PODER JUDICIÁRIO DO ESTADO DO PIAUÍ
STIC - GOVTIC - AQUISIÇÕES E CONTRATAÇÕES DE SOLUÇÕES DE TIC - ACSTIC
Pça Des. Edgard Nogueira s/n - Bairro Cabral - Centro Cívico - CEP 64000-830
Teresina - PI - www.tjpi.jus.br

Termo de Referência Nº 98/2021 - PJPI/TJPI/PRESIDENCIA/STIC/GOVTIC/ACSTIC

TERMO DE REFERÊNCIA PARA AQUISIÇÃO DE SOLUÇÃO DE GERENCIAMENTO DE ACESSOS PRIVILEGIADOS *(PRIVILEGED ACCESS MANAGEMENT - PAM)*

PARA O TRIBUNAL DE JUSTIÇA DO ESTADO DO PIAUÍ

1. FUNDAMENTO LEGAL

1.1. A contratação almejada deriva de procedimento licitatório que obedece, integralmente, às disposições da Lei nº 10.520, de 17 de julho de 2002, Decreto nº5.450 de 31 de maio de 2005, Lei complementar nº 123 de 14 de dezembro de 2006 e subsidiariamente pela Lei nº 8.666/93, de 21 de junho 1993 e suas alterações, e, ainda, pelo estabelecido no instrumento convocatório que tenha permeado o certame.

1.2. Objetivou-se atender também a resolução 182 do CNJ para efeito de auditoria futura pelo Conselho Nacional de Justiça - CNJ.

2. OBJETO

2.1. O objeto deste Termo de Referência é aquisição de licenças para solução de gerenciamento de acessos privilegiados (*Privileged Access Management - PAM*), com garantia de 36 (trinta e seis) meses, com capacidade para armazenar, proteger, controlar, gerenciar, auditar e monitorar o acesso privilegiado a ativos críticos incluindo software e serviço de instalação, configuração, suporte técnico e treinamento das equipes de administração e operação da ferramenta, para ser fornecida de forma única, conforme solicitações, para atender a todas as unidades integrantes do Tribunal de Justiça do Estado do Piauí, incluindo a Corregedoria Geral de Justiça e a EJUD, de acordo com as especificações, condições e quantidades estimadas, descritas neste Termo de Referência e seus Anexos.

3. FUNDAMENTAÇÃO DA CONTRATAÇÃO

3.1. Motivação da contratação (art. 18, §3, II, a)

Com a pandemia do COVID-19 e a utilização massiva da tecnologia para promover o home office, houve o incremento substancial de ações relacionadas ao roubo de credenciais. O Gartner, instituto mundial renomado de pesquisa e consultoria na área de TIC, no aspecto de Segurança da Informação, desde 2019 vem afirmando que investimentos em soluções para proteção das credenciais deve estar no topo de prioridade das empresas. *[Fonte: https://www.gartner.com/en/documents/3900996-top-10-security-projects-for-2019]*

Sendo assim, é dever do TJPI formalizar e conduzir o macroprocesso de segurança da informação, garantindo que os ativos críticos, riscos, ameaças, vulnerabilidades e os incidentes de segurança sejam identificados, monitorados e priorizados por meio de controles efetivos, já que o maior bem existente neste Tribunal são suas informações.

Á medida que são feitas alterações/inclusões nas bases de dados de servidores e magistrados, colaboradores, prestadores de serviços, usuários da sociedade em geral, cresce o volume de informações e dados sensíveis nos diversos sistemas do TJPI.

Essa constante alteração torna a administração dos usuários com acesso privilegiado (administradores das plataformas computacionais) bastante onerosa, o que dificulta sobremaneira sua gestão e auditoria, por não possuir centralização e um controle rígido, o que torna exponencial um possível acesso indevido a informações privilegiadas.

A contratação de uma solução que centralize e permita o **gerenciamento dos acessos privilegiados** é uma necessidade para trazer maior administração, gestão, auditoria e um rígido controle aos acessos privilegiados à infraestrutura de TIC e à todas as informações acerca das diversas plataformas existentes no TJPI. E principalmente, entrando em conformidade com as regulamentações das leis que exigem o cumprimento da segurança da informação.

3.2. Objetivos a serem alcançados (art. 18, §3, II, b)

Aquisição de licenças para solução de gerenciamento de acessos privilegiados (*Privileged Access Management - PAM*), com garantia de 36 (trinta e seis) meses, com capacidade para armazenar, proteger, controlar, gerenciar, auditar e monitorar o acesso privilegiado a ativos críticos incluindo software e serviço de instalação, configuração, suporte técnico e treinamento das equipes de administração e operação da solução.

3.3. Benefícios diretos e indiretos (art. 18, §3, II, c)

Com a contratação em epígrafe são esperados os seguintes resultados:

- Ampliação dos mecanismos de segurança da informação existentes no TJPI;
- Gerenciamento dos acessos privilegiados aos recursos tecnológicos do TJPI;
- Proteção avançada de cada acesso privilegiado, controlando o que é e o que não é permitido fazer baseado em perfis de acesso e operação.
- Redução da superfície de ataque, pois cada administrador só terá acesso aos sistemas que estiverem sob sua responsabilidade;
- Proteção do recurso tecnológico administrado em caso de roubo de credenciais privilegiadas;
- Auditoria e monitoração dos recursos tecnológicos, uma vez que todo acesso é registrado;
- Autenticação centralizada, evitando a necessidade de possuir credenciais espalhadas em vários sistemas diferentes.

3.4. Alinhamento estratégico (art. 18, §3, II, d)

A presente demanda está alinhada ao PLANO DIRETOR DE TECNOLOGIA DA INFORMAÇÃO E COMUNICAÇÃO 2021-2022 (SEI N. 2414707) e a ENTIC-JUD 2021-2026:

ALINHAMENTO - PDTI TJPI 2021-2022		
8.2.4. Objetivo Estratégico		
06: Aprimorar a Segurança da Informação e a Gestão de Dados		
ALINHAMENTO - ENTIC-JUD 2021-2026		
Perspectiva	**Objetivos Estratégicos**	**Iniciativa**
PROCESSOS INTERNOS	Aprimorar a Segurança da Informação e a Gestão de Dados	Melhorar os avanços voltados para a Segurança da Informação e dados pessoais frente aos mais diversos desafios, fazendo-se valer principalmente

		das vantagens oriundas da utilização de Inteligência Artificial e demais soluções disruptivas de TIC.

3.5. Referência aos estudos preliminares (art. 18, §3, II, e)

Este Termo de Referência foi elaborado considerando o Documento de Oficialização da Demanda (DOD) SEI Nº 2368736 e os Estudos Preliminares SEI Nº 2415179 constantes do Processo SEI Nº 21.0.000039416-2, encaminhados pelo setor de Aquisições e Contratações de Soluções de TIC da STIC - ACSTIC.

3.6. Relação entre a demanda prevista e a contratada (art. 18, §3, II, f)

Para promover o gerenciamento, auditoria e monitoração dos acessos privilegiados aos recursos tecnológicos do TJPI, faz-se necessário a aquisição de licenças para solução de gerenciamento de acessos privilegiados (*Privileged Access Management - PAM*) com capacidade para armazenar, proteger, controlar, gerenciar, auditar e monitorar o acesso privilegiado a ativos críticos incluindo software e serviço de instalação, configuração, suporte técnico e treinamento das equipes de administração e operação da ferramenta.

Para atender a demanda atual do TJPI, resta necessário a aquisição unitária de cada um dos seguintes itens:

GRUPO	ITEM	DESCRIÇÃO	CATMAT/CATSER	UN.	Quantidade
1	1	Licenciamento de uso para solução de Gerenciamento de Acessos Privilegiados *(Privileged Access Management - PAM),* com garantia de 36 meses	27472	Unidade	1
	2	Serviço de Instalação e Configuração da Solução de Gerenciamento de Acessos Privilegiados *(Privileged Access Management - PAM)*	26972	Serviço	1
	3	Treinamento de Administração da Solução	384-0	Serviço	1
	4	Treinamento de Operação da Solução	384-0	Serviço	1
	5	Suporte Técnico especializado	27022	Mês	36

3.7. Natureza do objeto (art. 18, §3, II, h)

O objeto a ser contratado enquadra-se na categoria de bens comuns de que tratam a Lei nº 10.520/02 e os Decretos nº 3.555/00 e nº 5.450/05, por possuir padrões de desempenho e características gerais e específicas que podem ser definidos de forma objetiva nas especificações técnicas, que são usualmente encontradas no mercado, podendo, portanto, ser licitado por meio da modalidade Pregão.

3.8. Parcelamento do objeto (art. 18, §3, II, i)

Considerando que se trata de Solução de PAM (Ferramenta de Gerenciamento de Acessos Privilegiados) a ser instalada no *datacenter* deste TJPI, cujo serviço de instalação e configuração, treinamentos e suporte técnico são completamente voltados para a Solução de PAM, não é viável dividir os itens a serem licitados em lotes. Portanto, é imprescindível que a contratação seja feita através de lote único.

3.9. Forma e critério de seleção do fornecedor (art. 18, §3, III, j)

Tratando-se de lote único, a adjudicação do objeto deverá ser realizada para o mesmo fornecedor com vias a garantir a interoperabilidade entre os itens constantes do lote.

Considerando que os bens e serviços são caracterizados como comuns no mercado de TIC, cujos padrões de desempenho e de qualidade podem ser objetivamente definidos, recomenda-se a utilização do sistema de pregão na sua modalidade eletrônica do tipo menor preço.

Os seguintes documentos servirão como condição para aceite da proposta:

i. Especificação clara, completa e minuciosa do produto cotado, informando a marca, o modelo e o fabricante, bem como a indicação precisa da comprovação de cada característica constante nas especificações técnicas deste Termo de Referência, pontuando em forma de planilha cada exigência do edital com sua respectiva comprovação, que deve conter uma ou mais das seguintes:

- Indicação da página/item do manual/*datasheet*;
- URL;
- Seção/subseção ou número de item de página WEB;
- Print de tela da solução;
- Imagem ou vídeo que demonstre a funcionalidade;
- Outra comprovação, desde que seja oficial do fabricante do produto ofertado.

a) Entende-se por documento(s) a documentação técnica oficial do fabricante do produto ofertado, seja em meio eletrônico ou materializada em papel;

b) Não serão aceitas declarações ou cartas de conformidade ou adequação ao solicitado e especificado no termo de referência em substituição ou complementação da documentação técnica oficial e original.

ii. Caso a licitante não seja o próprio fabricante, deverá apresentar documento emitido pelo fabricante dos produtos, que comprove que a licitante é um parceiro oficial habilitado a comercializar seus produtos. A instalação da solução, bem como sua configuração, deverá ser feita por profissional certificado pelo fabricante.

3.9.1. Documentos relativos à QUALIFICAÇÃO TÉCNICA

3.9.1.1. Comprovação de aptidão para o fornecimento de bens em características, quantidades e prazos compatíveis com o objeto desta licitação, ou com o Item pertinente, por meio da apresentação de atestados fornecidos por pessoas jurídicas de direito público ou privado.

3.9.1.2. Para fins da comprovação de que trata este subitem, os atestados deverão dizer respeito a contratos executados com as seguintes características mínimas:

3.9.1.2.1. Os atestados deverão referir-se aos bens fornecidos no âmbito de sua atividade econômica principal ou secundária especificadas no contrato social vigente;

3.9.1.2.2. Considerar-se-ão fornecimentos e/ou serviços semelhantes aqueles de natureza e complexidade similar ao objeto e compatível em características, quantidades e prazos de execução relacionada com o objeto de cada item desta licitação, conforme Acórdão nº 914/2019-Plenário TCU;

3.9.1.2.3. Somente serão aceitos atestados expedidos após a conclusão do contrato ou se decorrido, no mínimo, 12 (doze) meses do início de sua execução, exceto se firmado para ser executado em prazo inferior, conforme item 10.8 do Anexo VII-A da IN SEGES/MPDG Nº 5, de 2017;

3.9.1.2.4. Não serão aceitos atestados decorrentes de contratos em andamento, exceto quando se tratar de serviços executados de forma contínua, conforme definição do Art. 57, II da Lei nº 8.666/93;

3.9.1.3. Os produtos fornecidos, objeto desta licitação, deverão atender aos padrões de qualidade e estarem em conformidade com a legislação vigente no país;

3.9.1.4. Em todos os casos o pregoeiro poderá diligenciar a fim de comprovar o atendimento dos requisitos, antes de proceder à desclassificação do licitante;

3.9.1.5. Quando solicitado pelo pregoeiro, a empresa deverá disponibilizar todas as informações necessárias à comprovação da legitimidade do atestado entregue, apresentando, dentre outros documentos, cópia dos contratos, notas fiscais e dos documentos do responsável técnico pela execução do contrato, com registro no conselho de classe, conforme o caso;

3.10. Impacto ambiental (art. 18, §3, III, k)

Não haverá alteração das propriedades físicas, químicas e biológicas do meio ambiente, causada por qualquer forma de matéria ou energia resultante das atividades humanas que, direta ou indiretamente afetam as condições estéticas e sanitárias do meio ambiente. Dentro do quadro existente a melhoria das condições ambientais será trazida pela destinação adequada dos equipamentos e componentes não utilizados, descarte de resíduos eletrônicos e adoção de critérios de sustentabilidade evitando-se o consumo excessivo de energia elétrica, além de limitar o uso de materiais poluentes (graxas, óleos, gases, etc.).

