ESTUDO TÉCNICO PRELIMINAR

1. DESCRIÇÃO DA NECESSIDADE

1.1 Com a publicação da Lei n. 13.709/2018, intitulada como Lei Geral de Proteção de Dados – LGPD, ocorreu o regramento específico quanto à privacidade e proteção de dados pessoais no Brasil, sendo tal norma aplicável ao Setor Público e Privado, nos termos dos arts. 1º e 3º do diploma legal. O Setor Público ocupa um papel de destaque quanto ao tratamento de dados pessoais, visto que há necessidade recorrente de tratamento desse tipo de dado no exercício de suas atividades administrativas e na prestação do serviço público.

1.2 Nesse sentido, a Lei Geral de Proteção de Dados estabelece princípios e regras claras que devem ser respeitadas na atividade de tratamento de dados pelo Setor Público, em consonância com diversos métodos e normatizações de Segurança da Informação.

1.3 O Tribunal de Contas do Estado de RJ, no mês de janeiro de 2023, realizou auditoria em todos os seus 91 (noventa e um) municípios jurisdicionados e percebeu que o nível de maturidade de entidades públicas é extremamente inexpressivo. Por isso, determinou a realização de diversas medidas para que o Setor Público fosse melhorado. O processo de n. 206972-5/2022, que versa sobre a recomendação aos municípios demonstra a vulnerabilidade que municípios se encontram conta ataques cibernéticos.

1.4 Não são raras as situações em que Entidades Públicas são alvos diretos de ataques cibernéticos, havendo sequestro ou mesmo eliminação de dados de suma importância para as atividades administrativas e de governo. Segundo o Acórdão n. 1.768/2022 do Tribunal de Contas da União (TCU), após diversos levantamentos e estudos técnicos, incluindo incidentes ocorridos a nível de Ministério da Saúde, houve a conclusão da precariedade da Segurança da Informação no Setor Público Brasileiro e a premente necessidade de adequação frente a crescente onda de ataques cibernéticos. Veja-se:

> Conforme relatou a unidade técnica, o Brasil segue nas primeiras posições dos rankings internacionais no que tange à perpetração de ataques cibernéticos. Segundo narrou, o Brasil ocupou a oitava posição do mundo em número de ataques a dispositivos da internet das coisas (IOT) no período de abril a junho de 2021 e o quinto lugar em ataques de sequestro de dados em meados de 2021. Ainda de acordo com informações da empresa Fortinet, que coleta e analisa incidentes em todo o

mundo, em 2020 ocorreram 41 bilhões de tentativas de ataques cibernéticos na América Latina, sendo 8,4 bilhões no Brasil, número que, somente na primeira metade de 2021, subiu para 16,2 bilhões (Brasil).

1.5 No âmbito da administração pública, esse cenário é de extrema preocupação, conforme se observou no episódio do "apagão de dados" do Ministério da Saúde ocorrido em plena pandemia mundial da Covid-19, afetando de maneira central o monitoramento dos casos de Covid, tanto por instituições de saúde, quanto pelos órgãos de imprensa e pela população em geral.

1.6 Segundo cenário mapeado pelo CTIR Gov, destacaram-se, em 2021, alertas emitidos sobre vulnerabilidades em sistemas de autenticação de usuários, ações maliciosas em ambientes de nuvem e ataques de ransomware diversos. O CTIR Gov apontou também tendência de ameaças cibernéticas às infraestruturas críticas e aos sistemas de informação governamentais[1].

1.7 O cenário se demonstrou ainda mais presente, a nível local, diante das notícias veiculadas acerca do ataque cibernético ocorrido na cidade de Araguari-MG, em que criminosos invadiram os servidores do município e excluíram um grande volume de dados. Tal fato decorreu, evidentemente, em razão de falhas de segurança, bem como da ausência de camadas de proteção na própria Entidade Pública. O prejuízo com tal incidente de segurança é significativo e se espalhou por todas as atividades do órgão governamental. Em que pese a notícia de exclusão de dados, o incidente poderia ter ocorrido em um grau ainda maior, caso tivesse ocorrido vazamento de dados pessoais, com afronta absoluta aos ditames da Lei Geral de Proteção de Dados (LGPD).

