

Estudo Técnico Preliminar da Contratação

I - Necessidade da Contratação

1. Análise da Situação

O Tribunal de Justiça do Distrito Federal e dos Territórios (TJDFT) necessita de uma infraestrutura segura e compatível com as necessidades associadas às suas atividades, de modo a sustentar adequadamente os serviços de tecnologia da informação para garantir a operacionalização da função jurisdicional de sua responsabilidade. Para isso, é necessário que a equipe de Tecnologia da Informação e Comunicação (TIC) garanta a modernização tecnológica da infraestrutura por meio de recursos adequados em quantidade, capacidade operacional, atualização tecnológica e garantia de continuidade e segurança.

Com esse objetivo em foco, em 2023 foi realizado Estudo Técnico Preliminar (ETP) para estudar, analisar e definir o melhor cenário para contratação de suporte, garantia, atualização de ambiente e ampliação de licenças de uso de Solução de Gestão de Acessos Privilegiados (PAM) em uso no Tribunal, conforme definido no item ID SETI_044 do Plano Anual de Contratações de TIC do TJDFT do ano de 2023, e documentado no PA 0002778/2023. Todas as etapas do planejamento foram cumpridas em conformidade com os normativos vigentes e o processo seguiu normalmente para seleção de fornecedor. Nessa fase, a licitação ocorreu dentro da normalidade, contando inclusive com questionamentos pré e recurso pós habilitação da empresa vencedora do pregão eletrônico, respondidos com toda fundamentação necessária.

Contudo, após avaliação dos recursos à habilitação de proposta e em momento anterior à homologação, foi notificado fato superveniente que ensejou a revogação do referido certame. Este fato consistiu-se da inclusão do "Programa de Migração para Nuvem Corporativa" no Portfólio Estratégico do TJDFT, deliberada pelo Comitê de Governança e Gestão Estratégica – CGGE e aprovada pelo Tribunal Pleno em sua 22ª sessão extraordinária, além da aprovação do PDTIC 2024, pelo Comitê de Governança de Tecnologia da Informação e Comunicação - CGTIC, incluindo ações relacionadas à migração de serviços de infraestrutura do TJDFT para o ambiente de nuvem computacional a ser contratada em 2024.

Por esse motivo, o certame foi cancelado e o objeto da contratação retornou para a fase de estudos técnicos preliminares, visando adequá-lo à arquitetura surgida com o cenário superveniente. Assim, buscando o alinhamento dos requisitos da solução ao novo cenário, foi solicitado auxílio da Coordenadoria de Infraestrutura de Tecnologia da Informação - COTEC, unidade envolvida no planejamento da contratação e migração de serviços de infraestrutura para nuvem, que prontamente indicou um de seus servidores para compor a equipe de planejamento da nova contratação de uma solução de PAM.

O objetivo deste Estudo Técnico Preliminar (ETP) é estudar, analisar e definir o melhor cenário no **Estudo para contratação ou expansão de solução de gestão de acessos privilegiados (PAM)**, conforme definido no item SI40.1 do Plano Diretor de Tecnologia da Informação e Comunicação (PDTIC) do TJDFT do ano de 2025.

A gestão de acesso privilegiado, uma das formas de gestão de riscos em tecnologia, figura na lista dos dez principais projetos que todo gestor de segurança precisa se preocupar, segundo estudo divulgado pela renomada empresa de consultoria e aconselhamento empresarial Gartner.

A Coordenadoria de Segurança Cibernética (COSEC) tem como uma de suas competências, atribuída pela Portaria GPR 2091 de 26/09/2022, Art. 210-H, definir e auditar acessos privilegiados aos recursos de infraestrutura de tecnologia da informação.

Acessos privilegiados são necessários para que um administrador, aplicação ou dispositivo acesse um sistema, tais como: servidores, switches, firewalls, roteadores, entre outros, com permissões mais elevadas.

Muitos riscos são resultantes deste tipo de acesso, tanto feito por atacantes externos à organização quanto por usuários internos maliciosos. Se uma conta, credencial ou senha que forneça acesso privilegiado a ativos de TIC for comprometida, pode resultar em significativo dano ao órgão.

Para nortear o trabalho, foi consultado o relatório “Quadrante Mágico para Gestão de Acesso Privilegiado 2024” da Gartner Inc, que demonstra o posicionamento de várias fabricantes nesse segmento de mercado relacionado à segurança da informação:



Figura 01 - Quadrante Mágico para Gestão de Acesso Privilegiado

1.1. Percepção Estratégica do Problema

A crescente informatização dos processos de negócio do TJDFT, tanto os finalísticos quanto os gerenciais e de suporte, e consequente incremento no número de sistemas, usuários e tráfego de rede corporativa implicam na necessidade de constante aprimoramento das ações de segurança da informação para proteção dos dados utilizados nesses processos.

