TERMO DE REFERÊNCIA

Aquisição de Solução de Gerenciamento de Acessos Privilegiados (Privileged Access Management – PAM) e Monitoramento e Análise Comportamental, com possibilidade de proteção, monitoramento, detecção e resposta a atividade de credencial privilegiada, armazenamento de senhas e mitigação de riscos através de gestão de identidade, com serviço de implantação e treinamento *hands on.*

PROCESSO ADMINISTRATIVO PA-PRO-2021/02824

1. DO OBJETO

Esta contratação tem como objeto **Registro de Preço** para **Solução de Proteção e Auditoria do Uso de Credenciais – Monitoramento Comportamental e Repositório Seguro**, com possibilidade de proteção, monitoramento e alerta baseado em análise comportamental, detecção e resposta a atividade de conta privilegiada, armazenamento de senhas e mitigação de riscos.

2. DA FUNDAMENTAÇÃO

2.1. Da motivação

Os recentes ataques cibernéticos perpetrado contra o Poder Judiciário, em especial o ocorrido contra o Superior Tribunal de Justiça (STJ), divulgado em 03 de novembro de 2020, chamaram a atenção dos responsáveis pelas instituições ligadas à Justiça e elevaram, como nunca, o grau de alerta do Conselho Nacional de Justiça (CNJ) e dos demais Tribunais para a questão da Segurança Cibernética como requisito fundamental para a continuidade da prestação jurisdicional no Brasil.

Após investigações conduzidas sobre o ataque ao STJ, foi identificado que a técnica de invasão consistiu primeiramente na obtenção de credenciais simples de usuários de rede, para, em seguida, através de uma técnica conhecido como “escalação de privilégios”, ganhar o controle de credenciais de mais alto nível gerencial na rede da vítima. De posse de uma dessas credenciais com poderes administrativos, o atacante efetua a criptografia dos dados armazenados nos servidores da rede. Este tipo de ataque é conhecido como “ransomware”, através do qual valores pecuniários são exigidos em troca da liberação (descriptografia) dos dados sequestrados e indisponíveis. Em síntese o atacante obtém, por meios ilícitos, acesso a alguma credencial de alto poder administrativo da rede da instituição, realizando, em seguida, ações criminosas.

É absolutamente recomendável que tais vulnerabilidades sejam corrigidas o quanto antes. Entretanto, muito frequentemente, é impraticável ou impossível corrigir tais vulnerabilidades, restando apenas a alternativa da adoção de soluções de contorno, como é o caso das soluções de **Gestão de Acessos Privilegiados** ou, na sua terminologia original na língua inglesa, *Privileged Access Management* (PAM).

As soluções que compõem essa classe de aplicativos têm por incumbência gerir, de forma mais segura, o armazenamento de credenciais (nome de usuário e senha, certificados digitais etc.), tomando para si a responsabilidade de intermediar o uso dessas credenciais entre os usuários propriamente ditos (humanos ou outros programas) e as aplicações ou sistemas de autenticação. Além disso, algumas das soluções neste campo são dotadas de “inteligência computacional” capaz de identificar tentativas espúrias de acesso às credenciais com base em regras definidas pelos administradores ou no comportamento temporal dos usuários proprietários da credencial protegida.

Em 07 de junho de 2021, o Conselho Nacional de Justiça publicou a Resolução nº 396 a qual instituiu a Estratégia Nacional de Segurança Cibernética do Poder Judiciário (ENSEC-PJ). Este documento, de caráter cogente para todos os Tribunais nacionais, visa garantir a segurança cibernética do ecossistema digital do Poder Judiciário brasileiro. Entre outras medidas, a

Resolução nº 396/CNJ torna obrigatórias, entre outras medidas ligadas à segurança cibernética, ações dos Tribunais no sentido de garantir:

- segurança física e proteção de ativos de tecnologia da informação de forma geral;
- ações destinadas a assegurar a disponibilidade, a integridade, a confidencialidade e a autenticidade de dados e de informações;
- ações destinadas a assegurar o funcionamento dos processos de trabalho, continuidade operacional e a continuidade das atividades fim e administrativas dos órgãos do Poder Judiciário;
- ações de planejamento, de sistematização e de normatização sobre temas atinentes à segurança cibernética.

A contratação, alvo deste instrumento de oficialização de demanda, tem por objetivo exatamente a aquisição de recurso tecnológico capaz compor solução de segurança que se destina a atender os objetivos expressos e comandados pelo CNJ aos Tribunais através do ENSEC-PJ.

2.2. Dos objetivos a serem alcançados por meio da contratação

2.2.1. Dotar o Poder Judiciário do Pará de infraestrutura tecnológica capaz de fornecer segurança e proteção lógica aos equipamentos de processamento e armazenamento de dados situados no Data Center e nas demais estações e ativos de trabalho que compõem a rede de computadores do Tribunal.

2.2.2. Permitir o funcionamento contínuo dos serviços de tecnologia da informação, imprescindíveis ao cumprimento da função institucional, evitando indisponibilidade, reduções no desempenho, paradas não programadas ou perdas de informações.

2.2.3. Promover o aumento da credibilidade dos colaboradores e jurisdicionados do quanto à utilização dos recursos de tecnologia da informação e comunicação, qualificados como solução estável e confiável.

2.2.4. Permitir a gravação, registro, monitoramento, análise comportamental, controle e auditoria das ações realizadas pelos usuários, administradores, servidores e ativos de tecnologia com acessos privilegiados, a fim de promover e melhorar a produtividade, governança, segurança, auditoria e conformidade das mudanças realizadas no ambiente tecnológico do TJPA.

2.3. Dos benefícios diretos e indiretos resultantes da contratação

2.3.1. Dentre os benefícios destaca-se a redução do risco de vazamento de informações da justiça, dos magistrados, servidores e jurisdicionados; garantia da continuidade do negócio do TJPA; além da própria imagem institucional.

2.3.2. Uma solução em gerenciamento de acesso privilegiado permite o gerenciamento de usuários privilegiados de forma segura e automatizada, provendo auditoria, controle sobre as identidades privilegiadas, fluxo de trabalho, administração centralizada, automação de processo e aplicação de políticas de segurança.

2.3.3. Além disso, oferece funcionalidades relacionadas ao registro, gravação de sessão e auditoria de todas as operações realizadas com acessos privilegiados em servidores e demais ativos de tecnologia do ambiente computacional do Tribunal.

2.3.4. Além dos benefícios imediatos sentidos pela equipe de tecnologia: aumento de produtividade, governança e conformidade; redução do número de usuários e acessos privilegiados; administração centralizada e políticas de senhas automatizadas customizáveis.

2.4. Do alinhamento entre a demanda e os instrumentos de planejamento do TJPA

A contratação está alinhada ao **Plano de Gestão 2021-2023 do TJPA**.

- **Macrodesafio 12**: Fortalecimento da Estratégia Nacional de TIC e Proteção de Dados;

Da mesma forma, a contratação está alinhada com o Planejamento Estratégico 2021-2026.

- **Macrodesafio 12**: Fortalecimento da Estratégia Nacional de TIC e Proteção de Dados;

A contratação também foi prevista no **Plano de Contratações** no item:

- **Contratação de serviço de PAM** - *Privileged Access Management*, incluindo acompanhamento operacional.

Esta aquisição também está alinhada com a **Resolução 370/2021** do Conselho Nacional de Justiça (CNJ), que institui a Estratégia Nacional de Tecnologia da Informação e Comunicação do Poder Judiciário (**ENTIC-JUD**) para o sexênio 2021-2026:

- **Seção III**, que trata dos riscos, da segurança da informação e da proteção de dados.
- **Art. 38** - Cada órgão deverá elaborar e aplicar práticas e processos de segurança da informação e proteção de dados a serem adotadas na instituição, conforme disposto na Lei nº 13.709/2018 que dispõe sobre a Proteção de Dados Pessoais.

2.5. Da referência aos Estudos Preliminares

Os estudos preliminares foram protocolados no sistema SigaDoc através do PA-PRO-2021/02824.

2.6. Da relação entre a demanda prevista e a quantidade de bens e/ou serviços a serem contratados

Esta contratação se destina, fundamentalmente, a prover segurança para os servidores físicos, virtuais e às estações de trabalho, no gerenciamento, monitoramento e auditoria do acesso privilegiado às informações e ativos do TJPA.

E ainda ampliar a segurança das informações produzidas no ambiente do Poder Judiciário do Pará e otimizar o tempo de operações realizadas no gerenciamento de acesso privilegiado.

Entende-se que as demandas previstas e projetadas pela Secretaria de Informática do TJPA a serem atendidas pela contratação da solução de *Gerenciamento de Acessos Privilegiados (Privileged Access Management – PAM)*, serão cobertas em sua plenitude, durante o período de vigência de 30 meses, através do contrato estabelecido entre o CONTRATANTE e a CONTRATADA, que abaixo estão elas listadas:

Item	Descrição	QTD
1	SOLUÇÃO DE PROTEÇÃO E AUDITORIA DO USO DE CREDENCIAIS – Monitoramento Comportamental e Repositório Seguro, com o serviço de implantação e garantia dos equipamentos e softwares pelo período de 30 meses – SOFTWARE.	01 und.
2	SOLUÇÃO DE PROTEÇÃO E AUDITORIA DO USO DE CREDENCIAIS – Proteção Local para SERVIDORES Windows / Linux, com o serviço de implantação e garantia dos equipamentos e softwares pelo período de 30 meses – SOFTWARE.	184 und.
3	SOLUÇÃO DE PROTEÇÃO E AUDITORIA DO USO DE CREDENCIAIS – Proteção Local para ESTAÇÕES DE TRABALHO, com o serviço de implantação e garantia dos equipamentos e softwares pelo período de 30 meses – SOFTWARE.	500 und.
4	SUPORTE TÉCNICO especializado mensal, provido pela própria empresa vencedora.	30 meses
5	TREINAMENTO TÉCNICO da solução de proteção e auditoria para integrantes da Coordenadoria de Suporte Técnico, com certificação do fabricante. O treinamento será ministrado exclusivamente para aqueles que atuarão diretamente na operação da solução pretendida. O treinamento deverá ser voltado, tão somente, para o objeto que será mantido em funcionamento no TJPA – SOFTWARE.	05 vagas

2.7. Da análise de mercado de TIC

A presente contratação visa a aquisição de solução de gerenciamento de acessos privilegiados (*PAM – Privileged Access Management*), com diversas funcionalidades tais como análise comportamental, auditoria de credenciais, mitigações contra roubos e abusos de privilégios e aplicação do "privilégio mínimo" nos ativos protegidos, tudo isso com a finalidade de aumentar a proteção das credenciais utilizadas no âmbito do Tribunal e impedir que essas credenciais sejam usadas por agentes potenciais atacantes, prevenindo danos decorrentes de ataques cibernéticos que possam ser realizadas conta o tribunal. Cumpre destacar que, atualmente, o poder judiciário estadual não possui ferramenta específica de proteção supramencionada e, conforme detalhamento do potencial da solução, busca a aquisição da plataforma que apresentar melhor custo-benefício, em qualidade e preço a ser pago.