1.8 O ataque supramencionado ocorreu no mês de outubro de 2023 não só na cidade de Araguari-MG, mas também em outras localidades, tais como Teófilo Otoni, Divinópolis, Poços de Caldas, entre outras do estado de Minas Gerais. Tal fato revela ainda mais a precariedade de medidas de Segurança da Informação nos municípios mineiros.

1.9 A mera criação de documentos jurídicos, tais como Política de Privacidade, Termos de Uso, Política de Cookies, Aviso de Privacidade não é capaz de, efetivamente, proteger a Entidade Pública de incidentes de segurança e privacidade, vez que, apesar de regulamentar boas-práticas, requisitos, regras e princípios de proteção de dados, não oferece operacionalmente mecanismos de blindagem.

[1] (Disponível em: < https://pesquisa.apps.tcu.gov.br/redireciona/acordao-completo/ACORDAO-COMPLETO-2535414>

1.10 Por isso, faz-se necessário todo o processo de gestão de riscos, conforme previsão na ABNT NBR ISO/IEC 27001:2022, que estabelece que a instituição deve estabelecer e aplicar um processo de avaliação de riscos que estabeleça e mantenha critério de riscos de segurança da informação, que assegure que as contínuas avaliações produzam resultados comparáveis, válidos e consistentes, que identifique, analise e avalie tais riscos. Somente com um levantamento consistente de vulnerabilidades, gestão de riscos e aplicação de medidas tais como aquisição/atualização de firewall, políticas de controles de acesso, redundância de servidores, anonimização e criptografia de dados, política consistente de backups, é que se pode, de fato, criar uma maturidade da entidade quanto à Segurança da Informação.

1.11 Um dos principais pontos de adequação à LGPD é a implementação de um sistema de gestão e governança que permita à entidade a comprovação da conformidade de suas atividades com a LGPD e suportar todos os processos necessários à referida adequação. Esta gestão, se realizada de forma manual, acarreta uma sobrecarga evidente e potencializa os riscos e vulnerabilidades da Entidade Pública, visto que dificulta o acompanhamento efetivo dos planos de ações traçados, a avaliação do nível de maturidade da proteção de dados e a verificação do efetivo cumprimento aos requisitos legais. Ademais, o controle manual requer uma demanda significativa de recursos humanos, o que pode trazer maior oneração, maior tempo de adequação pela necessidade de diversos treinamentos e aperfeiçoamento, além de tornar o processo descontínuo por eventuais mudanças desses recursos.

1.12 Para o cumprimento dos requisitos legais, a entidade deve possuir registro de todo o processo de tratamento de dados pessoais, tais como o âmbito e a natureza dos dados, a forma e o fluxo de tratamento, demandando a necessidade de um mapeamento completo de todo esse fluxo.

1.13 O serviço de proteção de dados em suportes físicos tem o objetivo de mapear o armazenamento e uso de dados pessoais que não se encontram nos sistemas informatizados da entidade, permitindo a verificação de necessidade em se manter o documento físico em arquivo (de acordo com a tabela de temporalidade) e estabelecendo medidas de proteção e controle de acesso aos dados pessoais envolvidos. Essas medidas têm como base métodos e princípios de transformação digital e caminha em conformidade com a filosofia de Governo Digital instituída pela Lei n. 14.129/2021. Trata-se de mais uma forma de gestão documental eficiente e de desburocratização estatal com a garantia de proteção de dados de forma ampla, abrangendo suportes físicos e digitais da entidade.

1.14 A contratação de um serviço e solução especializada tem como finalidade a blindagem do Setor Público nos aspectos jurídicos, tecnológicos e gerenciais, permitindo à Entidade Pública ter o controle sobre os requisitos necessários à adequação, visibilidade sobre os dados pessoais que estão armazenados e facilidade em fornecer evidências de conformidade à Autoridade Nacional de Proteção de Dados (ANPD) e demais autoridades nas situações previstas na legislação e regulamentações. Esse processo deve garantir a devida proteção do órgão público em conformidade com a Lei Geral de Proteção de Dados e normas técnicas de Segurança da Informação, tais como as ISO/IEC 27.001, 27.002, 27.005, 27.701 e 29.184.

