. Centro Operacional

Conjunto que deverá ser montado no local especificado pela contratante, com as especificações mínimas para este serviço apresentadas a seguir, e deve se levar em conta as necessidades para a operacionalização deste centro de monitoramento, necessário para a operação de monitoramento, onde a operação conjunta entre os diversos órgãos será realizada. Deve possuir, em anexo, copa, sala de descompressão e sala de situação. Todos os sistemas devem possuir sistema de alimentação de energia elétrica secundário.

Este Centro de Monitoramento deve possuir os seguintes itens:

- 01 (um) *videowall* tipo A com área visual mínima de 25 metros quadrados, com suporte de fixação e painel de acabamento;

- 15 (quinze) estações de monitoramento tipo A;
- 15 (quinze) consoles de operação;
- 15 (quinze) cadeiras trabalho; e
- 01 (um) sistema de sonorização tipo A.

20.2.1.1. Copa

A montagem será de responsabilidade da CONTRATADA, devendo apresentar projeto antes da execução. Deve ser montada em local pertencente ao prédio do Centro de Monitoramento.

Os itens que comporão a copa serão:

- 1 mesa copa;
- 02 armários baixos 2 portas;
- 02 armários altos fechados 2 portas;
- 02 armários extra altos fechados 2 portas;
- 1 geladeira;
- 1 micro-ondas; e
- 01 purificador de água.

20.2.1.2. Sala de Contingência e Estratégia

A sala de deverá ser montada em sala anexa ao Centro de Monitoramento, com as especificações mínimas para este serviço apresentadas a seguir, e deve se levar em conta as necessidades para a operacionalização.

A sala deverá ser composta por:

- 01 (um) *videowall* tipo 2;
- 01 (um) sistema de sonorização – tipo 2;

- 01 (uma) estação de monitoramento Tipo A;
- 01 (um) console de operação;
- 01 (uma) mesa de reunião;
- 01 (dois) sofás de 5 lugares; e
- 08 (oito) cadeiras de trabalho.

20.3. Equipamentos

20.3.1. *Vídeowall* – Tipo A

Especificação técnica de *hardware*:

- Painel em LED *indoor* com pixel *pitch* de 1,25 mm;
- Projetado para operação 24 horas por dia, 7 dias por semana, com sistema de alimentação interno redundante;
- Resolução mínima do conjunto: 11.520 x 2.160 pixels;
- Acesso de manutenção frontal;
- Configuração dos *pixels*: 3 em 1 (1 vermelho, 1 verde, 1 azul);
- Relação de aspecto de cada gabinete: 16:9;
- Ângulo de visão horizontal (H) e vertical (V): 160º H e 160º V, taxa de atualização: 3.840 Hz;
- Brilho de 800 cd/m^2, contraste de 5.000:1;
- Cores do *display*: 4,39 trilhões – 14 bits, espaço de cor: 97% NTSC ("*National Television System Committee*");
- Tempo mínimo de vida útil do painel de 100.000 horas;
- Umidade de operação 20-70% *non-condensing*, temperatura operacional: 0 ºC a 40 ºC;
- Sistema de alimentação 100-240 VAC – 60 Hz, gabinetes fabricados em alumínio;
- Fator de Proteção IP30;
- Deve ser fornecido com pelo menos três processadores em LED em que cada um possua suporte à resolução 4K 60 Hz, HDR10 e pelo menos as seguintes entradas gráficas: uma HDMI 2.0, uma *DisplayPort* 1.2 e duas DVI-D;

- Deve possuir, no mínimo, as seguintes certificações: CE (incluindo EMC), FCC ("Federal *Communications Commission*"), IC; CB, cULus/cCSAus/cETLus("*Underwriters Laboratories*" do grupo CSA e "*Intertek Testing*") cTUVus e RCM;
- Deve ser fornecida estrutura metálica sob medida, em estrutura de piso com painel de acabamento em ACM ("*Aluminum Composite Material*") revestindo toda a estrutura metálica;
- A estrutura mecânica deverá permitir perfeito encaixe, nivelamento e alinhamento (horizontal, vertical e de profundidade) entre os módulos LED;
- Deverá possibilitar o gerenciamento e monitoramento de todos os módulos que compõem o sistema, através de *software* remotamente;
- O conjunto de módulos deverá ser tratado como um *display* lógico único em ambiente gráfico; e
- O equipamento deverá ser entregue instalado e licenciado. Deverão ser fornecidos todos os cabos, manuais e acessórios e nenhuma instalação ficará aparente.

20.3.2. Sistema de Gerenciamento Gráfico

Deve possuir as seguintes características mínimas:

O sistema de gerenciamento gráfico deve ser fornecido completo, com todos os recursos de *hardware* e *software* básicos (sistema operacional) e suas respectivas licenças necessárias para operar.

A arquitetura do sistema deverá ser com gerenciamento gráfico distribuído, em que o sistema gerenciador de imagens é composto por um grupo de módulos do mesmo fabricante, funcionando em conjunto para distribuir o processamento e disponibilizar imagens para o *videowall*. O protocolo de comunicação utilizado para o ambiente de rede será o TCP/IP. Todas as conexões com outras máquinas, tais como microcomputadores tipo PC, *workstations* etc., deverão utilizar este protocolo de comunicação.

A estação de trabalho do agente deverá enviar os sinais em formato digital ao *videowall* através de *encoders* de vídeo com conexões no padrão DVI ou HDMI ou *Display Port* fornecidos na solução e demais componentes, sem perdas de qualidade ou interferências nos cabos e conectores. Para distâncias superiores a cinco metros entre a estação de trabalho e o *encoder* de vídeo, deverão ser utilizados cabos de fibra óptica para conexão entre os dispositivos.

Solução Gerenciador Gráfico – Arquitetura de Processamento Distribuído:

O Sistema de Gerenciamento Gráfico deve ser fornecido completo, com todos os recursos de *hardware* e *software* básicos (sistema operacional e outros) e suas respectivas licenças necessárias para a perfeita operação dos painéis gráficos de visualização.

A arquitetura do sistema deverá ser com processamento distribuído, em que o sistema gerenciador de imagens é composto por um grupo de módulos funcionando em conjunto para distribuir o processamento e disponibilizar imagens para o *videowall*. Não serão aceitos sistemas de gerenciamento gráfico com topologia centralizada.

O protocolo de comunicação utilizado para o ambiente de rede será o TCP/IP. Todas as conexões com outras máquinas, tais como microcomputadores tipo PC, *workstations* etc., deverão utilizar este protocolo de comunicação, salvo as fontes com entrada através das *interfaces* DVI ou HDMI que deverão ser devidamente cabeadas até os processadores ou aos dispositivos de codificação de vídeo (*encoders*).

O sistema de gerenciamento do painel gráfico deve ser composto de módulos e deve permitir o controle único do sistema por somente uma *interface* de acesso e/ou controle, se comportando como um único elemento ou sistema.

Deverão ser fornecidas, no mínimo, 12 entradas de vídeo digital físicas, através de *encoders* com conexão DVI ou HDMI ou *Display Port*, para captura de imagens digitais provenientes das estações de trabalho em cada *videowall*.

Cada gerenciador de imagem distribuído, denominado nó de processamento, deverá possuir, no mínimo, duas *interfaces* gráficas com saídas DVI-D ou HDMI ou *DisplayPort* em resolução de 1.920 x 1.080 *pixels* em cada saída gráfica.

Cada módulo deve possuir *interface* de rede Ethernet 1000 Mbps – Conector RJ-45.

Suporte nativo aos formatos de vídeo MPEG2 e H.264.

O *hardware* do processador gráfico deve ser fornecido em chassis, com possibilidade de fixação em *rack* padrão 19” para uso 24 horas x 7 dias por semana.

Deve permitir operação em regime contínuo (7 dias/semana x 24 horas).

Todos os *encoders* de vídeo DVI ou HDMI ou *Display Port* deverão ser codificados na resolução mínima de 1.920 x 1.080 *pixels*, disponibilizando o seu conteúdo na rede *Gigabit* em protocolo de compressão H.264 via RTSP, garantindo baixo consumo de banda, baixa latência e alta qualidade de exibição, tornando-os disponíveis para compartilhamento, via rede, com outros *videowalls*.

As ferramentas de *software* devem permitir a captura de telas, no mínimo, nos sistemas operacionais *Microsoft Windows*.

Cada gerenciador de imagem distribuído deve ser capaz de exibir, simultaneamente, pelo menos 08 fluxos de vídeo distintos em *Full HD* (1.920 x 1.080) e 30 (trinta) *frames* (quadros) por segundo no padrão H.264 via *Real Time Streaming Protocol* (RTSP).

Cada gerenciador de imagem distribuído deve ser capaz de exibir os seguintes tipos de fontes em qualquer combinação no *videowall*: RTSP e *Remote Desktop* (RDP).

Virtual Networking *Computing* (VNC), fluxos de vídeo formato H264 e *encoder* de vídeo.

O sistema de gerenciamento gráfico deve ser fornecido com pelo menos 06 (seis) módulos gráficos distribuídos, para conexão com os processadores do painel em LED.

20.3.3. *Software* de Gerenciamento Gráfico

Deve possuir as seguintes características mínimas:

Sistema de Colaboração e Gerenciamento do *videowall*.

O sistema de colaboração deverá ser compatível com arquitetura de servidor e com ambiente virtualizado.

O sistema deverá integrar, gerenciar e controlar conteúdos (vídeos e imagens) no painel de *videowall*.

Deverá ser fornecido um único *software* de gerenciamento e visualização para a operação do sistema, com capacidade de colaboração entre usuários e o painel.

As ferramentas de *software* deverão controlar o conteúdo a ser exibido nos painéis de *videowall*.

Deverá ser possível a exibição de imagens oriundas de câmeras IP no painel de *videowall*.

As imagens capturadas deverão ser exibidas no painel de *videowall* em taxa mínima de 30 (trinta) *frames* (quadros) por segundo.

O *software* de controle deverá possibilitar o acesso e controle remoto de suas funcionalidades por um ou mais agente de modo simultâneo, através da rede local ou através de uma rede remota LAN ou WAN.

O sistema de colaboração deverá ser fornecido acompanhado das respectivas licenças perpétuas com direito de uso permanente, que sejam necessárias à execução das tarefas, e aplicativos descritos e/ou que sejam disponibilizados pela solução ofertada.

A ferramenta deverá criar, no painel *videowall,* uma área de trabalho única, onde diversas imagens possam ser executadas, livremente posicionadas e redimensionadas.

