

**TERMO DE REFERÊNCIA PARA CONTRATAÇÃO DE SERVIÇOS**

A Prefeitura Municipal de Ituiutaba-MG vem, por intermédio deste, apresentar demanda para contratação de empresa especializada para prestação de serviços de implementação, gestão e governança de dados (Lei nº13.709/2018), segurança da informação e aquisição de solução informatizada de privacidade, gestão de riscos e segurança quanto à privacidade e proteção de dados pessoais.

Objeto:

CONTRATAÇÃO DE EMPRESA ESPECIALIZADA PARA A PRESTAÇÃO DE SERVIÇOS DE IMPLEMENTAÇÃO, GESTÃO E GOVERNANÇA DE DADOS (LEI Nº13.709/2018), SEGURANÇA DA INFORMAÇÃO E AQUISIÇÃO DE SOLUÇÃO INFORMATIZADA DE PRIVACIDADE, GESTÃO DE RISCOS E SEGURANÇA QUANTO À PRIVACIDADE E PROTEÇÃO DE DADOS PESSOAIS.

1) Justificativa da Contratação

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.

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.

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 contra ataques cibernéticos.

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).

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.

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

AM

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).

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.

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.

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.

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.

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.

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.

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.

Resta evidente que se trata de um objeto de contratação frequente e que deve ser realizada pela entidade. Diante exposto, a Prefeitura Municipal de Ituiutaba-MG, através do objeto solicitado, busca adequar a Administração Pública Municipal à legislação de proteção de dados vigente e implementar medidas de segurança da informação necessárias à blindagem contra crimes cibernéticos e vazamentos de dados.

2) ESPECIFICAÇÃO DOS BENS/SERVIÇOS

At



Item	Descrição	Und	Quantidade Estimada	Valor Unitário Previsto	Valor Total
01	Solução Informatizada de Privacidade, Gestão de Riscos e Segurança da Informação	Licença de uso mensal	12	R\$ 10.550,00	R\$ 126.600,00
02	Suporte Técnico Continuado	Meses	12	R\$ 2.890,00	R\$ 34.680,00
02	Inventário e Mapeamento de Dados (ROPA), Gestão de Riscos de Segurança da Informação, Implantação de Programa de Conformidade à LGPD, medidas e ferramentas de Privacidade e Proteção de Dados	Meses	12	R\$ 89.955,00	R\$ 1.079.460,00
VALOR TOTAL					R\$ 1.240.740,00
* Licença de uso mensal (item 01) possui valor fixo, independentemente do porte da Entidade. ** Suporte Técnico + Implementação (itens 2 e 3) tem como dimensionamento o número de servidores (1984 servidores), resultando no custo de R\$ 561,56 por servidor. *** relação de quantitativo de servidores em anexo.					

A solução como um todo compreende 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 e aquisição de solução informatizada de privacidade, gestão de riscos e segurança quanto à Privacidade e Proteção de Dados Pessoais.

Os serviços e produtos mencionados têm como objetivo o atendimento da obrigação legal de conformidade de Entidades Públicas à Lei n. 13.709/2018 (Lei Geral de Proteção de Dados), bem como a proteção dos direitos fundamentais dos cidadãos à privacidade e à proteção de dados. Para isso, a solução integrada de serviços e ferramentas multidisciplinares se demonstram como a opção mais vantajosa para a Administração Pública, reunindo em uma só contratação serviços e produtos que, se contratados de forma isolada, poderiam gerar um custo significativamente maior e sem a devida integração de processos, o que causaria empecilhos à devida adequação. As soluções a serem contratadas englobam o escopo de tecnologia, jurídico, segurança da informação e de gestão de projetos, o que percorre em consonância às regras de conformidade previstas em legislações nacionais, internacionais e normas técnicas como as ISOs 27001, 27002, 27005, 27018, 27701, 29100 e 29134, além de diretrizes NIS e NIST.

2.1) ESPECIFICAÇÕES DA CONTRATAÇÃO

O serviço de Gestão da Segurança da Informação para a devida adequação à Lei Geral de Proteção de Dados deverá compreender:

- 2.1.1 Visitas técnicas presenciais com a análise do ambiente físico e mapeamento da infraestrutura tecnológica da CONTRATANTE, com o fim de se verificar eventuais vulnerabilidades e riscos de Segurança da Informação;
- 2.1.2. Realização de testes de vulnerabilidades no ambiente tecnológico, com a avaliação dos controles de segurança da informação voltados à confidencialidade, integridade e disponibilidade de dados (Firewall, Web Filter, Antivírus, VPN, Backup, redundância, etc.);
- 2.1.3. Levantamento de todo o ativo utilizado pela CONTRATANTE, tais como os recursos de hardware utilizados, softwares, licenças e documentações;
- 2.1.4. Análise pessoal com os integrantes-chaves da CONTRATANTE, para identificação dos riscos de informação que possam comprometer a segurança física e computacional da CONTRATANTE;
- 2.1.5. Definição do Nível de Maturidade da CONTRATANTE quanto à adequação aos requisitos de Segurança da Informação previstos em normas técnicas de padrões internacionais como ISO/IEC 27001, 27002, 27005, diretrizes NIST e NIS;

AL



2.1.6. Definição e apoio à implantação dos processos, sistemas e soluções necessárias para a adequação à Lei Geral de Proteção de Dados e à Segurança da Informação, através de definições de matrizes de riscos e planos de recomendações a fim de mitigação e tratamento dos riscos existentes;

2.1.7. Implementação de controles e medidas técnicas de Segurança da Informação e posterior monitoramento e auditoria para manutenção da conformidade com os padrões internacionais acima mencionados;

2.1.8. Treinamento na modalidade presencial ou remota, de acordo com as necessidades da CONTRATANTE, para o estabelecimento de cultura organizacional voltada às boas práticas de Segurança da Informação, bem como quanto à utilização e parametrização da solução informatizada de forma integrada ao processo de adequação, proporcionando a atualização e tratamento contínuo dos riscos de segurança da informação.