1.15 Com isso, levando-se em consideração a obrigação legal em adequar toda a atividade e estrutura de Entes Públicos às regras e princípios do Sistema de Privacidade, Proteção de Dados e Segurança da Informação, além da mitigação da possibilidade de serem impostas sanções em caso de descumprimento, indispensável é a contratação de empresa especializada na prestação de serviços e soluções para adequação da Administração Pública Municipal à Lei Geral de Proteção de Dados.

1.16 Resta evidente que se trata de um objeto de contratação frequente e que deve ser realizada por todas as Entidades que compõem o consórcio intermunicipal. Diante exposto, este consorcio através do objeto solicitado busca adequar a Administração Pública Municipal de seus componentes à legislação de proteção de dados vigente e implementar medidas de segurança da informação necessárias à blindagem contra crimes cibernéticos e vazamentos de dados.

1.17 O objeto deste estudo destina-se ao atendimento das demandas dos seguintes municípios:

Municípios	**Quantidade de servidores**	**Quantidade de Páginas (A4)**
Abadia dos Dourados	347	621.130
Cascalho Rico	438	784.020
Coromandel	1.389	2.486.310
Guarda Mor	657	1.176.030
Iturama	1.628	2.914.000
Lagamar	376	673.040
Lagoa Grande	492	880.680
Paracatu	4.082	3.500.000
Pedrinópolis	427	764.330

Pirajuba	456	816.240
Presidente Olegário	1.059	1.895.610
Sacramento	1.186	2.122.940
Uberaba	10.033	3.500.000
Unaí	2.909	3.500.000
Urucuia	785	1.405.000
Varjão de Minas	452	809.080
Vazante	1.368	2.448.720
CISALP	70	125.300

2. ÁREA REQUISITANTE

ÁREA REQUISITANTE	RESPONSÁVEL
SECRETARIA EXECUTIVA	LUCÉLIA SOARES DE LIMA

3. REQUISITOS DA CONTRATAÇÃO

3.1 Para atender às necessidades dos municípios consorciados ao CISALP, os serviços deverão ser prestados conforme as condições e especificações a seguir detalhadas.

ITEM	COD.	DESCRIÇÃO	UNIDADE	QUANT	VALOR UNITÁRIO	VALOR TOTAL
01	11325	Solução Informatizada de Privacidade, Gestão de Riscos e Segurança da Informação	Licença de uso mensal	216	R$ 5.275,00	R$1.139.400,00
02	11326	Solução Informatizada para Proteção de Dados em Acervo Documental Físico, contemplando controle de acesso, busca inteligente, rastreabilidade de uso, anonimização e mecanismos de prevenção à perda de dados	Licença de uso mensal	216	R$ 5.275,00	R$1.139.400,00
03	11327	Inventário e Mapeamento de Dados (ROTDP), Gestão de Riscos de Segurança da Informação, Implantação de Programa de Conformidade à LGPD, elaboração e revisão de políticas, medidas e	Servidor em sentido amplo (efetivo, comissionado, temporário, estagiário)	28.154	R$ 560,00	R$15.766.240,00

		ferramentas de Privacidade e Proteção de Dados.				
04	11328	Serviço de proteção e prevenção à perda de dados de acervo documental físico através de processo de digitalização de acervo documental de valor exclusivamente administrativo e aquisição de solução informatizada para leitura via OCR (optical character recognition), controle de acesso, logs de acesso, indexação e ferramenta de buscas inteligentes a partir de termos e expressões existentes no conteúdo do documento, bem como ferramenta de identificação e anonimização de dados pessoais em documentos digitalizados através de ferramenta de automatização e inteligência artificial que facilite a identificação e proteção de dados pessoais	Página A4	30.422.430	R$0,28	R$8.518.280,40
			VALOR TOTAL DE CONTRATAÇÃO			**R$ 26.563.320,40**

3.2 A contratação dos serviços elencados na tabela do item 3.1 deverão ser prestados por profissionais habilitados e com notória especialização que será comprovada por meio de atestados de capacidade técnica, diplomas, certificados e demais documentos correlatos que demonstram a sua expertise na área de Implementação, Gestão e Governança de Dados para conformidade com a Lei Geral de Proteção de Dados (Lei nº 13.709/2018), Segurança da Informação, serviço de prevenção à perda de dados e fornecimento de solução informatizada de privacidade, gestão de riscos e segurança quanto à Privacidade e Proteção de Dados Pessoais.

