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

Estudos Preliminares Nº 56/2021 - PJPI/TJPI/PRESIDENCIA/STIC/GOVTIC/ACSTIC

ANÁLISE DE VIABILIDADE DA CONTRATAÇÃO (art. 14)

1. Requisitos da contratação

De início, faz-se imprescindível definir com base nas carências do TJPI quais as principais características que a solução deve atender. Nesse sentido e em atenção à Resolução CNJ nº 182/2013, procede-se à definição das necessidades mínimas que se espera atender com a aquisição da solução de TIC objeto deste Estudo.

1.1 Necessidades do negócio

Com vias a melhor instruir o processo em epígrafe, bem como subsidiar a confecção do Termo de Referência, procede-se à listagem das principais necessidades com suas respectivas funcionalidades a serem atendidas com a contratação pretendida.

1.1.1. Necessidade: Gerenciar os acessos privilegiados aos sistemas e plataformas existentes neste Tribunal.

1.1.1.1. Funcionalidade 1: Garantir que somente usuários legítimos possam ter **acesso privilegiado** aos sistemas e plataformas do TJPI;

1.1.1.2. Funcionalidade 2: Definir ponto central de administração de qualquer sistema;

1.1.1.3. Funcionalidade 3: Proteger os sistemas de acesso em caso de roubo de credenciais privilegiadas;

1.1.1.4. Funcionalidade 4: Auditar as atividades gerenciais às plataformas e sistemas do TJPI;

1.1.1.5. Funcionalidade 5: Criar ponto de autenticação centralizado para atividades de gerenciamento;

1.1.1.6. Funcionalidade 6: Permitir controle baseado em análise comportamental para acessos privilegiados bloqueando ações suspeitas;

1.1.1.7. Funcionalidade 7: Possuir criptografia para comunicação entre os componentes da solução;

1.1.1.8. Funcionalidade 8: Ser capaz de controlar, filtrar e criar regras de permissões com base nos riscos para as operações que um administrador pode executar;

1.1.1.9. Funcionalidade 9: Possuir ambiente seguro (cofre) com redundância para armazenamento das credenciais administrativas do TJPI;

1.1.1.10. Funcionalidade 10: Possuir interface gráfica e relatórios detalhados para gestão facilitada;

1.1.2. Atores envolvidos: para o projeto em epígrafe ficam destinadas as seguintes partes fundamentais:

1.1.2.1. Gerente de projetos da CONTRATANTE: servidor indicado pela autoridade competente do TJPI para liderar o projeto de contratação da solução bem como atestar a regularidade das fases pertinentes e manter contato direto com o preposto da CONTRATADA.

1.1.2.2. Gerente de projetos da CONTRATADA: preposto indicado pela empresa fornecedora da solução com funções de gerência e/ou liderança que deverá manter contato direto com o gerente de projetos da CONTRATANTE em todas as fases do projeto com o fito de garantir a regularidade da aquisição.

1.1.2.3. Analistas de TIC da STIC com a função de descrever os requisitos técnicos bem como testar e homologar a conformidade do fornecimento da solução em aderência aos padrões descritos.

1.2. Requisitos não funcionais/tecnológicos

1.2.1. Requisitos de capacitação:

Como se trata de solução altamente especializada que envolve tecnologias proprietárias e complexas, faz-se necessário capacitar a equipe do Setor de Infraestrutura e Segurança da Informação da STIC com o treinamento oficial da solução a ser adquirida.

Como medida de eficiência e em atenção à atual pandemia de COVID19, recomenda-se que a capacitação seja realizada de forma presencial nas dependências do TJPI ou ao vivo, na modalidade EAD. O instrutor deve possuir certificação oficial do fabricante da solução.

Caso o fabricante/importador não disponibilize treinamento no molde supra, deverá ser disponibilizado voucher ou documento equivalente para treinamento oficial do fabricante. Ademais, todo o material didático de apoio deverá ser fornecido pela CONTRATADA.

Poderá ser utilizada máquina virtual ou tecnologia equivalente. Entretanto, o treinamento nesses moldes deve simular em tempo real todas as funcionalidades, telas, configurações, recursos da solução. Não será admitido treinamento com base unicamente em apresentação de slides, vídeos, fotos ou equivalentes, devendo ser fornecido certificado ao final da capacitação.

1.2.2. Requisitos legais:

Esta contratação busca atender as necessidades do PJPI, obedecendo rigorosamente às legislações federal e estadual pertinentes, às Resoluções do CNJ, bem como aos instrumentos legais emitidos pelos órgãos avaliadores de conformidade como a Associação Brasileira de Normas Técnicas – ABNT, o Instituto Nacional de Metrologia, Qualidade e Tecnologia – INMETRO, Instituto Brasileiro de Meio Ambiente – IBAMA, dentre outros.

No que tange à legislação específica, não fora encontrada nenhuma observância obrigatória para o projeto em epígrafe.

1.2.3. Requisitos de manutenção:

1.2.3.1. Requisito 1: Garantia e suporte técnico por um período de **36 (trinta e seis) meses** para toda a solução adquirida (hardware, software e componentes correlatos), que deverá ser contado a partir da expedição do Termo de Recebimento Definitivo ou documento equivalente.

1.2.3.1.1. A garantia para toda a solução adquirida deverá ser oferecida pela CONTRATADA e/ou pelo fabricante, sob a supervisão e responsabilização da primeira.

1.2.3.1.2. O suporte técnico para toda a solução adquirida deverá ser oferecido pela CONTRATADA e/ou pelo fabricante, sob a supervisão e responsabilização da primeira, durante os 365 (trezentos e sessenta e cinco) dias do ano, na modalidade 24x7 (vinte e quatro horas por dia, sete dias por semana).

1.2.3.1.3. Durante o período de garantia, a CONTRATADA, independentemente de ser ou não fabricante da solução obriga-se a disponibilizar novas versões do software e corrigir, substituir e/ou reparar software/equipamentos, sem ônus para o TJPI, conforme os Níveis Mínimos de Serviço Exigidos para esta contratação.

1.2.3.1.4. As solicitações serão feitas mediante abertura de chamados através das ferramentas disponibilizadas para tal fim.

1.2.3.2. Requisito 2: **Níveis Mínimos de Serviços Exigidos (NMSE)**:

a) Os Níveis Mínimos de Serviços Exigidos (NMSE) serão classificados da seguinte forma:

i. Prazo de Atendimento: Tempo decorrido entre o envio da mensagem de chamado técnico e o início da atividade de suporte;

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;

iii. 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.

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

Nível de Severidade	Descrição	Prazo de Atendimento
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
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 (quatro) horas
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 em horário comercial.	06 (seis) horas

1.2.4. Requisitos temporais:

1.2.4.1. Planejamento do processo de aquisição por parte da equipe de planejamento da contratação: para garantir eficiência no processo de contratação, ficam definidos um prazo máximo de 15 (quinze) dias para cada uma das seguintes fases:

i. Planejamento interno da contratação a ser realizado pela equipe de contratação;

ii. Tramitação processual, incluindo aprovação da demanda por parte da autoridade competente;

iii. Formulação do edital de licitação e aprovação da minuta por parte da autoridade máxima do TJPI;

iv. Realização do certame licitatório e contratação da empresa vencedora.

