TRIBUNAL DE JUSTIÇA DO ESTADO DO AMAZONAS
Av. André Araújo, S/N - Bairro Aleixo - CEP 69060-000 - Manaus - AM - www.tjam.jus.br

EDITAL DE LICITAÇÃO - PE - SECOP/SEAC

EDITAL DO PREGÃO ELETRÔNICO/SRP N.º 40/2024-TJAM

Objeto: Contratação de empresa especializada no fornecimento de solução de gerenciamento de acessos privilegiados (PAM – Privileged Access Management).

SISTEMA DE REGISTRO DE PREÇOS? (X) Sim ( ) Não

Valor Total Estimado: R$ 5.380.922,80 (cinco milhões, trezentos e oitenta mil novecentos e vinte e dois reais e oitenta centavos)

Data de divulgação do Edital: 21/08/2024
Início do cadastramento eletrônico de propostas.
Divulgação do Pregão, mediante aviso publicado no Diário de Justiça Eletrônico e nos sítios eletrônicos: **www.gov.br/compras** e **www.tjam.jus.br**.

Data de abertura: 04/09/2024, às 11h00 (Horário de Brasília)
No sítio www.gov.br/compras UASG: 925866

Licitação Exclusiva ME/EPP? ( ) Sim (X) Não	**Há Itens Exclusivos ME/EPP e/ou Reserva de cota ME/EPP?** ( ) Sim (X) Não
Decreto 7.174/10? ( ) Sim (X) Não	**Margem de preferência?** ( ) Sim (X) Não
Vistoria? ( ) Obrigatória (X) Facultativa ( ) Não se aplica, Telefone para contato: (92) 2129-6779; e-mail: infra.tic@tjam.jus.br	**Amostra/ Catálogo?** (X) Sim ( ) Não
Pedidos de esclarecimentos Até 30/08/2024 às 15 h (Horário de Brasília) exclusivamente pelo e-mail colic@tjam.jus.br	**Impugnação** Até 30/08/2024 às 15 h (Horário de Brasília) exclusivamente pelo e-mail colic@tjam.jus.br
Informações Adicionais	
Exclusivamente pelo e-mail colic@tjam.jus.br	**Endereço:** Av. André Araújo, s/nº, Aleixo Manaus/AM-CEP: 69060-000

Todas as referências de tempo contidas neste Edital observarão o horário de Brasília-DF.

Todos os documentos a serem encaminhados eletronicamente deverão ser configurados, preferencialmente, nos seguintes formatos: Adobe Acrobat Reader (extensão .PDF), Word (extensão .DOC ou .DOCX), Excel (extensão .XLS ou .XLSX), podendo ainda ser processados por compactação nos formatos ZIP (extensão .ZIP) ou RAR (extensão .RAR).

Telefone em caso de dúvidas ou problemas técnicos relacionados à utilização do Portal de Compras do Governo Federal: 0800-978-9001.

Acompanhe as sessões públicas dos Pregões do Tribunal de Justiça do Amazonas pelo endereço **www.gov.br/compras/pt-br/acesso-a-informacao/consulta-detalhada** selecionando as opções Pregões > Em

andamento > Cód. UASG “925866”. O Edital está disponível para download nos endereços **www.gov.br/compras** e www.tjam.jus.br (Licitações>Editais, Avisos, Erratas e Docs>Licitação 2024>Pregões Eletrônicos).		

O **Tribunal de Justiça do Estado do Amazonas (TJAM)**, por meio de sua **Presidência**, informa a designação de Pregoeiro(a) pelo Ato n.° 945/2023 de 07 de dezembro de 2023 e pela Portaria n.º 4.715/2023, de 07 de dezembro de 2023, e comunica aos interessados que realizará licitação na modalidade **PREGÃO ELETRÔNICO**, do tipo **MENOR PREÇO GLOBAL**, conforme **Processo Administrativo nº. 2024/000014603-00**, nos termos da Lei Federal n.º 14.133/2021, da Lei Complementar n.° 123/2006, do Decreto Estadual n.° 47.133/2023, do Decreto Federal n.º 3.555/2000, da Resolução n.° 64/2023 TJAM, demais legislações aplicáveis e, ainda, de acordo com as condições estabelecidas neste edital e seus anexos.

CLÁUSULA PRIMEIRA
DO OBJETO

1.1. O objeto da presente licitação é a Contratação de empresa especializada no fornecimento de solução de gerenciamento de acessos privilegiados (PAM – Privileged Access Management). conforme condições, quantidades e exigências estabelecidas neste Edital e seus anexos.

1.2. Em caso de discrepância entre as especificações deste objeto descritas no sistema Compras.gov.br e as constantes deste Edital, prevalecerão as últimas.

CLÁUSULA SEGUNDA
DA DOTAÇÃO ORÇAMENTÁRIA

2.1. A despesa com a execução do objeto desta licitação é estimada em **R$ 5.380.922,80 (cinco milhões, trezentos e oitenta mil novecentos e vinte e dois reais e oitenta centavos)**, conforme Termo de Referência e documentos correlatos em anexo, e será custeada pelo orçamento do Poder Judiciário do Estado do Amazonas por meio de suas Unidades Gestoras: Tribunal de Justiça do Estado do Amazonas – TJ, Fundo de Reaparelhamento do Poder Judiciário – FUNJEAM ou Fundo Especial do Tribunal de Justiça – FUNETJ.

2.2. Na licitação para registro de preços não é necessário indicar a dotação orçamentária, que somente será exigida para a formalização do contrato ou outro instrumento equivalente.

CLÁUSULA TERCEIRA
DAS COMUNICAÇÕES

3.1. A comunicação, durante o certame, entre Licitantes e a Coordenadoria de Licitação (COLIC), será realizada exclusivamente pelo sistema Comprasgov ou através do e-mail colic@tjam.jus.br.

3.2. Quando necessário, a COLIC publicará Comunicados atinentes ao andamento do certame no sistema Comprasgov e no site deste Poder (Licitação > Documentos > Editais, Avisos, Erratas e Docs > Licitações 2024 > Pregão Eletrônico).

CLÁUSULA QUARTA
DA IMPUGNAÇÃO E DO PEDIDO DE ESCLARECIMENTO

4.1. Até **03 (três) dias úteis** antes da data fixada para abertura da sessão pública, a encerrar em 30/08/2024, às 15h (horário de Brasília/DF), qualquer pessoa poderá **impugnar** o ato convocatório deste pregão mediante **petição**, que deverá obrigatoriamente conter a identificação da Impugnante (CPF/CNPJ), a ser enviada para o endereço eletrônico colic@tjam.jus.br.

4.2. O **pedido de esclarecimento**, mediante **petição**, que deverá obrigatoriamente conter a identificação do Interessado (CPF/CNPJ), deve ser enviado ao(à) Pregoeiro(a), em até **03 (três) dias úteis** anteriores à

data fixada para abertura da sessão pública, a encerrar em 30/08/2024, às 15h (horário de Brasília/DF), para o endereço eletrônico colic@tjam.jus.br.

4.3. A resposta à impugnação ou ao pedido de esclarecimento será divulgada em sítio eletrônico oficial no prazo de até **3 (três) dias úteis**, limitado ao último dia útil anterior à data da abertura do certame.

4.3.1. A concessão de efeito suspensivo à impugnação é medida excepcional e deverá ser motivada pelo(a) Pregoeiro(a), nos autos do processo de licitação.

4.4. Acolhidos os argumentos da(s) petição(ões) das Cláusulas 4.1 e 4.2, será designada nova data para a realização do certame, exceto quando, inquestionavelmente, a alteração não afetar a formulação das propostas.

4.5. As impugnações, esclarecimentos, bem como as devidas respostas serão disponibilizadas no sistema eletrônico Compras.gov.br (https://www.gov.br/compras/pt-br/acesso-a-informacao/consulta-detalhada/consulta-detalhada) e no site oficial do TJAM https://www.tjam.jus.br/index.php/documentos-licitacao/editais-avisos-erratas-e-docs.

CLÁUSULA QUINTA
DO CREDENCIAMENTO E DAS CONDIÇÕES DE PARTICIPAÇÃO

5.1. A sessão deste pregão será pública e realizada na data, horário e endereço eletrônico indicado.

5.2. Poderão participar deste Pregão os interessados que estiverem previamente credenciados no Sistema de Cadastramento Unificado de Fornecedores - SICAF e no Sistema de Compras do Governo Federal (www.gov.br/compras), por meio de Certificado Digital conferido pela Infraestrutura de Chaves Públicas Brasileira – ICP – Brasil.

5.3. Para ter acesso ao sistema eletrônico, os interessados em participar deste pregão deverão dispor de chave de identificação e senha pessoal, obtidas junto à Secretaria de Gestão do Ministério da Economia (SEGES), onde também deverão informar-se a respeito do seu funcionamento, regulamento e receber instruções detalhadas para sua correta utilização.

5.4. O licitante responsabiliza-se exclusiva e formalmente pelas transações efetuadas em seu nome, assume como firmes e verdadeiras suas propostas e seus lances, inclusive os atos praticados diretamente ou por seu representante, excluída a responsabilidade do provedor do sistema ou do órgão ou entidade promotora da licitação por eventuais danos decorrentes de uso indevido das credenciais de acesso, ainda que por terceiros.

5.5. É de responsabilidade do cadastrado conferir a exatidão dos seus dados cadastrais nos Sistemas relacionados no item anterior e mantê-los atualizados junto aos órgãos responsáveis pela informação, devendo proceder, imediatamente, à correção ou à alteração dos registros tão logo identifique incorreção ou aqueles se tornem desatualizados.

5.6. A não observância do disposto no item anterior poderá ensejar desclassificação no momento da habilitação.

5.7. Não poderá disputar esta licitação:

5.7.1. Aquele que não atenda às condições deste Edital e seu(s) anexo(s);

5.7.2. Impedidos de contratar no âmbito da Administração Pública direta e indireta do Estado do Amazonas, nos termos do art. 156, III, § 4º, da Lei Federal n.º 14.133/2021;

5.7.3. Suspensos de participar de licitações e impedidos de contratar com o Tribunal de Justiça do Estado do Amazonas, nos termos do art. 87, III, da Lei n.° 8.666/1993, por meio de punições pretéritas e ainda vigentes;

5.7.4. Declarados inidôneos para licitar ou contratar com a Administração Pública, na forma do art. 87, IV, da Lei n.° 8.666/1993, por meio de punições pretéritas e ainda vigentes;

5.7.5. Declarados inidôneos para licitar ou contratar com a Administração Pública, na forma do art. 156, IV, § 5º, da Lei Federal n.º 14.133/2021;

5.7.6. Estrangeiros que não tenham representação legal no Brasil com poderes expressos para receber citação e responder administrativa e judicialmente;

5.7.7. Entidades empresariais que estejam sob falência, concurso de credores, em processo de dissolução total ou liquidação;

5.7.8. Agente público do órgão ou entidade licitante;

5.7.9. Quaisquer interessados que se enquadrem nas vedações previstas no art. 14º da Lei Federal n.º 14.133/2021;

5.7.10. Empresas sob a forma de consórcio, haja vista a baixa complexidade e o valor estimado da contratação;

5.7.11. Empresas sob a forma de cooperativas, consoante a jurisprudência do Tribunal de Contas da União (Súmula 281 – TCU);

5.7.12. Organizações da Sociedade Civil de Interesse Público - OSCIP, atuando nessa condição;

5.7.13. Não poderá participar, direta ou indiretamente, da licitação ou da execução do contrato agente público do órgão ou entidade contratante, devendo ser observadas as situações que possam configurar conflito de interesses no exercício ou após o exercício do cargo ou emprego, nos termos da legislação que disciplina a matéria, conforme § 1º do art. 9º da Lei Federal n.º 14.133/2021.

5.8. Não será permitida a subcontratação total ou parcial do objeto desta licitação, ficando sob a inteira responsabilidade da licitante contratada o cumprimento de todas as condições contratuais, atendendo aos requisitos técnicos e legais para esta finalidade.

CLÁUSULA SEXTA
DA VISTORIA TÉCNICA

6.1. As interessadas poderão realizar, sob o acompanhamento de servidor especialmente designado, vistoria aos locais de execução dos serviços, no todo ou em parte, em data e horário previamente acordados segundo a conveniência deste Órgão, com o objetivo de conhecer as instalações onde serão executados os serviços e sanar as dúvidas porventura existentes, a fim de subsidiar a elaboração das propostas a serem submetidas ao certame.

6.2. As visitas deverão ser previamente agendadas, com 72 (setenta e duas) horas de antecedência, pelo telefone (92) 2129-6779 – DIVISÃO DE INFRAESTRUTURA DE TECNOLOGIA DA INFORMAÇÃO E COMUNICAÇÃO, no período das 8 às 14hs, ou via e-mail através de: infra.tic@tjam.jus.br.

6.3. A empresa licitante poderá apresentar Declaração de Vistoria Técnica (Anexo VII) de que, por meio do seu representante, visitou e conheceu o local de execução dos serviços ou entrega do objeto desta licitação.

6.4. A declaração da licitante de que conhece as condições locais para a execução do serviço ou entrega do objeto **supre a necessidade** de vistoria técnica.

CLÁUSULA SÉTIMA
DA APRESENTAÇÃO DA PROPOSTA E DOS DOCUMENTOS DE HABILITAÇÃO

7.1. A presente licitação seguirá as seguintes fases, em sequência: apresentação de propostas e lances, julgamento, habilitação, recursal e homologação.

7.2. Os licitantes encaminharão, exclusivamente por meio do sistema eletrônico, a proposta com o preço ou o percentual de desconto, conforme o critério de julgamento adotado neste Edital, até a data e o horário estabelecidos para abertura da sessão pública.

7.3. Os licitantes poderão retirar ou substituir a proposta até a abertura da sessão pública.

7.4. Após a abertura da sessão, fica vedada a alteração da proposta, exceto para ajustes diligenciados pelo(a) Pregoeiro(a).

7.5. A apresentação da proposta implica a aceitação plena e total das condições deste Edital e seus anexos.

7.6. Não haverá ordem de classificação na etapa de apresentação da proposta e dos documentos de habilitação pelo licitante, o que ocorrerá somente após os procedimentos de abertura da sessão pública e da fase de envio de lances.

7.7. Os documentos que compõem a proposta e a habilitação da licitante melhor classificada somente serão disponibilizados, pelo sistema, para avaliação do(a) Pregoeiro(a) e para acesso público após o encerramento do envio de lances.

7.8. Os documentos complementares à proposta e à habilitação, quando necessários à confirmação daqueles exigidos no Edital e já apresentados, serão exigidos da licitante melhor classificada após o julgamento das propostas.

7.9. Caberá ao licitante interessado em participar da licitação acompanhar as operações no sistema eletrônico durante o processo licitatório e se responsabilizar pelo ônus decorrente da perda de negócios diante da inobservância de mensagens emitidas pela Administração ou de sua desconexão.

7.10. O licitante deverá comunicar imediatamente ao provedor do sistema qualquer acontecimento que possa comprometer o sigilo ou a segurança, para imediato bloqueio de acesso.

CLÁUSULA OITAVA
DAS DECLARAÇÕES

8.1. Todas as declarações exigidas no sistema Compras.gov.br, bem como as supervenientes e eventualmente exigidas durante o certame, serão aferidas para fins de habilitação.

8.1.1. O não envio das declarações poderá ocasionar a inabilitação, observados os prazos de que trata este instrumento convocatório.

8.2. A licitante deverá declarar:

8.2.1. Que está ciente e de acordo com as condições contidas no Edital e que cumpre plenamente os requisitos de habilitação definidos no instrumento convocatório;

8.2.2. Que até a presente data, inexistem fatos impeditivos para sua habilitação no presente processo licitatório, ciente da obrigatoriedade de declarar ocorrências posteriores;

8.2.3. Que elaborou de maneira independente sua proposta de preço para participar desta licitação;

8.2.4. Que não emprega menores de dezoito anos em trabalho noturno, perigoso ou insalubre, nem menores de dezesseis anos em qualquer trabalho, salvo na condição de aprendiz, a partir dos quatorze anos;

8.2.5. Que, por ser enquadrado como microempresa ou empresa de pequeno porte, atende aos requisitos do art. 3º da Lei Complementar n.º 123/2006, para fazer jus aos benefícios previstos na legislação;

8.2.6. Que, conforme disposto no art. 93 da Lei nº 8.213/1991, está ciente do cumprimento da reserva de cargos prevista em lei para pessoa com deficiência ou para reabilitado da Previdência Social e que, se aplicado ao número de funcionários da empresa, atende às regras de acessibilidade previstas na legislação;

8.2.7. Que cumpre a cota de aprendizagem nos termos estabelecidos no art. 429 da CLT;

8.2.8. Que não possui em sua cadeia produtiva, empregados executando trabalho degradante ou forçado, nos termos do inciso III e IV do art.1º e no inciso III do Art. 5º da Constituição Federal.

8.3. O(A) Pregoeiro(a) poderá exigir declarações não previstas no Edital, justificando motivadamente a diligência.

8.3.1. O(A) Pregoeiro(a) poderá diligenciar o envio ou reenvio de declarações exigidas ou apresentadas no certame.

8.3.2. As declarações devem ser encaminhadas por meio da opção “enviar anexo” do sistema Compras.gov.br ou para o endereço eletrônico colic@tjam.jus.br.

8.4. A falsidade da declaração de que trata a Cláusula Oitava sujeitará a licitante às sanções previstas na Resolução n.° 64/2023 TJAM.

CLÁUSULA NONA
DO PREENCHIMENTO DA PROPOSTA

9.1. A Proposta de Preços deverá atender o Anexo III do Edital, acompanhada de catálogo, folder, manual ou sítio da internet, conforme disposto na Cláusula DÉCIMA deste Edital.

9.2. Todas as especificações do objeto contidas na proposta vinculam o licitante.

9.3. Nos valores propostos estarão inclusos todos os custos operacionais, encargos previdenciários, trabalhistas, tributários, comerciais e quaisquer outros que incidam direta ou indiretamente na execução do objeto.

9.4. A proposta de preços deverá estar devidamente datada e assinada pelo Responsável Legal, devendo ainda conter as informações dispostas no Formulário Proposta de Preços (Anexo III deste Edital), tais como os seus dados cadastrais, dados bancários, indicação de marcas, modelos, tipos e fabricantes dos produtos, se houver, preços unitários e totais.

9.5. Não é permitida a cotação de quantidade inferior àquela constante no Termo de Referência.

9.6. Os preços unitários e totais deverão estar em moeda nacional (R$), com apenas duas casas decimais após a vírgula, e em caso de divergência entre preços unitários e totais, prevalecerão os primeiros.

9.7. Poderão ser corrigidos automaticamente pelo(a) Pregoeiro(a) quaisquer erros aritméticos e o preço global da proposta, se necessário.

9.8. Não será aceita proposta com itens cujos valores estejam acima do estimado por este Poder.

9.8.1. Se houver necessidade de correção, não serão aceitas propostas contendo valores de itens superiores aos anteriormente apresentados pela licitante.

9.9. Não será admitida proposta que apresente valores simbólicos, irrisórios ou de valor zero, incompatíveis com os preços de mercado.

9.10. Não será considerada qualquer oferta de vantagem não prevista neste Edital.

9.11. Se a proposta não for aceitável, se a licitante deixar de enviá-la, se deixar de atender solicitação feita ou não atender às exigências deste Edital, o(a) Pregoeiro(a) examinará a proposta subsequente e, assim, sucessivamente, na ordem de classificação, até a apuração daquela que atenda aos requisitos.

9.12. Os preços ofertados, tanto na proposta inicial, quanto na etapa de lances, serão de exclusiva responsabilidade do licitante, não lhe assistindo o direito de pleitear qualquer alteração, sob alegação de erro, omissão ou qualquer outro pretexto.

9.13. Se o regime tributário da empresa implicar o recolhimento de tributos em percentuais variáveis, a cotação adequada será a que corresponde à média dos efetivos recolhimentos da empresa nos últimos doze meses.

9.14. Independentemente do percentual de tributo inserido na planilha, no pagamento serão retidos na fonte os percentuais estabelecidos na legislação vigente.

9.15. A apresentação das propostas implica obrigatoriedade do cumprimento das disposições nelas contidas, em conformidade com o que dispõe o Termo de Referência, assumindo o proponente o compromisso de executar o objeto licitado nos seus termos, bem como de fornecer os materiais, equipamentos, ferramentas e utensílios necessários, em quantidades e qualidades adequadas à perfeita execução contratual, promovendo, quando requerido, sua substituição.

9.16. O prazo de validade da proposta será de 60 (sessenta) dias, a contar da data de sua apresentação.

9.16.1. A data inicial de validade da proposta será renovada quando do envio da proposta adequada ao último lance ofertado após a negociação.

CLÁUSULA DÉCIMA

DAS AMOSTRAS, DOS FOLDERS, CATÁLOGOS, DOS PROSPECTOS OU MANUAIS

10.1. Deverá ser apresentado catálogo, folder, manual ou sítio da internet que comprove que todos os materiais e equipamentos a serem utilizados atendem rigorosamente as especificações técnicas mínimas exigidas.

10.2. A Divisão de Tecnologia da Informação e Comunicação do TJAM, sito a Avenida André Araújo s/n, Prédio Desembargador Arnoldo Péres - Bairro Aleixo – CEP 69.060-000 será a responsável por receber e validar os objetos desta contratação.

CLÁUSULA DÉCIMA PRIMEIRA

DA ABERTURA DA SESSÃO, CLASSIFICAÇÃO DAS PROPOSTAS E FORMULAÇÃO DE LANCES

11.1. A abertura da sessão pública deste pregão, conduzida pelo(a) Pregoeiro(a), ocorrerá na data e na hora indicada no preâmbulo deste Edital, no sítio www.gov.br/compras.

11.2. Durante a sessão pública, a comunicação entre o(a) Pregoeiro(a) e as licitantes ocorrerá exclusivamente mediante troca de mensagens, em campo próprio do sistema eletrônico.

11.2.1. Na intercorrência de qualquer dificuldade técnica, a comunicação poderá ser realizada por meio do endereço eletrônico colic@tjam.jus.br, sendo posteriormente publicado no site do TJAM e informado em sessão.

11.3. O sistema ordenará automaticamente as propostas classificadas, sendo que somente estas participarão da fase de lances.

11.4. Iniciada a etapa competitiva, os licitantes deverão encaminhar lances exclusivamente por meio de sistema eletrônico, sendo imediatamente informados do seu recebimento e do valor consignado no registro.

11.5. Os licitantes poderão oferecer lances sucessivos, observando o horário fixado para abertura da sessão e as regras estabelecidas no Edital.

11.6. Durante a sessão pública, as licitantes serão informadas, pelo sistema, em tempo real, do valor do menor lance registrado, vedada a identificação da licitante.

11.7. A licitante somente poderá oferecer valor inferior ao último lance por ela ofertado e registrado pelo sistema, observado o intervalo mínimo entre lances, que incidirá tanto em relação aos lances intermediários quanto em relação ao lance que cobrir a melhor oferta.

11.8. O sistema não aceitará dois ou mais lances iguais e prevalecerá aquele que for recebido e registrado primeiro.

11.9. O procedimento seguirá de acordo com o modo de disputa “aberto”.

11.10. No modo de disputa “aberto”, os licitantes apresentarão lances públicos e sucessivos, com prorrogações.

11.10.1. A etapa de lances da sessão pública terá duração de 10 (dez) minutos e, após isso, será prorrogada automaticamente pelo sistema quando houver lance ofertado nos últimos 2 (dois) minutos do período de duração da sessão pública.

11.10.2. A prorrogação automática da etapa de lances, de que trata o subitem anterior, será de 2 (dois) minutos e ocorrerá sucessivamente sempre que houver lances enviados nesse período de prorrogação, inclusive no caso de lances intermediários.

11.10.3. Não havendo novos lances na forma estabelecida nos itens anteriores, a sessão pública encerrar-se-á automaticamente, e o sistema ordenará e divulgará os lances conforme a ordem final de classificação.

11.11. Encerrada a fase competitiva sem que haja a prorrogação automática pelo sistema, poderá o(a) Pregoeiro(a), assessorado pela equipe de apoio, justificadamente, admitir o reinício da sessão pública de lances, em prol da consecução do melhor preço.

11.12. Após o término dos prazos estabelecidos nos subitens anteriores, o sistema ordenará e divulgará os lances segundo a ordem crescente de valores.

11.13. Os lances apresentados e levados em consideração para efeito de julgamento serão de exclusiva e total responsabilidade do licitante, não lhe cabendo o direito de pleitear qualquer alteração.

11.14. Durante a fase de lances, o(a) Pregoeiro(a) poderá excluir, justificadamente, lance cujo valor seja manifestamente inexequível.

11.15. Se ocorrer a desconexão do(a) Pregoeiro(a) no decorrer da etapa de lances, mas o sistema eletrônico permanecer acessível aos licitantes, os lances continuarão sendo recebidos, sem prejuízo dos atos realizados.

11.16. Quando a desconexão do sistema eletrônico para o(a) Pregoeiro(a) persistir por tempo superior a 10 (dez) minutos, a sessão pública será suspensa e reiniciada somente após decorridas 24 (vinte e quatro horas) da comunicação do fato pelo(a) Pregoeiro(a) aos participantes, no sítio eletrônico utilizado para divulgação.

11.17. Havendo eventual empate entre propostas ou lances, o critério de desempate será aquele previsto no art. 60 da Lei Federal n.º 14.133/2021.

CLÁUSULA DÉCIMA SEGUNDA
DOS BENEFÍCIOS ÀS MICROEMPRESAS, EMPRESAS DE PEQUENO PORTE E EQUIPARADAS

12.1. São consideradas microempresas, empresas de pequeno porte e equiparadas, aquelas definidas nos incisos I e II do caput e § 4° do art. 3° da Lei Complementar Federal n.° 123/2006, em face do que determina o art. 1°, §1° da Lei Estadual n.° 6.269/2023.

12.1.1. Nos termos do art. 34 da Lei n.° 11.488/2007, equipara-se às microempresas e empresas de pequeno porte as sociedades cooperativas, desde que tenham auferido, no ano-calendário anterior, receita bruta até o limite definido no inciso II do caput do art. 3° da Lei Complementar n.° 123/2006, nela incluídos os atos cooperados e não-cooperados.

12.2. Nos termos do art. 4º, §1º, inciso I da Lei nº 14.133, de 2021, não serão aplicados os benefícios e as disposições constantes dos arts. 42 a 49 da Lei Complementar nº 123, de 14 de dezembro de 2006 no caso de licitação para aquisição de bens ou contratação de serviços em geral, ao item cujo valor estimado for superior à receita bruta máxima admitida para fins de enquadramento como empresa de pequeno porte.

CLÁUSULA DÉCIMA TERCEIRA
DA FASE DE JULGAMENTO

13.1. Encerrada a etapa anterior, o(a) Pregoeiro(a) verificará se o licitante classificado em primeiro lugar atende às condições de participação no certame, conforme previsto no art. 14 da Lei Federal n.º 14.133/2021, legislação correlata e no item 5.7 do Edital, especialmente quanto à existência de sanção que impeça a participação no certame ou a futura contratação, mediante a consulta aos seguintes cadastros:

13.1.1. SICAF;

13.1.2. Inscrição no Cadastro de Pessoas Físicas (CPF) ou no Cadastro Nacional de Pessoa Jurídica (CNPJ);

13.1.3. Inscrição no cadastro de contribuintes estadual e/ou municipal, se houver, relativo ao domicílio ou sede do licitante, pertinente ao seu ramo de atividade e compatível com o objeto contratual;

13.1.4. Cadastro Nacional de Empresas Inidôneas e Suspensas - CEIS, mantido pela Controladoria-Geral da União (https://portaldatransparencia.gov.br/sancoes/consulta?cadastro=1&ordenarPor=nomeSancionado&direcao=asc https://www.https://portaldatransparencia.gov.br/sancoes/consulta?cadastro=1&ordenarPor=nomeSancionado&direcao=asc); e

13.1.5. Cadastro Nacional de Empresas Punidas – CNEP, mantido pela Controladoria-Geral da União (https://portaldatransparencia.gov.br/sancoes/consulta?cadastro=2&ordenarPor=nomeSancionado&direcao=asc... tps://portaldatransparencia.gov.br/sancoes/consulta?cadastro=2&ordenarPor=nomeSancionado&direcao=asc).

13.2. Caso atendidas as condições de participação, será iniciado o procedimento de julgamento da proposta.

13.3. Caso o licitante classificado em primeiro lugar tenha se utilizado de algum tratamento favorecido às ME/EPPs, o(a) Pregoeiro(a) verificará se faz jus ao benefício, em conformidade com a Cláusula Décima Segunda deste Edital.

13.4. Verificadas as condições de participação e de utilização do tratamento favorecido, o(a) Pregoeiro(a) examinará a proposta classificada em primeiro lugar quanto à adequação ao objeto e à compatibilidade do preço em relação ao máximo estipulado para contratação neste Edital e em seus anexos.

13.4.1. O(A) Pregoeiro(a) solicitará ao licitante mais bem classificado que, no prazo de 2 (duas) horas, envie a proposta adequada ao último lance ofertado, acompanhada, se for o caso, dos documentos complementares, quando necessários à confirmação daqueles exigidos neste Edital e já apresentados.

13.4.2. Os documentos elencados no item 13.4 deverão ser encaminhados via sistema Compras.gov.br.

13.4.3. Na intercorrência de qualquer dificuldade técnica, o envio mencionado no subitem anterior poderá ser realizado por meio do endereço eletrônico colic@tjam.jus.br, sendo posteriormente publicado no site do TJAM e informado em sessão.

13.4.4. É facultado ao(à) Pregoeiro(a) prorrogar o prazo estabelecido, a partir de solicitação fundamentada feita no chat pelo licitante ou por meio de e-mail à Coordenadoria de Licitação (colic@tjam.jus.br), antes de findo o prazo.

13.5. No caso de bens e serviços em geral, é indício de inexequibilidade das propostas valores inferiores a 50% (cinquenta por cento) do valor orçado pela Administração.

13.5.1. A inexequibilidade, na hipótese de que trata o caput, só será considerada após diligência do agente de contratação ou da comissão de contratação, quando o substituir, que comprove:

a) que o custo do licitante ultrapassa o valor da proposta; e

b) inexistirem custos de oportunidade capazes de justificar o vulto da oferta.

13.6. Se houver indícios de inexequibilidade da proposta de preço, ou em caso da necessidade de esclarecimentos complementares, poderão ser efetuadas diligências, para que a empresa comprove a exequibilidade da proposta.

13.7. Caso o custo global estimado do objeto licitado tenha sido decomposto em seus respectivos custos unitários por meio de Planilha de Custos e Formação de Preços elaborada pela Administração, o licitante classificado em primeiro lugar será convocado para apresentar Planilha por ele elaborada, com os respectivos valores adequados ao valor final da sua proposta, sob pena de não aceitação da proposta.

13.8. Erros no preenchimento da planilha não constituem motivo para a desclassificação da proposta. A planilha poderá ser ajustada pelo fornecedor, no prazo indicado pelo sistema, desde que não haja majoração do preço.

13.8.1. O ajuste de que trata este dispositivo se limita a sanar erros ou falhas que não alterem a substância das propostas.

13.8.2. Considera-se erro no preenchimento da planilha passível de correção a indicação de recolhimento de impostos e contribuições na forma do Simples Nacional, quando não cabível esse regime.

CLÁUSULA DÉCIMA QUARTA
DA NEGOCIAÇÃO

14.1. Definido o resultado do julgamento, o(a) Pregoeiro(a) poderá negociar condições mais vantajosas com o primeiro colocado.

14.1.1. O prazo de negociação oferecido aos licitantes não será inferior a 5 (cinco) minutos.

14.2. A negociação poderá ser feita com os demais licitantes, segundo a ordem de classificação inicialmente estabelecida, quando o primeiro colocado, mesmo após a negociação, for desclassificado em razão de sua proposta permanecer acima do preço máximo definido pela Administração.

14.3. A negociação será realizada por meio do sistema, podendo ser acompanhada pelos demais licitantes, cujo resultado será divulgado a todos os licitantes e anexado aos autos do processo licitatório.

14.4. O(A) Pregoeiro(a) solicitará ao licitante mais bem classificado que, no prazo de 2 (duas) horas, envie a proposta adequada ao valor atualizado após a negociação realizada, acompanhada, se for o caso, dos documentos complementares, quando necessários à confirmação daqueles exigidos neste Edital e já apresentados.

14.4.1. Os documentos elencados no item anterior deverão ser encaminhados na forma dos itens 13.4.1 a 13.4.4, adequando-se ao valor atualizado após a negociação realizada.

CLÁUSULA DÉCIMA QUINTA
DA FASE DE HABILITAÇÃO

15.1. Vencida a etapa anterior, promover-se-á a análise dos documentos para fins de habilitação.

15.2. A habilitação das licitantes será verificada por meio do Sistema de Cadastramento Unificado de Fornecedores (SICAF), bem como de outros sistemas públicos de consulta, e documentação complementar disposta nas Cláusulas seguintes.

15.2.1. No caso da documentação já cadastrada no SICAF estar em desconformidade com o previsto na legislação aplicável no momento da habilitação, ou haja a necessidade de solicitar documentos complementares aos já apresentados, o(a) Pregoeiro(a) deverá comunicar à licitante para que promova a regularização no prazo de 02 (duas) horas.

15.2.2. O referido prazo poderá ser dilatado motivadamente pelo(a) Pregoeiro(a) a depender das circunstâncias ou, havendo justo motivo, mediante solicitação formal de prorrogação por parte da licitante antes do fim do prazo concedido.

15.2.3. Os documentos elencados no item 15.2.1 deverão ser encaminhados via sistema Compras.gov.br.

15.2.4. Na intercorrência de qualquer dificuldade técnica, o envio mencionado no subitem anterior poderá ser realizado por meio do endereço eletrônico colic@tjam.jus.br, sendo posteriormente publicado no site do TJAM e informado em sessão.

15.3. Serão verificadas a Habilitação Jurídica, a Qualificação Econômico-Financeira, a Regularidade Fiscal (Federal, Estadual, Distrital e Municipal) e a Regularidade perante a Justiça do Trabalho.

15.3.1. A comprovação da Habilitação Jurídica será aferida mediante a apresentação de:

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

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

c) No caso de 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;

d) Nos casos de 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;

e) No caso de 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 n.° 77/2020;

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

g) Nos casos de 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;

h) No caso de 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 n.° 5.764/1971;

i) No caso de Agricultor familiar: Declaração de Aptidão ao Pronaf – DAP ou DAP-P válida, ou, ainda, outros documentos definidos pelo órgão regulador;

j) No caso de Produtor Rural: matrícula no Cadastro Específico do INSS – CEI, que comprove a qualificação como produtor rural pessoa física;

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

15.3.2. A comprovação da Qualificação Econômico-Financeira, será aferida mediante a apresentação de:

a) certidão negativa de falência ou recuperação judicial, expedida pelo distribuidor da sede da pessoa jurídica do licitante, com exceção das sociedades cooperativas que, por força de lei, não estão sujeitas à falência;

b) balanço patrimonial dos 2 (dois) últimos exercícios sociais, apresentado na forma da lei, com o cumprimento das seguintes formalidades:

b.1) Indicação do número das páginas e números do livro onde estão inscritos o balanço patrimonial e a Demonstração do Resultado do Exercício (DRE) no Livro Diário, além do acompanhamento do respectivo Termo de Abertura e Termo de Encerramento do mesmo;

b.1.1) Os Termos de Abertura e de Encerramento não serão exigidos:

b.1.1.1) para microempresas, empresas de pequeno porte e equiparadas, conforme definidas nos incisos I e II do caput e § 4° do art. 3° da Lei Complementar Federal n.° 123/2006, em face do que determina o art. 1°, §1° da Lei Estadual n.° 6.269/2023;

b.1.1.2) para as empresas obrigadas a adotar a Escrituração Contábil Digital (ECD), via Sistema Público de Escrituração Digital (SPED), na forma do art. 3° da Instrução Normativa RFB n.° 2.003/2021;

b.2) Assinatura do contador e do titular ou representante legal da empresa no balanço patrimonial, DRE e no recibo de entrega da ECD;

b.3) Prova de registro na Junta Comercial ou Cartório (devidamente carimbado, com etiqueta, chancela da Junta Comercial ou código de registro) ou recibo de entrega do ECD;

b.4) Demonstração da escrituração Contábil/Fiscal/pessoal regular;

b.5) Comprovante de habilitação do profissional, bem como sua situação regular perante o seu Conselho Regional de Contabilidade à época da assinatura do registro na Junta Comercial/Cartório ou da data da entrega do ECD;

b.5.1) Nos casos em que ocorrer a substituição do profissional responsável pela elaboração do balanço patrimonial da empresa, a qualificação do profissional atualmente encarregado será sujeita a avaliação;

b.5.2) Na mesma hipótese do subitem anterior, o profissional atualmente encarregado validará o(s) balanço(s) apresentados, anexando declaração expressa a ser juntado no momento do envio da proposta ajustada.

15.3.3. A comprovação da Regularidade Fiscal (Federal, Estadual, Distrital e Municipal) e Regularidade perante a Justiça do Trabalho, será aferida mediante a apresentação de:

a) prova de inscrição no Cadastro Nacional de Pessoas Jurídicas do Ministério da Fazenda (CNPJ);

b) prova de inscrição no cadastro de contribuintes estadual e/ou municipal, relativo à sede do licitante, pertinente ao seu ramo de atividade e compatível com o objeto contratual;

c) prova de regularidade para com a Fazenda Federal, Estadual e Municipal da sede do licitante ou outra prova equivalente, na forma da lei;

d) prova de regularidade relativa à Seguridade Social e ao Fundo de Garantia por Tempo de Serviço (FGTS), demonstrando situação regular no cumprimento dos encargos sociais instituídos por lei;

e) prova de inexistência de débitos inadimplidos perante a Justiça do Trabalho, mediante a apresentação de certidão negativa.

15.3.4. As licitantes deverão encaminhar a seguinte documentação complementar para verificação da sua Qualificação Técnica:

a) Apresentação de documento declarando ter capacitação técnica para atender a todos os requisitos especificados no Termo de Referência;

b) Declaração de que atende aos requisitos de habilitação e qualificação exigidas;

c) Comprovação de aptidão para o fornecimento de serviços de complexidade tecnológica e operacional similares com o objeto desta contratação, por meio da apresentação de certidões ou atestados, por pessoas jurídicas de direito público ou privado;

d) declaração de Vistoria Técnica ou de que conhece as condições locais para a execução do serviço. (Anexo VII)

15.4. O(A) Pregoeiro(a) poderá, no julgamento da habilitação, sanar erros ou falhas que não alterem a substância dos documentos e sua validade jurídica, mediante decisão fundamentada, registrada em ata e acessível aos licitantes, e lhes atribuirá validade e eficácia para fins de classificação, observado o disposto no art. 55, da Lei Estadual n.° 2.794/2003.

15.5. No que diz respeito à habilitação das microempresas, empresas de pequeno porte e as equiparadas, e caso se aplique, serão seguidas as diretrizes estabelecidas na Cláusula Décima Segunda.

15.6. Todos os documentos emitidos em língua estrangeira deverão ser entregues acompanhados da tradução para língua portuguesa, efetuada por tradutor juramentado, e também devidamente consularizados ou registrados no cartório de títulos e documentos.

15.7. Documentos de procedência estrangeira, mas emitidos em língua portuguesa, também deverão ser apresentados devidamente consularizados ou registrados em cartório de títulos e documentos.

15.8. A entidade que tiver unidade operacional ou de negócios, quer como filial, agência, sucursal ou assemelhada, e que optar por sistema de escrituração descentralizado, deve ter registros contábeis que permitam a identificação das transações de cada uma dessas unidades.

15.9. Se a licitante não atender às exigências de habilitação, se a licitante deixar de enviá-los ou deixar de atender diligência complementar solicitada em sessão, o(a) Pregoeiro(a) examinará a proposta subsequente e assim sucessivamente, na ordem de classificação, até a seleção da proposta que atenda a este Edital.

15.10. Constatado o atendimento às exigências fixadas neste Edital, a licitante será declarada vencedora.

CLÁUSULA DÉCIMA SEXTA
DOS RECURSOS

16.1. Declarada a vencedora, o(a) Pregoeiro(a) abrirá prazo de 10 (dez) minutos, durante o qual qualquer licitante poderá, de forma imediata, em campo próprio do sistema, manifestar sua intenção de recorrer.

16.1.1. A ausência de manifestação imediata do licitante quanto à intenção de recorrer, nos termos do disposto na Cláusula 16.1, importará na decadência desse direito.

16.2. A licitante que manifestou intenção de recurso deverá registrar as razões do recurso, em campo próprio do sistema, no prazo de 03 (três) dias, ficando as demais licitantes, desde logo, intimadas a apresentar contrarrazões, também via sistema, em igual prazo, que começará a correr do término do prazo da recorrente.

16.3. O acolhimento do recurso implicará a invalidação apenas dos atos insuscetíveis de aproveitamento.

16.4. Não serão providos recursos de caráter protelatório, fundada em mera insatisfação da licitante, podendo ainda ser aplicado, supletiva e subsidiariamente, no que couberem, as regras previstas na Lei n.° 13.105/2015.

CLÁUSULA DÉCIMA SÉTIMA
DA ADJUDICAÇÃO E HOMOLOGAÇÃO

17.1. O objeto deste pregão será adjudicado e homologado pela Presidência do Tribunal de Justiça do Amazonas, inclusive quando houver recurso.

CLÁUSULA DÉCIMA OITAVA
DO CONTRATO E DA GARANTIA CONTRATUAL

18.1. Será firmado o contrato com a empresa vencedora, que terá suas cláusulas e condições reguladas pela Lei Federal n.º 14.133/2021, pela Lei Complementar n.° 123/2006, pelo Decreto Estadual n.° 47.133/2023, pelo Decreto Federal n.º 3.555/2000, pela Resolução n.° 64/2023 TJAM, e no que couber pelas demais Cláusulas e condições constantes neste Edital e no Termo de Referência.

18.2. A Divisão de Contratos e Convênios deste Poder convocará a empresa licitante para a assinatura do Termo de Contrato.

18.3. Na hipótese da empresa vencedora não apresentar situação regular ou não comparecer para assinar o Termo de Contrato será convocado outro licitante para celebrar o Contrato, observada a ordem de classificação, e assim sucessivamente, sem prejuízo da aplicação das sanções cabíveis.

18.4. Para a execução do futuro contrato, decorrente desta licitação, **será exigida** prestação de garantia, nos termos da Cláusula DÉCIMA TERCEIRA da Minuta de Contrato (anexo VI).

CLÁUSULA DÉCIMA NONA
DOS PROCEDIMENTOS PARA O REGISTRO DE PREÇOS

19.1. A presente licitação será realizada mediante Sistema de Registro de Preços.

19.1.1. O(s) lance(s) encerrados será(ão) incluído(s) na respectiva Ata de Registro de Preços (ARP), na forma de anexo, o registro dos licitantes que aceitarem cotar os bens com preços iguais aos da licitante vencedora na sequência da classificação do certame.

19.2. A ordem de classificação das licitantes registradas na ARP deverá ser respeitada nas contratações.

19.3. O registro a que se refere a Cláusula 19.1 tem por objetivo a formação de cadastro de reserva no caso de impossibilidade de atendimento pelo primeiro colocado da ARP, nas hipóteses previstas no § 6° do art. 54 c/c os arts. 55 e 56 da Resolução n.° 64/2023 TJAM.

19.4. Se houver mais de uma licitante na situação de que trata a Cláusula 19.1, serão classificados segundo a ordem da última proposta apresentada durante a fase competitiva.