A SETI tem como missão prover serviços e soluções de tecnologia da informação que viabilizem o cumprimento da função institucional do TJDFT. Tal função perpassa pela disponibilização de soluções de tecnologia seguras e modernas de forma a garantir a excelência na prestação jurisdicional. Para tanto, várias ações contínuas são necessárias a fim de manter a conformidade com os objetivos da Estratégia Nacional de Tecnologia da Informação e Comunicação do Poder Judiciário (ENTIC-JUD 2021-2026). Dentre os objetivos, estão:

- 1. Aumentar a Satisfação dos Usuários do Sistema Judiciário;
- 2. Promover Transformação Digital;
- 3. Aprimorar as Aquisições e Contratações;
- 4. Promover Serviços de Infraestrutura e Soluções Corporativas;
- 5. Aperfeiçoar a Governança e a Gestão;
- 6. Aprimorar a Segurança da Informação e a Gestão de Dados.

Segundo estudos da empresa Microsoft, em seu relatório anual de vulnerabilidades de 2019, 92% das vulnerabilidades críticas nos navegadores Internet Explorer e Edge podem ser mitigadas removendo o acesso de administrador local das estações de trabalho. Ainda, de acordo com o mesmo estudo, 85% das vulnerabilidades críticas nas versões 7, 8.1 e 10 do Microsoft Windows poderiam ser mitigadas com a mesma ação de remoção do acesso administrativo à estação. Para os servidores de rede, equipamentos que processam a maior parte da informação digital do TJDFT, a redução de vulnerabilidades chegaria a 83%.

De acordo com a Gartner, em sua análise de "Capacidades Críticas para Gestão de Acesso Privilegiado", uma solução de PAM permanece como um controle fundamental de segurança, uma vez que incidentes de cibersegurança recentes demonstraram que o impacto dessas violações é sentido não apenas online mas também no mundo físico. Frameworks regulatórios e seguradoras estão gradativamente aumentando a exigência de implementação de ferramentas PAM como condição de conformidade e cobertura de seguros. Consequentemente, vem crescendo a adoção dessas ferramentas por empresas de todos os tamanhos, de organizações com atuação global a pequenas e médias empresas.

Por fim, importa ressaltar que a Estratégia Nacional de Segurança da Informação e Cibernética do Poder Judiciário (ENSEC-PJ) instituída pelo CNJ dispõe, em seu Art. 29, incisos I, II e III, a obrigatoriedade de gestão de usuários de sistemas informatizados, composta de gerenciamento de identidades, de acessos e de privilégios. Rotinas essas que exigem a utilização, dentre outras, de uma solução de PAM.

Ambiente Atual de Tecnologia da Informação do TJDFT

A solução de PAM utilizada atualmente no ambiente do TJDFT é a solução da fabricante CyberArk, empresa líder no segmento

conforme análise do quadrante mágico Gartner na figura 01. Desde sua implantação, houveram ganhos perceptíveis na proteção das credenciais gerenciadas pela ferramenta.

O quantitativo de 150 (cento e cinquenta) licenças adquiridas atendeu às necessidades dimensionadas à época da contratação mas, com a evolução da estratégia tecnológica e do parque computacional do Tribunal, com o consequente aumento no quantitativo de sistemas e administradores necessitando da proteção de credenciais privilegiadas, são em número insuficiente para o cenário atual.

A ampliação gradual da informatização de processos reflete diretamente na quantidade de ativos, sistemas e bases de dados necessários para suportar os serviços disponibilizados. Dessa forma, percebeu-se imprescindibilidade de aquisição de licenças complementares para devida adequação na proteção e gerenciamento de credenciais privilegiadas.

A defesa cibernética do TJDFT é fundamental para garantir a continuidade das atividades jurisdicionais. Conforme detalhado acima, o TJDFT possui licenças de algumas plataformas de segurança. No entanto, trata-se de produtos que, devido ao avanço e evolução das ameaças cibernéticas, podem não ser mais suficientes para manter o ambiente tecnológico completamente seguro. No dia 31/07/2022, a equipe de TIC detectou uma atividade maliciosa no acesso ao datacenter do TJDFT. As equipes técnicas realizaram contenções de forma a preservar os sistemas judiciais, administrativos e todas as respectivas bases de dados. Contudo, por cautela, o site e demais sistemas foram desativados para que se realizem as atividades de remediação e investigação com impacto imediato na prestação dos serviços jurisdicionais. Além disso, as equipes especializadas em cibersegurança realizaram tempestivamente a contenção das ações maliciosas, o que fez com que não houvesse comprometimento das bases de dados do Tribunal. Dessa forma, a aquisição, manutenção e ampliação do uso de soluções modernas, que possuem funcionalidades avançadas é de suma importância para manter o ambiente menos exposto aos riscos relacionados à segurança da informação.