3.11. Conformidade técnica e legal (art. 18, §3, III, l)

No escopo desta contratação, não foram identificados regulamentos técnicos que precisem ser observados.

3.12. Obrigações contratuais (art. 18, §3, III, m)

3.12.1. Das obrigações da CONTRATANTE

Além das obrigações resultantes da observância da Lei 8.666/93, a CONTRATANTE deverá:

3.12.1.1. Acompanhar, atestar e remeter nas notas fiscais/faturas a efetiva entrega do objeto;

3.12.1.1.1. Validar e aprovar os produtos e serviços liberados.

3.12.1.1.2. Receber o objeto de acordo com as disposições deste Termo de Referência.

3.12.1.1.3. Definir o Gestor do Contrato, responsável por gerir a execução contratual e, sempre que possível e necessário, o Fiscal Administrativo, responsáveis por fiscalizar a execução contratual, conforme disposto no Art. 16 da Resolução 182/2013 do Conselho Nacional de Justiça – CNJ.

3.12.1.2. Efetuar o pagamento do material, nas condições e preços pactuados, dentro do prazo fixado neste contrato, após a entrega da documentação pelo Fiscal de Contrato à SOF.

3.12.1.2.1. Nenhum pagamento será efetuado enquanto houver pendência de liquidação ou qualquer obrigação financeira em virtude de penalidade ou inadimplência;

3.12.1.3. Comunicar à CONTRATADA, o mais prontamente possível, qualquer anormalidade observada no fornecimento do objeto requisitado que possa comprometer a tempestividade, a qualidade e a eficácia do uso a que se destina;

3.12.1.4. Exigir o cumprimento de todos os compromissos assumidos pela CONTRATADA.

3.12.1.5. Fornecer, a qualquer tempo e com a máxima presteza, mediante solicitação escrita da CONTRATADA, informações adicionais, dirimir dúvidas e orientá-la em todos os casos julgados necessários;

3.12.1.6. Manter os contatos com a CONTRATADA por escrito, ressalvados os entendimentos verbais determinados pela urgência que, posteriormente, devem ser confirmados por escrito no prazo de até 72 (setenta e duas) horas.

3.12.1.7. A CONTRATANTE não aceitará, sob nenhum pretexto, transferência de responsabilidade da CONTRATADA para terceiros, sejam fabricantes, representantes ou quaisquer outros.

3.12.1.8. Permitir acesso dos empregados da CONTRATADA às dependências do TJPI para entrega do objeto.

3.12.1.8.1. Fornecer a infraestrutura necessária para a realização das atividades que devam ser executadas em suas instalações conforme as especificações estabelecidas neste Termo de Referência.

3.12.1.8.2. Providenciar o acesso controlado aos recursos de TIC do TJPI para os profissionais da CONTRATADA durante a fase de execução do objeto, caso necessário.

3.12.1.9. Supervisionar e gerenciar os procedimentos a serem realizados pelos fiscais de contrato.

3.12.1.10. Exigir o afastamento de qualquer funcionário ou preposto da CONTRATADA que venha a causar embaraço ou que adote procedimentos incompatíveis com o exercício das funções que lhe forem atribuídas.

3.12.1.11. Responsabilizar-se pela observância às Leis, Decretos, Regulamentos, Portarias e demais normas legais, direta e indiretamente aplicáveis ao contrato.

3.12.1.12. Aplicar à CONTRATADA as penalidades regulamentares e contratuais.

3.12.2. Das obrigações da CONTRATADA

Além das obrigações resultantes da observância da Lei 8.666/93, a CONTRATADA deverá:

3.12.2.1. Fornecer o(s) objeto(s) conforme especificações, quantidades, prazos e demais condições estabelecidas no Edital e seus anexos, na Proposta e no Contrato.

3.12.2.2. Responsabilizar-se integralmente pela sua equipe técnica, primando pela qualidade, desempenho, eficiência e produtividade, visando à execução dos trabalhos vinculados ao fornecimento, dentro dos prazos e condições estipulados, sob pena de ser considerada infração passível de aplicação de penalidades previstas contratualmente, caso os prazos e condições não sejam cumpridos.

3.12.2.3. Responsabilizar-se pela observância de Leis, Decretos, Regulamentos, Portarias e normas federais, estaduais e municipais direta e indiretamente aplicáveis ao objeto do contrato.

3.12.2.4. Atender prontamente às solicitações do Tribunal de Justiça do Estado do Piauí no fornecimento do objeto nas quantidades e especificações deste Termo de Referência, de acordo com a necessidade desta Corte, a partir da solicitação do Gestor do Contrato.

3.12.2.5. Seguir as instruções e observações efetuadas pelo Gestor do Contrato, bem como reparar, corrigir, remover, reconstruir ou substituir, às suas expensas, no todo ou em parte, partes do objeto em que se verificarem vícios, defeitos ou incorreções.

3.12.2.6. Reportar formal e imediatamente ao Gestor do Contrato quaisquer problemas, anormalidades, erros e irregularidades que possam comprometer a execução contratual.

3.12.2.7. Assumir responsabilidade irrestrita sobre a totalidade do fornecimento de insumos e serviços associados ao fornecimento do objeto.

3.12.2.8. Indicar, formalmente, preposto apto a representá-la junto a CONTRATANTE que deverá responder pela fiel execução do Contrato.

3.12.2.9. Cuidar para que o preposto indicado mantenha permanente contato com o Gestor do Contrato e adote as providências requeridas pelo TJPI, além de comandar, coordenar e controlar a atuação deste quando da execução do objeto.

3.12.2.10. Prestar todos os esclarecimentos que forem solicitados pelo Tribunal de Justiça do Piauí, devendo, ainda, atender prontamente às reclamações.

3.12.2.11. Comunicar, imediatamente e por escrito, qualquer anormalidade ou problema detectados, prestando à CONTRATANTE os esclarecimentos necessários.

3.12.2.12. Manter, durante a execução contratual, equipe técnica composta por profissionais devidamente habilitados, treinados e qualificados para o fornecimento do objeto.

3.12.2.13. Assumir inteira responsabilidade técnica e operacional pelo fornecimento do objeto e os serviços diretamente vinculados, não podendo, sob qualquer hipótese, transferir para outra empresa a responsabilidade por eventuais problemas na execução.

3.12.2.14. Responder integralmente por quaisquer perdas ou danos causados à CONTRATANTE ou a terceiros em razão de ação ou omissão, dolosa ou culposa, sua ou dos seus profissionais em razão da execução contratual, independentemente de outras cominações contratuais ou legais a que estiver sujeito.

3.12.2.15. Arcar com todas as despesas decorrentes de transporte, diárias, tributos, seguros, alimentação, assistência médica e de pronto socorro, ou qualquer outra despesa de seus empregados.

3.12.2.16. Arcar com o pagamento de todas as despesas decorrentes do fornecimento do objeto, incluindo as despesas definidas em leis sociais, trabalhistas, comerciais, tributárias e previdenciárias, impostos e todos os custos, insumos e demais obrigações legais, inclusive todas as despesas que onerem, direta ou indiretamente, o objeto ora contratado, não cabendo, pois, quaisquer reivindicações da CONTRATADA, a título de revisão de preço ou reembolso.

3.12.2.17. Promover, por sua conta e risco, o transporte de seus empregados, materiais e utensílios necessários à execução contratual, até as instalações da CONTRATANTE.

3.12.2.18. Respeitar e fazer com que seus empregados respeitem as normas de segurança do trabalho, disciplina e demais regulamentos vigentes no Estado do Piauí, bem como atentar para as regras de cortesia onde sejam executados os serviços.

3.12.2.19. Substituir qualquer de seus profissionais cuja qualificação, atuação, permanência ou comportamento durante a execução do objeto forem julgados prejudiciais, inconvenientes ou insatisfatórios à disciplina do órgão ou ao interesse do serviço público por outro de qualificação igual ou superior, sempre que exigido pela CONTRATANTE.

3.12.2.20. Garantir a execução dos serviços vinculados à execução contratual, mantendo equipe adequadamente dimensionada para tanto, sem ônus adicionais para o órgão contratante.

3.12.2.21. Zelar pela boa e completa execução dos serviços vinculados à execução contratual, mantendo recursos técnicos e humanos necessários para evitar a interrupção indesejada dos mesmos.

3.12.2.22. Facilitar, por todos os meios a seu alcance, a ampla ação fiscalizadora do órgão contratante, atendendo prontamente às observações e exigências que lhe forem dirigidas.

3.12.2.23 Manter sigilo, sob pena de responsabilidade civil, penal e administrativa, sobre todo e qualquer assunto de interesse da CONTRATANTE ou de terceiros de que tomar conhecimento em razão da execução do objeto do Contrato, especialmente em relação a: dados, informações, regras de negócios, documentos, e outros.

3.12.2.24. Honrar os honorários e encargos sociais devidos pela sua condição de única empregadora do pessoal designado para execução dos serviços vinculados ao fornecimento, incluindo indenizações decorrentes de acidentes de trabalhos, demissões, vales-transporte, entre outros, obrigando-se, ainda, ao fiel cumprimento das legislações trabalhistas e previdenciárias, sendo-lhe defeso invocar a existência deste contrato para eximir-se destas obrigações ou transferi-las para a CONTRATANTE.

3.12.2.25. Responder, perante a CONTRATANTE e terceiros, pela conduta dos seus empregados designados para execução do objeto do contrato, com o propósito de evitar condutas que possam comprometer a segurança ou a credibilidade da CONTRATANTE.

3.12.2.26. Adotar regras de vestimenta para seus profissionais adequadas com o ambiente do órgão, com trajes em bom estado de conservação e portando crachá de identificação funcional com foto e nome visível, arcando com o ônus de sua confecção.

3.12.2.27. Utilizar as melhores práticas de mercado no gerenciamento de recursos humanos e supervisão técnica e administrativa para garantir a qualidade da execução do objeto e o atendimento das especificações contidas no Contrato, Edital e seus Anexos.

3.12.2.28. Cumprir e fazer cumprir por seus profissionais as normas e procedimentos estabelecidos na Política de Segurança da Informação da CONTRATANTE.

3.12.2.29. Identificar qualquer equipamento de sua posse que venha a ser utilizado nas dependências do órgão contratante, afixando placas de controle patrimonial, selos de segurança, entre outros pertinentes, e responsabilizar-se por estes.

3.12.2.30. Manter os contatos com a CONTRATANTE sempre por escrito, ressalvados os entendimentos verbais determinados pela urgência na execução do Contrato que, posteriormente, devem sempre ser confirmados por escrito, dentro de até 72 (setenta e duas) horas, a contar da data de contato;

3.12.2.31. Aceitar, nas mesmas condições contratuais, os acréscimos ou supressões que se fizerem necessários de até 25% (vinte e cinco por cento) do valor inicial do contrato.

3.12.2.32. Comunicar à CONTRATANTE, com antecedência de 48 (quarenta e oito) horas os motivos que eventualmente impossibilitem a prestação dos serviços no prazo estipulado, nos casos em que houver impedimento justificado para funcionamento normal de suas atividades, sob a pena de sofrer as sanções da Lei 8.666/93.

3.12.2.33. Vincular-se ao que dispõe a lei nº 3.078, de 11/09/90 (Código de Proteção de Defesa do Consumidor).

3.12.2.34. São expressamente vedadas à CONTRATADA:

I. A contratação de servidor pertencente ao quadro de pessoal do TJ/PI, durante o período de fornecimento.

II. A subcontratação total do objeto do Contrato. E sendo parcial, somente para assistência técnica de garantia e treinamentos, desde que o prestador de serviço seja autorizado pelo fabricante, em qualquer caso, com a anuência do TJPI e com total responsabilidade da CONTRATADA, observadas as mesmas condições de habilitação e qualificação no ato convocatório.