19.5. A habilitação dos fornecedores que comporão o cadastro de reserva a que se refere a Cláusula 19.1 será efetuada, na hipótese prevista na Cláusula 19.8 e quando houver necessidade de contratação de fornecedor remanescente, nas hipóteses previstas no § 6° do art. 54 c/c os arts. 55 e 56 da Resolução n.° 64/2023 TJAM.

19.6. Homologado o resultado da licitação, a COLIC, formalizará a Ata de Registro de Preços com a(s) licitante(s) vencedor(as) do certame e, se for o caso, com as demais classificadas, obedecida à ordem de classificação e os quantitativos propostos.

19.7. A COLIC convocará a(s) empresa(s) a ser(em) registrada(s), que terá(ão) prazo de até 03 (três) dias úteis, contados do recebimento da Ata de Registro de Preços, inclusive por meio eletrônico, para a sua assinatura e reenvio a este Poder, salvo motivo justificado, e devidamente aceito.

19.8. É facultado à administração, quando o convocado não assinar a ata de registro de preços no prazo e condições estabelecidos, convocar as licitantes remanescentes, na ordem de classificação, para fazê-lo em igual prazo e nas mesmas condições propostas pela primeira classificada.

19.9. Como condição para assinatura da Ata de Registro de Preços, bem como para as aquisições dela resultante, a(s) licitante(s) vencedor(as) deverá(ão) manter todas as condições de habilitação, de acordo com inciso XVI, artigo 92 da Lei Federal n.º 14.133/2021.

19.10. A partir da publicação do extrato da Ata de Registro de Preços no Diário da Justiça Eletrônico, a licitante se obriga a cumprir, na sua íntegra, todas as condições estabelecidas, ficando sujeito, às penalidades pelo descumprimento de quaisquer de suas cláusulas.

19.11. O prazo de vigência da Ata de Registro de Preços, contado a partir da publicação do extrato da ata no Portal Nacional de Contratações Públicas e Diário da Justiça Eletrônico - DJE, será de 1 (um) ano, e poderá ser prorrogado, por igual período, desde que comprovado que as condições e o preço permanecem vantajosos.

19.12. Será realizada periódica pesquisa de mercado para comprovação da vantajosidade da ARP, de acordo com o art. 84, da Lei Federal n.° 14.133/2021.

19.13. As hipóteses de cancelamento do registro do fornecedor, dos preços registrados e da Ata de Registro de Preços, estão regulamentadas no § 6° do art. 54 c/c os arts. 55 e 56 da Resolução n.° 64/2023 TJAM.

19.14. Será permitida a adesão à Ata de Registro de Preços decorrente deste certame, por órgãos não participantes.

19.14.1. O quantitativo total registrado deverá ser utilizado pelo órgão gerenciador e órgãos participantes de maneira remanejada, de tal forma que o total aderido (gestor e participantes) não ultrapasse o quantitativo total registrado.

19.15. O quantitativo decorrente das adesões à Ata de Registro de Preços por órgãos ou entidades não participantes não poderá exceder, na totalidade, ao dobro do quantitativo de cada item registrado na Ata de Registro de Preços para o órgão gerenciador e órgãos participantes, independente do número de órgãos não participantes que aderirem.

19.15.1. As aquisições ou as contratações adicionais de que trata a Cláusula 19.15 não poderão exceder, por órgão ou entidade, a 50% (cinquenta por cento) dos quantitativos dos itens do instrumento convocatório e registrados na ata de registro de preços para o órgão gerenciador e para os órgãos participantes.

CLÁUSULA VIGÉSIMA
DA NOTA DE EMPENHO

20.1. O Tribunal de Justiça do Amazonas convocará a licitante vencedora para, no prazo máximo de 05 (cinco) dias úteis, retirar a Nota de Empenho ou a encaminhará via e-mail, devendo, nesse caso, ser acusado seu recebimento no mesmo prazo, sob pena de decair o direito do fornecimento ou da prestação do serviço sem prejuízo das sanções legais cabíveis.

20.2. O prazo da convocação poderá ser prorrogado uma vez, por igual período, quando solicitado pela licitante vencedora, desde que ocorra motivo justificado e aceito pelo Tribunal de Justiça do Amazonas.

20.3. Os acréscimos nos quantitativos fixados pela Ata de Registro de Preços deverão observar o disposto no art. 125, da Lei Federal n.° 14.133/2021.

20.4. A licitante vencedora fica obrigada a aceitar, nas mesmas condições das propostas, os acréscimos ou supressões que porventura se fizerem necessários em até 25% (vinte e cinco por cento) do valor inicial atualizado do contrato que se fizerem nas obras, nos serviços ou nas compras, e, no caso de reforma de edifício ou de equipamento, o limite para os acréscimos será de 50% (cinquenta por cento), nos termos do art. 125, da Lei Federal n.° 14.133/2021.

CLÁUSULA VIGÉSIMA PRIMEIRA
DO PRAZO E DAS CONDIÇÕES DE FORNECIMENTO OU DA PRESTAÇÃO DOS SERVIÇOS

21.1. O objeto desta licitação deverá ser executado de acordo com as especificações e as condições, e nos prazos definidos no Termo de Referência, no Termo de Contrato, na Ata de Registro de Preços e na proposta de preço.

21.2. As despesas com seguros, transporte, fretes, tributos, encargos trabalhistas e previdenciários e demais despesas envolvidas no fornecimento do objeto ou na prestação do serviço correrão por conta da empresa contratada.

21.3. Após o fornecimento do objeto ou a prestação do serviço pela empresa contratada, o Tribunal de Justiça do Amazonas verificará o cumprimento das exigências constantes no Termo de Referência, no Termo de Contrato, na Ata de Registro de Preços e na proposta de preços. As verificações serão realizadas pela Secretaria de Tecnologia da Informação e Comunicação deste Poder.

21.4. No caso de constatada divergência entre o objeto entregue ou o serviço prestado com as especificações ou as condições definidas no Termo de Referência, no Termo de Contrato, na Ata de Registro de Preços e/ou na Proposta de Preços, o licitante contratado deverá efetuar a troca e/ou a correção nos prazos estabelecidos no Termo de Referência, no Termo de Contrato e na Ata de Registro de Preços, contados a partir da comunicação da recusa.

21.5. Caso a licitante contratada não entregue o objeto ou preste o serviço nas condições estabelecidas neste Edital, deverá a Secretaria de Tecnologia da Informação e Comunicação deste Poder comunicar, de forma oficial e imediata, **à Presidência do Tribunal de Justiça do Amazonas** para as providências cabíveis.

CLÁUSULA VIGÉSIMA SEGUNDA
DAS OBRIGAÇÕES DO CONTRATANTE E DA CONTRATADA

22.1. Caberá ao Tribunal de Justiça do Amazonas, sem prejuízo das demais obrigações e responsabilidades constantes neste Edital, no Termo de Referência,no Termo de Contrato e na Ata de Registro de Preços:

22.1.1. Acompanhar e fiscalizar o contrato por 1 (um) ou mais fiscais do contrato, representantes da Administração especialmente designados conforme requisitos estabelecidos no art. 7.º da Lei Federal n.º 14.133/2021, ou pelos respectivos substitutos, permitida a contratação de terceiros para assisti-los e subsidiá-los com informações pertinentes a essa atribuição;

22.1.2. Proporcionar todas as condições necessárias, para que o credenciado contratado possa cumprir o estabelecido no contrato;

22.1.3. Prestar todas as informações e esclarecimentos necessários para a fiel execução contratual, que venham a ser solicitados pelo contratado;

22.1.4. Fornecer os meios necessários à execução, pelo contratado, dos serviços objeto do contrato;

22.1.5. Garantir o acesso e a permanência dos empregados do contratado nas dependências do contratante, quando necessário para a execução do objeto do contrato;

22.1.6. Efetuar os pagamentos pelos serviços prestados, dentro dos prazos previstos no contrato, no Edital de credenciamento e na legislação.

22.2. Caberá à empresa licitante contratada, sem prejuízo das demais obrigações e responsabilidades constantes neste Edital, no Termo de Referência, no Termo de Contrato e na Ata de Registro de Preços:

22.2.1. Executar o objeto desta licitação de acordo com as especificações e/ou condições constantes neste Edital, no Termo de Referência, no Termo de Contrato e na Ata de Registro de Preços;

22.2.2. Manter preposto para representá-lo durante a execução do contrato;

22.2.3. Responder, em relação aos seus empregados, por todas as despesas decorrentes da execução do objeto desta licitação, tais como: salários, seguros de acidentes, taxas, impostos e contribuições,

indenizações, vales refeição, vales transporte e outras que porventura sejam estabelecidas em convenções ou acordos coletivos, bem como as criadas e exigidas pelo Poder Público;

22.2.4. Ser responsável pelos danos causados ao Tribunal de Justiça do Amazonas ou a terceiros, decorrentes de sua culpa ou dolo quando da execução do objeto desta licitação, não excluindo ou reduzindo essa responsabilidade em virtude da fiscalização ou do acompanhamento pela contratante;

22.2.5. Solicitar a repactuação do contrato sempre que houver variação do equilíbrio econômico-financeiro, oferecendo para tanto os elementos e justificativas que fundamentam o pedido;

22.2.6. Solicitar a revisão da Ata de Registro de Preço, oferecendo para tanto os elementos e justificativas que fundamentam o pedido;

22.2.7. Comunicar por escrito ao Tribunal de Justiça do Amazonas qualquer anormalidade na execução do objeto desta licitação;

22.2.8. Observar as normas legais de segurança a que está sujeita a execução do objeto desta licitação;

22.2.9. Manter, durante toda a execução do contrato, em compatibilidade com obrigações assumidas, todas as condições de habilitação e qualificação exigidas nesta licitação.

CLÁUSULA VIGÉSIMA TERCEIRA
DAS OBRIGAÇÕES SOCIAIS, COMERCIAIS E FISCAIS

23.1. À empresa licitante contratada caberá, ainda:

23.1.1. Assumir a responsabilidade por todos os encargos previdenciários e obrigações sociais previstos na legislação social e trabalhista em vigor, obrigando-se a saldá-los na época própria, vez que os seus empregados não manterão nenhum vínculo empregatício com o Tribunal de Justiça do Amazonas;

23.1.2. Assumir, também, a responsabilidade por todas as providências e as obrigações estabelecidas na legislação específica de acidentes de trabalho, quando, em ocorrência da espécie, forem vítimas os seus empregados durante a execução do objeto desta licitação, ainda que acontecidos nas dependências do Tribunal de Justiça do Amazonas;

23.1.3. Assumir todos os encargos de demanda trabalhista, cível ou penal, relacionados a esse processo licitatório e ao respectivo contrato;

23.1.4. Assumir, ainda, a responsabilidade pelos encargos fiscais e comerciais resultantes da adjudicação desta licitação.

CLÁUSULA VIGÉSIMA QUARTA
DO PAGAMENTO

24.1. O pagamento será efetuado pela Secretaria de Orçamento e Finanças do TJAM, de acordo com a legislação vigente, após recebimento da Nota Fiscal ou Fatura, conferida e atestada pelo setor requisitante, comprovando a prestação do serviço de maneira satisfatória.

24.2. Poderão ser solicitados para o pagamento: Nota Fiscal, de acordo com a legislação vigente, provas de regularidade perante o Fundo de Garantia por Tempo de Serviço (Certidão de Regularidade do FGTS), perante o Instituto Nacional do Seguro Social (Certidão Negativa de Débito do INSS), perante a Fazenda Federal (Certidão Conjunta Negativa de Débitos relativos aos TRIBUTOS FEDERAIS e à DÍVIDA ATIVA DA UNIÃO), perante a Fazenda Estadual (Certidão Negativa de DÉBITO DO ESTADO), perante a Fazenda Municipal (Certidão Negativa de DÉBITO MUNICIPAL), e perante a Justiça do Trabalho.

24.3. Constatada qualquer incorreção na Nota Fiscal, de acordo com a legislação vigente, bem como qualquer outra circunstância que desaconselhe o seu pagamento, o prazo para pagamento fluirá a partir da respectiva regularização.

24.4. O pagamento observará o disposto na Cláusula OITAVA da Minuta de Contrato (anexo VI).

CLÁUSULA VIGÉSIMA QUINTA
DA EXTINÇÃO DO CONTRATO ou DA ATA DE REGISTRO DE PREÇOS

25.1. A inexecução total ou parcial do contrato enseja a sua rescisão, com as consequências previstas neste instrumento e na legislação pertinente à matéria.

25.2. Constituem motivo para rescisão do contrato:

25.2.1. O não cumprimento de cláusulas, especificações, condições ou prazos previstos neste instrumento e seus anexos;

25.2.2. O cumprimento irregular de cláusulas, especificações, condições ou prazos previstos neste instrumento e seus anexos;

25.2.3. A lentidão do seu cumprimento que impossibilite a conclusão do fornecimento ou da prestação do serviço nos prazos estipulados;

25.2.4. O atraso injustificado no início do fornecimento ou da prestação do serviço;

25.2.5. A subcontratação total ou parcial do seu objeto, nos termos do item 5.8 deste Edital;

25.2.6. O desatendimento das determinações regulares da autoridade designada para acompanhar e fiscalizar a contratação, assim como as de seus superiores;

25.2.7. O cometimento reiterado de faltas no fornecimento do objeto;

25.2.8. A decretação de falência ou a instauração de insolvência civil;

25.2.9. A dissolução da sociedade ou o falecimento do contratado;

25.2.10. A alteração social ou a modificação da finalidade ou da estrutura da empresa, que prejudique o fornecimento do objeto;

25.2.11. Razões de interesse público, de alta relevância e amplo conhecimento, justificadas e determinadas pela autoridade competente e exaradas no processo administrativo a que se refere o contrato;

25.2.12. A supressão da contratação, por parte da Administração, acarretando modificação do valor inicial do contrato além dos limites estabelecidos na legislação vigente;

25.2.13. A ocorrência de caso fortuito ou de força maior, regularmente comprovada, impeditiva da execução do contrato.

25.2.14. Descumprimento do disposto no inciso VI do art. 68 da Lei Federal n.° 14.133/21, sem prejuízo das sanções penais cabíveis;

25.2.15. Outras ocorrências previstas na legislação pertinente à matéria.

25.3. Os casos de rescisão contratual serão formalmente motivados nos autos do processo, assegurado o contraditório e a ampla defesa.

25.4. A rescisão do contrato poderá ser:

25.4.1. Determinada por ato unilateral e escrito da Administração, nos casos previstos na legislação pertinente;

25.4.2. Amigável, por acordo entre as partes, reduzida a termo no processo da licitação, desde que haja conveniência para a Administração;

25.4.3. Judicial, nos termos da legislação.

25.4.1.1. A rescisão administrativa ou amigável deverá ser precedida de autorização escrita e fundamentada da autoridade competente.

25.4.1.2. Quando a rescisão ocorrer com base nos subitens 25.2.11 a 25.2.13 do item 25.2, sem que haja culpa do contratado, será este ressarcido dos prejuízos regularmente comprovados que houver sofrido, nos termos da lei.

25.5. A rescisão contratual observará a legislação pertinente e em especial a Lei Federal n.° 14.133/2021 e suas alterações.

25.6. A rescisão contratual relativa a execução do objeto desta licitação observará o disposto na Cláusula DÉCIMA SÉTIMA da Minuta de Contrato (anexo VI).

CLÁUSULA VIGÉSIMA SEXTA
DA INEXECUÇÃO

26.1. Pelo descumprimento total ou parcial das obrigações assumidas e pela verificação de quaisquer situações previstas nos artigos 155 e 137, da Lei Federal n.º 14.133/2021, a Administração poderá, resguardados os procedimentos legais pertinentes, aplicar as sanções previstas na cláusula subsequente.

CLÁUSULA VIGÉSIMA SÉTIMA
DAS INFRAÇÕES ADMINISTRATIVAS E SANÇÕES

27.1. Comete infração administrativa, nos termos da lei, o licitante que, com dolo ou culpa:

27.1.1. Deixar de entregar a documentação exigida para o certame ou não entregar qualquer documento que tenha sido solicitado pelo(a) Pregoeiro(a) durante o certame;

27.1.2. Salvo em decorrência de fato superveniente devidamente justificado, não mantiver a proposta em especial quando:

a) não enviar a proposta adequada ao último lance ofertado ou após a negociação;

b) recusar-se a enviar o detalhamento da proposta quando exigível;

c) pedir para ser desclassificado quando encerrada a etapa competitiva; ou

d) deixar de apresentar amostra, quando for solicitado;

e) apresentar proposta ou amostra, quando for solicitado, em desacordo com as especificações do Edital;

27.1.3. Não celebrar o contrato ou não entregar a documentação exigida para a contratação, quando convocado dentro do prazo de validade de sua proposta;

a) recusar-se, sem justificativa, a assinar o contrato ou a ata de registro de preço, ou a aceitar ou retirar o instrumento equivalente no prazo estabelecido pela Administração;

27.1.4. Apresentar declaração ou documentação falsa exigida para o certame ou prestar declaração falsa durante a licitação;

27.1.5. Fraudar a licitação;

27.1.6. Comportar-se de modo inidôneo ou cometer fraude de qualquer natureza, em especial quando:

a) agir em conluio ou em desconformidade com a lei;

b) induzir deliberadamente a erro no julgamento;

c) apresentar amostra, quando for solicitado, falsificada ou deteriorada;

27.1.7. Praticar atos ilícitos com vistas a frustrar os objetivos da licitação;

27.1.8. Praticar ato lesivo previsto no art. 5º da Lei n.º 12.846/2013.

27.2. Com fulcro na Lei Federal n.º 14.133/2021, a Administração poderá, garantida a prévia defesa, aplicar aos licitantes e/ou adjudicatários as seguintes sanções, sem prejuízo das responsabilidades civil e criminal:

27.2.1. Advertência;

27.2.2. Multa;

27.2.3. Impedimento de licitar e contratar; e

27.2.4. Declaração de inidoneidade para licitar ou contratar, enquanto perdurarem os motivos determinantes da punição ou até que seja promovida sua reabilitação perante a própria autoridade que aplicou a penalidade.

27.3. Na instrução da aplicação das sanções administrativas devem ser observados os princípios do contraditório e da ampla defesa, considerando, ainda:

I - a natureza e a gravidade da infração cometida;

II - as peculiaridades do caso concreto;

III - os danos causados ao Tribunal;

IV - a implantação ou o aperfeiçoamento de programa de integridade, conforme normas e orientações dos órgãos de controle;

V - as circunstâncias agravantes ou atenuantes;

VI - o custo e benefício da instrução do processo em relação à sanção a ser aplicada.

Parágrafo único. A pena-base deve ser fixada levando-se em consideração as circunstâncias listadas nos incisos I a IV do caput deste artigo; em seguida serão aplicadas as circunstâncias agravantes e atenuantes, respeitando-se os limites mínimo e máximo das penas previstas nos artigos 23 e 24 do Anexo VIII da Resolução n.° 64/2023 TJAM.

27.4. A aplicação das sanções previstas neste Edital não exclui, em hipótese alguma, a obrigação de reparação integral dos danos causados.

27.5. O regramento para a instauração e instrução dos processos administrativos sancionatórios e para a definição da dosimetria da aplicação da pena decorrentes da prática de condutas previstas no art. 155 da Lei Federal n.º 14.133/2021, encontra-se estabelecido no Anexo VIII da Resolução n.° 64/2023 TJAM.

27.6. As penalidades aplicadas serão obrigatoriamente divulgadas no Diário da Justiça Eletrônico, no site do Tribunal de Justiça do Amazonas e registradas no Sistema de Cadastramento Unificado de Fornecedores (SICAF).

CLÁUSULA VIGÉSIMA OITAVA
DAS DISPOSIÇÕES GERAIS

28.1. Será divulgada ata da sessão pública ou documento equivalente no sistema eletrônico e no site do Tribunal de Justiça do Amazonas.

28.2. A critério do Tribunal de Justiça do Amazonas, a presente licitação poderá ser:

28.2.1. Adiada, por conveniência do Tribunal de Justiça do Amazonas, desde que devidamente justificada;

28.2.2. Revogada, a juízo do Tribunal de Justiça do Amazonas, se considerada inoportuna ou inconveniente ao interesse público, decorrente de fato superveniente devidamente comprovado, pertinente e suficiente para justificar tal conduta;

28.2.3. Anulada, de ofício ou mediante provocação de terceiros, sempre que presente ilegalidade insanável, mediante parecer escrito onde indicará expressamente os atos com vícios insanáveis, tornando sem efeito todos os subsequentes que deles dependam, e dará ensejo à apuração de responsabilidade de quem lhes tenha dado causa.

28.3. A anulação do procedimento licitatório induz a do contrato.

28.4. Não havendo expediente ou ocorrendo qualquer fato superveniente que impeça a realização do certame na data marcada, a sessão será automaticamente transferida para o primeiro dia útil subsequente, no mesmo horário anteriormente estabelecido, desde que não haja comunicação em contrário, pelo(a) Pregoeiro(a).

28.5. A participação nesta licitação implica na aceitação plena e irrevogável das normas constantes neste presente ato de convocação, independentemente de declaração expressa.

28.6. É vedada a manutenção, aditamento ou prorrogação de contrato de prestação de serviços com empresa que venha a contratar empregados que sejam cônjuges, companheiros ou parentes em linha reta, colateral ou por afinidade, até o terceiro grau, inclusive, de ocupantes de cargos de direção e de assessoramento, de membros ou juízes vinculados ao do Tribunal de Justiça do Amazonas.

28.7. É vedada, ainda a manutenção, aditamento ou prorrogação de contrato de prestação de serviços com empresa que tenha entre seus empregados colocados à disposição do Tribunal de Justiça do Amazonas para o exercício de funções de chefia, pessoas que incidam na vedação dos arts. 1º e 2º da Resolução nº 156/2012 CNJ, em atendimento ao disposto no art. 4º da Resolução supracitada.

28.8. Na hipótese de não constar prazo nos documentos exigidos para a participação nesta licitação, este Órgão aceitará como válidos os expedidos em até 90 (noventa) dias imediatamente anteriores à data de abertura da licitação, com exceção daqueles cuja validade seja indeterminada.

28.9. No caso de posteriores alterações das Normas Regulamentadoras (NRs) da Associação Brasileira de Normas Técnicas (ABNT) exigidas neste instrumento convocatório e seus anexos, serão consideradas para todos os efeitos cabíveis as NRs vigentes e atualizadas.

28.10. Quando houver indicação de marca, no Termo de Referência ou em qualquer dos anexos deste Edital, fica admitida a utilização de marcas similares com qualidade equivalente ou superior.

28.11. Todas as referências de tempo no Edital, no aviso e durante a sessão pública observarão o horário de Brasília - DF.

28.12. A homologação do resultado desta licitação não implicará direito à contratação.

28.13. As normas disciplinadoras da licitação serão sempre interpretadas em favor da ampliação da disputa entre os interessados, desde que não comprometam o interesse da Administração, o princípio da isonomia, a finalidade e a segurança da contratação.

28.14. Os licitantes assumem todos os custos de preparação e apresentação de suas propostas e a Administração não será, em nenhum caso, responsável por esses custos, independentemente da condução ou do resultado do processo licitatório.

28.15. Na contagem dos prazos estabelecidos neste Edital e seus Anexos, excluir-se-á o dia do início e incluir-se-á o do vencimento, considerando-se o expediente normal deste Órgão, de segunda a sexta-feira, das 8 às 14 horas (horário de Manaus), salvo expressa disposição em contrário.

28.16. O desatendimento de exigências formais não essenciais não importará o afastamento do licitante, desde que seja possível o aproveitamento do ato, observados os princípios da isonomia e do interesse público.

28.17. Em caso de divergência entre disposições deste Edital e de seus anexos ou demais peças que compõem o processo, prevalecerá as deste Edital.

28.18. O(A) Pregoeiro(a) ou autoridade superior poderão promover diligências destinadas a elucidar ou complementar a instrução do processo, em qualquer fase da licitação, fixando prazos para atendimento.

28.19. O(A) Pregoeiro(a) poderá solicitar parecer de técnicos pertencentes ao quadro de pessoal do Tribunal de Justiça do Amazonas, ou ainda, de pessoas físicas ou jurídicas, estranhas a ele, com notórios conhecimentos na matéria em análise, para orientar suas decisões.

28.20. O Edital e seus anexos estão disponíveis, na íntegra, no Portal Nacional de Contratações Públicas (PNCP) e endereço eletrônico https://www.tjam.jus.br/index.php/documentos-licitacao/editais-avisos-erratas-e-docs

28.21. Os casos omissos serão dirimidos pela Presidência do Tribunal de Justiça do Amazonas.

CLÁUSULA VIGÉSIMA NONA
DOS ANEXOS

29.1. São partes integrantes deste Edital os seguintes anexos:

29.1.1. Declaração conjunta de ciência e concordância com as condições contidas no Edital, de cumprimento das condições de habilitação, de inexistência de impedimento legal para licitar ou contratar com a Administração Pública e de cumprimento ao disposto no inciso XXXIII do art. 7º da CF e no Inciso VI do art. 68 da Lei Federal n.º 14.133/2021 (Anexo I);

29.1.2. Declaração de elaboração independente de proposta (Anexo II);

29.1.3. Formulário proposta de preços (Anexo III);

29.1.4. Minuta da Ata de Registro de Preços (Anexo IV);

29.1.5. Termo de Referência (Anexo V);

29.1.5.1. Apêndice do Anexo V - Estudo Técnico Preliminar;

29.1.6. Minuta de Termo de Contrato (Anexo VI);

29.1.7. Modelo de Declaração de Vistoria (Anexo VII).

CLÁUSULA TRIGÉSIMA
DO FORO

30.1. Fica eleito o foro da comarca de Manaus, capital do Estado do Amazonas, para dirimir quaisquer dúvidas decorrentes deste edital com exclusão de qualquer outro, por mais privilegiado que seja.

Manaus/AM, 16 de agosto de 2024.

Desembargadora NÉLIA CAMINHA JORGE

Presidente do Tribunal de Justiça do Amazonas

PREGÃO ELETRÔNICO/SRP N.º 40/2024-TJAM

ANEXO I – Modelo de declaração conjunta de cumprimento das condições de habilitação e de inexistência de impedimento legal para licitar ou contratar com a Administração Pública.

(nome da empresa) _____, inscrito(a) no CNPJ n°. _____, por intermédio de seu representante legal o(a) Sr. (a)_____, portador(a) da Carteira de Identidade nº..... e do CPF nº ....., **DECLARA**:

1) que está ciente e concorda com as condições contidas no edital e seus anexos, e que cumpre plenamente os requisitos de habilitação definidos no edital;

2) que até a presente data inexistem fatos impeditivos para sua habilitação no presente processo licitatório, ciente da obrigatoriedade de declarar ocorrências posteriores;

3) que não emprega menor de 18 (dezoito) anos em trabalho noturno, perigoso ou insalubre e não emprega menor de 16 (dezesseis) anos, salvo menor, a partir de 14 (quatorze) anos, na condição de aprendiz, nos termos do inciso XXXIII do art. 7º da Constituição Federal.

Manaus, XX de XXXXX de 202X.

_____

carimbo (ou nome legível) e assinatura

PREGÃO ELETRÔNICO/SRP N.º 40/2024-TJAM

ANEXO II – Modelo de declaração de elaboração independente de proposta

[IDENTIFICAÇÃO COMPLETA DO REPRESENTANTE DO LICITANTE], como representante devidamente constituído de [IDENTIFICAÇÃO COMPLETA DO LICITANTE OU DO CONSÓRCIO] doravante denominado [Licitante/Consórcio], em atendimento ao disposto no edital do Pregão Eletrônico nº. XXX/202X, declara, sob as penas da lei, em especial o art. 299 do Código Penal Brasileiro, que:

a) a proposta anexa foi elaborada de maneira independente [pelo Licitante/Consórcio], e que o conteúdo da proposta anexa não foi, no todo ou em parte, direta ou indiretamente, informado a, discutido com ou recebido de qualquer outro participante potencial ou de fato do Pregão Eletrônico nº. XXX/202X, por qualquer meio ou por qualquer pessoa;

b) a intenção de apresentar a proposta anexa não foi informada a, discutido com ou recebido de qualquer outro participante potencial ou de fato do Pregão Eletrônico nº. XXX/202X, por qualquer meio ou por qualquer pessoa;

c) que não tentou, por qualquer meio ou qualquer pessoa, influir na decisão de qualquer outro participante potencial ou de fato do Pregão Eletrônico nº. XXX/202X quanto a participar ou não da referida licitação;

d) que o conteúdo da proposta anexa não será, no todo ou em parte, direta ou indiretamente, comunicado a ou discutido com qualquer outro participante potencial ou de fato do Pregão Eletrônico nº. XXX/202X antes da adjudicação do objeto da referida licitação;

e) que o conteúdo da proposta anexa não foi, no todo ou em parte, direta ou indiretamente, informado a, discutido com ou recebido de qualquer integrante do Tribunal de Justiça do Amazonas antes da abertura oficial das propostas; e

f) que está plenamente ciente do teor e da extensão desta declaração e que detém plenos poderes e informações para firmá-la.

Manaus, XX de XXXXX de 202X.

_____

carimbo (ou nome legível) e assinatura

PREGÃO ELETRÔNICO/SRP N.º 40/2024-TJAM

ANEXO III – Formulário de Proposta de Preços

RAZÃO SOCIAL:		
CNPJ:		**TELEFONE (S):**
E-MAIL:		
ENDEREÇO:		
BANCO:	**AGÊNCIA:**	**CONTA CORRENTE:**

GRUPO OU LOTE

ITEM	DESCRIÇÃO	UNIDADE	QUANTIDADE	VALOR TOTAL (R$)
VALOR TOTAL (R$)				

Valor total por extenso da Proposta de Preços.

Validade da proposta: 60 (sessenta) dias.

Observação: Estão inclusos nos preços supramencionados todos os custos diretos e indiretos, inclusive de embalagens, transportes ou fretes, e ainda os resultantes da incidência de quaisquer tributos, contribuições ou obrigações decorrentes da legislação trabalhista, fiscal e previdenciária a que estiver sujeito.

Manaus, XX de XXXXXXXX de 202X.

_____

carimbo (ou nome legível) e assinatura

do Representante legal

PREGÃO ELETRÔNICO/SRP N.º 40/2024-TJAM
ANEXO IV – Minuta da ATA DE REGISTRO DE PREÇOS (ARP) Nº. XXX/202X
Vinculada ao Pregão Eletrônico para Registro de Preços nº. XXX/202X

Aos XXXXX dias do mês de XXXXXXXX do ano de 202X, o Estado do Amazonas, por intermédio do **Tribunal de Justiça do Estado do Amazonas**, situado à Av. André Araújo, s/n.°, Aleixo – Manaus/AM, inscrito no CNPJ nº. 04.812.509/0001-90, neste ato representado pela Presidente do Tribunal de Justiça do Estado do Amazonas, Excelentíssima Desembargadora **Nélia Caminha Jorge**, institui a **Ata de Registro de Preços (ARP) nº. XXX/202X**, nos termos da Lei Federal n.º 14.133/2021, da Lei Complementar n.° 123/2006, do Decreto Estadual n.° 47.133/2023, do Decreto Federal n.º 3.555/2000, da Resolução n.° 64/2023 TJAM, decorrente da licitação na modalidade de **Pregão Eletrônico para Registro de Preços nº. XXX/202X – TJAM**, conforme **Processo Administrativo nº. XXXX/20XX**, a qual se constitui em documento vinculativo e obrigacional às partes, obedecendo as condições descritas no Edital correspondente e seus anexos, conforme segue:

CLÁUSULA PRIMEIRA
DO OBJETO

1.1. O(s) preço(s), a(s) quantidade(s) e as especificações do(s) material(is) registrado(s) nesta Ata de Registro de Preços, bem como as respectivas empresas licitantes vencedoras – empresas registradas nesta ARP –, encontra(m)-se indicado(s) na(s) tabela(s) abaixo:

ITEM	DESCRIÇÃO	MARCA/ MODELO/ FABRICANTE	UNIDADE	QUANTIDADE	QUANTIDADE MÍNIMA POR CONTRATAÇÃO	VALOR UNITÁRIO (R$)
EMPRESA:						
CNPJ:				**TELEFONE(S):**		
E-MAIL:						
ENDEREÇO:						
REPRESENTANTE LEGAL:						
RG:			**CPF:**			

CLÁUSULA SEGUNDA
DAS CONDIÇÕES DE FORNECIMENTO OU DA PRESTAÇÃO DE SERVIÇOS

2.1. No quadro acima, é apresentado o quantitativo estimado do objeto da licitação, o qual será adquirido de acordo com a necessidade e conveniência do Tribunal de Justiça do Amazonas, mediante solicitação de fornecimento de materiais ou prestação de serviços e emissão da respectiva Nota de Empenho.

2.2. O Tribunal de Justiça do Amazonas convocará a empresa registrada para, no prazo máximo de **05 (cinco) dias úteis**, retirar a Nota de Empenho ou a encaminhará via e-mail, devendo, nesse caso, ser acusado seu recebimento no mesmo prazo, sob pena de decair o direito da prestação do serviço, sem prejuízo das sanções legais cabíveis.

2.3. O objeto desta licitação deverá ser **executado** de acordo com as especificações e nos prazos definidos no Termo de Referência do Edital do Pregão Eletrônico nº. XXX/202X – TJAM.

2.4. As despesas com seguros, transporte, fretes, tributos, encargos trabalhistas e previdenciários e demais despesas envolvidas no fornecimento do objeto ou na prestação do serviço correrão por conta da empresa registrada.

2.5. Após o fornecimento do objeto ou a prestação do serviço da licitação pela empresa registrada, o Tribunal de Justiça do Amazonas os submeterá às verificações quanto às especificações e condições estabelecidas no Termo de Referência do Edital do Pregão Eletrônico nº. XXX/20XX - TJAM e na proposta de preços. As verificações serão realizadas pela Secretaria de Tecnologia da Informação e Comunicação deste Poder, no prazo máximo de **30 (trinta) dias úteis**, procedendo-se desta forma o recebimento definitivo.

2.6. No caso de constatação de divergência entre o objeto entregue ou serviço prestado com as especificações no Termo de Referência do Edital do Pregão Eletrônico nº. XXX/202X - TJAM e/ou na proposta de preços, a empresa registrada deverá efetuar a troca dos mesmos no prazo máximo de **10 (dez) dias úteis,** contados a partir da comunicação da recusa.

2.7. Caso a empresa registrada não entregue o objeto ou preste o serviço nas condições estabelecidas no Termo de Referência do Edital do Pregão Eletrônico nº. XXX/202X - TJAM, deverá a Secretaria de Tecnologia da Informação e Comunicação deste Poder comunicar de maneira formal e imediata, à Presidência do Tribunal de Justiça do Amazonas para as providências cabíveis.

2.8. A inobservância dos prazos dispostos nesta cláusula pela empresa registrada a sujeitará às sanções legais cabíveis.

2.9. Quando por fato superveniente, excepcional, estranho à vontade das partes não for possível o cumprimento do prazo de entrega, a empresa registrada deverá, anteriormente ao término dos prazos estipulados neste instrumento, encaminhar documento com justificativas pelo atraso, comprovadamente, requerendo a extensão do prazo, devidamente fundamentado, para análise por parte do Tribunal de Justiça do Amazonas.

2.10. Quanto aos acréscimos nas quantidades de que trata o quadro da Cláusula Primeira, dever-se-á observar o disposto no artigo 125 da Lei Federal n.º 14.133/2021.

CLÁUSULA TERCEIRA
DA VALIDADE DOS PREÇOS

3.1 – A presente Ata de Registro de Preços terá a validade de **12 (doze) meses**, contados a partir da data de sua assinatura.

3.2 – Durante o prazo de validade desta Ata de Registro de Preço, o Tribunal de Justiça do Amazonas não será obrigado a firmar as contratações que dela poderão advir, facultando-se a realização de licitação específica para a contratação pretendida, sendo assegurado ao beneficiário do registro, preferência em igualdade de condições.

CLÁUSULA QUARTA
DA UTILIZAÇÃO DA ATA DE REGISTRO DE PREÇOS POR ÓRGÃOS NÃO PARTICIPANTES – <u>“CARONA”</u>

4.1. A presente licitação será realizada mediante Sistema de Registro de Preços.

4.1.1. O(s) lance(s) encerrados será(ão) incluído(s) na respectiva Ata de Registro de Preços (ARP), na forma de anexo, o registro dos licitantes que aceitarem cotar os bens com preços iguais aos da licitante vencedora na sequência da classificação do certame.

4.2. A ordem de classificação das licitantes registradas na ARP deverá ser respeitada nas contratações.

4.3. O registro a que se refere a Cláusula 4.1 tem por objetivo a formação de cadastro de reserva no caso de impossibilidade de atendimento pelo primeiro colocado da ARP, nas hipóteses previstas no § 6° do art. 54 c/c os arts. 55 e 56 da Resolução n.° 64/2023 TJAM.

4.4. Se houver mais de uma licitante na situação de que trata a Cláusula 4.1, serão classificados segundo a ordem da última proposta apresentada durante a fase competitiva.

4.5. A habilitação dos fornecedores que comporão o cadastro de reserva a que se refere a Cláusula 4.1 será efetuada, na hipótese prevista na Cláusula 4.8 e quando houver necessidade de contratação de fornecedor remanescente, nas hipóteses previstas no § 6° do art. 54 c/c os arts. 55 e 56 da Resolução n.° 64/2023 TJAM.

4.6. Homologado o resultado da licitação, a COLIC, formalizará a Ata de Registro de Preços com a(s) licitante(s) vencedor(as) do certame e, se for o caso, com as demais classificadas, obedecida à ordem de classificação e os quantitativos propostos.

4.7. A COLIC convocará a(s) empresa(s) a ser(em) registrada(s), que terá(ão) prazo de até 03 (três) dias úteis, contados do recebimento da Ata de Registro de Preços, inclusive por meio eletrônico, para a sua assinatura e reenvio a este Poder, salvo motivo justificado, e devidamente aceito.

4.8. É facultado à administração, quando o convocado não assinar a ata de registro de preços no prazo e condições estabelecidos, convocar as licitantes remanescentes, na ordem de classificação, para fazê-lo em igual prazo e nas mesmas condições propostas pela primeira classificada.

4.9. Como condição para assinatura da Ata de Registro de Preços, bem como para as aquisições dela resultante, a(s) licitante(s) vencedor(as) deverá(ão) manter todas as condições de habilitação, de acordo com inciso XVI, art. 92 da Lei Federal nº. 14.133/2021.

4.10. A partir da publicação do extrato da Ata de Registro de Preços no Diário da Justiça Eletrônico, a licitante se obriga a cumprir, na sua íntegra, todas as condições estabelecidas, ficando sujeito, às penalidades pelo descumprimento de quaisquer de suas cláusulas.

4.11. O prazo de vigência da Ata de Registro de Preços, contado a partir da publicação do extrato da ata no Portal Nacional de Contratações Públicas e Diário da Justiça Eletrônico - DJE, será de 1 (um) ano, e poderá ser prorrogado, por igual período, desde que comprovado que as condições e o preço permanecem vantajosos.

4.12. Será realizada periódica pesquisa de mercado para comprovação da vantajosidade da ARP, de acordo com o art. 84, da Lei Federal n.° 14.133/2021.

4.13. As hipóteses de cancelamento do registro do fornecedor, dos preços registrados e da Ata de Registro de Preços, estão regulamentadas no § 6° do art. 54 c/c os arts. 55 e 56 da Resolução n.° 64/2023 TJAM.

4.14. Será permitida a adesão à Ata de Registro de Preços decorrente deste certame, por órgãos não participantes.

4.14.1. O quantitativo total registrado deverá ser utilizado pelo órgão gerenciador e órgãos participantes de maneira remanejada, de tal forma que o total aderido (gestor e participantes) não ultrapasse o quantitativo total registrado.

4.15. O quantitativo decorrente das adesões à Ata de Registro de Preços por órgãos ou entidades não participantes não poderá exceder, na totalidade, ao dobro do quantitativo de cada item registrado na Ata de Registro de Preços para o órgão gerenciador e órgãos participantes, independente do número de órgãos não participantes que aderirem.

4.15.1. As aquisições ou as contratações adicionais de que trata a Cláusula 4.15 não poderão exceder, por órgão ou entidade, a 50% (cinquenta por cento) dos quantitativos dos itens do instrumento convocatório e registrados na ata de registro de preços para o órgão gerenciador e para os órgãos participantes.

CLÁUSULA QUINTA
DO PAGAMENTO

5.1. O pagamento constante da solicitação do serviço será efetuado pela Divisão de Orçamento e Finanças do TJAM, de acordo com a legislação vigente, após recebimento da Nota Fiscal ou Fatura, conferida e atestada pelo setor requisitante, comprovando a prestação do serviço de maneira satisfatória.

5.2. Poderão ser solicitados para o pagamento: Nota Fiscal, de acordo com a legislação vigente, provas de regularidade perante o Fundo de Garantia por Tempo de Serviço (Certidão de Regularidade do FGTS), perante o Instituto Nacional do Seguro Social (Certidão Negativa de Débito do INSS), perante a Fazenda Federal (Certidão Conjunta Negativa de Débitos relativos aos TRIBUTOS FEDERAIS e à DÍVIDA

ATIVA DA UNIÃO), perante a Fazenda Estadual (Certidão Negativa de DÉBITO DO ESTADO), perante a Fazenda Municipal (Certidão Negativa de DÉBITO MUNICIPAL), e perante a Justiça do Trabalho.

5.2.1. A regularidade de que trata a Cláusula 5.2 poderá ser verificada por meio do SICAF – Sistema de Cadastramento Unificado de Fornecedores.

5.3. Constatando-se qualquer incorreção na Nota Fiscal, de acordo com a legislação vigente, bem como qualquer outra circunstância que desaconselhe o seu pagamento, o prazo para pagamento fluirá a partir da respectiva regularização.

CLÁUSULA SEXTA
DA REVISÃO E DO CANCELAMENTO DOS PREÇOS REGISTRADOS

6.1. Os preços registrados poderão ser revistos em decorrência de eventual redução dos preços praticados no mercado ou de fato que eleve o custo dos serviços ou bens registrados, cabendo ao TJAM promover as negociações junto aos fornecedores, observadas as disposições contidas na alínea “d” do inciso II do caput do art. 124 da Lei Federal nº 14.133/21.

6.2. Quando o preço registrado se tornar superior ao preço praticado no mercado por motivo superveniente, a unidade gerenciadora da ARP convocará os fornecedores para negociarem a redução dos preços aos valores praticados pelo mercado.

6.2.1. Os fornecedores que não aceitarem reduzir seus preços aos valores praticados pelo mercado serão liberados do compromisso assumido, sem aplicação de penalidade.

6.2.2. Na hipótese prevista no item anterior, o gerenciador convocará os fornecedores do cadastro de reserva, na ordem de classificação, para verificar se aceitam reduzir seus preços aos valores de mercado.

6.2.3. Se não obtiver êxito nas negociações, a unidade gerenciadora da ARP procederá ao cancelamento da ata de registro de preços, mediante decisão da Presidência, nos termos dispostos nesta resolução e no instrumento convocatório, e adotará as medidas cabíveis para a obtenção de contratação mais vantajosa.

6.3. Na hipótese de o preço de mercado tornar-se superior ao preço registrado e o fornecedor não poder cumprir as obrigações estabelecidas na ata, será facultado ao fornecedor requerer ao gerenciador a alteração do preço registrado, mediante comprovação de fato superveniente que o impossibilite de cumprir o compromisso.

6.3.1. Para fins do disposto na Cláusula 6.3, o fornecedor encaminhará, juntamente com o pedido de alteração, a documentação comprobatória ou a planilha de custos que demonstre a inviabilidade do preço registrado em relação às condições inicialmente pactuadas.