1.2. **Necessidades de Negócio e Tecnológicas:**

Em consonância com as necessidades elencadas no Plano Estratégico do TJDFT (PE 2021 – 2026), notadamente, observa-se as seguintes demandas e funcionalidades esperadas relacionadas ao objeto deste estudo:

Necessidade 1: Incrementar a segurança da informação e a proteção de dados pessoais.	
Funcionalidades esperadas	Atores envolvidos
1. Prover níveis de segurança na infraestrutura de TIC aderentes às Políticas e Padrões internos e externos de segurança da informação aplicáveis ao TJDFT. 2. Manter a confidencialidade, integridade, disponibilidade e privacidade dos dados e das informações do TJDFT, inclusive para conformidade com a Lei Geral de Proteção de Dados (Lei nº 13.709/2018). 3. Suportar a atual demanda de utilização da rede e dos sistemas com alto nível de segurança. 4. Ampliar o quantitativo de usuários e credenciais privilegiadas protegidas por solução especializada. 5. Prover a segurança de todos os sistemas e aplicações utilizados no TJDFT. 6. Mitigar riscos de evasão e integridade das informações corporativas. 7. Rastrear e controlar o acesso de usuários e de aplicativos. 8. Adequar as soluções de segurança de informação para garantir o tráfego seguro dos dados no ambiente interno do Tribunal. 9. Adequar, padronizar e permitir expansões por meio do licenciamento e suporte técnico especializado dos softwares que sustentam o ambiente computacional do Tribunal. 10. Aprimorar a gestão de incidentes de segurança cibernética. 11. Proteger credenciais com acesso privilegiado a sistemas, bancos de dados e aplicações. 12. Aumentar a eficiência operacional.	SETI

2. **Definição e Especificação dos Requisitos da Contratação**

Requisitos de Negócio	Detalhamento (motivação, quantitativos, justificativas)
-----------------------	---

De Capacitação	(treinamentos necessários, carga horária, material didático, qtd de participantes, modalidade de transmissão do conhecimento [presencial ou remoto]) Repasso de conhecimento - A CONTRATADA deverá realizar repasse de conhecimento hands-on da solução para equipe técnica indicada pela CONTRATANTE, com as seguintes características: 1. Deverá ser realizado por um técnico com conhecimento certificado na solução ofertada. 2. Deverá possuir carga horária de no mínimo 20 horas; 3. Deverá fornecer uma comprovação de treinamento (certificado de conclusão/participação); 4. Deverá disponibilizar material didático, manuais técnicos ou qualquer outro material que auxilie no repasse de conhecimentos; 5. Deverá fornecer o treinamento para, no mínimo, uma turma com 10 (dez) servidores do TJDFT; 6. Deverá ser realizado nas dependências da CONTRATANTE ou de forma remota, conforme alinhamento prévio; 7. Poderá ser realizado em horário de expediente do TJDFT, ou em horário diverso, em dias úteis, conforme alinhamento prévio entre o CONTRATANTE e a CONTRATADA. 8. O CONTRATANTE não assumirá os custos de licenças e/ou softwares extras, diárias e transporte dos instrutores, assim como outros custos relativos a esta capacitação. Todos os custos devem ser previstos pela CONTRATADA da solução na elaboração de suas propostas. 9. Ao término do processo de Repasse de Conhecimentos, a CONTRATADA deverá realizar uma avaliação de satisfação em relação ao curso, como conteúdo, instalações, material didático e de aplicação à prática profissional, bem como do(s) instrutor(es). 10. Caso o curso seja considerado insatisfatório, a CONTRATADA deverá realizar um novo Repasse de Conhecimentos, com a finalidade de atender as demandas não supridas inicialmente.
Legais	• Lei nº 14.133/2021 - Estabelece normas gerais de licitação e contratação para as Administrações Públicas diretas, autárquicas e fundacionais da União, dos Estados, do Distrito Federal e dos Municípios. • Lei nº 10.520/2002 - Institui, no âmbito da União, Estados, Distrito Federal e Municípios, nos termos do art. 37, inciso XXI, da Constituição Federal, modalidade de licitação denominada pregão, para aquisição de bens e serviços comuns, e dá outras providências. • Decreto nº 10.024/2019 - Regulamenta o pregão, na forma eletrônica, para aquisição de bens e serviços comuns, e dá outras providências. • Decreto nº 7.174/2010 – Regulamenta a contratação de bens e serviços de informática e automação pela administração pública federal, direta ou indireta, pelas fundações instituídas ou mantidas pelo Poder Público e pelas demais organizações sob o controle direto ou indireto da União. • Resolução 468/2022 – CNJ – Dispõe sobre diretrizes para as contratações de Solução de Tecnologia da Informação e Comunicação pelos órgãos submetidos ao controle administrativo e financeiro do Conselho Nacional de Justiça. • Instrução Normativa 01/2019 – SGD/ME: Dispõe sobre o processo de contratação de soluções de Tecnologia da Informação e Comunicação – TIC pelos órgãos e entidades integrantes do Sistema de Administração dos Recursos de Tecnologia da Informação – SISF do Poder Executivo Federal. • Nota Técnica nº 01/2008 - SEFTI/TCU - Estabelece o conteúdo mínimo do Projeto Básico ou Termo de Referência da Contratação para contratação de serviços de Tecnologia da Informação e Comunicações – TIC. • Nota Técnica nº 02/2008 - SEFTI/TCU - Estabelece o uso do pregão para aquisição de bens e serviços de Tecnologia da Informação. • Resolução 21/2016 – TJDFT – Dispõe, no âmbito do Tribunal de Justiça do Distrito Federal e dos Territórios - TJDFT, sobre o Sistema de Gestão de Segurança da Informação - SGSI e a Política Corporativa de Segurança da Informação - PCSI. • Regimento Interno Administrativo do TJDFT. • Plano Estratégico 2021 – 2026. • Plano Diretor de Tecnologia da Informação e Comunicação 2025 do TJDFT.
De Manutenção	• A CONTRATADA/FABRICANTE deverá oferecer tempestivamente: correções, suporte e manutenções que estejam disponíveis e visem garantir o pleno uso do produto pela equipe do TJDFT. • Todos os softwares e serviços contratados devem contemplar atualizações e garantia total por todo o período de vigência das licenças. Caso haja renovação do licenciamento, será também renovada a garantia conforme quantidades, requisitos e especificações constantes deste documento. • A CONTRATADA/FABRICANTE deverá fornecer correções de bugs ou alternativa para corrigir defeitos no(s) software(s) especificado(s) neste documento, que façam com que eles não operem de acordo com a documentação pública para os usuários de softwares.