Deverá permitir criar, salvar e carregar perspectivas (conjunto de fontes de vídeo).

Deverá permitir a operação remota do *videowall* a partir de teclado e *mouse* das estações de trabalho simultâneas, através da conexão LAN/WAN.

Deverá permitir, aos usuários, privilégios diferenciados. Isto é, deverá permitir multiusuários, com permissões de utilização diferenciadas para cada usuário ou grupo de usuários através de senha.

O *software* deverá ser compatível com Modo de Aplicação de Diretório Ativo (*Active Directory Application Mode* – ADAM) ou LDAP.

O *software* deverá ser compatível com Interface Programável de Aplicativos (API), para a visualização e geração de alarmes de diferentes aplicativos, com funções pré-programadas de sequenciamento de ações.

O *software* de colaboração deverá permitir que cada usuário ou grupo de usuários tenha permissão de visualizar somente determinadas fontes definidas pelo administrador do sistema (câmeras ou aplicativos).

O *software* de colaboração deverá permitir que cada usuário ou grupo de usuários tenha permissão de exibir as fontes preestabelecidas no *videowall*.

O *software* deve possuir *interface* gráfica amigável, com comandos, entre outros, do tipo arrastar e soltar.

O sistema de colaboração deverá prever funcionalidade para o compartilhamento de conteúdo com o *videowall*, permitindo aos usuários, mediante níveis de permissões, receber imagens, capturas remotas, *streaming* de vídeo e também compartilhar informações, através de simples ação de "arrastar e soltar" (*Drag & Drop*) e utilizando a infraestrutura de rede TCP/IP, com renderização preferencialmente no *videowall*.

A ferramenta deverá permitir que cada agente envie o conteúdo completo de seu *desktop*, ou de uma aplicação ativa nele em execução, através de captura por TCP/IP (*cropping*), a uma janela independente no *videowall*.

Deverá possuir pré-visualização, nas estações de trabalho, de fontes de imagens, e também das informações exibidas no *videowall*.

Os usuários poderão ter acesso a um *menu* de atalhos diretamente no aplicativo instalado em sua estação de trabalho, de maneira a permitir rápido acesso a aplicativos.

20.3.4. *Switch* Gigabit Ethernet L3 24 Portas

- Deve possuir as seguintes características mínimas: 02 SFP *Slots* Combo 100/1000 mbps;
- 01 porta console;
- Deve suportar IEEE802.1q com grupos VLAN de 4K e VIDs de 4K;
- Protocolos necessários mínimos: IEEE 802.3i, IEEE 802.3u, IEEE 802.3ab e IEEE802.3z;

- Alimentação 100-240 V;
- 24 portas Ethernet 10/100/1000 mbps. 04 portas *uplink* 1 Gbps;
- Gerenciável *Layer* 3;
- Deve permitir empilhamento (*stacking*) de até 08 unidades, de forma que a gerência seja centralizada como uma única unidade;
- Largura de banda em *stacking*: 80 Gbps;
- Suporte nativo a *Protocol-Independent Multicast* (PIM), incluindo *Sparse Mode* (PIM-SM) e *Source-Specific Multicast* (SSM);
- IGMP v1, v2, v3;
- IGMP *Querier* IGMP *snooping*; e
- Capacidade de encaminhamentos pacotes: 95 Mpps, capacidade de comutação mínima: 128 Gbps

20.3.5. *Rack* para Instalação de Equipamentos

Deve possuir as seguintes características mínimas:

- *Rack* (UR) de altura compatível com os equipamentos;
- *Rack* fechado com portas no frontal e na traseira. Acabamento cor preta;
- Placas laterais e traseira removíveis por fecho rápido e porta em aço com fechadura e vidro temperado;
- Placas laterais e traseira removíveis;
- Bandejas fixas e móveis em número suficiente à acomodação de todos os equipamentos ofertados, que pertençam ao padrão 19";
- Painéis frontais cegos, para os espaços vagos, em aço e com acabamento em preto;
- Calhas de tomadas com 8 tomadas e cabo com 2,5 m, suficientes para alimentação dos equipamentos;
- Passa-cabos com tampa encaixável, construído em aço e com acabamento preto; e
- *Kit* de fixação, composto por: porca gaiola M5, parafuso *Phillips* M5x15 e arruelas lisas M5, suficientes para todos os equipamentos e acessórios do *rack*.

20.4. Instalação dos Equipamentos

Os equipamentos deverão ser entregues instalados e licenciados.

Deverão ser fornecidos todos os cabos, manuais e acessórios para a instalação dos equipamentos.

Não serão aceitas emendas desnecessárias e/ou realizadas que não sejam recomendação do fabricante envolvido na atualização ofertada.

Nenhuma instalação deverá ficar aparente ou atrapalhando a visualização das imagens projetadas.

A instalação e o suporte técnico deverão ser realizados por técnicos certificados pelo fabricante.

Deverá ser realizado o alinhamento geométrico, cores e brilho após a atualização dos componentes.

20.4.1. <u>Videowall</u> – Tipo B

O equipamento será composto por monitor profissional de 86” para *videowall*.

Os monitor deve possuir as seguintes características:

- Tecnologia ADS, IPS ou LED;
- Projetado para operação 24 horas por dia, 7 dias por semana, com fonte de alimentação confiável;
- Resolução mínima *Ultra HD* (3.840 x 2.160), tratamento antirreflexo;
- Tempo de resposta máxima: 8 ms. Relação de aspecto 16:9;
- Taxa de atualização: 60 Hz;
- Luminância de 500 cd/m^2 (valor típico), contraste típico de 1.200:1;
- Tempo mínimo de vida útil do painel *backlight* de 50.000 horas;
- Diagonal tela ativa de 98 polegadas;
- Entrada HDMI (ver. HDCP): 3 HDMI1/HDMI2: HDCP 2.2/1.4 HDMI3: HDCP 1.4;
- Saída HDMI: 1;
- Entrada RJ45 (LAN): 1;
- Saída de áudio: 1;
- Entrada de áudio: 1;
- Entrada USB: 1 USB 2.0 tipo A;
- Umidade de operação 20-80%;
- Temperatura de operação: 10 a 40 °C; e
- Sistema de fontes de alimentação 100-240 VAC – 60 Hz.

Deve ser fornecida estrutura metálica sob medida de acordo com o arranjo do *videowall*.

A estrutura mecânica deverá permitir perfeito encaixe, nivelamento e alinhamento (horizontal, vertical e de profundidade).

Deverá ser fornecido SISTEMA DE GERENCIAMENTO GRÁFICO para todos os ambientes previstos neste termo de referência, adequando a quantidade de módulos para que cada *videowall* possa operar na sua resolução nativa total, e possuir pelo menos quatro entradas de vídeo digital físicas (HDMI, DVI ou *Display Port*).

Os equipamentos deverão ser entregues instalados e licenciados. Deverão ser fornecidos todos os cabos, manuais e acessórios e nenhuma instalação ficará aparente.

As fontes externas e redundantes dos monitores deverão ser instaladas próximas ao *videowall*, em local de fácil acesso a ser estabelecido no *workstatement.Supervisor Station*

Deverão ser fornecidos todos os cabos, manuais e acessórios para a instalação dos equipamentos.

Não serão aceitas emendas desnecessárias e/ou realizadas que não sejam recomendação do fabricante envolvido na atualização ofertada.

Nenhuma instalação deverá ficar aparente ou atrapalhando a visualização das imagens projetadas.

A instalação e o suporte técnico deverão ser realizados por técnicos certificados pelo fabricante.

Deverá ser realizado o alinhamento geométrico, cores e brilho após a atualização dos componentes.

20.4.2. Estação de Monitoramento – Tipo A

As estações de monitoramento devem ser compostas por 01 (um) computador com capacidade necessária para o monitoramento, operações integradas de despacho, gerenciamento de equipamentos e alertas, e 01 monitor com suporte articulado fixado na mesa.

Os equipamentos devem possuir 01 (um) *headset* e 01 (uma) mesa controladora com *joystick* para câmeras PTZ.

Os equipamentos devem possuir sistema de alimentação de energia elétrica secundário.

Os equipamentos utilizados devem sempre estar atualizados para atender às necessidades da CONTRATANTE, sofrendo *upgrades* e sendo substituídos, se necessário for, para atender às demandas operacionais da CONTRATANTE.

20.4.3. Computador

Seguem os requisitos mínimos:

- Monitor: 49 polegadas *ultrawide* curvo IPS, resolução: 5.120 x 1.440 / 32:9;
- Processador: 3.6 Ghz - 4.6 Ghz - 8 cores 16 *threads*;
- Memória ram: 32 GB 3200 mhz;
- Placa de vídeo: deve possuir conexão suficiente para conectar o monitor e possuir memória e processamento para a operação da Plataforma e dos sistemas sem travamentos, sem *delay* ou qualquer outro problema proveniente do processamento de imagens, gráficos e modelos 3D complexos; e
- Rede: deve possuir placa de rede redundante de 1 Gbps ou superior.

20.4.5. *Headset*

- Tipo: Circumaural;
- Sensibilidade do *driver* a 1 kHz 1 mW (dB): 100, resposta de frequência dinâmica: 20 Hz - 20 kHz, impedância de entrada (ohms): 32;
- Resposta de frequência (passivo): 20 Hz – 20 kHz, microfone integrado: sim.

20.4.6. Mesa Controladora com *Joystick* para Câmeras PTZ

As *interfaces* e protocolos de comunicação para controle devem ser suportados pela Plataforma e controladora de PTZ, assim como toda solução apresentada.

20.4.7. Infraestrutura

A infraestrutura deve ser redundante, eliminando os pontos únicos de falhas, e de alto desempenho, atendendo às necessidades da CONTRATANTE.

20.5. Estação de Trabalho

As estações de trabalho devem ser compostas por 01 (um) computador, com capacidade necessária para o monitoramento, gerenciamento de equipamentos e alertas, e 01 (um) monitor com suporte articulado fixado na mesa.

Os equipamentos devem possuir 01 (um) *headset*.

Os equipamentos devem possuir sistema de alimentação de energia elétrica secundário.

Os equipamentos utilizados devem sempre estar atualizados para atender às necessidades da CONTRATANTE, sofrendo *upgrades* e sendo substituídos, se necessário for, para atender às demandas operacionais da CONTRATANTE.