6.3.2. Na hipótese de não comprovação da existência de fato superveniente que inviabilize o preço registrado, o pedido será indeferido pela unidade gerenciadora da ARP e o fornecedor deverá cumprir as obrigações estabelecidas na ata, sob pena de cancelamento do seu registro, nos termos dispostos na Resolução n.° 64/2023 TJAM e no instrumento convocatório, sem prejuízo da aplicação das sanções previstas na Lei Federal n.° 14.133/2021, e outras legislações aplicáveis.

6.3.3. Na hipótese de cancelamento do registro do fornecedor, nos termos do disposto no item anterior, o gerenciador convocará os fornecedores do cadastro de reserva, na ordem de classificação, para verificar se aceitam manter seus preços registrados.

6.3.4. Se não obtiver êxito nas negociações, a unidade gerenciadora da ARP, mediante decisão da Presidência, procederá ao cancelamento da ata de registro de preços, nos termos dispostos na Resolução n. ° 64/2023 TJAM e no instrumento convocatório, e adotará as medidas cabíveis para a obtenção da contratação mais vantajosa.

6.4. O registro do fornecedor será cancelado quando:

I - descumprir as condições da ata de registro de preços sem motivo justificado;

II - não retirar a nota de empenho, ou instrumento equivalente, no prazo estabelecido pela Administração sem justificativa razoável;

III - não aceitar manter seu preço registrado, na hipótese prevista no § 4o do art. 54 da Resolução n.° 64/2023 TJAM;

IV - sofrer sanção prevista nos incisos III ou IV do caput do art. 156 da Lei Federal n.° 14.133/2021.

6.5. Os preços registrados poderão ser cancelados, total ou parcialmente, pela unidade gerenciadora da ARP, mediante decisão da Presidência, desde que comprovadas e justificadas as seguintes hipóteses:

I - por razão de interesse público;

II - a pedido do fornecedor, decorrente de caso fortuito ou força maior; ou

III - se não houver êxito nas negociações, nos termos do disposto no § 3° do art. 52 e no § 6° do art. 54 da Resolução n.° 64/2023 TJAM.

6.5.1. Compete à Presidência decidir quanto ao cancelamento do registro de preços, com base em procedimento administrativo instaurado pela unidade gerenciadora da ARP.

6.5.2. Nas hipóteses em que se proceder ao cancelamento do registro de preços, tiver sido formado cadastro de reserva e houver interesse no seu acionamento, caberá à unidade gerenciadora da ARP, realizar os procedimentos operacionais destinados ao chamamento do cadastro de reserva.

CLÁUSULA SÉTIMA
DAS INFRAÇÕES ADMINISTRATIVAS E DAS SANÇÕES

7.1. Comete infração administrativa, nos termos da lei, o licitante que, com dolo ou culpa:

7.1.1. Deixar de entregar a documentação exigida para o certame ou não entregar qualquer documento que tenha sido solicitado pelo(a) Pregoeiro(a) durante o certame;

7.1.2. Salvo em decorrência de fato superveniente devidamente justificado, não mantiver a proposta em especial quando:

7.1.2.1. Não enviar a proposta adequada ao último lance ofertado ou após a negociação;

7.1.2.2. Recusar-se a enviar o detalhamento da proposta quando exigível;

7.1.2.3. Pedir para ser desclassificado quando encerrada a etapa competitiva; ou

7.1.2.4. Deixar de apresentar amostra, quando for solicitado;

7.1.2.5. Apresentar proposta ou amostra, quando for solicitado, em desacordo com as especificações do Edital;

7.1.3. Não celebrar o contrato ou não entregar a documentação exigida para a contratação, quando convocado dentro do prazo de validade de sua proposta;

7.1.3.1. Recusar-se, sem justificativa, a assinar o contrato ou a ata de registro de preço, ou a aceitar ou retirar o instrumento equivalente no prazo estabelecido pela Administração;

7.1.4. Apresentar declaração ou documentação falsa exigida para o certame ou prestar declaração falsa durante a licitação;

7.1.5. Fraudar a licitação;

7.1.6. Comportar-se de modo inidôneo ou cometer fraude de qualquer natureza, em especial quando:

7.1.6.1. Agir em conluio ou em desconformidade com a lei;

7.1.6.2. Induzir deliberadamente a erro no julgamento;

7.1.6.3. Apresentar amostra, quando for solicitado, falsificada ou deteriorada;

7.1.7. Praticar atos ilícitos com vistas a frustrar os objetivos da licitação;

7.1.8. Praticar ato lesivo previsto no art. 5º da Lei n.º 12.846/2013.

7.2. Com fulcro na Lei Federal nº 14.133/2021, a Administração poderá, garantida a prévia defesa, aplicar aos licitantes e/ou adjudicatários as seguintes sanções, sem prejuízo das responsabilidades civil e criminal:

7.2.1. Advertência;

7.2.2. Multa;

7.2.3. Impedimento de licitar e contratar; e

7.2.4. Declaração de inidoneidade para licitar ou contratar, enquanto perdurarem os motivos determinantes da punição ou até que seja promovida sua reabilitação perante a própria autoridade que aplicou a penalidade.

7.3. Na instrução da aplicação das sanções administrativas devem ser observados os princípios do contraditório e da ampla defesa, considerando, ainda:

I - a natureza e a gravidade da infração cometida;

II - as peculiaridades do caso concreto;

III - os danos causados ao Tribunal;

IV - a implantação ou o aperfeiçoamento de programa de integridade, conforme normas e orientações dos órgãos de controle;

V - as circunstâncias agravantes ou atenuantes;

VI - o custo e benefício da instrução do processo em relação à sanção a ser aplicada.

Parágrafo único. A pena-base deve ser fixada levando-se em consideração as circunstâncias listadas nos incisos I a IV do caput deste artigo; em seguida serão aplicadas as circunstâncias agravantes e atenuantes, respeitando-se os limites mínimo e máximo das penas previstas nos artigos 23 e 24 do Anexo VIII da Resolução n.° 64/2023 TJAM.

7.4. A aplicação das sanções previstas neste Edital não exclui, em hipótese alguma, a obrigação de reparação integral dos danos causados.

7.5. O regramento para a instauração e instrução dos processos administrativos sancionatórios e para a definição da dosimetria da aplicação da pena decorrentes da prática de condutas previstas no art. 155 da Lei Federal n.° 14.133/2021, encontra-se estabelecido no Anexo VIII da Resolução n.° 64/2023 TJAM.

7.6. As penalidades aplicadas serão obrigatoriamente divulgadas no Diário da Justiça Eletrônico, no site do Tribunal de Justiça do Amazonas e registradas no Sistema de Cadastramento Unificado de Fornecedores (SICAF).

CLÁUSULA OITAVA
DAS DISPOSIÇÕES FINAIS

8.1. Será incluído, nesta Ata de Registro de Preços, na forma de anexo, o registro dos licitantes que aceitarem cotar os bens ou serviços com preços iguais aos do licitante vencedor na sequência da classificação do certame.

8.1.1. A ordem de classificação dos licitantes registrados nesta Ata de Registro de Preços, na forma do item anterior, deverá ser respeitada nas contratações.

8.1.2. O registro a que se refere a Cláusula 8.1 tem por objetivo a formação de cadastro de reserva no caso de impossibilidade de atendimento pelo primeiro colocado da ata, nas hipóteses previstas na Cláusula Sexta deste instrumento.

8.1.3. A habilitação dos fornecedores que comporão o cadastro de reserva a que se refere a Cláusula 8.1 será efetuada quando houver necessidade de contratação de fornecedor remanescente, nas hipóteses previstas na Cláusula Sexta desta Ata de Registro de Preços.

8.2. A critério do Tribunal de Justiça do Amazonas, a presente licitação poderá ser:

a) adiada, por conveniência do Tribunal de Justiça do Amazonas, desde que devidamente justificada;

b) revogada, a juízo do Tribunal de Justiça do Amazonas, se considerada inoportuna ou inconveniente ao interesse público, decorrente de fato superveniente devidamente comprovado, pertinente e suficiente para justificar tal conduta;

c) anulada, de ofício ou mediante provocação de terceiros, sempre que presente ilegalidade insanável, mediante parecer escrito onde indicará expressamente os atos com vícios insanáveis, tornando sem efeito todos os subsequentes que deles dependam, e dará ensejo à apuração de responsabilidade de quem lhes tenha dado causa.

8.3. Na contagem dos prazos deste Edital será excluído o dia de início e incluído o dia do vencimento, considerando-se o expediente normal deste Órgão, de segunda a sexta-feira, das 8 às 14 horas, salvo

expressa disposição em contrário.

8.4. É vedada a manutenção, aditamento ou prorrogação de contrato de prestação de serviços com empresa que venha a contratar empregados que sejam cônjuges, companheiros ou parentes em linha reta, colateral ou por afinidade, até o terceiro grau, inclusive, de ocupantes de cargos de direção e de assessoramento, de membros ou juízes vinculados ao Tribunal de Justiça do Amazonas.

8.5. Integram esta ARP, o Edital do Pregão Eletrônico nº. XXX/202X - TJAM e seus anexos, e as proposta(s) da(s) empresa(s): xxxxxxxxxxxxxxxxxx, vencedoras do certame supramencionado.

8.6. Os casos omissos serão dirimidos pela Presidência do Tribunal de Justiça do Amazonas.

8.7. Fica eleito o foro da Comarca de Manaus, capital do Estado do Amazonas, para dirimir quaisquer dúvidas decorrentes desta Ata com exclusão de qualquer outro, por mais privilegiado que seja.

_____

Presidente do Tribunal de Justiça do Estado do Amazonas

_____

Empresa Registrada

ANEXO DA ATA DE REGISTRO DE PREÇOS (ARP) Nº. XXX/202X-TJAM VINCULADA AO PREGÃO ELETRÔNICO PARA REGISTRO DE PREÇOS Nº. XXX/202X-TJAM

Consta abaixo o registro das empresas que aceitaram cotar preços iguais ao da empresa vencedora do Pregão Eletrônico nº XXX/202X-TJAM, na sequência da classificação do certame

ITEM	EMPRESA	CNPJ	ENDEREÇO	TELEFONE/ CONTATO

PREGÃO ELETRÔNICO/SRP N.º 40/2024-TJAM
ANEXO V – TERMO DE REFERÊNCIA

PREGÃO ELETRÔNICO/SRP N.º 40/2024-TJAM
ANEXO VI – MINUTA DE TERMO DE CONTRATO

PREGÃO ELETRÔNICO/SRP N.º 40/2024-TJAM

ANEXO VII – MODELO DE DECLARAÇÃO DE VISTORIA

Declaro, em atendimento ao previsto no Edital de Licitação - PE nº ___/20__, que eu, _____, portador da Carteira de Identidade n.º _____, inscrito no CPF/MF sob n.º_____, representante da empresa _____, estabelecida no(a) _____, como seu(ua) representante legal para os fins da presente declaração, compareci perante o representante do Tribunal de Justiça do Estado do Amazonas e vistoriei os locais onde serão executados os serviços objeto da licitação em apreço, tomando plena ciência das condições e grau de dificuldades existentes.

Manaus, _____ de _____ de 20__.

(Assinatura e carimbo)
Nome do Representante
Nome da Empresa
CNPJ/MF nº

Visto:

Representante do TJ/AM
(Nome completo e matrícula)

Documento assinado eletronicamente por **Nélia Caminha Jorge**, **Desembargadora de Justiça**, em 16/08/2024, às 13:42, conforme art. 1º, III, "b", da Lei 11.419/2006.

A autenticidade do documento pode ser conferida no site https://sei.tjam.jus.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0 informando o código verificador **1744126** e o código CRC **710861D3**.

2024/000014603-00 1744126v2

Criado por matheus.barreto, versão 2 por matheus.barreto em 16/08/2024 12:29:13.

TRIBUNAL DE JUSTIÇA DO ESTADO DO AMAZONAS
Av. André Araújo, S/N - Bairro Aleixo - CEP 69060-000 - Manaus - AM - www.tjam.jus.br

TERMO DE REFERÊNCIA

1. OBJETO DA CONTRATAÇÃO

1.1. Definição do Objeto: Contratação de empresa especializada no fornecimento de solução de gerenciamento de acessos privilegiados (PAM – Privileged Access Management).

1.2. Justificativa para a contratação:

1.2.1. O TJAM possui diversos usuários internos, incluindo servidores, comissionados, terceirizados, estagiários, requisitados e afastados, além de inúmeros usuários externos que utilizam os sistemas e serviços disponibilizados, serviços digitais, sites e sistemas à sociedade.

1.2.2. Para o acesso dos envolvidos é imprescindível que os diversos recursos de Tecnologia da Informação e Comunicação, como, por exemplo: servidores, computadores, internet, sistemas, aplicações, serviços, e-mail, sites, dentre outros tantos, estejam seguros e acessíveis.

1.2.3. A justificativa para a contratação encontra-se pormenorizada em tópico específico do Estudo Técnico Preliminar, anexo deste Termo de Referência.

1.3. Especificação técnica do Objeto:

ITEM	ESPECIFICAÇÕES	QUANTIDADE MÍNIMA POR CONTRATAÇÃO	QUANTIDADE TOTAL
1	Solução de Segurança para Identidades e seus Privilégios – Monitoramento de comportamento e mitigação de riscos de usuários administradores da TI, com garantia pelo período de 12 (doze) meses.	50	75
2	Solução de Segurança para Identidades e seus Privilégios – Proteção para Aplicações Tradicionais, com garantia pelo período de 12 (doze) meses.	20	40
3	Solução de Segurança para Identidades e seus Privilégios – Proteção Local para ervidores Windows e Linux, com garantia pelo período de 12 (doze) meses.	200	400
4	Solução de Segurança para Identidades e seus Privilégios – Proteção Local para Estações de Trabalho, com garantia pelo período de 12 (doze) meses.	2500	3500
5	Serviço de instalação e configuração para Solução de Segurança para Identidades e seus Privilégios.	1	1
6	Transferência de Conhecimento para Solução de Segurança para Identidades e seus Privilégios (turma)	1	2
7	Serviço de Suporte Técnico Especializado	12	12

1.3.1. Solução de Segurança para Identidades e seus Privilégios – Proteção e Monitoração de Acessos:

1.3.1.1. A solução deverá atender usuários físicos, equipamentos servidores, estações de trabalho e usuários lógicos e ativos de rede;

1.3.1.2. A solução deve apoiar, no mínimo, aos requisitos (artigos 6, 42, 43, 46, 48 e 50) da Lei Geral de Proteção de Dados-LGPD, como: Determinar como os dados deverão ser tratados, mantidos e protegidos e a quem responsabilizar em caso de descumprimento; Proteger o acesso a dados pessoais sensíveis; Responsabilizar pessoal e responder a incidentes; Aplicar boas práticas de governança, através de regras que deverão respeitar os preceitos da lei, de maneira a mitigar os riscos inerentes ao tratamento de dados e implementar e demonstrar a efetividade das políticas de segurança relacionadas ao tratamento de dados;

1.3.1.3. Apoiando aos requisitos da LGPD a solução deverá proteger e monitorar acessos a dados pessoais sensíveis por meio da segurança de credenciais e acessos de alto privilégio em serviços críticos, detectando e respondendo rapidamente a incidentes de segurança, identificando e mitigando ações privilegiadas com comportamentos de alto risco, avaliando riscos e testando a efetividade dos processos de proteção de dados por meio de relatórios da solução com identificação e classificação do status de risco do ambiente privilegiado, demonstrando conformidade e prova de que os controles de segurança necessários estão nos lugares certos, provendo análise comportamental, auditoria e segurança dos acessos a sistemas por meio de todas credenciais administrativas de alto privilégio em dispositivos e sistemas-alvo diversos do ambiente;

1.3.1.4. Um sistema-alvo da solução é definido como um servidor, uma estação de trabalho, um ativo de rede e de segurança, dentre outros mencionados a seguir, cujas credenciais de acesso passem a ser protegidas e gerenciadas pela solução;

1.3.1.5. Um usuário da solução é definido como qualquer pessoa que acesse um sistema-alvo mediante logon na solução e uso de credenciais por ela gerenciadas;

1.3.1.6. Deve monitorar sessões, gravar, detectar, correlacionar e mitigar todos comportamentos anormais de, pelo menos, 75 usuários simultâneos acessando todos os sistemas-alvo, dentre eles servidores Linux/Unix ou Windows, Controladores de domínio Microsoft Active Directory, estações de trabalho Windows e demais ativos de rede e sistemas diversos;

1.3.1.7. A solução deverá ser entregue com acesso remoto privilegiado seguro (externo a rede corporativa) para os usuários simultâneos mencionados, sem a entrega de credenciais privilegiadas e sem a necessidade de instalação e uso de clientes (do tipo VPN ou outros) nos dispositivos dos usuários remotos por todo período contratado;

1.3.1.8. A solução deverá ser entregue com acesso Single-sign-on e múltiplo fator de autenticação adaptativo para, no mínimo, os 75 usuários internos e/ou remotos (externos a rede corporativa) mencionados, por todo período contratado, suportando, no mínimo:

1.3.1.8.1. Usuário e senha dos diretórios suportados, aplicativo para dispositivos móveis do tipo IOS e Android, oferecendo suporte para Biometria do tipo FaceID e através do leitor de digital, Smartphone push (Notificação para aprovar ou recusar uma autenticação), Geolocalização através de coordenadas GPS e

banco de dados de IP, Suporte a tokens OATH OTP, autenticação na tela de login via QRcode sem a necessidade de digitar usuário e senha, com opção de forçar a biometria no dispositivo móvel, Entrega de código via SMS e chamada de voz, perguntas de segurança, notificações por e-mail e telefone celular, tokens OTP (on-line, off-line, por e-mail, hardware);

1.3.1.8.2. Autenticação auto-ajustada baseada no contexto de risco e segurança aprendidos pela solução, permitindo a criação de um perfil para cada usuário, aproveitando atributos históricos e situacionais específicos do mesmo, como localização, dispositivo, rede, horário e índice de risco de comportamento;

1.3.1.8.3. Análise de solicitações de autenticação em relação a padrões históricos, atribuição de índice de risco a cada tentativa de logon, geração de alertas e criação de políticas de bloqueio a serem acionadas quando um comportamento anômalo é detectado e de acesso simplificado quando o usuário é entendido como legítimo;

1.3.1.8.4. Permitir que os usuários adicionem e modifiquem fatores de autenticação diretamente em um portal com definição de período de desvio do múltiplo fator de autenticação;

1.3.1.8.5. Prover relatórios e dashboards customizáveis com detalhamento de informações em tempo real sobre as atividades de autenticação, como falhas na autenticação secundária, tentativas bem-sucedidas de login e os fatores de autenticação mais usados;

1.3.1.8.6. Entenda-se como sistemas-alvo os baseados, em no mínimo, as seguintes tecnologias: S.O.: Linux/Unix e Microsoft Windows; Hypervisors: Acrópolis (Nutanix), VMWare, RedHat KVM e Microsoft Hyper-V; Contas de usuários de sistemas e de serviço; Credenciais do Microsoft COM+, IIS, Apache TomCat, RedHat Jboss, Nginx; Objetos (usuários, grupos e computadores) do Microsoft Active Directory e LDAP; Contas de usuários e administradores de bancos de dados Microsoft SQL Server, Oracle, PostgreSQL; Contas de equipamentos ativos de conectividade de redes LAN (Local Area Network) e WAN (Wide Area Network) – switches, roteadores, controladores/APs WiFi, SAN (Storage Area Network) e NAS (Network Attached Storage); Contas de usuários e administradores de consoles de gerenciamento de servidores e estações de trabalho; Contas de equipamentos dedicados à segurança, tais como Firewall, IPS, AntiSpam e filtros de conteúdo; Contas de equipamentos dedicados à segurança física, tais como câmeras de vigilância, catracas, etc.; Credenciais de nuvem em Google Workspace, VMWare ESXi, Azure, AWS, GCP, Office 365.
1.3.1.9 Gestão de dados do ciclo de vida e compartilhamento das contas privilegiadas, monitoramento e gravação de sessões privilegiadas:
1.3.1.9.1. A solução deve conceder acesso aos sistemas utilizando “Remote Desktop” e “SSH”, disponibilizados pelos sistemas-alvo do ambiente, sem que os usuários vejam qualquer senha e chave (vigentes no momento e providas para as aplicações e conexões remotas, devendo ser recuperadas de forma automática e transparente do repositório seguro de credenciais da solução), garantindo que não haja necessidade de instalação de aplicações e/ou agentes nas estações dos usuários para realizar o acesso a sistemas e aplicações parametrizáveis, onde a aplicação deverá ser executada, por meio de página web, devidamente autenticada com usuário e senha pré-determinados ou recuperados da base de dados da solução, sem que haja login interativo por parte do usuário no S.O. do servidor de destino, possibilitando habilitar gravação da sessão, caso seja necessário. Exemplo: Executar o SQL Management Studio com credencial de SA (System Administrator) sem que o usuário conheça a senha e sem necessidade de login interativo prévio do usuário no sistema operacional do host de destino;

1.3.1.9.2 A solução deve permitir Integração para gestão de acessos privilegiados em serviços de nuvem padrões de mercado, como Amazon Web Services (AWS), Google Cloud, IBM Cloud e Microsoft Azure, disponibilizando no mínimo as seguintes funcionalidades: Integração e gestão de acessos privilegiados em contas de serviços em nuvem; Integração com sessões de serviços de nuvem, incluindo início e finalização de sessão e Gravação e auditoria de acesso de sessões iniciadas em serviços de nuvem;
1.3.1.9.3. Deve possuir as sessões administrativas acessadas e monitoradas ao vivo, com compartilhamento de tela e controle de periféricos, como teclado e mouse (assistência remota), e por meio de gravação de comandos e vídeos das mesmas, em formato padrão de execução não proprietário da solução, possibilitando que os comandos e vídeos gerados possam ser indexados para pesquisa futura, permitindo o filtro de comandos e ações executadas ao longo da sessão gravada, possibilitando pesquisar ações específicas na sessão gravada;
1.3.1.9.4. Proteger contra a perda, roubo e gestão inadequada de credenciais através de regras de complexidade da senha que incluem comprimento da senha (quantidade de caracteres), frequência de troca automatizada das senhas e chaves SSH, especificação de caracteres permitidos ou proibidos na composição da senha e outras medidas e mitigar problemas de segurança relacionados ao compartilhamento indevido de credenciais privilegiadas que são armazenadas localmente em dispositivos e também de contas que não são gerenciadas de forma centralizada por serviços de diretórios;
1.3.1.9.5. Descobrir credenciais privilegiadas referenciadas por serviços e processos automatizados e propagar as senhas geradas de forma aleatória onde quer que estas estejam referenciadas e descobrir e alterar credenciais em ambiente Windows, incluindo contas nomeadas, administradores ‘built-in’ e convidados, para determinar movimentações laterais (pass-the-hash), exibidas em mapa de rede gráfico e interativo ou através de relatórios e interface de gerenciamento;
1.3.1.9.6. Gerenciar, de forma segura, senhas utilizadas por contas de serviço, evitando a utilização de senhas em texto claro por scripts ou rotinas dos equipamento e garantir a implementação dos privilégios mínimos necessários, provendo acesso às senhas das contas privilegiadas somente ao pessoal autorizado;
1.3.1.9.7. Possuir funcionalidade de “AD Bridge” para integração de servidores Linux/Unix no Active Directory, acompanhando a mesma nomenclatura e grupos do diretório LDAP ou AD; Provisionar na plataforma Unix-like as contas e grupos do Active Directory que possuam permissão de acesso, de maneira automatizada e transparente;
1.3.1.9.8. Permitir a definição de Fluxos de Aprovação (Workflows) para obtenção de acesso às Contas Privilegiadas, com as seguintes características: Personalização de fluxos: permitir a configuração de fluxos para aprovação, de acordo com a criticidade e características da conta, e aprovação de, pelo menos, um responsável; Permitir a aprovação perante um agendamento de ações administrativas; ou seja; a aprovação do acesso ocorrerá em um dia, mas a liberação da senha ocorrerá de forma automática somente na data e horário previstos; Ser capaz de encontrar contas de usuários privilegiados que possam ser gerenciadas pela solução, permitindo ou não que a conta descoberta seja gerenciada pela solução; Ser capaz de substituir as senhas de identidades privilegiadas que estejam sendo utilizadas por determinado serviço em todos os locais onde estejam sendo utilizadas; A descoberta automática deve ser realizada por buscas no Active Directory (AD) e por intervalos de endereços IP;
1.3.1.9.9. Oferecer em sua aplicação web diferentes visões e opções de acordo com as permissões dos usuários, mostrando, por exemplo, apenas as funcionalidades delegadas àquele usuário; Suportar métodos para registrar e relatar qualquer ação realizada e detectada pela solução, incluindo registros de aplicações baseadas em texto, auditoria de banco de dados, aplicações syslog, notificações de e-mail;
1.3.1.9.10. Registrar cada acesso, incluindo os acessos via aplicação web, para solicitações de senha, aprovações, checkout’s, mudanças de delegação, relatórios e outras atividades. Devem ser registrados os acessos à console de gerenciamento da solução, tanto para configuração quanto para relatórios, bem como todas as atividades de alterações de senhas; logoff dos usuários; Alterações nas funções de delegação; Adições, deleções e alterações de senhas gerenciadas pela solução; Operações das senhas dos usuários, incluindo check-in e check-out, solicitações negadas e permitidas; Os relatórios devem ser filtrados por período de tempo, tipo de operação, sistema, gerente e outros critérios;
1.3.1.9.11. Deve fornecer relatórios de conformidade detalhados das operações realizadas pela solução, tais como: Lista de sistemas gerenciados; Senhas armazenadas; Eventos de alteração de senha; Permissões de acesso web; Auditoria de contas, sistemas e usuários; Alerta em tempo real;
1.3.1.10. Análise comportamental e mitigações de risco no ambiente crítico:

1.3.1.10.1. A solução deverá realizar a identificação e o correlacionamento de todas as ações citadas abaixo, montando perfis de comportamento gerais (usuários, acessos, credenciais, máquinas, outros) do ambiente privilegiado e acessos aos sistemas-alvo por meio da solução;
1.3.1.10.2. Deve combinar ações que caracterizam abusos, comportamentos anormais e fora dos padrões aprendidos/mapeados, aplicando ações mitigatórias automáticas como solicitação de nova autenticação multi-fator, suspensão e encerramento de sessões e troca das credenciais privilegiadas, em caso de atividades suspeitas de alto risco, detectando, no mínimo:
1.3.1.10.3. Acessos a solução: durante horários irregulares (quando um usuário recupera uma senha de conta privilegiada em uma hora irregular de acordo com seu perfil comportamental); durante dias irregulares (quando um usuário recupera uma senha de conta privilegiada em um dia irregular de acordo com seu perfil comportamental); através de IP irregular e desconhecido (quando um usuário acessa contas privilegiadas de um endereço IP ou sub-rede incomum, de acordo com seu perfil comportamental); não gerenciados (quando uma conexão com uma máquina é feita com uma conta privilegiada que não é gerenciada na solução);
1.3.1.10.3.1. Acessos gerais: excessivos a contas privilegiadas (quando um usuário acessa contas privilegiadas com mais frequência do que o normal, de acordo com seu perfil comportamental); a uma máquina; anômalos a várias máquinas (quando uma conta efetuou login em um grande número de máquinas inesperadas durante um tempo relativamente curto) e realizados fora da solução (diretamente no sistema-alvo); Usuários incomuns logando de uma máquina de origem conhecida; quando ocorrem indicações de atividade de um usuário inativo da solução; Atividades definidas como suspeitas detectadas em sessões privilegiadas (comandos e anomalias na solução);

1.3.1.10.3.1.1. Máquinas: acessadas a partir de endereços IP incomuns; acessadas durante horários irregulares, de acordo com seu padrão de utilização; Incomuns originando acessos;
1.3.1.10.3.1.2. Suspeita de roubo de credenciais, quando um usuário se conecta a uma máquina sem primeiro recuperar as credenciais necessárias da solução; Alteração de senha suspeita, quando é identificada uma solicitação para alterar ou redefinir uma senha ignorando a solução; Credenciais expostas de contas de serviço que se conectam ao LDAP em texto não criptografado;
1.3.1.10.3.1.3. Delegação não restrita, através da análise das contas de domínio, que recebem privilégios de delegação permissivos e, portanto, expõem o domínio a um alto risco; Contas privilegiadas com configuração SPN (nome principal de serviço) vulneráveis a ataques de força bruta e de dicionário off-line, permitindo que um usuário interno malicioso recupere a senha de texto sem criptografia da conta e Contas de serviço conectadas por meio de logon interativo;
1.3.1.10.4. Deve permitir a classificação de eventos por níveis de risco e respostas automáticas (suspensão e terminação de sessões) baseadas nos mesmos, com a possibilidade de colocar sessões em quarentena, pendentes de liberação e terminação pelo administrador, permitindo a configuração de eventos críticos a serem reportados automaticamente, baseados em Comandos Linux, Comandos, janelas e aplicações Windows, expressões regulares para comandos em geral e eventos configurados manualmente, permitindo a atribuição de nível de risco customizado.
1.3.1.11. Segurança contra tomada de controle da rede por meio de credenciais do Active Directory – A solução deve proteger e monitorar Controladores de Domínio Active Directory contra roubo de identidade, acesso não autorizado e ataques visando a tomada de controle da rede via estrutura de diretórios, de acordo com as funções de monitoramento de atividades internas nos mesmos e tráfego de segmentos de rede que estes estejam instalados, para confirmação de integridade das solicitações e tickets Kerberos utilizados nos equipamentos e contas de usuário detectando, no mínimo:
1.3.1.11.1. Atividades anômalas em tempo real, típicas de ataques ao protocolo de autenticação Kerberos, como roubo de credenciais, movimentação lateral e escalonamento de privilégios; A extração e uso de um Kerberos TGT (ticket de concessão de tickets) da memória LSASS (Subsistema de autoridade de segurança local) em um host para obter acesso a outros recursos da rede (Pass-the-ticket);
1.3.1.11.2. A recuperação e exploração de hashes de senha armazenados no banco de dados do SAM (Security Accounts Manager) ou do Active Directory para representar um usuário legítimo (Pass-the-Hash); O uso do hash de uma conta de usuário para obter um ticket do Kerberos, que é usado para acessar outras contas e recursos de rede (Overpass-the-Hash);
1.3.1.11.3. A modificação das configurações de permissão de ticket do Kerberos para obtenção de acesso não autorizado aos recursos da rede - PAC Forjado (Manipulação de Certificado de Atributo de Privilégio); A obtenção de acesso ao KDC (Kerberos Key Distribution Center) para geração de token principal de segurança que fornece acesso completo a um domínio inteiro (Golden Ticket); A recuperação maliciosa de credenciais do controlador de domínio (DCSync);
1.3.1.12. Arquitetura e Segurança da Solução:
1.3.1.12.1. Incorporar medidas de segurança como Certificação Common Criteria (CC) – ISO/IEC 15408 – como garantia de segurança do método utilizado no desenvolvimento do sistema de repositório seguro de credenciais e Criptografia dos módulos da solução, a fim de proteger a informação em trânsito entre módulos da solução e aplicações web dos usuários finais e possibilitar a utilização de criptografia do banco de dados utilizado pela solução para armazenar as credenciais gerenciadas pela mesma, sendo compatível com; AES com chaves de 256 bits, FIPS 140-2 e Encriptação PKCS#11 ou superior;
1.3.1.12.2. Deve utilizar banco de dados em alta disponibilidade, para armazenamento de credenciais, com as melhores práticas de segurança: mecanismo de blindagem do sistema operacional através da desativação ou desinstalação de serviços e portas de acesso não essenciais ao funcionamento da solução. Caso o banco de dados utilizado para armazenamento de credenciais seja de terceiros, a solução deverá ser entregue com licenças de software, garantia e suporte que o compatibilize com a solução.
1.3.1.12.3. Suportar a implementação em parque computacional Windows Server 2012 R2, Windows Server 2016, Windows Server 2022 e/ou Linux em ambiente físico ou virtualizado com infraestrutura (servidores/software em ambiente virtualizado, S.O., camada de balanceamento/redirecionamento de tráfego, etc.) provida pela CONTRATANTE para implantação e uso da solução em alta disponibilidade.
1.3.1.12.4. Os elementos críticos da solução, como Repositório Seguro de credenciais, Gateways de Gravação e Monitoração Comportamental deverão ser instalados em alta disponibilidade ativo-ativo em cada uma das localidades (site principal e site redundante adicional), com chaveamento entre localidades (sites), garantindo que o processo seja transparente aos usuários conectados e a normalização das funcionalidades ocorra em até 5 (cinco) minutos, caso exista perda de comunicação e mecanismos para a recuperação de desastres compatível com soluções de backup e arquivamento disponíveis no mercado.
1.3.1.12.5. Prover, no mínimo, dois ambientes adicionais externos da solução em produção para testes e homologação, replicando as mesmas licenças e funcionalidades do ambiente de produção.

1.3.2. Solução de Segurança para Privilégios e Acessos – Proteção para Equipamentos Servidores:
1.3.2.1. Proteção local para Servidores Unix/Linux
1.3.2.1.1. As funcionalidades devem ser providas por meio de agentes instalados no sistema operacional dos servidores e permitir a proteção e controle dos privilégios em contas de usuário em equipamentos Unix, Linux, Solaris e AIX e associar os privilégios e comandos controlados às contas cadastradas no repositório seguro de credenciais, realizando o controle no próprio sistema operacional;
1.3.2.1.2. Garantir o controle e bloqueio de comandos, mesmo que o acesso seja realizado diretamente no servidor de destino (sem passar pelos monitores/gravadores de acessos) fazendo uso das funcionalidades instaladas no sistema operacional alvo.
1.3.2.1.3. Disponibilizar, como conjunto mínimo de atividades controladas no ativo de destino, as seguintes operações: criação e exclusão de arquivos e diretórios, mudança de nome de arquivos e diretórios, abertura de arquivos para escrita, comandos chown e chmod e ligações entre arquivos.
1.3.2.1.4. Implementar restrições, em uma plataforma, de maneira global ou em uma conta de usuário ou grupo de maneira granular.
1.3.2.1.5. Realizar o controle mediante interceptação do comando antes que ele seja executado, permitir a liberação de comandos privilegiados a usuários comuns, permitir que os comandos executados em sistemas monitorados sejam gravados em modo texto no repositório seguro de credenciais, permitir o agrupamento de comandos, bem como a utilização de coringas como (*), para uma definição ampla de parâmetros;
1.3.2.1.6. Permitir que sejam atribuídas permissões para usuários e grupos, inclusive do Active Directory e oferecer a capacidade de verificação da identidade da pessoa que executa comandos localmente no dispositivo alvo através de autenticação via usuário da ferramenta, LDAP ou RADIUS;
1.3.2.1.7. A solução deverá possuir funcionalidade que permita definir variáveis de ambiente no momento da execução de um comando, independentemente da definição realizada pelo usuário ou seu perfil. Sendo exigido no mínimo as seguintes variáveis: PATH, ENV, BASH_ENV, GLOBIGNORE, SHELLOPTS;
1.3.2.1.8. Possibilitar o uso da máscara de usuário na execução dos comandos (valores entre 0000 e 0777);
1.3.2.1.9. Impedir a utilização da técnica de ShellEscape, em que um programa autorizado e executado com privilégios permita a execução de outros programas e consequentemente escape dos controles definidos;
1.3.2.1.10. Disponibilizar a funcionalidade de restrição de Shell, que impossibilite que scripts e shells de sistema executem comandos não permitidos pelas regras definidas na solução;
1.3.2.1.11. Monitorar e exibir acessos e atividades realizadas no próprio sistema l) Possibilitar mapear e coletar atividades regulares de usuários através do modo observação, agregando e exportando os resultados para um perfil;
1.3.2.1.12. Prover um controle de comandos completo, com a possibilidade de criar uma lista de comandos permitidos e bloqueados (whitelisting/blacklisting), a serem alterados (criação de alias) ou prevenir que comandos sejam executados ou permitir trabalhar em Shell modificado/controlado;
1.3.2.1.13. Prover meios de permitir que os usuários executem comandos específicos e conduzam sessões remotamente baseado em regras sem autenticar-se diretamente utilizando credenciais privilegiadas;
1.3.2.2. Proteção local para Servidores Windows
1.3.2.2.1. Realizar varredura e inventário de aplicações instaladas no sistema operacional;
1.3.2.2.2. As funcionalidades devem ser providas por meio de agentes instalados no sistema operacional dos servidores e permitir a proteção e controle dos privilégios;
1.3.2.2.3. Garantir o controle e bloqueio de comandos, mesmo que o acesso seja realizado diretamente no servidor de destino (sem ser através dos monitores/gravadores de acessos);
1.3.2.2.4. Oferecer opções de execução sem aviso: de aplicações com privilégios em modo explícito e transparente, monitorada de aplicações em modo explícito e transparente, com restrições de aplicações em modo explícito e transparente;
1.3.2.2.5. Exibir a reputação do arquivo executado advinda de, pelo menos, 1 (uma) fonte externa e disponibilizar a opção de encaminhamento de arquivo suspeito para análise de malware em soluções de mercado;
1.3.2.2.6. Suportar, no mínimo, as versões Windows Server 2003 SP2 x32 & x64, Windows Server 2008 x32 & x64, Windows Server 2008 R2 x64, Windows Server 2012/2012 R2, Windows Server 2016, Windows Server 2019 e Windows Server 2022;
1.3.2.2.7. Implementar regras de controle de aplicações permitidas e bloqueadas para execução fazendo uso das funcionalidades instaladas no sistema operacional alvo, independentemente do acesso ao ativo ser realizado via monitores/gravadores de acessos ou diretamente no ativo;

1.3.2.2.8. Implementar regras de controle do nível de privilégio utilizado na execução das aplicações permitidas fazendo uso das funcionalidades instaladas no sistema operacional alvo, independentemente do acesso ao ativo ser realizado via monitores/gravadores de acessos ou diretamente no ativo;
1.3.2.2.9. Implementar controle de nível de privilégio independentemente da permissão que o usuário possua localmente no ativo ou no domínio, permitindo que usuários restritos executem atividades com nível administrativo;
1.3.2.2.10. Permitir atribuição granular para execução de aplicações com nível de privilégio administrativo, sem que esse privilégio seja global na máquina;
1.3.2.2.11. Fazendo uso das funcionalidades instaladas no sistema operacional alvo, deve permitir a criação de políticas reutilizáveis, contendo, no mínimo, os seguintes tipos de aplicações ou tipos de arquivos: executáveis, scripts, aplicações nativas Windows, bibliotecas dinâmicas (DLL), instaladores, controles ActiveX, objetos COM;
1.3.2.2.12. Implementar a verificação de checksum do arquivo, dos parâmetros permitidos e da assinatura de fabricante, para objetos reutilizáveis da solução;
1.3.2.2.13. Implementar o suporte ao nome exato da aplicação/arquivo/script e expressões regulares em qualquer formato, para objetos reutilizáveis da solução;
1.3.2.2.14. Utilizar eventos reportados na interface da ferramenta para criação de novas políticas ou incluí-los em políticas existentes;
1.3.2.2.15. Permitir agrupar aplicações com base em suas características, para facilitar a inserção de novas aplicações aos grupos ou políticas de segurança de aplicações já criadas;
1.3.2.2.16. Impedir a desativação das funcionalidades instaladas no sistema operacional alvo sem autorização e/ou registro da atividade por meio da interface de gerência;
1.3.2.2.17. Disponibilizar o registro das execuções e atividades dos usuários, facilitando a criação de políticas baseadas em comportamento conhecido;
1.3.2.2.18. Monitorar e exibir acessos e atividades realizadas na própria solução;
1.3.2.2.19. Deve permitir autorização de acesso às aplicações e arquivos, quando incluídos em regras, individualmente ou em grupos;
1.3.2.2.20. Deve realizar varreduras fazendo uso das funcionalidades instaladas no sistema operacional alvo para catalogar arquivos existentes nas máquinas e uni-los ao inventário populado mediante detecção durante a execução;
1.3.2.2.21. Deve verificar a reputação dos arquivos executados e detectados pelas funcionalidades instaladas no sistema operacional alvo ou órgãos de controle de ameaças, como por exemplo o VirusTotal.com ou similares;
1.3.2.2.22. Deve permitir a execução automática de tipos desconhecidos de arquivo, de acordo com sua origem, mesmo possuindo restrições;
1.3.2.2.23. Possibilitar o monitoramento e a criação de evidência em vídeo de certas execuções de arquivo e de execuções sob certas condições definidas em política;
1.3.2.2.24. Possibilitar ao usuário final a solicitação de liberação de atividades específicas fazendo uso das funcionalidades instaladas no sistema operacional alvo;
1.3.2.2.25. Possibilitar a liberação emergencial da execução de comandos e elevação de privilégios sem desativar a solução, caso o usuário esteja off-line;
1.3.2.2.26. Implementar as regras de controle de acordo com características do usuário final, incluindo nome de usuário, grupos a que o usuário pertence e endereço IP;
1.3.2.2.27. Oferecer monitoramento de atividade maliciosa dos processos em execução, visando detectar tentativas de roubo de credenciais;
1.3.2.2.28. Fazendo uso das funcionalidades instaladas no sistema operacional alvo, a solução deve alertar, reportar e bloquear atividade anômala de arquivos e usuários durante a interação com bases de senhas no formato hash, como por exemplo, SAM local e LSASS;
1.3.2.2.29. Caso o dispositivo não possa estar conectado de forma permanente aos monitores/gravadores de acessos da solução e repositório seguro de credenciais, deve, de forma autônoma e off-line, gerenciar as senhas das credenciais locais, aplicando políticas de randomização e sincronização das senhas definidas na central da solução;
1.3.2.2.30. Permitir o envio de arquivos suspeitos, executados sob sua supervisão, para soluções de análise de ameaça do tipo Sandbox;
1.3.2.2.31. Possibilitar a execução de aplicativos que precisam de privilégio de execução a usuários não-privilegiados;
1.3.2.2.32. Permitir criar uma whitelist, onde é configurado todos os aplicativos que podem ser executados e qualquer outra aplicação fora desta lista automaticamente seja bloqueada;
1.3.2.2.33. Possuir uma integração com Windows UAC, e conter relatórios do uso de prompts aos usuários feitos pelo UAC;
1.3.2.2.34. Suportar a guarda de políticas de hosts que não façam parte do Active Directory ii) Manter todas as políticas em cache e serem aplicadas ao endpoint, ainda que o mesmo não esteja conectado à rede corporativa;
1.3.2.2.35. Deve permitir que mensagens customizadas sejam mostradas antes que uma aplicação seja executada ou bloqueada;
1.3.2.2.36. Deve suportar adição múltiplas mensagens, estas mensagens devem possibilitar edição e suportar múltiplas linguagens;
1.3.2.2.37. Deve possuir capacidade de relatórios de aplicações e eventos de usuários inclusos na solução;
1.3.2.2.38. Realizar varredura e inventário de aplicações instaladas no sistema operacional;
1.3.2.2.39. Deve permitir a configuração de “iscas”, como senhas e credenciais falsas de administrador local para detecção de ataques em andamento e bloqueio proativo;