Temporais	A CONTRATADA deverá cumprir os eventos descritos na tabela a seguir, respeitando os prazos máximos estabelecidos:			
	Marco	Prazo máximo (em dias)	Evento	Responsável
	Dia D0	-	Assinatura do contrato entre o CONTRATANTE e a empresa licitante vencedora.	TJDFT e CONTRATADA
	Dia D1	D0 + 5	Reunião inicial do contrato.	TJDFT e CONTRATADA
	Dia D2	-	Emissão da Ordem de Serviço pelo CONTRATANTE.	TJDFT
	Dia D3	D2 + 15	Apresentação do Plano de Migração, caso necessário.	CONTRATADA
	Dia D4	D3 + 15	Aprovação do Plano de Migração, caso necessário.	TJDFT
	Dia D5	D2 + 30	Entrega dos documentos que comprovem o fornecimento e a ativação das licenças contratadas, da solução as-built' e instalação dos appliances.	CONTRATADA
	Dia D6	D5 + 7	Emissão do Termo de Recebimento Provisório, para conferência dos produtos e serviços entregues e autorização para emissão de faturamento.	TJDFT
	Dia D7	D4+90	Conclusão da Migração, caso necessária.	CONTRATADA
	Dia D8	D7 + 14	Emissão do Termo de Recebimento Definitivo, autorização para emissão de faturamento e início do período de garantia e de execução do serviço de suporte técnico.	TJDFT
Os tempos considerados na tabela deverão ser contados em dias corridos, exceto para os eventos dos marcos Dia D6 – Emissão do Termo de Recebimento Provisório – e Dia D8 – Emissão do Termo de Recebimento Definitivo, que serão contados em dias úteis. O fornecimento das licenças e instalação da solução e demais ações serão condicionados à emissão de Ordem de Serviço (OS), dentro do prazo contratual, de acordo com a necessidade do TJDFT. O fornecimento das licenças e a instalação, configuração e migração, caso necessária, será integral e com pagamento em 2(duas) parcelas: a primeira após a emissão do Termo de Recebimento Provisório (TRD) e a segunda após a emissão do Termo de Recebimento Definitivo (TRD). O suporte técnico terá início a partir da emissão do Termo de Recebimento Definitivo com pagamento mensal pelo prazo contratado.				
De Segurança	A CONTRATADA deverá atender ao Sistema de Gestão de Segurança da Informação – SGSI e a Política Corporativa de Segurança da Informação – PCS do TJDFT assim com os demais normativos legais. A CONTRATADA deverá garantir a segurança das informações do TJDFT e se compromete a não divulgar ou fornecer a terceiros quaisquer dados e informações que tenha recebido do Tribunal no curso da prestação dos serviços, a menos que autorizado formalmente e por escrito para tal. A CONTRATADA, após a assinatura do contrato, por meio de seu representante, assinará o TERMO DE CONFIDENCIALIDADE E SIGILO em que se responsabilizará pela manutenção de sigilo e confidencialidade das informações a que possa ter acesso em decorrência da contratação. A CONTRATADA se compromete a tratar os dados pessoais decorrentes deste instrumento de acordo com o estabelecido na Lei 13.709/2018 (Lei Geral de Proteção de Dados Pessoais - LGPD).			
Sociais, ambientais e culturais	Prefere-se, sempre que possível, que os manuais, ferramentas, interfaces, apostilas de treinamentos e materiais integrantes da solução sejam fornecidos no idioma português do Brasil – PT-BR.			
Demais disposições aplicáveis	As licenças fornecidas para toda a solução e todos seus módulos deverão ser por subscrição, com validade trienal, possibilitando o uso durante o período de contratação da subscrição e do suporte.			