20.5.1. Computador

Seguem os requisitos mínimos:

- Monitor: 49 polegadas *ultrawide* curvo IPS, resolução: 5.120 x 1.440 / 32:9;
- Processador: 3.6 Ghz - 4.6 Ghz - 8 cores 16 *threads*;
- Memória ram: 32 GB 3200 mhz;
- Placa de vídeo: deve possuir conexões suficientes para conectar os monitores, possuir memória e processamento para a operação da Plataforma e dos sistemas sem travamentos, sem *delay* ou qualquer outro problema proveniente do processamento de imagens, gráficos e modelos 3D complexos;
- Rede: deve possuir placa de rede redundante de 1 Gbps ou superior;
- *Headset*: tipo Circumaural;
- Sensibilidade do *Driver* a 1 kHz 1 mW (dB): 100;
- Resposta de frequência dinâmica: 20 Hz - 20 kHz, impedância de entrada (ohms): 32; e
- Resposta de frequência (passivo): 20 Hz – 20 kHz, microfone integrado: sim.

20.5.2. Infraestrutura

A infraestrutura deve ser redundante, eliminando os pontos únicos de falhas, e de alto desempenho, atendendo às necessidades da CONTRATANTE.

Sistema de Sonorização Tipo A.

Deve possuir as seguintes características:

- 04 caixas acústicas do tipo *array*, sistema de alto-falantes *line array*, formato de coluna;
- Deve possuir, no mínimo, 12 alto-falantes de, no mínimo, 02 polegadas, cobertura horizontal de 140° e vertical de 15°;
- Potência mínima de 300 Watts;
- SPL de 113 dB;
- Resposta de frequência de 100 Hz – 16 kHz;

- Cor preta; e
- Acompanhar suporte de parede.

20.6. Amplificador Multicanal

Deve possuir as seguintes características:

04 canais de amplificação independentes; potência de saída em 4 ohms: 700 W por canal; potência de saída em 8 ohms: 700 W por canal; capacidade de trabalhar a 2 ohms.

Capacidade de fazer ponte (*bridge*) entre até dois canais de amplificação. Proteções contra curto-circuito nos canais de saída.

THD máximo: 1%.

Resposta em frequência: 20 Hz a 20 kHz.

Deve possuir *interface* de rede Ethernet para gerência e controle.

Display e botões no painel frontal para configuração e informações de *status* do equipamento.

20.7. Sistema de Sonorização – TIPO B

Deve possuir as seguintes características:

- 02 caixas acústicas de sobrepor;
- Sistema de alto-falantes *line array*, formato de coluna;
- Deve possuir, no mínimo, 04 alto-falantes de 2,5 polegadas;
- Cobertura horizontal de 140° e vertical de 30°, potência mínima de 60 Watts;
- SPL de 105 dB;
- Resposta de frequência de 120 Hz – 19 kHz;
- Cor preta; e
- Acompanhar suporte de prede

20.8. Amplificador de Áudio

Deve possuir as seguintes características:

- 02 canais de amplificação independentes;
- Potência de saída em 4 ohms: 190 W por canal;
- Potência de saída em 8 ohms: 190 W por canal;

- Potência de saída em 70 V: 300 W; e
- Resposta em frequência: 20 Hz a 20 kHz Classe D.

20.9. Mobiliário Geral

Todo mobiliário deverá seguir as seguintes especificações mínimas:

20.9.1. Consoles de Operação

- Montagem por módulos sparados, com a base para fixação dos monitores em trilhos de alumínio horizontais, aos quais pode-se montar *slatwalls*;
- Medidas de cada módulo: largura 1.400 mm, profundidade 800 mm. Montagem totalmente modular, com *design* para acoplamentos laterais. Travessas e braços de apoio fabricados em aço de 2,0 mm;
- Calhas de cablagem unificadas no compartimento inferior;
- Perfil traseiro fabricado em alumínio extrudado, para fixação de suportes de monitores e acessórios;
- Pés estruturais retangulares, fabricados em chapa de aço de 2,0 mm, com reforço interno e parafusos niveladores;
- Tampo ultrarresistente fabricado em aglomerado de 25,0 mm, com revestimento em laminado melamínico de alta pressão, com bordas em PVC de 2,0 mm e encabeçamento frontal com *postforming*;
- Opção de tampos bipartidos, com acesso para cabos na parte posterior da mesa;
- Compartimento inferior com fechamentos frontal e traseiro fabricados em chapa de aço de 1,0 mm, com fechos rápidos;
- Capacidade estática dos tampos de até 150 kg. Altura do tampo: 760 mm;
- Suporte de monitor, para fixação em painel de alumínio *slatwall* para monitores;
- Laterais *office* fabricadas em aglomerado de 25,0 mm, com revestimento em laminado melamínico de baixa pressão (BP), com bordas em PVC de 2,0 mm;
- Normas, certificados e laudos aplicáveis: NRs, Normas Mobiliárias Técnicas e de Escritório: NR17, Norma disposta pelo Ministério do Trabalho e Emprego, pelo Portaria MTP nº 4.219, de 20 de dezembro de 2021;

- Acabamento dos mobiliários:
    - Laminados melamínicos (decorativos) de alta pressão;
    - Especificações de normas (desenhos), mobiliários e estações de trabalho;
    - Certificado de Ergonomia da linha de produtos, em conformidade com a Lei Federal nº 6.514 de 22 de dezembro de 1977 e Portaria nº 3.214/NR 17 de 08 de junho de 1978 do Ministério do Trabalho, emitido por profissional qualificado em Ergonomia (médico do trabalho ou ergonomista); e
    - Laudo de Resistência à Corrosão em névoa salina (*Salt Spray*), conforme Norma ABNT NBR nº 8.094/1983 ou ISO nº 9.227/2006.

20.9.2. Mesa de Trabalho

- Tamanho: 150 cm x 75 cm x 75 cm (largura x altura x profundidade). Tipo: gaveteiro embutido de 3 gavetas com chave;
- Cadeira trabalho com altura ajustável;
- Apoios de braços ajustáveis, suporte lombar regulável e apoio para cabeça;
- Base giratória tipo estrela com 5 rodas;
- Material do estofado: encosto tela *Mesh* / assento corino;
- Medidas do assento: 490 mm de largura, 430 mm de altura mínima desde o chão; 530 mm de altura máxima desde o chão e 490 mm de profundidade; e
- A cadeira atinge uma altura mínima de 1.140 mm e máxima de 1.240 mm, densidade mínima de 45 kg/m³.

20.9.3. Arquivo para Pasta Suspensa com 4 Gavetas Com 04 gavetas

- Suporte para pastas de 260 mm de altura e 390 mm de largura;
- Puxador estampado / embutido;
- Sistema de fechadura com travamento simultâneo de todas as gavetas, e acompanham 2 cópias de chaves; e
- Trilho telescópico ou microesfera.

20.9.4. Armário Baixo de 2 Portas

- Altura x Largura x Profundidade: 80 cm x 75 cm x 45 cm; e
- Quantidade de prateleiras: 1.

20.9.5. Armário Médio de 2 Portas

- Altura x Largura x Profundidade: 110 cm x 75 cm x 45 cm;
- Quantidade de prateleiras: 2;
- Armário fechado de 2 portas;
- 02 portas de 1,60 m;
- Altura x Largura x Profundidade: 160 cm x 80 cm x 45 cm, quantidade de portas: 2; e
- Quantidade de prateleiras: 3.

20.9.6. Armário Extra Alto Fechado com 2 Portas de 1,60 m

- Altura x Largura x Profundidade: 200 cm x 80 cm x 45 cm, quantidade de portas: 2; e
- Quantidade de prateleiras: 3.

20.9.7. Sofá de 5 Lugares Quantidade de Lugares

- Tipo: Simples; e
- Cor: preta, material: courino.

20.9.8. Mesa Reunião – Quantidade de Lugares

- 8 lugares;
- Tipo: semioval; e
- Cor: preta.

20.9.9. Mesa de Copa

- Comprimento: 80 cm;
- Largura: 190 cm;
- Altura: 76 cm;
- Quantidade de cadeiras: 8, tipo: simples;
- Cor: preta.

20.9.10. Micro-ondas – Capacidade Mínima de 25 Litros

- Cor: Branca;
- Alimentação: 110 volts; e
- Sistema digital.

20.9.11. Purificador de Água Natural ou Gelada

- Purificação com filtro;
- Alimentação: 110 volts; e
- Cor: branca.

20.9.12. Geladeira Sistema *Frost Free*

- Modelo: duplex;
- Capacidade mínima: entre 340 e 380 litros;
- Alimentação: 110 volts; e
- Cor: branca.

20.9.13. Máquina Multibebidas

- Seleções mínimas: 08 (café curto, café longo, capuccino, chocolate quente, chá quente, café com leite, mocaccino e água quente); e
- Alimentação: 220 volts.

20.9.14. TV

- Modelo: *Smart Televisor*;
- Tamanho: 55 polegadas; e
- Alimentação: 110 volts.

20.10. Responsabilidades

As responsabilidades impostas à CONTRATADA, no que se refere precisamente ao **Centro de Controle Operacional do Sistema de Monitoramento,** são apenas a instalação, implantação, disponibilização dos equipamentos e manutenção, quando for necessário.
Assim, após a entrega do Centro de Controle Operacional, toda a operação ficará a cargo e será realizada por funcionários da CONTRATANTE.

21. ARMAZENAMENTO DE DADOS E IMAGENS

As imagens geradas pelas câmeras deverão ficar armazenadas no sistema de nuvem pelo período mínimo de 30 dias, para posterior consulta.

Armazenamento em nuvem por tempo indeterminado.
Os vídeos em que constarem casos de flagrantes, acidentes e demais eventos que possam ser usados como provas, para qualquer tipo de investigação ou processo judicial, deverão ser salvos e permanecer armazenados na Plataforma até o término do contrato ou o seu envio à autoridade competente, tais como juiz, promotor e delegado.
O envio das imagens para as autoridades competentes deverá ter comprovante de envio e comprovante de recebimento.