4. ESPECIFICAÇÃO TÉCNICA (ART. 18, §3º, III)

4.1. Modelo de execução e gestão do contrato (art. 18, §3º, III, a)

4.1.1. Principais papéis

I – Equipe de Apoio à Contratação: equipe responsável por subsidiar a Área de Licitações em suas dúvidas, respostas aos questionamentos, recursos e impugnações, bem como na análise e julgamento das propostas das licitantes;

II – Equipe de Gestão da Contratação: equipe composta pelo Gestor do Contrato, responsável por gerir a execução contratual e, sempre que possível e necessário, pelos Fiscais Demandante, Técnico e Administrativo, responsáveis por fiscalizar a execução contratual, consoante às atribuições regulamentares;

III – Equipe de Fiscalização: equipe composta pelos Fiscais Demandante, Técnico e Administrativo, responsáveis por fiscalizar a execução contratual, consoante às atribuições regulamentares;

IV – Gestor do Contrato: servidor com atribuições gerenciais, técnicas ou operacionais relacionadas ao processo de gestão do contrato, sendo responsável por gerir a execução consoante às atribuições regulamentares;

V – Fiscal Demandante do Contrato: servidor representante da Área Demandante da Solução de Tecnologia da Informação e Comunicação, indicado pela respectiva autoridade competente para fiscalizar o Contrato quanto aos aspectos funcionais da solução;

VI – Fiscal Administrativo do Contrato: servidor representante da Área Administrativa, indicado pela respectiva autoridade competente para fiscalizar o Contrato quanto aos aspectos administrativos da execução, especialmente os referentes ao recebimento, pagamento, sanções, aderência às normas, diretrizes e obrigações contratuais;

VII – Fiscal Técnico do contrato: servidor representante da Área de Tecnologia da Informação e Comunicação, indicado pela respectiva autoridade competente para fiscalizar o contrato quanto aos aspectos técnicos da solução;

VIII – Preposto: funcionário representante da CONTRATADA, responsável por acompanhar a execução do Contrato e atuar como interlocutor principal junto ao Gestor do Contrato, incumbido de receber, diligenciar, encaminhar e responder as questões técnicas, legais e administrativas referentes ao andamento contratual. Em caso de substituição do Preposto, a CONTRATADA deverá comunicar formalmente à equipe de fiscalização, via e-mail, o nome do preposto substituto.

4.1.2. Prazos e condições de entrega e recebimento do objeto

4.1.2.1. O prazo de entrega do objeto é de **60 (sessenta) dias corridos**, contados a partir da publicação do extrato do Contrato ou da Ordem de Fornecimento.

4.1.2.1.1. Excepcionalmente, o prazo de recebimento poderá ser prorrogado por até 30 (trinta) dias, desde que solicitado pelo fornecedor e com apresentação de justificativa, nos termos do art. 57, §1º, da Lei nº 8.666/93.

4.1.2.1.2. Toda prorrogação de prazo deverá ser justificada por escrito e previamente autorizada pela autoridade competente a assinar o Contrato ou a Ordem de Fornecimento.

4.1.2.1.3. Caberá à Equipe de Fiscalização e ao setor demandante auxiliarem a autoridade competente na análise do deferimento da prorrogação.

4.1.2.2. A CONTRATADA deverá entregar o objeto em dias úteis, no horário de 08 (oito) às 14 (quatorze) horas, na Sala Cofre do Tribunal de Justiça do Estado do Piauí, situado na Praça Des. Edgard Nogueira s/n, Centro Cívico, CEP 64000-830 - Teresina-PI. É obrigatório o aviso e agendamento da entrega com 24 (vinte e quatro) horas de antecedência, por meio do e-mail: stic@tjpi.jus.br, e/ou dos telefones: (86) 3215-1120, (86) 3230-7869.

4.1.2.3. Por ocasião do recebimento do objeto serão aferidas a qualidade e a quantidade de acordo com o disposto neste Termo de Referência e na proposta vencedora.

4.1.2.4. O objeto deverá ser entregue acompanhado da Nota Fiscal e a cópia do Contrato e/ou Ordem de Fornecimento.

4.1.2.5. Nos termos dos artigos 73 a 76 da lei 8.666/93, o objeto deste Termo de Referência será recebido:

a) provisoriamente, por qualquer dos membros da Equipe de Fiscalização, para efeito de posterior verificação da conformidade do material com a especificação constante neste Termo de Referência;

b) definitivamente, mediante lavratura de Termo de Recebimento Definitivo assinado pela Equipe de Gestão da Contratação, em até 10 (dez) dias úteis do término da fase de instalação, configuração e testes da solução, onde a mesma deverá estar integral e plenamente funcional no ambiente da CONTRATANTE, ocasião em que se fará constar o Atesto na Nota Fiscal.

4.1.2.6. Os produtos entregues em desconformidade com o especificado neste Termo ou o indicado na proposta serão rejeitados parcial ou totalmente, conforme o caso, e a CONTRATADA será obrigada a substituí-los no prazo de até 30 (trinta) dias consecutivos, contados da data do recebimento da Notificação escrita, necessariamente acompanhada do Termo de Recusa do Material, sob pena de incorrer em atraso quanto ao prazo de execução.

4.1.2.6.1. A notificação de que trata o item anterior suspende os prazos de pagamento até que a irregularidade seja sanada.

4.1.2.7. O recebimento não exclui a responsabilidade da CONTRATADA pelo perfeito desempenho do material fornecido ou dos serviços prestados, cabendo-lhe sanar quaisquer irregularidades quando detectadas.

4.1.2.8. Na entrega do objeto, as despesas de embalagem, seguros, transportes, tributos, encargos trabalhistas e previdenciários decorrentes do fornecimento e/ou substituições do objeto, indicadas pela CONTRATANTE, deverão ser de responsabilidade da CONTRATADA, sem ônus para a CONTRATANTE.

4.1.3. Cronograma de execução dos serviços

4.1.3.1. Planejamento da instalação e entrada em operação: em até 15 (quinze) dias contados da publicação do extrato do contrato deverá ser realizada Reunião de Alinhamento entre a STIC e a CONTRATADA. Na ocasião serão acordadas as datas estimadas para entrega do objeto, instalação, testes, entrega definitiva e treinamento da solução, tendo em vista os prazos acordados pelas partes.

4.1.3.2. Prazo de entrega da solução: a CONTRATADA deverá fornecer os equipamentos no prazo máximo de 60 (sessenta) dias corridos contados da publicação do extrato do contrato. Excepcionalmente, o prazo retromencionado poderá ser prorrogado por mais 30 (trinta) dias desde que solicitado pela CONTRATADA acompanhado de justificativa e aprovação por parte da Administração.

4.1.3.3. Fase de instalação, configuração e testes da solução: a CONTRATADA deverá realizar a instalação, configuração e testes com base nas diretrizes e comandos apontados pelo gerente do projeto da CONTRATANTE, neste Termo de Referência e no acordado no item 4.1.3.1 no prazo máximo de 45 (quarenta e cinco) dias contados da entrega da solução. Nesse período, a solução passará por testes extensivos realizados pela equipe da CONTRATANTE. A aprovação desta fase pelo gerente do projeto da CONTRATANTE configura condição necessária para a expedição do termo de recebimento definitivo ou documento equivalente.

4.1.3.4. Prazo para emissão do Termo de Recebimento Definitivo ou documento equivalente: em até 10 (dez) dias úteis do término da fase de instalação, configuração e testes da solução a equipe de planejamento da contratação fornecerá o Termo de Recebimento Definitivo atestando a regularidade do fornecimento e dando início ao prazo da garantia da solução.

4.1.3.4.1. A emissão do Termo de Recebimento Definitivo está condicionada à entrega do documento atestando o início e o fim da vigência da garantia da solução contratada englobando todos os seus itens e serviços contratados (doravante nomeado de “CERTIFICADO DE GARANTIA”) para verificação por parte da equipe de fiscalização.

4.1.3.5. Cronograma da realização dos treinamentos: preferencialmente os treinamentos serão realizados antes da fase especificada do item 4.1.3.3 deste Termo, de acordo com o cronograma pactuado na Reunião de Alinhamento. Alternativamente, poderá ser definido prazo distinto deste item, como por exemplo, seguir o calendário oficial de treinamentos do fabricante do software da solução, desde que acordado expressamente entre CONTRATANTE e CONTRATADA.

4.1.4. Instrumentos formais de solicitação de fornecimento

4.1.4.1. Documento de solicitação de fornecimento: Contrato ou Ordem de fornecimento devidamente assinado por ambos os contratantes.

4.1.4.2. Documento de recebimento provisório: Termo de Recebimento Provisório assinado pela Equipe de Fiscalização da contratação.

4.1.4.3. Documento de recebimento definitivo: Termo de Recebimento Definitivo assinado pela Equipe de Gestão da contratação.

4.1.4.4. Solicitações de chamado técnico:

a) Chamado Técnico por meio de Mensagem eletrônica (e-mail) como ferramenta preferencial de solicitação, acompanhamento e de aferição do serviço prestado pela CONTRATADA;

b) Chamado Técnico de forma eletrônica por meio de Central on-line;

c) Chamado Técnico por meio telefônico para a Central de Atendimento.

4.1.5. Prazos de garantia, suporte e Níveis Mínimos de Serviços Exigidos (NMSE):

4.1.5.1. A CONTRATADA deverá prestar serviços de atendimento técnico, suporte e garantia, através do fabricante da solução, inclusive atualizações e correções, pelo período de **36 (trinta e seis) meses**, a contar da data do recebimento definitivo da instalação, compreendendo, sem custos a CONTRATANTE, dentre outros:

4.1.5.1.1. Manutenção corretiva de hardware dos produtos fornecidos, incluindo a reparação de eventuais falhas, mediante a substituição de peças e componentes por outros de mesma especificação ou superior, novos de primeiro uso e originais, de acordo com os manuais e normas técnicas específicas para os mesmos, com atendimento on-site e sem ônus a CONTRATANTE:

4.1.5.1.1.1. Os componentes danificados deverão ser substituídos, entregues, instalados e configurados, de modo a deixar o equipamento em perfeitas condições de uso e com todas as funcionalidades operacionais, nas dependências da CONTRATANTE, nos prazos de solução estabelecidos neste documento, sem a cobrança de quaisquer custos adicionais (frete, seguro, etc);

4.1.5.1.1.2. Dentro do período de garantia, em casos de falhas de hardware irrecuperáveis ou não solucionadas pelo suporte da CONTRATADA e do fabricante, este último ou seu distribuidor autorizado deverá providenciar troca por componente, módulo ou equipamento idêntico;

4.1.5.1.1.3. No caso de dispositivo de armazenamento que contenha informações de interesse da CONTRATANTE, tais como discos rígidos, a peça substituída ficará sob o poder da CONTRATANTE, na forma da Política de Segurança da Informação vigente;

4.1.5.1.1.4. No caso de troca de equipamento e/ou perda de configuração, a CONTRATANTE prestará o auxílio necessário à CONTRATADA, que será responsável pela atividade, independentemente de onde o equipamento estiver;

4.1.5.1.1.5. No caso de ser necessária a retirada do equipamento defeituoso das dependências da CONTRATANTE, a CONTRATADA deverá relatar por escrito a situação ao fiscal do Contrato ou seu substituto, que autorizará por escrito a saída do referido equipamento, após constatar tal necessidade;

4.1.5.1.2. Atualizações corretivas e evolutivas, de *drivers*, *firmwares*, *softwares* e manuais, durante a vigência da garantia e suporte da solução;

4.1.5.1.3. Ajustes e configurações conforme manuais e normas técnicas do fabricante;

4.1.5.1.4. Demais procedimentos destinados a recolocar a solução em perfeito estado de funcionamento;

4.1.5.1.5. Assistência técnica especializada para investigar, diagnosticar e resolver incidentes e problemas relativos aos produtos fornecidos;

4.1.5.1.6. Fornecimento de informações e esclarecimentos de dúvidas sobre instalação, administração, configuração, otimização, troubleshooting ou utilização dos produtos adquiridos.

4.1.5.2. Caso o equipamento incorpore software de propriedade de outros fabricantes, todo suporte deve ser feito pela CONTRATADA (ponto único de contato para suporte);

4.1.5.3 A garantia de 36 (trinta e seis) meses, para todos os componentes ofertados na proposta, deverá ser comprovada pelo fabricante (por meio de site, portal ou documentação) no momento da contratação, mediante propositura de carta de garantia com aval do fabricante;

4.1.5.3.1. A CONTRATADA deverá apresentar em até 10 dias após a data do recebimento definitivo da instalação, instrumento que comprove, junto ao fabricante, o início do serviço de suporte técnico da solução.