O serviço de Programa de Conformidade para adequação à Lei Geral de Proteção de Dados deverá compreender:

2.1.9. Definição e implementação do Ciclo Operacional de Proteção de Dados através dos cinco pilares de Gestão de Privacidade: Avaliação, Proteção, Manutenção e Resposta;

2.1.10. Assessoria e Consultoria na designação/nomeação do Encarregado de Dados (Data Protection Officer-DPO), bem como sua capacitação para cumprimento de suas atribuições legais, através de treinamentos presenciais ou remotos, a depender da necessidade da Entidade;

2.1.11. Diagnóstico Jurídico para definição das normas legais e infralegais aplicáveis aos processos de tratamentos de dados da Entidade Pública CONTRATANTE, bem como avaliação do grau de maturidade quanto à conformidade do Ente à Lei Geral de Proteção de Dados;

2.1.12. Entrevistas técnicas especializadas, presencialmente na Entidade CONTRATANTE, com os servidores-chaves de cada Secretaria/Departamento, a fim de se levantar o inventário de dados e o fluxo (mapeamento) informacional, bem como os riscos operacionais existentes nos processos de tratamento, para posterior gestão dos riscos de dados e recomendações para a devida adequação e conformidade;

2.1.13. Assessoria e Consultoria para elaboração de atos normativos necessários à implementação do Programa de Conformidade, incluindo redação de minutas de decretos, resoluções, portarias, quando necessária à regulamentação da Lei Geral de Proteção de Dados no âmbito da Entidade CONTRATANTE;

2.1.14. Revisão de processos de tratamentos de dados para implantação da Privacidade desde a Concepção (Privacy by Design) e por Padrão (Privacy by Default), a fim de adequar processos administrativos, essencialmente no campo de Compras Públicas, através de criação de cláusulas, aditivos contratuais, contratos, revisão de documentos e processos de contratação;

2.1.15. Elaboração e Revisão de Políticas de Privacidade, Aviso de Privacidade, Política de Cookies, Plano de Resposta a Incidentes de Privacidade e Política de Segurança da Informação;

2.1.16. Assessoria e Consultoria para elaboração do Relatório de Impacto à Proteção de Dados (RIPD), com apoio da solução informatizada contratada, com o objetivo de celeridade no processo de resposta quando requisitado;

2.1.17. Assessoria e Consultoria Jurídica Especializada em Privacidade e Proteção de Dados para eventuais necessidades de elaboração de respostas ou prestação de informação da Entidade CONTRATANTE às Entidades Fiscalizadoras (ANPD, MP, TCEs, TCMs);

2.1.18. Criação de boas-práticas de compliance para mitigação dos riscos no processo de atendimento aos direitos dos titulares de dados pessoais, com o fim de prevenir eventual responsabilização civil, administrativa ou criminal;

2.1.19. Treinamento do Encarregado de Dados com a definição e boas-práticas para a confecção do Relatório de Impacto à Proteção de Dados e relação com a Autoridade Nacional de Proteção de Dados – ANPD;

2.1.20. Treinamento dos servidores que operam dados pessoais, com o objetivo de criação e cultivo da cultura de privacidade na Entidade Pública, através de palestras, workshops e/ou cursos com a devida certificação pela participação e capacitação.

A solução informatizada deverá abranger:

2.1.21. Um conjunto de ferramentas integradas, que serão implantadas para assegurar mecanismos de inventário e mapeamento de dados, análise e gestão de riscos de adequação à Lei Geral de Proteção de Dados, identificação de vulnerabilidades e riscos no tratamento de dados pessoais e segurança da informação, estabelecimento de recomendações e planos de ação para a efetiva adequação, gestão de acesso do titular de dados aos seus registros e informações, geração de relatórios de adequação, gestão de consentimento para coleta de dados pessoais via política de cookies nas plataformas digitais:

Solução Informatizada de Privacidade, Proteção de Dados e Segurança da Informação	Item	Especificação
	1	Módulo de Mapeamento de Dados
	2	Módulo de Gestão de Riscos
	3	Módulo de Gestão de Dados
	4	Módulo de Gestão de Cookies
	5	Módulo de Treinamento
	6	Treinamento sobre a Solução Informatizada
	7	Suporte Técnico e acompanhamento da Administração Pública, através de responsável(is) técnico(s)

2.1.22. O licenciamento proposto é na modalidade Software as a Service (SaaS), o mais abrangente para esse tipo de solução, com vigência de 12 (doze) meses, contemplando, ainda, o serviço de implantação, suporte técnico fornecido pela empresa Contratada e fabricante pelo período de contratação, e o treinamento sobre as ferramentas implantadas.

2.1.23. A solução informatizada deverá ser fornecida e mantida exclusivamente pela empresa Contratada, sendo vedado o fornecimento da solução através de parceria ou representação comercial de terceiros, visto que tal fato traria diversos empecilhos e desvantagens à Administração Pública como ausência de identidade de fornecedores, inexistência de sincronismo na prestação do serviço e produto, além de aumento do risco de inexecução do objeto. Além disso, sua propriedade deve ser registrada no Instituto Nacional de Propriedade Industrial (INPI) sob o nome da empresa contratada, com o objetivo de se evitar conflitos futuros de registro de software.

2.1.24. O fornecedor deverá garantir padrões de segurança e privacidade, além de possuir banco de dados localizado no Brasil, sendo vedado o armazenamento de dados das soluções em país estrangeiro. A implementação deverá ser obrigatoriamente executada pela contratada.

2.1.25. A solução deve ter a capacidade de carregar/alterar usuários, bem como seus tipos de privilégios de uso, além de possibilitar a atualização de referenciais normativos como medida de parametrização do sistema (atualização de normas aplicáveis).

2.1.26. O suporte técnico quanto à solução informatizada deverá ser oferecido exclusivamente pela empresa contratada.

2.1.27. As soluções informatizadas utilizadas no processo de implementação e adequação à Lei Geral de Proteção de Dados deverão ser fornecidas em conjunto, exclusivamente pela empresa Contratada.