1.2.4.2. 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 será definida a equipe do projeto com os respectivos gerentes de projeto da CONTRATANTE e da CONTRATADA, bem como os papéis a serem desempenhados por cada uma das partes.

1.2.4.3. Prazo de entrega da solução: a CONTRATADA deverá fornecer a solução no **prazo máximo de 60 (sessenta) dias** 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.

1.2.4.4.: Prazo 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 e no Termo de Referência no prazo máximo de 45 (quarenta e cinco) dias. Neste 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.

1.2.4.5. 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.

1.2.5. Requisitos de segurança

A solução deve estar em conformidade com o Sistema de Gestão de Segurança da Informação - SGSI e com a Política de Segurança da Informação – PSI, do Tribunal de Justiça do Piauí - **RESOLUÇÃO Nº 232/2021, DE 05 DE JULHO DE 2021**, bem como com os procedimentos e documentações exigidos na contratação.

Todas as informações consideradas sensíveis pelo TJPI deverão ser resguardadas por parte da CONTRATANTE não sendo permitido, em hipótese alguma, o compartilhamento, cópia, retirada, reprodução, carga, levantamento, entre outros, de informações oriundas dos sistemas informatizados e/ou bancos de dados institucionais sem a devida autorização prévia e expressa por parte da autoridade competente do TJPI.

São consideradas sensíveis, para fins de aplicação do item anterior, aquelas informações que por sua natureza são consideradas de interesse confidencial, restrita ou sigilosa como, por exemplo:

- Dados, informações, códigos-fonte, artefatos, contidos em quaisquer documentos e em quaisquer mídias, não podendo, sob qualquer pretexto ser divulgadas, reproduzidas ou utilizadas por terceiros sob pena de lei, independentemente da classificação de sigilo conferida pelo TJPI a tais documentos;
- Resultados, parciais ou totais, sobre produtos gerados;
- Programas de computador, seus códigos-fonte e códigos-objeto, bem como suas listagens e documentações;
- Toda a informação relacionada a programas de computador existentes ou em fase de desenvolvimento no âmbito do TJPI e rotinas desenvolvidas por terceiros, incluindo fluxogramas, estatísticas, especificações, avaliações, resultado de testes, arquivo de dados, versões “beta” de quaisquer programas, dentre outros;
- Documentos relativos à lista de usuários do TJPI e seus respectivos dados, armazenados sob qualquer forma;
- Metodologias e ferramentas de serviços, desenvolvidas pelo TJPI;
- Parte ou totalidade dos modelos de dados que subsidiam os sistemas de informações do TJPI, sejam eles executados interna ou externamente;
- Parte ou totalidade dos dados ou informações armazenados nas bases de dados que subsidiam os sistemas de informações do TJPI, sejam elas residentes interna ou externamente;
- Circulares e comunicações internas do TJPI;
- Quaisquer processos ou documentos classificados como RESTRITO ou CONFIDENCIAL pelo TJPI.

1.2.6. Requisitos sociais, ambientais e culturais

O fabricante da solução deverá atender aos critérios de sustentabilidade ambiental de que trata a Instrução Normativa SLTI/MPOG nº 01/2010, no que couber, quanto ao uso de materiais, observando que esses sejam constituídos, no todo ou em parte, por material reciclado, atóxico, biodegradável, conforme Normas ABNT NBR – 15448-1 e 15448-2.

Deverão ser observados os requisitos ambientais para a obtenção de certificação do Instituto Nacional de Metrologia, Normalização e Qualidade Industrial – INMETRO como produtos sustentáveis ou de menor impacto ambiental em relação aos seus similares.

1.3. Levantamento das alternativas disponíveis no mercado de TIC

1.3.1. Contextualização

Nos últimos anos registrou-se um aumento substancial de ataques a sistemas e plataformas tecnológicas nos mais diversos setores, incluindo órgãos públicos, visando a obtenção de dados e informações corporativos para fins ilícitos, que compreendem sequestro de dados, extorsão e venda das informações, dentre outros.

A pandemia do COVID-19 potencializou ainda mais esses ataques devido à mudança ocorrida na forma de prestação laboral, que passou a ser feita fora das instalações corporativas, aumentando assim o risco envolvido nos acessos dos colaboradores aos sistemas e ativos institucionais.

Nesse sentido, um dos principais alvos tem sido o roubo de credenciais, privilegiadas ou não. Conseguindo uma credencial com poucos privilégios os atacantes buscam ampliar o ataque, visando credenciais com maior privilégio, objetivando o controle total do ambiente da vítima. As credenciais privilegiadas encurtam esse caminho dos atacantes, permitindo um acesso direto ao controle dos sistemas, o que mostra que esse tipo de credencial configura a parte mais crítica e sensível relacionada ao ambiente computacional.

Por esse motivo o Gartner, renomado instituto mundial de pesquisa e consultoria na área de TIC, vem afirmando, desde 2019, no tocante à Segurança da Informação, 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]*

Exemplo recente que ocorreu no Superior Tribunal de Justiça, que sofreu um ataque cibernético no dia 03 de novembro de 2020, onde todos os arquivos do seu ambiente de servidores virtualizados foram criptografados, inclusive com tentativa de destruição do ambiente de backup, causando a indisponibilidade de praticamente todos os seus sistemas de TI. É importante frisar que o STJ não contava com uma solução de PAM (Gerenciamento de Acessos Privilegiados) no momento do incidente, tendo sido crucial a aquisição de uma para a restauração segura do ambiente, garantindo que somente os administradores possuíam acesso aos sistemas restaurados.

A contratação de uma solução que centralize e permita a **gestão dos usuários com acessos privilegiados** é, portanto, uma necessidade urgente, que objetiva oferecer melhor gestão e auditoria dos acessos à infraestrutura de TIC e das diversas plataformas existentes no TJPI.

Objetivando atender as necessidades do negócio e alinhado com os recursos orçamentários deste órgão, propõe-se esta aquisição, que já evidencia-se como indispensável para alcançar os objetivos estratégicos traçados no PLANO DIRETOR DE TECNOLOGIA DA INFORMAÇÃO E COMUNICAÇÃO - PDTI TJPI 2021-2022 (SEI 2414707) e a ESTRATÉGIA NACIONAL DE TECNOLOGIA DA INFORMAÇÃO E COMUNICAÇÃO DO PODER JUDICIÁRIO - ENTIC-JUD 2021-2026.

Revela-se portanto, um dever do TJPI de formalizar e conduzir tal aquisição, estando a mesma compreendida no macroprocesso de segurança da informação, que objetiva garantir 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.