4.1.5.4. A CONTRATADA (ou o fabricante), durante a vigência do contrato, deverá ainda:

4.1.5.4.1. Revisar, semestralmente, as atualizações de *drivers*, *firmwares* e *patches* para todos os equipamentos e softwares contratados. Os serviços de atualizações deverão ocorrer somente para os classificados como críticos, e serão executados de forma remota ou on-site, com prévia anuência da CONTRATANTE;

4.1.5.4.2. Fazer uma avaliação semestral da "saúde" dos equipamentos sob contrato, de forma remota ou on-site, para auxiliar a identificar problemas relacionados à segurança, desempenho, configuração e disponibilidade, antes que causem impactos ou paradas não programadas ao ambiente da CONTRATANTE;

4.1.5.4.3. Revisar os boletins de suporte disponibilizados pelo respectivo fabricante, analisar suas aplicabilidades ao ambiente da CONTRATANTE e fazer recomendações específicas as quais poderão reduzir riscos e melhorar a operação;

4.1.5.4.4. Fornecer assistência de instalação remota para as devidas atualizações recomendadas.

4.1.5.5. Devem ser disponibilizados serviços de suporte (incluindo manutenção de hardware) durante 7 (sete) dias da semana, 24 (vinte e quatro) horas por dia, executando-os sempre que acionados pela CONTRATANTE, mediante a abertura de chamado técnico, prestados por técnicos devidamente habilitados e credenciados pelo fabricante, com nível de certificação compatível com as atividades a serem executadas, e sem qualquer ônus adicional;

4.1.5.6. Os serviços de atendimento da Central de Assistência técnica deverão ser providos das seguintes formas:

4.1.5.6.1. Um canal de suporte técnico através de um número telefônico de serviço, em língua portuguesa, para abertura de chamados técnicos de hardware e software. Este serviço deverá obrigatoriamente estar disponível 8x5 (oito horas por dia, 5 dias por semana, durante o horário comercial) sem custos para a CONTRATANTE;

4.1.5.6.2. Um canal de suporte técnico através de Portal web e/ou correio eletrônico (e-mail), deverá ser disponibilizado de forma ininterrupta 24x7 (vinte e quatro horas por dia, sete dias por semana);

4.1.5.6.3. Deverá ser disponibilizada, para a equipe técnica da CONTRATANTE, uma conta de acesso (somente leitura) para acompanhamento de chamados de suporte e manutenção abertos;

4.1.5.6.4. Deverá ser disponibilizada, para a equipe técnica da CONTRATANTE, uma conta de acesso para consulta de documentação técnica do fabricante e atualizações de software;

4.1.5.7. Os chamados técnicos deverão possuir identificador de ocorrência próprio, data e hora de abertura devidamente repassada a CONTRATANTE, a fim de registro e acompanhamento das ocorrências;

4.1.5.8. A CONTRATADA deverá informar o número do chamado e disponibilizar um meio de acompanhamento das ocorrências e de seus estados;

4.1.5.9. Ao final de cada atendimento, a CONTRATADA deverá emitir relatório técnico contendo as seguintes informações:

A) Número do chamado;

B) Categoria de prioridade;

C) Descrição do problema e da solução;

D) Procedimentos realizados (passo a passo);

E) Data e hora da abertura e do fechamento do chamado;

F) Data e hora do início e do término da execução dos serviços; e

G) Identificação do técnico da empresa.

4.1.5.10. O tempo de solução para os chamados técnicos abertos será contado a partir do registro dos mesmos em qualquer um dos meios disponíveis da Central de Atendimento da CONTRATADA;

4.1.5.10.1. O encerramento do chamado será dado por técnico da CONTRATANTE na conclusão dos serviços;

4.1.5.11. Em caso de atraso na conclusão do atendimento, em qualquer nível de prioridade, será admitida a proposição, pela CONTRATADA, de justificativa técnica, a qual deverá conter os motivos do atraso, acompanhados da devida comprovação;

4.1.5.11.1. A justificativa eventualmente apresentada será analisada pela Administração a qual emitirá parecer, para fins de sua aceitação ou não;

4.1.5.11.2. Em sendo aceita, ocorrerá tão somente a interrupção dos prazos contratuais, sem prejuízo da conclusão do chamado. Em não sendo aceita, impor-se-á as sanções previstas neste documento, bem como no Termo de Referência e eventual Contrato Administrativo.

4.1.5.11.3. Não será aceita justificativa cujo teor funde-se na:

a) Falta de peças comuns em estoque da CONTRATADA ou de mão de obra disponível para deslocamento imediato;

b) Para aplicação do item anterior, entender-se-á como peças comuns os itens cujo valor de mercado não ultrapasse o valor de 10% (dez por cento) do bem principal a ser suportado.

4.1.5.11.4. A justificativa deverá ser apresentada em até 03 (três) dias úteis da conclusão do chamado. Uma vez apresentada fora deste prazo, caberá à Administração conhecer ou não o documento;

4.1.5.12. A CONTRATADA/FABRICANTE deverá disponibilizar site na internet incluindo pelo menos a relação de licenças de uso disponíveis, base de conhecimento, fórum de discussão, documentação técnica dos produtos ofertados, comunidades técnicas, abertura e acompanhamento do histórico de chamados, sem limite de quantidade, download de produtos, atualizações e correções;

4.1.5.13. Durante todo período de vigência do contrato de suporte o Tribunal de Justiça do Estado do Piauí terá direito a atualização de versão de Software para todas as licenças de uso;

4.1.5.14. Os **Níveis Mínimos de Serviços Exigidos (NMSE)** serão classificados conforme os níveis de severidade a seguir:

Nível de Severidade	Descrição	Prazo de Atendimento	Prazo de Solução D

ALTA	Esse nível de severidade é aplicado quando há indisponibilidade de qualquer item de software ou hardware apresentando falha de funcionamento ou impactando diretamente toda a infraestrutura da solução;	02 (duas) horas	24 (vinte e quatro)
MÉDIA	Esse nível de severidade é aplicado quando há falha, simultânea ou não, de hardware ou software que não inviabilize o uso da solução, mas diminua alguma funcionalidade ou afete negativamente a performance;	04 (quarto) horas	48 (quarenta e oito
BAIXA	Este nível de severidade é aplicado para instalação, configuração, manutenções preventivas, esclarecimentos técnicos relativos ao uso e aprimoramento do(s) equipamento(s) e/ou software(s) da solução. Ou seja, chamados técnicos que não requeiram imediato atendimento e/ou solução. Para efeitos de Acordo de Nível de Serviço (SLA), não haverá abertura de chamados técnicos com esta severidade em sábados, domingos e feriados, sendo o tempo de SLA deslocado para o seguinte dia útil, horário comercial.	06 (seis) horas	72 (setenta e duas)

4.1.5.15. Os **Níveis Mínimos de Serviços Exigidos (NMSE)** serão tratados da seguinte forma:

i. Prazo de Solução Definitiva: Tempo decorrido entre o envio da mensagem de chamado técnico e a efetiva recolocação da solução em seu pleno estado de funcionamento;

ii. Caso seja verificado que a solução apresentada pela empresa não resolveu o problema definitivamente, o chamado será reaberto pelo Fiscal Técnico ou Gestor do Contrato e o prazo continuará a ser contado a partir do momento de sua suspensão.

iii. A interrupção do suporte de um chamado técnico classificado no tipo de criticidade MÉDIA ou ALTA pela CONTRATADA e que não tenha sido previamente autorizado pelo Fiscal Técnico ou Gestor do Contrato, poderá ensejar em aplicação de penalidades previstas.

iv. Após a conclusão do suporte, a equipe técnica da CONTRATADA comunicará formalmente (preferencialmente por mensagem eletrônica) ao Fiscal Técnico ou Gestor do Contrato e solicitará autorização para o fechamento do chamado;

v. Entende-se por término do atendimento técnico a hora em que a solução for disponibilizada para uso em perfeitas condições de funcionamento, estando condicionado à aprovação da CONTRATANTE.

vi. Caso não seja confirmada a solução definitiva do problema, o chamado permanecerá aberto até que seja efetivamente solucionado pela CONTRATADA. Nesse caso, o Fiscal Técnico ou Gestor do Contrato informará as pendências relativas ao chamado aberto.

vii. Por necessidade excepcional de serviço, o Fiscal Técnico ou Gestor do Contrato poderá solicitar o escalonamento de chamado para níveis superiores de criticidade. Nesse caso, o escalonamento deverá ser justificado e os prazos dos chamados técnicos reiniciar-se-ão.

viii. Sempre que houver quebra dos níveis de serviços exigidos ou problemas que afetem a execução do objeto, o Gestor do Contrato enviará notificação por mensagem eletrônica para a CONTRATADA que terá o prazo de até 48 (quarenta e oito) horas corridas e contadas a partir do recebimento da notificação para apresentar as justificativas para as falhas verificadas;

ix. Caso não haja manifestação dentro desse prazo ou caso o Gestor do Contrato entenda serem improcedentes as justificativas apresentadas, será iniciado processo de aplicação de penalidades previstas, conforme o nível de serviço transgredido.

x. Em qualquer das criticidades o chamado técnico que envolva o reparo ou a substituição de peças e/ou componentes da solução deve ser feito por técnicos da CONTRATADA on-site, onde o equipamento estiver instalado, salvo em caso de impossibilidade técnica devidamente justificada pela CONTRATADA, com a anuência da CONTRATANTE, obedecendo os prazos de garantia e Níveis de Serviço Exigidos (NSE) neste documento.

4.1.6.Formas de comunicação e acompanhamento

4.1.6.1. Além da reunião de alinhamento e validação de expectativas, deverão ser realizadas, se necessárias, outras reuniões, presenciais ou não, entre o Gestor do Contrato e o Preposto da CONTRATADA para avaliação do(s) serviço(s) prestado(s) no período, e verificação do atendimento aos requisitos contratuais estabelecidos;

4.1.6.2. Poderão ser realizados, alternativamente, e a critério do Gestor do Contrato, o controle e o acompanhamento da prestação de serviço mediante o uso de mensagens eletrônicas. Nesse caso, o Fiscal Técnico ou Gestor do Contrato deverá apresentar descritivo contendo situações merecedoras de avaliação por parte da CONTRATADA.

4.1.7. Forma de pagamento

4.1.7.1. O pagamento obedecerá, para cada fonte diferenciada de recursos, a estrita ordem cronológica das datas de suas exigibilidades, conforme determinado pela IN TCE/PI nº 02/2017 e art.5º da Lei 8.666/93.

4.1.7.2. O pagamento será efetuado pela Administração, em moeda corrente nacional, por Ordem Bancária, acompanhado dos seguintes documentos, remetidos pelo Fiscal de Contrato ou pela Comissão de Fiscalização:

a) Termo de Recebimento Definitivo ou Recibo, devidamente preenchido e assinado;

b) Apresentação da Nota Fiscal com dados bancários, fatura ou documento equivalente, atestado pelo setor competente;

c) Cópia do Contrato Administrativo ou da Ordem de Fornecimento; e

d) Cópia da Nota de Empenho;

e) Prova de regularidade perante o Instituto Nacional do Seguro Social – INSS;

f) Prova de regularidade do FGTS;

g) Prova de regularidade com a Fazenda Pública Federal, Estadual e Municipal do domicílio ou sede e dívida ativa;

h) Certidão Negativa de Débitos Trabalhistas; e

i) Consulta ao Cadastro de Empresas Inidôneas e Suspensas - CEIS.

4.1.7.3. As certidões extraídas do Sistema de Cadastramento Unificado de Fornecedores – SICAF substituirão os documentos relacionados nas letras e, f, g e h,nos termos da Instrução Normativa nº 03/2018 - SEGES/MPDG.

4.1.7.4. A Nota Fiscal/Fatura deverá ser emitida pela licitante vencedora, obrigatoriamente com o número de inscrição no CNPJ apresentado nos documentos de habilitação e das propostas, não se admitindo Notas Fiscais/Faturas emitidas com outros CNPJ, mesmo aquelas de filiais ou da matriz. As Notas Fiscais deverão conter discriminação idêntica à contida na respectiva Nota de Empenho.

4.1.7.5. O banco ao qual pertence a conta da empresa deve ser cadastrado no sistema do Banco Central do Brasil, para que seja possível a compensação bancária, na qual a SOF / FERMOJUPI creditará os pagamentos a que faz jus a empresa CONTRATADA.

4.1.7.6. Nenhum pagamento será efetuado enquanto houver pendência de liquidação ou qualquer obrigação financeira em virtude de penalidade ou inadimplência.

4.1.7.7. Na existência de erros, omissões ou irregularidades, a documentação será devolvida à empresa CONTRATADA/fornecedora, para as correções devidas, passando o novo prazo para pagamento a ser contado a partir da data da apresentação dos documentos corrigidos.

4.1.7.8. Não haverá, em hipótese alguma, pagamento antecipado.

4.1.7.9. Nos casos de eventuais atrasos de pagamento, desde que a licitante vencedora não tenha concorrido de alguma forma para tanto, incidirão correção monetária e juros moratórios.

4.1.7.10. Fica convencionado que a correção monetária e os encargos moratórios serão calculados entre a data do adimplemento da parcela e a do efetivo pagamento da nota fiscal/fatura, com a aplicação da seguinte fórmula:

EM = I x N x VP

Onde:

EM = Encargos moratórios;

N = Número de dias entre a data prevista para o pagamento e a do efetivo pagamento;

VP = Valor da parcela a ser paga.

I = Índice de compensação financeira = 0,0001638, assim apurado:

I = TX/365 I = 0,06/365 I = 0,0001644

TX = Percentual da taxa anual = 6%.

4.1.7.11. A correção monetária será calculada com a utilização do índice IGPM da Fundação Getúlio Vargas.

4.1.7.12. No caso de atraso na divulgação do IGPM, será pago à licitante vencedora a importância calculada pela última variação conhecida, liquidando a diferença correspondente tão logo seja divulgado o índice definitivo.

4.1.7.13. Caso o IGPM estabelecido venha a ser extinto ou de qualquer forma não possa mais ser utilizado, será adotado em substituição o que vier a ser determinado pela legislação então em vigor.

4.1.7.14. Na ausência de previsão legal quanto ao índice substituto, as partes elegerão novo índice oficial.

4.1.7.15. Qualquer atraso ocorrido na apresentação da nota fiscal, ou dos documentos exigidos como condição para pagamento por parte da CONTRATADA importará em prorrogação automática do prazo de vencimento da obrigação da CONTRATANTE.