3.2.1 Os atestados de capacidade técnica para a execução de serviços no mínimo, deverá conter as seguintes informações:

3.2.1.1 Nome ou razão social, CNPJ e endereço completo do emitente;

3.2.1.2 Descrição do escopo dos serviços prestados;

3.2.1.3 Nome ou razão social da empresa que prestou o serviço ao emitente;

3.2.1.4 Data de emissão do atestado ou da certidão;

3.2.1.5 Assinatura e identificação do signatário (nome, telefone, cargo e função que exerce junto à empresa emitente).

3.2.2 Considerando as peculiaridades na prestação dos referidos serviços em entidades e órgãos públicos, a empresa a ser contratada precisa comprovar, por meio de atestado de capacidade técnica que já executou os referidos em organizações públicas.

3.3 A Contratada deverá apresentar declaração e/ou certidão comprovando a exclusividade do software.

3.4 A contratada deve contar com equipe técnica de operação com as certificações/qualificações abaixo ou equivalentes:

Perfil	Qualificação/Certificação
No mínimo 01 (um) profissional da área de Tecnologia e Segurança da Informação	● Graduação na Área da Tecnologia da Informação e correlatas ● Certificação Information Security Management Professional based on ISO/IEC 27001
No mínimo 01 (um) profissional da área de Privacidade e Proteção de Dados	● Bacharelado em Direito ● Pós-graduação na área do Direito Digital, Compliance e/ou Privacidade e Proteção de Dados ● Certificação Profissional CDPO/BR emitida e vigente pela International Association of Privacy Professionals (IAPP)
No mínimo 02 (dois) profissionais da área Jurídica	● Bacharelado em Direito ● Pós-graduação na área do Direito Digital, Compliance e/ou Privacidade e Proteção de Dados

3.5 O objeto do contratual não poderá ser subcontratado.

3.6 Não será exigida garantia contratual.

4. LEVANTAMENTO DE MERCADO

4.1 Para atendimento à necessidade de prestação de serviços especializados voltados à implementação de governança de dados, conformidade à Lei Geral de Proteção de Dados (LGPD), segurança da informação e aquisição de solução informatizada de privacidade e gestão de riscos, realizou-se um levantamento de mercado com o objetivo de identificar possíveis alternativas viáveis à Administração Pública.

4.2 Inicialmente, foram consultadas bases públicas como o Portal Nacional de Contratações Públicas (PNCP) e o Compras.gov.br, a fim de verificar contratações similares realizadas por outros entes federativos. No entanto, observou-se que há uma limitação expressiva de fornecedores que atuem de forma integrada nas frentes demandadas (privacidade de dados, segurança da informação, prevenção à perda de dados, gestão de riscos e conformidade à LGPD). Em geral, os serviços são ofertados de forma fragmentada e por empresas distintas, muitas vezes dependentes de subcontratações, o que compromete a padronização, continuidade e a responsabilização técnica sobre o resultado global.

4.3 Em continuidade à pesquisa, identificou-se a empresa NeoGov Sistemas Ltda., inscrita no CNPJ nº 06.291.438/0001-52, como única fornecedora no Brasil capaz de prestar o conjunto de serviços e entregar a solução de forma totalmente integrada, sem subcontratações, abrangendo desde a implementação técnica das ferramentas até a gestão da conformidade legal. A exclusividade de seus serviços foi devidamente reconhecida por meio de Cartas de Exclusividade emitidas por entidades de renome, como a Associação Brasileira de Empresas de Software (ABES) e a Associação Comercial do Estado de Minas Gerais (ACMinas). Além disso, a empresa possui registro da solução informatizada no Instituto Nacional da Propriedade Industrial (INPI), reforçando a originalidade e a titularidade técnica sobre o sistema.

