

# ESTUDO TÉCNICO PRELIMINAR (ETP)

(Em conformidade com o Art. 18 da Lei nº 14.133/2021)

O presente estudo técnico preliminar, documento constitutivo da primeira etapa do planejamento da contratação, caracteriza o interesse público envolvido e evidencia o problema a ser resolvido e a sua melhor solução, de modo a permitir a avaliação da viabilidade da contratação, e fornecer base técnica ao Termo de Referência a ser elaborado.

**Processo:** Contratação de Solução de Segurança Patrimonial para as Unidades de Governo

**Data:** 16 de dezembro de 2025

**Unidade Requisitante:** Secretaria de Administração (SEAD) - Prefeitura Municipal de Lajeado/RS

## 1. DESCRIÇÃO DA NECESSIDADE (Art. 18, § 1º, I)

A necessidade-raiz da Administração é a contratação de uma solução completa e moderna de segurança e monitoramento patrimonial para as unidades de governo, visando mitigar riscos de vandalismo, furtos, agressões e outras atividades ilícitas. A solução deve aumentar a segurança dos servidores e cidadãos, inibir ações criminosas por meio de vigilância ativa e fornecer subsídios para a responsabilização em caso de ocorrências.

A necessidade de monitoramento e segurança patrimonial municipal está diretamente ligada à preservação dos bens públicos e à proteção das pessoas que frequentam esses espaços. Em um ambiente urbano, onde a circulação de cidadãos, servidores e visitantes é intensa, torna-se essencial adotar medidas de vigilância que garantam a integridade do patrimônio e a segurança dos usuários. Bens públicos, como praças, escolas, hospitais e edifícios administrativos, são investimentos coletivos que demandam cuidados especiais, e a adoção de sistemas de monitoramento visa prevenir danos, vandalismo, furtos e outras ações ilícitas.

Além da preservação física desses bens, o monitoramento também desempenha um papel importante na dissuasão de crimes, já que a presença de câmeras e outros dispositivos de segurança serve como um fator de inibição de atos criminosos. A tecnologia moderna permite a adoção de câmeras com reconhecimento facial, sensores de movimento e análise comportamental, que, em conjunto com uma central de monitoramento, tornam as ações de vigilância mais ágeis e eficazes. As câmeras também podem ser úteis para a identificação de incidentes naturais, assim como inundações, possibilitando ações proativas na proteção da vida humana e bens materiais.

O uso de monitoramento, no entanto, vai além da simples proteção material. Ele garante a segurança de quem circula nos ambientes públicos, oferecendo maior tranquilidade para os cidadãos e servidores. A presença de sistemas de vigilância cria um ambiente mais

seguro, onde a população pode usufruir dos serviços e espaços municipais com menos preocupações.

A solução a ser contratada também deve possibilitar a automatização das rotinas de segurança, proporcionando pronta resposta em caso de incidentes e auxiliando o trabalho dos operadores e agentes patrimoniais, gerando assim redução de custos operacionais.

Por sua vez, a locação destes dispositivos de segurança visa sinalizar situações de perigo em casos de invasão ou roubo e melhorar o controle de entrada e saída de pessoas agindo, preferencialmente nos âmbitos preventivo e proativo. Deve atuar, preferencialmente, na proteção da vida.

Desse modo, entende-se que o monitoramento eletrônico por vídeo e o emprego de dispositivos de segurança são ferramentas imprescindíveis para garantir uma condição mais segura, possibilitando a vigilância de todos os pontos de interesse e registro de eventos e incidentes para posterior investigação. Para além da investigação após ocorrência, deve possibilitar a atuação pró-ativa, considerando as proteções, preventiva, desencorajadora, limitadora, monitoradora, detectora e reativa.

## **2. PANORAMA GERAL**

Verifica-se um crescente aumento dos números da criminalidade em todas as áreas da nossa sociedade, inclusive nos espaços públicos. Constata-se também que as instituições de atendimento à população, postos de saúde, escolas e demais unidades de governo não estão imunes a essa realidade. Autoridades dos poderes público e privado buscam por modelos eficazes de políticas de segurança e, nesse contexto, o videomonitoramento vem surgindo como uma alternativa tecnologicamente eficiente, economicamente viável e de grande difusão na sociedade atual. Câmeras de monitoramento e segurança já podem ser percebidas em muitos espaços públicos e privados, porém geralmente disponíveis em caráter passivo para simples recuperação de fatos já ocorridos.

Entende-se que o princípio ativo de emprego da vigilância eletrônica é o do controle do comportamento das pessoas, pela inibição e modelagem, através do ato de vigiar, com possibilidade de punir, na perspectiva de desencorajar, mitigar ou controlar a criminalidade. Assim, as câmeras de vídeo estão sendo incluídas nas medidas atuais de enfrentamento do crime, através de um discurso que se apresenta como alternativo e que aponta as seguintes funcionalidades:

- a. visualizar, registrar e guardar a imagem de um fato ocorrido, no intuito de tirar o anonimato da autoria, já que a certeza do anonimato de autoria pode ser considerado um fator facilitador/estimulador do crime;
- b. produzir provas para a investigação policial, favorecendo a diminuição da impunidade, pois também a certeza da impunidade é outro fator facilitador/estimulador do crime
- c. vigilância ostensiva em tempo real, a qual possibilita identificar as condições de

início de uma determinada ocorrência, criando a possibilidade de imediata reação para salvaguardar o patrimônio e a integridade dos indivíduos presentes nesse ambiente.

Busca-se, portanto, apresentar solução de segurança que atue nas proteções, preventiva, desencorajadora, limitadora, monitoradora, detectora e reativa. Percebe-se, por óbvio, que tal desafio necessita de uso extensivo de tecnologia.

Existem casos de aplicação recentes e exitosas, inclusive no Município de Lajeado, de implantação de sistemas de videomonitoramento em via pública, com o intuito de ampliar a ação protetiva do Estado, através da visão eletrônica, permitindo uma ação efetiva do policiamento na intervenção precoce nos fatos que estão ocorrendo ou, então, na identificação e na descrição do evento ocorrido e de seus autores para as devidas responsabilizações, o que supostamente inibiria comportamentos criminosos e/ou violentos, prevenindo a ocorrência de delitos.