Requisitos Tecnológicos	Detalhamento (motivação, quantitativos, justificativas)
-------------------------	---

De arquitetura	(hardwares, softwares, padrões de interoperabilidade, interfaces, etc.) A arquitetura poderá ser híbrida ou totalmente on-premises, desde que o cofre digital (local de armazenamento das credenciais e políticas) esteja inteiramente sob custódia do CONTRATANTE, com possibilidade de replicação local para contingência. Caso a solução possua componentes SaaS ou em nuvem, será obrigatória a disponibilidade de modo offline ou failover local, garantindo o funcionamento ininterrupto das operações críticas (gestão de credenciais, autenticação, auditoria, proxy e workflows locais).
Projeto e implementação	(processo de desenvolvimento, técnicas aplicáveis, forma de gestão, de documentação, etc.) Migração da Solução Existente e Plano de Migração: Caso a solução vencedora seja diferente da atualmente em uso (CyberArk), a CONTRATADA será responsável por planejar e executar a migração completa da solução de PAM atualmente em uso (CyberArk) para a nova plataforma. Este processo deve incluir, no mínimo: • A migração de todos os cofres (safes), contas, políticas de acesso e configurações existentes. • A migração do histórico de gravações de sessão, na medida em que for tecnicamente viável e compatível entre as plataformas. • A reconfiguração ou desenvolvimento de todas as integrações e plugins atualmente em uso para garantir a continuidade operacional. A CONTRATADA deverá apresentar um Plano de Migração detalhado em até 15 (quinze) dias após a emissão da Ordem de Serviço inicial. Este Plano deve conter o cronograma de atividades, a alocação de recursos, a metodologia de migração e os critérios de aceite, e deverá ser formalmente aprovado pelo CONTRATANTE antes do início da execução.
Implantação	(processo de disponibilização em produção, dentre outros) Responsabilidade Integral: A CONTRATADA será integralmente responsável pela prestação de todos os serviços profissionais necessários para a completa implantação, configuração e operacionalização da solução ofertada, em conformidade com todos os requisitos estabelecidos neste documento. Cronograma de Implantação: A implantação completa da solução, incluindo a migração descrita no presente, deverá ser concluída no prazo máximo de 3 (três) meses a contar da data de aprovação do Plano de Migração.
Garantia e suporte	(forma de comunicação e prestação de suporte técnico, duração da garantia e os itens contemplados por ela) O serviço de suporte será executado pela Contratada, durante todo o período de vigência do contrato, que corresponde ao prazo mínimo de garantia dos softwares, devendo ser iniciado no primeiro dia útil após o aceite definitivo da solução, na seguinte forma: 1. Promover atualização de módulos e novas versões do software conforme disponibilização pela fabricante; 2. Promover instalação de releases e patches de manutenção desenvolvidos durante o período ; 3. Fornecer conectores, plugins e/ou quaisquer integradores necessários à adequação aos sistemas da contratante, tanto do executável quanto do código-fonte correspondente, bem como a documentação de todas modificações e configurações realizadas, quando não fornecidos pela fabricante; 4. Avaliar, sugerir e promover mudanças de arquitetura da solução, mediante solicitação da equipe do TJDFT; 5. Oferecer suporte via canais digitais (telefone, chat, e-mail) para atendimento de chamados em regime de 24 horas por dia e 7 dias por semana, garantindo atendimento em no máximo 2h para eventos com indisponibilidade da solução por completo, 24h para eventos com indisponibilidade em funcionalidades específicas/pontuais e 72h para eventos eventos não enquadrados nos anteriores;; 6. Acompanhar toda solicitação de chamado de suporte remoto através dos canais de atendimento da fabricante quando necessário; 7. Disponibilizar base de conhecimentos de solução de problemas e documentos técnicos; 8. Auxiliar o TJDFT no seu registro junto ao site de licenciamento da fabricante; 9. Auxiliar o TJDFT na ativação e consumo dos benefícios relacionados às licenças contratadas.
Demais requisitos aplicáveis	A CONTRATADA deverá garantir suporte técnico, atualizações de segurança e correções por, no mínimo, 36 (trinta e seis) meses após a entrega definitiva, com possibilidade de renovação contratual mediante cláusulas específicas. Todos os componentes da solução (inclusive agentes, SDKs, APIs, SOs, BDs, módulos de integração etc.) deverão estar devidamente licenciados para uso ilimitado no contexto da organização, respeitando as exigências previstas de alta disponibilidade, ambientes segregados (produção/homologação/testes) e integração com sistemas legados ou críticos. No momento da apresentação das propostas, todos os componentes de hardware e software constantes da Solução deverão possuir Fim de Vida (End-of-Life - EOL) e Fim de Suporte (End-of-Support - EOS) ainda não definidos ou anunciados publicamente para um prazo superior a 36 (trinta e seis) meses.

2.1. Conhecimentos sobre a Plataforma Digital do Poder Judiciário Brasileiro (PDPJ-Br)

Em se tratando de contratações de serviços (mão de obra) para atividades de TIC e o fundamento de dar efetividade ao conhecimento sobre a Plataforma Digital do Poder Judiciário Brasileiro (PDPJ-Br), exige-se do contratado:

- Conhecimento e assimilação dos atos normativos relacionados à segurança e tecnologia da informação aprovados pelo CNJ, conforme tudo o que dispõe a Portaria CNJ 25/2022 ou novo ato normativo que venha a substituí-la.
- Indicar aqui, o atendimento, pelo contratado, aos requisitos dispostos na norma supra.