4.4 A notória especialização técnica da NeoGov Sistemas Ltda. também restou evidenciada por seu acervo de atestados de capacidade técnica, inclusive provenientes de órgãos públicos, e pela qualificação de seus recursos humanos, os quais detêm certificações internacionais, produções científicas relevantes e participação ativa em eventos especializados nas áreas de tecnologia, segurança e proteção de dados. Tais elementos demonstram a singularidade e a robustez da empresa em relação ao objeto pretendido, não havendo no mercado fornecedor com condições equivalentes de atender integralmente à demanda da Administração.

4.5 Diante desse cenário, a alternativa mais eficiente, segura e vantajosa para os municípios consorciados é a contratação da NeoGov Sistemas Ltda. por meio de

inexigibilidade de licitação, nos termos do art. 74, incisos I e III, alíneas "c" e "f", combinado com o §6º do art. 82 da Lei nº 14.133/2021. O procedimento é adequado diante do nexo entre todos os itens, que compõem um pacote de prestação dos serviços, alinhados ao uso do software, tornando uma solução que traz a inviabilidade da competição.

4.6 Para possibilitar a contratação futura e eventual pelos entes consorciados conforme a demanda individual de cada um, será adotado o Sistema de Registro de Preços, o qual permite maior agilidade, economicidade e planejamento. O SRP é especialmente adequado ao caso em comento, uma vez que as contratações poderão ocorrer de forma parcelada, de acordo com a necessidade específica de cada consorciado, evitando contratações isoladas e proporcionando uma melhor gestão do gasto público.

5. DESCRIÇÃO DA SOLUÇÃO COMO UM TODO

5.1 A solução que atende a demanda exposta no item 1 deste Estudo é o Registro de Preços para a futura e eventual contratação de empresa especializada para a prestação de serviços de Implementação, Gestão e Governança de Dados para conformidade com a Lei Geral de Proteção de Dados (Lei nº 13.709/2018), Segurança da Informação, serviço de prevenção à perda de dados e fornecimento de solução informatizada de privacidade, gestão de riscos e segurança quanto à Privacidade e Proteção de Dados Pessoais, para atender os municípios consorciados ao CISALP.

5.2 A Ata de Registro de Preços será celebrada com a empresa NeoGov Sistemas Ltda. por meio de inexigibilidade de licitação, nos termos do art. 74, incisos I e III, alíneas "c" e "f" da Lei nº 14.133/2021.

5.3 A futura Ata de Registro de Preços atenderá os órgãos participantes, quais sejam, a Diretoria Administrativa e os municípios que compõe o Consórcio Intermunicipal de Saúde do Alto Paranaíba – CISALP.

5.4 Os serviços, objeto do registro de preço, poderão ser contratados por órgãos não participantes, mediante processo de adesão, que deverá ser autorizada pelo órgão gerenciador da ata.

6. ESTIMATIVA DA QUANTIDADE A SEREM CONTRATADAS

6.1 O quantitativo de cada item/serviço que integrará a Ata de Registro de Preços está detalhado na Tabela do item 3.1 deste Estudo Técnico Preliminar.

6.2 Considerando que os serviços de Inventário e Mapeamento de Dados (ROTDP), Gestão de Riscos de Segurança da Informação, Implantação de Programa de

Conformidade à LGPD cuja unidade de medida é **servidores,** temos que, o processo de mapeamento de dados pessoais no contexto da Administração Pública não pode ser concebido como uma atividade restrita ao corpo administrativo ou apenas aos setores cujas funções são formalmente reconhecidas como técnicas. Trata-se de uma obrigação legal e metodológica que deve envolver todo o corpo funcional da instituição, incluindo servidores efetivos, comissionados, contratados temporários, estagiários e profissionais terceirizados. Essa abrangência decorre do fato de que o tratamento de dados pessoais, nos termos da LGPD, engloba qualquer operação realizada com informações identificadas ou identificáveis, independentemente do grau de escolaridade atuação finalística ou nível hierárquico do agente público envolvido.