4.1.8. Transferência de conhecimento

4.1.8.1. Os seguintes procedimentos deverão ser seguidos durante toda a execução do objeto, em especial durante a prestação de serviço de garantia técnica:

i. A equipe da CONTRATADA deverá apresentar ao Fiscal Técnico do Contrato de forma objetiva e por escrito todos os procedimentos realizados nos chamados abertos pelo TJPI em vistas de problemas ou interrupções na solução que forem sanados.

ii. Para que ocorra a transferência de conhecimento, no fechamento dos chamados técnicos de garantia técnica, a CONTRATADA deverá apresentar por mensagem eletrônica ou em documento apropriado, a solução para o problema que originou a abertura do chamado;

iii. O envio da solução pelos meios devidos não exime a CONTRATADA da apresentação do Relatório Gerencial de Serviços com a consolidação dos chamados técnicos abertos;

iv. Os conhecimentos técnicos repassados para a equipe da Secretaria de Tecnologia da Informação serão utilizados em casos de interrupção, transição e encerramento contratual, de modo a minimizar impactos e permitir que as necessidades do TJPI não sejam prejudicadas ou interrompidas.

4.1.9. Direitos de propriedade intelectual

4.1.9.1. Os direitos de propriedade intelectual permanecerão de posse da empresa fabricante do produto a ser adquirido, não havendo transferência de direitos de propriedade em face de contratação, salvo os direitos de uso da solução contratada.

4.1.10. Qualificação técnica e formação dos profissionais envolvidos

4.1.10.1. Os profissionais da CONTRATADA deverão possuir qualificação condizente com o fornecimento do objeto, em especial deverão possuir certificação ou documento equivalente emitido pela fabricante da solução a ser fornecida, que ateste a qualificação técnica do profissional na operação, manutenção e instalação da solução

4.1.10.2. O instrutor que ministrará os treinamentos objeto dos Item 3 - Treinamento de Administração da Solução e 4 - Treinamento de Operação da Solução, do lote único deste Termo deverá ser credenciado como instrutor autorizado pela fabricante do software da solução.

4.1.11. Penalidades administrativas

4.1.11.1. Comete infração administrativa nos termos da Lei nº 8.666/93 e da Lei nº 10.520/02, a licitante vencedora que:

4.1.11.1.1. Não Celebrar o Contrato;

4.1.11.1.2. Deixar de entregar ou apresentar documentação falsa exigida para o certame;

4.1.11.1.3. Ensejar o retardamento da execução de seu objeto;

4.1.11.1.4. Não mantiver a proposta;

4.1.11.1.5. Falhar ou fraudar na execução do contrato;

4.1.11.1.6. Comportar-se de modo inidôneo;

4.1.11.1.7. Cometer fraude fiscal;

4.1.11.2. Para os fins do item 4.1.11.1.6, reputar-se-ão inidôneos atos tais como os descritos nos artigos 92, parágrafo único, 96 e 97, parágrafo único, da Lei n.º 8.666/93.

4.1.11.3. A CONTRATADA que cometer qualquer das infrações discriminadas acima ficará sujeita, sem prejuízo da responsabilidade civil e criminal, às seguintes sanções, tomando por base o Anexo I, do Termo de Referência.:

a) Advertência, em caso de faltas ou descumprimentos de regras contratuais que não causem prejuízo a CONTRATANTE

b) Multa:

b.1) Multa moratória de até 15% (quinze por cento) sobre o valor da parcela inadimplida, no caso de atraso injustificado, até o limite de 30 (trinta) dias;

b.2) Multa compensatória de até 30% (trinta por cento) sobre o valor do contrato, no caso de inexecução total do objeto, configurada após o nonagésimo dia de atraso;

b.3) Em caso de inexecução parcial, aplicar-se-á a multa compensatória, no mesmo percentual do subitem anterior, de forma proporcional à obrigação inadimplida;

c) Suspensão temporária de participação em licitação e impedimento de contratar com a Administração, por prazo não superior a 02 (dois) anos;

d) Declaração de inidoneidade para licitar ou contratar com a Administração Pública enquanto perdurarem os motivos determinantes da punição ou até que seja promovida a reabilitação perante a própria autoridade que aplicou a penalidade.

e) Impedimento de licitar e contratar com a União, Estados, Distrito Federal ou Municípios, pelo prazo de até 05 (cinco) anos, sem prejuízo das multas previstas neste Contrato e demais cominações legais.

4.1.11.4. As sanções previstas nas alíneas "a", "c" e "d" do subitem anterior poderão ser aplicadas cumulativamente à pena de multa, de acordo com o Anexo I, do Termo de Referência.

4.1.11.5. Também ficam sujeitas às penalidades do art. 87, III e IV da Lei nº 8.666, de 1993, as empresas ou profissionais que:

4.1.11.5.1. Tenham sofrido condenação definitiva por praticar, por meio dolosos, fraude fiscal no recolhimento de quaisquer tributos;

4.1.11.5.2. Tenham praticado atos ilícitos visando a frustrar os objetivos da licitação;

4.1.11.5.3. Demonstrem não possuir idoneidade para contratar com a Administração em virtude de atos ilícitos praticados.

4.1.11.6. Após o nonagésimo dia de atraso, o TJ/PI poderá rescindir o contrato, caracterizando-se a inexecução total do seu objeto.

4.1.11.7. A aplicação de qualquer das penalidades previstas realizar-se-á em processo administrativo que assegurará o contraditório e a ampla defesa à CONTRATADA, observando-se o procedimento previsto na Lei nº 8.666, de 1993.

4.1.11.8. A autoridade competente, na aplicação das sanções, levará em consideração a gravidade da conduta do infrator, o caráter educativo da pena, bem como o dano causado à Administração, observado o princípio da proporcionalidade.

4.1.11.9. O valor da multa aplicada será descontado da garantia prestada, se houver, ou descontado de pagamentos eventualmente devidos à CONTRATADA. Na inexistência destes, será pago mediante depósito bancário em conta a ser informada pela CONTRATANTE ou judicialmente.

4.1.11.10. Ad cautelam, o TJ/PI poderá efetuar a retenção do valor presumido da multa, antes da instauração do regular procedimento administrativo.

4.1.11.11. Se o valor do pagamento for insuficiente, fica a CONTRATADA obrigada a recolher a importância devida no prazo de 15 (quinze) dias, contado da comunicação oficial.

4.1.11.12. Esgotados os meios administrativos para cobrança do valor devido pela CONTRATADA ao TJ/PI, a CONTRATADA será encaminhada para inscrição em dívida ativa.

4.1.11.13. Do ato que aplicar a penalidade caberá recurso, no prazo de 05 (cinco) dias úteis, a contar da ciência da intimação, podendo a Administração reconsiderar ou não sua decisão ou nesse prazo, encaminhá-lo, devidamente informados para a apreciação e decisão superior, dentro do mesmo prazo;

4.1.11.14. Serão publicadas no Diário da Justiça do TJPI as sanções administrativas previstas, inclusive a reabilitação perante a Administração Pública.

5. REQUISITOS TÉCNICOS ESPECÍFICOS (ART. 18, §3º, IV)

1. QUANTO AOS COMPONENTES DA SOLUÇÃO

1.1. A solução de PAM deverá ser composta pelos itens abaixo:

GRUPO	ITEM	DESCRIÇÃO	UN.	QUANTIDADE
1	1	Licenciamento de uso para solução de Gerenciamento de Acessos Privilegiados *(Privileged Access Management - PAM),* com garantia de 36 meses	Unidade	1
	2	Serviço de Instalação e Configuração da Solução de Gerenciamento de Acessos Privilegiados *(Privileged Access Management - PAM)*	Serviço	1
	3	Treinamento de Administração da Solução	Serviço	1
	4	Treinamento de Operação da Solução	Serviço	1
	5	Suporte Técnico especializado	Mês	36

1.2. A solução de PAM deverá suportar o seguinte cenário atual (conforme tabela abaixo), com possibilidade de expansão **sem custos adicionais**, considerando a natureza do ambiente e as novas demandas que eventualmente serão solicitadas.

ITEM	QUANTIDADE
Dispositivos de rede: LAN, WAN, WI-FI, Firewalls, IPS, AntiSpam e Filtro de conteúdo	280
Servidores: hipervisor Vmware ESXI/VMs, hipervisor Hyper-V/VMs, Windows Server 2003, 2008 R2, 2012 e superiores, Linux CenOS, RHEL, Debian e Ubuntu	300
Instância de banco de dados MS SQL Server 2008 R2 ou superior, Postgres e MySQL	50
Instâncias de aplicações/serviços corporativos/senhas hardcode	200
Usuários com acesso à dispositivos geridos pela solução	100
Quantidade de acessos simultâneos à ferramenta PAM	80
Workstations (com sistema operacional Windows)	3000
Servidores Microsoft IIS, Apache, Jobss, Wildfly, Glassfish, etc	100
Horas de gravação diária/retenção	6 horas por dia / 120 dias

2. QUANTO AOS ASPECTOS GERAIS

2.1. Possuir licenças de forma a atender os quantitativos definidos no item “1. COMPONENTES DA SOLUÇÃO";

2.2. A solução deve, no que for aplicável, apoiar no atendimento aos requisitos (artigos 6, 42, 43, 46, 48 e 50) da Lei Geral de Proteção de Dados-LGPD, Lei Nº 13.709, de 14 de agosto de 2018, como:

2.2.1. Determinar como os dados deverão ser tratados, mantidos e protegidos e a quem responsabilizar em caso de descumprimento;

2.2.2. Proteger o acesso a dados pessoais sensíveis;

2.2.3. Auxiliar na resposta a incidentes.

2.2.4. 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.

2.3. Serão permitidas integrações com soluções de múltiplos fabricantes para determinadas funções ou funcionalidades, desde que a integração entre as soluções seja plenamente funcional.

2.4. A solução deverá prover mecanismos de atualização de segurança;

2.5. Ter a capacidade de gerenciar credenciais que estejam em sistemas localizados em múltiplas localidades geográficas ou domínios distintos;

2.6. Ter uma console de configuração unificada para gerenciamento de contas e ativos agregados ao cofre de senhas;

2.7. No momento da apresentação das propostas, todos os componentes de software constantes da Solução deverão possuir EOL (End-of-life) e EOS (End-of-support) não definidos, ou anunciados para um prazo superior a 36 (trinta e seis) meses.

2.8. Deve possuir interface única para gerenciamento de senhas e sessões, implementada em HTML5 ou cliente único compatível com sistema operacional Windows 10 e superiores.

2.9. Não deve depender da instalação de agentes para realizar a troca de senhas ou a gravação de sessão.

2.10. Deve proteger contra a perda, roubo e gestão inadequada de credenciais através de regras de complexidade da senha que incluam comprimento da senha (quantidade de caracteres), frequência de troca da senha, especificação de caracteres permitidos ou proibidos na composição da senha.

2.11. Deve ser capaz de descobrir credenciais privilegiadas utilizadas por serviços e processos automatizados.

2.12. Deve propagar as senhas geradas de forma aleatória onde quer que estas estejam referenciadas.

2.13. Deve possibilitar integração com sistema de chamados para aprovação de workflow.

2.14. Deve gerenciar de forma segura, no mínimo, 200 (duzentas) senhas utilizadas por contas de serviço, impedindo a utilização de senhas em texto claro por scripts ou rotinas dos equipamentos.

2.15. Deve garantir a aplicação exclusiva de privilégios adequados, provendo acesso às senhas das contas privilegiadas somente ao pessoal autorizado.

2.16. A solução não deve limitar o quantitativo de contas que podem ser gerenciadas em um dispositivo licenciado.

2.17. Deve permitir a opção de implementar o gerenciamento de troca de senhas em redes separadas e dispositivos remotos.

2.18. Deve criptografar o banco de dados utilizado pela solução para o armazenamento das senhas e credenciais gerenciadas por esta.

2.19. Deve ainda ser compatível com pelo menos dois dos seguintes métodos e padrões de criptografia:

2.19.1. AES com chaves de 256 bits;

2.19.2. FIPS 140-2;

2.19.3. Encriptação PKCS#11 ou superior por hardware utilizando dispositivos de HSM devidamente homologados pelo fabricante para a solução ofertada;

2.20. Deve incorporar medidas de segurança, incluindo criptografia a fim de proteger a informação em trânsito entre os módulos distribuídos e entre as aplicações Web dos usuários finais.

2.21. Não deve permitir a abertura do cofre com chaves criptográficas geradas por seus respectivos fornecedores e/ou fabricantes.

2.22. Deve permitir, através de interface gráfica, que administradores possam configurar as integrações com dispositivos e/ou plataformas que não são disponibilizadas nativamente, sem a necessidade de serviços profissionais de terceiros.

2.23. Deve permitir que o administrador configure a comunicação com aplicações de terceiros utilizando scripts, linguagens de programação diversas e aceite protocolos variados incluindo, no mínimo, SSH e HTTP/HTTPS.

2.24. Deve permitir o envio automático de logs para servidores SYSLOG de forma aderente ao disposto em RFC 5424 - The Syslog Protocol (IETF).