3) DEFINIÇÃO E ESPECIFICAÇÃO DAS NECESSIDADES DE NEGÓCIOS E TECNOLÓGICAS:

3.1. A solução informatizada deverá ser fornecida e mantida exclusivamente pela CONTRATADA, sendo vedado o fornecimento da solução através de parceria ou representação comercial de terceiros;

3.2. A solução deverá ser disponibilizada na modalidade de software como serviço (SaaS);





- 3.3. O fornecedor deve garantir os mais altos padrões de segurança e privacidade, além de possuir banco de dados localizado no Brasil, sendo vedado o armazenamento de dados em país estrangeiro;
- 3.4. A implementação deverá ser obrigatoriamente executada pelo fabricante da solução ofertada;
- 3.5. A solução deve ter a capacidade de carregar/alterar usuários, bem como seus tipos de funções;
- 3.6. A solução deve permitir parametrizações quanto às normas de conformidade, possibilitando alteração e atualização de referenciais normativos que subsidiarão os controles de requisitos e matrizes de gestão de riscos operacionais e de informação;
- 3.7. A solução deve permitir o gerenciamento de privilégios de usuários;
- 3.8. O suporte técnico quanto à solução informatizada deverá ser oferecido exclusivamente pela CONTRATADA;
- 3.9. As soluções informatizadas utilizadas no processo de implementação e adequação à Lei Geral de Proteção de Dados, deverão ser fornecidas em conjunto, exclusivamente pela CONTRATADA;
- 3.10. A solução informatizada deverá ser licenciada pelo período de 12 (doze) meses, podendo ser prorrogado por interesse da CONTRATANTE, nos termos legais.

4) ESPECIFICAÇÕES MÍNIMAS DA SOLUÇÕES E DOS SERVIÇOS

4.1. A solução informatizada para Privacidade, Gestão de Riscos e Segurança na Proteção de Dados deverá atender às seguintes especificações:

4.1.1. Módulo de Mapeamento de Dados (Data Mapping):

- A solução deve contemplar o registro (inventário) das operações de tratamento de dados, dos recursos utilizados nas operações de tratamento, dos fornecedores envolvidos nas operações de tratamento e de entidades envolvidas nas operações de tratamento (operadores);
- A solução deve permitir a criação de diferentes tipos de titulares de dados (servidores, cidadãos atendidos pela entidade, terceirizados, estagiários etc.);
- A solução deve permitir a criação de elementos de dados que podem ser vinculados a cada tipo de titular de dados;
- A solução deve gerar relatórios de acordo com os requisitos do artigo 38 da LGPD;
- A solução deve permitir a criação de relatórios personalizados;
- A solução deve permitir a reavaliação dos itens do inventário;
- A solução deve permitir o mapeamento de todos os recursos que compõem o ativo da contratante, demonstrando a participação de operadores de dados, a infraestrutura de rede, fluxo das informações, gestão de acesso e infraestrutura física;
- A solução deve permitir a vinculação de titulares, ativos, fornecedores, entidades, elementos de dados a cada operação de tratamento.

4.1.2. Módulo de Análise e Gestão de Riscos:

- A solução deve permitir a análise e registro de riscos e vulnerabilidades aos quais a instituição se encontra exposta;
- A solução deve permitir a parametrização de normas técnicas que baseiam a Gestão de Riscos de Operacionais e de Informação;
- A solução deve permitir a gestão de riscos operacionais (privacidade) e de segurança da informação com base em controles de requisitos previstos nas normas referenciais, mediante tratamento em matrizes de riscos que demonstrem as implicações sobre os requisitos de Confidencialidade, Integridade e Disponibilidade, bem como quanto aos impactos em áreas de atuação da entidade;

Handwritten signature



- A solução deve permitir o estabelecimento de planos de ação (recomendações), com a criação de tarefas de adequação à LGPD e à Segurança da Informação, com tarefas a serem cumpridas pela entidade;
- A solução deve permitir a análise dos riscos a luz de normas internacionais de Segurança da Informação e Privacidade, tais como ISOs 27001, 27002, 27005, 27701, NIS, NIS'I, LGPD, demonstrando matrizes de riscos e representação visual de conformidade;
- O processo de maturação e adequação à LGPD deve ser fornecido de forma visual e gráfica, a fim de possibilitar maior facilidade de utilização pelo Encarregado de Dados, permitindo a melhor gestão;
- A solução deve permitir o acompanhamento e atualização constante do processo de adequação, bem como o estabelecimento do nível de maturidade da instituição quanto à conformidade com a LGPD;
- A solução deve permitir o gerenciamento de incidentes e possíveis violações, permitindo o registro de relato de incidente e a geração de relatório automatizado para a comunicação à Autoridade Nacional de Proteção de Dados e titulares dos dados;
- A solução deve permitir a destinação de tarefas a envolvidos específicos ou grupo de pessoas responsáveis pelo seu cumprimento.

4.1.3. Módulo de Gestão de Dados:

- A solução deve permitir a devida interação entre o titular de dados e a instituição controladora, através do Encarregado de Dados;
- A solução deve permitir que a gestão de requisições de titulares quanto aos dados pessoais objetos de tratamento, sendo-lhe assegurado a confirmação de existência do dado, o acesso, a correção, a anonimização, bloqueio ou eliminação de dados desnecessários, excessivos ou tratados em desconformidade com a LGPD, informação quanto ao compartilhamento dos seus dados, além da gestão de consentimento nos casos legais necessários;
- A solução deve permitir o processamento dos requerimentos dos Titulares de Dados em formato de processo a ser analisado e tratado pelo Encarregado de Dados;
- A solução deve permitir o registro e processamento de requisições de Autoridades Fiscalizadoras (ANPD, MP, TCE) para acompanhamento e resposta no prazo estipulado, com apoio de relatórios gerados de forma automatizada durante as fases de adequação.

4.1.4. Módulo de Políticas de Cookies:

- A solução deve permitir a devida interação entre o titular de dados e os mais variados sistemas de informação da entidade CONTRATANTE, especialmente em plataformas digitais, conferindo transparência e requerendo consentimento no tratamento de dados pessoais coletados via cookies durante a navegação e utilização;
- A solução deve permitir que o titular de dados tenha conhecimento de quais os dados são coletados durante a navegação, os fins para os quais serão utilizados, além de apresentação de políticas pertinentes a este tratamento;
- A solução deve permitir a gestão do consentimento relacionado à utilização de cookies, possibilitando a evidenciação das opções realizadas pelos titulares.