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

Figura 1 - Quadrante mágico do Gartner para soluções PAM, de julho de 2021.

O Gartner realiza a mensuração da qualidade e relevância de soluções de TI através de um gráfico que ficou conhecido como "**Quadrante**", o qual reflete os estudos publicados anualmente sobre categorias de produtos e serviços, cuja composição utiliza diversos critérios para medir a qualidade das soluções oferecidas pelas empresas que atuam naquela categoria. Como o TJPA preza pela qualidade das soluções adquiridas para compor sua infraestrutura tecnológica, as soluções consideradas foram as que se estavam mais bem posicionadas no quadrante "*Leaders*" (líderes) da avaliação mais recente, publicada em julho de 2021. Os fabricantes mais bem localizados neste quadrante foram avaliados com os melhores resultados em suas soluções oferecidas.

Ao que podemos verificar no quadrante do Gartner, os dois fabricantes que estão melhor posicionados são a **CyberArk** e a **BeyondTrust**, cumprindo lembrar que o Tribunal ainda não possui qualquer solução de gerenciamento de acessos privilegiados.

Dado que o objeto da contratação é um elemento essencial para a construção de um ecossistema de segurança da informação no âmbito do TJPA, tendo sido observado a sua contribuição na garantia da segurança da informação no âmbito da administração pública municipal, estadual e federal, com diversos órgãos dos mais variados tamanhos e com a mais diversas funções o possuindo em sua infraestrutura de TI.

As contratações mencionadas abaixo, guardadas as peculiaridades de cada órgão, são similares ao objeto que o TJPA pretende adquirir:

1. Destaca-se a solução contratada pelo **Tribunal Regional do Trabalho da 8ª Região (TRT8)** que, através da **Ata de Registro de Preço (ARP) nº 16/2020** gerada **no Pregão Eletrônico 34/2020**, registrou preços para o objeto:

   "aquisição de Solução de Gerenciamento de Acesso Privilegiado (*Privileged Access Management* – PAM) e Monitoramento e Análise Comportamental, com possibilidade de proteção, monitoramento, detecção e resposta a atividade de conta privilegiada, armazenamento de senhas e mitigação de riscos".

2. A solução contratada pela **FUNDAÇÃO UNIVERSIDADE FEDERAL do AMAPÁ – UNIFAP** através da **ATA DE REGISTRO DE PREÇO Nº 001/2021**, referentes ao **Processo Administrativo n° 23125.019144/2020-67**:

   "aquisição de Solução de Segurança da Informação para Sistemas Críticos, conforme condições, quantidades e exigências estabelecidas neste instrumento, especificado(s) no(s) item(ns) 01 a 09 do Termo de Referência".

3. O **Tribunal de Justiça do Distrito Federal e Territórios (TJDFT)**, através do **item 1 do contrato 250/2019**, gerado através do **Pregão Eletrônico 065/2019**, adquiriu solução similar ao objeto de contratação do TJPA. cujo objeto é a:

   "a aquisição, suporte e atualização de solução de segurança da informação para a gestão de acessos privilegiados, armazenamento de credenciais, que possibilite o isolamento, gravação e o monitoramento de sessões de ativos de TIC do CONTRATANTE por um período de até 36 (trinta e seis) meses, incluindo serviço de instalação e repasse de conhecimento".

4. A **Secretaria de Fazenda do Estado de Santa Catarina (SEFAZ-SC)** que, através do **Pregão Eletrônico 0024/2020**, registrou preços para o objeto:

   "Contratação de empresa especializada objetivando o fornecimento de solução de segurança integrada em ambientes críticos, incluindo serviços de implantação da solução, repasse de conhecimento, garantia e suporte".

5. A **Empresa de Tecnologia e Informações da Previdência Social (DATAPREV)** que, através da **Ata de Registro de Preço (ARP) nº 420/2015**, gerada através do **Pregão Eletrônico 420/2015**, registrou preços para o objeto:

   "Aquisição de Solução de Cofre de Senhas, com garantia de 60 (sessenta) meses, para instalação nos Centros de Processamento no Rio de Janeiro (CPRJ), São Paulo (CPSP) e Brasília (CPDF), incluindo a prestação dos serviços de 2.000 (duas mil) horas de Orientação Técnica e Capacitação Técnica Formal a serem utilizadas sob demanda".

De acordo com o **item 1.7** e devido à urgência na contratação, além de ter sido verificado que a solução atende às necessidades do TJPA com qualidade e economicidade para os cofres públicos, **optou-se por aderir aos itens 01, 03, 04, 05 e 06 da Ata de Registro de Preço (ARP) nº 16/2020 gerada no Pregão Eletrônico 34/2020, realizado pelo TRT8**.

2.8. Da natureza do objeto

O objeto a ser contratado possui características comuns e usuais encontradas atualmente no mercado de Tecnologia de Informação, cujos padrões de desempenho e de qualidade podem ser objetivamente definidos neste Termo de Referência.

2.9. Do parcelamento do objeto

2.9.1. Visando atingir o maior número de interessados em participar da licitação sem prejudicar a compatibilidade técnica dos itens que compõem a solução de TI, optou-se pela divisão dos produtos a serem licitados neste certame em 01 (um) lote com 05 (cinco) itens, sempre em respeito à ampla competitividade e conforme previsto no artigo 23, § 1º da Lei 8666/93 e Súmula 247 do TCU.

2.9.2. A divisão em itens considerou a diferenciação das características técnicas dos produtos a serem adquiridos, porém agrupando em lote para não incorrer na perda de economia de escala, de produtividade e incompatibilidade técnica entre os itens.

2.9.3. Para efeito de adjudicação do objeto, será considerado o MENOR PREÇO GLOBAL POR LOTE, vez que todos os itens a serem fornecidos são componentes de uma única solução de TI, a qual não poderá ser desmembrada sem que haja perda de compatibilidade entre os itens do lote, de produtividade e de economia de escala.

2.10. Da seleção do fornecedor

Os itens a seguir estão estabelecidos de acordo com os princípios da legalidade, razoabilidade e competitividade.

2.10.1. Da forma e do critério de seleção

Caberá à Administração Pública realizar a aquisição do objeto com a empresa detentora da ARP (Ata de Registro de Preço) Nº 016/2020, referentes ao Pregão Eletrônico Nº 034/2020 – Processo TRT8 nº 3306/2020, realizado pelo Tribunal Regional do Trabalho da 8ª Região (TRT8).

2.10.2. Da modalidade e do tipo de licitação

A aquisição da solução de Gerenciamento de Acessos Privilegiados (*Privileged Access Management – PAM*) será realizada através de adesão a ARP (Ata de Registro de Preço) Nº 016/2020, referentes ao Pregão Eletrônico Nº 034/2020 – Processo TRT8 nº 3306/2020, realizado pelo Tribunal Regional do Trabalho da 8ª Região (TRT8), devido a ata ter se mostrado vantajosa do ponto de vista financeiro e atender, de forma objetiva, as necessidades do TJPA, no que diz respeito ao objeto da contratação.

2.10.3. Dos critérios técnicos de habilitação obrigatórios

A. Comprovação de aptidão para desempenho de atividade pertinente e compatível com o objeto deste Pregão, mediante atestado(s) ou declaração(ões) de Capacidade Técnica, expedido(s) por pessoa jurídica de direito público ou privado comprovando que a licitante prestou ou está prestando serviços objeto deste edital, conforme transcrição abaixo:

   i. Atestado de Capacidade Técnica, para fins de comprovação da capacidade técnica, fornecido por pessoa jurídica de direito público ou privado, declarando ter a empresa realizado ou estar realizando o fornecimento do objeto, compatível em características, quantidades e prazos com o objeto deste Termo de Referência;

   ii. Com a finalidade de tornar objetivo o julgamento da documentação de qualificação técnica, considera(m)-se compatível(eis) o(s) atestado(s) que expressamente certifique(m) que a empresa já forneceu solução de:

      - SOLUÇÃO DE PROTEÇÃO E AUDITORIA DO USO DE CREDENCIAIS;

- SUPORTE TÉCNICO EM SOLUÇÃO DE PROTEÇÃO E AUDITORIA DO USO DE CREDENCIAIS, além de comprovar que executou a contento serviço de manutenção e suporte técnico, pelo período de no mínimo 12 (doze) meses.
- TREINAMENTO TÉCNICO EM SOLUÇÃO DE PROTEÇÃO E AUDITORIA DO USO DE CREDENCIAIS.

iii. Admite-se a soma do quantitativo de serviços nos atestados apresentados, desde que tenham sido realizados de forma simultânea no período de 12 (doze) meses.

B. Apresentar documento probatório de que possui compromisso com a sustentabilidade ambiental, nos termos da Lei Distrital n° 4.770/2012, que poderá ser feito da seguinte forma:

i. Por Declaração, onde a licitante afirma possuir o compromisso e responsabilidade com a Sustentabilidade Ambiental, nos termos das exigências impostas pela Lei Distrital n° 4.770/2012, conforme modelo constante do Anexo deste edital, ou;

ii. Com a apresentação de documento probatório (atestado, declaração, certificado, registro, credenciamento etc.) emitido por Órgãos Públicos de qualquer ente da Federação que tenha competência legal na área ambiental que o produto ofertado, comercializado, ou o fornecedor, distribuidor ou fabricante está devidamente cadastrado, registrado etc. no respectivo Órgão, ou;

iii. Com a apresentação de documentos que o fornecedor está em fase de implantação de práticas sustentáveis, informando, no referido documento quais são as práticas já implantadas e, quais as metas pretendidas a atingir na questão da sustentabilidade ambiental.

iv. No caso de o licitante apresentar os documentos comprobatórios, conforme mencionado nas alíneas “i” e “iii” poderá ser designada pelo TJPA uma Comissão de Avaliadores que juntamente com o Pregoeiro e sua Equipe poderá inspecionar/vistoriar o estabelecimento ou o ponto comercial do licitante, a fim de verificar as informações e declarações apresentadas.

v. Caso seja detectado pelos inspetores/avaliadores que as informações declaradas pelo licitante não sejam verdadeiras, ou, que esteja de má fé, serão tomadas as medidas administrativas, e se for o caso, penal, cabível ao caso.

2.11. Do impacto ambiental

Pelo fato da solução a ser adquirida ser totalmente baseada em software, não haverá impactos ambientais relevantes a serem considerados em sua implantação.

2.12. Da conformidade técnica e legal

Serão de propriedade do TJPA todos os produtos gerados pela empresa CONTRATADA relacionados a presente contratação, incluindo estudos, relatórios, especificações, descrições técnicas, protótipos, dados, esquemas, planilhas, plantas, desenhos, diagramas, páginas na

Intranet e documentação, em papel ou em qualquer forma ou mídia, em conformidade com o artigo 111 da Lei 8.666/93, com a Lei 9.609/98, que dispõe sobre propriedade intelectual de programa de computador, e com a Lei 9.610/98, que dispõe sobre direito autoral, sendo vedada qualquer comercialização desses por parte da CONTRATADA.