22. POLÍTICA DE SEGURANÇA DA INFORMAÇÃO, SEGURANÇA CIBERNÉTICA E INTEGRIDADE E ÉTICA

22.1. Políticas de Segurança da Informação e *Compliance*

As Políticas de Segurança da Informação e *Compliance* serão definidas de forma conjunta entre CONTRATANTE e CONTRATADA, seguindo os parâmetros definidos neste Caderno de Encargos e em um Documento Técnico de Segurança Cibernética, 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 e *Compliance* devem ser desenvolvidas e implantadas de forma transparente aos colaboradores da CONTRATADA e aos servidores da CONTRATANTE, trazendo o

compliance para a operação, a fim de garantir o cumprimento das Políticas de Segurança e *Compliance* e mitigar possíveis vazamentos de dados e acessos indevidos. Fica a cargo da CONTRATADA prover todo o treinamento de pessoal necessário à implantação da Política de Segurança da Informação e *Compliance.*

A Política de Segurança da Informação e *Compliance* deve levar em conta todas as necessidades da LGPD (Lei nº 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 e *Compliance*, segurança cibernética e tecnologia implementadas 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* ou 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 e Internet), eliminando a necessidade do uso de *link*s dedicados em todos os locais onde os sistemas podem ser utilizados.

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 trabalhada em conjunto com controles de acesso físicos nos locais onde existe acesso total (Centro de Controle Operacional) às funções e dados dos sistemas, sendo limitada 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 realizados em locais seguros (Centro de Controle Operacional), 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 (Centro de Controle Operacionai), de forma a controlar o acesso físico e impedir o vazamento de dados por observação de tela (quando não é necessário copiar os arquivos, bastando que eles estejam esquecidos abertos). Todas as estações e equipamentos que farão acesso aos sistemas e dados que compõem a Plataforma devem bloquear automaticamente quando o agente de monitoramento se afastar (evitando o esquecer abertos), utilizando múltiplos sistemas (métodos) no controle de acesso.

22.2. *Compliance*

Devem ser definidos processos claros a serem seguidos para garantir a segurança das informações, a exemplo de processos para solicitações, controle, atendimento, auditoria e recuperação de desastres (DRP). Esses processos devem ser sustentados por um sistema concentrador (módulo da Plataforma).

Todos os processos e regras devem ser claros e conhecidos por todos, mostrando em detalhes como funcionam, quais os limites, o que se aplica e quando, automatizando-se o processo e eliminando dele a pessoalidade. O próprio sistema deve deliberar (analisar) a viabilidade e encaminhar o que precisar de validação para o Conselho e Equipe Gestora da Plataforma , que deverá fazer análise e definir sua posição.

A automação administrativa deve compor a base do *compliance*, eliminando casos em que usuários administradores utilizem seus privilégios para benefício próprio, trazendo uma análise automática e imparcial baseada em variáveis que compõem o processo e que, quando for necessário, será enviada ao Conselho para deliberação.

22.3. Lei Geral de Proteção de Dados (LGPD)

As Políticas de Segurança da Informação e *Compliance* 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 compartilhados e tratados de qualquer forma, bem como não compartilhados com terceiros quando não trouxerem qualquer benefício significativo à sociedade.

Devem evidenciar que a cooperação entre Poder Público e iniciativa privada é benéfica à sociedade e como pode ser feita sem ser invasiva à privacidade, trazendo ganhos à sociedade, aumentando a segurança no perímetro urbano e trazendo efeitos indiretos nos serviços oferecidos pela iniciativa privada à população – como a redução dos custos dos seguros, entre outros benefícios indiretos já conhecidos e associados às características de inteligência, automação, tecnologia e informação. Tais características, combinadas na gestão pública durante a construção das Cidades Inteligentes, deixam 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, isto é, sem resolver as causas.

Deve-se deixar claro como os dados serão capturados, tratados (quando, por quem e em quais 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 se possa passar segurança à população em relação a sua privacidade ao utilizar este grande volume de dados sensíveis.

22.4. Política de Segurança da Informação (PSI)

22.4.1. Introdução

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, assegurando a transparência no tratamento de dados. São estabelecidas 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 às 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.

22.4.2. Objetivo

A Política de Segurança da Informação se aplica aos seguintes ativos:

- Ativos de informação;
- Ativos de *softwares*; e
- Ativos físicos.

22.4.3. Abrangência

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

22.4.4. Diretrizes

As diretrizes da Política de Segurança da Informação (PSI) regem a conduta e o comportamento em relação a temas de segurança, utilizando normas e procedimentos para garantir os demais direitos individuais previstos na LGPD (Lei nº 13.709/2018). Podem 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 propósito de ampliar estas garantias.

A solução da Plataforma deve possuir criptografia de ponta a ponta e manter a informação armazenada segura e encriptada, utilizando *Zero Knowledge* e criptografia AES 265 bits (semelhante ou superior), em blocos segregados impedindo o acesso à informação não criptografada mesmo em caso de ataque / invasão da solução. Devem ser utilizadas múltiplas camadas de segurança, criando barreiras inclusive a ataques internos por equipamentos infectados, e deve-se, ainda, acompanhar a atividade dos agentes e garantir que não ocorra utilização inadequada da solução por eles. 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 finalidadea que se propõe tais dados. Como o Brasil é um 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.

22.4.5. Tratamento da Informação

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

22.4.6. Acesso à Informação

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

22.4.7. Sistema e Aplicativo

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

22.4.8. Classificação da Informação

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

22.4.9. Segurança Física de Computadores e Demais Equipamentos

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

22.4.10. 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 em que os usuários da Plataforma poderão solicitar informações referentes ao tratamento dos seus dados pessoais e terão acesso aos controladores das informações, conforme dispõe os artigos 9º, 17 e 22, todos da Lei nº 13.709 de 14/08/2018 (LGPD).

A CONTRATADA deverá manter, no portal público, documento contendo as informações a seguir relacionadas:

- A CONTRATADA deverá colocar sinais claramente visíveis para garantir que qualquer pessoa que possa ser capturada pelas câmeras esteja ciente da existência do videomonitoramento na área;
- A CONTRATADA deverá garantir que os sinais incluam os detalhes de contato para as Secretarias responsáveis pela vigilância da zona que está sendo monitorada, bem como incluir informações sobre a Secretaria de Segurança Urbana Pública e os pontos de contato; e
- A CONTRATADA deverá configurar um endereço *Web* em que serão fornecidas informações mais detalhadas sobre a *Smart* Rio Preto, contendo, no mínimo, as seguintes informações, conforme artigos 6º, 8º e 9º da LGPD:

22.4.11. 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), envolvidas no Projeto. Tal descrição será disponibilizada através do Portal da Transparência e demais canais da Prefeitura Municipal de São José do Rio Preto, 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.

Exemplo de dados utilizados:

- Dados de Atendimento;
- Dados de Identificação;

•Dados Biométricos;

•Características;

•Contextos e ações; e

•Dados e documentos relacionados.

O documento público de referência, a ser disponibilizado em locais como Portal da Transparência e demais canais, será alterado sempre que o sistema integrar novos agentes, controladores e encarregados, ou que os processos e contextos do tratamento de dados forem alterados durante o processo de expansão e aprimoramento da *Smart* Rio Preto, visando a transparência e *compliance* com a legislação vigente. Devem-se observar informações de *compliance* e de segurança na utilização da Plataforma.

b) Identificação do controlador:

Partes envolvidas no tratamento de dados: no atual escopo, são identificados os seguintes agentes(s) 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 alterados à medida que a *Smart* Rio Preto expanda, e devendo ser publicados de forma clara no Portal da Transparência e demais canais sempre que forem modificados:

- Encarregados;
- Agentes de tratamento; e
- Controladores.

c) Serão publicadas, nos canais de comunicação da Secretaria Municipal de Segurança Pública, as informações de contato do encarregado pela proteção de dados pessoais, tanto da Secretaria Municipal de Segurança Pública como das Secretarias responsáveis pela zona vigiada e processamento de dados.

d) Responsabilidades dos agentes que realizarão o tratamento:

Os agentes responsabilizados pela realização do tratamento precisarão realizar o tratamento apenas quando necessário, conforme legislação vigente, para:

- Garantir a confidencialidade, autenticidade, disponibilidade e integridade dos dados; e
- Garantir, ao titular dos dados, o acesso a essas informações.

Os dados captados serão os estritamente necessários para as atividades da *Smart* Rio Preto. Apenas os agentes responsáveis terão acesso aos dados, com total controle sobre mudanças e atualizações de informações.

e) Direitos do titular de dados pessoais:

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

22.4.12. 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 *logins* e senhas para acesso ao sistema.

22.4.13. 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.

22.4.14. 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. A Política, portanto, deve ser cumprida e aplicada em todas as áreas.

22.4.15. Definição e Conceitos

a) 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:

i. Integridade: tem como objetivo a preservação, precisão e confiabilidade dos dados durante todo o seu ciclo de vida;
ii. Disponibilidade: é fundamental que os dados estejam disponíveis e, para garantir esse requisito, são necessários estabilidade e acesso permanente às informações, por meio de processos de manutenção rápidos, eliminação de falhas de *software* e atualizações constantes;
iii. Confidencialidade: garante que os dados estejam acessíveis a determinados usuários e protegidos contra pessoas não autorizadas, o que se aplica essencialmente a dados sensíveis. A confidencialidade dos dados pessoais do usuário é um dos requisitos centrais de conformidade da LGPD; e
iv. Autenticidade: visa confirmar a identidade do usuário antes de liberar o acesso aos sistemas e recursos, garantindo que não se passem por terceiros.

22.4.16. Descrição da Política

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

22.4.17. Classificação da Informação e Ciclo de Vida

A classificação da informação é uma das exigências da ISO nº 27.001, e consiste em um processo focado em garantir o nível adequado de proteção de dados, de acordo com a sensibilidade deles, visando a garantia de que nenhum dado seja divulgado indevidamente e que apenas pessoas que têm o direito de 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 tiverem mais utilidade.

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

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

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

c) 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;

d) Uso Interno: a informação deve ser classificada como de uso interno quando não for desejável o seu conhecimento por pessoas de fora do âmbito da CONTRATADA e da CONTRATANTE. Não deve sair do escopo e 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 provocam-se danos em pequena ou média escala. Exemplos de informações de uso interno: relatórios e planilhas; e

e) Pública: são informações divulgadas aos meios públicos, sem distinção. Exigem esforço mínimo de segurança e há um fluxo de processos determinado para a liberação das informações ao público. Exemplos 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:

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

b) Descarte: quando a informação se torna desnecessária, a destruição e o descarte devem ser feitos de forma adequada e seguir todas as diretrizes estabelecidas;

c) Manuseio: toda informação é gerada com a classificação mínima de uso, até passar pela avaliação e rotulagem para o tratamento adequado à informação;

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

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

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

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

i. 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 para criptografar e descriptografar a informação;
ii. Arquivos de senha: sempre serão necessários, para acessar algum tipo de recurso, o Identificador do Usuário (ID) e a senha do usuário; e
iii. 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.