1.3.3. Solução de Segurança para Privilégios e Acessos – Proteção para Estações de Trabalho:
1.3.3.1. As funcionalidades devem ser instaladas no sistema operacional das estações de trabalho e permitir a proteção dos ativos;
1.3.3.2. As funcionalidades devem ser instaladas no sistema operacional das estações de trabalho e permitir o controle dos privilégios;
1.3.3.3. Garantir o controle e bloqueio de comandos, mesmo que o acesso seja realizado diretamente no servidor de destino (sem ser através dos monitores/gravadores de acessos);
1.3.3.4. Oferecer opções de execução sem aviso: de aplicações com privilégios em modo explícito e transparente, monitorada de aplicações em modo explícito e transparente, com restrições de aplicações em modo explícito e transparente;
1.3.3.5. Exibir a reputação do arquivo executado advinda de, pelo menos, 1 (uma) fonte externa e disponibilizar a opção de encaminhamento de arquivo suspeito para análise de malware em soluções de mercado;
1.3.3.6. Suportar, no mínimo, as versões de estações de trabalho: Windows XP SP3, Windows Vista SP1, Windows 7 x32 & x64, Windows 8/8.1 x32 & x64, Windows 10 x32 & x64, Windows 11 x32 & x64;
1.3.3.7. Implementar regras de controle de aplicações permitidas e bloqueadas para execução fazendo uso das funcionalidades instaladas no sistema operacional alvo, independentemente do acesso ao ativo ser realizado via monitores/gravadores de acessos ou diretamente no ativo;
1.3.3.8. Implementar regras de controle do nível de privilégio utilizado na execução das aplicações permitidas fazendo uso das funcionalidades instaladas no sistema operacional alvo, independentemente do acesso ao ativo ser realizado via monitores/gravadores de acessos ou diretamente no ativo;
1.3.3.9. Implementar controle de nível de privilégio independentemente da permissão que o usuário possua localmente no ativo ou no domínio, permitindo que usuários restritos executem atividades com nível administrativo;
1.3.3.10. Permitir atribuição granular para execução de aplicações com nível de privilégio administrativo, sem que esse privilégio seja global na máquina;
1.3.3.11. Fazendo uso das funcionalidades instaladas no sistema operacional alvo, deve permitir a criação de políticas reutilizáveis, contendo, no mínimo, os seguintes tipos de aplicações ou tipos de arquivos: executáveis, scripts, aplicações nativas Windows, bibliotecas dinâmicas (DLL), instaladores, controles ActiveX, objetos COM;
1.3.3.12. Implementar a verificação de checksum do arquivo, dos parâmetros permitidos e da assinatura de fabricante, para objetos reutilizáveis da solução;
1.3.3.13. Implementar o suporte ao nome exato da aplicação/arquivo/script e expressões regulares em qualquer formato, para objetos reutilizáveis da solução;
1.3.3.14. Utilizar eventos reportados na interface da ferramenta para criação de novas políticas ou incluí-los em políticas existentes;
1.3.3.15. Permitir agrupar aplicações com base em suas características, para facilitar a inserção de novas aplicações aos grupos ou políticas de segurança de aplicações já criadas;
1.3.3.16. Impedir a desativação das funcionalidades instaladas no sistema operacional alvo sem autorização e/ou registro da atividade por meio da interface de gerência;
1.3.3.17. Disponibilizar o registro das execuções e atividades dos usuários, facilitando a criação de políticas baseadas em comportamento conhecido;
1.3.3.18. Monitorar e exibir acessos e atividades realizadas na própria solução;
1.3.3.19. Deve permitir autorização de acesso às aplicações e arquivos, quando incluídos em regras, individualmente ou em grupos;
1.3.3.20. Deve realizar varreduras fazendo uso das funcionalidades instaladas no sistema operacional alvo para catalogar arquivos existentes nas máquinas e uni-los ao inventário populado mediante detecção durante a execução;
1.3.3.21. Deve verificar a reputação dos arquivos executados e detectados pelas funcionalidades instaladas no sistema operacional alvo ou órgãos de controle de ameaças, como por exemplo o VirusTotal.com ou similares;
1.3.3.22. Deve permitir a execução automática de tipos desconhecidos de arquivo, de acordo com sua origem, mesmo possuindo restrições;

1.3.3.23. Possibilitar o monitoramento e a criação de evidência em vídeo de certas execuções de arquivo e de execuções sob certas condições definidas em política;
1.3.3.24. Possibilitar ao usuário final a solicitação de liberação de atividades específicas fazendo uso das funcionalidades instaladas no sistema operacional alvo;
1.3.3.25. Possibilitar a liberação emergencial da execução de comandos e elevação de privilégios sem desativar a solução, caso o usuário esteja off-line;
1.3.3.26. Implementar as regras de controle de acordo com características do usuário final, incluindo nome de usuário, grupos a que o usuário pertence e endereço IP;
1.3.3.27. Oferecer monitoramento de atividade maliciosa dos processos em execução, visando detectar tentativas de roubo de credenciais;
1.3.3.28. Fazendo uso das funcionalidades instaladas no sistema operacional alvo, a solução deve alertar, reportar e bloquear atividade anômala de arquivos e usuários durante a interação com bases de senhas no formato hash, como por exemplo, SAM local e LSASS.
1.3.3.29. Caso o dispositivo não possa estar conectado de forma permanente aos monitores/gravadores de acessos da solução e repositório seguro de credenciais, deve, de forma autônoma e off-line, gerenciar as senhas das credenciais locais, aplicando políticas de randomização e sincronização das senhas definidas na central da solução;
1.3.3.30. Permitir o envio de arquivos suspeitos, executados sob sua supervisão, para soluções de análise de ameaça do tipo Sandbox;
1.3.3.31. Possibilitar a execução de aplicativos que precisam de privilégio de execução a usuários não-privilegiados;
1.3.3.32. Permitir criar uma whitelist, onde é configurado todos os aplicativos que podem ser executados e qualquer outra aplicação fora desta lista automaticamente seja bloqueada;
1.3.3.33. Possuir uma integração com Windows UAC, e conter relatórios do uso de prompts aos usuários feitos pelo UAC;
1.3.3.34. Suportar a guarda de políticas de hosts que não façam parte do Active Directory;
1.3.3.35. Manter todas as políticas em cache e serem aplicadas ao endpoint, ainda que o mesmo não esteja conectado à rede corporativa;
1.3.3.36. Deve permitir que mensagens customizadas sejam mostradas antes que uma aplicação seja executada ou bloqueada;
1.3.3.37. Deve suportar adição múltiplas mensagens, estas mensagens devem possibilitar edição e suportar múltiplas linguagens;
1.3.3.38. Deve possuir capacidade de relatórios de aplicações e eventos de usuários inclusos na solução;
1.3.3.39. Realizar varredura e inventário de aplicações instaladas no sistema operacional;
1.3.3.40. Deve permitir a configuração de “iscas”, como senhas e credenciais falsas de administrador local para detecção de ataques em andamento e bloqueio proativo;
1.3.3.41. A solução deverá ser capaz de atender minimamente os seguintes casos de uso para requisitar um e mais fatores de autenticação:
1.3.3.41.1. Nas telas de login e desbloqueio de sistemas operacionais Windows e MacOs;
1.3.3.41.2. Multi Fator de autenticação para soluções de VPN via RADIUS ou SAML;
1.3.3.41.3. Qualquer dispositivo ou sistema operacional que suporte RADIUS;
1.3.3.41.4. Plugin para ADFS (IDP, Identity Provider), Active Directory Federation Services;
1.3.3.41.5. Sob demanda utilizando o protocolo Oauth e REST APIs;
1.3.3.41.6. Para realizar o autosserviço de reset de senha ou desbloqueio de usuário;
1.3.3.42. A solução deverá ser capaz de oferecer minimamente os seguintes métodos para múltiplo fator de autenticação:
1.3.3.43. Usuário e senha dos diretórios suportados na solução:
1.3.3.43.1. Através de aplicativo para dispositivos móveis do tipo IOS e Android, oferecendo suporte para;
1.3.3.43.2. Biometria do tipo FaceID;
1.3.3.43.3. Biometria através do leitor de digital;
1.3.3.43.4. Smartphone push (Notificação para aprovar ou recusar uma autenticação);
1.3.3.43.5. Geolocalização através de coodernadas GPS e banco de dados de IPs;
1.3.3.43.6. Suporte a tokens OATH OTP;
1.3.3.43.7. Autenticação na tela de login via QRcode sem a necessidade de digitar usuário e senha, com opção de forçar a biometria no dispositivo móvel;
1.3.3.43.8. Confirmação de código via e-mail;
1.3.3.44. Clientes do tipo OATH OTP (exemplo, Google Authenticator);
1.3.3.45. Autenticadores que suportem FIDO2 / U2F, minimamente suportando:
1.3.3.45.1. Windows Hello;
1.3.3.45.2. Yubikey;
1.3.3.45.3. Google Titan Key;
1.3.3.45.4. MacOS TouchID;
1.3.3.46. Perguntas e respostas previamente configuradas;
1.3.3.47. Permitir que os usuários realizem o autosserviço de reset de senha e desbloqueio de usuário utilizando os métodos de múltiplo fator de autenticação citados para verificação positiva através do portal da solução, tela de login de sistemas operacionais Windows e através de REST APIs oferecidas pela solução;
1.3.3.48. Para cada caso de uso ou conjunto de casos de uso de múltiplo fator de autenticação citados, a solução de ser capaz de identificar os atributos de contexto de cada autenticação para disponibilizar os melhores métodos definidos para a autenticação, suportando minimamente:
1.3.3.48.1. Endereçamento IP;
1.3.3.48.2. Dia da Semana;
1.3.3.48.3. Datas específicas;
1.3.3.48.4. Janelas de tempo entre duas datas;
1.3.3.48.5. Janelas de tempo entre horários (exemplo, horário comercial);
1.3.3.48.6. Tipo do Sistema Operacional;
1.3.3.48.7. Tipo do Browser;
1.3.3.48.8. Perfis configurados na solução;
1.3.3.48.9. País que está sendo realizado o acesso;
1.3.3.48.10. Se é um dispositivo gerenciado;
1.3.3.48.11. Autenticação via certificado;
1.3.3.48.12. Nível de Risco da autenticação medido por um motor de análise de comportamento dos usuários;
1.3.3.49. A solução deve ter capacidade de detectar casos de uso e perfis de autenticação já validados pelo usuários e não requisitar mais os mesmos durante um período de tempo configurado pelo administrador da solução, evitando desta forma repetidas validações em um curto espaço de tempo;
1.3.3.50. O conjunto de fatores de autenticação disponibilizados devem ser baseados durante o acesso através de regras especificadas no item anterior e segregados por:
1.3.3.50.1. Conjunto de aplicações;
1.3.3.50.2. Uma única aplicação;
1.3.3.50.3. Regras para o autosserviço de reset de senha e desbloqueio de usuário;
1.3.3.50.4. Portal do Administrador;
1.3.3.50.5. Portal do Usuário;
1.3.3.51. A solução deve prover um aplicativo móvel para Android e IOS com as seguintes características:
1.3.3.51.1. Depois de efetuado o login apresentar as aplicações WEB disponíveis para realizar o SSO, através de um conjunto de ícones onde cada um representa uma aplicação que o usuário tem o direito de efetuar o SSO já integrado com os navegadores instalados nos dispositivos móvel;
1.3.3.51.2. Prover login através do scan de QRcode no portal web permitindo SSO sem identificação de usuário e senha;
1.3.3.51.3. Configurar OATH OTP adicionais provenientes de outras soluções;
1.3.3.51.4. Configurar OATH OTP para autenticação multi fator nos sistemas operacionais Windows (telas de login e bloqueio) quando os mesmos estão desconectados da internet;
1.3.3.51.5. Verificar dispositivos registrados (dispositivos móveis e sistemas operacionais);
1.3.3.51.6. Integração nativa com FaceID, TouchID, leitor biométrico dos dispositivos móveis alavancando os mesmos para autenticação biométrica durante login nas aplicações;
1.3.3.51.7. Reportar coordenadas GPS para os sistemas que utilizam geolocalização;

1.3.3.52. O aplicativo deve suportar autenticação do tipo push, onde o usuário tem a escolha de aceitar ou recusar o desafio, esta notificação de conter minimamente: IP de origem de acesso, Data e Hora, Cidade / Geolocalização do acesso, Aplicação sendo acessada;
1.3.3.53. A solução dever ser baseada em algoritmos de aprendizado de máquina (Machine Learning) não supervisionados, ou seja, os modelos estatísticos com os casos de uso já prontos e calibrados;
1.3.3.54. A solução deve medir o risco da autenticação verificando o comportamento histórico da identidade através do conjunto dos seguintes atributos;
1.3.3.55. Geo Velocidade, medindo velocidade de deslocamento do login, comparando a localização do último login com a atual, evitando "viagens impossíveis", e traçando o comportamento do usuário neste quesito, por exemplo, pessoas que viajam muito podem ter uma pontuação de risco baixa mesmo que sua Geo Velocidade seja maior que pessoas que não viajam;
1.3.3.56. Geo Localização: medindo o risco da autenticação verificando sua localização geográfica do acesso atual em comparação com o seu comportamento usual;
1.3.3.57. Dia da Semana: medindo o risco da autenticação verificando o dia da semana do acesso atual em comparação com seu comportamento usual;
1.3.3.58. Horário do Acesso: mede o risco da autenticação verificando o horário do acesso atual em comparação com seu comportamento usual;
1.3.3.59. Sistema Operacional: mede o risco da autenticação verificando o Sistema Operacional do acesso atual em comparação com seu comportamento usual;
1.3.3.60. Falhas de login consecutivas, mede o risco da autenticação verificando as falhas de login consecutivas do acesso atual em comparação com seu comportamento usual iii) Deve prover a personalização das faixas de pontuação (0 a 100) para os administradores da solução para, no mínimo, as categorias: Sem risco, Risco Baixo, Risco Médio e Risco Alto;
1.3.3.61. Deve prover para os administradores da solução a personalização da influência na medição do risco para cada atributo citado neste item. Por exemplo, para a CONTRATANTE a geo velocidade pode ser um fator que não possui relevância, desta forma deve ser possível configurar a influência deste risco como baixa na modelagem de risco da plataforma;
1.3.3.62. O risco calculado durante a autenticação pelo motor de análise do comportamento dos usuários deve ser compartilhado com funções de Múltiplo Fator de autenticação e Single Sign-On que realizam o login para os casos de uso citados neste documento e utilizar como contexto para:
1.3.3.62.1. Requisitar múltiplos fatores de autenticação de forma dinâmica;
1.3.3.62.2. Permitir o login sem o uso de múltiplos fatores;
1.3.3.62.3. Negar a autenticação;
1.3.3.63. Deve prover para os administradores da solução a capacidade de explorar os dados históricos através de dashboards, filtros e gráficos configuráveis sendo possível verificar os alertas e os fatores que os influenciaram, além da exploração dos eventos capturados e seus atributos;
1.3.3.64. Deve prover gráficos de linha do tempo, donuts, mapas com geolocalização dos eventos, gráfico de barras, tabelas analíticas, e mapas de relacionamento, sendo suas dimensões e categorias personalizáveis;
1.3.3.65. Deve ser capaz de exportar os dados dos alertas, riscos calculados, eventos para, no mínimo, CSV, adicionalmente gravar as visualizações na solução para consultas posteriores;
1.3.3.66. Deve possuir integração com fontes de inteligência cibernética de terceiros reconhecidas no mercado, como, por exemplo, Palo Alto Cloud;
1.3.3.67. Deve possuir interface para envio de alertas de forma automatizada, suportando, no mínimo E-mail com conteúdo do alerta e Webhooks (ex: envio de mensagem para um canal do Microsoft Teams ou Slack;
1.3.3.68. Possuir dashboards pré-configurados com informações e gráficos com as seguintes características:
1.3.3.68.1. Utilização do Motor de Análise do Comportamento dos Usuários;
1.3.3.68.2. Comportamento dos usuários na utilização das aplicações;
1.3.3.68.3. Visão sobre a segurança das aplicações;
1.3.3.68.4. Mapa com a geolocalização das autenticações;
1.3.3.68.5. Visão sobre o comportamento dos Endpoints (Mobile e Computadores);
1.3.3.68.6. Visão sobre o comportamento das Identidades;

1.3.4. Serviço especializado para implementação, configuração e transferência de conhecimento da solução de Segurança para Sistemas Críticos:
1.3.4.1. O serviço de implementação e configuração deve ser executado em até 30 dias após a instalação da solução no ambiente do TJAM;
1.3.4.2. O serviço de transferência de conhecimento abrange, entre outras, as seguintes atividades:
1.3.4.2.1. Elaboração de documentação técnica e de usuário;
1.3.4.2.2. Transferência de conhecimentos relacionados ao desenvolvimento, implantação e manutenção no ambiente do TJAM;
1.3.4.2.3. Levantamento de informações junto aos usuários, objetivando a definição e elaboração de regras e políticas;
1.3.4.2.4. Corrigir ou apoiar em problemas e defeitos em funcionalidades já existentes;
1.3.4.2.5. Realização de operação assistida e monitoramento de ambientes entregues com a solução;
1.3.4.2.6. Orientar na utilização dos softwares instalados no TJAM com a utilização das melhores práticas e orientações dos fabricantes;
1.3.4.2.7. Apoiar na atualização, instalação e/ou reinstalação de novas versões e dos produtos instalados no TJAM minimizando impactos;
1.3.4.2.8. Apoiar na configuração/parametrização do sistema em novas máquinas;
1.3.4.2.9. Orientar no levantamento de informações que possibilite a identificação de novas necessidades, detectadas no ambiente do TJAM;
1.3.4.2.10. Diagnosticar o bom funcionamento das ferramentas instaladas, garantindo a máxima utilização dos recursos oferecidos;
1.3.4.2.11. Identificar e elaborar proposição de melhoria em performance, desempenho, tunning, disponibilidade e confiabilidade em ambientes;
1.3.4.2.12. Otimizar a reinstalação e/ou adaptação das ferramentas em outros equipamentos que não seja onde originalmente os sistema e produtos foram instalados;
1.3.4.2.13. Definir metodologia, elaborar relatórios e projetos e acompanhar a configuração e utilização de solução de alta disponibilidade, repassando aos técnicos da TI do TJAM as melhores práticas para uso da solução, quanto a parametrização e configuração dos componentes e ferramentas utilizadas no TJAM;
1.3.4.2.14. Esclarecer dúvidas e orientar os técnicos de TI do TJAM, sobre integração das soluções, abrangendo as diversas plataformas existentes no ambiente computacional do TJAM;
1.3.4.2.15. Apoiar no planejamento, na execução e na avaliação das mudanças no ambiente;
1.3.4.2.16. Analisar patches, correções e novas versões e sugerir a aplicação ou não dos mesmos no ambiente;
1.3.4.2.17. Apoiar no planejamento, na execução e na avaliação das atualizações de versões e aplicação de patches da ferramenta;
1.3.4.2.18. Apoiar no planejamento, na execução e na avaliação de implantação de novas aplicações ou atualização de aplicações no ambiente;
1.3.4.2.19. Efetuar a transferência de tecnologia para a equipe do TJAM;

1.3.5. Solução de segurança para identidades e acessos – Proteção para Aplicações Tradicionais

1.3.5.1 Uma aplicação gerenciada é definida como a aplicação que faz uso direto dos recursos e credenciais gerenciadas pela solução para concessão de acesso ao seu ambiente (substituindo o uso de credenciais hard coded, por exemplo).

1.3.5.2 Deve permitir a integração de servidores de aplicação e o repositório digital seguro, eliminando a necessidade de senhas e chaves SSH embutidas em aplicações, scripts e arquivos de configuração.

1.3.5.3 Deve possuir mecanismo de segurança que evite a parada de aplicações críticas, mantendo a entrega das credenciais em caso de queda da rede ou parada total da solução que gerencia as credenciais por meio do repositório seguro.

1.3.5.4 Deve fornecer credenciais, pelo menos, via consulta de rede ou Web service.

1.3.5.5 Deve garantir a entrega de credenciais localmente nos servidores de aplicação, garantindo baixa latência para aplicações de missão crítica.

1.3.5.6 Deve manter um cache local atualizado das credenciais utilizadas no servidor de aplicação, a fim de prevenir falhas na comunicação com o repositório seguro e trazer velocidade às consultas

1.3.5.7 Deve suportar redundância de credenciais, oferecendo, de maneira transparente, mais de um usuário e senha à aplicação crítica, de forma que se evite qualquer possível indisponibilidade mínima durante o processo de troca de senhas;

1.3.5.8 Deverá oferecer SDKs documentados para integração com aplicações em Java, C/C++ e .Net

1.3.5.9 Deverá suportar a utilização de executável para scripts e aplicações nativas em plataforma Windows

1.3.5.10 Deverá suportar a utilização integração com servidores WebSphere, WebLogic, JBoss e Tomcat, para fornecimento de credenciais via XML datasources

1.3.5.11 Deverá suportar a autenticação de aplicações que consultam credenciais, permitindo definir o caminho da aplicação, usuário do sistema operacional, endereço do servidor e hash do código.

1.3.5.12 Ser disponibilizada com um SDK (Software Development Kit) que pode ser configurado para permitir que aplicações possam Solicitar as credenciais sob demanda, ao invés de utilizar credenciais estáticas;

1.3.5.13 Atualizar informações de contas automaticamente no banco de dados de senhas;

1.3.5.14 Inscrever automaticamente dispositivos alvo, sem aguardar por atualizações dinâmicas;

1.3.5.15 Alterar senhas em texto claro (incorporado em aplicações), de forma segura no banco de dados de senhas;

1.3.5.16 Visando a garantia do funcionamento da solução como um todo, este item deve ser entregue com total integração com o item 1 desta especificação.

1.4. Caracterização do Objeto:

1.4.1. O objeto desta contratação enquadra-se no conceito de bens e serviços comuns, trazido no inciso XIII do art. 6º, da Lei nº 14.133/21.

1.5. Fundamentação Legal:

1.5.1. A contratação para a execução das obras e serviços deverá obedecer, no que couber, ao disposto na legislação a seguir:

a) Lei nº 14.133, de 1º de abril de 2021;

b) Resolução n.º 64/2023, de 5 de dezembro de 2023;

c) Decreto 10.222, de 5 de fevereiro de 2020;

d) Lei 13.709, de 14 de agosto de 2018;

e) Resolução nº 370 de 28/01/2021;

f) Resolução CNJ nº 396 de 07/06/2021;

g) Resolução CNJ nº 468, de 15 de julho de 2022.

1.6. Indicação de necessidade de apresentação de amostras, catálogos, manuais, folders ou prospectos:

1.6.1. Deverá ser apresentado catálogo, folder, manual ou sítio da internet que comprove que todos os materiais e equipamentos a serem utilizados atendem rigorosamente as especificações técnicas mínimas exigidas.

1.6.2. A Divisão de Tecnologia da Informação e Comunicação do TJAM, sito a Avenida André Araújo s/n, Prédio Desembargador Arnoldo Péres - Bairro Aleixo – CEP 69.060-000 será a responsável por receber e validar os objetos desta contratação.

1.7. Valor estimado da contratação:

1.7.1. A estimativa de valor da contratação será discriminada no Mapa de Preços a ser elaborado pela Divisão de Compras e Operações.

1.7.2. Tabela exemplificativa de cotação:

Item	Descrição	Unid	Qnt Total	Preço (R$)	
				Unit	Total
1	Solução de Segurança para Identidades e seus Privilégios – Monitoramento de comportamento e mitigação de riscos de usuários administradores da TI, com garantia pelo período de 12 (doze) meses..	Unidades	75	R$	R$
2	Solução de Segurança para Identidades e seus Privilégios – Proteção para Aplicações Tradicionais, com garantia pelo período de 12 (doze) meses.	Unidades	40	R$	R$
3	Solução de Segurança para Identidades e seus Privilégios – Proteção Local para ervidores Windows e Linux, com garantia pelo período de 12 (doze) meses.	Unidades	400	R$	R$
4	Solução de Segurança para Identidades e seus Privilégios – Proteção Local para Estações de Trabalho, com garantia pelo período de 12 (doze) meses.	Unidades	3500	R$	R$
5	Serviço de instalação e configuração para Solução de Segurança para Identidades e seus Privilégios.	Unidades	1	R$	R$
6	Transferência de Conhecimento para Solução de Segurança para Identidades e seus Privilégios (turma)	Unidades	2	R$	R$
7	Serviço de Suporte Técnico Especializado	Mês	12	R$	R$
	Valor Estimado Total				R$

1.8. Adequação orçamentária:

1.8.1. A contratação pretendida está prevista no Plano de Contratação Anual 2024, sob o código: **SETIC-2024-25.**

2. CONDIÇÕES GERAIS DA CONTRATAÇÃO

2.1. O objeto deste Termo de Referência caracteriza-se como Licitação, na modalidade Pregão, conforme inciso I do artigo 28, da Lei nº 14.133/2021.

2.2. A presente contratação adotará a forma de execução indireta, no regime de empreitada por preço unitário.

2.3. O procedimento para a contratação pretendida neste instrumento **será** regido pelo Sistema de Registro de Preços.

2.4. O critério de julgamento da contratação será o de **MENOR PREÇO GLOBAL**.

2.5. O critério de adjudicação da contratação será GLOBAL, levando em consideração o prejuízo de ordem técnica que poderia ocorrer caso os serviços fossem prestados por diferentes empresas, uma vez que os serviços a serem contratados guardam estreita relação entre si e dependem de forte integração para que sejam efetivos e alcancem os resultados pretendidos.

2.6. Da Subcontratação:

2.6.1. Não será permitida a subcontratação do objeto deste Termo de Referência.

3. REQUISITOS DO FORNECEDOR

3.1. O fornecedor será selecionado por meio da realização de procedimento de LICITAÇÃO, na modalidade PREGÃO.

3.2. Vistoria:

3.2.1. As interessadas poderão realizar, sob o acompanhamento de servidor especialmente designado, vistoria aos locais de execução dos serviços, no todo ou em parte, em data e horário previamente acordados segundo a conveniência deste Órgão, com o objetivo de conhecer as instalações onde serão executados os serviços e sanar as dúvidas porventura existentes, a fim de subsidiar a elaboração das propostas a serem submetidas ao certame**.**

3.2.2. As visitas deverão ser previamente agendadas, com 72 (setenta e duas) horas de antecedência, pelo telefone (92) 2129-6779 – DIVISÃO DE INFRAESTRUTURA DE TECNOLOGIA DA INFORMAÇÃO E COMUNICAÇÃO, no período das 8 às 14hs, ou via e-mail através de: infra.tic@tjam.jus.br.

3.3. Qualificação Técnica:

3.3.1. A capacidade técnica da licitante será aferida mediante:

a) Apresentação de documento declarando ter capacitação técnica para atender a todos os requisitos especificados no Termo de Referência;

b) Declaração de que atende aos requisitos de habilitação e qualificação exigidas, de acordo com o art. 92, inciso XVI, da Lei n. 14.133/2021;

c) Comprovação de aptidão para o fornecimento de serviços de complexidade tecnológica e operacional similares com o objeto desta contratação, por meio da apresentação de certidões ou atestados, por pessoas jurídicas de direito público ou privado.

3.3.2. O(s) atestado(s) apresentado(s) poderão ser objeto de diligência a critério da Administração, para a verificação da autenticidade do conteúdo.

3.3.3. Deverão ser disponibilizadas todas as informações necessárias à comprovação da legitimidade dos atestados apresentados, informando, dentre outros dados, endereço atual do emissor do documento do atestado, bem como o local e data em que foram prestados os serviços ou realizada a execução do objeto.

4. MODELO DE GESTÃO

4.1. A execução dos serviços será acompanhada e fiscalizada pela Secretaria de Tecnologia da Informação e Comunicação.

4.1.1. A execução do objeto deverá ser acompanhada e fiscalizada por servidor designado como responsável ou por seu substituto.

4.1.2. A Fiscalização anotará em registro próprio, todas as ocorrências relacionadas à execução do contrato, determinando o que for necessário à regularização das faltas ou defeitos observados.

4.1.3. As decisões e providências que ultrapassem a competência da Fiscalização deverão ser solicitadas aos seus superiores para adoção das medidas convenientes.

4.2. À Fiscalização fica assegurado o direito de rejeitar os serviços que não satisfaçam aos padrões especificados e melhores práticas de mercado.

4.2.1. A existência da fiscalização de nenhum modo diminui ou altera a responsabilidade do fornecedor na total execução do objeto.

4.2.2. A CONTRATADA deverá manter preposto, aceito pela CONTRATANTE, durante o período de vigência do contrato, para representá-la sempre que for necessário. Despesas relativas ao preposto serão de exclusiva responsabilidade da CONTRATADA

4.2.3. 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 (e-mail) para esse fim.

4.2.4. A CONTRATADA deverá disponibilizar canais de comunicação, tais como número de telefone, endereço de correio eletrônico ou plataforma de abertura de chamados para atendimento de suporte técnico e consultoria.

4.3. Indicação de instrumento para efetivar a contratação:

4.3.1. Será necessária a formalização de Ata de Registro de Preços.

4.3.2. O prazo de vigência da ata de registro de preços será de 1 (um) ano e poderá ser prorrogado, por igual período, desde que comprovado o preço vantajoso.

4.3.3. Os órgãos e entidades poderão aderir à ata de registro de preços na condição de não participantes, observados os seguintes requisitos:

I - apresentação de justificativa da vantagem da adesão, inclusive em situações de provável desabastecimento ou descontinuidade de serviço público;

II - demonstração de que os valores registrados estão compatíveis com os valores praticados pelo mercado;

III - prévias consulta e aceitação do órgão ou entidade gerenciadora e do fornecedor.

4.3.4. A faculdade de aderir à ata de registro de preços na condição de não participante poderá ser exercida:

I - por órgãos e entidades da Administração Pública federal, estadual, distrital e municipal, relativamente a ata de registro de preços de órgão ou entidade gerenciadora federal, estadual ou distrital; ou

4.3.5. As aquisições ou as contratações não poderão exceder, por órgão ou entidade, a 50% (cinquenta por cento) dos quantitativos dos itens do instrumento convocatório registrados na ata de registro de preços para o órgão gerenciador e para os órgãos participantes.

4.3.6. O quantitativo decorrente das adesões à ata de registro de preços não poderá exceder, na totalidade, ao dobro do quantitativo de cada item registrado na ata de registro de preços para o órgão gerenciador e órgãos participantes, independentemente do número de órgãos não participantes que aderirem.

4.4. Será necessária a formalização de contrato para a execução do serviço objeto desse termo.

4.4.1. Após a assinatura do contrato, 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.

4.5. Vigência contratual:

4.5.1 A vigência do contrato a ser firmado será de 12 (doze) meses, podendo ser prorrogado na forma do art. 111 da Lei nº 14.133/21.

4.5.2. Os itens 5 e 6 serão contratados por escopo e os demais itens serão contínuos. Os itens 5 e 6 não serão solicitados na prorrogação contratual.

4.6. Índice de reajuste:

4.6.1. Os preços contratados poderão ser reajustados, após solicitação da CONTRATADA, observado o interregno mínimo de 12 (doze) meses, tendo como limite máximo a variação do Índice de Custos de Tecnologia da Informação - ICTI, ocorrida nos últimos 12 (doze) meses.

4.6.2. O interregno mínimo de 12 (doze) meses será contado a partir da data orçamento estimado, assim considerada a data de conclusão da apuração do valor estimado da contratação, ou, da planilha orçamentária, independentemente da data da tabela ou sistema referencial de custos utilizado.

4.6.3. Nos reajustamentos subsequentes ao primeiro, o interregno mínimo de 12 (doze) meses será contado da data de início dos efeitos financeiros do último reajustamento ocorrido.

4.6.4. O reajuste deverá ser solicitado antes do término da atual vigência do Contrato, sob pena de preclusão.

5. OBRIGAÇÕES DA CONTRATADA E DO CONTRATANTE.

5.1. São obrigações e responsabilidades do CONTRATANTE:

5.1.1. Promover o cumprimento do Contrato e prover documentos necessários para sua execução.

5.1.2. Dirimir eventuais dúvidas da CONTRATADA referentes aos serviços, Notas de Empenho etc.

5.1.3. Comunicar oficialmente à CONTRATADA quaisquer problemas verificados na execução dos serviços, Notas de Empenho e etc.

5.1.4. Permitir acesso dos funcionários da CONTRATADA às suas dependências para a execução dos serviços.

5.1.5. Recusar qualquer material ou serviço entregue em desacordo com o especificado ou fora das condições contratuais ou do bom padrão de qualidade.

5.1.6. Determinar à CONTRATADA a substituição de qualquer profissional vinculado a esta, cuja atuação, permanência ou comportamento sejam considerados prejudiciais, inconvenientes ou insatisfatórios à disciplina da repartição ou ao interesse da Administração Pública.

5.1.7. Certificar-se de efetuar os pagamentos devidos, nos termos estabelecidos.

5.1.8. Designar servidor para acompanhar e fiscalizar a execução do objeto.

5.1.9. Designar, e informar à CONTRATADA, o fiscal do contrato e seu substituto, mantendo tais dados atualizados.

5.1.10. Acompanhar e fiscalizar, como lhe aprouver e no seu exclusivo interesse o exato cumprimento das cláusulas e condições contratuais e editalícias.

5.1.11. Providenciar a aplicação das sanções administrativas à CONTRATADA quando couber em face dos termos do Contrato e das Leis Vigentes.

5.1.12. Os serviços não aceitos pela fiscalização deverão ser refeitos pela CONTRATADA sem nenhum ônus adicional para o Tribunal de Justiça do Estado do Amazonas.

5.1.13. Manter sigilo e confidencialidade de todas as informações – em especial os dados pessoais e os dados pessoais sensíveis – repassados em decorrência da execução contratual, em consonância com o disposto na Lei n. 13.709/2018 (Lei Geral de Proteção de Dados Pessoais - LGPD).

5.2. São obrigações e responsabilidades da CONTRATADA:

5.2.1. Manter durante a execução do CONTRATO as condições de habilitação e de qualificação que ensejaram sua contratação;

5.2.2. Executar o objeto desta contratação, atendendo às especificações estabelecidas neste Termo de Referência e as quantidades indicadas no instrumento contratual.

5.2.3. Assumir a responsabilidade por todas as providências e obrigações estabelecidas na legislação específica de acidentes de trabalho quando, em caso de ocorrência, forem vítimas seus empregados no desempenho dos serviços ou em conexão com eles, ainda que ocorridos nas dependências do CONTRATANTE.

5.2.4. Atender aos requisitos da Legislação Ambiental vigente quanto à armazenagem, emissões diversas, manuseio e descarte de resíduos que possam ser gerados quando da execução dos serviços, dando a devida destinação.

5.2.5. Providenciar às suas expensas, qualquer cópia de documento que venha a ser necessários, não só para licitação como para assinatura do Contrato e execução dos serviços.

5.2.6. Comunicar à Fiscalização em até 24 horas sempre que ocorrerem falhas, erros ou omissões nas especificações e demais elementos técnicos, assumindo integral responsabilidade pela correta execução de todos os serviços. As correções que forem necessárias somente serão efetuadas com a aprovação da Fiscalização, que por sua vez consultará os autores dos projetos para efeito de autorização.

5.2.7. Primar pelo bom planejamento das atividades, utilizar as boas práticas e técnicas de governança, avaliar previamente a viabilidade técnica, os riscos e os impactos de suas ações.

5.2.8. Facilitar a ação da Fiscalização na inspeção da execução dos serviços em qualquer dia ou hora, prestando todas as informações e esclarecimentos solicitados, inclusive de ordem administrativa.

5.2.9. Reparar, corrigir, remover, reconstruir ou substituir, total ou parcialmente, às suas expensas, o resultado dos serviços objeto do Contrato em que se verifiquem vícios, defeitos ou incorreções, resultantes de execução irregular, do emprego de materiais ou equipamentos inadequados ou não, correspondentes às especificações.

5.2.10. Manter permanentemente no local da execução dos serviços equipe técnica suficiente, composta de profissionais habilitados e de capacidade comprovada que assuma perante a fiscalização, a responsabilidade técnica dos mesmos até a entrega DEFINITIVA, inclusive com poderes para deliberar sobre qualquer determinação de emergência que se torne necessária.

5.2.11. Refazer os trabalhos recusados pela equipe de FISCALIZAÇÃO do TJAM em tempo acordado com a fiscalização a contar da notificação.

5.2.12. Manter todos os empregados devidamente uniformizados e com identificação apropriada, quando em acesso às dependências da contratante.

5.2.13. Possuir mão de obra qualificada e especializada para a perfeita execução do objeto, conforme especificado neste Termo de Referência e seus anexos, dimensionada de forma a cumprir os prazos estabelecidos.

5.2.14. Deverá designar responsável técnico pela execução do objeto.

5.2.15. Designar formalmente um preposto para lhe representar frente à Administração, em estrita observância ao Capítulo III do Código Civil Brasileiro (“Dos Prepostos”), ao art. 118 da Lei 14.133/2021, e demais regulamentos aplicáveis.

5.2.16. É expressamente vedada à CONTRATADA a veiculação de publicidade acerca da contratação, salvo se houver prévia autorização do CONTRATANTE.

5.2.17. São expressamente vedadas à CONTRATADA a contratação de servidor pertencente ao quadro de pessoal do CONTRATANTE para qualquer serviço, durante a vigência do Contrato.

5.2.18. Responsabilizar-se única e exclusivamente pelo pagamento de todos os encargos e demais despesas, diretas ou indiretas, decorrentes da execução do objeto do presente Termo de Referência, tais como impostos, taxas, contribuições fiscais, previdenciárias, trabalhistas, fundiárias; enfim, por todas as obrigações e responsabilidades, sem qualquer ônus adicional ao CONTRATANTE.

5.2.19. Cumprir os normativos e os procedimentos definidos pelo CONTRATANTE.

5.2.20. Realizar os serviços em conformidade com os horários e períodos determinados pelo CONTRATANTE.

5.2.21. Tratar todas as informações a que tenha acesso, em caráter de estrita confidencialidade, não podendo, sob qualquer pretexto, divulgar, revelar, reproduzir, ou delas dar conhecimento a terceiros estranhos a esta contratação, bem como utilizá-las para fins diferentes dos previstos na presente contratação.

5.2.22. Acatar as determinações feitas pela fiscalização do CONTRATANTE no que tange ao cumprimento do objeto do contrato.

5.2.23. Prestar, de imediato, todos os esclarecimentos solicitados pela fiscalização do CONTRATANTE no que diz respeito a execução do objeto contratado.

5.2.24. Selecionar e escalar os profissionais capacitados para a realização dos serviços.

5.2.25. Responsabilizar-se por danos causados ao patrimônio do CONTRATANTE, ou de terceiros, ocasionados por seus profissionais, em virtude de dolo ou culpa, durante a execução do objeto contratado.

5.2.26. A contratada deverá garantir as melhores práticas relacionadas à Segurança da Informação e à Lei Geral de Proteção de Dados Pessoais (LGPD), principalmente, no que diz respeito aos dados pessoais tratados durante a configuração dos privilégios.

5.2.27. A contratada durante a execução do objeto, deve implementar medidas técnicas e administrativas adequadas para proteger os dados pessoais contra acessos não autorizados.

5.2.28. Será exigido da Contratada que cada profissional que venha a prestar serviços assine um termo de compromisso, pelo qual se comprometerá a manter o sigilo das informações.

5.2.29. A Contratada deverá manter sigilo absoluto a respeito de quaisquer dados, informações e artefatos, contidos em documentos e mídias de que venha a ter conhecimento durante a execução dos trabalhos, não podendo, sob qualquer pretexto, divulgar, reproduzir ou utilizar, sob pena de aplicação das sanções cabíveis, além do pagamento de indenização por perdas e danos, independentemente da classificação de sigilo conferido pelo TJAM a tais documentos.

6. REGIME DE EXECUÇÃO

6.1. A Contratada deverá instalar e configurar os serviços nas dependências do TJAM e/ou remotamente de modo a viabilizar a execução do objeto.
6.1.1. Se houver necessidade ou risco de interrupção do serviço, a implantação deverá ser realizada em horário específico a ser indicado pela Divisão de Infraestrutura de TIC, podendo ser realizada em finais de semana ou feriados, sem qualquer custo adicional para o TJAM.

6.1.2. Os trabalhos serão coordenados e acompanhados por técnicos do TJAM e deve haver repasse de conhecimento durante a execução dos serviços.

6.1.2.1. A transição contratual com transferência de conhecimento, tecnologia e técnicas empregadas promove uma relação mais transparente e colaborativa entre as partes envolvidas. Ao adquirir o conhecimento e expertise, o órgão e setor responsável pelo mantenimento das operações demonstram comprometimento e responsabilidade com o sucesso do projeto, fortalecendo a confiança de autonomia na execução de atividades com complexidade aceitável, minimizando o tempo de espera e retorno às operações em caso de interrupções.

6.1.2.2. A transferência de conhecimento é essencial para garantir a continuidade das operações e a qualidade dos serviços prestados. Ao compartilhar informações relevantes sobre processos, metodologias e expertise acumulada durante a execução do contrato, torna-se capaz de assegurar que o órgão CONTRATANTE esteja plenamente capacitado para dar continuidade às atividades, minimizando qualquer interrupção ou perda de eficiência.

6.1.2.3. Ainda dentro da necessidade de aprendizado e absorção de conhecimento, a transferência de tecnologia e técnicas empregadas é crucial para manter o progresso e o desenvolvimento do projeto ou serviço contratado. Ao repassar as ferramentas e os métodos utilizados, nos é possibilitado que possamos explorar plenamente os recursos e obter resultados satisfatórios. Isso também contribui para a autonomia da contratante no futuro, permitindo que ela faça melhorias e adaptações de acordo com as necessidades específicas.

6.1.3. Para efeitos de aceite definitivo, a conclusão dos serviços de instalação e configuração será dada pela entrega da solução adquirida em pleno funcionamento, de acordo com as especificações.
6.1.4. No caso de serviços sob demanda, o prazo de entrega será aquele definido nas Ordens de Serviço.

6.2. Local e Prazos de Execução:

6.2.1. Em até 10 (dez) dias corridos, contados da assinatura do contrato, recebimento da Nota de Empenho e da Ordem de Serviço.

6.2.2. A CONTRATADA deverá entregar um projeto executivo para a implantação dos serviços contendo no mínimo:

6.2.2.1. Responsável pela implantação.

6.2.2.2. Cronograma de implantação.

6.2.2.3. Cronograma de reuniões de acompanhamento.

6.2.3 A CONTRATADA deverá concluir os serviços de instalação e ativação de todo o objeto nos seguintes prazos:

6.2.3.1. Em até 30 (trinta) dias corridos, contados da entrega do projeto executivo pela CONTRATADA.

6.2.3.2. Durante a implantação, independente da periodicidade das reuniões de acompanhamento, a CONTRATADA deverá apresentar semanalmente relatórios do andamento das ações previstas no cronograma.

6.2.3.3. Os desalinhamentos no cronograma que possam comprometer as datas previstas para as entregas devem ser informados a CONTRATANTE a fim de buscar alternativas de remediação dos problemas.

6.2.3.4. Considera-se o serviço ativado quando, após comunicação oficial da CONTRATADA informando a efetiva instalação, configuração e disponibilização do serviço, for realizado teste de conectividade pelos técnicos da CONTRATANTE, identificado o atendimento de todos os requisitos técnicos para os links, inclusive de monitoração.

6.2.3.5. O não cumprimento dos prazos e das condições de entrega dos serviços sujeitará a CONTRATADA às sanções administrativas previstas no Termo de Referência.

6.3**.** Forma de Execução dos serviços:

6.3.1 A execução dos serviços será sob demanda, no regime de empreitada por preço unitário.

6.3.2. Todos os itens serão atendidos por fornecedor único, uma vez que os serviços pretendidos estão intrinsecamente relacionados. A adjudicação dos itens para empresas diferentes poderia resultar na aquisição de soluções incompatíveis, o que acarretaria prejuízo à CONTRATANTE.

6.4. Previsão dos Recursos:

6.4.1. Para a execução dos serviços de instalação e configuração, a licitante Contratada deverá alocar profissionais devidamente habilitados pelo fabricante.