A contratação em análise não se destina à manutenção e desenvolvimento de aplicações para os sistemas judiciais dos órgãos integrantes do Poder Judiciário.

3. Alinhamento das necessidades e requisitos de negócio em relação aos requisitos tecnológicos da solução

- (X) Demanda incluída no PCA. Informe o documento SEI de autorização do CGGC: 3877286
() Demanda não incluída no PCA. Informe o documento SEI referente ao DOD – Documento de Oficialização da Demanda:

3.1. A demanda possui alinhamento com planos estratégicos e/ou diretores?

- (X) Sim. Indique:

Alinhamento entre a Contratação e os Planos da Administração e da Área de TIC

- **Alinhamento com o Plano Estratégico do Tribunal – PE 2021-2026**

Perspectiva: Processos Internos	
PI.8: Incrementar as políticas e os processos de segurança.	PI.8.E1: Incrementar a segurança da informação e a proteção de dados pessoais.

- **Congruência com os objetivos da Estratégia Nacional de Tecnologia da Informação e Comunicação - ENTIC-JUD 2021-2026**

Perspectiva: Processos Internos

Objetivo Estratégico 7: Aprimorar a Segurança da Informação e a Gestão de Dados

- **Aderência com as seguintes ações do Plano Diretor de Tecnologia da Informação e Comunicação - PDTIC 2025**

ID	Ação	ENTIC-JUD	PE/PLABI
SI40.1	Estudo para contratação ou expansão de solução de gestão de acessos privilegiados (PAM)	OE.7	PR.3

- **Conformidade com o Plano de Administração do Biênio - PLABI 2024-2026**

Tema: Gestão de tecnologia Diretriz: Promover a transformação digital no tribunal por meio da implementação de ações que assegurem qualidade, autenticidade, integridade, acessibilidade e tratamento adequado dos dados, bem como a segurança da informação, utilizando tecnologias baseadas em inteligência artificial e automização para otimizar a prestação jurisdicional. Objetivo Estratégico Priorizado: PR.3 - Intensificar a transformação digital no Tribunal
--

- **Conformidade com o Plano de Contratações Anual - PCA 2025**

ID	Objeto	Valor Estimado
SETI_013	Renovação de garantia, atualização e ampliação de licenças de uso de solução de gestão de acessos privilegiados.	R\$ 2.500.000,00*

* Cumpre salientar que o valor informado no Plano de Contratações Anual - PCA 2025 foi estimado considerando-se a perspectiva do **custo anual** da contratação, uma vez que o período de contratação ainda não fora determinado.

- () Não.

II - Descrição Resumida do Objeto

Definição da Solução Pretendida

Seleção de empresa especializada para fornecimento de solução de gestão de acessos privilegiados.

III - Análise de Mercado

Dica:

- Além do econômico, considerar a padronização e aspectos qualitativos para alcance dos objetivos da contratação;
- Modelos de prestação do serviço. Recomenda-se privilegiar modelos por entrega de resultados, conforme métricas estabelecidas;
- Os diferentes tipos de soluções (especificações, composição e características) e formas de contratação ofertadas (bens ou como serviço);
- Futuras ampliações ou substituição da solução.

Inicialmente, importa retomar a avaliação de cenários realizada na etapa de estudo técnico documentado no PA 0002778/2023. Com a revogação do certame anterior e retorno à fase de estudos técnicos para adequação ao cenário de migração para nuvem corporativa, a equipe de planejamento optou por reavaliar as principais soluções de mercado. Essa medida objetivou uma melhor compreensão das funcionalidades de integração com provedores de serviços de nuvem pelas soluções de PAM existentes. Em seu guia "Guidance for Privileged Access Management 2025", a Gartner postula que uma solução de PAM possui seis categorias de ferramentas/funcionalidades:

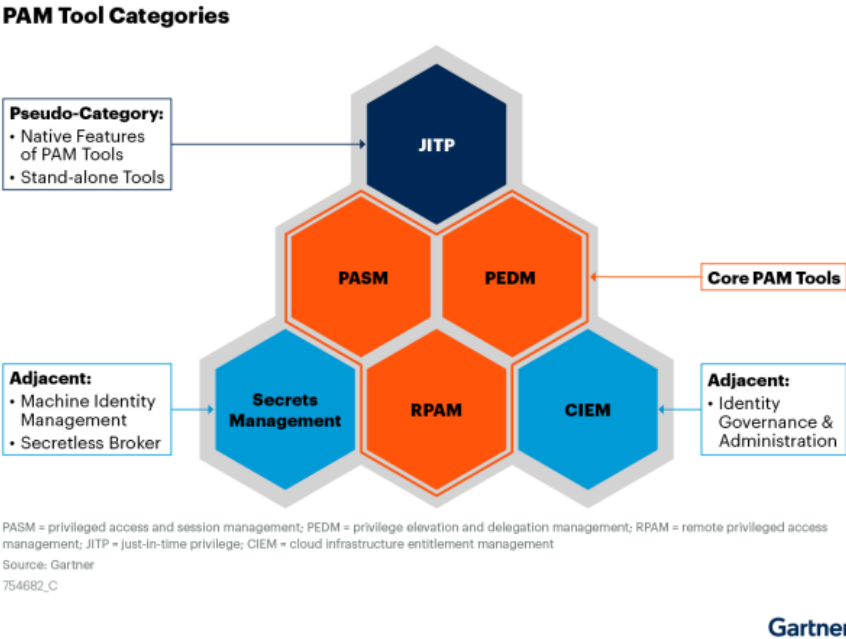


Figura 02 - Categorias de funcionalidades PAM segundo a Gartner

Categoria	Descrição resumida
Privileged Account and Session Management (PASM)	Cofre para proteção das credenciais e gerenciamento de sessões utilizando as credenciais protegidas.
Privilege Elevation and Delegation Management (PEDM)	Comando e controle baseado em agentes instalados nos dispositivos gerenciados, permitindo elevação e concessão de privilégios específicos.
Remote privileged access management (RPAM)	Gateway que permite acesso remoto sem acesso direto à rede (VPN-less) para execução de operações nos sistemas-alvo.
Secrets Management	Gestão de segredos (senhas, chaves, certificados etc.) utilizados por máquinas e sistemas, armazenados e acessados programaticamente via APIs ou SDKs.
Cloud Infrastructure Entitlement Management (CIEM)	Avaliação e gerenciamento de riscos de direitos (entitlements) em nuvens forçando a aplicação e remediação de políticas de privilégio mínimo.
Just-in-time privilege	Pseudo-categoria que envolve mecanismos para atribuição de privilégios temporários com atribuição sob demanda apenas no momento necessário.

Na consulta ao mercado, verificou-se que as principais fabricantes existentes oferecem módulos integradores. A análise foi realizada junto às fabricantes CyberArk, Delinea e BeyondTrust, classificadas como líderes no relatório “Quadrante Mágico para Gestão de Acesso Privilegiado 2024” da Gartner Inc (figura 01), além da fabricante Segura, antiga SenhaSegura, avaliada por ter sido vencedora de diversos certames federais e estaduais nos últimos anos. Reforçou-se o entendimento de que o mercado converge para oferta de licenciamento por subscrição/assinatura. Ainda que exista fabricante ofertando licenciamento perpétuo, atualmente o modelo de negócio mais negociado, apresentando maior vantagem técnica e comeral, e que permite maior concorrência é a contratação de licenças por subscrição.

Como o principal objetivo da contratação é a ampliação do quantitativo de usuários licenciados, reavaliou-se, inicialmente, a

conveniência de manter-se a solução atual em uso e contratar uma segunda solução com a quantidade necessária à ampliação ou de contratar todas as licenças necessárias em nova solução. O segundo demonstrou-se mais vantajoso, uma vez que, ainda que a vencedora seja a própria CyberArk, haveria duplicação de ambiente para o primeiro cenário avaliado, como demonstrado na análise das opções de solução levantadas no estudo anterior:

"(...) não são mais disponibilizadas novas licenças pela modalidade de licenciamento perpétuo, existindo apenas o modelo de licenciamento por subscrição. No modelo por subscrição há possibilidade de extensão de funcionalidades de proteção tais como Adaptative MFA (Adaptive Multi-factor Authentication) e SSO (Single Sign On), entre outras, não aplicáveis a licenças perpétuas.

- a) utilizar um ambiente misto de licenciamento usando as licenças perpétuas existentes e ampliando com modelo por subscrição;
- b) contratar o total de licenças desejado pelo modelo de licenciamento por subscrição.

As licenças perpétuas existentes são passíveis de utilização e suporte técnico durante o ciclo de vida dos componentes da solução, até que a fabricante defina o fim do seu ciclo de suporte - *End-Of-Life(EOL)*. Apesar disso, em caso de utilização conjunta das licenças perpétuas existentes com ampliação do quantitativo de licenças por subscrição, faz-se necessário a manutenção de dois ambientes distintos, um para cada tipo de licenciamento pois não há possibilidade de modalidade híbrida de licenciamento para um mesmo ambiente.

Verificou-se que, em num cenário de contratação do quantitativo total pelo modelo por subscrição, é possível utilizar as licenças perpétuas para abatimento no cálculo do quantitativo equivalente, ou seja, no caso da contratação de 300 licenças por subscrição, 150 (quantitativo atual de licenças perpétuas) teriam valor descontado. Nesse cenário, é necessário apenas um ambiente a ser gerenciado. Além disso, as licenças perpétuas continuam válidas até o EOL, permitindo a sua reutilização no caso de cancelamento das licenças por subscrição. Por fim, importa destacar que funcionalidades de aprimoramento de proteção (Adaptative MFA, SSO, etc.) estão disponíveis apenas nessa modalidade, não sendo possível utilizá-las com licenças perpétuas."

A primeira opção implicaria na provável duplicação de esforço de operacionalização, gerenciamento contratual e custos, além de menor proteção para credenciais que permanecessem na solução atual. A segunda segue no sentido contrário, minimizando esses impactos e reduzindo riscos operacionais e de segurança.