22.4.18. Violação

As violações de segurança devem ser informadas à equipe de TI e da área de Segurança da Informação, e 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, legais e contratuais.

22.4.19. Vigência e Revisões

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

22.5. 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. Tem o objetivo de estabelecer procedimentos de comunicação e mobilização para processos de tratamento de incidentes de emergências de extremo impacto. Em caso de emergências que possam ocorrer durante as atividades na execução dos serviços da *Smart* Rio Preto, 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;
- Sequestro de dados;
- Ataque DDOS na Plataforma *Smart* Rio Preto;
- Falha na infraestrutura;
- Falha na rede; e
- Não se limitando aos exemplos de incidentes aqui citados.

O Plano de Contingência deve assegurar que os riscos identificados sejam avaliados e classificados de acordo com o risco causado na *Smart* Rio Preto, visando a garantia da proteção das informações baseada na LGPD e trazendo a segurança de que os dados estarão seguros.

A CONTRATADA deverá implementar o Plano de Contingência juntamente com o Plano de Recuperação de Desastres (DRP).
A CONTRATADA deverá redigir um Plano de Contingência conforme exigido pela LGPD.

O Plano será submetido ao Centro de Controle Administrativo da concessionária da *Smart* Rio Preto, que poderá realizar alterações que julgar necessárias, e posteriormente deverá ser aprovado pelo Conselho.

O Conselho pode aprovar, desaprovar e determinar novas diligências até a sua efetiva aprovação.

A responsabilização por falhas no Plano será da concessionária. Deve ser realizada simulação semestral para validação do Plano.

23. SEGURANÇA CIBERNÉTICA

23.1. Introdução

Este item contempla a instituição da Política de Segurança , que tem o compromisso de assegurar a proteção de ativos. É 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.

23.2. Objetivo

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

23.3. Abrangência

A Política de Segurança Cibernética deve estar disponível para que seu conteúdo possa ser consultado a qualquer momento e aplica-se a todos os funcionários.

23.4. Normas de Referência

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

- ISO nº 27.000;
- ISO nº 31.000;
- ISO nº 22.301;
- Cobit 5 – DS4;
- LGPD (Lei nº 13.709/2018);
- ABNT ISO/TR nº 31.004;
- ABNT NBR/IEC nº 31.010;
- ABNT NBR ISO/IEC nº 27.001;
- ABNT NBR ISO /IEC nº 27.002;
- ABNT NBR ISO/IEC nº 27.701;
- ABNT NBR ISO/IEC nº 29.100;
- ABNT NBR ISO/IEC nº 29.134; e
- ABNT NBR ISO/IEC nº 29.151.

23.5. Definição / Conceitos

Segurança Cibernética é definida como um conjunto de tecnologias, processos e práticas projetados para proteger redes. Constitui-se de ações voltadas para segurança de operações, visando que os sistemas de informações sejam capazes de resistir a eventos no espaço cibernético.

Envolve os seguintes conceitos:

a) Risco: qualquer evento que possa ser considerado hostil à segurança da informação com objetivo de afetar o sistema, ou conforme, a ISO nº 31.000, trazer o efeito de incerteza nos objetivos;

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

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

d) Informação: qualquer conjunto organizado de dados que possua algum propósito e valor para o sistema;
e) Espaço Cibernético: engloba a internet, sistemas de informações e as tecnologias digitais que dão suporte;
f) 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 e desligar computadores;
g) Ativos Tecnológicos: qualquer dispositivo físico ou digital, que suporta atividades relacionadas às informações;
h) Incidente de Segurança Cibernética: todo e qualquer evento não esperado que gere algum tipo de instabilidade; e
i) *Threat Intelligence*: inteligência de ameaças cibernéticas, que engloba tudo o que envolve medidas necessárias à prevenção de ataques cibernéticos e a mitigar os efeitos causados por eles, visando a preservação da confidencialidade, integridade, disponibilidade e conformidade.

São obrigações da CONTRATADA:
a) Indicar, à CONTRATANTE, 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, e base de dados pública; ou indicar ferramenta de busca automatizada de vulnerabilidades que seja aceita por ambas as Partes;
b) Adoção de mecanismo reservado de comunicação de vulnerabilidade descoberta ou que mereça contorno, de modo que a vulnerabilidade identificada somente venha a público caso já se tenha solução (no mínimo preventiva) e de forma definitiva quando se superar totalmente o incidente;
c) Enviar os *logs* requeridos pela CONTRATANTE e determinar qual é o tempo médio para atendimento das requisições;
d) Deverá criptografar todos os dispositivos móveis e portáteis utilizados para prover o serviço à CONTRATANTE e que contenham dados confidenciais;
e) Quando do uso de criptografia, a resistência dos algoritmos de criptografia deverá ser a mais alta possível sem afetar a usabilidade dos sistemas, e ser aprovada pela CONTRATANTE; e
f) Todo desenvolvimento feito pela CONTRATADA deverá incluir testes de segurança, com a finalidade de evitar a vulnerabilidade e inserção de códigos não autorizados.

24. RESPONSABILIDADES

24.1. As Responsabilidades da Área de Gestão de Riscos

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

b) Definir controles para tratamento de riscos, ameaças e vulnerabilidades;

c) Conduzir o processo de gestão de riscos e segurança da informação; e

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

24.2. Responsável pela Segurança Cibernética

a) Comunicar os incidentes cibernéticos ocorridos;

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

c) Gerenciar a identidade e acessos, para garantir a autenticidade; e

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

24.3. Responsável pelo *Compliance*

a) Criar estratégias de gerenciamento de riscos;

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

c) Implementar um programa de integridade em que informar-se-á sobre todos os riscos, tendo como obrigação relatar, controlar e cumprir todos os regulamentos, leis e normas.

24.4. Princípios e Procedimentos de Segurança da Informação

A informação deve ser utilizada unicamente a finalidade à qual foi autorizada pelo gestor da informação. 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:

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

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

c) Confidencialidade: garante que os dados estejam acessíveis a determinados usuários e protegidos contra pessoas não autorizadas, o 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 *Smart* Rio Preto.

A CONTRATADA deverá considerar, desde a concepção dos serviços a serem criados / atualizados, 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, bem como coletar assinatura de Termos de Confidencialidade específicos, sobre o acesso às imagens do sistema, de 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 da *Smart* Rio Preto, bem como determinar os procedimentos 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 quem a situação foi endereçada; e buscar orientações quando necessário, seja internamente ou da Autoridade Nacional de Proteção de Dados (ANPD).

A CONTRATADA deverá garantir que:

- Todos os funcionários autorizados a acessar as câmeras estejam familiarizados com o sistema e sobre como revisar e extrair imagens, se necessário;
- Todos os funcionários estejam familiarizados com as prováveis penalidades disciplinares por uso indevido dos sistemas da *Smart* Rio Preto; e
- Sejam atendidos e registrados padrões de quando o papel de um membro da equipe inclui explicitamente o monitoramento do CFTV.

A CONTRATADA deve dispor de meios que permitam a categorização das informações presentes no sistema, devendo ser capazes de identificar dados pessoais, dados pessoais sensíveis e informações gerais que não sejam dados pessoais.

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

b) Irretratabilidade: tem foco na legitimidade do autor da informação e está relacionada à garantia de impossibilidade de o emissor negar a autoria de determinada mensagem ou transação.

Devem-se ter os seguintes procedimentos para garantir a Segurança da Informação:

a) Métodos de autenticação: todos os usuários devem utilizar o método de autenticação de dois fatores. Todos funcionários, servidores públicos e estagiários são responsáveis por todos os atos executados com seu identificador (*login*/senha), e devem 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. Deve ser feito uso de senhas fortes e exclusivas, e as senhas devem ter, pelo menos, 14 caracteres;

b) 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;

c) Desenvolvimento seguro e criptografia: mecanismos de criptografia para a proteção da autenticidade dos dados, podendo tais dados serem acessados apenas por pessoas autorizadas e conforme as classificações das informações, para a realização das atividades;
d) *Backup* de dados: ter um plano de *backup* de dados e 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. O armazenamento mínimo do *backup* deve ser por 120 dias, e deve estar devidamente protegido de ataques e armazenado em local distinto da operação da Plataforma;
e) Teste de penetração: é um método que avalia a segurança de um sistema ou de uma rede, simulando um ataque de uma fonte maliciosa. Envolve uma análise nas atividades do sistema, que busca alguma vulnerabilidade em potencial que possa ser resultado de uma má configuração do sistema ou de falhas em *hardware*s/*software*s; e
f) Gestão de identidade de usuários: com o IAM ("*Identity and Access Management*"), os administradores de TI gerenciam, 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, bem como rastrear e relatar as deles, visando garantir a segurança e a privacidade de dados.

24.5. 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. O registro e a classificação melhoram a capacidade de detecção de incidentes e podem ajudar a conter danos e prejuízos. Atividades suspeitas ou incidentes identificados devem ser comunicados ao responsável pela segurança, através do e-mail de incidentes de segurança cibernética.

Devem ser registrados eventos adversos relacionados à segurança dos sistemas ou das redes de computadores, como, por exemplo:
a) Tentativas de invasão, com ou sem sucesso, e de ganhar acesso não autorizado a um sistema ou conseguir seus dados;

b) Modificação do sistema;
c) Sistema desatualizado permitindo abuso;
d) *Malware*;
e) Vírus; e
f) *Worms.*

Todos os recursos de informação que estiverem expostos na internet devem ser protegidos por um IDS / IPS (Sistema de Detecção de Intrusão / Sistema de Prevenção de Intrusão). Sempre que o IDS / IPS (recursos que examinam o tráfego na rede) detectarem ou responderem a uma tentativa externa de invasão ao sistema, uma análise estruturada e procedimentos de resposta devem ser acionados para garantir a segurança dos dados.

Devem existir os seguintes procedimentos para tratar os incidentes de segurança cibernética:
a) Autenticação e criptografia simétrica e assimétrica;
b) Testes de invasão;
c) IDS e IPS (sistemas de detecção e prevenção de ataques a redes);
d) Controles de acessos (lógicos e físicos);
e) Proteção contra *software*s maliciosos;
f) Antecipação de ataques cibernéticos; e
g) Manter sistemas atualizados.

24.6. Classificação das Relevâncias dos Incidentes Cibernéticos

Devem existir 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 pela segurança deve comunicar os gestores sempre que identificado um incidente cibernético e, caso seja necessário, estabelecer os seguintes mecanismos:

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

b) 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.