2.13. Das obrigações

2.13.1. Das obrigações do CONTRATANTE

2.13.1.1. Permitir ao pessoal técnico da CONTRATADA, desde que identificado e incluído na relação de técnicos autorizados, o acesso às unidades para a execução das atividades, respeitadas as normas de segurança vigentes nas suas dependências.

2.13.1.2. Notificar a CONTRATADA quanto a defeitos ou irregularidades verificados na execução das atividades objeto deste Termo de referência, bem como quanto a qualquer ocorrência relativa ao comportamento de seus técnicos, quando em atendimento, que venha a ser considerado prejudicial ou inconveniente para o Tribunal.

2.13.1.3. Indicar os locais onde deverão ser instalados os equipamentos, caso necessários, e proporcionar à CONTRATADA as facilidades e instruções necessárias para a realização do serviço de instalação.

2.13.1.4. Verificar a regularidade da situação fiscal e dos recolhimentos sociais trabalhistas da CONTRATADA conforme determina a lei, antes de efetuar o pagamento devido.

2.13.1.5. Promover a fiscalização do contrato, sob os aspectos quantitativo e qualitativo, por intermédio de profissional designado, anotando em registro próprio as falhas detectadas e exigindo as medidas corretivas necessárias, bem como acompanhar o desenvolvimento do contrato, conferir os serviços executados e atestar os documentos fiscais pertinentes, quando comprovada a execução total, fiel e correta dos serviços, podendo ainda sustar, recusar, mandar fazer ou desfazer qualquer procedimento que não esteja de acordo com os termos contratuais.

2.13.1.6. Comunicar tempestivamente à CONTRATADA as possíveis irregularidades detectadas na execução das atividades.

2.13.1.7. Confeccionar Termo de Recebimento Definitivo para os itens do LOTE.

2.13.1.8. Observar para que durante a vigência do contrato sejam cumpridas as obrigações assumidas pela CONTRATADA, bem como sejam mantidas todas as condições de qualificação exigidas no processo de contratação.

2.13.2. Das obrigações da CONTRATADA

2.13.2.1. A CONTRATADA deverá responsabilizar-se integralmente pela execução das atividades contratadas, nos termos da legislação vigente, de modo que eles sejam realizados com esmero, sob sua inteira e exclusiva responsabilidade, obedecendo às normas e rotinas do Tribunal, em especial as que digam respeito à segurança, à confiabilidade e à integridade.

2.13.2.2. A CONTRATADA deverá assinar termo de responsabilidade e sigilo, comprometendo-se a não comentar nenhum assunto tratado nas dependências do Tribunal ou a serviço deste, salvo se expressamente autorizado por representante legal do Tribunal.

2.13.2.3. No termo de responsabilidade e sigilo assinado, a CONTRATADA declara estar ciente de que a estrutura computacional disponibilizada pelo Tribunal não poderá ser utilizada para fins particulares, e que a navegação em sítios da Internet e as correspondências em meio eletrônico utilizando o endereço do Tribunal ou acessado a partir dos seus equipamentos poderão ser auditadas.

2.13.2.4. A CONTRATADA responsabilizar-se-á pelo comportamento dos seus empregados e por quaisquer danos que estes ou seus prepostos venham porventura ocasionar ao Tribunal, ou a terceiros, durante a execução dos serviços, podendo o órgão descontar o valor correspondente ao dano dos pagamentos devidos.

2.13.2.5. A CONTRATADA deverá manter durante a vigência contratual, todas as condições que ensejaram a sua contratação.

2.13.2.6. A CONTRATADA deverá manter seus empregados, durante o horário de prestação do serviço, quando nas dependências do Tribunal, devidamente identificados mediante uso permanente de crachá.

2.13.2.7. A CONTRATADA deverá cumprir e fazer cumprir por seus empregados as normas e regulamentos disciplinares do Tribunal, bem como quaisquer determinações emanadas das autoridades competentes.

2.13.2.8. A CONTRATADA deverá providenciar a imediata correção das deficiências apontadas pelo Tribunal quanto à execução das atividades previstas.

2.13.2.9. A CONTRATADA não deverá se valer do contrato a ser celebrado para assumir obrigações perante terceiros, dando-o como garantia, nem utilizar os direitos de crédito, a serem auferidos em função das atividades prestadas, em quaisquer operações de desconto bancário, sem prévia autorização do Tribunal.

2.13.2.10. A CONTRATADA deverá comunicar, de forma detalhada, toda e qualquer ocorrência de acidentes verificada no curso da execução contratual.

2.13.2.11. A CONTRATADA deverá ter monitoração da qualidade das atividades executadas. Os registros gerados, depois de atendidos e dados por concluídos, sofrerão avaliação do próprio usuário quanto à conclusão do atendimento e sua satisfação.

2.13.2.12. Caso os usuários não se sintam satisfeitos com a execução do suporte, os registros originais serão imediatamente reabertos.

2.13.2.13. Os registros deverão conter todas as informações necessárias para a consecução do atendimento pela CONTRATADA, bem como suficientes para atender as necessidades do cliente.

2.13.2.14. A CONTRATADA deverá diligenciar no sentido de que os seus técnicos, ou prepostos, portem, obrigatoriamente, a respectiva identidade funcional, quando do atendimento ao Tribunal.

2.13.2.15. A CONTRATADA deverá encaminhar expediente ao Tribunal, informando os nomes dos técnicos que estão autorizados a executar as atividades contratadas.

2.13.2.16. A CONTRATADA deverá apresentar atestado(s) de capacidade técnica expedido por pessoa jurídica de direito público ou privado, onde comprove ter desenvolvido atividades pertinentes e compatíveis aos constantes com o objeto deste edital;

2.13.2.17. A CONTRATADA deverá apresentar documentação técnica dos serviços executados, nas datas aprazadas, visando homologação da mesma pela CONTRATANTE.

2.13.2.18. A CONTRATADA deverá pagar todos os impostos e taxas devidas sobre as atividades prestadas ao Tribunal, bem como as contribuições à previdência social, encargos trabalhistas, prêmios de seguro e acidentes de trabalho, emolumentos, quaisquer insumos e outras despesas diretas e indiretas que se façam necessárias à execução dos serviços contratados. A não comprovação do pagamento desobriga o CONTRATANTE do pagamento da fatura até a regularização.

3. ESPECIFICAÇÃO TÉCNICA DETALHADA

3.1. Dos papeis a serem desempenhados

Em atenção à legislação vigente, especialmente no que diz respeito a Resolução nº 182/2013 do CNJ e as Portarias nº 684/2020 e 685/2020, resume-se papeis e responsabilidades relacionados à contratação e fiscalização:

PAPEL	ENTIDADE	RESPONSABILIDADE
Equipe de Apoio da Contratação	TJPA	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.
Equipe de Gestão e Fiscalização do Contrato	TJPA	Equipe composta pelo gestor do contrato, responsável por gerir a execução contratual, e pelos fiscais demandante, técnico e administrativo, responsáveis por fiscalizar a execução contratual.
Fiscal Demandante do Contrato	TJPA	Servidor representante da área demandante da contratação, indicado pela referida autoridade competente, responsável por fiscalizar o contrato quanto aos aspectos funcionais do objeto, inclusive em relação à aplicação de sanções.
Fiscal Técnico do Contrato	TJPA	Servidor representante da área técnica, indicado pela respectiva autoridade competente, responsável por fiscalizar o contrato quanto aos aspectos técnicos do objeto, inclusive em relação à aplicação de sanções.
Fiscal Administrativo do Contrato	TJPA	Servidor representante da Secretaria de Administração, indicado pela respectiva autoridade, responsável por fiscalizar o contrato quanto aos aspectos administrativos da execução, especialmente os referentes ao recebimento, pagamento, sanções, aderência às normas, diretrizes e obrigações contratuais.

Gestor do Contrato	TJPA	Servidor com atribuições gerenciais, técnicas ou operacionais relacionadas ao processo de gestão do contrato, indicado por autoridade competente do órgão.
Preposto	Contratada	Funcionário representante da empresa contratada, responsável por acompanhar a execução do contrato e atuar como interlocutor principal junto ao órgão contratante, incumbido de receber, diligenciar, encaminhar e responder as questões técnicas, legais e administrativas referentes ao andamento contratual.

Equipe de apoio da contratação (quando se tratar de licitação)		
INTEGRANTE DEMANDANTE Nome: Arilson Galdino da Silva Matrícula: 183318 Telefone: 3289-7181 E-mail: arilson.silva@tjpa.jus.br	**INTEGRANTE TÉCNICO** Nome: Daniel Azevedo Ferreira Matrícula: 116394 Telefone: 3289-7177 E-mail: daniel.ferreira@tjpa.jus.br	**INTEGRANTE ADMINISTRATIVO** Nome: Helen Rose da Silva Saraiva Almeida Matrícula: 63860 Telefone: 3205-3571 E-mail: helen.rose@tjpa.jus.br

Equipe de gestão e fiscalização da contratação			
GESTOR DO CONTRATO Nome: Thiago do Rosário de Castro Matrícula: 174394 Telefone: 3289-7189 E-mail: thiago.rosario@tjpa.jus.br	**FISCAL DEMANDANTE** Nome: Arilson Galdino da Silva Matrícula: 183318 Telefone: 3289-7181 E-mail: arilson.silva@tjpa.jus.br	**FISCAL TÉCNICO** Nome: Daniel Azevedo Ferreira Matrícula: 116394 Telefone: 98483-8714 E-mail: daniel.ferreira@tjpa.jus.br	**FISCAL ADMINISTRATIVO** Nome: Matrícula: Telefone: E-mail:

Pela CONTRATANTE, deverá ser indicado um servidor da Coordenadoria de Suporte Técnico (CST) para acompanhar a implantação, onde também, eventualmente e formalmente, delegará competências conforme as necessidades do projeto.

Pela CONTRATADA, deverá ser indicado um responsável técnico encarregado de dar suporte ao esclarecimento das exigências técnicas contratuais.

Para fins de contrato, a empresa contratada deverá designar seu "PREPOSTO", ao qual serão transmitidas as instruções, orientações e normas para execução das obrigações contratuais.

Cabe ao PREPOSTO e ao RESPONSÁVEL TÉCNICO:

a) Coordenar, orientar e supervisionar toda a equipe técnica da CONTRATADA alocada para o cumprimento das obrigações contratuais, cabendo-lhe ainda,

a delegação e distribuição das tarefas entre as equipes, garantindo o cumprimento dos níveis de serviço estabelecidos.

b) Responder prontamente a todos os questionamentos e solicitações do TJPA, informando-os das necessidades de intervenção, inclusive, se necessário, aquelas que sejam efetuadas através de terceiros.

c) Propor ao TJPA mudanças nas rotinas e procedimentos técnicos, quando julgar pertinente, visando a otimização de custos, a racionalização e melhoria de processos.

d) Participar, quando solicitado pelo Tribunal, de reuniões relativas às atividades sob sua gestão, fornecendo informações e relatórios, apresentando sugestões, e propondo soluções que julgue pertinentes e necessárias.

e) Acompanhar os resultados globais das atividades sob sua gestão, fornecendo subsídios e informações à Secretaria de Informática do TJPA, visando o tratamento das prioridades e do planejamento global.

f) Ser o ponto de contato entre o TJPA e a CONTRATADA, no que se refere as atividades executadas, posicionando os servidores da Secretaria de Informática quanto ao cumprimento das metas estabelecidas.