Nos ambientes de instalações públicas frequentemente nos deparamos com registros de diversos tipos de ocorrências, muitos deles atentando contra o patrimônio, a integridade dos cidadãos e dos profissionais que lá atuam. Entre estes registros, pode-se destacar furtos e roubos do patrimônio, extravio ou desvio de insumos, agressão física aos profissionais da prefeitura, ameaças, coações, depredação de patrimônio, tentativas de homicídio, dentre outros. Ponto crucial para o contexto exposto, é saber que o Município não dispõe de efetivo policial para se fazer presente em todos os prédios públicos, tornando necessário o emprego de tecnologias efetivas.

A instalação de câmeras de segurança em prédios públicos envolve não apenas questões técnicas, mas também considerações éticas e morais, uma vez que afeta diretamente o direito à privacidade dos cidadãos, menores de idade e servidores públicos que frequentam esses espaços. Esse cenário traz à tona uma importante discussão legal, que deve guiar a implementação de sistemas de vigilância de maneira equilibrada, respeitando tanto os direitos individuais quanto os interesses coletivos.

### **3. PANORAMA DA SEGURANÇA PATRIMONIAL NA PREFEITURA MUNICIPAL DE LAJEADO**

A legislação brasileira apresenta diversas normas e regulamentações que tratam das questões relacionadas com a proteção de bens, serviços, logradouros públicos municipais e instalações do Município. (Vide ADPF 995). É, portanto, fundamental que o poder público municipal manifeste ações para demonstrar conformidade com essas normas de modo que possam garantir a segurança dos cidadãos, servidores públicos, bens, benfeitorias e serviços públicos. Entre as normas existentes pode-se citar a Lei nº 13.022/2014, que “dispõe sobre o Estatuto Geral das Guardas Municipais e estabelece diretrizes para a elaboração de políticas públicas de segurança cidadã e dá outras providências”.

O monitoramento e a segurança patrimonial das unidades de governo do município são aspectos fundamentais para a preservação dos bens públicos, a manutenção da ordem e a proteção dos cidadãos que utilizam esses espaços. O avanço da tecnologia tem transformado esse cenário, proporcionando soluções cada vez mais eficazes para a vigilância e o controle de

áreas de grande circulação, como praças, prédios públicos, escolas, postos de saúde e prédios administrativos.

O monitoramento por câmeras (CCTV) é uma das soluções mais empregadas pelas administrações municipais para reforçar a segurança patrimonial, atuando essencialmente no desencorajamento de ações hostis e na obtenção e guarda de registros por meio de imagens. Câmeras inteligentes, quando integradas a sistemas de reconhecimento facial e análise de comportamento, permitem a identificação de situações suspeitas em tempo real, facilitando a ação rápida das equipes de segurança. Esse monitoramento pode ser centralizado em uma central de controle, onde operadores acompanham as imagens e acionam os órgãos competentes em caso de irregularidades.

Além disso, tecnologias como drones, cercas eletrônicas e sensores de movimento também têm sido utilizadas para aumentar a cobertura de segurança, principalmente em áreas de difícil acesso. Essas ferramentas proporcionam uma visão mais ampla e eficiente do território a ser protegido, contribuindo para a prevenção de crimes como vandalismo, roubo e invasão.

No entanto, a implementação dessas tecnologias deve ser acompanhada de políticas e regulamentações que garantam a privacidade dos cidadãos, prevenindo o uso indevido dos dados capturados. A Lei Geral de Proteção de Dados (LGPD) no Brasil impõe desafios às gestões municipais, que precisam assegurar o tratamento adequado das informações coletadas pelos sistemas de monitoramento.

Outro aspecto importante é a criação de um ponto central de monitoramento e a integração entre os sistemas da segurança patrimonial e da segurança pública. A cooperação entre os órgãos de segurança municipais e estaduais, como a Guarda Municipal e a Polícia Militar, é crucial para a eficiência do monitoramento, garantindo uma resposta mais rápida e coordenada em situações de risco.

Por fim, o panorama atual também evidencia a necessidade de investimentos contínuos em capacitação de pessoal, manutenção de equipamentos e atualização de sistemas. A segurança patrimonial municipal não se resume apenas à instalação de equipamentos, mas também envolve uma gestão eficiente e estratégica, que inclui planejamento, governança e uso adequado dos recursos disponíveis.

#### **4. REQUISITOS DA CONTRATAÇÃO (Art. 18, § 1º, III)**

A presente contratação está alinhada com as normas e procedimentos de segurança previstos para as unidades de governo do Município de Lajeado.

O serviço, objeto de contratação, encontra-se também alinhado com a Política de Tecnologia e Segurança da Informação e Comunicação (PTSIC), em especial no seu Capítulo III, artigo 6º:

#### **CAPÍTULO III**

## DOS PRINCÍPIOS ORIENTADORES DA PTSCI

Art. 6º A PTSIC possui princípios orientadores a serem considerados nas diretrizes, normas administrativas e procedimentos de TIC com impacto em ações de planejamento, implantação de serviços, programas e projetos relacionados à disponibilização e uso da infraestrutura tecnológica, considerando o canal de relacionamento com o cidadão e a sua integração aos processos existentes e que possam vir a existir no âmbito do Poder Executivo Municipal:

I - Uso Estratégico de TIC: prover serviços apoiados por plataformas digitais que suportem a estratégia de governo e o apoio à tomada de decisão, mediante organização de recursos, processos e técnicas, visando a obtenção, processamento, armazenamento, o uso e disseminação de informações;

II - Governança de TIC: manter um modelo de governança que vise assegurar o alinhamento das decisões e ações do DTI à estratégia de governo, priorizando o planejamento, a avaliação e o monitoramento centralizado dos serviços e projetos de TIC;

III - Foco no Cidadão: considerar os processos administrativos e o atendimento ao cidadão, visando a oferta de novos serviços e a melhoria dos atuais, com foco em princípios como mobilidade, simplicidade, usabilidade e acessibilidade, fortalecendo assim o canal de relacionamento entre governo e sociedade;

IV - Integração e digitalização dos Processos e Serviços: assegurar a integração e digitalização de processos e serviços, zelando pela padronização de tecnologias, serviços e soluções, objetivando sempre a racionalização e otimização dos recursos públicos;

V - Evolução dos serviços e soluções: monitorar as tendências tecnológicas com foco em pessoas, retenção de talentos e qualificação continuada, com vistas a mitigar os gaps tecnológicos e o tempo com tramitações desnecessárias;

VI - Da segurança e adequado tratamento da Informação: o tratamento das informações ocorre em diferentes meios de suporte, armazenamento comunicação, estando os mesmos expostos à vulnerabilidades, bem como, a fatores externos e internos que podem comprometer a sua segurança, daí a necessidade do adequado tratamento das informações

Entre os principais instrumentos de planejamento também estão o diagnóstico situacional, o plano de segurança, a definição de tecnologias adequadas, a capacitação de equipes e o estabelecimento de protocolos de resposta.