24.7. Violação

As violações de segurança, externas ou internas, devem ser informadas à equipe de TI e à área de Segurança da Informação, que deverá comunicar, ao responsável pela segurança, toda violação ou desvio de informações, que serão investigados 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.

24.8. 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, ao menos a cada 6 meses, com objetivo de se manter em sintonia com as regras e com as melhores práticas de segurança, leis, regulamentos e procedimentos, visando melhor atender às necessidades.

25. INTEGRIDADE E ÉTICA

25.1. Introdução

Este item 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 que sejam atingidos 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 sobre quais os critérios a serem utilizados. A exemplo, o uso de tecnologia que automatize o tratamento de dados não poderá discriminar pessoas nem 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 a eles se limitando, os seguintes documentos:

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

b) Política de Governança de IA: definirá as regras e restrições para definir as responsabilidades dos agentes públicos e terceiros que atuarão diretamente com a *Smart* Rio Preto, compreendendo aspectos táticos e operacionais referentes ao sistema inteligente;

c) Procedimento para Avaliação de Impacto da IA (AIIA), 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;

d) Procedimento de Auditoria: 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; e

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

25.2. 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:

a) Prevenir, detectar e punir desvios de conduta, roubo de dados e prática de corrupção;

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

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

d) Respeitar o conjunto de valores morais que conduzem o ambiente de trabalho de forma mais respeitosa, com transparência e equidade; e

e) Elevar a produtividade e a qualidade.

25.3. 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.

25.4. Princípios

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

Os princípios adotados são:

a) Legalidade – sempre atender à legislação vigente;

b) Integridade – seguir com retidão todas as normas estabelecidas;

c) Eficiência – entrega de atividades com rapidez, excelência e zelo pela economia;

d) Transparência – atender à legislação vigente, sempre observando primeiramente a LGPD; e

e) Respeito – manter o respeito nos relacionamentos interpessoais, em qualquer circunstância.

25.5. Diretrizes

A Política de Integridade e Ética deverá estar alinhada com as diretrizes apresentadas nos subtópicos a seguir, visando a garantia da integridade e utilizando normas e procedimentos previstos na Lei Anticorrupção (Lei nº 12.846).

25.5.1. Prevenção e Combate à Corrupção

A corrupção pode assumir muitas formas, mas na maioria das vezes acontece através de suborno. Não será tolerada qualquer forma de corrupção.

De acordo com a Lei Anticorrupção, deve-se constituir os seguintes procedimentos para adotar medidas anticorrupção:

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

b) Monitoramento contínuo das diretrizes, visando seu aperfeiçoamento na prevenção, detecção e combate à corrupção previstos no art. 5° da Lei Federal nº 12.846, de 1º de agosto de 2013.;

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

d) Disponibilização de canal de denúncia de irregularidades ou infrações detectadas; e

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

25.5.2. Conduta Ética

Diz respeito ao conjunto de valores morais que conduzem os comportamentos no ambiente de trabalho e durante o exercício das atividades, com o objetivo de:

a) Orientar a tomada de decisões em momentos de conflito de interesses;

b) Estabelecer padrões de integridade, respeito e transparência no exercício da profissão;

c) Atuar com base na legalidade, impessoalidade, moralidade, transparência e eficiência; e

d) Agir com dignidade e cortesia e com equipes orientadas a ouvir críticas e sugestões.

25.5.3. Compromissos

Em todos os relacionamentos devem ser obedecidas as orientações a seguir, para buscar um ambiente de trabalho com mais respeito, transparência e integridade:

a) Repúdio a qualquer tipo de discriminação;

b) Prevenção à fraude e ao roubo de dados (externo ou internamente);

c) Sigilo e confidencialidade das informações não públicas;

d) Lisura, transparência e imparcialidade; e

e) Prevenção e combate à corrupção.

25.5.4. Gerenciamento Disciplinar

Aplicação de gerenciamento disciplinar, com o objetivo de apurar, analisar, avaliar e julgar as ocorrências que foram cometidas, em que o empregado tenha omitido, permitido ou infringido as normas legais e/ou o contrato de concessão.

25.5.5. Relacionamentos Externos

Os relacionamentos externos devem ocorrer de forma profissional, transparente e igualitária com o público externo.

Devem obedecer às seguintes orientações, para manter um relacionamento profissional:

a) Postura ética, pautada em respeito e integridade;

b) Prestação de informações com transparência, integridade e veracidade; e

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

25.5.6. Gestão de Riscos

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

25.5.7. Controle Interno

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

25.5.8. Confidencialidade

Todos os níveis hierárquicos deverão manter a confidencialidade de todas as informações às 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.

A Concessionária deve manter rigorosamente a confidencialidade de todas as informações, mediante a adoção das seguintes práticas:

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

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

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

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

25.5.9. Transparência Ativa

Refere-se ao processo de disponibilização de informações de órgãos e entidades da Administração Pública, 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.

25.5.10.Canal de Comunicação

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

26. COMPOSIÇÃO DA REDE DE VIDEOMONITORAMENTO

A rede de videomonitoramento do município é composta por 160 (cento e sessenta) câmeras externas operadas pela GCM- Guarda Civil Municipal.

PREFEITURA DE
RIO PRETO

RELAÇÃO DE CÂMERAS EXTERNAS - LOCALIZAÇÃO EM VIAS PÚBLICAS						
Nº de Ordem	Externa	Endereço	Numero	Tipo	Facial/LRP	IA embarcada
1	VIA PUBLICA - VIA PUBLICA	R. São Paulo	2030	RTSP	NÃO	NÃO
2	VIA PUBLICA - VIA PUBLICA	Rua Bernardino de Campos	2770	RTSP	NÃO	NÃO
3	VIA PUBLICA - VIA PUBLICA	R. Coronel Espínola de Castro x R. Prudente de Moraes	s/n	RTSP	NÃO	NÃO
4	VIA PUBLICA - VIA PUBLICA	R. Coronel Espínola de Castro x R. Prudente de Moraes	s/n	RTSP	NÃO	NÃO
5	VIA PUBLICA - VIA PUBLICA	R. Voluntários de São Paulo x R. Silva Jardim	s/n	RTSP	NÃO	NÃO
6	VIA PUBLICA - VIA PUBLICA	R. Quinze de Novembro x R. Siqueira Campos	s/n	RTSP	NÃO	NÃO
7	VIA PUBLICA - VIA PUBLICA	R. Quinze de Novembro x R. Siqueira Campos	s/n	RTSP	NÃO	NÃO
8	VIA PUBLICA - VIA PUBLICA	Rua General Glicério x Rua Jorge Tibiriçá	s/n	RTSP	NÃO	NÃO
9	VIA PUBLICA - VIA PUBLICA	Rua Bernardino de Campos x Rua Siqueira Campos	s/n	RTSP	NÃO	NÃO
10	VIA PUBLICA - VIA PUBLICA	Rua General Glicério x Rua Siqueira Campos	s/n	RTSP	NÃO	NÃO
11	VIA PUBLICA - VIA PUBLICA	Rua Bernardino de Campos x Rua Tiradentes	s/n	RTSP	NÃO	NÃO
12	VIA PUBLICA - VIA PUBLICA	Avenida Philadelpho Gouveia Netto	3165	RTSP	NÃO	NÃO
13	VIA PUBLICA - VIA PUBLICA	Rua Arthur Roma	4307	RTSP	NÃO	NÃO
14	VIA PUBLICA - VIA PUBLICA	Rua José Tebar	144	RTSP	NÃO	NÃO
15	VIA PUBLICA - VIA PUBLICA	Rua Jaqkeline Freitas do Prado	393	RTSP	NÃO	NÃO
16	VIA PUBLICA - VIA PUBLICA	Av. Feliciano Sales	2130	RTSP	NÃO	NÃO
17	VIA PUBLICA - VIA PUBLICA	Av. Antoninho Marmo	3810	RTSP	NÃO	NÃO
18	VIA PUBLICA - VIA PUBLICA	R. Renato Pereira de Campos	s/n	RTSP	NÃO	NÃO
19	VIA PUBLICA - VIA PUBLICA	R. José Domingues Neto	220	RTSP	NÃO	NÃO
20	VIA PUBLICA - VIA PUBLICA	R. Waldir Lacerda	140	RTSP	NÃO	NÃO
21	VIA PUBLICA - VIA PUBLICA	R. Antônio Francisco Coutinho	65	RTSP	NÃO	NÃO
22	VIA PUBLICA - VIA PUBLICA	Av. São José do Rio Preto	4365	RTSP	NÃO	NÃO
23	VIA PUBLICA - VIA PUBLICA	R. Reginaldo Perpétuo Raimundo Salgado	266	RTSP	NÃO	NÃO
24	VIA PUBLICA - VIA PUBLICA	R. Reginaldo Perpétuo Raimundo Salgado	266	RTSP	NÃO	NÃO
25	VIA PUBLICA - VIA PUBLICA	Av. Antonio Buzzini	270	RTSP	NÃO	NÃO
26	VIA PUBLICA - VIA PUBLICA	R. Professora Zulmira da Silva Salles	897	RTSP	NÃO	NÃO
27	VIA PUBLICA - VIA PUBLICA	R. Luiza Maria de Jesus	135	RTSP	NÃO	NÃO
28	VIA PUBLICA - VIA PUBLICA	Rua Manoel Miceli	500	RTSP	NÃO	NÃO
29	VIA PUBLICA - VIA PUBLICA	R. Dr. Irlan Leite de Abreu	s/n	RTSP	NÃO	NÃO
30	VIA PUBLICA - VIA PUBLICA	R. Mal. Eurico Gaspar Dutra	s/n	RTSP	NÃO	NÃO
31	VIA PUBLICA - VIA PUBLICA	R. Maria Ceron Volpe	751	RTSP	NÃO	NÃO
32	VIA PUBLICA - VIA PUBLICA	R. Maria Elías Cury	s/n	RTSP	NÃO	NÃO
33	VIA PUBLICA - VIA PUBLICA	R. Gumercindo de Oliveira Barros	919	RTSP	NÃO	NÃO
34	VIA PUBLICA - VIA PUBLICA	R. Marcelo Alessandro Cavallini	486	RTSP	NÃO	NÃO
35	VIA PUBLICA - VIA PUBLICA	R. Beatriz da Conceição	470	RTSP	NÃO	NÃO
36	VIA PUBLICA - VIA PUBLICA	R. Antônio Severo dos Santos	878	RTSP	NÃO	NÃO
37	VIA PUBLICA - VIA PUBLICA	Av. São José do Rio Preto	3050	RTSP	NÃO	NÃO
38	VIA PUBLICA - VIA PUBLICA	R. Maria Onófre Lopes Santos	1203	RTSP	NÃO	NÃO
39	VIA PUBLICA - VIA PUBLICA	Av. Luiz Martins Filho	s/n	RTSP	NÃO	NÃO
40	VIA PUBLICA - VIA PUBLICA	R. Jesus Cristo	441	RTSP	NÃO	NÃO
41	VIA PUBLICA - VIA PUBLICA	R. José Elías Abraão	105	RTSP	NÃO	NÃO
42	VIA PUBLICA - VIA PUBLICA	R. Joao Gagliardo	145	RTSP	NÃO	NÃO
43	VIA PUBLICA - VIA PUBLICA	R. Brg. Eduardo Gomes	176	RTSP	NÃO	NÃO
44	VIA PUBLICA - VIA PUBLICA	R. Cezar Pupin	1150	RTSP	NÃO	NÃO
45	VIA PUBLICA - VIA PUBLICA	R. Almelinda Aparecida de Paula Amaral	149	RTSP	NÃO	NÃO
46	VIA PUBLICA - VIA PUBLICA	R. Manoel da Costa Branco	870	RTSP	NÃO	NÃO
47	VIA PUBLICA - VIA PUBLICA	R. Walder Antonio Sbrogio	s/n	RTSP	NÃO	NÃO
48	VIA PUBLICA - VIA PUBLICA	Av. Abelardo Menezes	121	RTSP	NÃO	NÃO
49	VIA PUBLICA - VIA PUBLICA	R. Joaquim Rodrigues	1085	RTSP	NÃO	NÃO
50	VIA PUBLICA - VIA PUBLICA	R. Antônio de Godoy, 3048	3048	RTSP	NÃO	NÃO
51	VIA PUBLICA - VIA PUBLICA	R. Antônio de Godoy, 3048	3048	RTSP	NÃO	NÃO
52	VIA PUBLICA - VIA PUBLICA	R. Antônio de Godoy, 3048	3048	RTSP	NÃO	NÃO
53	VIA PUBLICA - VIA PUBLICA	R. Antônio de Godoy, 3048	3048	RTSP	NÃO	NÃO
54	VIA PUBLICA - VIA PUBLICA	R. Antônio de Godoy, 3048	3048	RTSP	NÃO	NÃO
55	VIA PUBLICA - VIA PUBLICA	R. Antônio de Godoy, 3048	3048	RTSP	NÃO	NÃO
56	VIA PUBLICA - VIA PUBLICA	R. Voluntários de São Paulo	3491	RTSP	NÃO	NÃO
57	VIA PUBLICA - VIA PUBLICA	R. Geraldo de Paiva Ferreira	550	RTSP	NÃO	NÃO
58	VIA PUBLICA - VIA PUBLICA	Av. Dr. Solon Varginha	374	RTSP	NÃO	NÃO
59	VIA PUBLICA - VIA PUBLICA	Estrada Vicinal João Parise	4310	RTSP	NÃO	NÃO
60	VIA PUBLICA - VIA PUBLICA	R. Alberto Targas	755	RTSP	NÃO	NÃO