6.4.2 A licitante deverá apresentar, no mínimo, um profissional certificado, dentro da equipe que irá executar os serviços.

6.5. O objeto deste Termo de referência será recebido da seguinte forma:

6.5.1. **Provisoriamente**, no prazo máximo de 30 dias úteis após a entrega e configuração inicial dos produtos para posterior averiguação.

6.5.2. **Definitivamente**, no prazo máximo de 30 dias úteis a contar da data de emissão do termo de recebimento provisório.

6.5.3. O objeto será recusado caso não atenda as especificações técnicas solicitadas no Termo de Referência, devendo a contratada providenciar os ajustes necessários para adequação dos serviços, em um prazo de 10 (dez) dias contados a partir da comunicação do contratante, quando do não aceite.

6.5.4. A fiscalização não efetuará o ateste da última e/ou única medição de serviços até que sejam sanadas todas as eventuais pendências que possam vir a ser apontadas no Recebimento Provisório.

6.5.5. O recebimento provisório ou definitivo não excluirá a responsabilidade civil pela solidez e pela segurança do serviço nem a responsabilidade ético-profissional pela perfeita execução do contrato.

6.6. Garantia ou Assistência Técnica:

6.6.1. Cada produto deverá ser entregue ao TJAM na sua versão e release mais recente e durante a vigência do contrato deverá ser atualizado sem custo adicional.

6.6.2. A contratada deve possuir contrato de representante do fornecedor da solução.

6.6.3. Para a solução envolvida na contratação, a Contratada deverá prever garantia dos produtos, durante a vigência do contrato, a partir da data de sua ativação, fornecendo sem custo adicional todos os ajustes às falhas que porventura forem encontradas. Garantia integral durante 12 (doze) meses, “on-site” com atendimento vinte e quatro horas por dia e sete dias por semana, a contar da data de homologação do produto, contra qualquer defeito ou problema em toda a solução.

6.6.4. A Contratada, durante o período de garantia, se obriga ao fornecimento dos componentes de software, para manutenções, update de produtos, suporte técnico ou ampliações, de forma que possam ser mantidas todas as funcionalidades inicialmente contratadas. Caso haja neste período a descontinuidade de fabricação dos componentes, deve ser também garantida à total compatibilidade dos itens substitutos com os originalmente fornecidos.

7. PENALIDADES POR DESCUMPRIMENTO CONTRATUAL

7.1. Serão aplicadas as seguintes sanções no caso de descumprimento total ou parcial das regras estabelecidas no edital de licitação e/ou contrato:

a) advertência;

b) multa;

c) impedimento de licitar e contratar;

d) declaração de inidoneidade para licitar ou contratar.

7.2. As sanções de advertência, impedimento de licitar e contratar e declaração de inidoneidade para licitar ou contratar poderão ser aplicadas cumulativamente com a sanção de multa.

7.3. A sanção de impedimento de licitar e contratar com o ente federativo não poderá ser aplicada cumulativamente com a de declaração de inidoneidade.

7.4. A aplicação das sanções acima previstas não exclui a obrigação de reparação integral do dano causado à administração pública.

8. ADOÇÃO DE IMR OU ANS

8.1. Os serviços deverão ser prestados tendo sua qualidade medida por meio de Acordo de Nível de Serviço – ANS.

8.2. Havendo qualquer interrupção no funcionamento da solução o TJAM efetuará abertura de chamado reportando todos os sintomas.

8.3. Os níveis de serviço serão classificados conforme as severidades Emergencial, Grave e Normal.

8.4. Todos os prazos especificados na tabela "Acordo de Nível de Serviço / Penalidades" são contados a partir da abertura do respectivo número de identificação do chamado.

8.5. A abertura do chamado com fornecimento do seu número de identificação (protocolo de atendimento) deve ocorrer no prazo máximo de 15 minutos a partir da tentativa de contato pela Contratante com o número fornecido pela Contratada.

8.6. O atendimento aos chamados pode ocorrer remotamente ou de forma presencial. Atendimentos remotos não resolvidos que ultrapassem 24 horas devem ser continuados de forma presencial.

8.7. Após a conclusão do suporte, a Contratada comunicará ao TJAM e solicitará autorização para o fechamento do chamado. Caso o TJAM não confirme a solução definitiva do problema, o chamado permanecerá aberto até que seja efetivamente solucionado pela Contratada. Neste caso, o TJAM informará as pendências relativas ao chamado aberto.

8.8. Sempre que houver quebra dos ANS, o TJAM emitirá notificação à Contratada, que terá o prazo de, no máximo, 5 (cinco) dias úteis, contados a partir do recebimento da notificação, para apresentar as justificativas para as falhas verificadas.

8.9. Caso não haja manifestação dentro desse prazo ou caso o TJAM entenda serem improcedentes as justificativas apresentadas, será iniciado processo de aplicação das penalidades previstas, conforme o nível de atendimento transgredido.

8.10. Caso não sejam observados os prazos para atendimento previstos, incidirão glosas, calculadas sobre o valor do contrato, e penalidades conforme o disposto na tabela a seguir:

Acordo de Nível de Serviço / Penalidades			
Severidade	Prazos	Descrição Severidade	Penalidades
1 - Emergencial	6 Horas	Até 2 horas corridas de atraso.	1 – Advertência; 2 – Havendo recorrência, multa de 0,8%(zero vírgula oito por cento) por hora de atraso, calculada sobre o valor mensal do item.
		Superior a 2 horas e inferior ou igual a 8 horas corridas de atraso, além do prazo definido nos Níveis Mínimos de Serviços	3 – Multa de 1,0% (um por cento) por hora de atraso, calculada sobre mensal do item, sem prejuízo ao item anterior.
		Superior a 8 horas corridas.	4 – Multa de 1,2% (um vírgula dois por cento) por hora de atraso, calculada sobre o valor mensal do Item, sem prejuízo ao item anterior, e outras sanções administrativas a critério da Contratante.
2 - Grave	12 Horas	Até 4 horas corridas de atraso.	5 – Advertência; 6 – Para as demais ocorrências, multa de 0,6% (zero vírgula seis por cento) por hora de atraso, calculada sobre o valor mensal do Item.
		Superior a 4 horas e inferior ou igual a 24 horas corridas de atraso, além do prazo definido nos Níveis Mínimos de Serviços.	7- Multa de 0,8% (zero vírgula oito por cento) por hora de atraso, calculada sobre o valor mensal do Item, sem prejuízo ao item anterior.
		Superior a 24 horas corridas de atraso, além do prazo definido nos Níveis Mínimos de Serviços.	8 – Multa de 1.0% (um por cento) por hora de atraso, calculada sobre o valor mensal do Item, sem prejuízo ao item anterior, e outras sanções administrativas a critério da Contratante.
3 - Normal	24 Horas	Até 48 horas corridas de atraso.	9 – Advertência; 10 – Para as demais ocorrências, multa de 0,5% (zero vírgula cinco por cento) por hora de atraso, calculada sobre o valor mensal do Item; 11. – Se o somatório das multas aplicadas com relação às obrigações relativas a um mesmo equipamento ultrapasse 20% do seu valor de aquisição, poderá ensejar a rescisão do Contrato, independentemente de aplicação das sanções administrativos cabíveis.

9. FORMA DE PAGAMENTO

9.1. O pagamento será efetuado em até 30 (trinta) dias, mediante apresentação da Nota Fiscal/Fatura, após ser devidamente atestada a sua conformidade pelo Gestor designado para acompanhar e fiscalizar a execução.

9.2. Para fins de liquidação, o setor competente deve verificar se a Nota Fiscal ou Fatura apresentada expressa os elementos necessários e essenciais do documento, tais como:

a) o prazo de validade;

b) a data da emissão;

c) os dados do contrato e do órgão contratante;

d) o período respectivo de execução do contrato;

e) o valor a pagar; e

f) eventual destaque do valor de retenções tributárias cabíveis.

9.3. Havendo erro na apresentação da Nota Fiscal/Fatura, ou circunstância que impeça a liquidação da despesa, esta ficará sobrestada até que o contratado providencie as medidas saneadoras, reiniciando-se o prazo após a comprovação da regularização da situação, sem ônus à contratante.

9.4. A Nota Fiscal ou Fatura deverá ser obrigatoriamente acompanhada da comprovação da regularidade fiscal, constatada por meio de consulta *on-line* ao SICAF ou, na impossibilidade de acesso ao referido Sistema, mediante consulta aos sítios eletrônicos oficiais.

9.5. A Administração deverá realizar consulta ao SICAF para:

a) verificar a manutenção das condições de habilitação exigidas no edital;

b) identificar possível razão que impeça a participação em licitação, no âmbito do órgão ou entidade, proibição de contratar com o Poder Público, bem como ocorrências impeditivas indiretas.

9.6. Constatando-se, junto ao SICAF, a situação de irregularidade do contratado, será providenciada sua notificação, por escrito, para que, no prazo de 5 (cinco) dias úteis, regularize sua situação ou, no mesmo prazo, apresente sua defesa. O prazo poderá ser prorrogado uma vez, por igual período, a critério do contratante.

9.7. Não havendo regularização ou sendo a defesa considerada improcedente, o contratante deverá comunicar aos órgãos responsáveis pela fiscalização da regularidade fiscal quanto à inadimplência do contratado, bem como quanto à existência de pagamento a ser efetuado, para que sejam acionados os meios pertinentes e necessários para garantir o recebimento de seus créditos.

9.8. Persistindo a irregularidade, o contratante deverá adotar as medidas necessárias à rescisão contratual nos autos do processo administrativo correspondente, assegurada ao contratado a ampla defesa.

9.9. Havendo a efetiva execução do objeto, os pagamentos serão realizados normalmente, até que se decida pela rescisão do contrato, caso o contratado não regularize sua situação junto ao SICAF.

9.10. O pagamento do Item 7 será mensal, e os demais serão em parcela única.

10. GARANTIA CONTRATUAL

10.1. A Administração, em contratos acima do montante de R$ 100.000,00, poderá exigir garantia de execução do contrato, nos moldes do art. 96 c/c art. 98, da Lei nº 14.133, de 2021 em valor de até 5% (cinco por cento) do valor total/anual do contrato;

10.1.1. O contratante deverá apresentar a garantia no prazo mínimo de 1(um) mês, contado da data de assinatura do contrato;

10.1.2. Caberá ao contratado optar por uma das seguintes modalidades de garantia:

a) caução em dinheiro ou em títulos da dívida pública emitidos sob a forma escritural, mediante registro em sistema centralizado de liquidação e de custódia autorizado pelo Banco Central do Brasil, e avaliados por seus valores econômicos, conforme definido pelo Ministério da Economia;

b) seguro-garantia;

c) fiança bancária emitida por banco ou instituição financeira devidamente autorizada a operar no País pelo Banco Central do Brasil.

10.2. Caso utilizada a modalidade de seguro-garantia, a apólice deverá ter validade durante a vigência do contrato, permanecendo em vigor mesmo que o contratado não pague o prêmio nas datas convencionadas.

10.3. A apólice do seguro garantia deverá acompanhar as modificações referentes à vigência do contrato principal mediante a emissão do respectivo endosso pela seguradora.

10.4. Será permitida a substituição da apólice de seguro-garantia na data de renovação ou de aniversário, desde que mantidas as condições e coberturas da apólice vigente e nenhum período fique descoberto.

10.5. Caso utilizada outra modalidade de garantia, somente será liberada ou restituída após a fiel execução do contrato ou após a sua extinção por culpa exclusiva da Administração e, quando em dinheiro, será atualizada monetariamente.

10.6. Na hipótese de suspensão do contrato por ordem ou inadimplemento da Administração, o contratado ficará desobrigado de renovar a garantia ou de endossar a apólice de seguro até a ordem de reinício da execução ou o adimplemento pela Administração.

10.7. A garantia assegurará, qualquer que seja a modalidade escolhida, o pagamento de:

10.7.1. prejuízos advindos do não cumprimento do objeto do contrato e do não adimplemento das demais obrigações nele previstas;

10.7.2. multas moratórias e punitivas aplicadas pela Administração à contratada; e

10.7.3. obrigações trabalhistas e previdenciárias de qualquer natureza e para com o FGTS, não adimplidas pelo contratado, quando couber.

10.8. A modalidade seguro-garantia somente será aceita se contemplar todos os eventos indicados no item 4.4, observada a legislação que rege a matéria.

10.9. A garantia em dinheiro deverá ser efetuada em favor do contratante, em conta específica na Caixa Econômica Federal, com correção monetária.

10.10. Caso a opção seja por utilizar títulos da dívida pública, estes devem ter sido emitidos sob a forma escritural, mediante registro em sistema centralizado de liquidação e de custódia autorizado pelo Banco Central do Brasil, e avaliados pelos seus valores econômicos, conforme definido pelo Ministério da Economia.

10.11. No caso de garantia na modalidade de fiança bancária, deverá ser emitida por banco ou instituição financeira devidamente autorizada a operar no País pelo Banco Central do Brasil, e deverá constar expressa renúncia do fiador aos benefícios do artigo 827 do Código Civil.

10.12. No caso de alteração do valor do contrato, ou prorrogação de sua vigência, a garantia deverá ser ajustada ou renovada, seguindo os mesmos parâmetros utilizados quando da contratação.

10.13. Se o valor da garantia for utilizado total ou parcialmente em pagamento de qualquer obrigação, o Contratado obriga-se a fazer a respectiva reposição no prazo máximo de 10 (dez) dias úteis, contados da data em que for notificada.

10.14. Contratante executará a garantia na forma prevista na legislação que rege a matéria.

10.15. O emitente da garantia ofertada pelo contratado deverá ser notificado pelo contratante quanto ao início de processo administrativo para apuração de descumprimento de cláusulas contratuais (art. 137, § 4º, da Lei n.º 14.133, de 2021).

10.16. Caso se trate da modalidade seguro-garantia, ocorrido o sinistro durante a vigência da apólice, sua caracterização e comunicação poderão ocorrer fora desta vigência, não caracterizando fato que justifique a negativa do sinistro, desde que respeitados os prazos prescricionais aplicados ao contrato de seguro, nos termos do art. 20 da Circular Susep n° 662, de 11 de abril de 2022.

10.17. Extinguir-se-á a garantia com a restituição da apólice, carta fiança ou autorização para a liberação de importâncias depositadas em dinheiro a título de garantia, acompanhada de declaração do contratante, mediante termo circunstanciado, de que o contratado cumpriu todas as cláusulas do contrato.

10.18. O garantidor não é parte para figurar em processo administrativo instaurado pelo contratante com o objetivo de apurar prejuízos e/ou aplicar sanções à contratada.

10.19. O contratado autoriza o contratante a reter, a qualquer tempo, a garantia, na forma prevista no Edital e no Contrato.

10.20. O contrato oferece maior detalhamento das regras que serão aplicadas em relação à garantia da contratação.

10.21. A garantia de execução é independente de eventual garantia do produto prevista especificamente no Termo de Referência.

11. CRITÉRIOS E PRÁTICAS DE SUSTENTABILIDADE

11.1. A empresa contratada deverá contribuir para a promoção do desenvolvimento nacional sustentável no cumprimento de diretrizes e critérios de sustentabilidade ambiental, de acordo com o art. 225 da Constituição Federal de 1988, e em conformidade com o art. 5º da Lei nº 14.133/21.

11.2. Adicionalmente, a empresa contratada deverá, sempre que viável, observar as normas vigentes relacionadas à sustentabilidade ambiental e aderir às melhores práticas delineadas no Guia Prático de Critérios de Sustentabilidade para Compras no TJAM, Guia Nacional de Contratações Sustentáveis da AGU, Resolução CNJ nº 400 de 16 de junho de 2021 que dispõe sobre a política de sustentabilidade no âmbito do Poder Judiciário, e Política Nacional de Resíduos Sólidos, instituída pela Lei nº 12.305, de 2 de agosto de 2010, durante a execução dos serviços.

11.3. Recomenda-se que a contratada deverá cumprir as cotas raciais, de gênero e de pessoas com deficiência.

11.4. Recomenda-se exigir da contratada um programa interno de treinamento visando a redução de consumo de energia elétrica, de consumo de água e redução de produção de resíduos sólidos.

11.5. Estabelecer a separação adequada e o descarte responsável de resíduos, incluindo a reciclagem de materiais quando aplicável.

11.6. Respeitar as Normas Brasileiras – NBR publicadas pela Associação Brasileira de Normas Técnicas sobre resíduos sólidos.

12. RESPONSÁVEIS PELO TERMO DE REFERÊNCIA

12.1. Subscrevem o Termo de Referência os servidores responsáveis por sua elaboração, nos moldes e parâmetros estabelecidos pelo Tribunal de Justiça do Estado do Amazonas. Além da exigência legal da aprovação da autoridade competente, o instrumento em tela carece da ratificação de que retrata o que fora ordenado aos responsáveis por sua elaboração.

13. DOS ANEXOS

13.1. São partes integrantes deste Termo de Referência os seguintes anexos:

a) Mapa de Gerenciamento de Riscos na Contratação;

b) Estudo Técnico Preliminar;

c) Mapa de Preços.

Manaus, *data do sistema*

Karla Rozeana Bau Zarth

Seção de Elaboração de Artefatos da Contratação

Mapa de Gerenciamento de Riscos

FASE DE ANÁLISE	
( ) Planejamento - ETP **(X) Planejamento - TR**	( ) Seleção de Fornecedor ( ) Gestão e Fiscalização Contratual
Tabela de Probabilidade: **Baixa**: É Incomum para o TJAM, existe uma ação de controle sobre o risco. A chance de ocorrer é remota e mínima. Não há histórico de ocorrência registrados nos últimos 5 anos pelo TJAM. GRAU 1 **Média**: Existem registros de ocorrência do risco no TJAM, houve uma tomada de ação sobre o risco. Houve ocorrência do risco nos últimos 2 anos. GRAU 3 **Alta**: Ocorre pelo menos uma vez por ano. Existe o registro de ocorrência recente no TJAM. GRAU 5 **Tabela de Impacto:** **Baixo:** Possuem danos reversíveis em curto prazo para o TJAM, com custos e perdas poucos significativos. Pequena extensão, é facilmente remediada ou desprezível através de uma ação. Não gera impacto no atingimento das estratégias do TJAM. GRAU 1 **Médio:** Possuem danos reversíveis em médio prazo com custos e perdas consideráveis e reversíveis para o TJAM, podendo ter média extensão e/ou gerador de algum impacto paras as estratégias do TJAM. GRAU 3 **Alto:** Impacto com perdas e danos graves para o TJAM. Tem grande extensão, e pode ser irreversível e/ou dificilmente reversível. É um dano, perda, ou prejuízo alto para o TJAM, ou de longo prazo de resolução. GRAU 5 **Tabela Nível de Risco:** Baixo – Menor e/ou igual a 5. Moderado – Entre 6 e 9 Alto – Maior que 9	

Matriz probabilidade x impacto:

Probabilidade (P)				
5	5	15	25
3	3	9	15
1	1	3	5
	1	3	5

Impacto (I)

Risco 01 – Ausência de DFD ou DOD que origina a contratação			
Probabilidade:	(x) Baixa	( ) Média	( ) Alta
Impacto	(x) Baixo	( ) Médio	( ) Alto

Causa
Falta de padronização do processo ou de um modelo padrão para abertura da demanda; desconhecimento da necessidade de utilização do DFD ou DOD por parte da unidade demandante.
Dano
Contratação que não atenda a uma necessidade da organização.

Ação Preventiva	**Responsável**
1. Manualizar o processo de oficialização da demanda, descrevendo todas as etapas/rotinas do processo, estabelecendo prazos e responsáveis para o início e término do processo.	Unidades técnicas; unidades demandantes
Ação de Contingência	**Responsável**
1. Criar checklist para verificação de atendimento dos requisitos iniciais necessários para a abertura de uma demanda na Unidade. 2. Instituir sistema, ferramenta ou procedimento para padronização de todo o procedimento de oficialização da demanda, de forma a controlar prazos e responsáveis pelo processo.	Unidades técnicas; unidades demandantes

Risco 02 – Falha na indicação dos agentes públicos para exercerem as funções do processo (equipe de planejamento, pregoeiro ou comissão julgadora e executor/fiscal do contrato)			
Probabilidade:	(x) Baixa	( ) Média	( ) Alta
Impacto:	(x) Baixo	( ) Médio	( ) Alto

Causa
Ausência ou falha na identificação das competências necessárias para o desempenho das funções.
Dano
Erros na elaboração dos artefatos da etapa de planejamento da contratação; atraso no processo de contratação.

Ação Preventiva	**Responsável**
1. Realizar o mapeameto das habilidades e treinamentos, incluindo os periódicos, necessários para participar da equipe de planejamento da contratação.	Chefias dos setores de planejamento.
Ação de Contingência	**Responsável**
1. Realizar o levantamento das ações de contratação realizadas a fim de permitir a identificação dos integrantes e gerenciar o número de trabalhos envolvidos.	Chefias dos setores de planejamento.

Risco 03 – Ausência de Estudos Técnicos Preliminares.			
Probabilidade:	(x) Baixa	( ) Média	( ) Alta
Impacto:	( ) Baixo	(x) Médio	( ) Alto

Causa
Contratação sem realização de estudos técnicos preliminares; falha no planejamento da contratação.
Dano
Contratação não produz resultados capazes de atender à necessidade da administração, com consequente desperdício de recursos públicos; ou levando à impossibilidade de contratar.

Ação Preventiva	**Responsável**
1. Elaborar os estudos técnicos preliminares mediante modelo padronizado.	Unidades técnicas
Ação de Contingência	**Responsável**
1. Não aprovação do processo de contratação que não contenha os estudos técnicos preliminares.	Assessoria Jurídica

Risco 04 – Indefinição do conteúdo dos estudos técnicos preliminares			
Probabilidade:	(x) Baixa	( ) Média	( ) Alta
Impacto:	( ) Baixo	(x) Médio	( ) Alto

Causa
Falta de padronização e indefinição do conteúdo e características essenciais do objeto.
Dano

Conteúdo não permite atingir seu objetivo.			
Ação Preventiva			**Responsável**
1.Mapear e padronizar o processo de contratação, construindo checklist de controle para auxiliar no acompanhamento e cumprimento do conteúdo necessário à elaboração do ETP.			Unidades técnicas
Ação de Contingência			**Responsável**
1. Realizar plano de capacitação permanente para os colaboradores e servidores que elaboram os ETP.			Chefias das unidades técnicas
<u>Risco 05</u> – Contratações desalinhadas ao PCA			
Probabilidade:	(x) Baixa	( ) Média	( ) Alta
Impacto:	( ) Baixo	( ) Médio	(x) Alto
Causa			
Execução de contratações desalinhadas dos objetivos estabelecidos nos planos da organização.			
Dano			
Contratação indevida ou que não atenda às necessidades ou demandas do órgão / entidade; gastos não planejados.			
Ação Preventiva			**Responsável**
1. Aprovação do resultado do planejamento conjunto de todas as contratações e do orçamento da organização, verificando o alinhamento das contratações previstas com os objetivos que constam dos planos, em especial as contratações de maior importância ou materialidade.			Alta Administração
Ação de Contingência			**Responsável**
1. Ao aprovar os artefatos das principais contratações verificar se foi estabelecido o alinhamento entre cada uma dessas contratações e os objetivos dos planos da organização.			Alta Administração
<u>Risco 06</u> – Requisitos inadequados			
Probabilidade:	(x) Baixa	( ) Média	( ) Alta
Impacto:	( ) Baixo	( ) Médio	(x) Alto
Causa			
Definição de requisitos da contratação insuficientes, levando a contratação de solução que não atende à necessidade que originou a contratação.			
Dano			
Limitação indevida da competição, com consequente elevação do preço contratado ou dependência de um único fornecedor; desperdício de recursos.			
Ação Preventiva			**Responsável**
1. Revisão dos artefatos de planejamento para verificar suficiência e adequação dos requisitos.			Unidades técnicas e Seção de Artefatos
Ação de Contingência			**Responsável**
1. Início da elaboração do Termo de Referência após a aprovação dos estudos técnicos preliminares.			Seção de Artefatos
<u>Risco 07</u> – Estimativas inadequadas de quantidades			
Probabilidade:	(x) Baixa	( ) Média	( ) Alta
Impacto:	( ) Baixo	(x) Médio	( ) Alto
Causa			
Estimativa de quantidades menores ou maiores que as necessidades da organização.			
Dano			
Sobra ou faltas de produtos ou serviços; celebração de aditivos contratuais que poderiam ter sido evitados; utilização de orçamento superior ao previsto.			
Ação Preventiva			**Responsável**
1. Definir método para estimar as quantidades necessárias e documentar a aplicação do método no processo de contratação. 2. Armazenar dados da execução contratual, de modo que a equipe de planejamento da contratação que elaborar os artefatos da próxima licitação da mesma solução ou de solução similar conte com informações de contratos anteriores.			Unidades técnicas e unidades demandantes. Fiscal do Contrato
Ação de Contingência			**Responsável**
1. Não aprovar processo de contratação que não contenha, nos autos, a memória de cálculo das quantidades dos itens que serão contratados.			Assessoria Jurídica
<u>Risco 08</u> – Estimativas inadequadas de preços			
Probabilidade:	(x) Baixa	( ) Média	( ) Alta
Impacto:	( ) Baixo	( ) Médio	(x) Alto
Causa			
Coleta insuficiente de preços ou falta de método para realizar a estimativa.			

Dano			
Estimativas inadequadas, com consequente utilização de parâmetro inadequado para análise da viabilidade da contratação e dificuldade de justificar as estimativas quando questionados por partes interessadas.			
Ação Preventiva			**Responsável**
1. Publicar normativo estabelecendo procedimento consistente para elaboração de estimativas de preço.			Órgão
Ação de Contingência			**Responsável**
1. Elaborar memória de cálculo das estimativas de preço, considerando uma cesta de preços.			DVCOP
Risco 09 – Parcelamento inadequado			
Probabilidade:	(x) Baixa	( ) Média	( ) Alta
Impacto:	( ) Baixo	( ) Médio	(x) Alto
Causa			
Não parcelar solução cujo parcelamento é viável; parcelar solução cujo parcelamento é inviável.			
Dano			
Diminuição da competição nas licitações por não permitir que empresas especializadas participem da licitação, com consequente aumento dos valores contratados; contratações por inexigibilidade ou a licitações com poucos fornecedores, com consequente aumento dos valores contratados em comparação à compra conjunta da solução			
Ação Preventiva			**Responsável**
1. Avaliar se a solução é divisível ou não, levando em conta o mercado que a fornece.			Unidades técnicas
Ação de Contingência			**Responsável**
1. Avaliar todas as formas de parcelamento possíveis para escolher a que melhor se adequa a contratação pretendida.			Unidades técnicas
Risco 10 – Termo de Referência incompleto ou inconsistente			
Probabilidade:	(x) Baixa	( ) Média	( ) Alta
Impacto:	( ) Baixo	(x) Médio	( ) Alto
Causa			
Termo de referência (TR) incompleto ou inconsistente, cujo conteúdo não permite selecionar a proposta mais vantajosa para a Administração.			
Dano			
Contratação ou aquisição sem mecanismos adequados para a gestão, com consequente desperdício de recursos.			
Ação Preventiva			**Responsável**
1. Elaborar lista de verificação (checklist) para verificar a completude do TR.			Seção de Artefatos
Ação de Contingência			**Responsável**
1. Utilizar modelo de Termo de Referência previamente aprovado para cada tipo de contratação.			Seção de Artefatos
Risco 11 – Declaração imprecisa do objeto ou da solução			
Probabilidade:	(x) Baixa	( ) Média	( ) Alta
Impacto:	( ) Baixo	( ) Médio	(x) Alto
Causa			
Ausência da descrição do objeto ou da solução, ou descrição incompleta.			
Dano			
Falta de compreensão dos licitantes do contexto em que se insere a solução objeto da licitação, com consequente oferecimento de proposta que não atende a necessidade da contratação.			
Ação Preventiva			**Responsável**
1. Revisar os artefatos do planejamento, incluindo a consistência da declaração do objeto ou da solução.			Unidades técnicas e Seção de Artefatos
Ação de Contingência			**Responsável**
1. Incluir no ETP e no TR ou PB seção destinada a descrever a solução como um todo, explicitando que o objeto da licitação é uma parte desta solução.			Unidades técnicas e Seção de Artefatos
Risco 12 – Indisponibilidade orçamentária			
Probabilidade:	(x) Baixa	( ) Média	( ) Alta
Impacto:	( ) Baixo	( ) Médio	(x) Alto
Causa			
Ausência da solução no PCA.			
Dano			
Contratações acima do valor previsto e aditivos contratuais em outros contratos não previstos, levando a indisponibilidade orçamentária, com consequente impossibilidade de contratação.			
Ação Preventiva			**Responsável**
1. Manter informações sobre a disponibilidade orçamentária e financeira.			SECOF

Ação de Contingência			Responsável
1. Incluir informações atualizadas sobre a situação de cada contratação da organização sobre os valores empenhados, liquidados e pagos, e sobre a dotação disponível.			SECOF
Risco 13 – Ausência de padronização dos editais			
Probabilidade:	(x) Baixa	( ) Média	( ) Alta
Impacto:	(x) Baixo	( ) Médio	( ) Alto
Causa			
Licitações com editais não padronizados, elaborados sem modelos previamente aprovados.			
Dano			
Multiplicidade de esforços para realizar licitações de objetos correlatos, com consequente esforço desnecessário para elaborar editais e repetição de erros.			
Ação Preventiva			**Responsável**
1. Padronização de Editais para diferentes tipos de licitação.			COLIC e Seção de Artefatos
Ação de Contingência			**Responsável**
1. Disponibilização no SEI de minutas prontas de editais após aprovação dos mesmos.			COLIC e Seção de Artefatos.

Documento assinado eletronicamente por **Karla Rozeana Bau Zarth**, **Servidor**, em 22/07/2024, às 13:35, conforme art. 1º, III, "b", da Lei 11.419/2006.

A autenticidade do documento pode ser conferida no site https://sei.tjam.jus.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0 informando o código verificador **1689378** e o código CRC **1EA12186**.

2024/000014603-00 1689378v3

TRIBUNAL DE JUSTIÇA DO ESTADO DO AMAZONAS
Av. André Araújo, S/N - Bairro Aleixo - CEP 69060-000 - Manaus - AM - www.tjam.jus.br

ESTUDO TÉCNICO PRELIMINAR - TJ/AM/SETIC/DVITIC

Responsáveis pela elaboração:

Washington Neto

Diogo Mendonça

Categoria do Objeto: Serviços de segurança da informação e privilégios de Acesso.

1. PREVISÃO NO PLANO DE CONTRATAÇÕES ANUAL

1.1. A contratação está prevista no Plano de Contratações Anual de 2024, aprovado pela Resolução TJAM nº 52/2023, podendo ser consultado através do link: https://bit.ly/pca2024.

1.2. A presente demanda encontra-se registrada sob o Código PCA SETIC-2024-25 do referido documento.

2. DESCRIÇÃO DA NECESSIDADE DA CONTRATAÇÃO

2.1. O TJAM possui diversos usuários internos, incluindo servidores, comissionados, terceirizados, estagiários, requisitados e afastados, além de inúmeros usuários externos que utilizam os sistemas e serviços disponibilizados, serviços digitais, sites e sistemas à sociedade.

2.1.1 Para o acesso dos envolvidos é imprescindível que os diversos recursos de Tecnologia da Informação e Comunicação, como, por exemplo: servidores, computadores, internet, sistemas, aplicações, serviços, e-mail, sites, dentre outros tantos, estejam seguros e acessíveis.

2.1.2 Cada novo sistema, equipamento e software que passa a integrar o parque computacional deste órgão, disponibiliza credenciais, contas e acessos de alto poder administrativo. Essas credenciais são as mais críticas e poderosas dentro da infraestrutura de TIC e da área de desenvolvimento. Sendo extremamente visadas por ataques cibernéticos para obter recursos e acesso a dados confidenciais.

2.2. Diante disso, garantir que toda essa gama de recursos tenha pleno funcionamento é uma competência da Secretaria de Tecnologia da Informação e Comunicação (SETIC). Nesse sentido, observa-se como principal desafio a garantia da sustentação do ambiente tecnológico, que requer trabalho constante devido às atualizações contínuas relacionadas a esta área.

2.2.1 Todo esse complexo de atividades é essencial para dar suporte seguro às áreas meio e finalísticas do TJAM, de modo que possam desempenhar suas funções legais e assim realizar a missão institucional, e caso alguma dessas áreas seja prejudicada, estará prejudicando também, diretamente, a função institucional perante o Governo e a sociedade.

2.2.2 Credenciais, contas e acessos administrativos são necessários para administradores, serviços e dispositivos acessarem sistemas críticos como, servidores, aplicações, bancos de dados, sistemas operacionais, switches, firewalls, roteadores, entre outros, localizados no data center local ou na nuvem.

2.2.3 Os acessos de alto privilégio podem parecer muito vantajosos em termos de prerrogativas de controle sobre o parque tecnológico, entretanto o cenário se torna rapidamente desencorajador quando se conhecem os riscos e ameaças envolvidas. Muitos riscos surgem como resultado desse tipo de acesso e podem advir de invasores externos e usuários maliciosos dentro da própria empresa.

2.2.4 Se uma conta, credencial ou acesso que fornece permissões privilegiadas para sistemas e ativos confidenciais é comprometida, isso pode resultar em danos significativos para o órgão e o governo, e permitir ao atacante realizar ações drásticas como: vazamento ou roubo de dados confidenciais que levam a problemas financeiros e danos à reputação, liberação de acesso a servidores de comando e controle (isso é tipicamente um sistema que permite que um atacante fique escondido em sua rede operando sistemas remotamente, extraindo dados, sem ser percebido), captura da atividade do usuário (como pressionamentos de tecla: tudo o que comunicar eletronicamente) e instalação de software indevido na máquina acessada (malware), bloqueio de usuários verdadeiros em suas máquinas para que apenas o invasor tenha acesso (ransomware), realização de mineração de moeda criptografada ilegal ou não autorizada.

2.3. As motivações também estão alinhadas com as recomendações de diferentes órgãos e instruções normativas à respeito da adoção de controles gerais de segurança da informação, dentre os quais destacam-se:

2.3.1 O decreto 10.222, de 5 de fevereiro de 2020, que dispõe sobre a Estratégia Nacional de Segurança Cibernética, tem como um dos seus objetivos a elevação do nível de proteção do Governo, onde cita: “Aperfeiçoar e manter atualizados os sistemas informacionais, as infraestruturas e os sistemas de comunicação dos órgãos públicos, em relação aos requisitos de segurança cibernética".

2.3.2 A Lei 13.709, de 14 de agosto de 2018, intitulada como a Lei Geral de Proteção de Dados Pessoais (LGPD), em seu artigo 46 cita que: “os agentes de tratamento devem adotar medidas de segurança, técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito”.

2.3.3 A Resolução 370 de 28/01/2021, Estabelece a Estratégia Nacional de Tecnologia da Informação e Comunicação do Poder Judiciário (ENTIC-JUD), onde orientada em seu preâmbulo pelos objetivos dos seguintes componentes: “Objetivo 7: Aprimorar a Segurança da Informação e a Gestão de Dados”.

2.3.4 Na Resolução 396 de 07/06/2021 do CNJ, que institui a Instituir a Estratégia Nacional de Segurança da Informação e Cibernética do Poder Judiciário (ENSEC-PJ) no âmbito dos órgãos do Poder Judiciário, à exceção do Supremo Tribunal Federal (STF), destaca-se o artigo:

"Art. 9º São ações da ENSEC-PJ:

I - fortalecer as ações de governança cibernética;

II - elevar o nível de segurança das infraestruturas críticas;

III - estabelecer rede de cooperação do Judiciário para a segurança cibernética;

IV - estabelecer modelo centralizado de governança cibernética nacional."

2.3.5. Diante do exposto e considerando o aumento no volume de acessos e de novas ameaças cibernéticas, tentativas de invasão aos sistemas e o risco de vazamento de credenciais, que podem impactar de modo negativo a eficiente gestão do ambiente de trabalho e a manutenção da qualidade dos serviços prestados, faz-se presente a obrigação de preservar a integridade, confidencialidade e disponibilidade das informações custodiadas neste Tribunal, resguardando a conduta de manuseio, controle e proteção das informações contra destruição, modificação, comercialização, divulgação indevida e acessos não autorizados, acidentais ou intencionais.

3. UNIDADE DEMANDANTE

3.1. Secretaria de Tecnologia da Informação e Comunicação do TJAM.

4. REQUISITOS DA CONTRATAÇÃO

4.1 O serviço objeto da contratação pretendida é a aquisição de produtos com características comuns de mercado e, também, possui natureza continuada, uma vez que ocorra a interrupção, pode comprometer a continuidade das atividades do TJAM, tendo em vista que a solução implementa segurança através da mediação de credenciais privilegiadas, desta forma, a interrupção da solução implica em interrupção no acesso aos recursos gerenciados pelas referidas credenciais. Além do mais, a Resolução CNJ 396/2021, que estabelece a Estratégia Nacional de Segurança Cibernética do Poder Judiciário (ENSEC-JUD), em seu capítulo 8, artigo 29, que trata sobre gestão de usuários elabora as seguintes determinações:

> “Art. 29. Cada órgão do Poder Judiciário, com exceção do STF, deverá implementar a gestão de usuários de sistemas informatizados composta de:
> I – gerenciamento de identidades;
> II – gerenciamento de acessos; e
> III – gerenciamento de privilégios.
> Parágrafo único. A gestão de usuários será disciplinada por ato do Presidente do CNJ, que definirá o padrão a ser adotado para utilização de credenciais de login único e interface de interação dos sistemas, com o objetivo de uniformizar e garantir a experiência única de interação com os sistemas judiciais.”

4.2. A Contratada deverá observar, no que couber, as práticas e os critérios de sustentabilidade disponíveis respectivamente no Guia Prático de Critérios de Sustentabilidade para Compras no TJAM e na Política Nacional de Resíduos Sólidos, instituída pela Lei nº 12.305, de 2 de agosto de 2010.

4.3. A duração do contrato de prestação de serviços de natureza continuada será de 12 meses.

4.4. Por tratar-se de serviço comum, já que possui padrões de desempenho e características gerais e específicas, usualmente encontradas no mercado, sugerimos que o objeto seja licitado por meio da modalidade Pregão Eletrônico por menor preço global.

4.5 A transição contratual com transferência de conhecimento, tecnologia e técnicas empregadas promove uma relação mais transparente e colaborativa entre as partes envolvidas. Ao adquirir o conhecimento e expertise, o órgão e setor responsável pelo mantenimento das operações demonstram comprometimento e responsabilidade com o sucesso do projeto, fortalecendo a confiança de autonomia na execução de atividades com complexidade aceitável, minimizando o tempo de espera e retorno às operações em caso de interrupções.

4.5.1. A transferência de conhecimento é essencial para garantir a continuidade das operações e a qualidade dos serviços prestados. Ao compartilhar informações relevantes sobre processos, metodologias e expertise acumulada durante a execução do contrato, torna-se capaz de assegurar que o órgão CONTRATANTE esteja plenamente capacitado para dar continuidade às atividades, minimizando qualquer interrupção ou perda de eficiência.

4.5.2. Ainda dentro da necessidade de aprendizado e absorção de conhecimento, a transferência de tecnologia e técnicas empregadas é crucial para manter o progresso e o desenvolvimento do projeto ou serviço contratado. Ao repassar as ferramentas e os métodos utilizados, nos é possibilitado que possamos explorar plenamente os recursos e obter resultados satisfatórios. Isso também contribui para a autonomia da contratante no futuro, permitindo que ela faça melhorias e adaptações de acordo com as necessidades específicas.

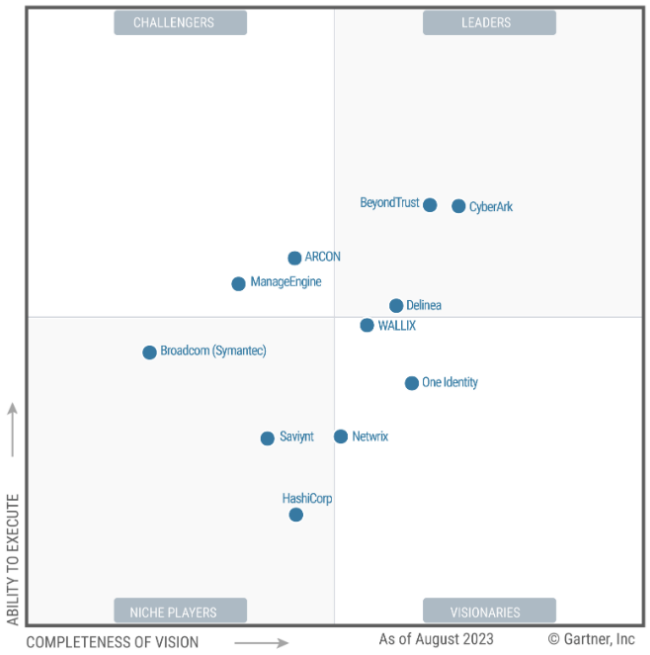
4.6. Por fim, sugerimos que se utilize o sistema de Registro de Preço para esta pretensa contratação.

5. LEVANTAMENTO DE MERCADO E JUSTIFICATIVA DA ESCOLHA DO TIPO DE SOLUÇÃO A CONTRATAR

5.1 Como solução mercadológica que venha a atender as necessidades deste Tribunal não se vislumbra outra que não seja a contratação de empresa especializada no fornecimento de solução de gerenciamento de acessos privilegiados (PAM – Privileged Access Management), com diversas funcionalidades tais como análise comportamental, auditoria de credenciais, mitigações contra roubos e abusos de privilégios e aplicação do “privilégio mínimo” nos ativos protegidos, tudo isso com a finalidade de aumentar a proteção das credenciais utilizadas no âmbito do Tribunal e impedir que essas credenciais sejam usadas por agentes potenciais atacantes, prevenindo danos decorrentes de ataques cibernéticos que possam ser realizadas conta o tribunal.

5.2 Sendo uma solução comum de mercado, existem diversos fabricantes que podem oferecer soluções de proteção de credenciais, com diferentes graus de qualidade e diversos preços a serem pagos. Sendo inviável avaliar todas as opções disponíveis, recorreu-se ao Gartner, que é empresa amplamente respeitada e prestigiada no campo da Tecnologia da Informação, servido como referência na área, para delimitar as melhores opções a serem consideradas em processos de aquisição.

Figure 1: Magic Quadrant for Privileged Access Management



5.3 O Gartner realiza a mensuração da qualidade e relevância de soluções de TI através de um gráfico que ficou conhecido como “Quadrante”, o qual reflete os estudos publicados anualmente sobre categorias de produtos e serviços, cuja composição utiliza diversos critérios para medir a qualidade das soluções oferecidas pelas empresas que atuam naquela categoria. Como o TJAM preza pela qualidade das soluções contratadas para compor sua infraestrutura tecnológica, as soluções consideradas foram as que se estavam mais bem posicionadas no quadrante “Leaders” (líderes) da avaliação mais recente, publicada em Agosto de 2023. Os fabricantes mais bem localizados neste quadrante foram avaliados com os melhores resultados em suas soluções oferecidas.

5.4 Ao que podemos verificar no quadrante do Gartner, os três fabricantes que estão melhor posicionados são a CyberArk, BeyondTrust e Delinea.Cumprindo lembrar que o TJAM ainda não possui qualquer solução de gerenciamento de acessos privilegiados.