Ao longo das entrevistas técnicas especializadas, conduzidas por profissionais qualificados da área jurídica e de segurança da informação, é comum a constatação de uma percepção equivocada: a de que apenas servidores que desempenham atividades administrativas tratam dados pessoais. Entretanto, uma análise fidedigna da realidade operacional demonstra que o fluxo informacional no setor público é amplamente distribuído e permeia praticamente todas as funções desempenhadas, incluindo atividades essencialmente operacionais.

Exemplos concretos ilustram esse cenário. Motoristas de veículos oficiais registram rotas, destinos, horários e identificação de usuários transportados. Agentes de saúde e equipes de combate à dengue lidam com dados sensíveis relacionados ao estado de saúde, endereço e situação sanitária de moradores. Profissionais de limpeza urbana, varredores, equipes de obras, vigilância e zoonoses podem ter contato com cadastros, requisições, formulários impressos e listas de controle contendo dados pessoais tanto de munícipes quanto de outros servidores. Da mesma forma, copeiros, atendentes, auxiliares de setores diversos e colaboradores de empresas terceirizadas muitas vezes acessam, manipulam, armazenam ou transmitem dados pessoais de forma formal ou informal, sem que a organização tenha plena visibilidade desses fluxos.

Esse cenário reforça que o mapeamento de dados pessoais não pode ser restrito a setores administrativos tradicionais, como RH, Protocolo, Tributação, Administração, Controle Interno, Saúde, Educação, Procuradoria ou Assistência Social. O fluxo informacional público é híbrido, multifacetado e dependente da atuação integrada de todos os agentes. Assim, a ausência de participação plena no processo de entrevistas e coleta de

informações resultaria em um diagnóstico incompleto, prejudicando a identificação de riscos, ameaças, vulnerabilidades e pontos críticos de exposição.

Da mesma forma, os programas de gestão de riscos, treinamentos obrigatórios e implementação de medidas técnicas e organizacionais dependem de uma compreensão transversal sobre todas as áreas que, direta ou indiretamente, participam do ciclo de vida da informação. Ao envolver todo o quadro funcional, garante-se não apenas a conformidade jurídica, mas também o fortalecimento da cultura institucional de proteção de dados pessoais, elemento essencial para um programa de privacidade efetivo e sustentável.

Diante desse cenário, conclui-se que os serviços de Inventário e Mapeamento de Dados (ROTDP), Gestão de Riscos de Segurança da Informação, Implantação de Programa de Conformidade à LGPD, bem como a elaboração, revisão e consolidação de políticas, medidas e ferramentas de Privacidade e Proteção de Dados devem ser dimensionados e aplicados de forma ampla, abarcando todos os servidores públicos em suas diversas naturezas de vínculo e atribuições. Qualquer abordagem restrita apenas a setores administrativos comprometeria a precisão do mapeamento, a identificação adequada dos riscos e a efetividade do programa de conformidade, resultando em lacunas jurídicas, operacionais e estratégicas. Portanto, a estimativa e execução desses serviços deve refletir a realidade multifuncional da Administração Pública, assegurando que o fluxo informacional seja avaliado em sua totalidade e que todos os agentes envolvidos no tratamento de dados pessoais sejam devidamente contemplados no processo, conforme os parâmetros legais, técnicos e de governança exigidos pela LGPD.

6.3 Em relação ao item cuja unidade de medida é por **página (A4),** cumpre esclarecer que a quantidade estimada para cada município foi definida com base nos seguintes parâmetros:

Para fins de estimativa de quantidades de páginas a serem objeto de proteção de dados pessoais, estabeleceu-se levantamento de Entidades já contratantes do mesmo objeto da empresa NEOGOV Tecnologia, de modo a criar critério claro e objetivo na relação “páginas por servidor”. Vejamos:

Entidade	N. de Servidores	Quantidade de Páginas	Razão Página/Servidor

Prefeitura Municipal de Monte Carmelo-MG	1267	2.500.000	1.973
Prefeitura Municipal de Machado-MG	1026	2.128.000	2.074
Prefeitura Municipal de Frutal - MG	1930	2.550.000	1.321
Média de Páginas			1.790 páginas/servidor

Portanto, considerando os contratos administrativos já firmados com mesmo objeto, estima-se que que o acervo de documentos a serem objeto de proteção, correspondentes a páginas A4 de valor estritamente administrativo, é de 1.790 páginas por servidor.