1.3.2 Soluções

Considerando os requisitos básicos dessa demanda, visualizou-se no mercado de TIC três modalidades de soluções possíveis:

1.3.2.1. Solução de Gestão de Identidade e Acesso (GIA):

As soluções de GIA (Gestão de identidade e Acesso), tem o objetivo de automatizar e auditar as concessões de acesso à credenciais de usuários dentro do ambiente de rede para que, de forma centralizada, os processos de autenticação sejam automatizados. Podendo assim, os acessos a diversos sistemas e ativos serem autorizados ou revogados de forma automatizada. Permite realizar o inventário de sistemas e perfis de acesso e identidade, definição de fluxos e responsabilidades para cada usuário e/ou grupo de usuários, fluxos de aprovação para atividades através de *sponsors* ou abertura de *tickets* de mudança.

Essa solução permite a auditoria automatizada para que quando haja alguma credencial revogada ou não aprovada, esta seja bloqueada automaticamente e seja gerado um registro (log do evento) para fins de controle. E por fim, permite uma organização através de perfis de negócios (*Role Based Access Control*), permitindo que as credenciais tenham um pacote de privilégios e direitos em múltiplos sistemas, função esta que elimina a necessidade de novas aprovações junto a administração para elevação de privilégios.

1.3.2.2. Solução de PAM (*Privileged Access Management* - "Gerenciamento de Acesso Privilegiado")

As soluções de PAM permitem a gestão de credenciais de contas privilegiadas, protegendo-as em um repositório seguro (cofre de senhas), permitem também a gravação das sessões privilegiadas e a trilha de ações dos usuários com relatórios. Proativamente é possível mitigar ações que contém ameaças realizadas pelos usuários através de análise comportamental e proteção para sistemas críticos. Possuem a capacidade de gerência de acesso remotos seguros, troca de senhas, rotação de chaves criptográficas (SSH) e de credenciais/*secrets* embarcadas nas aplicações containerizadas e tradicionais.

Além disso, implementam proteção para as estações de trabalho, controladores de domínios e servidores, com a possibilidade de elevação de privilégio para determinados serviços e remoção de administração local para mitigar roubo de credencias (técnica de *overpass-the-hash*).

1.3.2.3. Soluções com "Software Livre"

Tratam-se de soluções unicamente para a finalidade de cofre de senhas, sem possibilidades de recursos de auditoria, integração com os ativos existentes, análise comportamental, agentes para proteção etc. Algumas soluções como KeePass, bitwarden e Passbolt foram avaliadas durante este estudo.

1.3.3. Comparativo entre as Soluções

As "**Soluções com Software Livre**", não atendem aos requisitos técnicos do projeto por não possuírem recursos de auditoria, integração com os ativos existentes, análise comportamental, agentes para proteção dos controladores de domínio, agentes para proteção dos servidores e estações de trabalho, integração com aplicações containerizadas, proteção para aplicações que possuem credenciais embarcadas em texto claro, etc. Ademais, soluções baseadas em software livre dependem do trabalho não remunerado da "comunidade" de desenvolvedores, portanto, não seria possível manter central de atendimento ao usuário com prazos de SLA, ou sequer garantir que o sistema esteja livre de vulnerabilidades ou falhas. Fica evidente que, devido à complexidade e a criticidade que se espera desta solução para um ambiente de grande porte como deste Tribunal de Justiça, não é possível considerar as soluções baseadas em software livre que estão disponíveis atualmente.

De forma sucinta, elencamos mais alguns pontos que torna essa solução inviável:

- Depende para o seu desenvolvimento de pessoas que não possuem vínculo ou acesso aos códigos das soluções e sistemas corporativos, para dessa forma, criar a melhor estratégia de mitigação e resposta às vulnerabilidades e proteção contra os ataques aos controladores de domínio;
- Utiliza métodos abertos para integração às soluções de autenticação do tipo corporativas, dependendo de uma comunidade para, caso essas soluções sejam modificadas pelos seus fabricantes, realizar a alteração nos métodos de integração, causando assim períodos inoperantes e ou falhas de segurança em sua operação;

- Se limita ao gerenciamento das contas privilegiadas, não realizando controle granular, filtro, nem regras de bloqueio ou terminação de sessões com base nos riscos dos comandos ou das aplicações;
- Não possui proteção para credenciais embarcadas nos *containers* e aplicações tradicionais;
- Não possui proteção para estações de trabalho e servidores.

A "**Solução de Gestão de Identidade e Acesso (GIA)**" não atende a todas as demandas de segurança necessárias ao projeto descrito neste estudo, tais quais:

- Não possui nativamente a proteção contra ataques avançados aos controladores de domínio;
- Não contempla análise comportamental das credenciais administrativas;
- Não permite a elevação de privilégio de uma credencial comum para que ela tenha acesso privilegiado à apenas uma parte de um sistema;
- Se limita apenas ao gerenciamento de credenciais, não entregando solução efetiva de cofre centralizado para armazenamento e troca dinâmica de senhas;
- Apesar de existir os provisionamentos através de perfis de negócios ou de perfis padrão, os acessos aos ativos de rede e sistemas, ainda podem ser feitos de forma local, desde que o usuário possua a senha atual do equipamento, o que infringe um ponto crítico da segurança.

A **Solução de PAM (*Privileged Access Management* - "Gerenciamento de Acesso Privilegiado")**, item 1.3.2.2. deste documento, contempla, dentre outras características:

- **Cofre de senhas:** Armazenamento seguro de credenciais e senhas incluindo gerenciamento e proteção de credencias críticas através de monitoramento de sessões;
- **Limite de uso:** limitação do uso da conta com base em um tempo específico e/ou uma quantidade de aprovação determinada; Definição de grupos para segregação de acessos com base em perfis de usuário; Flexibilidade no processo de aprovação para o acesso a contas privilegiadas (acessos pré-aprovados, acessos com aprovação única ou com aprovação múltipla), etc;
- **Discovery:** Descoberta automática de credenciais privilegiadas que possam estar no sistema sem o conhecimento do administrador; Troca de senha automatizada nas principais plataformas tecnológicas de rede, servidores, bancos de dados, aplicações web e equipamentos de segurança;
- **Visibilidade:** visão do que acontece quando um acesso é requisitado, aprovado e executado; Integração com os principais serviços de diretório para gerenciamento de Grupos e Perfis de acesso, e assim controlar a utilização de credenciais;
- **Auditoria:** gravação de evidências de acessos realizados de forma correta ou não; Revisão de sessão realizada através da solução, ou exportação para formato de vídeo.

Dessa forma **contempla** todas as funcionalidades requeridas nos itens 1.1.1.1 a 1.1.1.10, necessárias para cumprimento da demanda requisitada, **atendendo** ao objetivo da contratação: "Gerenciar os acessos privilegiados aos sistemas e plataformas existentes neste Tribunal".