2.25. A solução deve ser disponibilizada com um SDK (Software Development Kit) ou API (Application Programming Interface) que pode ser configurado para permitir que aplicações possam:

2.25.1. Solicitar as credenciais sob demanda ao invés de utilizar credenciais estáticas;

2.25.2. Atualizar informações de contas automaticamente no banco de dados de senhas;

2.25.3. Inscrever automaticamente em sistemas alvo sem aguardar por atualizações dinâmicas;

2.26. Deve permitir o agrupamento lógico de sistemas a fim de simplificar a configuração de políticas apropriadas para diferentes tipos de sistema salvo;

2.27. Deve permitir a atualização de uma mesma conta em múltiplos sistemas alvo com uma única tarefa de alteração de senhas.

2.28. Deve proteger as senhas de credenciais compartilhadas que seriam normalmente armazenadas em planilhas e arquivos em texto claro.

2.29. Deve conceder acesso aos sistemas utilizando "Remote Desktop" e "SSH" sem que os usuários vejam qualquer senha, garantindo que não haja necessidade de instalação de aplicações e/ou agentes nos servidores para realizar o acesso, devendo conceder acesso a:

2.29.1. Sistemas ou 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 sistema operacional 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;

2.29.2. Sistemas baseados em Remote Desktop e SSH sem que os usuários vejam a senha. A senha vigente no momento (estática ou dinâmica) deverá ser provida para as aplicações ou conexões remotas devendo ser recuperadas de forma automática e transparente do banco de dados da solução;

2.30. Deve permitir que os usuários solicitem acesso aos gestores através de interface Web intuitiva.

2.31. Deve oferecer em sua aplicação diferentes visões e opções de acordo com as permissões dos usuários, mostrando, por exemplo, apenas as funcionalidades delegadas àquele usuário.

2.32. A solução deve ser configurável para enviar alertas disparados pelo sistema, no mínimo, por e-mail e SNMP, para eventos customizados pelo administrador do sistema que contemplem pelo menos um dos seguintes serviços:

2.32.1. Caso serviços essenciais estejam parados;

2.32.2. Caso atinja o limite de processamento da CPU;

2.32.3. Caso atinja o limite de processamento da memória;

2.32.4. Caso atinja o limite de capacidade do armazenamento de dados;

2.32.5. A solução deve ser monitorável via ferramenta Zabbix ou similar;

2.33. Deve registrar cada acesso, incluindo os acessos via aplicação web para solicitações de senha, aprovações, checkouts, mudanças de delegação, relatórios e outras atividades. Devem ser registrados os acessos à console de gerenciamento tanto para configuração quanto para relatórios, bem como todas as atividades de alterações de senhas.

2.34. Caso seja separado em componentes, nenhum deles deve conter senhas em texto claro para autenticação.

2.35. O gerenciamento de identidades privilegiadas deverá disponibilizar:

2.35.1. Mecanismo de retirada e devolução de contas e senhas compartilhadas;

2.35.2. Definição de Tempo de Validade: permitir o estabelecimento de tempo de validade para as senhas de identidades privilegiadas gerenciadas que forem requisitadas;

2.35.3. Troca automática da senha no sistema gerenciado, após a sua devolução ou após o vencimento do tempo de validade estabelecido;

2.35.4. Configuração de calendário de requisição de senhas de identidades privilegiadas com base em usuários ou grupos de usuários;

2.35.5. Troca de Senhas por Demanda: Permitir a troca de senhas nos Sistemas Gerenciados, de forma individual ou por grupos customizáveis, manualmente ou de forma automática, por agendamento (Grupo de Todos os Sistemas Operacionais UNIX, por exemplo);

2.36. No processo de definição da política de composição de senha, a solução deve ser capaz de:

2.36.1. Gerar senhas aleatórias com extensão de 127 (cento e vinte e sete) caracteres ou mais;

2.36.2. Utilizar caracteres alfabéticos (maiúsculos e minúsculos), numéricos e símbolos;

2.36.3. Especificar qual o tipo de caractere na composição das senhas a serem geradas;

2.36.4. Controle de Acesso baseado em Papéis, garantindo aderência ao princípio dos privilégios mínimos, e viabilizando a segregação de funções entre Usuários de uma mesma Aplicação Gerenciada.

2.37. Deve permitir a formação de Grupos de Usuários, Dispositivos ou Identidades, bem como a atribuição de Privilégios de Acesso a esses Grupos, ou grupos abertos definidos a critério do administrador na própria ferramenta.

2.38. Garantir que a senha gerada seja diferente do nome da conta correspondente. Exemplo: se a credencial ou conta tem o nome Administrador a senha gerada jamais pode ser composta da mesma forma;

2.39. Permitir a determinação de quais símbolos estão excluídos ou exclusivamente permitidos na composição da senha;

2.40. Permitir que a senha seja segmentada em partes proporcionais ao número de segmentos definidos na política de segmentação da senha, seja por fracionamento da senha, seja mediante autorização por múltiplos aprovadores;

2.41. Garantir a configuração de mecanismo para que as senhas randomizadas sejam únicas para cada credencial;

2.42. Garantir a configuração de mecanismo para que determinados grupos de senhas randomizadas sejam as mesmas para cada credencial pertencente a este grupo;

2.43. Deve permitir a configuração e definição de fluxos de aprovação (Workflows) para obtenção de acesso às Contas Privilegiadas, com as seguintes características:

2.44. Permitir a configuração de fluxos para aprovação, de acordo com a criticidade e características da conta (como de acesso emergencial, de uso por terceiros), e aprovação de pelo menos um responsável;

2.45. 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;

2.46. Sobre as características da interface Web para acesso de recuperação das senhas, a solução deverá ser capaz de suportar de forma nativa a personalização dinâmica e automática dos acessos atribuídos ao usuário conforme privilégios delegados pelo administrador da solução.

2.47. A interface de administração deverá ser compatível com, no mínimo, os seguintes métodos de autenticação de duplo fator:

2.47.1. Algoritmo de One-time Password (TOTP), compatível com pelo menos um dos seguintes aplicativos autenticadores: Microsoft Authenticator, Google Authenticator, Authy, YubioAth, GAuth Authenticator, Authentication Codes, OATHTool, RSA SecureID, SAASPASS e 1Password;

2.47.2. Tokens em geral;

2.47.3. Smart Cards;

2.48. A solução deve possuir função de monitoramento e análise de comportamento para os sistemas e/ou dispositivos que contemplem, no mínimo, as especificações técnicas do parque computacional da CONTRATANTE.

2.49. Através dos eventos coletados, deve montar perfis de comportamento dos usuários do sistema.

2.50. Deve alertar abusos e comportamentos fora dos padrões aprendidos / mapeados.

2.51. Deve monitorar e exibir acessos e atividades realizadas no próprio sistema.

2.52. Deve detectar pelo menos os seguintes comportamentos anormais:

2.52.1. Acesso realizado fora de um horário predeterminado;

2.52.2. Acessos excessivos a contas privilegiadas;

2.52.3. Máquina ou credencial acessada fora de um horário predeterminado;

2.52.4. Acessos excessivos a uma máquina ou credencial;

2.53. As detecções não devem limitar-se a um tipo específico de comportamento anormal, possibilitando a correta demonstração de eventos complexos. Exemplo: análise de comportamento de usuários.

2.54. Deve fornecer meio de integração nativa e\ou via customizações a pedido do TJPI por meio de componentes API ou SDK da solução para que sistemas de terceiros também possam encerrar sessões suspeitas (ex: SIEM\VCENTER\SQL executa terminação de sessão automaticamente ou chamando a API ou SDK da solução contratada).

2.55. Deve permitir a configuração de eventos críticos a serem reportados automaticamente, baseados, no mínimo, em:

2.55.1. Comandos Linux;

2.55.2. Expressões regulares para comandos, no mínimo, em SSH;

3. QUANTO À ARQUITETURA DA SOLUÇÃO

3.1. Deve prover alta disponibilidade para todas as funcionalidades com opção ativo/passivo ou ativo/ativo, com failover automático para todas as arquiteturas de implantação, utilizando as licenças e a infraestrutura da CONTRATANTE;

3.2. A solução deve ser implantada localmente na sede do TJPI, com modelo de alta disponibilidade, continuidade de negócios e formas de recuperação de desastre.

3.3. A solução deve suportar métodos de alta disponibilidade para TODOS os componentes que fazem parte da solução, a fim de mitigar riscos inerentes à indisponibilidade destes.

3.4. Deverá possuir a capacidade de operação nativa de todas as funcionalidades a partir de nós (servidores) físicos e virtuais, permitindo arranjos do tipo: físico-físico e físico-virtual.

3.4.1. Pelo menos um dos nós da solução deverá ser instalado em host físico, utilizando as licenças e a infraestrutura da CONTRATANTE;

3.4.2. O equipamento físico ofertado pela CONTRATADA deve ser instalado em rack padrão 19 polegadas com dimensão máxima de 3U, acompanhado de trilhos e demais componentes necessários para sua ativação;

3.4.3. O equipamento deve suportar retenção de logs de até 120 (cento e vinte) dias, com gravações na ordem de 6 (seis) horas/dia, 5 dias por semana, NO MÍNIMO;

3.5. A solução não deve utilizar ferramentas de terceiros para completar a solução excetuando-se a camada de sistema operacional e banco de dados;

3.6. Todos os componentes da solução, incluindo seu Banco de Dados, deverão ser manutenidos pela CONTRATADA, sendo esta responsável pela manutenção, atualização e correção destes, durante a vigência contratual;

3.7. O módulo do cofre de senhas, em caso de contingência, poderá ser utilizado plenamente em apenas um nó, seja ele servidor virtual ou físico.

3.8. Não deve haver cobranças à parte no licenciamento de software para opção de ambiente de suporte ativo/passivo ou ativo/ativo ou arranjos de arquitetura; físico-físico e físico-virtual.

3.9. A CONTRATANTE irá prover a seguinte infraestrutura:

3.9.1. Ambiente de virtualização;

3.9.2. Espaço de armazenamento em *storage*;

3.9.3. Camada de comunicação necessária à operação da solução;

3.9.4. Host físico para a instalação descrita no item **3.4.1**;

3.9.5. Sistema Operacional licenciado para atendimento do item **3.4.1**.

3.10. Deve possuir funcionalidade para monitoramento de saúde, com a capacidade de chaveamento automático entre nós no caso de falhas.

3.11. Deve manter sincronização de dados e versões de aplicação entre os dois ou mais nós da solução em alta disponibilidade, sendo gerenciada nativamente pela solução e garantindo a sincronia entre os nós da solução;

3.12. Deve utilizar um banco de dados com as melhores práticas de segurança, em ambiente “hardenizado”, com mecanismo de blindagem e criptografia do sistema operacional e documentação que comprove a contemplação destes requisitos.

3.13. A solução deverá possuir hardening de seus componentes e banco de dados, devendo seguir as melhores práticas de segurança definidas por seus respectivos fabricantes.

3.14. "Hardening" implica em utilização de mecanismos de criptografia, aplicação de correções e atualizações de segurança, remoção de perfis desnecessários, remoção de aplicações/serviços desnecessários, imposição de critérios rígidos de acesso, princípio de mínimo privilégio, dentre outras ações de "endurecimento" para proteger o sistema contra atacantes e ameaças.

3.15. Deve utilizar uma arquitetura de banco de dados e aplicação que permita alta disponibilidade e mecanismos para a recuperação de desastres em todos os componentes da solução.

3.16. A solução deverá ser entregue com a(s) licença(s) de software de banco de dados, com suporte e garantia que compatibilize sua plena operação, bem como, com qualquer outro componente necessário para o seu pleno funcionamento, sem custos adicionais para a CONTRATANTE.

3.17. Deve permitir o backup e restore de seu banco de dados, bem como das configurações de software estabelecidas, com as seguintes capacidades:

3.17.1. Permitir a execução de tarefas de backup e criptografia sem a necessidade de agentes de terceiros ou parada do ambiente ou comprometimento de qualquer funcionalidade; provendo assim o maior nível possível de segurança e integridade dos dados a serem copiados;

3.17.2. Permitir a execução de Backups automatizados, permitindo a programação/agendamento de horários e configuração de locais para seu armazenamento local e remoto;

3.18. Caso a solução faça uso de mecanismos para controle e otimização da carga de trabalho interna, de modo a possibilitar o controle de parâmetros, melhorar ou ajustar o seu desempenho de acordo com as características do ambiente onde está localizado, estes mecanismos deverão ser providos pela solução.

3.19. Deve ser capaz de exportar a chave de criptografia ou credencial equivalente do local de armazenamento das credenciais (cofre), por meio de backup ou método análogo, para ser utilizada nos cenários de recuperação de desastres, de forma a conceder acesso à todas as senhas de identidades privilegiadas e dados gerenciados pela solução.

3.20. O acesso primário (em situação normal) dos usuários à solução deve ser sempre através dos elementos instalados em sua rede local.

4. QUANTO A DESCOBERTA E GERENCIAMENTO DE CREDENCIAIS PRIVILEGIADAS

4.1. Deve ser capaz de descobrir e alterar credenciais Windows, incluindo contas nomeadas, administradores 'built-in' e convidados, exibindo em mapa de rede gráfico e interativo ou através de relatórios e interface de gerenciamento.