O diagnóstico situacional direciona para a necessidade de soluções centralizadas e vinculadas aos objetivos e diretrizes da segurança municipal. A solução de monitoramento e segurança patrimonial deve ser definida com critérios de compatibilidade e interoperabilidade aos serviços já existentes, bem como às estratégias de segurança do município.

A escolha das tecnologias adequadas e padronizadas é crucial, pois existem câmeras de monitoramento, sensores de movimento, cercas eletrônicas, drones e sistemas de alarme de diversos fabricantes e para finalidades distintas. Também deve-se considerar que essas tecnologias devem estar integradas em uma central de monitoramento, que permite o acompanhamento em tempo real e a rápida resposta a qualquer incidente.

Deverá ser provida capacitação adequada das equipes envolvidas, desde os operadores das centrais de vigilância até os agentes de segurança responsáveis por intervenções diretas com o objetivo de garantir que esses profissionais saibam lidar com as ferramentas tecnológicas e estejam preparados para agir de forma eficiente em situações de ameaças ou incidentes.

Por fim, é necessário definir e padronizar protocolos de resposta claros, que garantam a rápida atuação em caso de emergências, como tentativas de invasão, furtos ou vandalismo. As soluções hoje adotadas não são padronizadas e por vezes impedem o resgate de imagens em tempo hábil.

A solução a ser contratada deverá, obrigatoriamente, atender aos seguintes requisitos essenciais:

- Operação Contínua: Prestação dos serviços em regime 24x7x365 (vinte e quatro horas, sete dias por semana e trezentos e sessenta e cinco dias por ano).
- Detecção de intrusão e cruzamento de linha: Gerar alertas no sistema de monitoramento quando ocorrer intrusão em ambientes controlados por câmeras que possuem o recurso para tal.
- Disponibilidade: Garantia de disponibilidade mensal do serviço de, no mínimo, 99,5%.
- Armazenamento de Imagens: Retenção das imagens por um período de

30 dias em ambiente centralizado e disponibilizado pela CONTRATADA em nuvem privada ou pública, assumindo todos os custos da solução.

→ A solução proposta deve considerar a **possibilidade** de redundância em armazenamento local (interface para DVR ou NVR) por, pelo menos, 7 dias para garantir (quando necessário) a gravação nos casos de falha de comunicação.

- Qualidade de Imagem: As câmeras deverão suportar captura em alta definição mínima de Full HD (2 Megapixels).
- Inteligência Artificial (IA): A CONTRATADA deve apresentar solução que permita futura incorporação de recursos de IA ao sistema de gestão de imagens, como:
  - Reconhecimento facial para controle de acesso e alerta de pessoas não autorizadas.
  - Análise forense para otimizar investigações.
  - Avaliação e análise comportamental.
  - Detecção de objetos que representem ameaça, assim como armas de fogo.
- Infraestrutura: Fornecimento de toda a infraestrutura necessária para cada local em regime de locação com opção de reversão, incluindo câmeras Full HD, switches gerenciáveis POE+ e POE++, racks e demais passivos de rede como ferragens, eletrocalhas, eletrodutos, parafusos etc. Toda a infraestrutura será transferida para o patrimônio da Prefeitura Municipal de Lajeado após o término do contrato.
- Suporte e Manutenção: Serviço completo de suporte técnico, manutenção preventiva e corretiva, e reposição de equipamentos com Acordo de Nível de Serviço (SLA) definido.

## 4.1 Requisitos de Segurança da Informação

Durante a manutenção de equipamentos e gestão dos serviços de gerenciamento, os seguintes requisitos de segurança deverão ser seguidos de modo a garantir a disponibilidade e integridade das informações:

- A CONTRATADA deverá garantir a segurança das informações da Prefeitura Municipal de Lajeado, e se compromete a não divulgar ou

fornecer a terceiros quaisquer dados e informações que tenha recebido da Prefeitura;

- A manutenção dos equipamentos deverá ser realizada, preferencialmente, nas dependências da Prefeitura. Havendo necessidade de remoção dos mesmos para as dependências da empresa CONTRATADA, as despesas de transporte, seguros e embalagens, correrão por conta da empresa CONTRATADA;
- Somente os técnicos da empresa CONTRATADA, ou pessoas de outra empresa, a quem ela autorizar por escrito, poderão executar os serviços de manutenção;
- Os técnicos, ou pessoas autorizadas pela empresa CONTRATADA, deverão apresentar, no ato do atendimento, credenciamento (crachá da empresa) e documento oficial de identidade pessoal com foto, para efetuar qualquer serviço nas dependências da Prefeitura Municipal;
- A CONTRATADA se obriga a tratar como informações sigilosas e privadas da Prefeitura Municipal de Lajeado quaisquer informações, dados, controle de uso e relatórios relacionados à prestação dos serviços, não podendo revelá-los ou facilitar informações de terceiros;
- A CONTRATADA se compromete a tomar providências, quando de sua competência, para reduzir ou solucionar as causas relacionadas aos incidentes e/ou problemas de segurança da informação, quando identificados que são de sua responsabilidade;
- A CONTRATANTE se compromete em comunicar imediatamente e oficialmente à CONTRATADA sob incidentes, falhas, problemas e/ou riscos relacionados à segurança das informações e dados envolvendo os produtos contratados;
- Toda a comunicação realizada entre dispositivos envolvendo o ambiente de rede, bem como informações da Prefeitura (seja na entrada como saída), deve estar protegida por protocolos de criptografia de ponta-a-ponta e túneis seguros (como TLS 1.3 ou superior), em conformidade com as normas **ISO/IEC 17799, ISO/IEC 27001/27002** e as diretrizes de segurança da **Lei Geral de Proteção de Dados (LGPD)**.

- Definição de critérios para a sanitização de dados (limpeza de discos rígidos) em equipamentos substituídos ou devolvidos para evitar vazamento de imagens.
- Além dos pontos acima, a CONTRATADA deverá apresentar declaração de que tem pleno conhecimento das condições necessárias para a prestação do serviço como requisito para celebração do contrato.