3.2. Da dinâmica de execução do contrato

3.3. Etapas

3.4. Dos prazos

3.4.1. Prazos de entrega dos bens/execução dos serviços

O prazo de entrega dos bens adquiridos e de serviços prestados deverá ser executado de acordo com os prazos máximos definidos no cronograma abaixo:

#	EVENTO	RESPONSÁVEL	PRAZO
1	Assinatura do Contrato.	CONTRATANTE e CONTRATADA	Até 5 (cinco) dias após a convocação pelo CONTRATANTE.
2	Entrega de todos os componentes da Solução.	CONTRATADA	Até 30 (trinta) dias após o evento 1.
3	Conferência dos componentes da solução.	CONTRATANTE	Até 05 (cinco) dias após o evento 2.
4	Entrega da versão inicial do Plano de Implantação.	CONTRATADA	Até 10 (dez) dias após o evento 1.
5	Aceite do Plano de Implantação.	CONTRATANTE	Até 05 (cinco) dias após o evento 4.
6	Entrega da versão final do Plano de Implantação.	CONTRATADA	Até 2 (dois) dias úteis após o evento 5.
7	Implantação da Solução – Primeira Etapa*.	CONTRATADA	Até 10 (dez) dias úteis após o evento 6.
8	Emissão do Termo de Aceitação Provisória 1 (TAP1).	CONTRATADA	Até 5 (cinco) dias após o evento 7.
9	Implantação da Solução – Segunda Etapa*.	CONTRATADA	Até 10 (dez) dias úteis após o evento 7.

10	Emissão do Termo de Aceitação Provisória 2 (TAP2).	CONTRATADA	Até 5 (cinco) dias após os eventos 9.
11	Implantação da Solução – Terceira Etapa*.	CONTRATADA	Até 10 (dez) dias úteis após o evento 9.
12	Emissão do Termo de Aceitação Definitiva (TAD) da Implantação.	CONTRATADA	Até 5 (cinco) dias úteis após o evento 11.
13	Operação Assistida.	CONTRATADA	Até 30 (trinta) dias úteis de operação assistida após emissão do Termo de Aceitação Definitiva (TAD).

3.4.2. Prazo de vigência do contrato

O prazo de vigência do contrato assinado será de 30 (trinta) meses, a partir da data da assinatura.

3.4.3. Logística de implantação

Por tratar-se de software, não haverá necessidade de entrega de equipamentos, cabendo apenas o processo de implantação, configuração e sintonia da solução contratada a qual será realizada segundo agendamento prévio com o fiscal técnico do contrato.

3.4.4. Cronograma

Não haverá nenhum cronograma específico a ser cumprido pela CONTRATADA, mas somente a exigência de cumprimento dos prazos citados no item 3.4.1.

3.5. Dos instrumentos formais de solicitação

As comunicações formais ocorrerão, preferencialmente, por e-mail, especialmente no que tange à formalização de pedidos, prazos e intercâmbio de documentação, sem prejuízo da utilização de recursos telefônicos quando da prestação da garantia e dos seus serviços atrelados de suporte técnico ou quando couber a agilização do contato para a consecução de atividade específica, ficando estas discricionariamente a cargo da CONTRATANTE.

3.6. Garantia e Nível de Serviço

3.6.1. Garantia do produto/serviço

De acordo com o item 3.6.3 dos estudos preliminares, o prazo de garantia do software, suporte e licenciamento que serão renovados deverá ser de 30 (trinta) meses.

3.6.2. Garantia contratual

A Contratada, no prazo de 10 (dez) dias corridos, após a assinatura do Termo de Contrato, prestará garantia no valor correspondente a 5% (cinco por cento) do valor do Contrato, podendo optar por qualquer das modalidades previstas no Art. 56, da Lei n° 8.666, de 1993.

3.6.3. Nível de Serviço

A tabela abaixo descreve os prazos de atendimento que deverão ser cumpridos pela CONTRATADA, de acordo com a severidade de cada chamado aberto:

Tabela de Solução dos chamados

Severidade	Descrição	Tempo para primeiro contato após abertura do chamado	Tempo de resolução do chamado
Urgente	Serviço crítico parado em produção.	30 minutos	Até 01 (uma) hora
Alta	Erros e problemas que estão impactando no ambiente de produção.	60 minutos	Até 04 (quatro) hora
Média	Problemas ou erros contornáveis que afetam o ambiente em produção, mas não possuem alto impacto.	90 minutos	Até 06 (seis) horas
Baixa	Problemas ou erros contornáveis que não impactam significativamente no ambiente em produção.	120 minutos	Até 08 (oito) horas
Informações	Consulta Técnica, dúvidas em geral, monitoramento.	150 minutos	Até 24 (vinte e quatro) horas

3.7. Da forma de comunicação e acompanhamento da execução do contrato

A CONTRATADA deverá fornecer previamente os contatos de e-mail e telefone dos envolvidos na execução do objeto da contratação. Estes serão os principais canais de comunicação a serem utilizados durante a execução do contrato, devendo a comunicação ser realizada preferencialmente por e-mails, para geração de registros documentais. Pela CONTRATANTE, os componentes da Equipe de Gestão e Fiscalização da Contratação se encarregarão da comunicação com a CONTRATADA no tocante à execução do contrato.

3.8. Do recebimento

3.8.1. Do recebimento provisório e definitivo

3.8.1.1. Com o objetivo de verificar sua conformidade com as especificações constantes neste Termo de Referência, o recebimento dos bens será realizado:

3.8.1.2. Provisoriamente, no ato da entrega, para posterior verificação de conformidade dos bens com as especificações constantes neste Termo de Referência.

3.8.1.3. Definitivamente, no prazo máximo de até 30 (trinta) dias corridos, contados a partir da data de assinatura do Termo de Recebimento Provisório;

3.8.1.4. O TJPA designará equipe específica para o recebimento e conferência dos produtos integrantes do objeto deste Termo de Referência.

3.8.1.5. A equipe técnica designada pelo TJPA será responsável pela conferência e avaliação dos serviços de instalação, configuração prestados pela empresa contratada, além de avaliar as atividades de gerenciamento da execução do projeto e a realização dos testes de todo ambiente implementado.

3.8.1.6. Os materiais que forem entregues em desacordo com o especificado deverão ser substituídos pela contratada em até 10 (dez) dias úteis. O seu descumprimento poderá acarretar sanções conforme previsto na legislação vigente;

3.8.1.7. Caso após o Recebimento Provisório constatar-se que os materiais possuem vícios aparentes ou redibitórios ou estão em desacordo com as especificações ou

a proposta, serão interrompidos os prazos de recebimento e suspenso o pagamento até que sanado o problema;

3.8.1.8. O Recebimento Provisório ou Definitivo não exclui a responsabilidade civil pela solidez e segurança do serviço, nem a responsabilidade pela perfeita execução do contrato, dentro dos limites estabelecidos pela lei ou por este instrumento.

3.9. Da forma de pagamento

Para efeito de pagamento, a Contratada deverá apresentar os seguintes documentos:

3.9.1. Certificado de Regularidade do Fundo de Garantia por Tempo de Serviço – FGTS, fornecido pela CEF – Caixa Econômica Federal, devidamente atualizado (Lei n.º 8.036/90);

3.9.2. Prova de regularidade com a Fazenda Federal por meio da Certidão Conjunta Negativa de Débitos relativos aos Tributos Federais, inclusive contribuições previdenciárias, e a Dívida Ativa da União, expedida pelo Ministério da Fazenda/Secretaria da Receita Federal do Brasil (Portaria Conjunta RFB/PGFN nº 1.751/2014);

3.9.3. Certidão de Regularidade com a Fazenda do Distrito Federal.

3.9.4. Certidão de regularidade relativa a débitos inadimplidos perante o Poder Judiciário do Pará, mediante a apresentação de certidão negativa, em plena validade.

O pagamento será efetuado em até 30 (trinta) dias, contados a partir da data de apresentação da Nota Fiscal, desde que o documento de cobrança esteja em condições de liquidação de pagamento.

Passados 30 (trinta) dias sem o devido pagamento por parte da Administração, a parcela devida será atualizada monetariamente, desde o vencimento da obrigação até a data do efetivo pagamento de acordo com a variação “pro rata tempore” do IPCA.

Nenhum pagamento será efetuado ao licitante enquanto pendente de liquidação qualquer obrigação que lhe for imposta, em virtude de penalidade ou inadimplência, sem que isso gere direito ao pleito de reajustamento de preços ou correção monetária.

A retenção dos tributos não será efetivada caso a contratada apresente junto com sua Nota Fiscal a comprovação de que ele é optante do Sistema Integrado de Pagamento de Impostos e Contribuições das Microempresas e Empresas de Pequeno Porte – SIMPLES.

Documentos de cobrança rejeitados por erros ou incorreções em seu preenchimento serão formalmente devolvidos à Contratada, no prazo máximo de 5 (cinco) dias úteis contados da data de sua apresentação.

Os documentos de cobrança, escoimados das causas que motivaram a rejeição, deverão ser reapresentados num prazo máximo de 2 (dois) dias úteis.

Em caso de rejeição da Nota Fiscal/Fatura, motivada por erro ou incorreções, o prazo de pagamento passará a ser contado a partir da data de sua reapresentação.

Os valores para essa contratação foram relacionados no Plano de Orçamentário do Tribunal de Justiça do Estado do Pará, referente à Secretaria de Informática, vigente para o exercício de 2021, e no Plano de Contratações de Soluções de TIC para o referido exercício. Os valores serão remanejados das Notas de Reservas originalmente autorizadas para aquisição de solução de VDI, especificamente nas 2021/497, 2021/502, 2021/536 e 2021/570 (relacionadas às ações

8651, 8652 e 8653, fontes 0101 e 0112, elemento de despesa 3.3.90.40), as quais estão rateadas em 65% no 1G, 9% no 2G e 26% no Apoio Indireto.

3.10. Da transferência de conhecimento

3.10.1. A CONTRATADA deverá entregar ao Tribunal toda e qualquer documentação gerada em meio magnético e/ou físico em função da prestação de serviços.

3.10.2. As informações geradas pela CONTRATADA estarão disponíveis em ferramentas e em documentos conforme a definições e padrões utilizados pelo Tribunal.

3.10.3. Deverá haver transferência de conhecimento da CONTRATADA para o Tribunal em relação às tecnologias utilizadas na prestação de serviços para melhor eficiência, eficácia, efetividade e economicidade com sua adoção.

3.10.4. Será de inteira responsabilidade da CONTRATADA, sem ônus adicional para o Tribunal, garantir o repasse bem-sucedido de todas as informações necessárias para a continuidade dos serviços pelo órgão ou empresa por este designada.