1.3.4. Análise dos custos totais das soluções de TIC identificadas (art. 14, III)

Considerando a Pesquisa de Preços 91 (SEI Nº 2629951), foram encontrados os seguintes valores:

GRUPO	ITEM	DESCRIÇÃO	CATMAT/CATSER	Preço considera
1	1	Licenciamento de uso para solução de Gerenciamento de Acessos Privilegiados *(Privileged Access Management - PAM),* com garantia de 36 meses	27472	R$ 847.(
	2	Serviço de Instalação e Configuração da Solução de Gerenciamento de Acessos Privilegiados *(Privileged Access Management - PAM)*	26972	R$ 14.4
	3	Treinamento de Administração da Solução	384-0	R$ 11.1
	4	Treinamento de Operação da Solução	384-0	R$ 11.1
	5	Suporte Técnico Especializado	27022	R$ 110.5
VALOR TOTAL ESTIMADO PARA A CONTRATAÇÃO				**R$ 995.(

2. Detalhamento das alternativas existentes

DETALHAMENTO DAS ALTERNATIVAS EXISTENTES				
Solução de PAM (*Privileged Access Management* - "Gerenciamento de Acesso Privilegiado")				
Requisito	**Nome da Solução**	**SIM**	**NÃO**	**N**
A Solução encontra-se implantada em outro órgão ou entidade da Administração Pública (art. 14, II, a)?	CyberArk	x		
	BeyondTrust	x		
	senhasegura	x		
A Solução encontra-se implantada em outro órgão ou entidade do Judiciário? (Opcional)	CyberArk	x		
	BeyondTrust	x		
	senhasegura	x		
A Solução existe no Portal de Software Público Brasileiro (art. 14, II, b)?	CyberArk		x	
	BeyondTrust		x	
	senhasegura		x	
A Solução é um software livre ou software público (art. 14, II, c)?	CyberArk		x	
	BeyondTrust		x	

DETALHAMENTO DAS ALTERNATIVAS EXISTENTES				
Solução de PAM (*Privileged Access Management* - "Gerenciamento de Acesso Privilegiado")				
	senhasegura		x	
A Solução observa as políticas, premissas e especificações técnicas definidas no Modelo Nacional de Interoperabilidade (MNI) do Poder Judiciário (art. 14, II, d)?	CyberArk			
	BeyondTrust			
	senhasegura			
Caso haja necessidade de certificação digital, a Solução é aderente às regulamentações da ICP-Brasil (art. 14, II, e)?	CyberArk			
	BeyondTrust			
	senhasegura			
A Solução é aderente às orientações, premissas e especificações técnicas e funcionais do Modelo de Requisitos para Sistemas Informatizados de Gestão de Processos e Documentos do Judiciário – MoReq-Jus (art. 14, II, f)?	CyberArk			
	BeyondTrust			
	senhasegura			

3. Justificativa da solução escolhida (art. 14, IV)

3.1. Solução escolhida: Solução de PAM (*Privileged Access Management* - "Gerenciamento de Acesso Privilegiado")

3.2. Descrição (art. 14, IV, a)

Trata-se de contratação de solução de segurança de infraestrutura de TIC para o Tribunal de Justiça do Estado do Piauí, tendo em vista a necessidade de uma solução de gerenciamento de credenciais para usuários com acesso privilegiado à esta infraestrutura, visando proteger controladores de domínios, servidores de rede, sistemas operacionais, bancos de dados e demais ativos de rede.

A necessidade é de uma solução que seja o mais abrangente possível no que diz respeito ao gerenciamento de credenciais, o que mostra que, para o pleno atendimento das necessidades do TJPI, apenas uma solução do tipo PAM (*Privileged Access Management* - "Gerenciamento de Acesso Privilegiado") se mostra adequada, conforme explicado no **comparativo entre soluções (item 1.3.3)** e demonstrado abaixo de forma mais clara.

Funcionalidades necessárias para atendimento das necessidades do negócio	Gerenciamento de Acessos Privilegiados	I
1: Garante que somente usuários legítimos possam ter acesso privilegiado aos sistemas e plataformas do TJPI;	SIM	
2: Define ponto central de administração de qualquer sistema;	SIM	
3: Protege os sistemas de acesso em caso de roubo de credenciais;	SIM	
4: Audita os acessos às plataformas e sistemas do TJPI;	SIM	
5: Cria ponto de autenticação centralizado;	SIM	
6: Permite controle baseado em análise comportamental para acessos privilegiados bloqueando ações suspeitas;	SIM	
7: Possui criptografia para comunicação entre os componentes da solução;	SIM	
8: É capaz de controlar, filtrar e criar regras de permissões com base nos riscos para as operações que um administrador pode executar;	SIM	
9: Possui ambiente seguro (cofre) com redundância para armazenamento das senhas administrativas do TJPI;	SIM	
10: Possui interface gráfica e relatórios detalhados para gestão facilitada;	SIM	

Ainda correlacionando com o ataque sofrido pelo STJ, o que ocorreu foi que, antes do ataque, o tribunal dispunha de proteção de suas credencias de acessos privilegiados apenas baseada em padrões de senha de alta complexidade, o mesmo utilizado no TJPI atualmente .

O ataque aconteceu por um falha de segurança onde uma credencial privilegiada foi comprometida e o atacante conseguiu fazer a escalação de privilégios comprometendo outras credencias e plataformas.

Após o ataque o STJ desligou sua conectividade de rede tirando o tribunal do "ar" e com a ajuda de empresas fornecedoras de soluções de segurança, dentre elas, de soluções de PAM, ajustou na emergência do caso, uma Prova de Conceito (PoC), para promover a restauração do ambiente, que englobou aproximadamente 500 servidores virtuais e consistiu em isolar cada servidor recuperado em uma rede segura, verificando-se eventuais contaminações e procedendo-se com sua limpeza.

Adicionalmente foi necessário modificar e controlar todas as credenciais de acesso aos sistemas, especialmente as contas de administração, recadastrando as senhas de todas as credenciais de rede dos usuários daquele órgão em um cofre de senhas seguro, disponível e íntegro. Esta etapa não seria possível sem as funcionalidades de uma ferramenta de Gerenciamento de Acessos Privilegiados (*Privileged Access Management - PAM).*

Posteriormente, o STJ adquiriu uma solução de PAM através de licitação (P.E. 22/2021 UASG 50001), implementando uma solução moderna, segura, íntegra, auditável e com monitoramento, aumentando o seu nível de segurança no gerenciamento dos acessos privilegiados às suas plataformas.

Este estudo mostra que uma solução desse tipo é imprescindível para evitar que uma credencial privilegiada seja explorada, à medida que implementa todas as funcionalidades apresentadas no quadro acima, sendo uma ferramenta fundamental para garantir que somente as pessoas autorizadas (administradores da infraestrutura) possam ter acesso privilegiado às plataformas de sustentação da instituição.

Considerando o risco iminente de novos ataques ao judiciário, faz-se necessário manter no TJPI medidas de proteção ao ambiente, dentre elas a que fora tomada no STJ para proteção de suas credenciais de acesso privilegiado, o que inclui tanto as novas regras de uso dos recursos computacionais através da

Política de Segurança da Informação do TJPI - **RESOLUÇÃO Nº 232/2021, DE 05 DE JULHO DE 2021**, quanto as novas soluções e serviços que estão sendo propostos pelo Comitê Gestor de Segurança da Informação do Tribunal e estão contempladas no Plano Diretor de Tecnologia - PDTI 2021/2022.