Todavia, considerando a capacidade técnica de transformação digital e da existência de entes com quantitativo superior a **4 mil servidores**, fixa-se, para fins de dimensionamento dentro do limite temporal do contrato (12 meses), o limite máximo de **3.500.000 páginas por ano**, garantindo adequada margem operacional para atendimento da demanda.

7. ESTIMATIVA DO VALOR DA CONTRATAÇÃO

7.1 O VALOR TOTAL estimado do Registro de Preços é **R$ 26.563.320,40 (vinte e seis milhões, quinhentos e sessenta e três mil, trezentos e vinte reais e quarenta centavos).**

7.2 O valor unitário a ser registrado, referente a cada serviço/item, está previsto na Tabela constante do item 3.1 deste Estudo Técnico Preliminar.

7.3 Consideram-se integrados ao valor total do item todos os encargos tributários e trabalhistas, despesas (para serviços de terceiros) e demais agregadas a prestação dos serviços.

8. JUSTIFICATIVA PARA O PARCELAMENTO OU NÃO DA SOLUÇÃO

8.1 Considerando que todos os serviços registrados possuem natureza singular e somente podem ser prestados por uma única empresa**,** não houve o registro de itens em

nome de fornecedores distintos**.** Assim, não se justifica o parcelamento do objeto entre diferentes empresas**,** tendo em vista a notória especialização da empresa NeoGov Sistemas Ltda**.** na execução de todos os serviços, bem como o fato de que o registro de preços será precedido de procedimento de inexigibilidade de licitação, conforme disposto no artigo 74 da Lei nº 14.133/2021.

8.2 Embora os municípios consorciados possam, conforme suas necessidades, contratar os serviços de forma individualizada**,** a centralização da prestação em um único fornecedor contribui significativamente para a padronização, eficiência operacional e responsabilização técnica unificada, assegurando maior controle, qualidade e economicidade à Administração Pública.

9. CONTRATAÇÕES CORRELATAS E/OU INTERDEPENDENTES

9.1 Não se verifica contratações correlatas nem interdependes para a viabilidade desta contratação.

9.2 ANÁLISE DE RISCOS

9.2.1 A tabela a seguir apresenta uma síntese dos possíveis riscos da contratação:

<table>
<tr><td colspan="2">Risco 1: Contratante cometer infração administrativa (não assinar a ata de registro de preços quando convocado dentro do prazo de validade da proposta ou não assinar o termo de contrato decorrente da ata de registro de preços; apresentar documentação falso e deixar de entregar os documentos exigidos para a contratação; ensejar o retardamento da execução do objeto; não mantiver a proposta; cometer fraude fiscal; comportar-se de modo inidôneo).</td></tr>
<tr><td colspan="2">Probabilidade: Médio</td></tr>
<tr><td colspan="2">Impacto: Médio</td></tr>
<tr><td colspan="2">Dano: Retardamento da contratação.</td></tr>
<tr><td>Ação Preventiva</td><td>Responsável</td></tr>
<tr><td>Dar ciência a futura contratada que os atos de infração administrativa serão sujeitos às sanções administrativas previstas em lei.</td><td>Setor de Licitação / Agente de Contratação</td></tr>
<tr><td>Ação de Contingência</td><td>Responsável</td></tr>
<tr><td>Instaurar processo de sanção administrativa, observada a fase da contratação.</td><td>Setor de Licitação ou Gestor da Ata de Registro de Preços.</td></tr>
<tr><td>Iniciar imediatamente um novo Estudo para verificar a alternativa viável para solucionar a demanda dos entes consorciados.</td><td>Secretaria Executiva</td></tr>
<tr><td colspan="2">Risco 2: O fornecedor prestar os serviços em discordância com as especificações constantes no Termo de Referência.</td></tr>
<tr><td colspan="2">Probabilidade: Média</td></tr>
<tr><td colspan="2">Impacto: Alto</td></tr>
<tr><td colspan="2">Dano: Cancelamento do registro de preço</td></tr>
</table>