4.1.5. Módulo de Treinamento:

- A solução deverá possuir um ambiente de disponibilização de vídeos avulsos e trilhas de ensino para treinamento e atualização de colaboradores da CONTRATANTE sobre a Lei Geral de Proteção de Dados, além de noções e boas práticas de Segurança da Informação e Compliance;
- Os vídeos e trilhas de ensino deverão ser fornecidos pela CONTRATADA através de produção própria;
- As trilhas de ensino deverão ser compostas por um conjunto pedagogicamente orientado de videoaulas (ementa lógica), com controle de fluxo de visualização pelo participante, seguido de avaliação e emissão de certificado de conclusão de curso;

- O módulo deverá disponibilizar a documentação, incluindo orientações, manuais, códigos, políticas, entre outros documentos confeccionados pela Assessoria Jurídica e Operacional durante o processo de implementação e adequação da entidade CONTRATANTE à LGPD;

4.1.6. Treinamento sobre a Solução informatizada e Conscientização do Programa de Conformidade:

- Deverá ser fornecido o treinamento presencial ou remoto, com carga horária mínima de 20 (vinte) horas, sendo ministrado todo o conteúdo requerido para a devida compreensão e operação das soluções informatizadas implantadas;
- O treinamento contemplará até duas turmas, de até 10 (dez) pessoas cada, devendo ser compostas pelos agentes responsáveis pela operação da solução informatizada;
- A gravação dos treinamentos, em sua íntegra, será disponibilizada em formato de vídeo padrão de mercado;
- A empresa CONTRATADA deverá fornecer o material didático utilizado no treinamento, em formato digital;
- Deverá ser fornecido Certificado de Conclusão aos participantes do treinamento, comprovando sua efetiva habilitação para operar a solução implantada;
- As datas do treinamento deverão ser acordadas com a entidade Contratante, respeitando o processo de implementação da solução pela empresa Contratada.

4.1.7. Serviço de Suporte Técnico e acompanhamento continuado:

- O serviço de suporte técnico deverá ser executado pela equipe técnica especializada da CONTRATADA, de forma presencial e remota, visando a garantia de um crescimento gradual da maturidade dos agentes operadores da solução informatizada, bem como a implementação de melhores práticas, fluxos de trabalho, novas funcionalidades disponibilizadas pela CONTRATADA e demais necessidades de apoio técnico;
- A Contratada deverá oferecer todo o suporte necessário para a operacionalização das tecnologias ofertadas, minimizando o risco na implantação e proporcionando condições ideais para a transferência da tecnologia envolvida, até que a equipe da CONTRATANTE possa ter conhecimento e vivência na operacionalização de toda a solução;
- Serão devidas as horas de serviço de suporte técnico independentemente da utilização pela CONTRATANTE, visto que a equipe da CONTRATADA estará disponibilizada para tal atividade;

4.2. SERVIÇO DE IMPLEMENTAÇÃO, GESTÃO E GOVERNANÇA DE DADOS PARA CONFORMIDADE COM A LEI GERAL DE PROTEÇÃO DE DADOS (LEI Nº 13.709/2018):

4.2.1. O serviço de Implementação, Gestão e Governança de Dados deverá ser composto por duas fases, as quais deverão compor o ciclo operacional de proteção de dados (avaliar, proteger, manter e responder):

a) Fase de Diagnóstico; e b) Fase de Programa de Conformidade;

4.2.1.1. Na Fase de Diagnóstico:

O Deverá ser realizado pela CONTRATADA, através de visitas técnicas presenciais, o levantamento geral da cultura organizacional da CONTRATANTE quanto às políticas de proteção de dados, privacidade e de segurança da informação correntes, bem como realizado o inventário e fluxo de todo o ciclo de vida dos dados pessoais sujeitos a tratamento através de entrevistas pessoais e presenciais com os operadores de dados chaves da Entidade;

O A empresa CONTRATADA deve levantar os papéis e responsabilidades de cada um dos operadores de dados pessoais integrantes da CONTRATANTE, seja servidor, contratado ou terceirizado, identificando as lacunas e vulnerabilidades, através de trabalho de campo no ambiente físico da CONTRATANTE, em conformidade com sua estrutura orgânica;

O A empresa CONTRATADA deverá realizar testes de Segurança da Informação com o objetivo de identificar vulnerabilidades na estrutura tecnológica e ambiental da CONTRATANTE, apontando todos os riscos de segurança da informação detectados;

O A empresa CONTRATADA deve realizar o levantamento de todos os ativos da CONTRATANTE, especialmente quanto aos recursos de hardware e software utilizados, as medidas, aplicações e métodos de Segurança da Informação adotados, identificando possíveis vulnerabilidades;

O A empresa CONTRATADA deve realizar o levantamento e revisão da documentação jurídica relacionada a Privacidade e Proteção de Dados, especialmente quanto à base legal de tratamento, políticas de privacidade, confidencialidade, termos de uso, informes, cartilhas, dentre outros aplicáveis;

O A empresa CONTRATADA deverá realizar a avaliação e levantamento acerca das legislações e normativas aplicáveis às atividades da Entidade, bem como analisar a necessidade de regulamentação por intermédio de diplomas legais a serem publicados em âmbito municipal (decretos, portarias, resoluções etc.);

O Caso haja a necessidade de confecção de diplomas normativos, a empresa CONTRATADA deverá prestar assessoria jurídica na elaboração das minutas correspondentes (decretos, portarias, resoluções etc.), empenhando seus conhecimentos técnicos com a devida adequação à estrutura organizacional da Entidade;

O A empresa CONTRATADA deverá realizar a análise dos atos documentais praticados, especialmente na área de Compras Públicas, com o objetivo de adequar os procedimentos de contratação de fornecedores às práticas de Privacy by Design (Privacidade desde a Concepção) e Privacy by Default (Privacidade como Padrão), através de cláusulas, aditivos, termos e contratos;

O Todos os riscos operacionais (privacidade e proteção de dados) e de informação (segurança da informação) deverão ser registrados e tratados na solução informatizada, com a devida gestão de riscos através de matrizes e em consonância com normas técnicas de padronização internacional, apontando para a próxima fase as recomendações e planos de adequação;

O A empresa CONTRATADA deverá apresentar relatório durante a fase de diagnóstico, com o objetivo de avaliar o escopo da adequação como entregável à Entidade;

O A empresa CONTRATADA deve realizar entrevista e análise do nível de conhecimento e maturidade de gestão e processos do Encarregado de Dados (Data Protection Officer) designado pela CONTRATANTE.