5.5 Contratações públicas similares

5.5.1 Dado que o objeto da contratação é um elemento essencial para a construção de um ecossistema de segurança da informação no âmbito do TJAM, tendo sido observado a sua contribuição na garantia da segurança da informação no âmbito da administração pública municipal, estadual e federal, com diversos órgãos dos mais variados tamanhos e com a mais diversas funções o possuindo em sua infraestrutura de TI. As contratações mencionadas abaixo, guardadas as peculiaridades de cada órgão, são similares ao objeto que o TJAM pretende adquirir:

5.5.1.1 Destaca-se a solução contratada pelo Tribunal do Estado do Pará que, através da Ata de Registro de Preço (ARP) nº 16/2020 do Tribunal Regional do Trabalho da 8º Região, formalizada pelo Pregão Eletrônico 34/2020, registrou preços para o objeto: “aquisição de Solução de Gerenciamento de Acesso Privilegiado (Privileged Access Management – PAM) e Monitoramento e Análise Comportamental, com possibilidade de proteção, monitoramento, detecção e resposta a atividade de conta privilegiada, armazenamento de senhas e mitigação de riscos”.

5.5.1.2 A solução contratada pelo Tribunal Regional do Trabalho da 8ª Região (TRT8) que, através da Ata de Registro de Preço (ARP) nº 16/2020 gerada no Pregão Eletrônico 34/2020, registrou preços para o objeto: “aquisição de Solução de Gerenciamento de Acesso Privilegiado (Privileged Access Management – PAM) e Monitoramento e Análise Comportamental, com possibilidade de proteção, monitoramento, detecção e resposta a atividade de conta privilegiada, armazenamento de senhas e mitigação de riscos”.

5.5.1.3 Tribunal de Justiça do Distrito Federal e Territórios (TJDFT), através do item 1 do contrato 250/2019, gerado através do Pregão Eletrônico 065/2019, adquiriu solução similar ao objeto de contratação do TJPA. cujo objeto é a: “a aquisição, suporte e atualização de solução de segurança da informação para a gestão de acessos privilegiados, armazenamento de credenciais, que possibilite o isolamento, gravação e o monitoramento de sessões de ativos de TIC do CONTRATANTE por um período de até 36 (trinta e seis) meses, incluindo serviço de instalação e repasse de conhecimento”.

5.5.1.4 A Secretaria de Fazenda do Estado de Santa Catarina (SEFAZ-SC) que, através do Pregão Eletrônico 0024/2020, registrou preços para o objeto: “Contratação de empresa especializada objetivando o fornecimento de solução de segurança integrada em ambientes críticos, incluindo serviços de implantação da solução, repasse de conhecimento, garantia e suporte”.

5.5.1.5 A Imprensa Nacional que, através do Pregão nº 04/2021 e ATA de Registro de Preço 005/2022, registrou preços para o objeto: contratação de empresa especializada no fornecimento de Solução de Segurança para Privilégios e Acessos a Sistemas Críticos, incluindo instalação, atualização de versão, transferência de conhecimento, suporte técnico e garantia.

5.6. Escolha e Justificativa da Solução

5.6.1 As soluções oferecidas pelos fabricantes classificados como líderes no quadrante do Gartner, foram avaliadas pela SETIC e atendem aos padrões técnicos e de confiabilidade exigidos.

5.6.2. Comparativo de Requisitos Tecnológicos

5.6.2.1 Itens em Verde (Plenamente Atendido), Itens em Amarelo (Parcialmente Atendido) e Itens em Vermelho (Não atende);

Requisitos	Delinea	Cyberark	BeyoundTrust
Prover mecanismos de segurança da informação			
Abranger todos os tipos de acessos e identidades			
Assegurar mecanismos de gerenciamento de privilégios elevados			
Prover registro de uso de privilégio e trilhas de auditoria			
Detectar e mitigar incidentes de forma mais eficaz através de mecanismos de inteligência artificial			
Ganhar agilidade e eficiência no tratamento de incidentes e na criação de relatórios			
Confiança zero (zero trust) para identidades			
Prover políticas para acessos adaptativos baseados em riscos e contextos conhecidos de uma autenticação			
Prover múltiplo fator de autenticação para diversos casos de uso com capacidade de interpretação de risco adaptativo			
Prover capacidade de acesso remoto a infraestrutura privilegiada e aplicações web de negócio sem VPN			
Prover ganhos operacionais para recuperação de acessos e senhas			
Gravação e proteção de sessões de aplicações do tipo web de negócio de forma não intrusiva			
Possuir a capacidade de disparar gatilhos de gravação em vídeo relacionado a ações do usuário na estação de trabalho que estejam cumprindo atividades críticas			
Proteger identidades, credenciais e acessos de forma fim-a-fim			
Proteger silos de armazenamento de credenciais em servidores e estações			
Possuir capacidade de definição de políticas granulares para cada etapa da proteção de identidades			
Deve se comunicar com outras ferramentas de segurança e ampla capacidade de integrações			
Portal de Login Único para aplicações (SSO, Single Sign-On)			
Gestão de senhas de aplicações de negócio que não suportam SingleSign-On (login único)			
Diretório em nuvem IDP (Identity Provider)			
Prover licenciamento em modalidade simples, preferencialmente, poridentidade			
Capacidade de gestão de senhas para usuários de negócio, com armazenamento em cofre de senhas			
Capacidade de controle de autenticação e autorização em nível granular para identidades não humanas			
Capacidade de proteção para chaves de API			
Capacidade de proteção de identidades não humanas em plataformas de conteinerização			
Disponibilizar pacote de desenvolvimento para proteção de identidades não humanas			
Capacidade de proteção de identidade não humanas para aplicações tradicionais (não conteinerizadas ou não nativas em nuvem)			

5.6.2.2 Agrupando o resultado da análise dos requisitos tecnológicos referente a cada uma das soluções, temos o seguinte quantitativo:

Requisitos	Delinea	Cyberark	BeyondTrust
Plenamente Atendido	7	27	7
Parcialmente Atendido	7	0	7
Não atendido	13	0	13

5.7. Baseado nos requisitos técnicos e em pesquisas de mercado, a CyberArk ganhou mais destaque ao longo dos últimos anos, sendo reconhecido como um dos principais fornecedores de soluções de gestão de privilégios. Além disso, constatou-se que foi a solução mais implantada nos órgãos públicos. Como exemplo: TJAP, TJPA, TJDFT, TRT8 e outros.

6. DESCRIÇÃO DA SOLUÇÃO ESCOLHIDA

6.1. A solução escolhida deve abranger os itens descritos no quadro abaixo:

ITEM	CÓDIGO SIASG	ESPECIFICAÇÕES
1	27502	Solução de Segurança para Identidades e seus Privilégios – Monitoramento de comportamento e mitigação de riscos de usuários administradores da TI, com garantia pelo período de 12 (doze) meses.
2	27502	Solução de Segurança para Identidades e seus Privilégios – Proteção para Aplicações Tradicionais, com garantia pelo período de 12 (doze) meses.
3	27502	Solução de Segurança para Identidades e seus Privilégios – Proteção Local para servidores Windows e Linux, com garantia pelo período de 12 (doze) meses.
4	27502	Solução de Segurança para Identidades e seus Privilégios – Proteção Local para Estações de Trabalho, com garantia pelo período de 12 (doze) meses.
5	26972	Serviço de instalação e configuração para Solução de Segurança para Identidades e seus Privilégios.
6	21172	Transferência de Conhecimento para Solução de Segurança para Identidades e seus Privilégios (turma)
7	27340	Serviço de Suporte Técnico Especializado

6.2 Solução de Segurança para Identidades e seus Privilégios – Proteção e Monitoração de Acessos

6.2.1. Características;
6.2.1.1. A solução deverá atender usuários físicos, equipamentos servidores, estações de trabalho e usuários lógicos e ativos de rede;
6.2.1.2. A solução deve apoiar, no mínimo, aos requisitos (artigos 6, 42, 43, 46, 48 e 50) da Lei Geral de Proteção de Dados-LGPD, como: Determinar como os dados deverão ser tratados, mantidos e protegidos e a quem responsabilizar em caso de descumprimento; Proteger o acesso a dados pessoais sensíveis; Responsabilizar pessoal e responder a incidentes; Aplicar boas práticas de governança, através de regras que deverão respeitar os preceitos da lei, de maneira a mitigar os riscos inerentes ao tratamento de dados e implementar e demonstrar a efetividade das políticas de segurança relacionadas ao tratamento de dados;
6.2.1.3. Apoiando aos requisitos da LGPD a solução deverá proteger e monitorar acessos a dados pessoais sensíveis por meio da segurança de credenciais e acessos de alto privilégio em serviços críticos, detectando e respondendo rapidamente a incidentes de segurança, identificando e mitigando ações privilegiadas com comportamentos de alto risco, avaliando riscos e testando a efetividade dos processos de proteção de dados por meio de relatórios da solução com identificação e classificação do status de risco do ambiente privilegiado, demonstrando conformidade e prova de que os controles de segurança necessários estão nos lugares certos, provendo análise comportamental, auditoria e segurança dos acessos a sistemas por meio de todas credenciais administrativas de alto privilégio em dispositivos e sistemas-alvo diversos do ambiente;
6.2.1.4. Um sistema-alvo da solução é definido como um servidor, uma estação de trabalho, um ativo de rede e de segurança, dentre outros mencionados a seguir, cujas credenciais de acesso passem a ser protegidas e gerenciadas pela solução;
6.2.1.5. Um usuário da solução é definido como qualquer pessoa que acesse um sistema-alvo mediante logon na solução e uso de credenciais por ela gerenciadas;
6.2.1.6. Deve monitorar sessões, gravar, detectar, correlacionar e mitigar todos comportamentos anormais de, pelo menos, 75 usuários simultâneos acessando todos os sistemas-alvo, dentre eles servidores Linux/Unix ou Windows, Controladores de domínio Microsoft Active Directory, estações de trabalho Windows e demais ativos de rede e sistemas diversos ;
6.2.1.7. A solução deverá ser entregue com acesso remoto privilegiado seguro (externo a rede corporativa) para os usuários simultâneos mencionados, sem a entrega de credenciais privilegiadas e sem a necessidade de instalação e uso de clientes (do tipo VPN ou outros) nos dispositivos dos usuários remotos por todo período contratado;
6.2.1.8. A solução deverá ser entregue com acesso Single-sign-on e múltiplo fator de autenticação adaptativo para, no mínimo, os 75 usuários internos e/ou remotos (externos a rede corporativa) mencionados, por todo período contratado, suportando, no mínimo:
6.2.1.8.1. Usuário e senha dos diretórios suportados, aplicativo para dispositivos móveis do tipo IOS e Android, oferecendo suporte para Biometria do tipo FaceID e através do leitor de digital, Smartphone push (Notificação para aprovar ou recusar uma autenticação), Geolocalização através de coordenadas GPS e banco de dados de IP, Suporte a tokens OATH OTP, autenticação na tela de login via QRcode sem a necessidade de digitar usuário e senha, com opção de forçar a biometria no dispositivo móvel, Entrega de código via SMS e chamada de voz, perguntas de segurança, notificações por e-mail e telefone celular, tokens OTP (on-line, off-line, por e-mail, hardware);
6.2.1.8.2. Autenticação auto-ajustada baseada no contexto de risco e segurança aprendidos pela solução, permitindo a criação de um perfil para cada usuário, aproveitando atributos históricos e situacionais específicos do mesmo, como localização, dispositivo, rede, horário e índice de risco de comportamento;
6.2.1.8.3. Análise de solicitações de autenticação em relação a padrões históricos, atribuição de índice de risco a cada tentativa de logon, geração de alertas e criação de políticas de bloqueio a serem acionadas quando um comportamento anômalo é detectado e de acesso simplificado quando o usuário é entendido como legítimo;
6.2.1.8.4. Permitir que os usuários adicionem e modifiquem fatores de autenticação diretamente em um portal com definição de período de desvio do múltiplo fator de autenticação;
6.2.1.8.5. Prover relatórios e dashboards customizáveis com detalhamento de informações em tempo real sobre as atividades de autenticação, como falhas na autenticação secundária, tentativas bem-sucedidas de login e os fatores de autenticação mais usados;
6.2.1.8.6. Entenda-se como sistemas-alvo os baseados, em no mínimo, as seguintes tecnologias: S.O.: Linux/Unix e Microsoft Windows; Hypervisors: Acrópolis (Nutanix), VMWare, RedHat KVM e Microsoft Hyper-V; Contas de usuários de sistemas e de serviço; Credenciais do Microsoft COM+, IIS, Apache TomCat, RedHat Jboss, Nginx; Objetos (usuários, grupos e computadores) do Microsoft Active Directory e LDAP; Contas de usuários e administradores de bancos de dados Microsoft SQL Server, Oracle, PostgreSQL; Contas de equipamentos ativos de conectividade de redes LAN (Local Area Network) e WAN (Wide Area Network) – switches, roteadores, controladores/APs WiFi, SAN (Storage Area Network) e NAS (Network Attached Storage); Contas de usuários e administradores de consoles de gerenciamento de servidores e estações de trabalho; Contas de equipamentos dedicados à segurança, tais como Firewall, IPS, AntiSpam e filtros de conteúdo; Contas de equipamentos dedicados à segurança física, tais como câmeras de vigilância, catracas, etc.; Credenciais de nuvem em Google Workspace, VMWare ESXi, Azure, AWS, GCP, Office 365.
6.2.2. Gestão de dados do ciclo de vida e compartilhamento das contas privilegiadas, monitoramento e gravação de sessões privilegiadas:
6.2.2.1. A solução deve conceder acesso aos sistemas utilizando “Remote Desktop” e “SSH”, disponibilizados pelos sistemas-alvo do ambiente, sem que os usuários vejam qualquer senha e chave (vigentes no momento e providas para as aplicações e conexões remotas, devendo ser recuperadas de forma automática e transparente do repositório seguro de credenciais da solução), garantindo que não haja necessidade de instalação de aplicações e/ou agentes nas estações dos usuários para realizar o acesso a sistemas e aplicações parametrizáveis, onde a aplicação deverá ser executada, por meio de página web, devidamente autenticada com usuário e senha pré-determinados ou recuperados da base de dados da solução, sem que haja login interativo por parte do usuário no S.O. do servidor de destino, possibilitando habilitar gravação da sessão, caso seja necessário. Exemplo: Executar o SQL Management Studio com credencial de SA (System Administrator) sem que o usuário conheça a senha e sem necessidade de login interativo prévio do usuário no sistema operacional do host de destino;

6.2.2.2 A solução deve permitir Integração para gestão de acessos privilegiados em serviços de nuvem padrões de mercado, como Amazon Web Services (AWS), Google Cloud, IBM Cloud e Microsoft Azure, disponibilizando no mínimo as seguintes funcionalidades: Integração e gestão de acessos privilegiados em contas de serviços em nuvem; Integração com sessões de serviços de nuvem, incluindo início e finalização de sessão e Gravação e auditoria de acesso de sessões iniciadas em serviços de nuvem;
6.2.2.3. Deve possuir as sessões administrativas acessadas e monitoradas ao vivo, com compartilhamento de tela e controle de periféricos, como teclado e mouse (assistência remota), e por meio de gravação de comandos e vídeos das mesmas, em formato padrão de execução não proprietário da solução, possibilitando que os comandos e vídeos gerados possam ser indexados para pesquisa futura, permitindo o filtro de comandos e ações executadas ao longo da sessão gravada, possibilitando pesquisar ações específicas na sessão gravada;
6.2.2.4. Proteger contra a perda, roubo e gestão inadequada de credenciais através de regras de complexidade da senha que incluem comprimento da senha (quantidade de caracteres), frequência de troca automatizada das senhas e chaves SSH, especificação de caracteres permitidos ou proibidos na composição da senha e outras medidas e mitigar problemas de segurança relacionados ao compartilhamento indevido de credenciais privilegiadas que são armazenadas localmente em dispositivos e também de contas que não são gerenciadas de forma centralizada por serviços de diretórios;
6.2.2.5. Descobrir credenciais privilegiadas referenciadas por serviços e processos automatizados e propagar as senhas geradas de forma aleatória onde quer que estas estejam referenciadas e descobrir e alterar credenciais em ambiente Windows, incluindo contas nomeadas, administradores ‘built-in’ e convidados, para determinar movimentações laterais (pass-the-hash), exibidas em mapa de rede gráfico e interativo ou através de relatórios e interface de gerenciamento;
6.2.2.6. Gerenciar, de forma segura, senhas utilizadas por contas de serviço, evitando a utilização de senhas em texto claro por scripts ou rotinas dos equipamento e garantir a implementação dos privilégios mínimos necessários, provendo acesso às senhas das contas privilegiadas somente ao pessoal autorizado;
6.2.2.7. Possuir funcionalidade de “AD Bridge” para integração de servidores Linux/Unix no Active Directory, acompanhando a mesma nomenclatura e grupos do diretório LDAP ou AD; Provisionar na plataforma Unix-like as contas e grupos do Active Directory que possuam permissão de acesso, de maneira automatizada e transparente;
6.2.2.8. Permitir a definição de Fluxos de Aprovação (Workflows) para obtenção de acesso às Contas Privilegiadas, com as seguintes características: Personalização de fluxos: permitir a configuração de fluxos para aprovação, de acordo com a criticidade e características da conta, e aprovação de, pelo menos, um responsável; Permitir a aprovação perante um agendamento de ações administrativas; ou seja; a aprovação do acesso ocorrerá em um dia, mas a liberação da senha ocorrerá de forma automática somente na data e horário previstos; Ser capaz de encontrar contas de usuários privilegiados que possam ser gerenciadas pela solução, permitindo ou não que a conta descoberta seja gerenciada pela solução; Ser capaz de substituir as senhas de identidades privilegiadas que estejam sendo utilizadas por determinado serviço em todos os locais onde estejam sendo utilizadas; A descoberta automática deve ser realizada por buscas no Active Directory (AD) e por intervalos de endereços IP;
6.2.2.9. Oferecer em sua aplicação web diferentes visões e opções de acordo com as permissões dos usuários, mostrando, por exemplo, apenas as funcionalidades delegadas àquele usuário; Suportar métodos para registrar e relatar qualquer ação realizada e detectada pela solução, incluindo registros de aplicações baseadas em texto, auditoria de banco de dados, aplicações syslog, notificações de e-mail;
6.2.2.10. Registrar cada acesso, incluindo os acessos via aplicação web, para solicitações de senha, aprovações, checkout’s, mudanças de delegação, relatórios e outras atividades. Devem ser registrados os acessos à console de gerenciamento da solução, tanto para configuração quanto para relatórios, bem como todas as atividades de alterações de senhas; logoff dos usuários; Alterações nas funções de delegação; Adições, deleções e alterações de senhas gerenciadas pela solução; Operações das senhas dos usuários, incluindo check-in e check-out, solicitações negadas e permitidas; Os relatórios devem ser filtrados por período de tempo, tipo de operação, sistema, gerente e outros critérios;
6.2.2.11. Deve fornecer relatórios de conformidade detalhados das operações realizadas pela solução, tais como: Lista de sistemas gerenciados; Senhas armazenadas; Eventos de alteração de senha; Permissões de acesso web; Auditoria de contas, sistemas e usuários; Alerta em tempo real;
6.2.3. Análise comportamental e mitigações de risco no ambiente crítico:

6.2.3.1. A solução deverá realizar a identificação e o correlacionamento de todas as ações citadas abaixo, montando perfis de comportamento gerais (usuários, acessos, credenciais, máquinas, outros) do ambiente privilegiado e acessos aos sistemas-alvo por meio da solução;
6.2.3.2. Deve combinar ações que caracterizam abusos, comportamentos anormais e fora dos padrões aprendidos/mapeados, aplicando ações mitigatórias automáticas como solicitação de nova autenticação multi-fator, suspensão e encerramento de sessões e troca das credenciais privilegiadas, em caso de atividades suspeitas de alto risco, detectando, no mínimo:
6.2.3.3. Acessos a solução: durante horários irregulares (quando um usuário recupera uma senha de conta privilegiada em uma hora irregular de acordo com seu perfil comportamental); durante dias irregulares (quando um usuário recupera uma senha de conta privilegiada em um dia irregular de acordo com seu perfil comportamental); através de IP irregular e desconhecido (quando um usuário acessa contas privilegiadas de um endereço IP ou sub-rede incomum, de acordo com seu perfil comportamental); não gerenciados (quando uma conexão com uma máquina é feita com uma conta privilegiada que não é gerenciada na solução);
6.2.3.3.1. Acessos gerais: excessivos a contas privilegiadas (quando um usuário acessa contas privilegiadas com mais frequência do que o normal, de acordo com seu perfil comportamental); a uma máquina; anômalos a várias máquinas (quando uma conta efetuou login em um grande número de máquinas inesperadas durante um tempo relativamente curto) e realizados fora da solução (diretamente no sistema-alvo); Usuários incomuns logando de uma máquina de origem conhecida; quando ocorrem indicações de atividade de um usuário inativo da solução; Atividades definidas como suspeitas detectadas em sessões privilegiadas (comandos e anomalias na solução);
6.2.3.3.1.1. Máquinas: acessadas a partir de endereços IP incomuns; acessadas durante horários irregulares, de acordo com seu padrão de utilização; Incomuns originando acessos;
6.2.3.3.1.2. Suspeita de roubo de credenciais, quando um usuário se conecta a uma máquina sem primeiro recuperar as credenciais necessárias da solução; Alteração de senha suspeita, quando é identificada uma solicitação para alterar ou redefinir uma senha ignorando a solução; Credenciais expostas de contas de serviço que se conectam ao LDAP em texto não criptografado;
6.2.3.3.1.3. Delegação não restrita, através da análise das contas de domínio, que recebem privilégios de delegação permissivos e, portanto, expõem o domínio a um alto risco; Contas privilegiadas com configuração SPN (nome principal de serviço) vulneráveis a ataques de força bruta e de dicionário off-line, permitindo que um usuário interno malicioso recupere a senha de texto sem criptografia da conta e Contas de serviço conectadas por meio de logon interativo;
6.2.3.4. Deve permitir a classificação de eventos por níveis de risco e respostas automáticas (suspensão e terminação de sessões) baseadas nos mesmos, com a possibilidade de colocar sessões em quarentena, pendentes de liberação e terminação pelo administrador, permitindo a configuração de eventos críticos a serem reportados automaticamente, baseados em Comandos Linux, Comandos, janelas e aplicações Windows, expressões regulares para comandos em geral e eventos configurados manualmente, permitindo a atribuição de nível de risco customizado.

6.2.4. Segurança contra tomada de controle da rede por meio de credenciais do Active Directory – A solução deve proteger e monitorar Controladores de Domínio Active Directory contra roubo de identidade, acesso não autorizado e ataques visando a tomada de controle da rede via estrutura de diretórios, de acordo com as funções de monitoramento de atividades internas nos mesmos e tráfego de segmentos de rede que estes estejam instalados, para confirmação de integridade das solicitações e tickets Kerberos utilizados nos equipamentos e contas de usuário detectando, no mínimo:
6.2.4.1. Atividades anômalas em tempo real, típicas de ataques ao protocolo de autenticação Kerberos, como roubo de credenciais, movimentação lateral e escalonamento de privilégios; A extração e uso de um Kerberos TGT (ticket de concessão de tickets) da memória LSASS (Subsistema de autoridade de segurança local) em um host para obter acesso a outros recursos da rede (Pass-the-ticket);
6.2.4.2. A recuperação e exploração de hashes de senha armazenados no banco de dados do SAM (Security Accounts Manager) ou do Active Directory para representar um usuário legítimo (Pass-the-Hash); O uso do hash de uma conta de usuário para obter um ticket do Kerberos, que é usado para acessar outras contas e recursos de rede (Overpass-the-Hash);
6.2.4.3. A modificação das configurações de permissão de ticket do Kerberos para obtenção de acesso não autorizado aos recursos da rede - PAC Forjado (Manipulação de Certificado de Atributo de Privilégio); A obtenção de acesso ao KDC (Kerberos Key Distribution Center) para geração de token principal de segurança que fornece acesso completo a um domínio inteiro (Golden Ticket); A recuperação maliciosa de credenciais do controlador de domínio (DCSync);
6.2.5. Arquitetura e Segurança da Solução:
6.2.5.1. Incorporar medidas de segurança como Certificação Common Criteria (CC) – ISO/IEC 15408 – como garantia de segurança do método utilizado no desenvolvimento do sistema de repositório seguro de credenciais e Criptografia dos módulos da solução, a fim de proteger a informação em trânsito entre módulos da solução e aplicações web dos usuários finais e possibilitar a utilização de criptografia do banco de dados utilizado pela solução para armazenar as credenciais gerenciadas pela mesma, sendo compatível com; AES com chaves de 256 bits, FIPS 140-2 e Encriptação PKCS#11 ou superior;
6.2.5.2. Deve utilizar banco de dados em alta disponibilidade, para armazenamento de credenciais, com as melhores práticas de segurança: mecanismo de blindagem do sistema operacional através da desativação ou desinstalação de serviços e portas de acesso não essenciais ao funcionamento da solução. Caso o banco de dados utilizado para armazenamento de credenciais seja de terceiros, a solução deverá ser entregue com licenças de software, garantia e suporte que o compatibilize com a solução.
6.2.5.3. Suportar a implementação em parque computacional Windows Server 2012 R2, Windows Server 2016, Windows Server 2022 e/ou Linux em ambiente físico ou virtualizado com infraestrutura (servidores/software em ambiente virtualizado, S.O., camada de balanceamento/redirecionamento de tráfego, etc.) provida pela CONTRATANTE para implantação e uso da solução em alta disponibilidade.
6.2.5.4. Os elementos críticos da solução, como Repositório Seguro de credenciais, Gateways de Gravação e Monitoração Comportamental deverão ser instalados em alta disponibilidade ativo-ativo em cada uma das localidades (site principal e site redundante adicional), com chaveamento entre localidades (sites), garantindo que o processo seja transparente aos usuários conectados e a normalização das funcionalidades ocorra em até 5 (cinco) minutos, caso exista perda de comunicação e mecanismos para a recuperação de desastres compatível com soluções de backup e arquivamento disponíveis no mercado.
6.2.5.5. Prover, no mínimo, dois ambientes adicionais externos da solução em produção para testes e homologação, replicando as mesmas licenças e funcionalidades do ambiente de produção.

6.3. Solução de Segurança para Privilégios e Acessos – Proteção para Equipamentos Servidores:
6.3.1. Proteção local para Servidores Unix/Linux
6.3.1.1. As funcionalidades devem ser providas por meio de agentes instalados no sistema operacional dos servidores e permitir a proteção e controle dos privilégios em contas de usuário em equipamentos Unix, Linux, Solaris e AIX e associar os privilégios e comandos controlados às contas cadastradas no repositório seguro de credenciais, realizando o controle no próprio sistema operacional;
6.3.1.2. Garantir o controle e bloqueio de comandos, mesmo que o acesso seja realizado diretamente no servidor de destino (sem passar pelos monitores/gravadores de acessos) fazendo uso das funcionalidades instaladas no sistema operacional alvo.
6.3.1.3. Disponibilizar, como conjunto mínimo de atividades controladas no ativo de destino, as seguintes operações: criação e exclusão de arquivos e diretórios, mudança de nome de arquivos e diretórios, abertura de arquivos para escrita, comandos chown e chmod e ligações entre arquivos.
6.3.1.4. Implementar restrições, em uma plataforma, de maneira global ou em uma conta de usuário ou grupo de maneira granular.
6.3.1.5. Realizar o controle mediante interceptação do comando antes que ele seja executado, permitir a liberação de comandos privilegiados a usuários comuns, permitir que os comandos executados em sistemas monitorados sejam gravados em modo texto no repositório seguro de credenciais, permitir o agrupamento de comandos, bem como a utilização de coringas como (*), para uma definição ampla de parâmetros;
6.3.1.6. Permitir que sejam atribuídas permissões para usuários e grupos, inclusive do Active Directory e oferecer a capacidade de verificação da identidade da pessoa que executa comandos localmente no dispositivo alvo através de autenticação via usuário da ferramenta, LDAP ou RADIUS;
6.3.1.7. A solução deverá possuir funcionalidade que permita definir variáveis de ambiente no momento da execução de um comando, independentemente da definição realizada pelo usuário ou seu perfil. Sendo exigido no mínimo as seguintes variáveis: PATH, ENV, BASH_ENV, GLOBIGNORE, SHELLOPTS;
6.3.1.8. Possibilitar o uso da máscara de usuário na execução dos comandos (valores entre 0000 e 0777);
6.3.1.9. Impedir a utilização da técnica de ShellEscape, em que um programa autorizado e executado com privilégios permita a execução de outros programas e consequentemente escape dos controles definidos;
6.3.1.10. Disponibilizar a funcionalidade de restrição de Shell, que impossibilite que scripts e shells de sistema executem comandos não permitidos pelas regras definidas na solução;
6.3.1.11. Monitorar e exibir acessos e atividades realizadas no próprio sistema l) Possibilitar mapear e coletar atividades regulares de usuários através do modo observação, agregando e exportando os resultados para um perfil;
6.3.1.12. Prover um controle de comandos completo, com a possibilidade de criar uma lista de comandos permitidos e bloqueados (whitelisting/blacklisting), a serem alterados (criação de alias) ou prevenir que comandos sejam executados ou permitir trabalhar em Shell modificado/controlado;
6.3.1.13. Prover meios de permitir que os usuários executem comandos específicos e conduzam sessões remotamente baseado em regras sem autenticar-se diretamente utilizando credenciais privilegiadas;
6.3.2. Proteção local para Servidores Windows
6.3.2.1. Realizar varredura e inventário de aplicações instaladas no sistema operacional;
6.3.2.2. As funcionalidades devem ser providas por meio de agentes instalados no sistema operacional dos servidores e permitir a proteção e controle dos privilégios;
6.3.2.3. Garantir o controle e bloqueio de comandos, mesmo que o acesso seja realizado diretamente no servidor de destino (sem ser através dos monitores/gravadores de acessos);
6.3.2.4. Oferecer opções de execução sem aviso: de aplicações com privilégios em modo explícito e transparente, monitorada de aplicações em modo explícito e transparente, com restrições de aplicações em modo explícito e transparente;
6.3.2.5. Exibir a reputação do arquivo executado advinda de, pelo menos, 1 (uma) fonte externa e disponibilizar a opção de encaminhamento de arquivo suspeito para análise de malware em soluções de mercado;
6.3.2.6. Suportar, no mínimo, as versões Windows Server 2003 SP2 x32 & x64, Windows Server 2008 x32 & x64, Windows Server 2008 R2 x64, Windows Server 2012/2012 R2, Windows Server 2016, Windows Server 2019 e Windows Server 2022;
6.3.2.7. Implementar regras de controle de aplicações permitidas e bloqueadas para execução fazendo uso das funcionalidades instaladas no sistema operacional alvo, independentemente do acesso ao ativo ser realizado via monitores/gravadores de acessos ou diretamente no ativo;
6.3.2.8. Implementar regras de controle do nível de privilégio utilizado na execução das aplicações permitidas fazendo uso das funcionalidades instaladas no sistema operacional alvo, independentemente do acesso ao ativo ser realizado via monitores/gravadores de acessos ou diretamente no ativo;
6.3.2.9. Implementar controle de nível de privilégio independentemente da permissão que o usuário possua localmente no ativo ou no domínio, permitindo que usuários restritos executem atividades com nível administrativo;
6.3.2.10. Permitir atribuição granular para execução de aplicações com nível de privilégio administrativo, sem que esse privilégio seja global na máquina;
6.3.2.11. Fazendo uso das funcionalidades instaladas no sistema operacional alvo, deve permitir a criação de políticas reutilizáveis, contendo, no mínimo, os seguintes tipos de aplicações ou tipos de arquivos: executáveis, scripts, aplicações nativas Windows, bibliotecas dinâmicas (DLL), instaladores, controles ActiveX, objetos COM;
6.3.2.12. Implementar a verificação de checksum do arquivo, dos parâmetros permitidos e da assinatura de fabricante, para objetos reutilizáveis da solução;
6.3.2.13. Implementar o suporte ao nome exato da aplicação/arquivo/script e expressões regulares em qualquer formato, para objetos reutilizáveis da solução;
6.3.2.14. Utilizar eventos reportados na interface da ferramenta para criação de novas políticas ou incluí-los em políticas existentes;
6.3.2.15. Permitir agrupar aplicações com base em suas características, para facilitar a inserção de novas aplicações aos grupos ou políticas de segurança de aplicações já criadas;
6.3.2.16. Impedir a desativação das funcionalidades instaladas no sistema operacional alvo sem autorização e/ou registro da atividade por meio da interface de gerência;
6.3.2.17. Disponibilizar o registro das execuções e atividades dos usuários, facilitando a criação de políticas baseadas em comportamento conhecido;
6.3.2.18. Monitorar e exibir acessos e atividades realizadas na própria solução;
6.3.2.19. Deve permitir autorização de acesso às aplicações e arquivos, quando incluídos em regras, individualmente ou em grupos;
6.3.2.20. Deve realizar varreduras fazendo uso das funcionalidades instaladas no sistema operacional alvo para catalogar arquivos existentes nas máquinas e uni-los ao inventário populado mediante detecção durante a execução;
6.3.2.21. Deve verificar a reputação dos arquivos executados e detectados pelas funcionalidades instaladas no sistema operacional alvo ou órgãos de controle de ameaças, como por exemplo o VirusTotal.com ou similares;
6.3.2.22. Deve permitir a execução automática de tipos desconhecidos de arquivo, de acordo com sua origem, mesmo possuindo restrições;
6.3.2.23. Possibilitar o monitoramento e a criação de evidência em vídeo de certas execuções de arquivo e de execuções sob certas condições definidas em política;
6.3.2.24. Possibilitar ao usuário final a solicitação de liberação de atividades específicas fazendo uso das funcionalidades instaladas no sistema operacional alvo;
6.3.2.25. Possibilitar a liberação emergencial da execução de comandos e elevação de privilégios sem desativar a solução, caso o usuário esteja off-line;
6.3.2.26. Implementar as regras de controle de acordo com características do usuário final, incluindo nome de usuário, grupos a que o usuário pertence e endereço IP;
6.3.2.27. Oferecer monitoramento de atividade maliciosa dos processos em execução, visando detectar tentativas de roubo de credenciais;
6.3.2.28. Fazendo uso das funcionalidades instaladas no sistema operacional alvo, a solução deve alertar, reportar e bloquear atividade anômala de arquivos e usuários durante a interação com bases de senhas no formato hash, como por exemplo, SAM local e LSASS;
6.3.2.29. Caso o dispositivo não possa estar conectado de forma permanente aos monitores/gravadores de acessos da solução e repositório seguro de credenciais, deve, de forma autônoma e off-line, gerenciar as senhas das credenciais locais, aplicando políticas de randomização e sincronização das senhas definidas na central da solução;
6.3.2.30. Permitir o envio de arquivos suspeitos, executados sob sua supervisão, para soluções de análise de ameaça do tipo Sandbox;
6.3.2.31. Possibilitar a execução de aplicativos que precisam de privilégio de execução a usuários não-privilegiados;
6.3.2.32. Permitir criar uma whitelist, onde é configurado todos os aplicativos que podem ser executados e qualquer outra aplicação fora desta lista automaticamente seja bloqueada;
6.3.2.33. Possuir uma integração com Windows UAC, e conter relatórios do uso de prompts aos usuários feitos pelo UAC;
6.3.2.34. Suportar a guarda de políticas de hosts que não façam parte do Active Directory ii) Manter todas as políticas em cache e serem aplicadas ao endpoint, ainda que o mesmo não esteja conectado à rede corporativa;
6.3.2.35. Deve permitir que mensagens customizadas sejam mostradas antes que uma aplicação seja executada ou bloqueada;
6.3.2.36. Deve suportar adição múltiplas mensagens, estas mensagens devem possibilitar edição e suportar múltiplas linguagens;
6.3.2.37. Deve possuir capacidade de relatórios de aplicações e eventos de usuários inclusos na solução;
6.3.2.38. Realizar varredura e inventário de aplicações instaladas no sistema operacional;
6.3.2.39. Deve permitir a configuração de "iscas", como senhas e credenciais falsas de administrador local para detecção de ataques em andamento e bloqueio proativo;

6.3.3. Solução de Segurança para Privilégios e Acessos – Proteção para Estações de Trabalho:
6.3.3.1. As funcionalidades devem ser instaladas no sistema operacional das estações de trabalho e permitir a proteção dos ativos;
6.3.3.2. As funcionalidades devem ser instaladas no sistema operacional das estações de trabalho e permitir o controle dos privilégios;
6.3.3.3. Garantir o controle e bloqueio de comandos, mesmo que o acesso seja realizado diretamente no servidor de destino (sem ser através dos monitores/gravadores de acessos);
6.3.3.4. Oferecer opções de execução sem aviso: de aplicações com privilégios em modo explícito e transparente, monitorada de aplicações em modo explícito e transparente, com restrições de aplicações em modo explícito e transparente;
6.3.3.5. Exibir a reputação do arquivo executado advinda de, pelo menos, 1 (uma) fonte externa e disponibilizar a opção de encaminhamento de arquivo suspeito para análise de malware em soluções de mercado;
6.3.3.6. Suportar, no mínimo, as versões de estações de trabalho: Windows XP SP3, Windows Vista SP1, Windows 7 x32 & x64, Windows 8/8.1 x32 & x64, Windows 10 x32 & x64, Windows 11 x32 & x64;
6.3.3.7. Implementar regras de controle de aplicações permitidas e bloqueadas para execução fazendo uso das funcionalidades instaladas no sistema operacional alvo, independentemente do acesso ao ativo ser realizado via monitores/gravadores de acessos ou diretamente no ativo;
6.3.3.8. Implementar regras de controle do nível de privilégio utilizado na execução das aplicações permitidas fazendo uso das funcionalidades instaladas no sistema operacional alvo, independentemente do acesso ao ativo ser realizado via monitores/gravadores de acessos ou diretamente no ativo;
6.3.3.9. Implementar controle de nível de privilégio independentemente da permissão que o usuário possua localmente no ativo ou no domínio, permitindo que usuários restritos executem atividades com nível administrativo;
6.3.3.10. Permitir atribuição granular para execução de aplicações com nível de privilégio administrativo, sem que esse privilégio seja global na máquina;
6.3.3.11. Fazendo uso das funcionalidades instaladas no sistema operacional alvo, deve permitir a criação de políticas reutilizáveis, contendo, no mínimo, os seguintes tipos de aplicações ou tipos de arquivos: executáveis, scripts, aplicações nativas Windows, bibliotecas dinâmicas (DLL), instaladores, controles ActiveX, objetos COM;
6.3.3.12. Implementar a verificação de checksum do arquivo, dos parâmetros permitidos e da assinatura de fabricante, para objetos reutilizáveis da solução;
6.3.3.13. Implementar o suporte ao nome exato da aplicação/arquivo/script e expressões regulares em qualquer formato, para objetos reutilizáveis da solução;
6.3.3.14. Utilizar eventos reportados na interface da ferramenta para criação de novas políticas ou incluí-los em políticas existentes;
6.3.3.15. Permitir agrupar aplicações com base em suas características, para facilitar a inserção de novas aplicações aos grupos ou políticas de segurança de aplicações já criadas;