3.10.5. O apoio na fase de implantação, pela transferência técnica, no uso das soluções implantadas pela CONTRATADA, deverá ser viabilizada, sem ônus adicionais para o Tribunal, e baseado em documentos funcionais, técnicos e/ou manuais específicos da solução desenvolvida. O cronograma e horários dos eventos deverão ser previamente aprovados pelo órgão.

3.11. Dos direitos de propriedade intelectual e autoral

Após a completa implantação da solução adquirida e atestado que a solução está em conformidade com todos os itens do contrato firmado, tanto em termo de qualidade, quando em quantidade, será emitido um TRD (Termo de Recebimento Definitivo) da solução, caracterizando a transferência definitiva da solução e de todos os componentes necessários para o seu total funcionamento, para o Tribunal.

Eventuais softwares que são necessários ao funcionamento da solução são de propriedade do fabricante e deverão ser fornecidos em conjunto com o respectivo *hardware*, sendo que os direitos de propriedade intelectual pertencem ao fabricante da solução, de acordo com a Lei 9609/98, que dispõe sobre a proteção da propriedade intelectual de programa de computador.

3.12. Da qualificação técnica dos profissionais

A Contratada deverá possuir, após a assinatura do contrato, pelo menos 1 (um) profissional com certificação técnica oficial do fabricante, compatível com o objeto deste processo, capaz de prestar o suporte técnico aos produtos em garantia e escalar o chamado ao fabricante, conforme a necessidade.

3.13. Das sanções

A aplicação das sanções de natureza pecuniárias e restritivas de direito pelo cumprimento das normas previstas neste edital e dos contratos dele decorrentes, bem como pela prática das condutas tipificadas nos arts. 81, 86, 87 e 88 da Lei 8.666/93 e artigo 7º da Lei 10.520/2002, também obedecerão às prescrições do Decreto 26.851/2006 e alterações posteriores.

Aplicam-se aos Licitantes nessa aquisição todas as disposições referentes às Práticas Proibidas e à incorporação do reconhecimento recíproco de sanções por parte de Instituições

Financeiras Internacionais (IFI), conforme disposto no Anexo deste Edital e no site do Banco (www.iadb.org/integrity).

4. Da confidencialidade de informações

4.1. Os conhecimentos, dados e informações de propriedade do CONTRATANTE, tanto tecnológicos como administrativos, tais como: produtos, sistemas, técnicas, estratégias, métodos de operação e todos e quaisquer outros, repassados por força do objeto do contrato, constituem informação privilegiada e possuem caráter de confidencialidade.

4.2. Estas informações poderão ser utilizadas, só e exclusivamente, no cumprimento da execução das cláusulas e condições estabelecidas no contrato, sendo expressamente vedado à CONTRATADA:

4.2.1. Utilizá-las para fins não previstos no instrumento contratual;

4.2.2. Repassá-las a terceiros e/ou empregados não vinculados diretamente à execução do objeto contratado.

5. DOS REQUISITOS TÉCNICOS ESPECÍFICOS

5.1. Requisitos Gerais

5.1.1. Cada pacote da solução ofertada deve ser instalado em sua última versão estável e estar coberto por contrato de suporte e atualização de versão pelo(s) fabricante(s) durante a vigência da garantia de 30 meses.

5.1.2. O conjunto de requisitos especificados para CADA UM DOS ITENS QUE COMPÕEM A SOLUÇÃO PODERÁ SER ATENDIDO POR MEIO DE COMPOSIÇÃO DE PRODUTOS DE MÚLTIPLOS FABRICANTES/FORNECEDORES, desde que sejam atendidas as especificações técnicas mínimas e obrigatórias do respectivo item e que haja integração entre os produtos.

5.1.3. No momento da apresentação das propostas, todos os componentes constantes da solução deverão possuir EOL (End-of-life) e EOS (End-of-support) não definidos ou anunciados para um prazo de no mínimo 30 meses.

5.1.4. Um ativo da solução é definido como um servidor, uma estação de trabalho, um ativo de rede e/ou de segurança, dentre outros mencionados a seguir, cujas credenciais de acesso passem a ser gerenciadas pela solução.

5.1.5. Um usuário da solução é definido como qualquer pessoa que acesse um ativo da rede mediante logon na solução e uso de credenciais por ela gerenciadas.

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

5.1.7. A Solução deverá prover monitoramento comportamental, auditoria e segurança de acessos por meio de credenciais administrativas para Servidores, Ativos de Infraestrutura e estações de trabalho, conforme quantitativos descritos na Tabela de Definição de Objetos (Anexo I).

5.1.8. Consideram-se ativos de infraestrutura: servidores windows/linux, estações de trabalho, access points, switches, appliances de segurança e componentes diversos (como robôs de backup, switches SAN, storages e afins) mencionados nesta especificação técnica.

5.2. Solução de Proteção e Auditoria do Uso de Credenciais – Monitoramento Comportamental e Repositório Seguro, com o serviço de implantação e o de garantia dos equipamentos e softwares pelo período de 30 meses.

5.2.1. As licenças fornecidas para a solução deverão ser perpétuas;

5.2.2. Quanto a forma de licenciamento, serão aceitas soluções que permitam:

5.2.2.1. No mínimo 50 (cinquenta) acessos simultâneos com funções privilegiadas e gerenciamento ilimitado de ativos; e/ou

5.2.2.2. O gerenciamento de pelo menos o número de ativos presentes na Tabela de Definição de Objetos (Anexo I), mais 50%, considerando o crescimento vegetativos do parque de ativos nos 30 meses de garantia da solução;

5.2.3. Gerenciar dispositivos-alvo baseados, em no mínimo, as seguintes tecnologias:

5.2.3.1. Sistemas operacionais: Linux; Microsoft Windows.

5.2.3.2. Hypervisors: VMWare, RedHat KVM e Microsoft Hyper-V;

5.2.3.3. Contas de usuários de sistemas;

5.2.3.4. Contas de usuários de serviço;

5.2.3.5. Credenciais do Microsoft COM+;

5.2.3.6. Credenciais do Microsoft Internet Information Service – IIS;

5.2.3.7. Credenciais do Apache TomCat;

5.2.3.8. Credenciais do RedHat JBoss;

5.2.3.9. Objetos do Microsoft Active Directory (usuários, grupos e computadores);

5.2.3.10. Objetos do Lightweight Directory Access Protocol – LDAP (usuários, grupos e computadores);

5.2.3.11. Contas de usuários e administradores de bancos de dados Microsoft SQL Server, Oracle, PostgreSQL e MySQL;

5.2.3.12. Contas de equipamentos ativos de conectividade de redes LAN (Local Area Network) e WAN (Wide Area Network) – switches, roteadores, controladores/APs WiFi;

5.2.3.13. Contas de equipamentos ativos de conectividade de redes SAN (Storage Area Network) e NAS (Network Attached Storage);

5.2.3.14. Contas de usuários e administradores de consoles de gerenciamento de computadores servidores;

5.2.3.15. Contas de usuários e administradores de estações de trabalho;

5.2.3.16. Contas de equipamentos dedicados à segurança, tais como Firewall, WAF, IPS e filtros de conteúdo;

5.2.3.17. Credenciais de serviço em nuvem em Oracle, Google e Azure;

5.2.4. Proteger contra a perda, roubo e gestão inadequada de credenciais através de regras de complexidade de senha que incluem, no mínimo, o comprimento da

senha (quantidade de caracteres), a frequência de troca da senha, a especificação de caracteres permitidos ou proibidos na composição da senha e o gerenciamento do histórico das senhas geridas;

5.2.5. Mitigar problemas de segurança relacionados ao compartilhamento indevido de credenciais privilegiadas que são armazenadas localmente em dispositivos e também de contas que não são gerenciadas de forma centralizada por serviços de diretórios;

5.2.6. Descobrir credenciais privilegiadas referenciadas por serviços e processos automatizados. Além disso, a solução deve propagar as senhas geradas de forma aleatória onde quer que estas estejam referenciadas;

5.2.7. Gerenciar, de forma segura, senhas utilizadas por contas de serviço, evitando a utilização de senhas em texto claro por scripts ou rotinas dos equipamentos;

5.2.8. Garantir a implementação dos privilégios mínimos necessários, provendo acesso às senhas das contas privilegiadas somente ao pessoal autorizado;

5.2.9. Não será aceita limitação do número de contas que poderão ser gerenciadas.

5.2.10. A solução deve utilizar banco de dados, para armazenamento de credenciais, com as melhores práticas de segurança, com mecanismo de blindagem do sistema operacional através da desativação ou desinstalação de serviços e portas de acesso não essenciais ao funcionamento da solução.

5.2.10.1. Caso o banco de dados utilizado para armazenamento de credenciais seja de terceiros, a solução deverá ser entregue com licenças de software que o compatibilize com a solução;

5.2.10.2. Para o caso acima, a empresa contratada deverá prestar suporte também dos componentes adicionais a serem entregues, diretamente ou por subcontratação;

5.2.10.3. O banco de dados adotado pela solução deve:

5.2.10.3.1. Permitir a configuração em modo de alta disponibilidade, com a utilização nos dois sites do Tribunal;

5.2.10.3.2. Permitir o Backup e Recovery incluindo as configurações da solução;

5.2.10.3.3. Permitir a configuração de Backups automatizados, com a programação/agendamento de horários;

5.2.11. Suportar a implementação em parque computacional Windows Server 2012, Windows Server 2012 R2, Windows Server 2016 e/ou Linux CentOS 7 ou superior;

5.2.12. Suportar instalação em VMWare nas versões do Windows Server 2012 e/ou superiores;

5.2.13. Caso não seja compatível, a solução deverá ser entregue com hardware e licenças de software (exemplo: hypervisor diverso ao do item acima ou sistema operacional específico) que a compatibilize com as ferramentas de infraestrutura do CONTRATANTE;

5.2.13.1. Para o caso acima, a empresa contratada deverá prestar suporte também dos componentes adicionais a serem entregues, diretamente ou por subcontratação.

5.2.14. A solução deve ser configurada para uso em alta disponibilidade Ativo/Ativo: Em modo transparente. Sem custo adicional para o Tribunal;

5.2.15. Ter a capacidade de gerenciar credenciais que estejam em sistemas localizados em múltiplas localidades geográficas ou domínios, independentemente de sua quantidade;

5.2.16. Permitir a opção de implementar o gerenciamento de troca de senhas em redes segregadas e/ou remotas a fim de acomodar links de alta latência, redes isoladas (DMZ) e outras restrições semelhantes;

5.2.17. Possibilitar a utilização de criptografia do banco de dados utilizado pela solução para armazenar as credenciais gerenciadas pela mesma. A solução deve ainda ser compatível com pelo menos um dos seguintes métodos e padrões de criptografia:

5.2.17.1. AES com chaves de 256 bits;

5.2.17.2. FIPS 140-2;

5.2.17.3. Encriptação PKCS#11 ou superior por hardware utilizando dispositivos de HSM devidamente homologados pelo(s) fabricante(s) da solução ofertados.