4.2.1.2. Na Fase de Diagnóstico:

O A empresa CONTRATADA deverá implementar um Plano de Ação com o objetivo de conscientizar todos os integrantes da CONTRATANTE que tenham alguma responsabilidade no processo de tratamento de dados pessoais, através de orientações escritas e/ou expositivas;

O A empresa CONTRATADA deverá prestar toda a assessoria jurídica e de segurança da informação necessária para acompanhar a Entidade na implementação do Programa de Conformidade em consonância com os planos de ações delimitados a partir da gestão de riscos realizada na fase anterior;

O A empresa CONTRATADA deverá realizar workshops/treinamentos de conscientização dos colaboradores/servidores da Entidade Pública, com o objetivo de fomentar a Cultura de Privacidade, de modo a disponibilizar, no mínimo, um workshop para todos os servidores durante o período de vigência contratual, de forma presencial ou remota;

O A empresa CONTRATADA deverá propor as melhorias e adequações quanto à documentação jurídica relacionada a termos de uso, políticas e avisos de privacidade, cookies, confidencialidade, bem como estabelecimento de cláusulas contratuais ou normas de condutas para assegurar o cumprimento dos requisitos dispostos na Lei Geral de Proteção de Dados;

O A empresa CONTRATADA deverá prestar toda consultoria e assessoria jurídica necessária à Entidade para responder e/ou prestar informações a órgãos fiscalizadores quanto ao campo da Privacidade e Proteção de Dados;

O A empresa CONTRATADA deverá orientar e estabelecer procedimentos em Plano de Comunicação de Incidente de Segurança, capacitando o Encarregado de Dados e demais envolvidos no processo de comunicação à Autoridade Nacional e aos titulares de dados pessoais;

O A empresa CONTRATADA poderá propor a revisão ou criação, caso não exista, de uma Cartilha de Privacidade e Segurança e Informes de Segurança da Informação;

O A empresa CONTRATADA deverá realizar treinamento do Encarregado de Dados (DPO), de forma presencial e remota (trilha de conhecimento do módulo de treinamento da solução informatizada), com o objetivo de capacitá-lo a cumprir todas as atribuições que lhe são legalmente conferidas;

AK



O A empresa CONTRATADA deverá aplicar métricas para monitoramento e auditoria no grau de maturidade de conformidade à Lei Geral de Proteção de Dados, com o objetivo de conferir perenidade e atualização no processo de adequação.

4.3. Licenciamento, Garantia e Suporte Técnico:

- Todas as licenças deverão ser emitidas pela fabricante da solução, ora CONTRATADA, com as respectivas atualizações de versão e garantia, durante a vigência do contrato;
- Todos os produtos deverão ser fornecidos em sua versão/release mais recente;
- Caso, durante o período de execução dos serviços, haja mudanças de nomenclatura e/ou reajustes na composição dos produtos ofertados, a CONTRATADA deve garantir o uso dessas novas funcionalidades no serviço prestado à CONTRATANTE;
- A CONTRATADA deve manter a solução disponibilizada à CONTRATANTE sempre na sua versão mais atualizada, não sendo admitido um prazo superior a 05 (cinco) dias úteis após o lançamento oficial da versão pelo fabricante;
- Chamados de suporte técnico e de abertura de serviços serão abertos exclusivamente por meio do sistema de abertura e gerenciamento de chamados provido e mantido pela CONTRATADA. Cada chamado deverá conter, no mínimo, as seguintes informações:
 - número de identificação exclusivo;
 - data e hora do início da ocorrência;
 - descrição da ocorrência;
 - nível de severidade;
 - providências adotadas para o diagnóstico;
 - indicação de solução provisória e/ou solução definitiva;
 - data e hora do término da ocorrência, com solução definitiva;
 - identificação do agente da CONTRATANTE que solicitou e validou o chamado técnico;
 - identificação do técnico da CONTRATADA responsável pela execução do chamado técnico, bem como outras informações pertinentes.
- Deverá existir canal de atendimento para realização e acompanhamento de chamados técnicos, com acesso permanente para os técnicos da CONTRATADA, contemplando no mínimo, sítio eletrônico/e-mail e telefone;
- O sistema de abertura de chamados deverá estar disponível 24 x 7 x 365 (vinte e quatro horas por dia, sete dias por semana, trezentos e sessenta e cinco dias por ano), inclusive feriados. No entanto, a análise e resposta aos chamados serão realizados apenas em dias úteis, no mesmo período de funcionamento da CONTRATANTE.
- O suporte técnico deverá estar disponível para todos os produtos e incluem:
 - solução de problemas relativos à indisponibilidade da solução;
 - esclarecimentos de dúvidas sobre o funcionamento e operação da solução.

4.4. Implantação da Solução:

- Antes do início do projeto, a contratada se reunirá com a equipe de Tecnologia da Informação da CONTRATADA para apresentar os aspectos de concepção do projeto, políticas e configurações.
- Até o 15º (décimo quinto) dia útil após a assinatura do contrato, deverá ser realizada reunião presencial ou remota com a equipe ou representante do Setor de Tecnologia da Informação da CONTRATANTE, com o objetivo de a CONTRATADA apresentar sua metodologia de trabalho, planejamento e coordenação das atividades de entrega da solução.

AL

4.5. Transferência de conhecimento:

A configuração será efetuada de forma a não afetar o funcionamento dos sistemas, recursos ou equipamentos em operação e nem interromper, por períodos prolongados, a rotina de trabalho dos servidores e colaboradores da CONTRATANTE;

Todos os componentes de software requeridos para atender as funcionalidades e tornar a solução operante, mesmo que não tenham sido especificados ou cotados na proposta apresentada, serão considerados partes integrantes da solução e devem ser fornecidos.

5. DA CONTRATAÇÃO INTEGRADA DA SOLUÇÃO:

• A solução irá atender as necessidades técnicas e legais para aprimorar o nível de segurança de Tecnologia da Informação, Privacidade e Proteção de Dados da CONTRATANTE. A escolha por um software único com um conjunto de módulos integrados como uma solução ofertada por uma única contratada em detrimento da aquisição individual de cada produto de software se faz necessária, principalmente, pela complexidade das opções possíveis para atender a necessidade da contratação objeto deste Termo de Referência.