PREFEITURA DE
RIO PRETO

RELAÇÃO DE CÂMERAS EXTERNAS - LOCALIZAÇÃO EM VIAS PÚBLICAS						
Nº de Ordem	Externa	Endereço	Numero	Tipo	Facial/LRP	IA embarcada
61	VIA PUBLICA - VIA PUBLICA	Av. Nagib Gabriel	5564	RTSP	NÃO	NÃO
62	VIA PUBLICA - VIA PUBLICA	Av Sabino Cardoso Filho	2520	RTSP	NÃO	NÃO
63	VIA PUBLICA - VIA PUBLICA	Rua Caio Nogueira Bertozzi	183	RTSP	NÃO	NÃO
64	VIA PUBLICA - VIA PUBLICA	Rua Caio Nogueira Bertozzi	183	RTSP	NÃO	NÃO
65	VIA PUBLICA - VIA PUBLICA	Av Duque de Caxias	s/n	RTSP	NÃO	NÃO
66	VIA PUBLICA - VIA PUBLICA	Av Lino José de Seixas	s/n	RTSP	NÃO	NÃO
67	VIA PUBLICA - VIA PUBLICA	Av Lino José de Seixas	s/n	RTSP	NÃO	NÃO
68	VIA PUBLICA - VIA PUBLICA	Av Lino José de Seixas	s/n	RTSP	NÃO	NÃO
69	VIA PUBLICA - VIA PUBLICA	Av Lino José de Seixas	s/n	RTSP	NÃO	NÃO
70	VIA PUBLICA - VIA PUBLICA	Av Lino José de Seixas	s/n	RTSP	NÃO	NÃO
71	VIA PUBLICA - VIA PUBLICA	R. Silva Jardim	3157	RTSP	NÃO	NÃO
72	VIA PUBLICA - VIA PUBLICA	R. Silva Jardim	3157	RTSP	NÃO	NÃO
73	VIA PUBLICA - VIA PUBLICA	R. Ipiranga	280	RTSP	NÃO	NÃO
74	VIA PUBLICA - VIA PUBLICA	R. Ipiranga	280	RTSP	NÃO	NÃO
75	VIA PUBLICA - VIA PUBLICA	Av. Nova Granada	3320	RTSP	NÃO	NÃO
76	VIA PUBLICA - VIA PUBLICA	R. Ida Tagliavini Polachini	580	RTSP	NÃO	NÃO
77	VIA PUBLICA - VIA PUBLICA	R. Alpalice Margarida Veronizi Ferrari	440	RTSP	NÃO	NÃO
78	VIA PUBLICA - VIA PUBLICA	Avenida Philadelpho Manoel Gouveia Neto	3165	RTSP	NÃO	NÃO
79	VIA PUBLICA - VIA PUBLICA	R. Professora Aureliana Ferrari	250	RTSP	NÃO	NÃO
80	VIA PUBLICA - VIA PUBLICA	R. Odilon Amadeu	710	RTSP	NÃO	NÃO
81	VIA PUBLICA - VIA PUBLICA	Av. Pres. Getúlio Vargas	381	RTSP	NÃO	NÃO
82	VIA PUBLICA - VIA PUBLICA	R. Ida Tagliavini Polachini	580	RTSP	NÃO	NÃO
83	VIA PUBLICA - VIA PUBLICA	Rua Bernardino de Campos x Av. Philadelpho Manoel Gouveia Neto	2491	RTSP	NÃO	NÃO
84	VIA PUBLICA - VIA PUBLICA	Rua Bernardino de Campos x Av. Philadelpho Manoel Gouveia Neto	2491	RTSP	NÃO	NÃO
85	VIA PUBLICA - VIA PUBLICA	Rua Bernardino de Campos x Av. Philadelpho Manoel Gouveia Neto	2491	RTSP	NÃO	NÃO
86	VIA PUBLICA - VIA PUBLICA	Rua Bernardino de Campos x Av. Philadelpho Manoel Gouveia Neto	2491	RTSP	NÃO	NÃO
87	VIA PUBLICA - VIA PUBLICA	Rua Bernardino de Campos x Av. Philadelpho Manoel Gouveia Neto	2491	RTSP	NÃO	NÃO
88	VIA PUBLICA - VIA PUBLICA	Rua Bernardino de Campos x Av. Philadelpho Manoel Gouveia Neto	2491	RTSP	NÃO	NÃO
89	VIA PUBLICA - VIA PUBLICA	Rua Bernardino de Campos x Av. Philadelpho Manoel Gouveia Neto	2491	RTSP	NÃO	NÃO
90	VIA PUBLICA - VIA PUBLICA	Rua Bernardino de Campos x Av. Philadelpho Manoel Gouveia Neto	2491	RTSP	NÃO	NÃO
91	VIA PUBLICA - VIA PUBLICA	Rua Bernardino de Campos x Av. Philadelpho Manoel Gouveia Neto	2491	RTSP	NÃO	NÃO
92	VIA PUBLICA - VIA PUBLICA	Rua Bernardino de Campos x Av. Philadelpho Manoel Gouveia Neto	2491	RTSP	NÃO	NÃO
93	VIA PUBLICA - VIA PUBLICA	Rua Bernardino de Campos x Av. Philadelpho Manoel Gouveia Neto	2491	RTSP	NÃO	NÃO
94	VIA PUBLICA - VIA PUBLICA	Rua Bernardino de Campos x Av. Philadelpho Manoel Gouveia Neto	2491	RTSP	NÃO	NÃO
95	VIA PUBLICA - VIA PUBLICA	Rua Bernardino de Campos x Av. Philadelpho Manoel Gouveia Neto	2491	RTSP	NÃO	NÃO
96	VIA PUBLICA - VIA PUBLICA	Rua Bernardino de Campos x Av. Philadelpho Manoel Gouveia Neto	2491	RTSP	NÃO	NÃO
97	VIA PUBLICA - VIA PUBLICA	Rua Bernardino de Campos x Av. Philadelpho Manoel Gouveia Neto	2491	RTSP	NÃO	NÃO
98	VIA PUBLICA - VIA PUBLICA	Rua Bernardino de Campos x Av. Philadelpho Manoel Gouveia Neto	2491	RTSP	NÃO	NÃO
99	VIA PUBLICA - VIA PUBLICA	Rua Bernardino de Campos x Av. Philadelpho Manoel Gouveia Neto	2491	RTSP	NÃO	NÃO
100	VIA PUBLICA - VIA PUBLICA	Rua Bernardino de Campos x Av. Philadelpho Manoel Gouveia Neto	2491	RTSP	NÃO	NÃO
101	VIA PUBLICA - VIA PUBLICA	Rua Bernardino de Campos x Av. Philadelpho Manoel Gouveia Neto	2491	RTSP	NÃO	NÃO
102	VIA PUBLICA - VIA PUBLICA	Rua Bernardino de Campos x Av. Philadelpho Manoel Gouveia Neto	2491	RTSP	NÃO	NÃO
103	VIA PUBLICA - VIA PUBLICA	Rua Bernardino de Campos x Av. Philadelpho Manoel Gouveia Neto	2491	RTSP	NÃO	NÃO
104	VIA PUBLICA - VIA PUBLICA	Rua Bernardino de Campos x Av. Philadelpho Manoel Gouveia Neto	2491	RTSP	NÃO	NÃO
105	VIA PUBLICA - VIA PUBLICA	Rua Bernardino de Campos x Av. Philadelpho Manoel Gouveia Neto	2491	RTSP	NÃO	NÃO
106	VIA PUBLICA - VIA PUBLICA	Rua Bernardino de Campos x Av. Philadelpho Manoel Gouveia Neto	2491	RTSP	NÃO	NÃO
107	VIA PUBLICA - VIA PUBLICA	Rua Bernardino de Campos x Av. Philadelpho Manoel Gouveia Neto	2491	RTSP	NÃO	NÃO
108	VIA PUBLICA - VIA PUBLICA	Rua Bernardino de Campos x Av. Philadelpho Manoel Gouveia Neto	2491	RTSP	NÃO	NÃO
109	VIA PUBLICA - VIA PUBLICA	Rua Bernardino de Campos x Av. Philadelpho Manoel Gouveia Neto	2491	RTSP	NÃO	NÃO
110	VIA PUBLICA - VIA PUBLICA	Rua Bernardino de Campos x Av. Philadelpho Manoel Gouveia Neto	2491	RTSP	NÃO	NÃO
111	VIA PUBLICA - VIA PUBLICA	Rua Bernardino de Campos x Av. Philadelpho Manoel Gouveia Neto	2491	RTSP	NÃO	NÃO
112	VIA PUBLICA - VIA PUBLICA	Rua Bernardino de Campos x Av. Philadelpho Manoel Gouveia Neto	2491	RTSP	NÃO	NÃO
113	VIA PUBLICA - VIA PUBLICA	Rua Bernardino de Campos x Av. Philadelpho Manoel Gouveia Neto	2491	RTSP	NÃO	NÃO
114	VIA PUBLICA - VIA PUBLICA	Rua Bernardino de Campos x Av. Philadelpho Manoel Gouveia Neto	2491	RTSP	NÃO	NÃO
115	VIA PUBLICA - VIA PUBLICA	Rua Bernardino de Campos x Av. Philadelpho Manoel Gouveia Neto	2491	RTSP	NÃO	NÃO
116	VIA PUBLICA - VIA PUBLICA	Rua Bernardino de Campos x Av. Philadelpho Manoel Gouveia Neto	2491	RTSP	NÃO	NÃO
117	VIA PUBLICA - VIA PUBLICA	Rua Bernardino de Campos x Av. Philadelpho Manoel Gouveia Neto	2491	RTSP	NÃO	NÃO
118	VIA PUBLICA - VIA PUBLICA	Rua Bernardino de Campos x Av. Philadelpho Manoel Gouveia Neto	2491	RTSP	NÃO	NÃO
119	VIA PUBLICA - VIA PUBLICA	Rua Bernardino de Campos x Av. Philadelpho Manoel Gouveia Neto	2491	RTSP	NÃO	NÃO
120	VIA PUBLICA - VIA PUBLICA	Rua Bernardino de Campos x Av. Philadelpho Manoel Gouveia Neto	2491	RTSP	NÃO	NÃO