## 4.2 Requisitos de suporte, manutenção e reposição de equipamentos

Após a implantação da solução, a CONTRATADA deverá realizar, de forma contínua e sem interrupções, todos os procedimentos de aquisição, recebimento, estocagem, transporte, distribuição e substituição dos equipamentos e insumos, mantendo disponibilidade de estoque suficiente para garantir os níveis de serviços acordados.

O fornecimento de todos os equipamentos e eventuais insumos necessários à prestação dos serviços de monitoramento e alerta, correm por conta da CONTRATADA.

A CONTRATADA também deverá prestar serviço contínuo de manutenção preventiva e corretiva, em conformidade às orientações técnicas estabelecidas pelo fabricante. Instalação e substituição de equipamentos após detecção e ou comunicação de problema por parte da CONTRATANTE.

## 4.3 Dos sistemas de chamados e de monitoramento e alerta do parque de equipamentos e serviços

- A CONTRATADA deverá disponibilizar e manter software de monitoramento dos equipamentos com o objetivo de constatar rapidamente ou até com antecedência problemas de conexão, captação e armazenagem das imagens ou qualquer outra situação que impacte na qualidade e disponibilidade do serviço prestado, devendo este monitoramento criar automaticamente chamados técnicos (em ferramenta sob responsabilidade da CONTRATADA) e disparar a demanda para o pronto atendimento da equipe da CONTRATADA;
- Uma solução de gerenciamento de chamados técnicos também deverá estar contemplada nos serviços, de forma que qualquer usuário possa registrar e acompanhar as demandas técnicas. O referido sistema deverá ser alimentado automaticamente pela solução de monitoramento dos equipamentos;

- A CONTRATADA deverá disponibilizar linha telefônica e sistema de chamados técnicos para a abertura de Chamados de Suporte Técnico em sua Central de Atendimento, e fornecer Protocolo de Atendimento, com possibilidade de acompanhamento online ou por outro meio, por parte da Prefeitura, possibilitando obter informações em tempo real sobre o andamento do chamado técnico.
- Ambos os sistemas (de monitoramento e chamados técnicos) deverão ficar armazenados em ambiente de nuvem (privada ou pública), sob responsabilidade da CONTRATADA, cabendo-lhe todas as responsabilidades e ações necessárias para garantir o perfeito e adequado funcionamento, assim como a conformidade aos requisitos de segurança necessários;
- Todas as demandas de atendimento (inseridas automaticamente, bem como de forma manual) deverão ser registradas no sistema de chamados, com geração de protocolo/nº de chamado, de forma que ambas as partes possuam acesso ao relatório de ocorrências registradas.

#### 4.4 Da forma de atendimento e prestação de suporte

Entende-se como suporte de primeiro nível aquele que desempenha ao menos as atividades de resolução de problemas comuns como reposicionamento de câmeras, substituição de equipamentos defeituosos, instalação e reinstalação de equipamentos e drivers, orientação sobre uso dos equipamentos, configurações e manutenções básicas. Problemas e demandas mais complexas poderão ser encaminhados para níveis superiores de suporte da CONTRATADA.

Para fins de cumprimento dos níveis de acordo de serviço, considera-se a soma dos tempos de ambos os níveis de suporte, quando for o caso.

Para este profissional, empregado pela CONTRATADA, sob regime empregatício direto (CLT), será a CONTRATADA a única responsável por todos e quaisquer encargos trabalhistas, impostos, execuções judiciais, ficando desde já acordado que a Prefeitura não é solidária ou corresponsável a qualquer tipo de ação que estes empregados venham a mover contra quaisquer uma das partes e, em especial, fica claro que não existirá qualquer tipo de vínculo empregatício entre os empregados da CONTRATADA e a Prefeitura.

Todos os empregados disponibilizados pela CONTRATADA deverão ser treinados em equipamentos e softwares iguais ou similares aos fornecidos por ela. A

Prefeitura, no início da prestação dos serviços ou a qualquer tempo, poderá solicitar a comprovação dos treinamentos.

Unicamente para a prestação dos serviços de suporte de primeiro nível (ajustes, substituições e configurações básicas), poderá a CONTRATADA proceder com a quarteirização do serviço junto à alguma empresa parceira, ficando esta responsável por todo e qualquer ônus, compromisso e responsabilidade, não recaindo qualquer obrigação de qualquer natureza para a Prefeitura.

Caso a CONTRATADA opte por prestar o serviço de suporte de primeiro nível por intermédio de empresa parceira, deverá informar formalmente a Prefeitura, por escrito, da relação e dos serviços que serão prestados, cabendo à Prefeitura aceitar ou não.

A CONTRATADA, após concluído o serviço de manutenção, será responsável pela imediata retirada de peças, materiais descartados e quaisquer outros resquícios das dependências da Prefeitura. As peças que substituirão outras defeituosas deverão ser novas e originais do fabricante do equipamento.

As manutenções devem ser realizadas de modo a causar o mínimo de interferência no ambiente e na rotina de seus ocupantes ou usuários. Os ambientes devem ser mantidos em perfeitas condições de limpeza, higiene e segurança, durante e após a conclusão dos serviços.

A CONTRATADA deverá elaborar um Relatório de Atendimento Técnico para cada chamado de suporte técnico atendido e concluído. Este relatório deve incluir as seguintes informações: horário do chamado, horário de início do atendimento, horário de conclusão dos serviços, número do protocolo de atendimento, identificação dos equipamentos que apresentaram defeito, descrição dos serviços executados, nome do responsável pelo atendimento, e quaisquer outras observações relevantes para o caso.

## 4.5 Do acordo de nível de serviço

Em caso de necessidade de troca de equipamento, os mesmos deverão ser realizados em até 2 dias úteis após a identificação e notificação do problema. A CONTRATANTE considerará o problema efetivamente solucionado quando a equipe responsável por administrar o contrato receber a confirmação pelo usuário da conclusão do chamado. O chamado rejeitado pela equipe será reaberto quantas vezes for necessário, não cabendo ônus por parte dos reclamados.

Para efeito de cumprimento dos Acordos de Níveis de Serviço estabelecidos, considera-se prazo para solução do problema o período compreendido entre o horário da abertura do chamado de suporte técnico feito pela Prefeitura e o horário de término

da solução, quando o equipamento e ou o serviço estiver em condições normais de operação.