• Portanto, os serviços a serem executados estão relacionados a uma solução de software, sem viabilidade de desmembramento. visto que diversas ferramentas existentes na solução informatizada são partes integrantes do processo de implementação e adequação da CONTRATANTE à Lei Geral de Proteção de Dados, tais como a gestão de riscos, geração de relatórios de inventário e Relatório de Impacto à Proteção de Dados, geração de Comunicação de Incidentes de Privacidade, além de varredura continuada de dados para manutenção do mapeamento e segurança da informação.

6. REQUISITOS MÍNIMOS DE QUALIFICAÇÃO TÉCNICA

• Para aferir a qualificação técnica, será solicitado atestado de capacidade técnica que comprove a aptidão da licitante para o desempenho de atividades pertinentes e compatíveis em características, quantidades e prazos com o objeto em questão, contendo, no mínimo, as seguintes informações:

- Nome ou razão social, CNPJ e endereço completo do emitente;
- Descrição do escopo dos serviços prestados;
- Nome ou razão social da empresa que prestou o serviço ao emitente;
- Data de emissão do atestado ou da certidão;
- Assinatura e identificação do signatário (nome, telefone, cargo e função que exerce junto à empresa emitente).

• Os atestados que comprovem a aptidão descrita acima deverão ser emitidos por pessoas jurídicas de direito público.

• Os atestados deverão referir-se a serviços prestados no âmbito de sua atividade econômica principal ou secundária especificadas no contrato social vigente.

• O licitante disponibilizará todas as informações necessárias à comprovação da legitimidade dos atestados apresentados.

• A empresa licitante deverá demonstrar atuação em, pelo menos, 02 (duas) Entidades Públicas em que seus serviços e produtos objetos deste procedimento foram ou estão sendo prestados, com a apresentação de Atestado de Capacidade Técnica, ainda que parcial (em caso de contrato em execução), hipótese em que deverão ser descritos os serviços já executados.

6.1. QUALIFICAÇÃO TÉCNICA

• A Contratada deverá apresentar declaração e/ou certidão comprovando que é fabricante do software e fornecedora dos serviços, objeto deste procedimento.

• A fim de garantir que os profissionais envolvidos possuem conhecimento e habilidade para executar o serviço e a devida implementação e adequação da Lei Geral de Proteção de Dados à entidade Contratante, a Contratada deverá, obrigatoriamente, compor a equipe técnica de operação com as certificações/qualificações abaixo ou equivalentes:

Mh



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) /

7) REQUISITOS DA CONTRATAÇÃO**Sustentabilidade:**

Não se aplica.

Indicação de marcas ou modelos (Art. 41, inciso I, da Lei nº 14.133, de 2021):

Não se aplica.

Da vedação de contratação de marca ou produto

Não se aplica.

Da exigência de amostra

Não se aplica.

Da exigência de carta de solidariedade

Não se aplica.

Subcontratação

Vedada na integralidade.

Garantia da contratação

Não se aplica.

8) MODELO DE EXECUÇÃO DO OBJETO**Condições de Prestação dos Serviços**

O serviço deverá ser prestado, conforme cronograma do setor requisitante.

Em caso fortuito, dentro de nova data a ser remarcada pelo setor requisitante;

O local da prestação dos serviços será na cidade de Ituiutaba/MG.

At

Garantia manutenção e assistência técnica

Não se aplica.

9) MODELO DE GESTÃO DO CONTRATO

O contrato deverá ser executado fielmente pelas partes, de acordo com as cláusulas avençadas e as normas da Lei nº 14.133, de 2021, e cada parte responderá pelas consequências de sua inexecução total ou parcial.

Em caso de impedimento, ordem de paralisação ou suspensão do contrato, o serviço será prorrogado automaticamente pelo tempo correspondente, anotadas tais circunstâncias mediante simples apostila, sendo remarcada nova data.

As comunicações entre o órgão e a contratada devem ser realizadas por escrito sempre que o ato exigir tal formalidade, admitindo-se o uso de mensagem eletrônica para esse fim.

O órgão poderá convocar representante da empresa para adoção de providências que devam ser cumpridas de imediato.

Após a assinatura do contrato ou instrumento equivalente, o órgão poderá convocar o representante da empresa contratada para reunião inicial para apresentação do plano de fiscalização, que conterá informações acerca das obrigações contratuais, dos mecanismos de fiscalização, das estratégias para execução do objeto, do plano complementar de execução da contratada, quando houver, do método de aferição dos resultados e das sanções aplicáveis, dentre outros.

Fiscalização

A execução do contrato deverá ser acompanhada e fiscalizada pelo(s) fiscal(is) do contrato, ou pelos respectivos substitutos (Lei nº 14.133, de 2021, art. 117, caput) e ficará por conta do seguinte servidor:

Gestor: Othavio Lemes Fernandes Alves Valentim; Matrícula: 5141; Fiscal: Viviane Aparecida Carvalho; Matrícula: 9728.

10) CONDIÇÕES E PRAZOS DE PAGAMENTO:**Prazo de pagamento**

O pagamento será efetuado no prazo de **até 10 (dez) dias** contados da finalização da apresentação da Nota Fiscal pelo Fornecedor, após o ateste pela Fiscal do contrato ou servidor nomeado para esta função, sendo efetuada a retenção de tributos sobre o pagamento a ser realizado, conforme determina a legislação vigente.

Forma de pagamento

O pagamento será realizado por meio de ordem bancária, para crédito em banco, agência e conta corrente, indicados pelo contratado.

Será considerada data do pagamento o dia em que constar como emitida a ordem bancária para pagamento.

O contratado regularmente optante pelo Simples Nacional, nos termos da Lei Complementar nº 123, de 2006, não sofrerá a retenção tributária quanto aos impostos e contribuições abrangidos por aquele regime. No entanto, o pagamento ficará condicionado à apresentação de comprovação, por meio de documento oficial, de que faz jus ao tratamento tributário favorecido previsto na referida Lei Complementar.