Sendo assim, mostra-se necessário que sejam tomadas medidas adequadas que visem o enfrentamento da exposição do ambiente a riscos de ataques da mesma natureza sofrida pelo STJ, como também de outros tipos de ataques que possam comprometer os sistemas através da exploração de credenciais privilegiadas.
Portanto, é evidente a necessidade de aquisição de uma solução de PAM, objetivando garantir que os acessos privilegiados aos recursos tecnológicos do TJPI sejam seguros, auditados e monitorados.

3.3. Composição da solução (art. 14, IV, a):

Lista-se, abaixo, os itens que deverão compor a solução: 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.

GRUPO	ITEM	DESCRIÇÃO
1	1	Licenciamento de uso para solução de Gerenciamento de Acessos Privilegiados *(Privileged Access Management - PAM),* com garantia de 36 meses
	2	Serviço de Instalação e Configuração da Solução de Gerenciamento de Acessos Privilegiados *(Privileged Access Management - PAM)*
	3	Treinamento de Administração da solução para no mínimo 4 (quatro) participantes, em turma única, nas dependências do TJPI (ou "ao vivo" na modalidade EAD), cobrindo todas as funcionalidades da ferramenta
	4	Treinamento de Operação da solução para 10 (dez) participantes, em turma única, nas dependências do TJPI (ou "ao vivo" na modalidade EAD), cobrindo todas as funcionalidades para operação da ferramenta
	5	Suporte Técnico especializado

3.4. Alinhamento em relação às necessidades (art. 14, IV, b)

Em todas as soluções de PAM pesquisadas, foi possível identificar o atendimento das funcionalidades exigidas no item **1.1 Necessidades do negócio** deste documento.

No tocante aos requisitos não tecnológicos, afirme-se que todos os possíveis fabricantes de soluções de PAM utilizam tecnologias e metodologias próprias o que faz necessário que, independentemente do vencedor de possível certame licitatório, a equipe técnica da STIC do TJPI seja treinada na operação e configuração da solução com vias a garantir a perfeita operacionalização da mesma.

Ainda, todas as soluções são aderentes aos demais requisitos constantes no item **1.2** deste Estudo, haja vista que a solução segue padrões bem definidos no mercado de TIC.

3.5. Benefícios esperados (art. 14, IV, 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.

3.6. Relação entre a demanda prevista e a quantidade a ser contratada (art. 14, IV, d)

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 operação e de administração da ferramenta.

Em todas as soluções encontradas no mercado o licenciamento é baseado no quantitativo de dispositivos que terão suas credencias de acesso privilegiadas gerenciados pela solução.

Desta forma, procedemos com a análise do quantitativo necessário para o atendimento imediato do cenário atual do TJPI, bem como a previsão de expansão para os próximos 36 meses (duração esperada para essa contratação, com possibilidade de extensão). As informações estão apresentadas na tabela abaixo:

CENÁRIO ATUAL DO TJPI		
ITEM	**QUANTIDADE APROXIMADA**	**DESCRIÇÃO**
Dispositivos de rede: LAN, WAN, WI-FI, Firewalls, IPS, AntiSpam e Filtro de conteúdo	200	Soma de 100 switches + 50 pontos de acesso wifi instalados na Sede, Fórum e Anexo + cerca 50 dispositivos (switches, firewall, storages, rede SAN, etc, instalados Sala Cofre.
Servidores: hipervisor Vmware ESXI/VMs, hipervisor Hyper-V/VMs, Windows Server 2003, 2008 R2, 2012 e superiores, Linux CenOS, HREL, Debian e Ubuntu	220	200 máquinas virtuais (Windows, Linux, Appliances, etc em ambiente Vmware) + 20 servidores físicos (DELL e HPE), instalados na Sala Cofre

Instância de banco de dados MS SQL Server 2008 R2 ou superior, Postgres e MySQL	35	06 MS SQL Server 2014 SP2 ou superior, +14 Postgres +15 MySQL
Instâncias de aplicações/serviços corporativos/senhas hardcoded	140	Cerca de 100 contextos + 40 aplicações em subdomínios
Usuários com acesso à dispositivos geridos pela solução	0	Hoje todos os acessos são realizados diretamente aos dispositivos. Deverá ser necessário no mínimo o total de colaboradores da STIC (analistas e técnicos de suporte da capital e do interior) atualmente cadastrados no Sistema Intranet (cerca de 80 pessoas)
Quantidade de acessos simultâneos à ferramenta PAM	0	Hoje não temos a solução implantada no TJPI. Deverão ter acesso a ela todos os colaboradores da STIC (analistas e técnicos de suporte da capital e do interior, com exceção dos atendentes administrativos)
Workstations (Windows)	2700	Quantidade aproximada de desktops ativos em toda rede do TJPI (capital e interior)
Servidores Microsoft IIS, Apache, Jobss, Wildfly, Glassfish, etc	80	Quantidade aproximada de servidores WEB (Apache, Tomcat, Wildfly, etc) executando as diversas aplicações e sistemas do TJPI
Horas de gravação diária/retenção	0	Atualmente nenhum acesso é gravado

É apresentado abaixo o cenário proposto (que será levado em consideração para a composição do termo de referência) baseado na expectativa de crescimento do ambiente do TJPI para cada um dos itens:

CENÁRIO PROPOSTO PARA A CONTRATAÇÃO		
ITEM	**QUANTIDADE ESTIMADA**	**DESCRIÇÃO**
Dispositivos de rede: LAN, WAN, WI-FI, Firewalls, IPS, AntiSpam e Filtro de conteúdo	280	200 atuais + cerca de 80 dispositivos de rede da Nova Sede do TJPI
Servidores: hipervisor Vmware ESXI/VMs, hipervisor Hyper-V/VMs, Windows Server 2003, 2008 R2, 2012 e superiores, Linux CenOS, HREL, Debian e Ubuntu	300	220 atuais + 80 (previsão de crescimento médio de 12% ao ano, aproximadamente 27 novos servidores / ano)
Instância de banco de dados MS SQL Server 2008 R2 ou superior, Postgres e MySQL	50	35 atuais + 15 (previsão de crescimento médio de 12% ao ano, aproximadamente 05 novas instâncias / ano)
Instâncias de aplicações/serviços corporativos/senhas hardcode	200	140 atuais + 60 (previsão de crescimento aproximado de 20 novas aplicações/serviços / ano)
Usuários com acesso à dispositivos geridos pela solução	100	80 colaboradores da STIC + 20 (expansão para 03 anos)
Quantidade de acessos simultâneos à ferramenta PAM	80	Quantidade de analistas e técnicos de suporte (da capital e do interior) que farão uso simultâneo da ferramenta
Workstations (Windows)	3000	2700 atuais + 300 (previsão de expansão)
Servidores Microsoft IIS, Apache, Jobss, Wildfly, Glassfish, etc	100	80 atuais + 20 (previsão de expansão)
Horas de gravação diária/retenção	6 horas por dia / 120 dias	Retenção prevista para análise de acesso/logs. Na Política de Segurança da Informação do TJPI ainda não há o anexo referente ao prazo para armazenamento de logs de acesso. Desta feita, baseamos esse número na média dos quantitativos solicitados pelo STF (SEI N. 2644249) e pelo STJ (SEI N. 2641685) em seus processos de aquisição de Solução de PAM. Ainda dizer que há a possibilidade de implementação da solução em ambiente virtual e essa quantidade poderá ser aumentada/diminuída quando sair a definição deste tema na PSI do TJPI. E que esse valor de retenção não é fator preponderante para definição do preço da solução.