Deverão ser considerados e respeitados os seguintes prazos:

**Quadro 04:** Do acordo de nível de serviço a ser praticado

|                           | <b>GRAVIDADE</b>     | <b>Situações</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                              | <b>Prazos</b>        |
|---------------------------|----------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------|
| <b>Tempo de Resolução</b> | Incidentes Críticos  | Englobam qualquer falha, indisponibilidade ou evento de alta gravidade que comprometa a prestação global do serviço ou impeça o cumprimento das finalidades essenciais do sistema. <ul style="list-style-type: none"> <li>• <b>Exemplo:</b> Queda total ou parcial do link WEB, parada ou queda total ou parcial do sistema de armazenamento, processamento, interrupção do acesso às imagens ou ao painel central de controle das câmeras. Queda total de uma unidade de governo.</li> </ul> | Dentro de 1 dia útil |
|                           | Incidentes Moderados | Referem-se a interrupções ou defeitos em pontos focais ou equipamentos isolados que não representam a parada global da solução ou a parada total de uma unidade de governo. <ul style="list-style-type: none"> <li>• <b>Exemplo:</b> Defeito técnico em uma câmera específica, switch ou necessidade de substituição de um switch em uma unidade isolada.</li> </ul>                                                                                                                          | 2 dias úteis         |
|                           | Incidentes Menores   | Abrangem solicitações de suporte, ajustes de rotina e demandas administrativas que não interferem na operação principal ou na integridade do sistema. <ul style="list-style-type: none"> <li>• <b>Exemplo:</b> Necessidade de orientação para extração de relatórios ou solicitação de</li> </ul>                                                                                                                                                                                             | Até 6 dias úteis     |

|  |  |                                      |  |
|--|--|--------------------------------------|--|
|  |  | configuração de usuários no sistema. |  |
|--|--|--------------------------------------|--|

A disponibilidade dos serviços de armazenamento e visualização central deve ter uma garantia mensal de *Uptime SLA (Service Level Agreement)* de 99,5% que representa um tempo máximo de parada anual não programado de 1 dia 19 horas 49 minutos e 45 segundos.

## 5. LEVANTAMENTO DE SOLUÇÕES (Art. 18, § 1º, IV)

Considerando a infraestrutura de fibra óptica de 1 Gbps que conecta as unidades a um ponto central (contrato vigente), foram identificadas e analisadas as seguintes arquiteturas de solução para atender aos requisitos:

- Solução 1 - Modelo On-Premise: A infraestrutura de servidores e armazenamento principal é alocada no Data Center da própria Prefeitura. A CONTRATADA entrega os equipamentos em comodato, e todo o tráfego de imagens converge para a estrutura municipal.
- Solução 2 - Modelo 100% em Nuvem (Cloud): As câmeras e switches são instalados nas unidades, mas todo o armazenamento e processamento de imagens e IA ocorrem em um provedor de nuvem pública (ex: AWS, Azure, Google Cloud).
- Solução 3 - Modelo Híbrido: Cada unidade possui um gravador local (NVR) responsável pelo armazenamento principal. Apenas eventos específicos, alertas de IA ou trechos de vídeo sob demanda são replicados para um ambiente em nuvem para backup ou análise avançada.
- Solução 4 - Modelo Hospedado em Data Center de Provedor de Conectividade Local (IX.Lajeado): A infraestrutura de servidores e armazenamento é alocada no Data Center de um provedor de acesso WEB com acesso ao IX.Lajeado (Ponto de Tráfego da Internet). O tráfego de imagens ocorre dentro da rede do provedor e da rede da PML, sem consumir um link de internet externo. No caso de necessitar conexão externa, esta será de responsabilidade da CONTRATADA, devendo considerar equipamentos e custo do acesso WEB.

## ANÁLISE COMPARATIVA DAS SOLUÇÕES (Art. 18, § 1º, V)

| <b>Critério</b>                  | <b>Solução<br/>(On-Premise)</b>                                                                                  | <b>Solução<br/>(Nuvem<br/>externa)</b>                                                         | <b>Solução<br/>(Híbrido)</b>                                                       | <b>Solução<br/>(VSaaS)</b>                                                                           |
|----------------------------------|------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------|
| <b>Custo de Link de Internet</b> | <b>Muito Baixo.</b><br>Necessário apenas para acesso remoto eventual.                                            | <b>Muito Alto.</b><br>Requer link de upload massivo e caro para o fluxo de 1.000 câmeras 24/7. | <b>Moderado.</b> O upload é limitado a eventos, mas pode gerar picos de consumo.   | <b>Praticamente Nulo.</b> O tráfego é interno à rede por meio de provedores que acessam o IX.Lajeado |
| <b>Custo de Infraestrutura</b>   | <b>Alto.</b> Exige investimento e manutenção do Data Center municipal (energia, climatização, segurança física). | <b>Baixo.</b> Elimina a necessidade de um Data Center local robusto.                           | <b>Distribuído.</b> Custo elevado pela necessidade de 95 NVRs robustos.            | <b>Baixo.</b> A infraestrutura é de responsabilidade do provedor.                                    |
| <b>Escalabilidade</b>            | Limitada à capacidade local                                                                                      | Escalabilidade elástica (pode aumentar custo)                                                  | Distribuída (depende da capacidade de cada NVR + espaço na nuvem)                  | Relativamente fácil de expandir junto ao provedor (se ele tiver capacidade e SLA)                    |
| <b>Hospedagem (30 dias)</b>      | Storage local no data center municipal                                                                           | Armazenamento total na nuvem (custo OPEX pode ser significativo a longo prazo)                 | Principais gravações nos NVRs; nuvem recebe apenas incidentes ou recortes de vídeo | Storage no data center do provedor (custos mensais, porém sem custo extra de link) OPEX              |