5.2.18. Incorporar medidas de segurança, incluindo criptografia, a fim de proteger a informação em trânsito entre os módulos da solução e entre as aplicações dos usuários finais;

5.2.19. Ser capaz de exportar a chave de criptografia ou credencial equivalente do local de armazenamento das credenciais (repositório seguro), para ser utilizada nos cenários de recuperação de desastres, de forma a conceder acesso a todas as senhas de identidades privilegiadas gerenciadas pela solução;

5.2.20. A solução deve permitir a realização de autenticação com duplo fator através de protocolo RADIUS ou outros meios de comunicação;

5.2.21. Prover interface gráfica para que os administradores possam configurar as integrações com dispositivos e/ou plataformas que não são disponibilizadas nativamente, sem a necessidade de serviços profissionais de terceiros. Tal funcionalidade deve permitir que o administrador configure a comunicação com aplicações de terceiros utilizando, no mínimo, SSH e HTTP/HTTPS;

5.2.22. Integrar-se diretamente com soluções de SIEM, a fim de garantir o registro e a visualização, a partir da aplicação existente nesses sistemas, das seguintes ações:

5.2.22.1. Atividades administrativas de delegação e revogação de acesso às credenciais privilegiadas;

5.2.22.2. Atividades de recuperação, liberação e alterações de senhas;

5.2.22.3. Atividades executadas pelos usuários na aplicação web;

5.2.22.4. Eventos agendados;

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

5.2.23. Descobrir e alterar credenciais em ambiente Windows, incluindo contas nomeadas, administradores 'built-in' e convidados;

5.2.24. Descobrir e alterar credenciais privilegiadas em ambientes Linux;

5.2.25. Gerenciar credenciais em interfaces de gerenciamento de servidores “out-of-band”, tais como Dell iDrac, IBM IMM ou compatíveis com o padrão IPMI – Intelligent Platform Management Interface;

5.2.26. Descobrir e alterar credenciais do Active Directory (AD) e todos os outros serviços de diretório compatíveis com LDAP;

5.2.27. Descobrir e alterar processos interdependentes e credenciais de serviço, incluindo credenciais em ambientes clusterizados;

5.2.28. Permitir o agrupamento lógico de sistemas, obedecendo a uma hierarquia, a fim de simplificar a configuração e aplicação de políticas apropriadas para diferentes tipos de sistemas;

5.2.29. Ser capaz de redefinir senhas individuais ou grupos de senhas sob demanda e realizar 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. Caso a senha da conta gerenciada pela solução seja diferente daquela armazenada no banco de dados, a solução deve ser capaz de gerar relatórios e alertas notificando este evento;

5.2.30. Proteger as senhas de credenciais compartilhadas que seriam normalmente armazenadas em planilhas ou arquivos em texto claro;

5.2.31. 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 nas estações dos usuários para realizar o acesso, devendo conceder acesso a:

5.2.31.1. Sistemas e aplicações parametrizáveis, onde a aplicação deverá ser executada, por meio de página web, devidamente autenticada com usuário e senha pré-determinados ou recuperados da base de dados da solução, sem que haja login interativo por parte do usuário no 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;

5.2.31.2. 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;

5.2.31.3. As sessões acessadas podem ser monitoradas por meio de gravação de vídeos das mesmas, em formato padrão de execução não proprietário da solução, possibilitando que os vídeos gerados possam ser armazenados de modo seguro em drivers locais de rede, pastas compartilhadas, etc.;

5.2.31.4. Filtrar comandos executados ao longo da sessão gravada, possibilitando pesquisar ações específicas no vídeo gravado;

5.2.31.5. A função de gravação de sessões deve ser provida em alta disponibilidade, no modelo ativo-ativo, tanto no site principal quanto em um site adicional;

5.2.31.6. Ainda que as gravações estejam armazenadas em locais diferentes, a solução deve permitir que essas evidências sejam consultadas a partir de qualquer console web instalada, de maneira centralizada.

5.2.32. Permitir que os usuários solicitem acesso aos gestores através de interface web intuitiva;

5.2.33. Realizar a descoberta automática de chaves SSH em sistemas Linux;

5.2.34. Permitir que os comandos executados em sistemas Linux monitorados sejam gravados em modo texto;

5.2.35. Possuir funcionalidade de "AD Bridge" para integração de servidores Linux no Active Directory, acompanhando a mesma nomenclatura e grupos do diretório LDAP ou AD;

5.2.36. Provisionar na plataforma Linux as contas e grupos do Active Directory que possuam permissão de acesso, de maneira automatizada e transparente;

5.2.37. Fornecer aplicação web para acesso às funcionalidades básicas da solução que seja compatível com ao menos dois dos principais navegadores do mercado (Edge, Google Chrome e Firefox);

5.2.38. Oferecer em sua aplicação web diferentes visões e opções, de acordo com as permissões dos usuários, mostrando, por exemplo, apenas as funcionalidades delegadas aquele usuário;

5.2.39. Suportar uma variedade de métodos para registrar e relatar qualquer ação realizada e detectada pela solução, incluindo registros de aplicações baseadas em texto, auditoria de banco de dados, aplicações syslog, notificações de e-mail;

5.2.40. Permitir o envio automático de logs para servidores SYSLOG, de forma aderente ao disposto em RFC 5424 – The Syslog Protocol (IETF);

5.2.41. Ser configurável para disparar alertas baseados em eventos registrados a partir de alterações nos valores de registro, logs de evento do Windows, Syslog, enfileiramento de mensagens Microsoft e execução de aplicações específicas;

5.2.42. Controlar o acesso aos relatórios se baseando nas permissões configuradas na solução;

5.2.43. Registrar cada acesso, incluindo os acessos via aplicação web, para solicitações de senha, aprovações, checkout's, mudanças de delegação, relatórios e outras atividades. Devem ser registrados os acessos à console de gerenciamento da solução, tanto para configuração quanto para relatórios, bem como todas as atividades de alterações de senhas;

5.2.44. Caso os componentes da solução sejam segregados uns dos outros, a sua intercomunicação não deverá conter senhas em texto claro;

5.2.45. Criar relatórios que possam ser exportados em pelo menos um dos formatos editáveis como HTML, CSV, XLSX ou XLS;

5.2.46. A solução deverá disponibilizar:

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

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

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

5.2.47.3. 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 LINUX, por exemplo);

5.2.48. Ser capaz de, durante o processo de definição da política de composição de senha:

5.2.48.1. Gerar senhas aleatórias com extensão de no mínimo 127 (cento e vinte e sete) caracteres;

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

5.2.48.3. Especificar quais os tipos de caracteres devem ser utilizados na composição das senhas a serem geradas;

5.2.48.4. Implementar 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. Deve permitir a formação de grupos de usuários e dispositivos, bem como a atribuição de privilégios de acesso a esses grupos, onde esses privilégios de acesso possam ser atribuídos por critérios como tipo de dispositivo, sistemas operacionais, banco de dados e aplicativos de virtualização;

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

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

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

5.2.49. Suportar, através da interface Web para acesso e recuperação das senhas, de forma nativa, a personalização dinâmica e automática dos acessos atribuídos ao usuário conforme privilégios delegados pelo administrador da solução;

5.2.50. A interface web e de administração deverá ser compatível com pelo menos dois dos seguintes métodos de autenticação de duplo fator: certificados digitais, smart cards, tokens RSA ou OAuth 2.0, para todos os usuários da solução;

5.2.51. 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;

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

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

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

5.2.53.2. Alterações nas funções de delegação;

5.2.53.3. Adições, deleções e alterações de senhas gerenciadas pela solução;

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

5.2.53.5. Os relatórios devem ser filtrados por período de tempo, tipo de operação, sistema, gerente e outros critérios;

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

5.2.54.1. Lista de sistemas gerenciados;

5.2.54.2. Senhas armazenadas;

5.2.54.3. Eventos de alteração de senha;

5.2.54.4. Permissões de acesso web;

5.2.54.5. Auditoria de contas, sistemas e usuários;

5.2.54.6. Alerta em tempo real.

5.2.55. A solução deve possuir função de monitoramento e análise de comportamento, que toma por base os eventos gerados por todos os itens desta especificação técnica (repositório digital, gravador e auditor de sessões, agentes para proteção local de servidores, controladores de domínio e estações de trabalho);

5.2.56. Deve montar perfis de comportamento dos usuários acessando todos os dispositivos-alvo através da solução, por meio dos eventos coletados;

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

5.2.58. A Solução deve possuir função de monitoramento e análise de comportamento que toma por base os eventos gerados por todos os itens desta especificação técnica:

5.2.58.1. Deve monitorar e exibir acessos e atividades realizadas no próprio sistema;

5.2.58.2. Deverá exibir o somatório das atividades diárias divididos por origem;

5.2.58.3. Deve detectar, de forma automática ou por meio de parametrização, em caso de composição com solução de fabricantes distintos, pelo menos os seguintes comportamentos anormais:

5.2.58.3.1. Acesso Privilegiado em horários incomuns;

5.2.58.3.2. Acessos excessivos a contas privilegiadas;

5.2.58.3.3. Acesso Privilegiado a partir de endereços IP incomuns;

5.2.58.3.4. Máquina acessada a partir de endereços IP incomuns;

5.2.58.3.5. Máquina acessada em horários incomuns;

5.2.58.3.6. Acessos excessivos a uma máquina;

5.2.58.3.7. Máquina incomum originando acesso;

5.2.58.3.8. Usuário incomum logando de uma máquina de origem conhecida;

5.2.58.3.9. Acesso simultâneo, ou em intervalo de tempo relativamente curto, de uma conta privilegiada à várias máquinas;

5.2.58.3.10. Suspeita de roubo de credenciais.

5.2.58.4. As detecções não devem limitar-se a um tipo específico de comportamento anormal, possibilitando a correta demonstração de eventos complexos. Ex: usuário acessando o sistema em horário incomum e originando acesso de IP incomum e utilizando conta não anteriormente utilizada (Suspeita de roubo de credencial);

5.2.59. Deve permitir a configuração de eventos críticos a serem reportados automaticamente, baseados em:

5.2.59.1. Comandos Linux;

5.2.59.2. Expressões regulares para comandos em geral;

5.2.59.3. Eventos configurados manualmente que permitem a atribuição de nível de risco customizado.

5.2.60. Monitorar e avaliar as atividades de contas ou grupos privilegiados que não são administrados pela solução;

5.2.61. Possuir funcionalidade para monitoramento de saúde da solução, com a capacidade de chaveamento entre nós no caso de falhas (alta disponibilidade ativo / ativo).

5.3. Solução de Proteção e Auditoria do Uso de Credenciais – PROTEÇÃO LOCAL PARA SERVIDORES WINDOWS / LINUX, com o serviço de implantação e o de garantia dos equipamentos e softwares pelo período de 30 meses.