A tabela acima, com exceção da coluna descrição, (por se tratar de informações internas do órgão) será colacionada no descritivo técnico dos itens que compõem a solução no Termo de Referência (SEI 2641675).

Sendo assim, em resumo, para atender ao cenário do TJPI, resta necessário a aquisição dos seguintes itens com seu respectivo quantitativo:

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

Após criteriosa análise das contratações públicas similares, bem como da(s) proposta(s) orientativa(s) de preços que ajudaram na composição do item **1.3.4. Análise dos custos totais das soluções de TIC identificadas (art. 14, III),** esta equipe de planejamento da contratação verificou que a adesão à ATA DE REGISTRO DE PREÇOS N.º 001/2021 da FUNDAÇÃO UNIVERSIDADE FEDERAL DO AMAPÁ - UNIFAP (SEI 2842190) é **mais vantajosa para o TJPI** pelos motivos expostos abaixo:

- **Vantajosidade econômica**

  A adesão à ARP da UNIFAP (SEI 2842190) se demonstrou **mais vantajosa economicamente**, já que de acordo com o item **1.3.4. Análise dos custos totais das soluções de TIC identificadas (art. 14, III)** o valor total estimado para a contratação **(R$ 995.011,52) está acima** do valor da proposta de preços (SEI 2857029) e respectiva documentação (SEI 2857058) necessária para adesão à ARP da UNIFAP (SEI 2842190), feita pela licitante vencedora da ARP, APPROACH TECNOLOGIA LTDA, recebidos por e-mail (SEI 2857127), onde são contemplados todos os itens exigidos no Termo de Referência (SEI 2641675) pelo valor total de **R$ 899.000,00.**

- **Celeridade no processo de contratação**

  Tendo em vista que processos internos e externos de licitação demandam tempo e engajamento de inúmeras equipes do órgão contratante e levando em consideração que a solução de segurança da informação objeto dessa contratação é de suma importância para a **proteção dos acessos privilegiados das plataformas críticas do TJPI**, que precisam ser protegidas de forma mais adequada o mais rápido possível, é imprescindível que o processo de aquisição seja feito da forma mais célere possível, o que torna a adesão à ARP da UNIFAP (SEI 2842190) **mais vantajosa para o TJPI em relação ao tempo**, já que diminui os possíveis percalços que podem acontecer numa licitação como pedidos de esclarecimentos, impugnações, judicializações, etc.

- **A solução da fabricante CyberArk, objeto da ARP, é considerada atualmente umas das melhores, figurando como principal líder neste segmento do mercado.**

  De acordo com órgãos avaliadores a nível mundial, dentre eles o Gartner, que é uma das principais empresas mundiais especializadas em pesquisa e consultoria em tecnologia da informação, cuja missão consiste em gerar informações, métricas e análises a respeito de tecnologia para que seus clientes tomem decisões estratégicas, a solução CyberArk, objeto da ARP da UNIFAP (SEI 2842190), **é líder no ramo de segurança e proteção de acessos privilegiados com a melhor avaliação em 2021**.

A solução CyberArk foi estudada a fundo por esta equipe de planejamento da contratação e atende plenamente às necessidades relacionadas a proteção dos acessos privilegiados do TJPI à medida que proporciona uma série de proteções dentre as quais:*

- **CyberArk Core Privileged Access Security Solution**
  - A plataforma unifica as funções de cofre de senha, gerenciamento de sessões de administração do sistema e prevenção a ameaças. A plataforma abrange também funcionalidades como:
- **Discovery**
  - Varredura, classificação e aplicação de políticas de credenciais privilegiadas.
- **Isolamento de credenciais e sessões**
  - Restringe acesso a ativos de informação críticos.
- **Gravação e auditoria**
  - Para sessões com acessos privilegiados.
- **Monitoramento, mitigação e remediação de ameaças**
  - Identificação rápida de comportamentos de risco minimizam tempo de resposta.

- **A solução da Cyberark possui integração com o firewall Palo Alto em uso no TJPI**

Outro ponto importante a se considerar é a integração da solução CyberArk com o firewall Palo Alto (instalado e em uso no TJPI) conforme URL da documentação oficial:

https://docs.cyberark.com/Product-Doc/OnlineHelp/Idaptive/Latest/en/Content/Applications/AppsWeb/PaloAltoNetworks.htm

Com essa integração o SAML do CyberArk pode ser utilizado para SSO na interface Web do firewall da Palo Alto, Global Protect Gateways e Portais.

Desta forma, a solução CyberArk **possibilita um adicional de segurança no processo de autenticação dos acessos privilegiados às ferramentas disponíveis no firewall do TJPI e na sua própria interface WEB**.

- **O valor para adesão à ARP está abaixo do orçamento estimado do TJPI para esta contratação**

O valor estimado para essa contratação no PDTI 2021-2022 (SEI 21.0.000031573-4, item **9. INVESTIMENTOS EM TIC, subitem 9.1. Infraestrutura de TIC / Segurança da Informação)** é o seguinte:

Item	Grau de Jurisdição	Valor Estimado (R$)
Ferramenta para Gerenciamento de Acessos Privilegiados	2°	R$1.000.000,00

Dessa forma, o valor para adesão à ARP da UNIFAP (SEI 2842190) de acordo com a proposta de preços (SEI 2857029) e respectiva documentação (SEI 2857058) necessária para à adesão, feita pela licitante vencedora, APPROACH TECNOLOGIA LTDA no valor de R$ 899.000,00, está abaixo do valor estimado no PDTI 2021-2022, constituindo-se em **mais um ponto de vantajosidade tendente a viabilizar uma possível adesão**.

CONCLUSÃO

A adesão à ARP da UNIFAP (SEI 2842190) atende aos requisitos desta contratação e enfatizamos que, dentre os motivos de vantajosidade para a adesão relacionados acima, a respectiva proposta de preços (SEI 2857029) da APPROACH TECNOLOGIA LTDA, licitante vencedora no certame, **está com o valor abaixo (R$ 899.000,00)** do valor estimado para esta contratação, **R$ 995.011,52**.

Portanto, esta equipe de contratação **sugere que seja feita a adesão** à ATA DE REGISTRO DE PREÇOS N.º 001/2021 da FUNDAÇÃO UNIVERSIDADE FEDERAL DO AMAPÁ - UNIFAP (SEI 2842190), de acordo com a proposta de preços (SEI 2857029) e respectiva documentação (SEI 2857058) necessária para adesão, enviados pela APPROACH TECNOLOGIA LTDA, licitante vencedora no certame da UNIFAP, conforme orientação descrita no item **4. DA ADESÃO À ATA DE REGISTRO DE PREÇOS** do SEI 2842190.