6.3.3.16. Impedir a desativação das funcionalidades instaladas no sistema operacional alvo sem autorização e/ou registro da atividade por meio da interface de gerência;
6.3.3.17. Disponibilizar o registro das execuções e atividades dos usuários, facilitando a criação de políticas baseadas em comportamento conhecido;
6.3.3.18. Monitorar e exibir acessos e atividades realizadas na própria solução;
6.3.3.19. Deve permitir autorização de acesso às aplicações e arquivos, quando incluídos em regras, individualmente ou em grupos;
6.3.3.20. Deve realizar varreduras fazendo uso das funcionalidades instaladas no sistema operacional alvo para catalogar arquivos existentes nas máquinas e uni-los ao inventário populado mediante detecção durante a execução;
6.3.3.21. Deve verificar a reputação dos arquivos executados e detectados pelas funcionalidades instaladas no sistema operacional alvo ou órgãos de controle de ameaças, como por exemplo o VirusTotal.com ou similares;
6.3.3.22. Deve permitir a execução automática de tipos desconhecidos de arquivo, de acordo com sua origem, mesmo possuindo restrições;
6.3.3.23. Possibilitar o monitoramento e a criação de evidência em vídeo de certas execuções de arquivo e de execuções sob certas condições definidas em política;
6.3.3.24. Possibilitar ao usuário final a solicitação de liberação de atividades específicas fazendo uso das funcionalidades instaladas no sistema operacional alvo;
6.3.3.25. Possibilitar a liberação emergencial da execução de comandos e elevação de privilégios sem desativar a solução, caso o usuário esteja off-line;
6.3.3.26. Implementar as regras de controle de acordo com características do usuário final, incluindo nome de usuário, grupos a que o usuário pertence e endereço IP;
6.3.3.27. Oferecer monitoramento de atividade maliciosa dos processos em execução, visando detectar tentativas de roubo de credenciais;
6.3.3.28. Fazendo uso das funcionalidades instaladas no sistema operacional alvo, a solução deve alertar, reportar e bloquear atividade anômala de arquivos e usuários durante a interação com bases de senhas no formato hash, como por exemplo, SAM local e LSASS.
6.3.3.29. Caso o dispositivo não possa estar conectado de forma permanente aos monitores/gravadores de acessos da solução e repositório seguro de credenciais, deve, de forma autônoma e off-line, gerenciar as senhas das credenciais locais, aplicando políticas de randomização e sincronização das senhas definidas na central da solução;
6.3.3.30. Permitir o envio de arquivos suspeitos, executados sob sua supervisão, para soluções de análise de ameaça do tipo Sandbox;
6.3.3.31. Possibilitar a execução de aplicativos que precisam de privilégio de execução a usuários não-privilegiados;
6.3.3.32. Permitir criar uma whitelist, onde é configurado todos os aplicativos que podem ser executados e qualquer outra aplicação fora desta lista automaticamente seja bloqueada;
6.3.3.33. Possuir uma integração com Windows UAC, e conter relatórios do uso de prompts aos usuários feitos pelo UAC;
6.3.3.34. Suportar a guarda de políticas de hosts que não façam parte do Active Directory;
6.3.3.35. Manter todas as políticas em cache e serem aplicadas ao endpoint, ainda que o mesmo não esteja conectado à rede corporativa;
6.3.3.36. Deve permitir que mensagens customizadas sejam mostradas antes que uma aplicação seja executada ou bloqueada;
6.3.3.37. Deve suportar adição múltiplas mensagens, estas mensagens devem possibilitar edição e suportar múltiplas linguagens;
6.3.3.38. Deve possuir capacidade de relatórios de aplicações e eventos de usuários inclusos na solução;
6.3.3.39. Realizar varredura e inventário de aplicações instaladas no sistema operacional;
6.3.3.40. Deve permitir a configuração de "iscas", como senhas e credenciais falsas de administrador local para detecção de ataques em andamento e bloqueio proativo;
6.3.3.41. A solução deverá ser capaz de atender minimamente os seguintes casos de uso para requisitar um e mais fatores de autenticação:
6.3.3.41.1. Nas telas de login e desbloqueio de sistemas operacionais Windows e MacOs;
6.3.3.41.2. Multi Fator de autenticação para soluções de VPN via RADIUS ou SAML;
6.3.3.41.3. Qualquer dispositivo ou sistema operacional que suporte RADIUS;
6.3.3.41.4. Plugin para ADFS (IDP, Identity Provider), Active Directory Federation Services;
6.3.3.41.5. Sob demanda utilizando o protocolo Oauth e REST APIs;
6.3.3.41.6. Para realizar o autosserviço de reset de senha ou desbloqueio de usuário;
6.3.3.42. A solução deverá ser capaz de oferecer minimamente os seguintes métodos para múltiplo fator de autenticação:
6.3.3.43. Usuário e senha dos diretórios suportados na solução:
6.3.3.43.1. Através de aplicativo para dispositivos móveis do tipo IOS e Android, oferecendo suporte para;
6.3.3.43.2. Biometria do tipo FaceID;
6.3.3.43.3. Biometria através do leitor de digital;
6.3.3.43.4. Smartphone push (Notificação para aprovar ou recusar uma autenticação);
6.3.3.43.5. Geolocalização através de coodernadas GPS e banco de dados de IPs;
6.3.3.43.6. Suporte a tokens OATH OTP;
6.3.3.43.7. Autenticação na tela de login via QRcode sem a necessidade de digitar usuário e senha, com opção de forçar a biometria no dispositivo móvel;
6.3.3.43.8. Confirmação de código via e-mail;
6.3.3.44. Clientes do tipo OATH OTP (exemplo, Google Authenticator);
6.3.3.45. Autenticadores que suportem FIDO2 / U2F, minimamente suportando:
6.3.3.45.1. Windows Hello;
6.3.3.45.2. Yubikey;
6.3.3.45.3. Google Titan Key;
6.3.3.45.4. MacOS TouchID;
6.3.3.46. Perguntas e respostas previamente configuradas;
6.3.3.47. Permitir que os usuários realizem o autosserviço de reset de senha e desbloqueio de usuário utilizando os métodos de múltiplo fator de autenticação citados para verificação positiva através do portal da solução, tela de login de sistemas operacionais Windows e através de REST APIs oferecidas pela solução;
6.3.3.48. Para cada caso de uso ou conjunto de casos de uso de múltiplo fator de autenticação citados, a solução de ser capaz de identificar os atributos de contexto de cada autenticação para disponibilizar os melhores métodos definidos para a autenticação, suportando minimamente:
6.3.3.48.1. Endereçamento IP;
6.3.3.48.2. Dia da Semana;
6.3.3.48.3. Datas específicas;
6.3.3.48.4. Janelas de tempo entre duas datas;
6.3.3.48.5. Janelas de tempo entre horários (exemplo, horário comercial);
6.3.3.48.6. Tipo do Sistema Operacional;
6.3.3.48.7. Tipo do Browser;
6.3.3.48.8. Perfis configurados na solução;
6.3.3.48.9. País que está sendo realizado o acesso;
6.3.3.48.10. Se é um dispositivo gerenciado;
6.3.3.48.11. Autenticação via certificado;
6.3.3.48.12. Nível de Risco da autenticação medido por um motor de análise de comportamento dos usuários;
6.3.3.49. A solução deve ter capacidade de detectar casos de uso e perfis de autenticação já validados pelo usuários e não requisitar mais os mesmos durante um período de tempo configurado pelo administrador da solução, evitando desta forma repetidas validações em um curto espaço de tempo;
6.3.3.50. O conjunto de fatores de autenticação disponibilizados devem ser baseados durante o acesso através de regras especificadas no item anterior e segregados por:
6.3.3.50.1. Conjunto de aplicações;
6.3.3.50.2. Uma única aplicação;
6.3.3.50.3. Regras para o autosserviço de reset de senha e desbloqueio de usuário;
6.3.3.50.4. Portal do Administrador;
6.3.3.50.5. Portal do Usuário;
6.3.3.51. A solução deve prover um aplicativo móvel para Android e IOS com as seguintes características:
6.3.3.51.1. Depois de efetuado o login apresentar as aplicações WEB disponíveis para realizar o SSO, através de um conjunto de ícones onde cada um representa uma aplicação que o usuário tem o direito de efetuar o SSO já integrado com os navegadores instalados nos dispositivos móvel;
6.3.3.51.2. Prover login através do scan de QRcode no portal web permitindo SSO sem identificação de usuário e senha;
6.3.3.51.3. Configurar OATH OTP adicionais provenientes de outras soluções;
6.3.3.51.4. Configurar OATH OTP para autenticação multi fator nos sistemas operacionais Windows (telas de login e bloqueio) quando os mesmos estão desconectados da internet;
6.3.3.51.5. Verificar dispositivos registrados (dispositivos móveis e sistemas operacionais);
6.3.3.51.6. Integração nativa com FaceID, TouchID, leitor biométrico dos dispositivos móveis alavancando os mesmos para autenticação biométrica durante login nas aplicações;
6.3.3.51.7. Reportar coordenadas GPS para os sistemas que utilizam geolocalização;
6.3.3.52. O aplicativo deve suportar autenticação do tipo push, onde o usuário tem a escolha de aceitar ou recusar o desafio, esta notificação de conter minimamente: IP de origem de acesso, Data e Hora, Cidade / Geolocalização do acesso, Aplicação sendo acessada;
6.3.3.53. A solução dever ser baseada em algoritmos de aprendizado de máquina (Machine Learning) não supervisionados, ou seja, os modelos estatísticos com os casos de uso já prontos e calibrados;
6.3.3.54. A solução deve medir o risco da autenticação verificando o comportamento histórico da identidade através do conjunto dos seguintes atributos;
6.3.3.55. Geo Velocidade, medindo velocidade de deslocamento do login, comparando a localização do último login com a atual, evitando "viagens impossíveis", e traçando o comportamento do usuário neste quesito, por exemplo, pessoas que viajam muito podem ter uma pontuação de risco baixa mesmo que sua Geo Velocidade seja maior que pessoas que não viajam;
6.3.3.56. Geo Localização: medindo o risco da autenticação verificando sua localização geográfica do acesso atual em comparação com o seu comportamento usual;
6.3.3.57. Dia da Semana: medindo o risco da autenticação verificando o dia da semana do acesso atual em comparação com seu comportamento usual;
6.3.3.58. Horário do Acesso: mede o risco da autenticação verificando o horário do acesso atual em comparação com seu comportamento usual;
6.3.3.59. Sistema Operacional: mede o risco da autenticação verificando o Sistema Operacional do acesso atual em comparação com seu comportamento usual;
6.3.3.60. Falhas de login consecutivas, mede o risco da autenticação verificando as falhas de login consecutivas do acesso atual em comparação com seu comportamento usual iii) Deve prover a personalização das faixas de pontuação (0 a 100) para os administradores da solução para, no mínimo, as categorias: Sem risco, Risco Baixo, Risco Médio e Risco Alto;
6.3.3.61. Deve prover para os administradores da solução a personalização da influência na medição do risco para cada atributo citado neste item. Por exemplo, para a CONTRATANTE a geo velocidade pode ser um fator que não possui relevância, desta forma deve ser possível configurar a influência deste risco como baixa na modelagem de risco da plataforma;
6.3.3.62. O risco calculado durante a autenticação pelo motor de análise do comportamento dos usuários deve ser compartilhado com funções de Múltiplo Fator de autenticação e Single Sign-On que realizam o login para os casos de uso citados neste documento e utilizar como contexto para:
6.3.3.62.1. Requisitar múltiplos fatores de autenticação de forma dinâmica;
6.3.3.62.2. Permitir o login sem o uso de múltiplos fatores;
6.3.3.62.3. Negar a autenticação;
6.3.3.63. Deve prover para os administradores da solução a capacidade de explorar os dados históricos através de dashboards, filtros e gráficos configuráveis sendo possível verificar os alertas e os fatores que os influenciaram, além da exploração dos eventos capturados e seus atributos;
6.3.3.64. Deve prover gráficos de linha do tempo, donuts, mapas com geolocalização dos eventos, gráfico de barras, tabelas analíticas, e mapas de relacionamento, sendo suas dimensões e categorias personalizáveis;
6.3.3.65. Deve ser capaz de exportar os dados dos alertas, riscos calculados, eventos para, no mínimo, CSV, adicionalmente gravar as visualizações na solução para consultas posteriores;
6.3.3.66. Deve possuir integração com fontes de inteligência cibernética de terceiros reconhecidas no mercado, como, por exemplo, Palo Alto Cloud;
6.3.3.67. Deve possuir interface para envio de alertas de forma automatizada, suportando, no mínimo E-mail com conteúdo do alerta e Webhooks (ex: envio de mensagem para um canal do Microsoft Teams ou Slack;
6.3.3.68. Possuir dashboards pré-configurados com informações e gráficos com as seguintes características:
6.3.3.68.1. Utilização do Motor de Análise do Comportamento dos Usuários;
6.3.3.68.2. Comportamento dos usuários na utilização das aplicações;
6.3.3.68.3. Visão sobre a segurança das aplicações;
6.3.3.68.4. Mapa com a geolocalização das autenticações;
6.3.3.68.5. Visão sobre o comportamento dos Endpoints (Mobile e Computadores);
6.3.3.68.6. Visão sobre o comportamento das Identidades;

6.3.4. Serviço especializado para implementação, configuração e transferência de conhecimento da solução de Segurança para Sistemas Críticos:
6.3.4.1. O serviço de implementação e configuração deve ser executado em até 30 dias após a instalação da solução no ambiente do TJAM;
6.3.4.2. O serviço de transferência de conhecimento abrange, entre outras, as seguintes atividades:
6.3.4.2.1. Elaboração de documentação técnica e de usuário;
6.3.4.2.2. Transferência de conhecimentos relacionados ao desenvolvimento, implantação e manutenção no ambiente do TJAM;
6.3.4.2.3. Levantamento de informações junto aos usuários, objetivando a definição e elaboração de regras e políticas;
6.3.4.2.4. Corrigir ou apoiar em problemas e defeitos em funcionalidades já existentes;
6.3.4.2.5. Realização de operação assistida e monitoramento de ambientes entregues com a solução;
6.3.4.2.6. Orientar na utilização dos softwares instalados no TJAM com a utilização das melhores práticas e orientações dos fabricantes;
6.3.4.2.7. Apoiar na atualização, instalação e/ou reinstalação de novas versões e dos produtos instalados no TJAM minimizando impactos;
6.3.4.2.8. Apoiar na configuração/parametrização do sistema em novas máquinas;
6.3.4.2.9. Orientar no levantamento de informações que possibilite a identificação de novas necessidades, detectadas no ambiente do TJAM;
6.3.4.2.10. Diagnosticar o bom funcionamento das ferramentas instaladas, garantindo a máxima utilização dos recursos oferecidos;
6.3.4.2.11. Identificar e elaborar proposição de melhoria em performance, desempenho, tunning, disponibilidade e confiabilidade em ambientes;
6.3.4.2.12. Otimizar a reinstalação e/ou adaptação das ferramentas em outros equipamentos que não seja onde originalmente os sistema e produtos foram instalados;
6.3.4.2.13. Definir metodologia, elaborar relatórios e projetos e acompanhar a configuração e utilização de solução de alta disponibilidade, repassando aos técnicos da TI do TJAM as melhores práticas para uso da solução, quanto a parametrização e configuração dos componentes e ferramentas utilizadas no TJAM;
6.3.4.2.14. Esclarecer dúvidas e orientar os técnicos de TI do TJAM, sobre integração das soluções, abrangendo as diversas plataformas existentes no ambiente computacional do TJAM;
6.3.4.2.15. Apoiar no planejamento, na execução e na avaliação das mudanças no ambiente;
6.3.4.2.16. Analisar patches, correções e novas versões e sugerir a aplicação ou não dos mesmos no ambiente;
6.3.4.2.17. Apoiar no planejamento, na execução e na avaliação das atualizações de versões e aplicação de patches da ferramenta;
6.3.4.2.18. Apoiar no planejamento, na execução e na avaliação de implantação de novas aplicações ou atualização de aplicações no ambiente;
6.3.4.2.19. Efetuar a transferência de tecnologia para a equipe do TJAM;

6.3.5. Solução de segurança para identidades e acessos – Proteção para Aplicações Tradicionais

6.3.5.1 Uma aplicação gerenciada é definida como a aplicação que faz uso direto dos recursos e credenciais gerenciadas pela solução para concessão de acesso ao seu ambiente (substituindo o uso de credenciais hard coded, por exemplo).

6.3.5.2 Deve permitir a integração de servidores de aplicação e o repositório digital seguro, eliminando a necessidade de senhas e chaves SSH embutidas em aplicações, scripts e arquivos de configuração.

6.3.5.3 Deve possuir mecanismo de segurança que evite a parada de aplicações críticas, mantendo a entrega das credenciais em caso de queda da rede ou parada total da solução que gerencia as credenciais por meio do repositório seguro.

6.3.5.4 Deve fornecer credenciais, pelo menos, via consulta de rede ou Web service.

6.3.5.5 Deve garantir a entrega de credenciais localmente nos servidores de aplicação, garantindo baixa latência para aplicações de missão crítica.

6.3.5.6 Deve manter um cache local atualizado das credenciais utilizadas no servidor de aplicação, a fim de prevenir falhas na comunicação com o repositório seguro e trazer velocidade às consultas

6.3.5.7 Deve suportar redundância de credenciais, oferecendo, de maneira transparente, mais de um usuário e senha à aplicação crítica, de forma que se evite qualquer possível indisponibilidade mínima durante o processo de troca de senhas;

6.3.5.8 Deverá oferecer SDKs documentados para integração com aplicações em Java, C/C++ e .Net

6.3.5.9 Deverá suportar a utilização de executável para scripts e aplicações nativas em plataforma Windows

6.3.5.10 Deverá suportar a utilização integração com servidores WebSphere, WebLogic, JBoss e Tomcat, para fornecimento de credenciais via XML datasources

6.3.5.11 Deverá suportar a autenticação de aplicações que consultam credenciais, permitindo definir o caminho da aplicação, usuário do sistema operacional, endereço do servidor e hash do código.

6.3.5.12 Ser disponibilizada com um SDK (Software Development Kit) que pode ser configurado para permitir que aplicações possam Solicitar as credenciais sob demanda, ao invés de utilizar credenciais estáticas;

6.3.5.13 Atualizar informações de contas automaticamente no banco de dados de senhas;

6.3.5.14 Inscrever automaticamente dispositivos alvo, sem aguardar por atualizações dinâmicas;

6.3.5.15 Alterar senhas em texto claro (incorporado em aplicações), de forma segura no banco de dados de senhas;

6.3.5.16 Visando a garantia do funcionamento da solução como um todo, este item deve ser entregue com total integração com o item 1 desta especificação.

6.4. Catálogo e/ou Amostras

6.4.1 Deverá ser apresentado catálogo, folder, manual ou sítio da internet que comprove que todos os materiais e equipamentos a serem utilizados atendem rigorosamente as especificações técnicas mínimas exigidas.

6.4.2 Não há necessidade de apresentar amostra de nenhum item.

6.4.3 A Divisão de Tecnologia da Informação e Comunicação do TJAM, sito a Avenida André Araújo s/n, Prédio Desembargador Arnoldo Péres - Bairro Aleixo – CEP 69.060-000 será a responsável por receber e validar os objetos desta contratação.

6.5 Vistoria Técnica.

6.5.1 As interessadas poderão realizar, sob o acompanhamento de servidor especialmente designado, vistoria aos locais de execução dos serviços, no todo ou em parte, em data e horário previamente acordados segundo a conveniência deste Órgão, com o objetivo de conhecer as instalações onde serão executados os serviços e sanar as dúvidas porventura existentes, a fim de subsidiar a elaboração das propostas a serem submetidas ao certame;

6.5.2 As visitas deverão ser previamente agendadas, com 72 (setenta e duas) horas de antecedência, pelo telefone (92) 2129-6779 – DIVISÃO DE INFRAESTRUTURA DE TECNOLOGIA DA INFORMAÇÃO E COMUNICAÇÃO, no período das 8 às 14hs, ou via e-mail através de: infra.tic@tjam.jus.br.

6.6 Planejamento e execução dos serviços

6.6.1 A Contratada deverá instalar e configurar os serviços nas dependências do TJAM e/ou remotamente de modo a viabilizar a execução do objeto.
6.6.2 Se houver necessidade ou risco de interrupção do serviço, a implantação deverá ser realizada em horário específico a ser indicado pela Divisão de Infraestrutura de TIC, podendo ser realizada em finais de semana ou feriados, sem qualquer custo adicional para o TJAM.

6.6.3 Os trabalhos serão coordenados e acompanhados por técnicos do TJAM e deve haver repasse de conhecimento durante a execução dos serviços.
6.6.4 Para efeitos de aceite definitivo, a conclusão dos serviços de instalação e configuração será dada pela entrega da solução adquirida em pleno funcionamento, de acordo com as especificações.
6.6.5 No caso de serviços sob demanda, o prazo de entrega será aquele definido nas Ordens de Serviço.

6.7 Local e Prazos de Execução

6.7.1 Em até 10 (dez) dias corridos, contados da assinatura do contrato, recebimento da Nota de Empenho e da Ordem de Serviço.

6.7.2 A CONTRATADA deverá entregar um projeto executivo para a implantação dos serviços contendo no mínimo:

6.7.2.1 Responsável pela implantação.

6.7.2.2 Cronograma de implantação.

6.7.2.3 3. Cronograma de reuniões de acompanhamento.

6.7.3 A CONTRATADA deverá concluir os serviços de instalação e ativação de todo o objeto nos seguintes prazos:

6.7.3.1. Em até 30 (trinta) dias corridos, contados da entrega do projeto executivo pela CONTRATADA.

6.7.3.3. Durante a implantação, independente da periodicidade das reuniões de acompanhamento, a CONTRATADA deverá apresentar semanalmente relatórios do andamento das ações previstas no cronograma.

6.7.4. Os desalinhamentos no cronograma que possam comprometer as datas previstas para as entregas devem ser informados a CONTRATANTE a fim de buscar alternativas de remediação dos problemas.

6.7.5. Considera-se o serviço ativado quando, após comunicação oficial da CONTRATADA informando a efetiva instalação, configuração e disponibilização do serviço, for realizado teste de conectividade pelos técnicos da CONTRATANTE, identificado o atendimento de todos os requisitos técnicos para os links, inclusive de monitoração.

6.7.6. O não cumprimento dos prazos e das condições de entrega dos serviços sujeitará a CONTRATADA às sanções administrativas previstas no Termo de Referência.

6.8 Forma de Execução dos serviços

6.8.1 A execução dos serviços será sob demanda, no regime de empreitada por preço unitário.

6.8.2 Todos os itens serão atendidos por fornecedor único, uma vez que os serviços pretendidos estão intrinsecamente relacionados. A adjudicação dos itens para empresas diferentes poderia resultar na aquisição de soluções incompatíveis, o que acarretaria prejuízo à CONTRATANTE.

6.9 Previsão dos Recursos

6.9.1 Para a execução dos serviços de instalação e configuração, a licitante Contratada deverá alocar profissionais devidamente habilitados pelo fabricante.

6.9.2 A licitante deverá apresentar, no mínimo, um profissional certificado, dentro da equipe que irá executar os serviços.

6.10 Garantia ou Assistência Técnica

6.10.1 Cada produto deverá ser entregue ao TJAM na sua versão e release mais recente e durante a vigência do contrato deverá ser atualizado sem custo adicional.

6.10.2 A contratada deve possuir contrato de representante do fornecedor da solução.

6.10.3 Para a solução envolvida na contratação, a Contratada deverá prever garantia dos produtos, durante a vigência do contrato, a partir da data de sua ativação, fornecendo sem custo adicional todos os ajustes às falhas que porventura forem encontradas. Garantia integral durante 12 (doze) meses, “on-site” com atendimento vinte e quatro horas por dia e sete dias por semana, a contar da data de homologação do produto, contra qualquer defeito ou problema em toda a solução.
6.10.4. A Contratada, durante o período de garantia, se obriga ao fornecimento dos componentes de software, para manutenções, update de produtos, suporte técnico ou ampliações, de forma que possam ser mantidas todas as funcionalidades inicialmente contratadas. Caso haja neste período a descontinuidade de fabricação dos componentes, deve ser também garantida à total compatibilidade dos itens substitutos com os originalmente fornecidos.

6.11. Solicitação de Serviços

6.11.1 A CONTRATADA deverá disponibilizar canais de comunicação, tais como número de telefone, endereço de correio eletrônico ou plataforma de abertura de chamados para atendimento de suporte técnico e consultoria.

6.11.2 A CONTRATADA deverá indicar um funcionário para que seja ponto de contato (preposto) entre o TJAM e a CONTRATADA.

6.11.3 Despesas relativas ao preposto serão de exclusiva responsabilidade da CONTRATADA.

6.12 Instrumento de Medição de Resultado (IMR) ou de Acordo de Nível de Serviço (ANS)

6.12.1 Os serviços deverão ser prestados tendo sua qualidade medida por meio de Acordo de Nível de Serviço – ANS

6.12.2 Havendo qualquer interrupção no funcionamento da solução o TJAM efetuará abertura de chamado reportando todos os sintomas.

6.12.3 Os níveis de serviço serão classificados conforme as severidades Emergencial, Grave e Normal.

6.12.4 Todos os prazos especificados na tabela "Acordo de Nível de Serviço / Penalidades" são contados a partir da abertura do respectivo número de identificação do chamado.

6.12.5 A abertura do chamado com fornecimento do seu número de identificação (protocolo de atendimento) deve ocorrer no prazo máximo de 15 minutos a partir da tentativa de contato pela Contratante com o número fornecido pela Contratada.

6.12.6 O atendimento aos chamados pode ocorrer remotamente ou de forma presencial. Atendimentos remotos não resolvidos que ultrapassem 24 horas devem ser continuados de forma presencial.

6.12.7 Após a conclusão do suporte, a Contratada comunicará ao TJAM e solicitará autorização para o fechamento do chamado. Caso o TJAM não confirme a solução definitiva do problema, o chamado permanecerá aberto até que seja efetivamente solucionado pela Contratada. Neste caso, o TJAM informará as pendências relativas ao chamado aberto.

6.12.8 Sempre que houver quebra dos ANS, o TJAM emitirá notificação à Contratada, que terá o prazo de, no máximo, 5 (cinco) dias úteis, contados a partir do recebimento da notificação, para apresentar as justificativas para as falhas verificadas.

6.12.9 Caso não haja manifestação dentro desse prazo ou caso o TJAM entenda serem improcedentes as justificativas apresentadas, será iniciado processo de aplicação das penalidades previstas, conforme o nível de atendimento transgredido.

6.12.10 Caso não sejam observados os prazos para atendimento previstos, incidirão glosas, calculadas sobre o valor do contrato, e penalidades conforme o disposto na tabela a seguir:

Acordo de Nível de Serviço / Penalidades			
Severidade	Prazos	Descrição Severidade	Penalidades
1 - Emergencial	6 Horas	Até 2 horas corridas de atraso.	1 – Advertência; 2 – Havendo recorrência, multa de 0,8%(zero vírgula oito por cento) por hora de atraso, calculada sobre o
		Superior a 2 horas e inferior ou igual a 8 horas corridas de atraso, além do prazo definido nos Níveis Mínimos de Serviços	3 – Multa de 1,0% (um por cento) por hora de atraso, calculada sobre mensal do item, sem prejuízo ao item
		Superior a 8 horas corridas.	4 – Multa de 1,2% (um vírgula dois por cento) por hora de atraso, calculada sobre o valor mensal do Item, administrativas a critério da Contratante.
2 - Grave	12 Horas	Até 4 horas corridas de atraso.	5 – Advertência; 6 – Para as demais ocorrências, multa de 0,6% (zero vírgula seis por cento) por hora de atraso, calculada so
		Superior a 4 horas e inferior ou igual a 24 horas corridas de atraso, além do prazo definido nos Níveis Mínimos de Serviços.	– Multa de 0,8% (zero vírgula oito por cento) por hora de atraso, calculada sobre o valor mensal do Item, s
		Superior a 24 horas corridas de atraso, além do prazo definido nos Níveis Mínimos de Serviços.	8 – Multa de 1.0% (um por cento) por hora de atraso, calculada sobre o valor mensal do Item, sem prejuízo critério da Contratante.
3 - Normal	24 Horas	Até 48 horas corridas de atraso.	9 – Advertência; 10 – Para as demais ocorrências, multa de 0,5% (zero vírgula cinco por cento) por hora de atraso, calculada 11. – Se o somatório das multas aplicadas com relação às obrigações relativas a um mesmo equipamento ul rescisão do Contrato, independentemente de aplicação das sanções administrativos cabíveis.

6.13 Dos prazos para recebimento provisório e definitivo

6.13.1 O recebimento será feito em duas etapas:

6.13.1.1 Recebimento provisório: No prazo máximo de 30 dias úteis após a entrega e configuração inicial dos produtos para posterior averiguação.

6.13.1.2 Recebimento definitivo: No prazo máximo de 30 dias úteis a contar da data de emissão do termo de recebimento provisóio.

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

7. DA NECESSIDADE DE FORMALIZAÇÃO DE CONTRATO

7.1. Deverá ser formalizado contrato para os serviços previstos neste Estudo Técnico Preliminar (ETP), tendo em vista as características do objeto a ser contratado, com a existência de obrigações futuras, incluindo a garantia, continuidade e confiabilidade do mesmo.

8. ESTIMATIVAS DAS QUANTIDADES PARA A CONTRATAÇÃO

8.1. Tendo por objetivo promover a proteção das credenciais administrativas utilizadas no âmbito dos sistemas computacionais do TJAM, além de criar mecanismos que impeçam a utilização dessas credenciais com o objetivo de potenciais ataques cibernéticos, prevenindo danos e principalmente evitando solução de continuidade na prestação jurisdicional, estima-se adquirir:

ITEM	ESPECIFICAÇÕES	QUANTIDADE MÍNIMA POR CONTRATAÇÃO	QUANTIDADE TOTAL
1	Solução de Segurança para Identidades e seus Privilégios – Monitoramento de comportamento e mitigação de riscos de usuários administradores da TI, com garantia pelo período de 12 (doze) meses.	50	75
2	Solução de Segurança para Identidades e seus Privilégios – Proteção para Aplicações Tradicionais, com garantia pelo período de 12 (doze) meses.	20	40
3	Solução de Segurança para Identidades e seus Privilégios – Proteção Local para ervidores Windows e Linux, com garantia pelo período de 12 (doze) meses.	200	400
4	Solução de Segurança para Identidades e seus Privilégios – Proteção Local para Estações de Trabalho, com garantia pelo período de 12 (doze) meses.	2500	3500
5	Serviço de instalação e configuração para Solução de Segurança para Identidades e seus Privilégios.	1	1
6	Transferência de Conhecimento para Solução de Segurança para Identidades e seus Privilégios (turma)	1	2
7	Serviço de Suporte Técnico Especializado	12	12

9. ESTIMATIVAS DAS QUANTIDADES PARA A CONTRATAÇÃO

9.1 Os valores estimados para esta contratação seguem na planilha abaixo.

Item	Descrição	Unid	Qnt Total	Preço (R$) Unit	Total
1	Solução de Segurança para Identidades e seus Privilégios – Monitoramento de comportamento e mitigação de riscos de usuários administradores da TI, com garantia pelo período de 12 (doze) meses..	Unidades	75	R$ 4.800,00	R$ 360.000,00
2	Solução de Segurança para Identidades e seus Privilégios – Proteção para Aplicações Tradicionais, com garantia pelo período de 12 (doze) meses.	Unidades	40	R$ 4.050,00	R$ 162.000,00
3	Solução de Segurança para Identidades e seus Privilégios – Proteção Local para ervidores Windows e Linux, com garantia pelo período de 12 (doze) meses.	Unidades	400	R$ 632,00	R$ 252.800,00
4	Solução de Segurança para Identidades e seus Privilégios – Proteção Local para Estações de Trabalho, com garantia pelo período de 12 (doze) meses.	Unidades	3500	R$ 236,00	R$ 826.000,00
5	Serviço de instalação e configuração para Solução de Segurança para Identidades e seus Privilégios.	Unidades	1	R$ 355.000,00	R$ 355.000,00
6	Transferência de Conhecimento para Solução de Segurança para Identidades e seus Privilégios (turma)	Unidades	2	R$ 31.000,00	R$ 62.000,00
7	Serviço de Suporte Técnico Especializado	Unidades	12	R$ 23.500,00	R$ 282.000,00
	Valor Estimado Total				R$ 2.299.800,00

10. JUSTIFICATIVA PARA PARCELAMENTO OU NÃO DA CONTRATAÇÃO

10.1 O objeto da contratação possui características comuns e usuais, fornecido por várias empresas, porém deverá ser realizada por único fornecedor. O parcelamento do objeto, neste caso, é inviável já que não se justifica técnica e economicamente, além do que a solução de TI contratada é composta de serviços integrados e correlatos que visam manter em funcionamento toda infraestrutura de solução.

11. CONTRATAÇÕES CORRELATAS/INTERDEPENDENTES

11.1 Não há contratações correlatas.

12. RESULTADOS PRETENDIDOS

12.1 Economicidade, eficácia, eficiência: com esta pretensa contratação, busca-se preservar os investimentos realizados no ambiente do TJAM, mantendo-se a eficácia, integração e a qualidade da plataforma de segurança em um ambiente de TI complexo como o do TJAM, bem como reduzir possíveis impactos gerados pela indisponibilidade dos serviços e sistemas de TIC e também evitar a reimplementação das barreiras de seguranças já em operação do TJAM;

12.2. Melhor aproveitamento dos recursos humanos, materiais e financeiros disponíveis: com a efetivação da contratação, o CONTRATANTE poderá direcionar seus esforços na capacitação da equipe técnica da SETIC para matérias mais relevantes, estratégicas e alinhadas com o negócio do TJAM, já que durante o período de vigência dos equipamentos o corpo técnico da SETIC adquiriu amplo conhecimento e experiência na solução de segurança atual;

12.3. Impactos ambientais positivos: não se aplica;

12.4. Melhoria da qualidade de produtos ou serviços oferecidos à sociedade: com a efetivação da contratação, a tendência esperada é a de menos ataques cibernéticos, reduzindo-se assim as indisponibilidades nos serviços oferecidos à sociedade.

13. PROVIDÊNCIAS PARA ADEQUAÇÃO DO AMBIENTE DO ÓRGÃO

13.1 Não haverá necessidade de adequação de ambiente.

14. IMPACTOS AMBIENTAIS

14.1 Pelo fato da solução a ser adquirida ser totalmente baseada em software, não haverá impactos ambientais relevantes a serem considerados em sua implantação.

15. SERVIÇOS DE MANUTENÇÃO E ASSISTÊNCIA TÉCNICA

15.1 Esta pretensa contratação, por tratar-se de um softtware, não prevê manutenção física e/ou assistênica técnica, somente garantia, conforme item 6.10, assim como também a contratação do serviço de suporte técnico especializado, destacada pelo item 7 do tópico 6.1.

16. DECLARAÇÃO DE VIABILIDADE (OU NÃO) DA CONTRATAÇÃO

16.1 Considerando todo o exposto acima, esta Secretaria de Tecnologia da Informação e Comunicação declara que a aquisição da Solução de Segurança para Gestão de Credenciais e Acessos da Cyberark é fundamental e viável, dada a necessidade de tornar o Judiciário do Estado do Amazonas mais seguro e inclusivo no ambiente digital, aumentar a resiliência às inevitáveis ameaças cibernéticas, estabelecer governança de segurança cibernética e fortalecer a gestão integrada de ações de segurança cibernética. Cumprindo lembrar que o TJAM ainda não possui qualquer solução de gerenciamento de acessos privilegiados.

17. OBRIGAÇÕES PERTINENTES À LEI GERAL DE PROTEÇÃO DE DADOS

17.1 A contratada deverá garantir as melhores práticas relacionadas à Segurança da Informação e à Lei Geral de Proteção de Dados Pessoais (LGPD), principalmente, no que diz respeito aos dados pessoais tratados durante a configuração dos privilégios.

17.2 A contratada durante a execução do objeto, deve implementar medidas técnicas e administrativas adequadas para proteger os dados pessoais contra acessos não autorizados.

17.3 Será exigido da Contratada que cada profissional que venha a prestar serviços assine um termo de compromisso, pelo qual se comprometerá a manter o sigilo das informações.

17.4 A Contratada deverá manter sigilo absoluto a respeito de quaisquer dados, informações e artefatos, contidos em documentos e mídias de que venha a ter conhecimento durante a execução dos trabalhos, não podendo, sob qualquer pretexto, divulgar, reproduzir ou utilizar, sob pena de aplicação das sanções cabíveis, além do pagamento de indenização por perdas e danos, independentemente da classificação de sigilo conferido pelo TJAM a tais documentos.

Manaus, data registrada no sistema.

Washington Alves da Cunha Neto	**Diogo Mendonça de Sousa**	**Breno Figueiredo Corado**
Assessor de Segurança da Informação e Proteção de Dados	Diretor da Divisão de Infraestrutura de Tecnologia da Informação e Comunicação	Secretário de Tecnologia da Informação e Comunicação
Assinado Digitalmente	Assinado Digitalmente	Assinado Digitalmente

Documento assinado eletronicamente por **WASHINGTON NETO**, **Coordenador(a)**, em 04/04/2024, às 18:28, conforme art. 1º, III, "b", da Lei 11.419/2006.

Documento assinado eletronicamente por **DIOGO MENDONCA DE SOUSA**, **Diretor(a)**, em 04/04/2024, às 18:30, conforme art. 1º, III, "b", da Lei 11.419/2006.

Documento assinado eletronicamente por **BRENO FIGUEIREDO CORADO**, **Secretário(a)**, em 05/04/2024, às 05:43, conforme art. 1º, III, "b", da Lei 11.419/2006.

A autenticidade do documento pode ser conferida no site https://sei.tjam.jus.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0 informando o código verificador **1502255** e o código CRC **CB53A34F**.

TRIBUNAL DE JUSTIÇA DO ESTADO DO AMAZONAS
Av. André Araújo, S/N - Bairro Aleixo - CEP 69060-000 - Manaus - AM - www.tjam.jus.br

MAPA DE PREÇOS

ITEM	SERVIÇO	UNIDADE	QUANT.	VALOR UNITÁRIO ESTIMADO		MÉDIA BRUTA	DESVIO PADRÃO	LIMITE INFERIOR	LIMITE SUPERIOR	MÉDIA AJUSTADA	VALOR TOTAL ESTIMADO
				EMPRESA	PREÇO						
1	Solução de Segurança para Identidades e seus Privilégios – Monitoramento de comportamento e mitigação de riscos de usuários administradores da TI, com garantia pelo período de 12 (doze) meses.	UN	75	FORNECEDOR 1	R$ 13.291,39	R$ 14.895,85	R$ 1.154,51	R$ 13.741,34	R$ 16.050,36	R$ 14.895,85	R$ 1.117.188,75
				FORNECEDOR 2	R$ 15.949,66						
				FORNECEDOR 3	R$ 15.456,00						
				FORNECEDOR 4	R$ 14.886,35						
2	Solução de Segurança para Identidades e seus Privilégios – Proteção para Aplicações Tradicionais, com garantia pelo período de 12 (doze) meses.	UN	40	FORNECEDOR 1	R$ 9.390,65	R$ 10.359,91	R$ 694,53	R$ 9.665,38	R$ 11.054,44	R$ 10.359,91	R$ 414.396,40
				FORNECEDOR 2	R$ 10.799,25						
				FORNECEDOR 3	R$ 10.920,00						
				FORNECEDOR 4	R$ 10.329,72						
3	Solução de Segurança para Identidades e seus Privilégios – Proteção Local para servidores Windows e Linux, com garantia pelo período de 12 (doze) meses.	UN	400	FORNECEDOR 1	R$ 3.033,90	R$ 3.369,80	R$ 270,75	R$ 3.099,05	R$ 3.640,55	R$ 3.369,80	R$ 1.347.920,00
				FORNECEDOR 2	R$ 3.640,68						
				FORNECEDOR 3	R$ 3.528,00						
				FORNECEDOR 4	R$ 3.276,62						
4	Solução de Segurança para Identidades e seus Privilégios – Proteção Local para Estações de Trabalho, com garantia pelo período de 12 (doze) meses.	UN	3500	FORNECEDOR 1	R$ 505,65	R$ 554,05	R$ 38,37	R$ 515,68	R$ 592,42	R$ 554,05	R$ 1.939.175,00
				FORNECEDOR 2	R$ 581,50						
				FORNECEDOR 3	R$ 588,00						
				FORNECEDOR 4	R$ 541,05						
5	Serviço de instalação e configuração para Solução de Segurança para Identidades e seus Privilégios.	UN	1	FORNECEDOR 1	R$ 196.910,00	R$ 187.902,65	R$ 40.010,58	R$ 147.892,07	R$ 227.913,23	R$ 187.902,65	R$ 187.902,65
				FORNECEDOR 2	R$ 218.570,10						
				FORNECEDOR 3	R$ 129.375,00						
				FORNECEDOR 4	R$ 206.755,50						
6	Transferência de Conhecimento para Solução de Segurança para Identidades e seus Privilégios (turma)	UN	2	FORNECEDOR 1	R$ 45.000,00	R$ 85.437,50	R$ 76.393,56	R$ 9.043,94	R$ 161.831,06	R$ 47.250,00	R$ 94.500,00
				FORNECEDOR 2	R$ 49.050,00						
				FORNECEDOR 3	R$ 200.000,00						
				FORNECEDOR 4	R$ 47.700,00						
7	Serviço de Suporte	MÊS	12	FORNECEDOR 1	R$ 22.000,00	R$ 27.490,00	R$ 8.399,75	R$ 19.090,25	R$ 35.889,75	R$ 23.320,00	R$ 279.840,00
				FORNECEDOR	R$						

	Técnico Especializado			2	24.420,00						
				FORNECEDOR 3	R$ 40.000,00						
				FORNECEDOR 4	R$ 23.540,00						
TOTAL GLOBAL ESTIMADO											R$ 5.380.922,80

OBS.: OS VALORES ESTIMADOS FORAM PROVENIENTES DE PESQUISA DE MERCADO.
FORNECEDOR 1: ALLTECH SOLUÇÕES EM TECNOLOGIA LTDA CNPJ 21547011/0001-66
FORNECEDOR 2: DFENSE SECURITY TÉCNOLOGIA DA INFORMAÇÃO LTDA CNPJ 29.559.799/0001-32
FORNECEDOR 3: SHIELD SECURITY TECNOLOGIA LTDA CNPJ 31.746.312/0001-72
FORNECEDOR 4: 3STRUCTURE IT LTDA CNPJ 35.194.946/0001-10

Manaus, 23 de julho de 2024
Cotado por
ILDEMAR DA SILVA RODRIGUES
Assistente Judiciário

THIAGO LIMA DOS SANTOS
Diretor da Divisão de Compras e Operações

Documento assinado eletronicamente por **Ildemar Da Silva Rodrigues**, **Servidor**, em 23/07/2024, às 10:28, conforme art. 1º, III, "b", da Lei 11.419/2006.

Documento assinado eletronicamente por **THIAGO LIMA DOS SANTOS**, **Diretor(a)**, em 23/07/2024, às 10:35, conforme art. 1º, III, "b", da Lei 11.419/2006.

A autenticidade do documento pode ser conferida no site https://sei.tjam.jus.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0 informando o código verificador **1696117** e o código CRC **56B3CD29**.

TRIBUNAL DE JUSTIÇA DO ESTADO DO AMAZONAS
Av. André Araújo, S/N - Bairro Aleixo - CEP 69060-000 - Manaus - AM - www.tjam.jus.br

CONTRATO - SECOP/DVCC/ATJ

*** MODELO DE DOCUMENTO**

PODER JUDICIÁRIO
TRIBUNAL DE JUSTIÇA DO ESTADO DO AMAZONAS
DIVISÃO DE CONTRATOS E CONVÊNIOS

CONTRATO ADMINISTRATIVO Nº ___/20__-FUNJEAM

CONTRATO ADMINISTRATIVO Nº ___/20__-FUNJEAM, que entre si celebram o **TRIBUNAL, DE JUSTIÇA DO ESTADO DO AMAZONAS,** por intermédio do **FUNDO DE MODERNIZAÇÃO E REAPARELHAMENTO DO PODER JUDICIÁRIO ESTADUAL-FUNJEAM,** e a empresa _____, na forma abaixo.

O **TRIBUNAL DE JUSTIÇA DO ESTADO DO AMAZONAS**, por intermédio do **FUNDO DE MODERNIZAÇÃO E REAPARELHAMENTO DO PODER JUDICIÁRIO ESTADUAL-FUNJEAM**, sediado na Cidade de Manaus, Estado do Amazonas, à Avenida André Araújo, s/nº, Aleixo, inscrito no CNPJ/MF sob nº 04.301.769/0001-09, neste ato representado por sua Presidente, Desembargadora **NÉLIA CAMINHA JORGE**, neste instrumento simplesmente denominado **CONTRATANTE**, e do outro lado, a empresa XXXXXXXXXXXXXX, pessoa jurídica de direito privado, com seus atos constitutivos devidamente registrados na Junta Comercial do Estado XXXXXXX, em XX/XX/XXXX, sob o nº XXX, inscrita no CNPJ/MF sob nº XXXXXXX, estabelecida na Cidade de XXXXXXX, Estado XXXXXXX, à XXXXXXX, neste ato representada pelo(a) Sr(a). XXXXXXX, daqui por diante simplesmente denominada **CONTRATADA**, em consequência da licitação na modalidade XXXXXXXX, sob o nº XXX/2024-COLIC/TJAM, cuja homologação foi publicada no Diário da Justiça Eletrônico, Ano XXX, Edição nº XXX, Caderno Administrativo, em XX/XX/XXXX, à pág. XX, tendo em vista o que consta do Processo Administrativo Digital nº 2024/000011472-00, doravante referido apenas por **PROCESSO**, celebram, na presença das testemunhas adiante nominadas, o presente **CONTRATO ADMINISTRATIVO Nº XXXX/2024- FUNJEAM**, que se regerá pelas normas instituídas pela Lei 14.133/21 e suas alterações, bem como pela Resolução nº 64/2023 TJAM, ou a norma que a substituir, que a regulamenta, pelas cláusulas e condições seguintes:

CLÁUSULA PRIMEIRA – OBJETO

1.1. O objeto do presente instrumento é a contratação de fornecimento de **solução de gerenciamento de acessos privilegiados** (PAM – Privileged Access Management), sob demanda, nas condições estabelecidas no Termo de Referência e seus anexos.

1.2. Objeto da contratação:

ITEM	OBJETO	UND.	QUANT.	VALOR UNITÁRIO	VALOR TOTAL
1	Solução de Segurança para Identidades e seus Privilégios – Monitoramento de comportamento e mitigação de riscos de usuários administradores da TI, com garantia pelo período de 12 (doze) meses..	und	75		
2	Solução de Segurança para Identidades e seus Privilégios – Proteção para Aplicações Tradicionais, com garantia pelo período de 12 (doze) meses.	und	40		
3	Solução de Segurança para Identidades e seus Privilégios – Proteção Local para ervidores Windows e Linux, com garantia pelo período de 12 (doze) meses.	und	400		
4	Solução de Segurança para Identidades e seus Privilégios – Proteção Local para Estações de Trabalho, com garantia pelo período de 12 (doze) meses.	und	3500		
5	Serviço de instalação e configuração para Solução de	und	1		

	Segurança para Identidades e seus Privilégios.				
6	Transferência de Conhecimento para Solução de Segurança para Identidades e seus Privilégios (turma)	und	2		
7	Serviço de Suporte Técnico Especializado	mês	12		

1.3. Vinculam esta contratação, independentemente de transcrição, o Termo de Referência, o Edital da Licitação, a Proposta da **CONTRATADA** e os eventuais anexos destes documentos.

1.4. Estão inclusos no objeto desta contratação todo o aparato necessário à execução do objeto contratual, como o fornecimento de materiais, mão de obra, acessórios e insumos inerentes à sua execução, observando-se tipo, especificações, quantidades e condições descritas no Termo de Referência.