4.2. Deve ser capaz de descobrir e alterar credenciais privilegiadas em ambientes Linux e Unix.

4.3. Deve gerenciar credenciais em interfaces de gerenciamento de servidores "out-of-band" ou outros compatíveis com IPMI (Intelligent Plataform Management Interface).

4.4. Deve descobrir e alterar credenciais do Active Directory (AD) e todos os outros serviços de diretório compatíveis com LDAP.

4.5. A solução deve possibilitar a descoberta e alteração de contas privilegiadas usadas em serviços web de forma automática ou através de adaptações via script integrados ao SDK ou API da solução. Ex: aplicações baseadas em Microsoft IIS.

4.6. Deve descobrir e alterar processos interdependentes e credenciais de serviço, incluindo credenciais em ambientes clusterizados.

4.7. Deve ser capaz de redefinir senhas individuais ou grupos de senhas sob demanda, realizando verificações agendadas e automáticas a fim de garantir que as senhas das contas gerenciadas pela solução no dispositivo de destino correspondam às mesmas senhas armazenadas no banco de

dados da solução.

4.8. A solução deve ser capaz de realizar a descoberta, armazenamento e gestão automática de chaves SSH em sistemas Linux.

4.9. No que diz respeito à descoberta automatizada de identidades privilegiadas, a solução deve 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.

4.10. A solução deve ser capaz, caso seja necessário, de substituir as senhas de identidades privilegiadas que estejam sendo utilizadas por determinado serviço em todos os locais onde estejam sendo utilizadas.

4.11. Deve ser capaz de realizar discovery automatizado de credencias em servidores e bancos de dados.

4.12. A descoberta automática de credenciais deve ser realizada por buscas no Active Directory(AD) e/ou por ranges de endereços IP.

5. QUANTO AO GERENCIAMENTO DAS SESSÕES

5.1. Todas as sessões acessadas devem ser gravadas, possibilitando que os vídeos gerados possam ser armazenados em drivers locais de rede ou storage externo.

5.2. As sessões acessadas por usuários poderão ser monitoradas pelo administrador da solução, o qual poderá bloquear e/ou interromper o acesso a qualquer tempo. Caso ocorra o bloqueio e/ou interrupção, estas ações exercidas pelo administrador também deverão ser gravadas.

5.3. Deve permitir a configuração de fluxo de aprovação de acordo com a criticidade e características da conta (como de acesso emergencial ou de terceiros), e aprovação de pelo menos um responsável.

5.4. Deve filtrar comandos executados ao longo das sessões gravadas, possibilitando pesquisar ações específicas nos vídeos gravados.

5.5. A pesquisa textual deve remeter ao momento exato em que o texto ou comando foi realizado no vídeo da gravação da sessão.

5.6. Deve permitir que os comandos executados nas sessões sejam monitorados e gravados em modo texto.

5.7. Deve ser possível colocar a sessão em quarentena ficando pendente de liberação e terminação pelo administrador ou permitir o monitoramento da sessão em tempo real permitindo sua terminação pelo administrador.

5.8. Deve possibilitar assistir o vídeo de uma sessão diretamente na solução, sem a necessidade de converter em formato de vídeo ou realizar download.

6. QUANTO AOS RELATÓRIOS

6.1. Deve controlar o acesso aos relatórios se baseando nas permissões configuradas na solução.

6.2. Deve possibilitar a criação de relatórios que podem ser exportados em formatos editáveis,em pelo menos um dos seguintes formatos: HTML, CSV, XLSX ou XLS.

6.3. A solução deve fornecer dados ad-hoc agendados, relatórios em tempo real dos usuários,contas, configuração da solução e informações sobre os processos da solução.

6.4. A solução deve apresentar relatórios com visibilidade hierárquica, contendo listas e filtros de ordenação de tal forma que os usuários possam detalhar as informações e os recursos que desejam acessar.

6.5. A solução deve fornecer relatórios de auditoria que disponibilizem detalhes das interações dos usuários com a solução, tais como:

6.5.1. Auditoria detalhada, com no mínimo, atividade de login e logoff dos usuários;

6.5.2. Alterações nas funções de delegação;

6.5.3. Adições, deleções, alterações de senhas gerenciadas pela solução;

6.5.4. Operações das senhas dos usuários, incluindo check-in e check-out, solicitações negadas e permitidas;

6.5.5. Os relatórios devem ser filtrados por tempo, tipo de operação, sistema;

6.6. A solução deve fornecer relatórios de conformidade detalhados das operações realizadas pela solução, tais como:

6.6.1. Lista de sistemas e/ou dispositivos gerenciados;

6.6.2. Senhas armazenadas/Contas gerenciadas;

6.6.3. Eventos de alteração de senha;

6.6.4. Nível hierárquico de acesso a ferramenta;

6.6.5. Auditoria de contas gerenciadas e não gerenciadas;

6.6.6. Auditoria de sistemas e/ou dispositivos;

6.6.7. Auditoria de utilização e mudanças na ferramenta;

6.6.8. Programação de atualização de senha:

6.6.9. Atividades de liberação de senhas

7. QUANTO AO(S) MÓDULO(S) PARA DESKTOPS E SERVIDORES

7.1. São requisitos mínimos da gestão de usuários privilegiados para estações de trabalho e servidores:

7.1.1. Permitir a salvaguarda das contas privilegiadas em um único repositório seguro.

7.1.2. Implementar regras para autorização do uso das contas privilegiadas;

7.1.3. Entrega de sessão autenticada, sem que o usuário do domínio tenha contato com a senha real;

7.1.4. Definir o tempo em que o usuário do domínio autorizado poderá usufruir da conta privilegiada.

7.1.5. Registrar as ações realizadas em posse de conta privilegiada e permitir gravação de sessão (gravação de telas) uma vez que fora solicitada a elevação de privilégio;

7.1.6. Permitir o controle impessoal sobre a utilização de recursos privilegiados do ambiente computacional;

7.1.7. Obter o monitoramento das ações de funcionários e terceiros com o uso de credenciais privilegiadas;

7.1.8. Permitir a auditoria de uso de contas privilegiadas no ambiente computacional;

7.1.9. Todas os componentes deste grupo devem ser fornecidos pelo mesmo fabricante, sem dependência de ferramentas de terceiros ou adaptações;

7.1.10. O Gerenciamento de senhas e sessões devem estar conjuntos na mesma solução, sem necessidade de duas interfaces diferentes ou de ser cobrado separadamente para cada função.

7.1.11. Possuir facilidade de acesso rápido e imediato para alteração de senhas de ambientes críticos definidos por grupo de ativos;

7.1.12. Para plataforma Windows possuir a possibilidade de ter um agente local capaz de iniciar aplicações injetando credenciais automaticamente.

7.1.13. Todos os componentes de software da solução deverão constar no catálogo do respectivo fabricante e o seu gerenciamento deve ser feito na mesma console, sem necessidade de infraestrutura adicional;

7.1.14. A solução deve possuir opcional de agentes locais para Windows e Linux que permitam tanto a remoção do privilégio administrativo dos usuários, quanto a elevação de privilégios através de regras pré-definidas;

7.1.15. Possuir mecanismos para fazer a elevação de privilégios de aplicações autorizadas no Windows, a fim de atribuir o direito de administrador somente as tarefas autorizadas para cada tipo de usuário (mesmo que este não tenha direitos de administrador) e implementar a segregação de funções;

7.1.16. Permitir criar regras de privilégios, onde o privilégio de administrador é concedido para cada aplicativo/processo autorizado, de forma que cada usuário, mesmo com o privilégio de usuário convencional (usuário padrão) possa instalar programas permitidos e possa executar os aplicativos legados que requerem o privilégio de administrador para funcionar, como controles ActiveX, e outros;

7.1.17. A solução deve fornecer proteção de grupos de privilégios, o que significa que os usuários não podem adulterar ou modificar grupos privilegiados locais, como o grupo Administradores ou Power Users.

7.1.18. A solução deve automaticamente permitir os aplicativos de lista branca implantados por ferramentas de implantação de software por administradores confiáveis, incluindo o SCCM (Microsoft System Center Configuration Manager).

7.1.19. A solução deve permitir criar uma lista de aplicativos permitidos (white list), onde seja possível configurar todos os aplicativos que podem ser executados e qualquer outra aplicação fora desta lista seja bloqueada automaticamente.

7.1.20. Permitir integração com interface do Windows da estação de trabalho, onde o usuário possa requerer privilégio sob demanda, utilizando o botão direito do mouse, para executar uma aplicação;

7.1.21. Possuir uma integração com Windows UAC (User Account Control), e conter relatórios do uso de prompts aos usuários feitos pelo UAC;

7.1.22. Possuir relatórios de aplicações e eventos de usuários. Estes relatórios devem estar centralizados na mesma console de relatórios do sistema de gerenciamento seguro;

8. QUANTO AO PLANO DE IMPLANTAÇÃO DA SOLUÇÃO

8.1. A CONTRATADA deverá apresentar Plano de Implantação da Solução, em até 15 (quinze) dias corridos da assinatura do contrato, detalhando os aspectos da implantação da solução compreendendo a instalação e configuração de todos os seus componentes, incluindo, no mínimo:

8.1.1. Detalhamento do Escopo.

8.1.2. Descrição de atividades em cada etapa do projeto.

8.1.3. Cronograma de atividades.

8.1.4. Definição de responsabilidades.

8.1.5. Pontos de controle.

8.1.6. Descrição detalhada dos componentes.

8.1.7. Documentação a ser entregue, incluindo todos os detalhes das instalações a serem realizadas, devendo apresentar informações para procedimentos, incluindo comandos e testes aplicáveis, procedimentos de inicialização e procedimentos de configuração.

8.1.8. Requisitos necessários.

8.2. O Plano de Implantação da Solução deverá atender aos requisitos técnicos e de infraestrutura do CONTRATANTE e estar em conformidade com as recomendações do fabricante da solução de PAM.

8.3. O cronograma deverá contar o prazo em dias corridos para a execução dos serviços e atividades projetadas.

8.4. O plano poderá ter propostas de alteração do CONTRATANTE, devendo ser executado somente após a aprovação deste.

9. QUANTO A ENTREGA E AO SERVIÇO DE INSTALAÇÃO E CONFIGURAÇÃO DA SOLUÇÃO

9.1. A entrega da solução e o serviço de instalação e configuração deverão ser prestados deverão ser prestados na Secretaria de Tecnologia da Informação (STIC) do Tribunal de Justiça do Estado do Piauí (CONTRATANTE), localizado na Pça. Des. Edgard Nogueira s/n, Centro Cívico, CEP 64000-830 - Teresina-PI. Telefone: (86) 3215-1120 / (86) 3215-7419.

9.2. Todos os componentes, sejam de softwares e hardwares, deverão ser entregues em dias úteis, na Secretaria de Tecnologia da Informação (STIC) do Tribunal de Justiça do Estado do Piauí (CONTRATANTE), localizado na Pça. Des. Edgard Nogueira s/n, Centro Cívico, CEP 64000-830 - Teresina-PI. Telefone: (86) 3215-1120 / (86) 3215-7419.

9.3. O serviço de instalação e configuração da solução de PAM deverá ser realizada em conformidade com o Plano de Implantação aprovado.

9.4. A implantação contemplará a instalação e configuração da solução de PAM, no ambiente computacional do TJPI, por meio de técnicos comprovadamente especializados na solução, designados para esta atividade.

9.5. A Implantação da solução deverá atender todos os requisitos da especificação técnica, recomendações do fabricante, e incluir, no mínimo:

9.5.1. Instalação e configuração do ambiente tecnológico e operacional considerando também o(s) appliance(s) virtual(is) e físico(s) componentes da solução ofertada pela CONTRATADA, em local a ser definido pela CONTRATANTE;

9.5.2. Configuração da ferramenta em alta disponibilidade, em modo de operação ativo/ativo ou ativo/passivo;

9.5.3. Migração da estrutura existente para a solução ofertada pela CONTRATADA;

9.5.4. Adição dos dispositivos a serem monitorados;

9.5.5. Adição das credenciais a serem gerenciadas;

9.5.6. Configuração dos perfis de acesso conforme instruído pela CONTRATANTE;

9.5.7. Implementação das configurações necessárias para o gerenciamento das contas de serviços, conforme instruído pela CONTRATANTE;

9.5.8. Implementação das configurações necessárias para automação do processo de autenticação de contas administrativas, conforme instruído pela CONTRATANTE;

9.5.9. Instalação dos clientes para gerenciamento de privilégio nas Estações de Trabalho, se aplicável, conforme instruído pela CONTRATANTE.

9.6. Até o final da implantação, a CONTRATADA deverá comprovar o registro das licenças fornecidas em conta específica do TJPI, no sítio de Internet do fabricante, encaminhando documento comprobatório do registro ao gestor do contrato. A utilização de licenças "trial", com todas as funcionalidades habilitadas, só será aceita até o final da implantação.

10. QUANTO AO SUPORTE TÉCNICO ESPECIALIZADO

10.1. Os serviços de suporte técnico mensal deverão ser prestados na Secretaria de Tecnologia da Informação (STIC) do Tribunal de Justiça do Estado do Piauí (CONTRATANTE), localizado na Pça. Des. Edgard Nogueira s/n, Centro Cívico, CEP 64000-830 - Teresina-PI, ou remotamente, se o caso assim o permitir, a critério da CONTRATANTE.