PREFEITURA DE
RIO PRETO

RELAÇÃO DE CÂMERAS EXTERNAS - LOCALIZAÇÃO EM VIAS PÚBLICAS						
Nº de Ordem	Externa	Endereço	Numero	Tipo	Facial/LRP	IA embarcada
121	VIA PUBLICA - VIA PUBLICA	Rua Bernardino de Campos x Av. Philadelpho Manoel Gouveia Neto	2491	RTSP	NÃO	NÃO
122	VIA PUBLICA - VIA PUBLICA	Rua Bernardino de Campos x Av. Philadelpho Manoel Gouveia Neto	2491	RTSP	NÃO	NÃO
123	VIA PUBLICA - VIA PUBLICA	Rua Bernardino de Campos x Av. Philadelpho Manoel Gouveia Neto	2491	RTSP	NÃO	NÃO
124	VIA PUBLICA - VIA PUBLICA	Rua Bernardino de Campos x Av. Philadelpho Manoel Gouveia Neto	2491	RTSP	NÃO	NÃO
125	VIA PUBLICA - VIA PUBLICA	Rua Bernardino de Campos x Av. Philadelpho Manoel Gouveia Neto	2491	RTSP	NÃO	NÃO
126	VIA PUBLICA - VIA PUBLICA	Rua Bernardino de Campos x Av. Philadelpho Manoel Gouveia Neto	2491	RTSP	NÃO	NÃO
127	VIA PUBLICA - VIA PUBLICA	Rua Bernardino de Campos x Av. Philadelpho Manoel Gouveia Neto	2491	RTSP	NÃO	NÃO
128	VIA PUBLICA - VIA PUBLICA	Rua Bernardino de Campos x Av. Philadelpho Manoel Gouveia Neto	2491	RTSP	NÃO	NÃO
129	VIA PUBLICA - VIA PUBLICA	Rua Bernardino de Campos x Av. Philadelpho Manoel Gouveia Neto	2491	RTSP	NÃO	NÃO
130	VIA PUBLICA - VIA PUBLICA	Rua Bernardino de Campos x Av. Philadelpho Manoel Gouveia Neto	2491	RTSP	NÃO	NÃO
131	VIA PUBLICA - VIA PUBLICA	Rua Bernardino de Campos x Av. Philadelpho Manoel Gouveia Neto	2491	RTSP	NÃO	NÃO
132	VIA PUBLICA - VIA PUBLICA	Rua Bernardino de Campos x Av. Philadelpho Manoel Gouveia Neto	2491	RTSP	NÃO	NÃO
133	VIA PUBLICA - VIA PUBLICA	Rua Bernardino de Campos x Av. Philadelpho Manoel Gouveia Neto	2491	RTSP	NÃO	NÃO
134	VIA PUBLICA - VIA PUBLICA	Rua Bernardino de Campos x Av. Philadelpho Manoel Gouveia Neto	2491	RTSP	NÃO	NÃO
135	VIA PUBLICA - VIA PUBLICA	Rua Bernardino de Campos x Av. Philadelpho Manoel Gouveia Neto	2491	RTSP	NÃO	NÃO
136	VIA PUBLICA - VIA PUBLICA	Rua Bernardino de Campos x Av. Philadelpho Manoel Gouveia Neto	2491	RTSP	NÃO	NÃO
137	VIA PUBLICA - VIA PUBLICA	Rua Bernardino de Campos x Av. Philadelpho Manoel Gouveia Neto	2491	RTSP	NÃO	NÃO
138	VIA PUBLICA - VIA PUBLICA	Rua Bernardino de Campos x Av. Philadelpho Manoel Gouveia Neto	2491	RTSP	NÃO	NÃO
139	VIA PUBLICA - VIA PUBLICA	Rua Bernardino de Campos x Av. Philadelpho Manoel Gouveia Neto	2491	RTSP	NÃO	NÃO
140	VIA PUBLICA - VIA PUBLICA	Rua Bernardino de Campos x Av. Philadelpho Manoel Gouveia Neto	2491	RTSP	NÃO	NÃO
141	VIA PUBLICA - VIA PUBLICA	Rua Bernardino de Campos x Av. Philadelpho Manoel Gouveia Neto	2491	RTSP	NÃO	NÃO
142	VIA PUBLICA - VIA PUBLICA	Rua Bernardino de Campos x Av. Philadelpho Manoel Gouveia Neto	2491	RTSP	NÃO	NÃO
143	VIA PUBLICA - VIA PUBLICA	Rua Bernardino de Campos x Av. Philadelpho Manoel Gouveia Neto	2491	RTSP	NÃO	NÃO
144	VIA PUBLICA - VIA PUBLICA	Rua Bernardino de Campos x Av. Philadelpho Manoel Gouveia Neto	2491	RTSP	NÃO	NÃO
145	VIA PUBLICA - VIA PUBLICA	Rua Bernardino de Campos x Av. Philadelpho Manoel Gouveia Neto	2491	RTSP	NÃO	NÃO
146	VIA PUBLICA - VIA PUBLICA	Rua Bernardino de Campos x Av. Philadelpho Manoel Gouveia Neto	2491	RTSP	NÃO	NÃO
147	VIA PUBLICA - VIA PUBLICA	Rua Bernardino de Campos x Av. Philadelpho Manoel Gouveia Neto	2491	RTSP	NÃO	NÃO
148	VIA PUBLICA - VIA PUBLICA	Rua Bernardino de Campos x Av. Philadelpho Manoel Gouveia Neto	2491	RTSP	NÃO	NÃO
149	VIA PUBLICA - VIA PUBLICA	Rua Bernardino de Campos x Av. Philadelpho Manoel Gouveia Neto	2491	RTSP	NÃO	NÃO
150	VIA PUBLICA - VIA PUBLICA	Rua Bernardino de Campos x Av. Philadelpho Manoel Gouveia Neto	2491	RTSP	NÃO	NÃO
151	VIA PUBLICA - VIA PUBLICA	Rua Bernardino de Campos x Av. Philadelpho Manoel Gouveia Neto	2491	RTSP	NÃO	NÃO
152	VIA PUBLICA - VIA PUBLICA	Rua Bernardino de Campos x Av. Philadelpho Manoel Gouveia Neto	2491	RTSP	NÃO	NÃO
153	VIA PUBLICA - VIA PUBLICA	Rua Bernardino de Campos x Av. Philadelpho Manoel Gouveia Neto	2491	RTSP	NÃO	NÃO
154	VIA PUBLICA - VIA PUBLICA	Rua Bernardino de Campos x Av. Philadelpho Manoel Gouveia Neto	2491	RTSP	NÃO	NÃO
155	VIA PUBLICA - VIA PUBLICA	Rua Bernardino de Campos x Av. Philadelpho Manoel Gouveia Neto	2491	RTSP	NÃO	NÃO
156	VIA PUBLICA - VIA PUBLICA	Rua Bernardino de Campos x Av. Philadelpho Manoel Gouveia Neto	2491	RTSP	NÃO	NÃO
157	VIA PUBLICA - VIA PUBLICA	Rua Bernardino de Campos x Av. Philadelpho Manoel Gouveia Neto	2491	RTSP	NÃO	NÃO
158	VIA PUBLICA - VIA PUBLICA	Rua Cristóvão Colombo x Rua Emílio Nicoletti	s/n	RTSP	NÃO	NÃO
159	VIA PUBLICA - VIA PUBLICA	Rua Calixto Fauaz x Rua Emílio Nicoletti	s/n	RTSP	NÃO	NÃO
160	VIA PUBLICA - VIA PUBLICA	Rua Prof Francisco Felipe Caputo x Rua Prof José Felício Miziara	s/n	RTSP	NÃO	NÃO