5.3.1. As licenças fornecidas para a solução deverão ser perpétuas;

5.3.2. Deverão ser fornecidas tantas licenças quantas forem necessárias para instalação da solução em cada um dos servidores Windows e/ou Linux, em funcionamento no TJPA, conforme Tabela de Definição de Objetos (Anexo I);

5.3.3. A solução, para servidores Linux, deverá possuir, no mínimo, as seguintes funcionalidades:

5.3.3.1. Permitir o gerenciamento dos privilégios em contas de usuário em equipamentos Linux, Solaris e AIX.

5.3.3.2. A solução deve associar os privilégios e comandos controlados às contas cadastradas no repositório seguro digital, realizando o controle no próprio sistema operacional do destino;

5.3.3.3. Garantir o controle e bloqueio de comandos, mesmo que o acesso seja realizado diretamente no servidor de destino (sem passar pelo repositório seguro digital) fazendo uso do agente instalado no sistema operacional de destino, Windows ou Linux;

5.3.3.4. Disponibilizar, como conjunto mínimo de atividades controladas no ativo de destino, as seguintes operações: criação e exclusão de arquivos e diretórios, mudança de nome de arquivos e diretórios, abertura de arquivos para escrita, comandos *chown* e *chmod* e ligações entre arquivos;

5.3.3.5. Implementar restrições, em uma plataforma, de maneira global ou em uma conta de usuário ou grupo de maneira granular;

5.3.3.6. Realizar o controle mediante interceptação do comando antes que ele seja executado;

5.3.3.7. Permitir a liberação de comandos privilegiados a usuários comuns em Windows ou Linux;

5.3.3.8. Permitir que os comandos executados em sistemas monitorados sejam gravados em modo texto no repositório seguro digital;

5.3.3.9. Permitir que sejam atribuídas permissões para usuários e grupos, inclusive do Active Directory;

5.3.3.10. Permitir o agrupamento de comandos, bem como a utilização de coringas como (*), para uma definição ampla de parâmetros;

5.3.3.11. A solução deverá possuir funcionalidade que permita definir variáveis de ambiente no momento da execução de um comando, independente da definição realizada pelo usuário ou seu perfil. Sendo exigido no mínimo as seguintes variáveis: PATH, ENV, BASH_ENV, GLOBIGNORE, SHELLOPTS;

5.3.3.12. Possibilitar o uso da máscara de usuário na execução dos comandos (valores entre 0000 e 0777);

5.3.3.13. Impedir a utilização da técnica de ShellEscape, em que um programa autorizado e executado com privilégios permita a execução de outros programas e consequentemente escape dos controles definidos;

5.3.3.14. Disponibilizar a funcionalidade de restrição de Shell, que impossibilite que scripts e shells de sistema executem comandos não permitidos pelas regras definidas na solução em Windows ou Linux;

5.3.3.15. Oferecer a capacidade de verificação da identidade da pessoa que executa comandos localmente no dispositivo alvo através de autenticação via usuário da ferramenta, LDAP ou RADIUS;

5.3.3.16. Monitorar e exibir acessos e atividades realizadas no próprio sistema;

5.3.3.17. Possibilitar o mapeamento de atividades regulares de usuários através do modo observação, depois coletar os resultados e exportá-los para um perfil.

5.3.4. Para servidores Microsoft Windows deverá possuir, no mínimo, as seguintes funcionalidades:

5.3.4.1. Garantir o controle e bloqueio de comandos, mesmo que o acesso seja realizado diretamente no servidor de destino (sem ser através do mecanismo de Monitoramento Comportamental e Repositório Seguro), fazendo uso do agente instalado, em Windows ou Linux;

5.3.4.2. Oferecer opção de execução de aplicações com privilégios em modo explícito e transparente (sem avisos);

5.3.4.3. Oferecer opção de execução monitorada de aplicações em modo explícito e transparente (sem avisos);

5.3.4.4. Oferecer opção de execução com restrições de aplicações em modo explícito e transparente (sem avisos);

5.3.4.5. Suportar, no mínimo, as versões de servidores Windows: 2012 R2 e 2016 (64-bit);

5.3.4.6. Implementar regras de controle de aplicações permitidas e bloqueadas para execução por meio do uso de agente, independentemente do acesso ao ativo ser realizado via mecanismo de Monitoramento Comportamental e Repositório Seguro ou diretamente no ativo;

5.3.4.7. Implementar regras de controle do nível de privilégio utilizado na execução das aplicações permitidas por meio do uso de agente, independentemente do acesso ao ativo ser realizado via mecanismo de Monitoramento Comportamental e Repositório Seguro ou diretamente no ativo;

5.3.4.8. Implementar controle de nível de privilégio independentemente da permissão que o usuário possua localmente no ativo ou no domínio, permitindo que usuários restritos executem atividades com nível administrativo;

5.3.4.9. Permitir atribuição granular para execução de aplicações com nível de privilégio administrativo, sem que esse privilégio seja global na máquina;

5.3.4.10. Implementar a verificação de checksum ou hash do arquivo, dos parâmetros permitidos e da assinatura de fabricante, para objetos reutilizáveis da solução;

5.3.4.11. Implementar o suporte ao nome exato da aplicação/arquivo/script e expressões regulares em qualquer formato, para objetos reutilizáveis da solução;

5.3.4.12. Utilizar eventos reportados na interface da ferramenta para criação de novas políticas ou incluí-los em políticas existentes;

5.3.4.13. Permitir agrupar aplicações com base em suas características, para facilitar a inserção de novas aplicações aos grupos ou políticas de segurança de aplicações já criadas;

5.3.4.14. Impedir a desativação do agente sem autorização e/ou registro da atividade por meio da interface de gerência;

5.3.4.15. Disponibilizar modo de observação, em que não há bloqueios, mas há o registro das execuções e atividades dos usuários, facilitando a criação de políticas baseadas em comportamento conhecido;

5.3.4.16. Monitorar e exibir acessos e atividades realizadas na própria solução;

5.3.4.17. Deve permitir autorização de acesso às aplicações e arquivos, quando incluídos em regras, individualmente ou em grupos;

5.3.4.18. Possibilitar o monitoramento e a criação de vídeos de execução de procedimentos realizados por usuários, de acordo com políticas e regras configuradas;

5.3.4.19. Possibilitar ao usuário final a solicitação de liberação de atividades específicas por meio do agente;

5.3.4.20. Possibilitar a liberação emergencial da execução de comandos e elevação de privilégios sem desativar a solução, caso o usuário esteja off-line;

5.3.4.21. Implementar as regras de controle de acordo com características do usuário final, incluindo nome de usuário, grupos a que o usuário pertence e endereço IP;

5.3.4.22. Oferecer monitoramento de atividade maliciosa dos processos em execução, visando detectar tentativas de roubo de credenciais;

5.3.4.23. Caso o dispositivo não possa estar conectado de forma permanente ao mecanismo de Monitoramento Comportamental e Repositório Seguro da solução, deve, de forma autônoma e off-line, gerenciar as senhas das credenciais locais, aplicando políticas de randomização e sincronização das senhas definidas na central da solução;

5.3.4.24. Possibilitar a execução de aplicativos que precisam de privilégio de execução a usuários não-privilegiados.

5.4. Solução de Proteção e Auditoria do Uso de Credenciais – PROTEÇÃO LOCAL PARA ESTAÇÕES DE TRABALHO, com o serviço de implantação e o de garantia dos equipamentos e softwares pelo período de 30 meses.

5.4.1. Deverão ser fornecidas tantas licenças quantas forem necessárias para instalação da solução em cada uma das estações de trabalho em uso no TJPA, conforme Tabela de Definição de Objetos (Anexo I);

5.4.1.1. As licenças fornecidas deverão ser perpétuas;

5.4.2. Para as estações de trabalho Microsoft Windows a solução deverá possuir, no mínimo, as seguintes funcionalidades:

5.4.2.1. Oferecer opção de execução de aplicações com privilégios em modo explícito e transparente (sem avisos);

5.4.2.2. Oferecer opção de execução monitorada de aplicações em modo explícito e transparente (sem avisos);

5.4.2.3. Oferecer opção de execução com restrições de aplicações em modo explícito e transparente (sem avisos);

5.4.2.4. Suportar pelo menos as seguintes versões de estações de trabalho Windows: 10 (ten) de 32 e 64-bit, 8 (eight) de 32 e 64-bits e 7 (seven) de 32 e 64-bit;

5.4.2.5. Implementar regras de controle de aplicações permitidas e bloqueadas para execução por meio do uso de agente, independentemente do acesso ao ativo ser realizado via mecanismo de Monitoramento Comportamental e Repositório Seguro ou diretamente no ativo.

5.4.2.6. Implementar regras de controle do nível de privilégio utilizado na execução das aplicações permitidas por meio do uso de agente, independentemente do acesso ao ativo ser realizado via mecanismo de Monitoramento Comportamental e Repositório Seguro ou diretamente no ativo.

5.4.2.7. Implementar controle de nível de privilégio independentemente da permissão que o usuário possua localmente no ativo ou no domínio, permitindo que usuários restritos executem atividades com nível administrativo.

5.4.2.8. Permitir atribuição granular para execução de aplicações com nível de privilégio administrativo, sem que esse privilégio seja global na máquina.

5.4.2.9. Implementar a verificação de *checksum* ou *hash* do arquivo, dos parâmetros permitidos e da assinatura de fabricante, para objetos reutilizáveis da solução.

5.4.2.10. Implementar o suporte ao nome exato da aplicação/arquivo/script e expressões regulares em qualquer formato, para objetos reutilizáveis da solução.

5.4.2.11. Utilizar eventos reportados na interface da ferramenta para novas políticas ou incluí-los em políticas existentes.

5.4.2.12. Impedir a desativação do agente sem autorização e/ou registro da atividade por meio da interface de gerência.

5.4.2.13. Disponibilizar modo de observação, em que não há bloqueios, mas há o registro das execuções e atividades dos usuários, facilitando a criação de políticas baseadas em comportamento conhecido.

5.4.2.14. Monitorar e exibir acessos e atividades realizadas na própria solução.

5.4.2.15. Deve permitir autorização de acesso às aplicações e arquivos, quando incluídos em regras, individualmente ou em grupos.

5.4.2.16. Possibilitar o monitoramento e a criação de vídeos de execução de procedimentos realizados por usuários, de acordo com políticas e regras configuradas.

5.4.2.17. Possibilitar ao usuário final a solicitação de liberação de atividades específicas por meio do agente.

5.4.2.18. Possibilitar a liberação emergencial da execução de comandos e elevação de privilégios sem desativar a solução, caso o usuário esteja off-line.

5.4.2.19. Implementar as regras de controle de acordo com características do usuário final, incluindo nome de usuário, grupos a que o usuário pertence e endereço IP.

5.4.2.20. Oferecer monitoramento de atividade maliciosa dos processos em execução, visando detectar tentativas de roubo de credenciais.

5.4.2.21. Caso o dispositivo não possa estar conectado de forma permanente ao mecanismo de Monitoramento Comportamental e Repositório Seguro da solução, deve, de forma autônoma e off-line, gerenciar as senhas das credenciais locais, aplicando políticas de randomização e sincronização das senhas definidas na central da solução.