| <b>Critério</b>          | <b>Solução (On-Premise)</b>                                                                              | <b>Solução (Nuvem externa)</b>                                                                 | <b>Solução (Híbrido)</b>                                                                 | <b>Solução (VSaaS)</b>                                                                                                                  |
|--------------------------|----------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------|
| <b>Gestão e Operação</b> | <b>Complexa.</b><br>Exige equipe de TI local para gerenciar servidores, storage e infraestrutura física. | <b>Simples.</b> A gestão da infraestrutura é terceirizada para o provedor de nuvem.            | <b>Muito Complexa.</b><br>Gerenciamento distribuído de 95 equipamentos distintos (NVRs). | <b>Simples.</b><br>Gestão da infraestrutura terceirizada completa ( <i>data center</i> , <i>link</i> de Internet e software de gestão). |
| <b>Riscos Principais</b> | Ponto único de falha no Data Center municipal. Custo de manutenção e escalabilidade.                     | Dependência total do link de internet. Custos mensais podem escalar e se tornar imprevisíveis. | Falhas individuais nos NVRs. Complexidade de suporte e padronização.                     | Dependência contratual ( <i>lock-in</i> ). Menor controle físico sobre os dados.                                                        |
| <b>Vantagens</b>         | Soberania total sobre os dados. Baixa latência.                                                          | Alta escalabilidade. Acesso remoto facilitado.                                                 | Resiliência local (gravação contínua sem internet). Custo de link controlado.            | Custo de link quase nulo. Infraestrutura profissional. Simplicidade de implementação.<br><br>Baixa latência e alta escalabilidade       |
| <b>Desvantagens</b>      | Custo de manter data center e energia, risco de falha local                                              | Alto custo de link, possível custo variável enorme, dependência total da nuvem                 | Muitos dispositivos (NVRs) para manter, risco de falha local sem redundância             | Dependência contratual de provedor local, menor soberania sobre dados físicos, lock-in                                                  |

## 6. SOLUÇÃO ESCOLHIDA E JUSTIFICATIVA (Art. 18, § 1º, V e VI)

Com base na análise comparativa, a **Solução 4 - Modelo Hospedado em Data Center de Provedor de Conectividade Local** apresenta-se como a mais vantajosa para a

Administração Municipal. Considera-se neste cenário o fácil acesso da infraestrutura de comunicação e rede a partir do IX-Lajeado, do qual o município faz parte.

### **Avaliação:**

- Cenário A (On Premise):

Indicado quando há investimento prévio em data center robusto e equipe técnica capacitada.

Menor custo de banda, mas maior responsabilidade em infraestrutura interna.

- Cenário B (Cloud):

Focado em escalabilidade e simplicidade de gestão, mas com alto custo de link e maior custo de armazenamento contínuo na nuvem.

Bom para situações em que o município quer evitar qualquer expansão de seu data center e aceita o custo operacional (OPEX) de nuvem.

- Cenário C (Híbrido):

Gravações locais em NVRs reduzem a dependência de link; a nuvem serve como backup/IA, com transmissão apenas de incidentes.

Complexidade maior na manutenção de 95 NVRs.

- Cenário D (Data Center de Provedor Local):

Garante uso da infraestrutura profissional do provedor sem custos de link adicionais.

Dependência significativa desse provedor local, podendo haver risco de lock-in e negociações contratuais complexas.

Em termos de custo de hospedagem para 30 dias de retenção, os cenários B e D inevitavelmente terão um componente de mensalidade (storage e processamento em nuvem ou no DC do provedor). O cenário A concentra esse custo na infraestrutura local (energia, refrigeração, espaço físico). Já o cenário C dilui a exigência de grande *storage* central, pois cada unidade armazena localmente — contudo, soma-se o custo de gerenciar 95 gravadores.

Por fim, quanto ao custo de link de acesso web, O Cenário B é onde se verifica o maior custo de link, pois todo o fluxo de 1000 câmeras precisa subir para a nuvem. O Cenário C exige link moderado para envio de incidentes/eventos e os Cenários A e D praticamente não demandam grande link externo, pois a gravação acontece on premise (A) ou dentro da rede do provedor (D).

### **Justificativa:**

A escolha se fundamenta na busca pela melhor relação **custo-benefício-risco**. A Solução 4 neutraliza a principal desvantagem do modelo em nuvem (Solução 2), que seria o **custo proibitivo de um link de internet** para o tráfego de 1.000 câmeras. Ao mesmo tempo, ela oferece os benefícios de uma infraestrutura de Data Center profissional (segurança, redundância de energia e climatização), eliminando os riscos e os custos de capital e operacionais que a Prefeitura teria ao manter uma estrutura própria (Solução 1).

Embora a Solução 3 (Híbrida) ofereça resiliência, sua complexidade de gerenciamento e manutenção de 95 equipamentos distribuídos representa um risco operacional e um custo oculto significativo. Portanto, a Solução 4 emerge como a arquitetura mais equilibrada, financeiramente previsível e operacionalmente eficiente para o escopo do projeto.

## 7 Descrição da solução como um todo

A solução escolhida foi a solução de contratação de prestação de serviço de monitoramento e segurança patrimonial com emprego de infraestrutura computacional hiperconvergente totalmente terceirizada e em nuvem por meio de hospedagem em *Data Center* (público ou privado) administrado pela CONTRATADA. Este modelo integra um conjunto de recursos, compreendendo recursos tecnológicos de hardware, software, treinamento, transferência tecnológica (*hands-on*), migração de dados, operação assistida e manutenção de modo a compor um conjunto de recursos computacionais virtualizados, com armazenamento distribuído definido por software.

A contratação será dividida em grupos com adjudicação por lote, vedada a adjudicação por item. A modalidade de pregão eletrônico será usada, sendo o regime adotado empreitada por preço global, com critério de menor preço global por lote. O grupo terá um valor global, mas todos os itens do grupo devem ser precificados individualmente.

Não será permitido o fornecimento parcial de itens de qualquer dos grupos.

Para a solução de monitoramento e segurança patrimonial com emprego de infraestrutura computacional hiperconvergente, a empresa vencedora do certame licitatório deverá fornecer minimamente, de acordo com as especificações e quantitativos de cada local informado no Termo de Referência, os seguintes itens ou serviços:

- Infraestrutura computacional hiperconvergente;
- Infraestrutura local e de comunicação;

- Solução de reconhecimento facial;
- Solução de controle de perímetro, intrusão e presença física;
- Implantação;
- Treinamento, operação assistida e manutenção da solução.
- Ao finalizar o contrato, mesmo com o sistema inoperante, a CONTRATADA deverá manter as imagens disponíveis para consulta ou resgate à CONTRATANTE por um período de 30 dias contados a partir do distrato, salvo registros atrelados a processos judiciais ou sindicância, os quais devem ser exportados para a CONTRATANTE.

De maneira geral, em relação aos componentes da solução, as suas respectivas definições serão abordadas nos tópicos a seguir.