Condições de aquisição e pagamento semelhantes aos do Setor Privado, nos termos do artigo 40, Inciso I da Lei 14.133/2021.

Não haverá, sob hipótese alguma, pagamento antecipado.

Não será aplicada tal condição de pagamento nesta contratação tendo em vista que esta contratação não contempla das mesmas flexibilidades das condições de aquisição e pagamento semelhantes aos do Setor

AA

Privado, além disso, as condições de execução do contrato, recebimento e pagamento estão descritas neste Termo de Referência.

Não deve a contratação em hipótese alguma ser mais onerosa e menos eficiente do que a do setor privado.

Havendo erro na Nota Fiscal ou circunstância que impeça a liquidação da despesa, esta será devolvida à CONTRATADA, e o pagamento ficará pendente até que ela providencie as medidas saneadoras. Nesta hipótese, o prazo para pagamento iniciar-se-á após a regularização da situação ou reapresentação do documento fiscal não acarretando qualquer ônus para a CONTRATANTE.

Previamente à data do pagamento, a CONTRATANTE juntará aos autos a Certidão Negativa (ou Positiva, com efeito de negativa) de Débitos Trabalhistas, Certidão junto INSS, FGTS, Estadual e Municipal, para verificar a manutenção das condições de habilitação da CONTRATADA.

Os tributos e as contribuições fiscais, bem como quaisquer outras despesas necessárias à entrega dos bens/materiais são de responsabilidade da CONTRATADA, podendo a CONTRATANTE exigir, a qualquer tempo, a comprovação de sua regularidade.

11) DEVERES DO CONTRATANTE E DO CONTRATADO

DAS OBRIGAÇÕES DO CONTRATANTE:

- a) Efetuar o pagamento dos serviços prestados;
- b) Fiscalizar se os serviços entregues estão em conformidade com o solicitado pelo Termo de Referência;
- c) Rejeitar, no todo ou em parte, o objeto contratual entregue em desacordo com o previsto neste contrato, justificando as razões da recusa.

DAS OBRIGAÇÕES DO CONTRATADO:

- a) Entregar os serviços, de acordo com as especificações constantes neste Termo de Referência;
- b) Garantir a boa qualidade dos serviços ofertados, efetuando a correção do que for considerado de má qualidade pela Administração;
- c) Arcar com as responsabilidades fiscais, trabalhistas, tributárias e demais encargos que vierem a incidir sobre objeto deste contrato;
- d) Responder por qualquer dano ou prejuízo causado à Prefeitura Municipal ou a terceiros, por ação ou omissão culposa ou dolosa de seus prepostos, subcontratados e/ou decorrência da entrega do objeto, após apuração de responsabilidades;
- e) Manter, durante a vigência do contrato, de acordo com as obrigações assumidas, todas as condições de habilitação e qualificação exigida na licitação.

12) FORMA E CRITÉRIOS DE SELEÇÃO DO FORNECEDOR E FORMA DE FORNECIMENTO

Forma de seleção e critério de julgamento da proposta

Não há.

Forma de fornecimento

O serviço será prestado conforme especificação da tabela do subitem 1 deste documento.

At

Exigências de habilitação

Para fins de habilitação, deverá o licitante comprovar os seguintes requisitos:

Habilitação jurídica

Pessoa física: cédula de identidade (RG) ou documento equivalente que, por força de lei, tenha validade para fins de identificação em todo o território nacional;

Empresário individual: inscrição no Registro Público de Empresas Mercantis, a cargo da Junta Comercial da respectiva sede;

Microempreendedor Individual - MEI: Certificado da Condição de Microempreendedor Individual - CCMEI, cuja aceitação ficará condicionada à verificação da autenticidade no sítio <https://www.gov.br/empresas-e-negocios/pt-br/empreendedor>;

Sociedade empresária, sociedade limitada unipessoal – SLU ou sociedade identificada como empresa individual de responsabilidade limitada - EIRELI: inscrição do ato constitutivo, estatuto ou contrato social no Registro Público de Empresas Mercantis, a cargo da Junta Comercial da respectiva sede, acompanhada de documento comprobatório de seus administradores;

Sociedade empresária estrangeira: portaria de autorização de funcionamento no Brasil, publicada no Diário Oficial da União e arquivada na Junta Comercial da unidade federativa onde se localizar a filial, agência, sucursal ou estabelecimento, a qual será considerada como sua sede, conforme Instrução Normativa DREI/ME nº 77, de 18 de março de 2020.

Sociedade simples: inscrição do ato constitutivo no Registro Civil de Pessoas Jurídicas do local de sua sede, acompanhada de documento comprobatório de seus administradores;

Filial, sucursal ou agência de sociedade simples ou empresária: inscrição do ato constitutivo da filial, sucursal ou agência da sociedade simples ou empresária, respectivamente, no Registro Civil das Pessoas Jurídicas ou no Registro Público de Empresas Mercantis onde opera, com averbação no Registro onde tem sede a matriz;

Sociedade cooperativa: ata de fundação e estatuto social, com a ata da assembleia que o aprovou, devidamente arquivado na Junta Comercial ou inscrito no Registro Civil das Pessoas Jurídicas da respectiva sede, além do registro de que trata o art. 107 da Lei nº 5.764, de 16 de dezembro 1971.

Os documentos apresentados deverão estar acompanhados de todas as alterações ou da consolidação respectiva.

Habilitação fiscal, social e trabalhista

Prova de inscrição no Cadastro Nacional de Pessoas Jurídicas ou no Cadastro de Pessoas Físicas, conforme o caso;

Prova de regularidade fiscal perante a Fazenda Nacional, mediante apresentação de certidão expedida conjuntamente pela Secretaria da Receita Federal do Brasil (RFB) e pela Procuradoria-Geral da Fazenda Nacional (PGFN), referente a todos os créditos tributários federais e à Dívida Ativa da União (DAU) por elas administrados, inclusive aqueles relativos à Seguridade Social, nos termos da Portaria Conjunta nº 1.751, de 02 de outubro de 2014, do Secretário da Receita Federal do Brasil e da Procuradora-Geral da Fazenda Nacional.