Ação Preventiva	Responsável
Dar ciência ao fornecedor das penalidades decorrentes do descumprimento do pactuado na ata de registro de ou do descumprimento das obrigações contratuais, em relação as suas próprias contratações.	Gestor da Ata de Registro de Preços
Ação de Contingência	**Responsável**
Cancelamento do(s) registro(s), formalizado por despacho do órgão gerenciador, assegurado o contraditório e a ampla defesa	Gestor da Ata de Registro de Preços
Iniciar imediatamente um novo Estudo para verificar a alternativa viável para solucionar a demanda dos entes consorciados.	Secretaria Executiva
Risco 3: ***Fornecedor não executar os serviços no prazo previsto na Ordem de Serviço.***	
Probabilidade: Média	
Impacto: Alta	
Dano: Cancelamento do registro do fornecedor	
Ação Preventiva	**Responsável**
Dar ciência ao fornecedor da possibilidade de cancelamento do(s) registro(s) no caso de não prestar os serviços dentro do prazo previsto na Ata de Registro de Preços, no Contrato ou na Ordem de serviço, sem justificativa aceitável.	Gestor da Ata de Registro de Preço
Ação de Contingência	**Responsável**
Instauração de processo de sanção administrativa e cancelamento do(s) registro(s), formalizado por despacho do órgão gerenciador, assegurado o contraditório e a ampla defesa.	Gestor da Ata de Registro de Preços
Realizar imediatamente novo estudo para identificar a melhor alternativa para disponibilizar os serviços aos municípios consorciados.	Secretaria Executiva
Risco 5: Fornecedor não aceitar reduzir o seu preço registrado, na hipótese deste se tornar superior aqueles praticados no mercado	
Probabilidade: Média	
Impacto: Alto	
Dano: Cancelamento do registro do fornecedor	
Ação Preventiva	**Responsável**

Dar ciência ao fornecedor da possibilidade de cancelamento do(s) registro(s) no caso de não aceitar reduzir o seu preço registrado, na hipótese deste se tornar superior àqueles praticados no mercado.	Gestor da Ata de Registro de Preços

Ação de Contingência	Responsável
Cancelamento do(s) registro(s), formalizado por despacho do órgão gerenciador	Gestor da Ata de Registro de Preços
Iniciar imediatamente um novo Estudo para verificar a alternativa viável para solucionar a demanda dos entes consorciados.	Secretaria Executiva

10. RESULTADOS PRETENDIDOS:

10.1 A contratação visa proporcionar aos municípios consorciados a efetiva adequação à Lei Geral de Proteção de Dados (LGPD), por meio da implementação de soluções integradas de governança de dados, segurança da informação, prevenção à perda de dados e gestão de riscos. Com isso, busca-se fortalecer a proteção dos dados pessoais sob responsabilidade da Administração Pública, garantir conformidade com a legislação vigente, mitigar riscos de incidentes cibernéticos e promover uma gestão mais segura, eficiente e transparente. Ademais, pretende-se assegurar padronização, continuidade técnica e suporte especializado para o pleno atendimento das demandas dos entes consorciados.

11. PROVIDÊNCIAS A SEREM ADOTADAS

11.1 Não existem providências a serem tomadas para viabilizar a pretendida contratação.

12. POSSÍVEIS IMPACTOS AMBIENTAIS

12.1 Dada a natureza do objeto a ser contratado, não se identificam impactos ambientais significativos decorrentes da sua execução.

13. DECLARAÇÃO DE VIABILIDADE

13.1 Com base nos elementos anteriores do presente Estudo Técnico Preliminar, declara-se que é viável técnica, operacional e financeiramente proceder com o Registro de Preço e, posteriormente, com as contratações, nos termos definidos e dispostos no presente documento.

Lagoa Formosa, 11 de dezembro de 2025.

Aline Souto da Costa

DIRETORA DE RECURSOS HUMANOS DO CISALP

Setor Requisitante