5.4.2.22. Possibilitar a execução de aplicativos que precisam de privilégio de execução a usuários não-privilegiados.

5.5. Suporte Técnico Especializado.

5.5.1. A CONTRATADA deverá fornecer serviços de manutenção e suporte técnico pelo período de 30 (trinta) meses, contados da data da assinatura do contrato de suporte técnico especializado, contemplando o suporte técnico para os sistemas que compõem a solução de Gerenciamento de Acesso Privilegiado;

5.5.2. O serviço deve contemplar manutenção e suporte técnico para a Solução de Proteção e Auditoria do Uso de Credenciais – Monitoramento Comportamental e Repositório Seguro.

5.5.3. A CONTRATADA deverá prestar serviço de manutenção e suporte técnico destinados a:

5.5.3.1. Restabelecimento de serviços interrompidos ou degradados;

5.5.3.2. Solução de problemas de configuração e falhas técnicas nos serviços;

5.5.3.3. Esclarecimentos de dúvidas sobre configurações e utilização dos serviços;

5.5.3.4. Implementação de novas funcionalidades.

5.5.3.5. Entre outras situações correlatas às acima exemplificadas;

5.5.4. A CONTRATADA deverá atender as seguintes premissas:

5.5.4.1. Os serviços serão solicitados mediante a abertura de chamados a serem efetuados por técnicos do Tribunal, via chamada telefônica local ou gratuita, e-mail ou website, sem custos para a CONTRATANTE.

5.5.4.2. Não haverá limitação de quantidade de abertura de chamados para suporte.

5.5.4.3. O suporte deve estar disponível 24 (vinte e quatro) horas por dia, 7 (sete) dias por semana, nos 365 (trezentos e sessenta dias) do ano, sendo o Português Brasileiro o idioma de suporte técnico obrigatório.

5.5.4.4. Os serviços de suporte deverão ser prestados por técnicos devidamente capacitados nos respectivos componentes da solução. Caberá a contratada fornecer aos seus técnicos todas as ferramentas e os instrumentos necessários à execução dos serviços.

5.5.4.5. Todas as solicitações feitas pelo CONTRATANTE deverão ser registradas pela CONTRATADA em sistema informatizado para acompanhamento e controle da execução dos serviços.

5.5.4.6. O acompanhamento da prestação de serviço deverá ser através de um número de protocolo fornecido pela CONTRATADA, no momento da abertura da solicitação.

5.5.4.7. Dos prazos de atendimento:

5.5.4.8. A tabela abaixo descreve os prazos de atendimento que deverão ser cumpridos pela CONTRATADA, de acordo com a severidade de cada chamado aberto:

Tabela de Solução dos chamados			
Severidade	**Descrição**	**Tempo para primeiro contato após abertura do chamado**	**Tempo de resolução do chamado**
Urgente	Serviço crítico parado em produção.	30 minutos	Até 01 (uma) hora
Alta	Erros e problemas que estão impactando no ambiente de produção.	60 minutos	Até 04 (quatro) hora
Média	Problemas ou erros contornáveis que afetam o ambiente em produção, mas não possuem alto impacto.	90 minutos	Até 06 (seis) horas
Baixa	Problemas ou erros contornáveis que não impactam significativamente no ambiente em produção.	120 minutos	Até 08 (oito) horas
Informações	Consulta Técnica, dúvidas em geral, monitoramento.	150 minutos	Até 24 (vinte e quatro) horas

5.5.4.9. O prazo de atendimento deve começar a ser contabilizado a partir do momento de efetivação da abertura do suporte, através de telefone ou e-mail;

5.5.4.10. A CONTRATADA deve apresentar relatório de visita para cada solicitação de suporte on-site, contendo a data e hora da solicitação de suporte técnico, o início e o término do atendimento, identificação do problema, providências adotadas e demais informações pertinentes;

5.5.4.11. O relatório de visita deverá ser assinado pelo técnico responsável pela abertura do chamado e o fiscal do CONTRATANTE responsável pelo contrato;

5.5.4.12. O nível de severidade será informado no momento da abertura de cada chamado pelo técnico responsável do CONTRATANTE;

5.5.4.13. Todas as solicitações de suporte técnico devem ser registradas pela CONTRATADA para acompanhar e controlar a execução dos chamados;

5.5.4.14. O descumprimento dos prazos de atendimento implicará na aplicação de glosas conforme tabela abaixo:

Tabela de aplicação de Glosas		
Severidade	**Fórmula de cálculo da glosa**	**Limite da glosa**
Urgente	HS x 0,5% * VFM	20% da VFM
Alta	HS x 0,4% * VFM	15% da VFM
Média	HS x 0,3% * VFM	10% da VFM
Baixa	HS x 0,2% * VFM	10% da VFM
Informações	HS x 0,1% * VFM	10% da VFM
HS = Horas totais que extrapolaram o limite de resolução dos chamados, no caso de hora quebrada, será apurado o percentual da hora descumprida.		

VFM = Valor da Fatura Mensal para pagamento do serviço de suporte.
Em caso de descumprimento contumaz pela CONTRATADA nos prazos para atendimento do suporte técnico a fiscalização poderá adotar o entendimento de

5.5.4.15. A LICITANTE deve emitir relatório mensal em arquivo eletrônico ou em sistema de consulta online, com informações dos chamados da garantia abertos e fechados no período;

5.5.4.16. O relatório deve possuir os seguintes parâmetros:

5.5.4.16.1. Quantidade de ocorrências (chamados) registradas no período;

5.5.4.16.2. Número do chamado registrado e nível de severidade;

5.5.4.16.3. Data e hora de abertura;

5.5.4.16.4. Data e hora de início e conclusão do atendimento;

5.5.4.16.5. Identificação do técnico que fez o registro do chamado;

5.5.4.16.6. Descrição do problema;

5.5.4.16.7. Descrição da solução;

5.5.4.16.8. Lista de chamados concluídos fora do prazo de solução estabelecido.

5.5.4.17. Problemas cuja solução dependa de correção de falhas (bugs) ou da liberação de novas versões e patches de correção, desde que comprovados pelo fabricante da solução, não deverão se encaixar nos prazos estabelecidos acima;

5.5.4.17.1. A CONTRATADA deverá, de acordo com o nível de criticidade, prover solução paliativa para atender os problemas de falhas (bugs), atualizações ou patches de correção que ainda não foram disponibilizadas pela fabricante, no prazo de 24 (vinte e quatro) horas, para restabelecer o ambiente do CONTRATANTE;

5.5.4.17.2. A solução definitiva deverá ser disponibilizada no prazo máximo de 60 (sessenta) dias, sendo a CONTRATADA responsável pelos trâmites juntamente a fabricante da liberação das correções.

5.5.4.18. Nas manutenções que necessitem de intervenção para parada física ou reinicialização do equipamento, o CONTRATANTE deverá ser notificado previamente para que faça o agendamento da manutenção e aprovação;

5.5.4.19. As paradas de manutenção deverão acontecer fora do horário de expediente, de preferência após a 20 (vinte) horas devendo ser restabelecida antes das 8 (oito) horas da manhã do dia seguinte. Poderá ocorrer durante o dia da semana ou aos finais de semana, sem ônus para o CONTRATANTE;

5.5.4.20. Todo o procedimento de manutenção deverá ser documentado, explicando o passo a passo completo e fazendo registro das ocorrências incoerentes para subsidiar novas paradas que possam acontecer;

5.5.4.21. O relatório deverá ser assinado pelo fiscal técnico do contrato ou responsável pelo acompanhamento do serviço por parte do CONTRATANTE.

5.6. Treinamento técnico da Solução de Proteção e Auditoria do Uso de Credenciais.

5.6.1. O treinamento técnico da Solução de Proteção e Auditoria do Uso de Credenciais – Monitoramento Comportamental e Repositório Seguro será de, no mínimo, 40 horas, para turma de, no máximo, 10 alunos;

5.6.2. O treinamento, ou parte dele, poderá ser realizado no modelo telepresencial (online por videoconferência), em português, utilizando ferramenta própria disponibilizada pelo contratado (ex.: Cisco Webex, Adobe Connect, Google Meet, etc.), desde que autorizado pelo Contratante;

5.6.3. O Contratante disponibilizará os computadores a serem utilizados pelos participantes do curso;

5.6.4. A CONTRATADA disponibilizará material didático oficial do curso em formato digital (PDF) aos participantes e quaisquer conteúdos e ferramentas adicionais que venham a ser necessárias para o treinamento;

5.6.5. Caso não haja disponibilidade para realização nos modelos presencial ou tele presencial, a Contratada custeará os gastos de passagens e estadia para o centro de treinamento mais próximo de Brasília.

5.6.6. O treinamento deverá ser ministrado em português, por técnico certificado pelo fabricante da solução, e composto de aulas teóricas e práticas (*hands on*).

5.6.7. A CONTRATADA deverá confeccionar e disponibilizar aos participantes todo o material didático necessário ao treinamento.

5.6.8. A ementa e material utilizado no treinamento deverão ser enviados previamente ao Tribunal para avaliação e aprovação.

5.6.9. O treinamento deverá desenvolver o conhecimento e habilidades necessárias para fazer uso de todos os recursos disponíveis na Solução adquirida, incluindo, principalmente a utilização de chaves, configuração, proteção, monitoramento e demais atividades relacionadas à Solução de Proteção e Auditoria do Uso de Credenciais.

5.6.10. Ao final do treinamento, deverá ser realizada junto aos participantes uma avaliação do curso. As avaliações deverão ser preenchidas e assinadas pelos alunos e posteriormente entregues ao Tribunal para a assinatura do aceite da Ordem de Serviço do treinamento.

5.6.11. Caso o treinamento seja avaliado como insatisfatório pela maioria dos participantes da turma, o treinamento deverá ser refeito.

5.6.12. Será considerado insatisfatório o treinamento que obtiver maioria dos itens da avaliação de treinamento julgados como RUIM ou REGULAR, observadas todas as avaliações preenchidas.

5.6.13. O treinamento a ser refeito por ocasião de ter sido mal avaliado não pode gerar novas despesas para o CONTRATANTE.

5.6.14. Ao final do treinamento, cada participante deverá receber um certificado assinado pela CONTRATADA, contendo informações de data, carga horária, conteúdo ministrado, além do nome completo do instrutor, do aluno e da instituição que forneceu o curso, bem como o seu período.

5.6.15. A Contratada deverá fornecer certificado para cada aluno contendo identificação da instituição que forneceu o treinamento, nome do aluno, local do treinamento, período do treinamento, carga horária, nome do instrutor e conteúdo programático.

6. PROPOSTA DE MODELOS A SEREM UTILIZADOS

Os modelos a serem utilizados devem ser como os especificados no Registro de Preço do Tribunal Regional do Trabalho da 8ª Região.

7. INFORMAÇÕES COMPLEMENTARES

Não há

Belém, 15 de setembro de 2021

(ASSINATURA DOS MEMBROS DA EQUIPE DE PLANEJAMENTO DA CONTRATAÇÃO)