Prova de regularidade com o Fundo de Garantia do Tempo de Serviço (FGTS);

Prova de inexistência de débitos inadimplidos perante a Justiça do Trabalho, mediante a apresentação de certidão negativa ou positiva com efeito de negativa, nos termos do Título VII-A da Consolidação das Leis do Trabalho, aprovada pelo Decreto-Lei nº 5.452, de 1º de maio de 1943;

Prova de inscrição no cadastro de contribuintes [Estadual/Distrital] ou [Municipal/Distrital] relativo ao domicílio ou sede do fornecedor, pertinente ao seu ramo de atividade e compatível com o objeto contratual;

Prova de regularidade com a Fazenda [Estadual/Distrital] ou [Municipal/Distrital] do domicílio ou sede do fornecedor, relativa à atividade em cujo exercício contrata ou concorre;

Mor



Caso o fornecedor seja considerado isento dos tributos [Estadual/Distrital] ou [Municipal/Distrital] relacionados ao objeto contratual, deverá comprovar tal condição mediante a apresentação de declaração da Fazenda respectiva do seu domicílio ou sede, ou outra equivalente, na forma da lei.

O fornecedor enquadrado como microempreendedor individual que pretenda auferir os benefícios do tratamento diferenciado previstos na Lei Complementar n. 123, de 2006, estará dispensado da prova de inscrição nos cadastros de contribuintes estadual e municipal.

Qualificação Econômico-Financeira

Certidão negativa de falência expedida pelo distribuidor da sede do fornecedor - Lei nº 14.133, de 2021, art. 69, caput, inciso II);

Qualificação Técnica

A qualificação técnica exigida será conforme detalhado no item 6.

13) ESTIMATIVAS DO VALOR DA CONTRATAÇÃO

O custo estimado total da contratação é de R\$ 1.240.740,00 (um milhão, duzentos e quarenta mil e setecentos e quarenta reais).

14) DOTAÇÃO ORÇAMENTÁRIA

Esta contratação ocorrerá por conta da dotação:

01.13.00 - SEC. MUNICIPAL DE ADMINISTRAÇÃO E REC.HUMANOS
01.13.04 - DEPTO DE TECNOLOGIA DA INFORMAÇÃO
04.126.0002.2.086 - GESTÃO DA TECNOLOGIA DA INFORMAÇÃO
3.3.90.40.00 - SER. DE TECNOLOGIA DA INFOR. E COMUNICAÇÃO – PESSOA JURIDICA
1.500.000.0000 - RECURSOS ORDINÁRIOS

01.07.00 - SEC. MUN. EDUCAÇÃO, ESPORTE E LAZER
01.07.01 - GABINETE DO SECRETARIO
12.122.0002.2.087 GESTAO DAS AÇOES DE EDUCAÇÃO
3.3.90.40.00 - SER. DE TECNOLOGIA DA INFOR. E COMUNICAÇÃO – PESSOA JURIDICA

15) DOS ENCARGOS TRABALHISTAS, PREVIDENCIÁRIOS E FISCAIS:

Compromete-se a contratada a arcar com as responsabilidades fiscais, tributárias e trabalhistas que incidirem sobre o objeto.

16) DAS SANÇÕES:

O descumprimento total ou parcial das obrigações assumidas pela contratada, sem justificativa aceita pela Prefeitura Municipal de Ituiutaba-MG, resguardados os procedimentos legais pertinentes, poderá acarretar nas seguintes sanções:

- Multa de mora no percentual correspondente a 1% (um por cento) calculada sobre o valor total estimado na nota de empenho, por dia de atraso, até o limite de 20 (vinte) dias, caracterizando a inexecução parcial;
- Suspensão temporária do direito de licitar e contratar com a Administração Municipal de Ituiutaba;
- Declaração de inidoneidade para licitar e contratar com a Administração Pública enquanto perdurarem os motivos determinantes da punição, ou até que seja promovida a reabilitação perante a autoridade que aplicou a penalidade;
- Advertência escrita;
- Caso venha desistir de fornecer os itens, além de outras cominações legais, a multa será de 20% (vinte por cento) sobre o valor do total do empenho.

A multa deverá ser recolhida aos cofres públicos da Prefeitura Municipal de Ituiutaba-MG, via Tesouraria, no prazo máximo de 10 (dez) dias corridos, a contar da data de recebimento da notificação enviada pela Prefeitura.

At



As sanções aqui previstas são independentes entre si, podendo ser aplicadas isoladas ou cumulativamente, sem prejuízo de outras medidas cabíveis previstas na Lei 14.133/21, inclusive a responsabilização da empresa contratada por eventuais perdas e danos causados à Administração.

Em qualquer hipótese e aplicações de sanções será assegurado à Contratada o contraditório e a ampla defesa.

17) DA EXTINÇÃO DO CONTRATO

Todos os casos de extinção contratual serão formalmente motivados nos autos, assegurado o contraditório e a ampla defesa.

A inexecução total ou parcial do CONTRATO enseja sua extinção, com as consequências a seguir previstas no art. 137 da Lei Federal n.º 14.133/21.

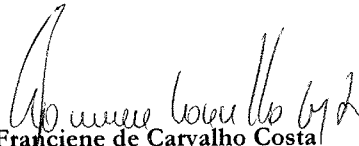
A extinção contratual poderá ser:

- a) Determinada por Ato unilateral e escrito do CONTRATANTE, conforme o artigo 138 da Lei Federal n.º 14.133/21.
- b) Amigável, por acordo entre as partes, mediante autorização escrita e fundamentada pelo CONTRATANTE, reduzida a termo no processo de licitação, desde que haja conveniência do CONTRATANTE;
- c) Judicial, nos termos da legislação.

Constituem motivos para a extinção do contrato, todos aqueles previstos no art. 137, da Lei Federal n.º 14.133/21.

Em caso de extinção contratual, sem que haja culpa do CONTRATADO, será este ressarcido dos prejuízos regularmente comprovados, quando os houver sofrido, com direito a:

- a) Devolução de garantia, se houver;
- b) Pagamentos devidos pela execução do CONTRATO até a data da rescisão.


Franciene de Carvalho Costa

Ituiutaba-MG, 07 de julho de 2025.

Secretária Municipal de Administração e Recursos Humanos


Érika Ferreira Lima Franco
Secretária Municipal de Educação, Esporte e Lazer