## 7.1 Infraestrutura computacional hiperconvergente

Infraestrutura hiperconvergente é uma arquitetura centrada em software que integra fortemente os recursos de computação, armazenamento e virtualização em um único sistema. As empresas modernas dependem do *data center* para fornecer os recursos de computação, armazenamento, rede e gerenciamento necessários para hospedar cargas de trabalho e dados corporativos vitais. *Data centers* podem ser lugares notoriamente complexos onde uma infinidade de fornecedores competem para fornecer uma miríade de dispositivos, sistemas e softwares diferentes. Essa mistura heterogênea muitas vezes luta para interoperar e raramente alcança o pico de desempenho para o negócio sem otimizações cuidadosas e demoradas. Hoje, as equipes de TI simplesmente não têm tempo para enfrentar os desafios de implantação, integração e gerenciamento de data centers exigidos por ambientes heterogêneos tradicionais.

A noção de convergência surgiu originalmente como um meio de enfrentar os desafios da heterogeneidade. No início, um único fornecedor reuniria os sistemas e softwares de diferentes fornecedores em um único conjunto pré-configurado e otimizado de equipamentos e ferramentas que eram vendidos como um pacote. Isso era conhecido como infraestrutura convergente, ou IC. Mais tarde, os fornecedores de convergência deram o próximo passo para projetar e produzir sua própria linha de equipamentos de computação, armazenamento e rede pré-embalados e altamente integrados para o data center. Foi um passo evolutivo agora chamado infraestrutura hiperconvergente.

A infraestrutura hiperconvergente baseia-se nas duas premissas essenciais de integração e gestão, que surgiram como forma de resolver dois dos problemas mais

desconcertantes dos data centers heterogêneos tradicionais: desempenho abaixo do ideal e gestão de sistemas fraturada e problemática. O objetivo é fornecer recursos virtualizados para computar, armazenar e escalar recursos de rede para que todos sejam identificáveis e gerenciáveis através de uma única plataforma.

Ambientes corporativos são amplos, densos e bastante movimentados. Esse contexto propicia diversos comportamentos que geram insegurança e dificultam muito o controle de tais ações. É preciso encarar não só as possibilidades internas, mas também as externas. A partir do momento em que temos a real dimensão dos riscos, conseguimos nos proteger com mais eficácia.

O uso de câmeras ainda é o modo mais garantido de manter a segurança em um espaço. Com esse método, as unidades de governo podem contar com um sistema de vigilância integrado a uma central de monitoramento, com armazenamento de dados, profissionais altamente treinados para respostas imediatas e monitoramento 24h por dia, 7 dias por semana.

O sistema de monitoramento deve contar com câmeras de qualidade posicionadas estrategicamente. A instalação das câmeras deve seguir etapas muito importantes para que todos possam se beneficiar. Após uma vistoria do espaço realizada pela equipe, o CFTV é instalado de acordo com os pontos ideais para observação de todo o espaço, sem pontos-cegos. Com os ângulos corretos e a quantidade apropriada de câmeras, a unidade monitorada ficará sempre protegida.

A solução deverá permitir o emprego de recursos de Inteligência Artificial para aprender e detectar eventos em câmeras de monitoramento. A inteligência artificial é baseada em redes neurais artificiais, que são algoritmos que tentam imitar o comportamento do cérebro humano. Operacionalmente podemos considerar uma rede neural como uma “caixa de processamento” que pode ser treinada para que, a partir de um conjunto de dados de entrada (inputs), possa gerar uma ou mais saídas (outputs), permitindo “ensinar” e “treinar” a aplicação para que reconheça um objeto específico em diversas imagens ou contabilize quantas vezes o objeto aparece, sendo possível reduzir a quantidade de alarmes “falso positivo”.

Os recursos de IA, embora devam ser suportados pela proposta vencedora como um recurso a ser adicionado no futuro, deve ser disputado como um objeto específico a ser contratado em separado sob demanda para os casos específicos de uso por meio de um processo de licitação específico.

O panorama a ser ofertado consiste no emprego de equipamentos de videomonitoramento inteligentes, dotados de processamento local, interligados a armazenamento em nuvem pública ou privada. O sistema deve permitir

armazenamento local e em nuvem, além de permitir o emprego de outras características, como:

- Captura da biometria facial e registro, com análise comparativa com o banco de dados pré-cadastrado;
- Disponibilidade de relatório pré-configurado para consulta de acesso.
- Alarme via metadados de barreiras pré-configuradas;
- Pré agendamento de horários para ativação de alarmes;
- Alarme de detecção de movimento;
- Análise de intrusão;
- Detecção de armas de fogo, pessoa com posicionamento suspeito, capacete de moto, máscara, chapéu, boné, celular, mãos, pessoas, fogo e fumaça;

Na solução prevista não será empregada a definição tradicional de datacenter, devendo, de forma geral, o processamento e o armazenamento ocorrerem em infraestrutura de nuvem. A solução deverá ser provida de mecanismos que permitam a rápida adição de equipamentos aos sistemas de controle. Softwares que necessitem da utilização de servidores de rede físicos deverão ter estrutura adequada a seu funcionamento.

Deverá haver a possibilidade de implantação de salas de monitoramento, que são sistemas profissionais de monitoramento, os quais permitem a integração de diversos subsistemas, monitorando centenas de câmeras num único local. Isso significa que uma única sala de controle pode centralizar a vigilância de diversas unidades de governo de Lajeado. Sistemas de vigilância modernos permitem monitorar diferentes edifícios por várias centrais de monitoramento, em tempo real e de forma simultânea.

Essas soluções permitem dupla vigilância, onde os alertas podem ser compartilhados imediatamente com o pessoal de segurança por qualquer profissional autorizado.

Além disso, recursos sofisticados de vigilância como a criação de barreiras eletrônicas, sistemas que calculam a velocidade de deslocamento e soluções de reconhecimento facial também podem disparar alertas.

## 7.2 Infraestrutura local e de comunicação

A rede de comunicação de dados deve contemplar o acesso a rede de dados nos pontos de monitoramento. A solução de comunicação de dados deve, minimamente, conter camada de distribuição e camada de acesso.

A camada de distribuição é o segmento da rede de comunicação em cada unidade do município, responsável pela capilaridade e distribuição dos pontos de acesso, a partir da infraestrutura de rede e comunicação de dados já existentes e mantidos pela prefeitura.

Todas as unidades de governo já estão interligadas por meio de cabos de fibra óptica com a tecnologia de *VLAN Stacking* ou QinQ (802.1ad), concentrados no *data center* da prefeitura.