Sendo assim, o valor considerado para esta contratação levando em consideração a adesão à ATA DE REGISTRO DE PREÇOS N.º 001/2021 da FUNDAÇÃO UNIVERSIDADE FEDERAL DO AMAPÁ - UNIFAP (SEI 2842190) é apresentado abaixo:

ITEM ARP	DESCRIÇÃO	QTDE	VALOR UNITÁRIO	VALOR TOTAL
ITEM 1	CORE PAS 50 /ALERO* Solução de Segurança para Sistemas Críticos -Análise comportamental e Resposta a Ações de Risco, comgarantia pelo período de 36 meses. Subscrição 3 anos para acessos remotos seguros sem VPN, com SSO e MFA adaptativo dos usuários privilegiados a ILIMITADOS sistemas-alvo, com proteção de todas as credenciais (incluindo local admin de estações de trabalho), gravando e monitorando sessões e comportamentos e respondendo a ações de alto risco, sem instalação de agentes. Inclui até 6 Cofres digitais em HA, Gateways ilimitados (Win, SSH) e Analytics de Ameaças para 3 ambientes iguais (Prod, Homolog e Testes).	1	R$ 840.000,00	R$ 840.000,00
ITEM 8	Serviço de instalação e configuração para Solução de Segurança para Sistemas Críticos (CORTESIA)	14	R$ 0,00	R$ 0,00
ITEM 9	Treinamento oficial com o(s) fabricante(s) da Solução de Segurança para Sistemas Críticos (CORTESIA - 50% de desconto)	01	R$ 118.000,00	R$ 59.000,00
			TOTAL	**R$ 899.000,00**

- ITEM 1 da ARP - equivale ao **ITEM 1** - Licenciamento de uso para solução de Gerenciamento de Acessos Privilegiados *(Privileged Access Management - PAM),* com garantia de 36 meses e **ITEM 5** - Suporte Técnico especializado, do cenário do TJPI.
- ITEM 8 da ARP - equivale ao **ITEM 2** - Serviço de Instalação e Configuração da Solução de Gerenciamento de Acessos Privilegiados (Privileged Access Management - PAM), do cenário do TJPI.
- ITEM 9 da ARP - equivale aos **ITENS 3 e 4** - Treinamentos de Administração e Operação da Solução, do cenário do TJPI

Além disso, de acordo com a proposta de preços (SEI 2857029) estão sendo oferecidas CORTESIAS ADICIONAIS para o atendimento de 100% do que está sendo exigido no Termo de Referência (SEI 2641675) bem como **possibilitarão proteção adicional ao ambiente do TJPI**, caso seja feita a adesão à respectiva ARP.

- CORTESIAS ADICIONAIS:
  - 2 (duas) licenças DC PROTECTION
  - CORE PAS ALERO – adicional de 30 usuários, totalizando 80 usuários ADMIN;
  - 10 (dez) Licenças – Harded Coded;
  - 50% de desconto no treinamento oficial 40 horas para até 20 participantes indicados pelo TJPI;
  - Garantia e suporte técnico já contemplado no CORE (ITEM 01) da solução por 36 meses;
  - A solução atende a todas demandas principais do conceito de PAM por meio da entrega não só do pilar principal de PASM (Privilege Accounts and Session Management), mas também de capacidades de proteção automáticas contra movimentação lateral/vertical de Ransomwares;
  - Instalação e configuração em 14 dias;

4. Necessidades de adequação do ambiente do órgão (art. 14, V)

Tipo	Necessidade
Infraestrutura tecnológica (art. 14, V, a)	Não há.
Infraestrutura elétrica (art. 14, V, b)	Não há.

Logística de implantação (art. 14, V, c)	Após a assinatura do contrato será realizada uma Reunião de Alinhamento com a CONTRATADA para definição das etapas de implantação com os respectivos prazos para entrega e requisitos para aceite.
Espaço físico (art. 14, V, d)	Não há.
Mobiliário (art. 14, V, e)	Não há.
Impacto ambiental (art. 14, V, f)	Não há.

SUSTENTAÇÃO DO CONTRATO (art. 15)

5. Recursos necessários à continuidade do objeto contratado (art. 15, I)

5.1 Recursos materiais:

A aquisição da solução em epígrafe não necessita de recursos materiais adicionais aos que serão minuciosamente definidos no Termo de Referência que será elaborado com base neste Estudo.

5.2 Recursos humanos:

5.2.1 Recurso 1: Equipe de Infraestrutura e Segurança da Informação da STIC.

5.2.1.1 Função: Operar e manter a solução de TIC em aderência às regras da governança e da alta administração do TJPI.

5.2.1.2 Responsabilidades:

- Manter a solução de TIC em funcionamento, possibilitando que os acessos privilegiados aos recursos tecnológicos do TJPI possam ser seguros, auditados e melhor monitorados.
- Manter contato direto com a CONTRATADA quando do aparecimento de incidentes e/ou problemas na solução.
- Ampliar os mecanismos de segurança da informação existentes no TJPI fortalecendo seus pilares: confidencialidade, integridade e disponibilidade;

5.2.2 Recurso 2: Preposto da CONTRATADA e/ou fabricante da solução.

5.2.2.1 Função: Manter a solução de TIC em perfeito funcionamento independentemente da atuação da Equipe do setor de Infraestrutura e Segurança da Informação da STIC do TJPI.

5.2.2.2 Responsabilidades:

- Atender a todas as requisições do TJPI em tempo hábil e de acordo com os Níveis Mínimos de Serviços Exigidos (NMSE) acordados;
- Atualizar, sempre que necessário, os softwares integrantes e/ou componentes da solução de TIC;
- Manter a confidencialidade dos dados que tiver acesso em decorrência do contrato a ser firmado.

6. Estratégia de continuidade em eventual interrupção contratual (art. 15. II)

6.1 Evento 1: Descontinuidade da solução de PAM por parte do fabricante.

6.1.1 Ação de contingência: Realizar contratação de nova solução.

6.1.2 Responsável: Equipe de contratação.

6.2 Evento 2: Rescisão contratual por parte da Administração ou da CONTRATADA.

6.2.1 Ação de contingência: Contratar outra empresa que forneça suporte à solução adquirida.

6.2.2 Responsável: Equipe de contratação.

7. Ações para transição e encerramento contratual (art. 15, III)

Ação	Responsável	Data de Início	Data de Fim
Entrega de versões finais dos produtos alvos da contratação (art. 15, inc. III, a)	Contratada	A partir da emissão do Termo de Recebimento Provisório	Até a emissão d Definitivo ou d
Transferência final de conhecimentos sobre a execução e a manutenção da Solução de Tecnologia da Informação e Comunicação (art. 15, inc. III, b)	Contratada	Pelo menos um mês antes da entrada em produção da solução	No máximo um entrada em prod
Devolução de recursos materiais (art. 15, inc. III, c)	Não há necessidade de devolução de qualquer dos materiais contratados.		
Revogação de perfis de acesso (art. 15, inc. III, d)	TJPI	Um mês antes do término do contrato	Até o termo fina
Eliminação de caixas postais (art. 15, inc. III, e)	Poderão ser criadas caixas postais para atendimento da implantação desta solução.		