1.5. O regime de execução é o de empreitada por preço unitário.

CLÁUSULA SEGUNDA – LEGISLAÇÃO APLICÁVEL

2.1. O presente Contrato rege-se por toda a legislação aplicável à espécie e ainda pelas disposições que a complementarem, alterarem ou regulamentarem, cujas normas, desde já, entendem-se como integrantes do presente Termo, especialmente às normas constantes da Lei 14.133/21, a Resolução nº 64/2023 deste Tribunal de Justiça, ou outra que vier a substituí-la, e demais normas legais pertinentes.

2.2. A **CONTRATADA** declara conhecer todas essas normas e concorda em se sujeitar às estipulações, sistemas de penalidades e demais regras delas constantes, mesmo que não expressamente transcritas no presente instrumento.

CLÁUSULA TERCEIRA – VIGÊNCIA E PRORROGAÇÃO

3.1. O prazo de vigência da contratação é de 12 (doze) meses, contados da assinatura do contrato, prorrogável por até 10 anos, na forma do art. 106 e 107 da Lei 14.133/21.

3.1. Os itens 5 e 6 da tabela indicada na cláusula 1.2 são por escopo, razão pela qual não possuem fornecimento contínuo.

3.2. A prorrogação de que trata este item é condicionada ao ateste, pela autoridade competente, de que as condições e os preços permanecem vantajosos para a Administração, permitida a negociação com o contratado.

3.3. É vedada a manutenção, aditamento ou prorrogação de contrato de prestação de serviços com empresa que venha a contratar empregados que sejam cônjuges, companheiros ou parentes em linha reta, colateral ou por afinidade, até o terceiro grau, inclusive, de ocupantes de cargos de direção e de assessoramento, de membros ou juízes vinculados ao **CONTRATANTE**, nos termos do art. 3.º da Resolução CNJ n.º 07/2005

CLÁUSULA QUARTA – PREÇO

4.1. O valor mensal da contratação é de R$ XXXX,XX (XXXXXXX), perfazendo o valor total de R$ XXXXX,XX (XXXXX) no que refere **ao item 7**. Por sua vez, o valor da contratação dos **itens 1 a 6** é de RS XXXXX (XXXXXX), perfazendo, assim, o valor total da contratação de R$ XXXXX (XXXXX).

4.2. No valor acima estão incluídas todas as despesas ordinárias diretas e indiretas decorrentes da execução do objeto, inclusive tributos e/ou impostos, encargos sociais, trabalhistas, previdenciários, fiscais e comerciais incidentes, taxa de administração, frete, seguro e outros necessários ao cumprimento integral do objeto da contratação.

4.3. No interesse da **CONTRATANTE** o valor deste Contrato poderá ser aumentado ou suprimido até o limite de 25% (vinte e cinco por cento), conforme disposto no artigo 125 da Lei nº 14.133/2021.

4.4. A **CONTRATADA** fica obrigada a aceitar, nas mesmas condições, os acréscimos e supressões que se fizerem necessários, até o limite ora previsto, não podendo os mesmos excederem o limite estabelecido no parágrafo anterior.

4.5. O valor acima é meramente estimativo, de forma que os pagamentos devidos ao contratado dependerão dos quantitativos efetivamente fornecidos.

CLÁUSULA QUINTA – MODELO DE EXECUÇÃO, MODELO DE GESTÃO CONTRATUAL E REEQUILÍBRIO ECONÔMICO-FINANCEIRO

5.1. O regime de execução contratual, os modelos de gestão e de execução, assim como os prazos e condições de conclusão, entrega, observação e recebimento do objeto constam no Termo de Referência, anexo a este Contrato.

5.2. O objeto contratual deverá ser executado no prazo máximo de vigência desta contratação.

5.3. Fica estabelecida a comunicação, preferencialmente, formal, eletrônica e escrita entre as partes, devendo a **CONTRATANTE**, sempre que comunicar/notificar a parte **CONTRATADA**, indicar prazo para acusação de recebimento do documento.

5.4 Transcorrido o prazo indicado no parágrafo anterior, presumir-se-á comunicada/notificada a **CONTRATADA** para todos os efeitos jurídicos.

5.5. A recomposição do equilíbrio econômico financeiro do contrato, além de obedecer aos requisitos previstos na Lei Federal nº 14.133/2021, será proporcional ao desequilíbrio efetivamente suportado, cuja existência e extensão deverão ser comprovados pela **CONTRATADA** ou pelo **CONTRATANTE**, conforme o caso, e darão ensejo à alteração do valor do contrato para mais ou para menos, respectivamente.

5.6. O pleito da recomposição do equilíbrio econômico-financeiro não será acolhido quando a parte interessada falhar em comprovar os requisitos previstos no item anterior, em especial nas seguintes hipóteses:
5.6.1. A efetiva elevação dos encargos não resultar em onerosidade excessiva ou não restar comprovada e quantificada por memória de cálculo a ser apresentada pela parte interessada;
5.6.2. O evento que houver dado causa ao desequilíbrio houver ocorrido em data anterior à entrega de proposta ou posterior à expiração da vigência do contrato;
5.6.3. Não for comprovado o nexo de causalidade entre o evento e a majoração dos encargos suportados pela parte interessada;
5.6.4. A parte interessada houver, direta ou indiretamente, contribuído para a majoração de seus próprios encargos, seja pela previsibilidade do evento, seja pela possibilidade de evitar a sua ocorrência;
5.6.5. A elevação dos encargos decorrer exclusivamente de variação inflacionária, hipótese já contemplada nos critérios de reajuste previstos neste instrumento.

5.7. Havendo a revisão contratual em razão da recomposição do equilíbrio econômico-financeiro, a formalização será realizada por meio de Termo Aditivo.

CLÁUSULA SEXTA – REAJUSTAMENTO

6.1. Os preços inicialmente contratados são fixos e irreajustáveis no prazo de um ano contado da data do orçamento estimado, conforme art. 92, §3º, da Lei 14.133/2021.

6.2. Após o interregno de um ano, independente do pedido da **CONTRATADA**, os preços iniciais serão **reajustados**, mediante a aplicação, pelo contratante, do Índice de Custos de Tecnologia da Informação - ICTI, exclusivamente para as obrigações iniciadas e concluídas após a ocorrência da anualidade.

6.3. Nos reajustes subsequentes ao primeiro, o interregno mínimo de um ano será contado a partir dos efeitos financeiros do último reajuste.

6.4. No caso de atraso ou não divulgação do(s) índice (s) de reajustamento, o contratante pagará ao contratado a importância calculada pela última variação conhecida, liquidando a diferença correspondente tão logo seja(m) divulgado(s) o(s) índice(s) definitivo(s).

6.5. Caso o(s) índice(s) estabelecido(s) para reajustamento venha(m) a ser extinto(s) ou de qualquer forma não possa(m) mais ser utilizado(s), será(ão) adotado(s), em substituição, o(s) que vier(em) a ser determinado(s) pela legislação então em vigor.

6.6. Na ausência de previsão legal quanto ao índice substituto, as partes elegerão novo índice oficial, para reajustamento do preço do valor remanescente, por meio de termo aditivo.

6.7. O reajuste será realizado por apostilamento.

CLÁUSULA SÉTIMA – RECEBIMENTO

7.1. Os **serviços** serão **recebidos provisoriamente**, no prazo de 30 (trinta) dias úteis, pelo(a) responsável pelo acompanhamento e fiscalização do contrato, mediante termos detalhados, quando verificado o cumprimento das exigências de caráter técnico, conforme Termo de Referência.

7.1.1. O prazo da disposição acima será contado do recebimento de comunicação de cobrança oriunda da **CONTRATADA** com a comprovação da prestação dos serviços a que se refere a parcela a ser paga.

7.2. A **CONTRATADA** fica obrigado a reparar, corrigir, remover, reconstruir ou substituir, às suas expensas, no todo ou em parte, o objeto em que se verificarem vícios, defeitos ou incorreções resultantes da execução ou materiais empregados, cabendo à fiscalização não atestar a última e/ou única medição de serviços até que sejam sanadas todas as eventuais pendências que possam vir a ser apontadas no Recebimento Provisório.

7.2.1. A fiscalização não efetuará o ateste da última e/ou única medição de serviços até que sejam sanadas todas as eventuais pendências que possam vir a ser apontadas no Recebimento Provisório.

7.2.2. Os serviços poderão ser rejeitados, no todo ou em parte, quando em desacordo com as especificações constantes neste Termo de Referência e na proposta, sem prejuízo da aplicação das penalidades.

7.3. Os serviços serão **recebidos definitivamente** no prazo de 30 (trinta) dias úteis, contados do recebimento provisório, por servidor ou comissão designada pela autoridade competente, após a verificação da qualidade e quantidade do serviço e consequente aceitação mediante termo detalhado.

7.4. No caso de controvérsia sobre a execução do objeto, quanto à dimensão, qualidade e quantidade, deverá ser observado o teor do art. 143 da Lei nº 14.133, de 2021, comunicando-se à empresa para emissão de Nota Fiscal no que pertine à parcela incontroversa da execução do objeto, para efeito de liquidação e pagamento.

7.5. Nenhum prazo de recebimento ocorrerá enquanto pendente a solução, pela **CONTRATADA**, de inconsistências verificadas na execução do objeto ou no instrumento de cobrança.

7.6. O recebimento provisório ou definitivo não excluirá a responsabilidade civil pela solidez e pela segurança do serviço nem a responsabilidade ético-profissional pela perfeita execução do contrato.

CLÁUSULA OITAVA - PAGAMENTO

8.1. O pagamento será efetuado **em parcela única** à **CONTRATADA**, em até 30 (trinta) dias, mediante apresentação da Nota Fiscal/Fatura, dos serviços efetivamente prestados, após ser devidamente atestada a sua conformidade pelo Fiscal designado para acompanhar e fiscalizar a execução contratual.

8.1.1. O pagamento do item 7 será realizado mensalmente.

8.2. O pagamento será efetuado por meio de **Ordem Bancária Eletrônica** em conta corrente indicada na Nota Fiscal/Fatura, devendo, para isso, ficar explícito o nome do banco, agência, localidade e número da conta corrente em que deverá ser efetivado o crédito.

8.3. Caso a **CONTRATADA** seja optante pelo Sistema Integrado de Pagamento de Impostos e Contribuições das Microempresas e Empresas de Pequeno Porte – SIMPLES, a mesma deverá apresentar, juntamente com a Nota Fiscal/Fatura, a devida comprovação, a fim de evitar a retenção na fonte dos tributos e contribuições, conforme legislação em vigor.

8.4. Para a efetivação do pagamento deverão ser mantidas as mesmas condições iniciais de habilitação, cumpridos os seguintes requisitos: Comprovação da **regularidade fiscal** da **CONTRATADA** para com a **Fazenda Federal**, **Estadual** e **Municipal**; Comprovação da **regularidade fiscal** da **CONTRATADA** relativa à **Seguridade Social** e ao **Fundo de Garantia por Tempo de Serviço (FGTS)**, demonstrando situação regular no cumprimento dos encargos sociais instituídos por lei; Comprovação de **inexistência de débitos inadimplidos perante a Justiça do Trabalho**, mediante a apresentação de **Certidão Negativa de Débitos Trabalhistas (CNDT)**; e Inexistência de fato impeditivo para o qual tenha concorrido a **CONTRATADA**.

8.5. A **CONTRATADA** deverá encaminhar ao **CONTRATANTE**, através do e-mail contratos@tjam.jus.br: a Nota Fiscal/Fatura acompanhada dos documentos previstos nesta Cláusula, bem como das certidões que comprovem a regularidade fiscal da **CONTRATADA,** requerimento de solicitação de pagamento, recibo, a fim de que sejam adotadas as medidas inerentes ao pagamento.

8.6. A Nota Fiscal/Fatura correspondente será examinada diretamente pelo Fiscal designado pela **CONTRATANTE**, o qual somente atestará a prestação do serviço contratado e liberará a referida Nota Fiscal/Fatura para pagamento quando cumpridas, pela **CONTRATADA**, todas as condições pactuadas.

8.6.1 Em nenhuma hipótese será efetuado pagamento de Nota Fiscal/Fatura com o número do CNPJ/MF diferente do que foi apresentado na proposta de preços, mesmo que sejam empresas consideradas matriz e filial ou vice versa, ou pertencentes ao mesmo grupo ou conglomerado.

8.7. Havendo erro na Nota Fiscal/Fatura ou circunstância que impeça a liquidação da despesa, aquela será devolvida pelo Fiscal à **CONTRATADA** e o pagamento ficará pendente até que a mesma providencie as medidas saneadoras. Nesta hipótese, o prazo para pagamento será interrompido e reiniciado a partir da regularização da situação ou reapresentação do documento fiscal, não acarretando qualquer ônus para o **CONTRATANTE**.

8.8. A não disponibilização das informações e/ou documentos exigidos nesta cláusula caracteriza descumprimento de cláusula contratual, sujeitando a **CONTRATADA** à aplicação de penalidade(s) prevista(s) neste contrato.

8.9. O **CONTRATANTE** pode deduzir do montante a pagar os valores correspondentes a multas ou indenizações devidas pela **CONTRATADA**, nos termos deste contrato.

8.10. Ocorrendo atraso no pagamento, e desde que para tal não tenha concorrido de alguma forma a **CONTRATADA**, **haverá incidência de atualização monetária sobre o valor devido, pela variação acumulada do Índice de Preço ao Consumidor Amplo (IPCA)**, publicado pelo Instituto Brasileiro de Geografia e Estatística – IBGE, ocorrida entre a data final prevista para o pagamento e a data de sua efetiva realização.

CLÁUSULA NONA - DOTAÇÃO ORÇAMENTÁRIA

9.1. As despesas com a prestação de serviços do presente Contrato serão custeadas, no exercício em curso, por conta do Programa de Trabalho _____, Elemento de Despesa _____, Fonte de Recurso _____, Unidade Orçamentária _____ (_____), **Nota de Empenho _____**, de __/__/_____, no valor de **R$ _____ (_____)**.

CLÁUSULA DÉCIMA - OBRIGAÇÕES DAS PARTES

10.1. São obrigações da **CONTRATANTE**:

a)Exigir o cumprimento de todas as obrigações assumidas pela **CONTRATADA**, de acordo com o contrato e seus anexos;

b)Receber o objeto no prazo e condições estabelecidas no Termo de Referência;

c)Notificar a **CONTRATADA**, por escrito, sobre vícios, defeitos ou incorreções verificadas na execução do objeto, para que seja por ele substituído, reparado ou corrigido, no total ou em parte, às suas expensas, fixando prazo para a sua correção, certificando-se de que as soluções por ele propostas sejam as mais adequadas;

d)Acompanhar e fiscalizar a execução do contrato e o cumprimento das obrigações pela **CONTRATADA**;

e)Efetuar o pagamento à **CONTRATADA** do valor correspondente à execução do objeto, no prazo, forma e condições estabelecidos no presente Contrato e seus anexos;

f)Aplicar à **CONTRATADA** as sanções previstas na lei e neste Contrato;

g)Explicitamente emitir decisão sobre todas as solicitações e reclamações relacionadas à execução do presente Contrato, ressalvados os requerimentos manifestamente impertinentes, meramente protelatórios ou de nenhum interesse para a boa execução do ajuste, no prazo de 30 dias, a contar da data do protocolo do requerimento para decidir, admitida a prorrogação motivada, por igual período;

h)Responder eventuais pedidos de reestabelecimento do equilíbrio econômico-financeiro feitos pelo contratado no prazo máximo de 30 dias, admitida a prorrogação motivada, por igual período;

i)Prestar esclarecimentos e fornecer por escrito as informações necessárias para a execução do objeto do contrato.

j)Não responder por quaisquer compromissos assumidos pela **CONTRATADA** com terceiros, ainda que vinculados à execução do contrato, bem como por qualquer dano causado a terceiros em decorrência de ato do **CONTRATADO**, de seus empregados, prepostos ou subordinados;

k)Rejeitar, no todo ou em parte, serviço ou fornecimento executado em desacordo com este contrato e com o Termo de Referência;

10.2. São obrigações da **CONTRATADA**:

a)A **CONTRATADA** deve cumprir todas as obrigações constantes deste Contrato e em seus anexos, assumindo como exclusivamente seus os riscos e as despesas decorrentes da boa e perfeita execução do objeto;

b)Atender às determinações regulares emitidas pelo fiscal ou gestor do contrato ou autoridade superior e prestar todo esclarecimento ou informação solicitadas;

c)Informar imediatamente à **CONTRATANTE** qualquer ocorrência anormal, acidentes, condições inadequadas, quaisquer atos ou fatos que possam ser causa de prejuízos ou transtornos à perfeita execução do objeto;

d)Comunicar, por escrito, eventual atraso ou interrupção da execução do objeto, apresentando razões justificadoras que serão objeto de apreciação pelo **CONTRATANTE**, sem prejuízo das eventuais sanções cabíveis;
e)Prestar todas as informações e esclarecimentos solicitadas pela **CONTRATANTE** no prazo por ela estabelecido, inclusive, facilitando a ação da Fiscalização na inspeção da execução dos serviços, quando for o caso, em qualquer dia ou hora;

f)Reparar, corrigir, remover, reconstruir ou substituir, às suas expensas, no total ou em parte, no prazo fixado pelo fiscal do contrato, os bens e/ou serviços nos quais se verificarem vícios, defeitos ou incorreções resultantes da execução ou dos materiais empregados;

g)Efetuar comunicação ao **CONTRATANTE**, assim que tiver ciência da impossibilidade de entrega do bem ou realização/finalização do serviço no prazo estabelecido, para adoção de ações de contingência cabíveis;

h)Responsabilizar-se pelos vícios e danos decorrentes da execução do objeto, de acordo com o Código de Defesa do Consumidor (Lei nº 8.078, de 1990), bem como por todo e qualquer dano causado à Administração ou terceiros, não reduzindo essa responsabilidade a fiscalização ou o acompanhamento da execução contratual pelo **CONTRATANTE**, que ficará autorizado a descontar dos pagamentos devidos ou da garantia, caso exigida no edital, o valor correspondente aos danos sofridos, consoante art. 120 da Lei 14.133/2021;

i)Responsabilizar-se pelo cumprimento de todas as obrigações trabalhistas, previdenciárias, fiscais, comerciais e as demais previstas em legislação específica, cuja inadimplência não transfere a responsabilidade ao contratante e não poderá onerar o objeto do contrato, consoante art. 121 da Lei 14.133/2021;
j)Responsabilizar-se, integral e exclusivamente, pelas obrigações com mão de obra, materiais, transporte, refeições, uniformes, ferramentas, equipamentos, encargos sociais, trabalhistas, previdenciários, fiscais, cíveis e criminais, resultantes da execução do Contrato, inclusive no tocante aos seus empregados, dirigentes e prepostos;
k)Apresentar, sempre que solicitado, as seguintes informações e/ou os documentos listados: **Nota Fiscal/Fatura**; Comprovação da **regularidade fiscal** da **CONTRATADA** para com a **Fazenda Federal**, **Estadual** e **Municipal**; Comprovação da **regularidade fiscal** da **CONTRATADA** relativa à **Seguridade Social** e ao **Fundo de Garantia por Tempo de Serviço (FGTS)**, demonstrando situação regular no cumprimento dos encargos sociais instituídos por lei; Comprovação de **inexistência de débitos inadimplidos perante a Justiça do Trabalho**, mediante a apresentação de **Certidão Negativa de Débitos Trabalhistas (CNDT)**; Comprovação de regularidade junto ao **Cadastro Nacional de Empresas Inidôneas e Suspensas (Ceis) e o Cadastro Nacional de Empresas Punidas (Cnep);**
l)Manter durante toda a vigência do contrato, em compatibilidade com as obrigações assumidas, todas as condições exigidas para habilitação na licitação;

m)Guardar sigilo sobre todas as informações obtidas em decorrência do cumprimento do contrato;
n)É expressamente vedada à **CONTRATADA** a veiculação de publicidade acerca da contratação, salvo se houver prévia autorização do **CONTRATANTE**;
o)Sempre que a natureza da execução do objeto exigir, esta Administração promoverá reunião inicial com participação obrigatória da **CONTRATADA** 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.
p)Cumprir e atender às normas relativas à Política de Prevenção e Enfrentamento do Assédio Moral, do Assédio Sexual e da Discriminação, a fim de promover o trabalho digno, saudável, seguro e sustentável no âmbito do Poder Judiciário instituidas pela Resolução nº 518 de 31/08/2023 do Conselho Nacional de Justiça (CNJ);
q)Manter preposto aceito pela Administração para representá-lo na execução do contrato;
r)A indicação ou a manutenção do preposto da empresa poderá ser recusada por este Tribunal de Justiça do Amazonas, desde que devidamente justificada, devendo a empresa designar outro para o exercício da atividade;
s)Informar contatos (e-mails, telefones e endereços de correspondência) do(s) preposto(s) técnico e administrativo, previamente aceito pela **CONTRATANTE** para representar a **CONTRATADA** sempre que for necessário;
t)Observar e cumprir todas as demais obrigações previstas no Termo de Referência não descritas nesta cláusula.

CLÁUSULA DÉCIMA PRIMEIRA - OBRIGAÇÕES PERTINENTES À LEI GERAL DE PROTEÇÃO DE DADOS

11.1. As cláusulas seguintes são aplicáveis ao tratamento de dados pessoais.

11.2. As partes deverão cumprir a Lei nº 13.709, de 14 de agosto de 2018 (Lei Geral de Proteção de Dados), quanto a todos os dados pessoais a que tenham acesso em razão deste Contrato Administrativo, a partir da apresentação da proposta no procedimento de contratação, independentemente de declaração ou de aceitação expressa.

11.3. A **CONTRATADA** terá acesso aos dados pessoais que estão de posse da **CONTRATANTE** apenas para as finalidades definidas pela **CONTRATANTE**.

11.4. A **CONTRATADA** deve tratar os dados pessoais que tiver acesso apenas de acordo com as instruções documentadas da **CONTRATANTE**, durante a vigência do contrato, e em conformidade com estas cláusulas, e que, na eventualidade, não conseguir seguir as instruções ou de não mais poder cumprir estas obrigações, por qualquer razão, deve oficiar de modo formal este fato imediatamente à **CONTRATANTE**, sob pena de rescisão do contrato que terá o direito de rescindir o contrato sem qualquer ônus, multa ou encargo.

11.5. É dever da **CONTRATADA** orientar e treinar seus empregados sobre os deveres, requisitos e responsabilidades decorrentes da Lei Geral de Proteção de Dados.

11.6. A **CONTRATADA** deverá exigir de suboperadores e subcontratados, se houver, o cumprimento dos deveres da presente cláusula, permanecendo integralmente responsável por garantir sua observância.

11.7. A **CONTRATADA** ao tomar conhecimento de que os dados pessoais que recebeu são imprecisos ou desatualizados, deve informar a **CONTRATANTE**, sem demora injustificada. Neste caso, o **CONTRATANTE** deve apoiar a **CONTRATADA** para apagar ou retificar os dados.

11.8. No caso de uma violação de dados pessoais relativos a dados pessoais tratados pela **CONTRATADA** sob este contrato, a **CONTRATADA** deve tomar as medidas apropriadas para lidar com a violação, incluindo medidas para mitigar seus efeitos adversos. A **CONTRATADA** também deve notificar a **CONTRATANTE** sem demora injustificada, e no prazo de 24 horas, logo após tomar conhecimento da violação. Esta notificação deve conter os detalhes de um ponto de contato, onde mais informações podem ser obtidas, uma descrição da natureza da violação (incluindo, sempre que possível, categorias e número aproximado de titulares de dados e registros de dados pessoais em questão), suas prováveis consequências e as medidas tomadas ou propostas para resolver a violação, incluindo, quando apropriado, medidas para mitigar seus possíveis efeitos adversos.

11.9. A **CONTRATADA** deve apoiar e auxiliar a **CONTRATANTE** para permitir que a mesma cumpra suas obrigações nos termos da Lei 13.709/2018 (Lei Geral de Proteção de Dados Pessoais – LGPD), em particular para notificar a Agência Nacional de Proteção de Dados – ANPD e os titulares de dados afetados, levando em consideração a natureza do tratamento e as informações disponíveis para a **CONTRATADA**.

11.10. As Partes concordam que, a **CONTRATADA** ou o **CONTRATANTE** que, em razão do exercício de atividade de tratamento de dados pessoais, causar a outrem dano patrimonial, moral, individual ou coletivo, em violação à legislação de proteção de dados pessoais, é obrigado a repará-lo, e as demais hipóteses em relação a responsabilidade e ressarcimento de danos serão regidos pelos arts. 42 a 46 e seus incisos da Lei 13.709/2018 (Lei Geral de Proteção de Dados Pessoais – LGPD).

11.11. O **CONTRATANTE** poderá realizar diligência para aferir o cumprimento dessa cláusula, devendo a **CONTRATADA** atender prontamente eventuais pedidos de comprovação formulados, esclarecimentos e/ou informações, no prazo estipulado pela **CONTRATANTE**.

11.12. Ao encerrar as atividades que fazem tratamento de Dados Pessoais, a **CONTRATADA** deve, à escolha do **CONTRATANTE**, apagar ou devolver os Dados Pessoais em sua posse, e apagar as cópias existentes. O tratamento pela **CONTRATADA** deve ocorrer apenas pelo período especificado no Termo de Referência. Até que os dados sejam apagados ou devolvidos, a **CONTRATADA** continuará a garantir o cumprimento do contrato.

CLÁUSULA DÉCIMA SEGUNDA - SUBCONTRATAÇÃO

12.1. Não será admitida a subcontratação do objeto contratual.

CLÁUSULA DÉCIMA TERCEIRA - GARANTIA DE EXECUÇÃO

13.1. A **CONTRATADA** deverá apresentar ao **CONTRATANTE**, em até 05 (cinco) dias úteis, contados da assinatura do contrato, comprovante de garantia, no valor correspondente a **5% (cinco por cento) do valor total do contrato**, cabendo-lhe optar por uma das modalidades de garantia prevista no art. 96, § 1º da Lei n.º 14.133/2021.

13.2. A garantia deverá ser prestada com vigência de 03 (três) meses após o término da vigência do Contrato e será restituída automaticamente, ou por solicitação, **no prazo de até 60 (sessenta) dias contados do final da vigência do contrato ou da rescisão**, somente após comprovação de que a empresa pagou todas as verbas rescisórias trabalhistas decorrentes da contratação.

13.2.1. Caso a **CONTRATADA** não efetive o cumprimento das obrigações previstas no subitem anterior, **a garantia será utilizada para o pagamento dessas verbas trabalhistas diretamente pelo CONTRATANTE**.

13.3. A garantia assegurará, qualquer que seja a modalidade escolhida, o pagamento de:

13.3.1. Prejuízos advindos do não cumprimento do objeto do contrato e do não adimplemento das demais obrigações nele previstas;

13.3.2. Multas moratórias e punitivas aplicadas pela Administração à contratada; e

13.3.3. Obrigações trabalhistas e previdenciárias de qualquer natureza e para com o FGTS, não adimplidas pelo contratado, quando couber.

13.4. Quando a garantia for apresentada em dinheiro, ela será atualizada monetariamente, conforme os critérios estabelecidos pela instituição bancária em que for realizado o depósito.

13.5. Quando a opção da garantia for a modalidade de seguro-garantia, a apólice deverá conter cláusulas específicas, oferecendo cobertura para despesas com obrigações contratuais e riscos trabalhistas, bem como multas que tenham caráter punitivo.

13.6. Aditado o Contrato, prorrogado o prazo de sua vigência ou alterado o seu valor, fica a **CONTRATADA** obrigada a apresentar garantia complementar ou substituí-la, no mesmo percentual e modalidades constantes desta cláusula. Nesses casos, a garantia será liberada após a apresentação da nova garantia e da assinatura do termo aditivo ao Contrato.

13.7. Nas hipóteses em que a garantia for utilizada total ou parcialmente – como para corrigir quaisquer imperfeições na execução do objeto do contrato ou para reparar danos decorrentes da ação ou omissão da **CONTRATADA**, de seu preposto ou de quem em seu nome agir, ou ainda nos casos de multas aplicadas depois de esgotado o prazo recursal – a **CONTRATADA** deverá, no prazo de 03 (três) dias, recompor o valor total dessa garantia, sob pena de aplicação de penalidades previstas neste Contrato.

13.8. Além da garantia de que tratam os arts. 96 e seguintes da Lei nº 14.133/21, a presente contratação possui previsão de **garantia técnica** do serviço a ser fornecido, incluindo manutenção e assistência técnica, conforme condições estabelecidas no Termo de Referência.

13.9. A garantia de execução é independente de eventual garantia do produto prevista especificamente no Termo de Referência.

CLÁUSULA DÉCIMA QUARTA - ALTERAÇÕES CONTRATUAIS

14.1. Eventuais alterações contratuais reger-se-ão pela disciplina dos arts. 124 e seguintes da Lei nº 14.133, de 2021, bem como pela Resolução nº 64/2023, ou outra que vier a substituí-la, e seu anexo VI deste Tribunal de Justiça do Amazonas.

14.2. Registros que não caracterizam alteração do contrato podem ser realizados por simples apostila, dispensada a celebração de termo aditivo, na forma do art. 136 da Lei nº 14.133, de 2021.

CLÁUSULA DÉCIMA QUINTA - FISCALIZAÇÃO

15.1. A existência e a atuação da fiscalização pelo CONTRATANTE em nada restringem a responsabilidade, única, integral e exclusiva da **CONTRATADA**, no que concerne à execução do objeto do contrato.

15.2. O **CONTRATANTE** designará servidor(es) para acompanhamento e fiscalização da prestação dos serviços, que registrará(ão) todas as ocorrências relacionadas com a execução do contrato, estabelecendo prazo para a regularização das falhas ou defeitos observados, observando o disposto no artigo 117 da Lei 14.133/2021

15.3. Ficam reservados à Fiscalização o direito e a autoridade para resolver todo e qualquer caso singular, duvidoso ou omisso, não previstos neste Contrato, no Edital de Licitação e seus anexos, e em tudo mais que, de qualquer forma, se relacione direta ou indiretamente, com os serviços em questão, podendo determinar o que for necessário à regularização das faltas ou defeitos observados.

15.4 Compete à fiscalização técnica além de outras atribuições:

a) Participação em reuniões iniciais, de trabalho e de conclusão da execução contratual;

b) Verificação da conformidade da entrega de material, execução de obra ou prestação de serviço com as especificações, valor unitário ou total, quantidade e prazos estabelecidos no contrato;

c) Registro de todas as ocorrências relacionadas à execução do contrato, indicando o necessário para regularização de falhas ou defeitos;

d) Monitoramento constante da qualidade dos serviços, intervindo para solicitar à contratada a correção de faltas, falhas e irregularidades identificadas, mediante envio de SEP - Solicitação de Esclarecimentos e Providências ou Notificação Contratual.Avaliação periódica, diária, semanal ou mensal, conforme a natureza do objeto, para aferir o desempenho e a qualidade da prestação dos serviços;

e) Registro e comunicação ao gestor das atividades realizadas e pendências observadas na execução do contrato;

f) Manifestação sobre solicitações da contratada para prorrogação da execução/entrega do objeto contratual, abordando interesse na continuidade, prejuízos ao Tribunal decorrentes de atrasos e justificativas para a prorrogação de prazos;

g) Submissão à Seção de Gestão Contratual das manifestações de prorrogação sobre a execução/entrega do objeto contratual, para deliberação da SECAD;

h) Elaboração e assinatura do termo de recebimento provisório, detalhando o cumprimento das exigências técnicas referentes a aquisições, obras ou serviços conforme as regras contratuais;

i) Análise, em conjunto com o fiscal administrativo, dos documentos apresentados para pagamento, submetendo-os ao gestor para ateste ou notificação da contratada para regularização de impropriedades;

j) Proposição de revisão de valores a serem pagos à contratada, registrando em relatório situações como não alcance de resultados, não execução ou execução insatisfatória das obrigações contratadas;

k) Apresentação de relatórios que subsidiem o ateste da nota fiscal pelo gestor do contrato;

l) Participação na atualização do relatório de riscos durante a fase de gestão, juntamente com o fiscal administrativo e setorial;

m) Comunicação imediata à gestão contratual e à Assessoria Técnica de Fiscalização, sobre qualquer ocorrência ou incapacidade técnica da empresa contratada que possa prejudicar a execução nas datas estabelecidas;

n) Proposição ao gestor, em caso de descumprimento contratual, da aplicação de sanções à contratada, conforme as regras do ato convocatório e/ou contrato, seguindo os procedimentos estabelecidos na Resolução n° 64, de 05 de dezembro de 2023;

o) Elaboração, quando necessário, de relatórios, laudos e pareceres referentes às atividades de fiscalização técnica da execução do contrato;

p) Realização de vistorias, atestando o cumprimento de orientações técnicas e indicações de segurança;

q) Assistência à Seção de Gestão Contratual com informações necessárias para elaborar o documento comprobatório da avaliação realizada na fiscalização do cumprimento de obrigações assumidas pelo contratado;

r) Execução de outras atribuições derivadas das cláusulas e especificidades contratuais.

CLÁUSULA DÉCIMA SEXTA - INFRAÇÕES E SANÇÕES ADMINISTRATIVAS

16.1. O processamento e julgamento das infrações e sanções administrativas que incorrer a **CONTRATADA** tramitarão na forma de Processo Administrativo Sancionatório (PAS), consoante as normas previstas no Anexo VIII da Resolução 64/2023 deste Tribunal de Justiça do Amazonas, ou outra que vier a substituí-la.

16.2. Poderão ser aplicadas à **CONTRATADA** que incorrer nas infrações previstas neste Contrato as seguintes sanções:

a) **Advertência**;
b) **Impedimento de licitar e contratar**;
c) **Declaração de inidoneidade para licitar e contratar**;
d) **Multa** de 0,5% a 30% do valor do contrato.

16.3. Comete infração administrativa, nos termos dos artigos 155 e 156 da Lei nº 14.133, de 2021, a **CONTRATADA** que incorrer nas seguintes infrações, cabendo-a as respectivas sanções:

a) **Der causa à inexecução parcial do contrato**;
Sanções: Advertência **e/ou** Multa compensatória de 20% (vinte por cento) sobre o valor da parcela não cumprida, observando que o valor final apurado não poderá ser inferior a 0,5% do valor total do contrato.

b) **Der causa à inexecução parcial do contrato que cause grave dano à Administração ou ao funcionamento dos serviços públicos ou ao interesse coletivo**;
Sanções: Impedimento de licitar/contratar **ou** Declaração de inidoneidade para licitar/contratar **e/ou** Multa compensatória de 20% (vinte por cento) sobre o valor da parcela não cumprida, observando que o valor final apurado não poderá ser inferior a 0,5% do valor total do contrato.

c) **Der causa à inexecução total do contrato;**
Sanções: Impedimento de licitar/contratar **ou** Declaração de inidoneidade para licitar/contratar **e/ou** Multa compensatória de 30% do valor do contrato.

d) **Ensejar o retardamento da execução ou da entrega do objeto da contratação sem motivo justificado;**
Sanções: Impedimento de licitar/contratar **ou** Declaração de inidoneidade para licitar/contratar **e/ou** Multa compensatória.

e) **Apresentar documentação falsa ou prestar declaração falsa durante a execução do contrato;**
Sanções: Declaração de inidoneidade para licitar/contratar **e/ou** Multa compensatória.

f) **Praticar ato fraudulento na execução do contrato;**
Sanções: Declaração de inidoneidade para licitar/contratar **e/ou** Multa compensatória.

g) **Comportar-se de modo inidôneo ou cometer fraude de qualquer natureza;**
Sanções: Declaração de inidoneidade para licitar/contratar **e/ou** Multa compensatória.

h) **Praticar ato lesivo previsto no art. 5º da Lei nº 12.846, de 1º de agosto de 2013;**
Sanções: Declaração de inidoneidade para licitar/contratar **e/ou** Multa compensatória.

i) **Inobservância dos prazos contratuais;**
Sanção: Multa moratória, nos percentuais previstos no art. 18 do Anexo VIII da Resolução 64/2023 deste Tribunal de Justiça do Amazonas, ou outra que vier a substituí-la.

f) **Inobservância do prazo fixado para apresentação, suplementação ou reposição da garantia, quando houver previsão contratual de sua exigência.**
Sanção: Multa moratória, nos percentuais previstos no art. 18 do Anexo VIII da Resolução 64/2023 deste Tribunal de Justiça do Amazonas, ou outra que vier a substituí-la.

16.4. Na aplicação das sanções serão considerados, conforme o art. 156, §1º, da Lei nº 14.133, de 2021):

a) A natureza e a gravidade da infração cometida;
b) As peculiaridades do caso concreto;
c) As circunstâncias agravantes ou atenuantes;
d) Os danos que dela provierem para o Tribunal;
e) A implantação ou o aperfeiçoamento de programa de integridade, conforme normas e orientações dos órgãos de controle;

16.5. A aplicação das sanções realizar-se-á em processo administrativo que assegure o contraditório e a ampla defesa à **CONTRATANTE**, observando-se o procedimento previsto no caput e parágrafos do art. 158 da Lei nº 14.133, de 2021, para as penalidades de impedimento de licitar e contratar e de declaração de inidoneidade para licitar ou contratar.

16.6. Antes da aplicação da multa será facultada a defesa do interessado no prazo de 15 (quinze) dias úteis, contado da data de sua intimação, conforme art. 157, da Lei nº 14.133, de 2021.

16.7. Se a multa aplicada e as indenizações cabíveis forem superiores ao valor do pagamento eventualmente devido pelo **CONTRATANTE** à **CONTRATADA**, além da perda desse valor, a diferença será descontada da garantia prestada ou será cobrada judicialmente, conforme art. 156, §8º, da Lei nº 14.133, de 2021.

16.8. Excepcionalmente, *ad cautelam*, o **CONTRATANTE** poderá efetuar a retenção do valor presumido da multa, antes da instauração do regular procedimento administrativo. Nesta hipótese, instaurará o procedimento em até 30 (trinta) dias contados da retenção.

16.9. A personalidade jurídica do Contratado poderá ser desconsiderada sempre que utilizada com abuso do direito para facilitar, encobrir ou dissimular a prática dos atos ilícitos previstos neste Contrato ou para provocar confusão patrimonial, e, nesse caso, todos os efeitos das sanções aplicadas à pessoa jurídica serão estendidos aos seus administradores e sócios com poderes de administração, à pessoa jurídica sucessora ou à empresa do mesmo ramo com relação de coligação ou controle, de fato ou de direito, com o Contratado, observados, em todos os casos, o contraditório, a ampla defesa e a obrigatoriedade de análise jurídica prévia, conforme art. 160, da Lei nº 14.133, de 2021.

16.10. O **CONTRATANTE** deverá, no prazo máximo 15 (quinze) dias úteis, contado da data de aplicação da sanção, informar e manter atualizados os dados relativos às sanções por ela aplicadas, para fins de publicidade no Cadastro Nacional de Empresas Inidôneas e Suspensas (Ceis) e no Cadastro Nacional de Empresas Punidas (Cnep), instituídos no âmbito do Poder Executivo Federal, conforme art. 161, da Lei nº 14.133, de 2021.

16.11. As sanções de impedimento de licitar e contratar e declaração de inidoneidade para licitar ou contratar são passíveis de reabilitação na forma do art. 163 da Lei nº 14.133/21.

CLÁUSULA DÉCIMA SÉTIMA - EXTINÇÃO CONTRATUAL

17.1. O contrato se extingue quando vencido o prazo nele estipulado, independentemente de terem sido cumpridas ou não as obrigações de ambas as partes contraentes.

17.2. O contrato pode ser extinto antes do prazo nele fixado, sem ônus para o contratante, quando esta não dispuser de créditos orçamentários para sua continuidade ou quando entender que o contrato não mais lhe oferece vantagem.

17.3. A extinção nesta hipótese ocorrerá na próxima data de aniversário do contrato, desde que haja a notificação do contratado pelo contratante nesse sentido com pelo menos 2 (dois) meses de antecedência desse dia, consoante art. 106, § 1º, da Lei 14.133/2021.

17.4. Caso a notificação da não-continuidade do contrato de que trata este subitem ocorra com menos de 2 (dois) meses da data de aniversário, a extinção contratual ocorrerá após 2 (dois) meses da data da comunicação.

17.5. O contrato pode ser extinto antes de cumpridas as obrigações nele estipuladas, ou antes do prazo nele fixado, por algum dos motivos previstos no artigo 137 da Lei nº 14.133/21, bem como amigavelmente, assegurados o contraditório e a ampla defesa.

17.5.1. Nesta hipótese, aplicam-se também os artigos 138 e 139 da mesma Lei.

17.5.2. A alteração social ou a modificação da finalidade ou da estrutura da empresa não ensejará a rescisão se não restringir sua capacidade de concluir o contrato.

17.5.2.1 Se a operação implicar mudança da pessoa jurídica contratada, deverá ser formalizado termo aditivo para alteração subjetiva.

17.6. O termo de rescisão, sempre que possível, será precedido:

17.6.1. Balanço dos eventos contratuais já cumpridos ou parcialmente cumpridos;

17.6.2. Relação dos pagamentos já efetuados e ainda devidos;

17.6.3. Indenizações e multas.

17.7. A extinção do contrato não configura óbice para o reconhecimento do desequilíbrio econômico-financeiro, desde que o pedido ainda tenha ocorrido enquanto vigente a contratação, hipótese em que será concedida indenização por meio de termo indenizatório, conforme art. 131, *caput,* da Lei n.º 14.133, de 2021.

CLÁUSULA DÉCIMA OITAVA - CASOS OMISSOS

18.1. Os casos omissos serão decididos pelo **CONTRATANTE**, segundo as disposições contidas na Lei nº 14.133, de 2021, e demais normas federais aplicáveis e, subsidiariamente, segundo as disposições contidas na Lei nº 8.078, de 1990 – Código de Defesa do Consumidor – e normas e princípios gerais dos contratos.

CLÁUSULA DÉCIMA NONA - PUBLICAÇÃO

19.1. Incumbirá ao **CONTRATANTE** a publicação do **instrumento contratual** no **Portal Nacional de Contratações Públicas (PNCP)**, na forma prevista no art. 94 da Lei 14.133, de 2021, bem como no respectivo **sítio oficial na Internet (Portal Eletrônico do TJAM)**, em atenção ao art. 8º, §2º, da Lei n. 12.527, de 2011, sendo, ainda, facultativa a publicação do **extrato deste Contrato no Diário da Justiça Eletrônico**, conforme dispõe o art. 4º, da Lei nº 11.419, de 19 de dezembro de 2006.

CLÁUSULA VIGÉSIMA - FORO

20.1. Obriga-se a **CONTRATADA**, por si e seus sucessores, ao fiel cumprimento de todas as cláusulas e condições do presente Contrato e elege seu domicílio contratual, o da Comarca de Manaus, capital do Estado do Amazonas, para dirimir eventuais dúvidas originadas pelo presente Termo, com expressa renúncia a qualquer outro, por mais privilegiado que seja, consoante 92, §1º, da Lei 14.133 de 2021.

E assim, por estarem às partes justas e contratadas, foi lavrado o presente instrumento contratual, que lido e achado conforme pelas partes, vai por elas assinado para que produza todos os efeitos de Direito, na presença das testemunhas abaixo identificadas.

Desembargador(a) XXXXXXXX
Presidente do Tribunal de Justiça do Estado do Amazonas
CONTRATANTE

Sr. _____
Representante Legal da Empresa
CONTRATADA

TESTEMUNHAS:

Nome: _____ Nome: _____

Matrícula: _____ Matrícula: _____

Documento assinado eletronicamente por **EDIVAM DE LUCENA NASCIMENTO JUNIOR**, **Servidor**, em 05/08/2024, às 12:02, conforme art. 1º, III, "b", da Lei 11.419/2006.

A autenticidade do documento pode ser conferida no site https://sei.tjam.jus.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0 informando o código verificador **1697518** e o código CRC **3DD4C349**.