Caso haja a necessidade de comunicação externa (Internet), a CONTRATADA é responsável pelas instalações e custos do link, o qual deve ser dimensionado a suportar toda a demanda gerada pelo somatório de banda requerida pelas câmeras instaladas.

Os pontos de acesso final serão providos a partir de switches com suporte a POE+ e POE++, dispositivos responsáveis pelo acesso e distribuição da comunicação com as câmeras de monitoramento na abrangência da rede local. Itens fornecidos pela CONTRATADA.

A solução também deverá contemplar a infraestrutura de dutos, eletrodutos e/ou canaletas, cabeamento apropriado para cada tipo de dispositivo a ser instalado e ativado, respeitando integralmente os padrões já existentes. Itens fornecidos pela CONTRATADA. Neste caso, visitas técnicas poderão ser solicitadas, desde que respeitados os prazos estabelecidos no edital.

## 7.3 Solução de reconhecimento facial, acesso e presença

A solução de reconhecimento facial está baseada em sistemas de análise inteligente de imagens com reconhecimento facial, sendo desejado emprego de inteligência artificial.

Cada unidade é uma comunidade que inclui dezenas, senão centenas de pessoas, quer sejam cidadãos, administradores, prestadores de serviços ou servidores públicos. A análise de vídeo, embasado por estatísticas e análise de imagens, acaba se tornando a melhor maneira de otimizar as atividades internas e os fluxos de trabalho. Com a realização de análises de presença se torna mais fácil descobrir quais são as horas críticas com maior fluxo de pessoas.

O algoritmo empregado poderá permitir o controle de presença de visitantes autorizados no local e responder, de forma instantânea, à existência de pessoas não autorizadas nos edifícios da administração pública. O sistema deve detectar rostos no fluxo de vídeo em tempo real, verificando listas de observação, com envio de notificações quando da detecção de correspondências.

A solução de segurança de presença e acesso está baseada em sistemas de análise inteligente de imagens. Deve empregar software com as seguintes características mínimas obrigatórias:

- O software ofertado deve ser capaz de visualização de um determinado vídeo para fins de análise investigativa;
- O software ofertado deverá ser capaz de indexar as imagens capturadas adicionando, às mesmas, uma marcação com pelo menos hora e minuto (no formato hh:mm) do acontecimento de cada um dos eventos, de forma tal que o usuário veja, em tempo real e durante a visualização do resumo, o momento exato do acontecimento de cada evento;
- O software ofertado não poderá, de nenhuma forma, alterar e/ou editar o vídeo original para executar qualquer das funcionalidades exigidas neste pleito - o resumo criado deverá existir independentemente do vídeo original. O vídeo original deve manter-se inalterado para que não se perca sua eficiência jurídica;
- O software ofertado deverá aceitar os DVRs já instalados (legado) e permitir um canal de transmissão de vídeo, utilizando os protocolos RTSP ou RTMP (ou outro compatível), mesmo que estejam configurados com câmeras analógicas.
- O software ofertado deverá ser capaz de exportar qualquer trecho do vídeo original, escolhido aleatoriamente pelo usuário, pelo menos no formato de arquivo AVI com a possibilidade de, na hora da exportação, incluir hora e minuto do evento referente ao trecho exportado, bem como a sua marcação (bounding box);
- O software ofertado deverá ser capaz de exportar vários arquivos de vídeo das todas câmeras conectadas no VMS existente e processá-los;
- O software ofertado deverá ser capaz de exportar imagens congeladas retiradas do vídeo original, escolhidas aleatoriamente pelo usuário, pelo menos no formato de arquivo nativo e padrões comuns como JPEG, PNG e outros, com a possibilidade de, na hora da exportação, incluir hora e minuto dos eventos exibidos.

## 7.4 Implantação

Os serviços de implantação concentram todas as atividades necessárias para o correto funcionamento de todos os sistemas inteligentes. São atividades indispensáveis para o funcionamento das soluções a serem operacionalizadas enquanto a implantação estiver em curso.

## 7.5 Treinamento, operação assistida e manutenção da solução

A solução deverá contemplar o fornecimento de módulos adequados de treinamento e operação assistida, os quais deverão abranger cada item fornecido, propiciando às equipes de cada unidade o completo entendimento e a noção exata de manipulação e operação dos sistemas a serem implementados.

## 8. ESTIMATIVA DE QUANTIDADES E CUSTOS (Art. 18, § 1º, II e VI)

- **Quantitativo:** A contratação abrangerá a prestação de serviço para **as unidades de governo**, incluindo o fornecimento, instalação e manutenção de até **1.200 câmeras** e toda a infraestrutura de rede e armazenamento associada.
- **Estimativa de Valor:** O valor estimado da contratação será apurado na fase de pesquisa de preços, com base em cotações formais de fornecedores que oferecem a solução no modelo de serviço hospedado em Data Center de provedor (Solução 4), considerando o custo mensal por ponto (câmera) ou um valor global para o serviço.

## 9. RESULTADOS PRETENDIDOS (Art. 18, § 1º, VII)

Espera-se, com esta contratação, alcançar os seguintes resultados:

- Redução dos índices de ocorrências (vandalismo, furtos) nas unidades monitoradas.
- Aumento da percepção de segurança por parte de servidores e cidadãos.
- Otimização do tempo de resposta a incidentes através de alertas em tempo real.
- Geração de provas materiais para processos investigativos.
- Centralização e padronização da gestão de segurança patrimonial do Município.

## 10. PROVIDÊNCIAS E PRAZOS (Art. 18, § 1º, VIII e IX)

- **Providências:** O presente Estudo Técnico Preliminar será encaminhado para a

elaboração do Termo de Referência (ou Projeto Básico), que detalha todas as especificações técnicas, obrigações e o Acordo de Nível de Serviço (SLA). Posteriormente, será realizada a pesquisa de preços formal.

- **Prazos:** Como as implantações (instalações iniciais) irão ocorrer por secretaria ou por unidade de governo, estas devem ocorrer em até 60 dias após emissão de cada empenho.

Declaração de Viabilidade:

Com base nos elementos apresentados, a contratação é considerada tecnicamente e economicamente viável.

## **11. Responsáveis pela Elaboração:**

Luis Antônio Schneiders

Diretor de Governo – Coordenadoria de TI e Modernização Administrativa

Patrícia Haenssger

Secretária de Administração