8. Estratégia de independência (art. 15, IV)

No que se refere à licença de uso de software, tratando-se de prestador exclusivo, não há possibilidade de definir estratégias de independência tecnológica.

Uma possibilidade seria substituir a solução objeto desta contratação por uma nova solução de segurança. No entanto, continuaria havendo dependência tecnológica da solução substituta.

Quanto aos direitos de propriedade intelectual, estes 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.

ESTRATÉGIA PARA CONTRATAÇÃO (art. 16)

9. Natureza do objeto (art. 16, I)

O objeto a ser contratado enquadra-se na categoria de bens/serviços 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 adquirido por meio de **adesão** à ATA DE REGISTRO DE PREÇOS N.º 001/2021 da FUNDAÇÃO UNIVERSIDADE FEDERAL DO AMAPÁ - UNIFAP (SEI 2842190), de acordo com a proposta de preços (SEI 2857029) e respectiva documentação (SEI 2857058) necessária para adesão, enviados pela APPROACH TECNOLOGIA LTDA, licitante vencedora no certame da UNIFAP, conforme orientação descrita no item **4. DA ADESÃO À ATA DE REGISTRO DE PREÇOS** do SEI 2842190.

Caso a Administração do TJPI entenda que não é possível a adesão à ARP acima, o objeto poderá ser ser licitado por meio da modalidade Pregão, pelo qual esta equipe de planejamento da contratação apresenta o Termo de Referência SEI 2641675.

10. Parcelamento do objeto (art. 16, II)

Considerando que se trata de Solução de PAM (Ferramenta de Gerenciamento de Acessos Privilegiados) a ser instalada no *datacenter* deste TJPI, não se vislumbra a possibilidade de parcelamento do objeto.

11. Adjudicação do objeto (art. 16, III)

Tratando-se de item único, a adjudicação do objeto deverá ser realizada para o mesmo fornecedor com vias a garantir a interoperabilidade deste.

12. Modalidade e tipo de licitação (art. 16, IV)

Considerando que os bens/serviços são caracterizados como comuns no mercado de TIC, cujos padrões de desempenho e de qualidade podem ser objetivamente definidos, recomenda-se a adesão à ARP citada no item **9. Natureza do objeto**. Em caso de entendimento diverso a Administração deste TJPI poderá utilizar-se do sistema de **pregão do tipo menor preço, na sua modalidade eletrônica**.

13. Classificação e indicação orçamentária (art. 16, V)

Para atendimento da demanda objeto do presente processo, sugere-se a seguinte classificação orçamentária:

GRUPO	ITEM	DESCRIÇÃO	CÓDIGO	ESPE
1	1	Licenciamento de uso para solução de Gerenciamento de Acessos Privilegiados *(Privileged Access Management - PAM),* com garantia de 36 meses	04.101.02.061.0015.2865	CUSTEIO DAS UNID E JUDICIÁRIAS - 2
	2	Serviço de Instalação e Configuração da Solução de Gerenciamento de Acessos Privilegiados *(Privileged Access Management - PAM)*		
	3	Treinamento de Administração da Solução		
	4	Treinamento de Operação da Solução		
	5	Suporte Técnico especializado		

14. Vigência da garantia e da prestação dos serviços (art. 16, VI)

A Solução de PAM (Ferramenta de Gerenciamento de Acessos Privilegiados) deverá vir com garantia por um período não inferior a **36 (trinta e seis)** meses. Nesse item está incluído a atualização dos softwares integrantes da solução bem como o suporte nos moldes deslindados no item **1.2.3** deste Estudo.

15. Equipe de apoio à contratação (art. 16, VII)

Integrante Requisitante	Fabiano Galeno da Costa Pereira	Matrícula	3786
E-mail	fabiano.galeno@tjpi.jus.br	Telefone	(86) 3215-1120
Integrante Técnico	Natanael Henrique Corrêa	Matrícula	5027
E-mail	natanael.henrique@tjpi.jus.br	Telefone	(86) 3215-1120
Integrante Administrativo	Giovanny Lima de Castro	Matrícula	28631
E-mail	giovanny.castro@tjpi.jus.br	Telefone	(86) 3215-1120

16. Equipe de gestão da contratação (art. 16, VIII)

Gestor do Contrato	Agnaldo Abreu Almendra	Matrícula	30267
E-mail	agnaldo@tjpi.jus.br	Telefone	(86) 3215-1120
Fiscal Demandante	Ernani Moura Lima	Matrícula	27683

E-mail	ernani.lima@tjpi.jus.br	Telefone	(86) 3215-1120
Fiscal Técnico	Eric Barbosa Jales de Carvalho	Matrícula	27683
E-mail	ericjales@tjpi.jus.br	Telefone	(86) 3215-1120
Fiscal Administrativo	Marcus Vinicius Alcantara de Almeida	Matrícula	1635
E-mail	marcus.almeida@tjpi.jus.br	Telefone	(86) 3215-1120

ANÁLISE DE RISCOS (art. 17)

17. Riscos do processo de contratação (art. 17, I)

Risco 1 – Restrição orçamentária					
Probabilidade	Impacto	Ação Preventiva	Responsável	Ação de Contingência	Responsá
Média	Alto	Priorização deste projeto em detrimento de outras iniciativas	Equipe de Planejamento da Contratação	Reduzir escopo da demanda	Integrant
Risco 2 - Falhas na especificação dos produtos em relação à capacidade e alinhamento às demandas do órgão					
Probabilidade	Impacto	Ação Preventiva	Responsável	Ação de Contingência	Responsá
Baixo	Alto	Especificar com minúcia suficiente os requisitos técnicos da solução	Equipe de Planejamento da Contratação	Rever o projeto atual e prospectar alteração de configurações para adequação à solução proposta	Integrant
Risco 3 – Não cumprimento dos prazos acordados					
Probabilidade	Impacto	Ação Preventiva	Responsável	Ação de Contingência	Responsá
Média	Alto	Troca de informações para acompanhamento dos serviços a serem executados	Servidor responsável pelo acompanhamento dos serviços	Aplicar sanções previstas em contrato	Gestor do
Risco 4 – Não cumprimento dos itens contratuais					
Probabilidade	Impacto	Ação Preventiva	Responsável	Ação de Contingência	Responsá
Baixa	Alto	Previsão contratual	Equipe de Planejamento da Contratação	Cancelar contrato e contratar outra empresa	Gestor do
Risco 5 – Problemas no software da Solução de PAM					
Probabilidade	Impacto	Ação Preventiva	Responsável	Ação de Contingência	Responsá
Baixa	Alto	Testar exaustivamente a solução	Fiscal técnico	Abrir chamado técnico em garantia para suporte e manutenção	Fiscal Té

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 11:51, 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 **2415179** e o código CRC **D4AB940D**.