10.2. Realizar a manutenção evolutiva dos softwares da solução, fornecendo, instalando e configurando as novas versões e/ou releases e atualizações lançadas durante a vigência contratual, mantendo-os funcionais e compatíveis com o ambiente utilizado pelo TJPI.

10.2.1. Garantir o funcionamento do ambiente com relação à solução instalada pela CONTRATADA, incluindo todos os serviços, configurações e fornecimento de "fixes" e "releases", durante toda a vigência do contrato.

10.3. Executar, durante o período de vigência do contrato, o suporte preventivo e corretivo da solução objeto do contrato, para as seguintes atividades:

10.3.1. Parametrização e auditoria técnica de disponibilidade e funcionamento da solução;

10.3.2. Manutenção e suporte a todo o ambiente de software básico da solução, atuando em casos de incidentes escalonados pela equipe técnica do CONTRATANTE, mediante identificação da causa raiz do problema, definição e implantação da solução de contorno para garantir o nível de disponibilidade do ambiente, e aplicação da solução definitiva;

10.3.3. Promover o escalonamento dos incidentes e problemas graves ou de solução que demore mais tempo que o previsto contratualmente ao suporte especializado do fabricante, para rápida normalização do ambiente;

10.3.4. Relatar e implementar melhorias, atualizações e ajustes finos para aprimorar a solução de proteção de dados.

10.3.4.1. As implementações deverão ser fruto de análise das atualizações e correções disponibilizadas pelo fabricante, da análise do ambiente e do conjunto de melhores práticas para o ambiente;

10.3.4.2. As implementações deverão ser planejadas, detalhadas em atividades, com análise dos riscos e impacto no ambiente e de indicação de benefícios para sua execução.

10.3.5. Ações de aperfeiçoamento de funcionalidade, disponibilidade e configuração dos produtos da solução;

10.3.6. Execução de procedimentos de instalação em conformidade com as recomendações do fabricante, documentações existentes e as boas práticas de mercado;

10.3.7. Execução dos procedimentos descritos na documentação e proposições para a melhoria contínua desses procedimentos;

10.3.8. Suporte, configuração, customização, parametrização e implantação de sistemas auxiliares, visando manter a disponibilidade e o desempenho da solução;

10.3.9. Análise e proposição de soluções adequadas para o ambiente contratado, sob orientação da equipe técnica do CONTRATANTE;

10.3.10. Detecção, análise e resolução dos problemas de funcionalidade, configuração e parametrização, atuando preventivamente para evitar ocorrência de incidentes, identificação de pontos de falhas, análise de potenciais de riscos da infraestrutura de backup e identificação de tendências

de capacidade e disponibilidade do ambiente de backup;

10.3.11. Análise de "logs" e registros dos equipamentos, ferramentas e softwares envolvidos na solução, com anotações e geração de relatórios estatísticos.

10.3.12. Geração de relatórios de ocorrências para todas as falhas de serviços classificados pelo CONTRATANTE como críticos, com informações de causa e efeito, providências e correções aplicadas e recomendações sobre as lições aprendidas;

10.4. Realizar manutenção preventiva programada, que se destina a prevenir indisponibilidades e/ou falhas dos componentes da solução contratada, seus subsistemas e componentes envolvidos, mantendo-as em perfeito estado de funcionamento e conservação, conforme especificado em projeto, manuais e normas técnicas específicas.

10.4.1. O suporte preventivo deverá ser realizado mediante visita mensal da contratada, ou remotamente, se o caso assim o permitir, a critério da CONTRATANTE, visando analisar desempenho e funcionalidades da solução, emitindo relatório mensal de serviços e resultados, com as sugestões de melhoria possíveis, visando garantir melhor performance da solução de PAM.

10.5. Realizar manutenção corretiva, que compreende providências para reparar e corrigir os componentes da solução contratada deixando-a em seu pleno estado de funcionamento, removendo definitivamente os defeitos eventualmente apresentados.

10.6. Acompanhar mensalmente a qualidade e os níveis de serviços alcançados com vistas a efetuar eventuais ajustes e correções de rumo.

10.7. Manter canal de comunicação aberto diretamente com o fabricante para, a critério do TJPI, promover o escalonamento dos incidentes e problemas graves ao suporte especializado do fabricante, para rápida normalização do ambiente, sem ônus ao Tribunal;

10.8. Executar as atividades previstas no edital e seus anexos, de acordo com os procedimentos e prazos previstos;

11. QUANTO A QUALIFICAÇÃO TÉCNICA DOS PROFISSIONAIS

11.1. A CONTRATANTE, a qualquer momento, poderá requerer à CONTRATADA a apresentação de documentos necessários para a comprovação da qualificação técnica dos profissionais;

11.2. Será necessário a comprovação de experiência profissional da equipe que projetará, implementará e implantará a Solução de Tecnologia da Informação, que definem a natureza da experiência profissional exigida e as respectivas formas de comprovação dessa experiência, dentre outros. A comprovação se dará por meio de documento que comprove a participação do profissional em outros projetos da mesma natureza e de porte equivalente ao definido no Atestado de Capacidade Técnica, devendo o(s) documento(s) conter o nome, endereço, telefone dos atestadores, ou por meio de certificado fornecido pelo fabricante da solução indicando a participação do técnico em curso oficial da solução. Tal exigência tem por objetivo mitigar falhas na execução do projeto, bem como tornar sua implementação mais ágil.

12. QUANTO AOS TREINAMENTOS NA SOLUÇÃO

12.1. Os treinamentos deverão ser prestados no Tribunal de Justiça do Estado do Piauí, localizado na Pça. Des. Edgard Nogueira s/n, Centro Cívico, CEP 64000-830 - Teresina-PI, ou na EJUD - Escola Judiciária do Piauí, localizada na Rua Professor Joca Vieira, 1449 - Fátima, CEP 64049-514, Teresina - PI, ou remotamente, na modalidade EAD, "ao vivo", em dias úteis, em língua portuguesa. Não serão aceitos cursos gravados;

12.2. Todos os custos envolvidos em locomoção, coffee-break, material didático e demais materiais serão de responsabilidade da CONTRATADA.

12.3. Todo o material didático utilizado deve estar em língua inglesa ou em português do Brasil, e ser entregue a todos os participantes de forma digital;

12.4. Os equipamentos e ambiente utilizados no treinamento são de responsabilidade da CONTRATADA, podendo ser acordado em casos especiais a infraestrutura física do Tribunal de Justiça do Estado do Piauí;

12.4.1. Caso ocorra à distância, na modalidade EAD, toda a infraestrutura de transmissão remota do treinamento, será de responsabilidade da CONTRATADA.

12.5. Os treinamentos deverão ocorrer da seguinte forma:

12.5.1. Um treinamento oficial do fabricante para Administração da Solução, em turma única, de no mínimo 04 (quatro) pessoas, cobrindo todas as funcionalidades da ferramenta, englobando, mas não se limitando, nos seguintes tópicos:

12.5.1.1. Visão geral da solução (Introdução à solução, topologia, arquitetura física, opções de configuração e de gerência);

12.5.1.2. Instalação, configuração, integração com ferramentas e sistemas, administração e monitoramento;

12.5.1.3. Alertas, eventos, agendamentos, atualizações e *troubleshooting*;

12.5.1.4. Geração de relatórios;

12.5.2. Um treinamento oficial do fabricante para Operação da Solução, em turma única, de no mínimo 10 (dez) pessoas, englobando, mas não se limitando, nos seguintes tópicos:

12.5.2.1. Visão geral da solução (Introdução à solução, topologia, opções de configuração e de gerência);

12.5.2.2. Integração com ferramentas e sistemas e monitoramento;

12.5.2.3. Alertas, eventos, agendamentos;

12.5.2.4. Geração de relatórios;

12.6. Os treinamentos deverão ter carga horária mínima de 20 (vinte) horas aula cada.

12.7. O instrutor deverá ser certificado na solução.

12.8. Ao final do treinamento devem ser entregues os certificados de conclusão para cada participante, contendo nome do curso, nome do instrutor com a respectiva assinatura, nome do aluno, data de início, data de término e carga horária total.

ANEXO I

(Infrações, graus, multas e penalidades)

Item	Infração	Grau	Multa
1	Descumprimento de quaisquer outras obrigações contratuais, não explicitadas nos demais itens, que sejam consideradas leves.	1	Moratória
2	Não entrega de documentação simples solicitada pela CONTRATANTE.	1	Moratória
3	Atraso parcialmente justificado na entrega até 30 dias.	1	Moratória
4	Atraso parcialmente justificado na entrega acima de 30 dias até 60 dias.	2	Moratória
5	Atraso parcialmente justificado ou injustificado na entrega acima de 60 dias.	2	Compensatória
6	Descumprimento de outros prazos, previstos do TR.	2	Moratória
7	Erros de execução do objeto.	3	Moratória
8	Desatendimento às solicitações da CONTRATANTE.	3	Moratória
9	Descumprimento de quaisquer outras obrigações contratuais, não explicitadas nos demais anteriores, que seriam consideradas médias.	3	Moratória
10	Execução imperfeita do objeto.	3	Moratória
11	Não manutenção das condições de habilitação e de licitar e contratar com a Administração Pública durante a vigência contratual.	4	Compensatória
12	Não entrega de documentação importante solicitada pela CONTRATANTE.	4	Compensatória
13	Descumprimento de quaisquer outras obrigações contratuais, não explicitadas nos demais itens, que seriam consideradas graves.	4	Compensatória
14	Inexecução parcial do Contrato.	4	Compensatória
15	Descumprimento da legislação (legais e infralegais) afeta à execução do objeto (direta ou indireta).	5	Compensatória
16	Cometimento de atos protelatórios durante a execução visando adiamento dos prazos contratados.	5	Compensatória
17	Inexecução total do Contrato.	5	Compensatória

Grau	Advertência - 1ª Ocorrência	Mora moratória Valor Mensal	Multa Compensatória	Impedimento Prazo
1	Sim	Não	Não	Não
2	Não	1% a 4,9% por ocorrência ou contrato	1,5% a 4,9% por ocorrência ou contrato	Mínimo: 1 mês Máximo: 2 anos
3	Não	5% a 8,9% por ocorrência ou contrato	8,0% a 14,9% por ocorrência ou contrato	Mínimo: 6 meses Máximo: 3 anos
4	Não	9% a 11,9% por ocorrência ou contrato	15,0% a 24,9% por ocorrência ou contrato	Mínimo: 3 anos Máximo: 5 anos
5	Não	12% a 15% por ocorrência ou contrato	25% a 30% por ocorrência ou contrato	Mínimo: 4 anos Máximo: 5 anos

ANEXO II

MODELO DE PROPOSTA DE PREÇOS

GRUPO	ITEM	DESCRIÇÃO	UN.	QUANTIDADE	VALOR UNITÁRIO	VALOR TOTAL
1	1	Licenciamento de uso para solução de Gerenciamento de Acessos Privilegiados *(Privileged Access Management - PAM),* com garantia de 36 meses	Unidade	1		
	2	Serviço de Instalação e Configuração da Solução de Gerenciamento de Acessos Privilegiados *(Privileged Access Management - PAM)*	Serviço	1		
	3	Treinamento de Administração da Solução	Serviço	1		
	4	Treinamento de Operação da Solução	Serviço	1		
	5	Suporte Técnico especializado	Mês	36		
TOTAL DA PROPOSTA						

ANEXO III

MODELO DE DOCUMENTO COM AS COMPROVAÇÕES DAS ESPECIFICAÇÕES TÉCNICAS EXIGIDAS NO EDITAL

Item do Edital	Item de Comprovação
Item de referência do edital	Especificação clara, completa e minuciosa do produto cotado, informando a marca, o modelo e o fabricante, bem como a indicação precisa da comprovação de cada característica constante nas especificações técnicas deste Termo de Referência, pontuando em forma de planilha cada exigência do edital com sua respectiva comprovação, que deve conter uma ou mais das seguintes: • Indicação da página/item do manual/datasheet; • URL; • Seção/subseção ou número de item de página WEB; • Print de tela da solução; • Imagem ou vídeo que demonstre a funcionalidade; • Outra comprovação, desde que seja oficial do fabricante do produto ofertado.
...	...
...	...

Documento assinado eletronicamente por **Giovanny Lima de Castro**, **Analista de Sistemas / Desenvolvimento**, em 19/11/2021, às 11:49, conforme art. 1º, III, "b", da Lei 11.419/2006.

Documento assinado eletronicamente por **Fabiano Galeno da Costa Pereira**, **Analista de Sistemas / Desenvolvimento**, em 19/11/2021, às 11:50, conforme art. 1º, III, "b", da Lei 11.419/2006.

Documento assinado eletronicamente por **Natanael Henrique Corrêa**, **Técnico em Informática**, em 19/11/2021, às 11:53, conforme art. 1º, III, "b", da Lei 11.419/2006.

A autenticidade do documento pode ser conferida no site http://sei.tjpi.jus.br/verificar.php informando o código verificador **2641675** e o código CRC **66F27570**.