Avaliou-se, ainda, junto aos principais provedores de serviços em nuvem - Microsoft, Amazon e Google - os recursos de gerenciamento de acessos privilegiados e proteção de credenciais ofertadas na Azure, AWS e GCP. Com o contrato assinado recentemente com o Serpro (como integrador de multi-nuvem), o Tribunal tem flexibilidade para selecionar o provedor que melhor atender às necessidades para migração dos sistemas e aplicações. Dessa forma, os recursos de segurança presentes na plataforma do provedor podem fazer parte do escopo da migração, eliminando a necessidade de contratação adicional de ferramental, caso atendam aos requisitos técnicos. Haveria, assim, a possibilidade de se transferir o orçamento da aquisição de uma solução para ampliação dos créditos do referido contrato visando a ativação das funcionalidades necessárias. Infelizmente, observou-se que não é o caso do objeto em estudo. Embora existam recursos de gestão de identidade e acesso, proteção de secrets e outros elementos de segurança, há limitações ou ausência de recursos essenciais a uma solução de PAM propriamente dita, como: gravação e monitoramento de sessões, gestão avançada de credenciais e análise comportamental, integração com ambiente onprem e/ou de outras nuvens, entre outros.

Em razão dos contatos realizados com os provedores de serviços em nuvem, descobriu-se a possibilidade de oferta de soluções de PAM por meio de *marketplaces* (plataforma online que reúne diversos vendedores, marcas e empresas em um ambiente digital para oferta de produtos e serviços) desses provedores. Esse cenário possibilitaria o aproveitamento do contrato existente com o integrador de multi-nuvem Serpro para escolha da solução diretamente nos *marketplaces*, ao invés da abertura de licitação. Contudo, verificou-se que esse cenário ainda não tem maturidade no mercado brasileiro, inexistindo casos de contratação pública por essa modalidade. Os próprios fabricantes alegaram não estar familiarizados com o modelo no mercado brasileiro e não apresentaram casos e critérios para aplicação desse cenário que, portanto, mostrou-se como opção inviável para contratação.

Dessa forma, as seguintes possibilidades foram consideradas:

- a) utilizar um ambiente misto de soluções: usando as licenças perpétuas existentes da plataforma CyberArk e ampliando com licenças por subscrição em uma nova plataforma;
- b) contratar uma nova solução considerando o total de licenças desejado pelo modelo de licenciamento por subscrição em nova licitação;
- c) utilizar funcionalidades e serviços ofertados pelos próprios provedores de serviços em nuvem;
- d) contratação via marketplace dos provedores de serviços em nuvem por meio do contrato com Serpro.

1. Levantamento das Diferentes Soluções de Mercado que Possam Atender aos Requisitos

Diante das necessidades levantadas, foram analisadas as seguintes soluções:

Solução 1	Ambiente misto com 2 soluções.
Alternativa Viável	() SIM (X) NÃO

Descrição: A Solução 1 implica na seleção de empresa especializada para o fornecimento de solução com licenças por subscrição, atualização do ambiente atual, instalação de novo ambiente, garantia e suporte técnico para as duas plataformas. Justificativa da Solução não ser considerada viável para a presente contratação: Nesse cenário, há necessidade de se instalar e gerenciar dois ambientes distintos para utilização das licenças: manter ambiente atual utilizando as licenças perpétuas CyberArk já contratadas e instalar novo ambiente para utilização das nova solução. Ainda que a solução vencedora seja a própria CyberArk, um novo ambiente deve ser instalado, pois não há possibilidade de coexistência de licenciamento híbrido (perpétuo + subscrição) no mesmo ambiente. Agrava-se, assim, a complexidade do cenário pois, além de todos os requisitos da nova contratação, faz-se necessária a contratação adicional de suporte técnico e atualização para o ambiente existente incorrendo no aumento da complexidade de gestão de usuários da solução, no gerenciamento de ambientes distintos para a mesma funcionalidade e na necessidade de ampliação do suporte técnico e componentes de atualização de forma duplicada, elevando o custo final e riscos de segurança da informação. Além disso, somente os usuários da nova solução contratada possuiriam novos recursos de proteção, restando menor proteção aos usuários da solução existente. Ante o exposto, a Solução 1 foi considerada não viável para a presente contratação por não atender a todos os requisitos técnicos e de negócio.	
Fornecedor	
Valor Estimado Anual	

Solução 2	Licenciamento de nova solução via licitação.
Alternativa Viável	(X) SIM () NÃO
Descrição: A Solução 2 implica na seleção de empresa especializada para o fornecimento de nova solução com licenças no modelo por subscrição, garantia e suporte técnico. Desta forma, há necessidade de se realizar a contratação de novas licenças pela modalidade de subscrição considerando o quantitativo total desejado, além de suporte técnico e atualização em um único ambiente integrado, provendo recursos atualizados para proteção de credenciais privilegiadas em uso no TJDF.	
Fornecedor	A ser definido por pregão eletrônico.
Valor Estimado	Obtido pela média aritmética tratada dos processos de contratação pública elencados na Seção "V - Estimativas do Valor da Contratação" R\$ 7.526.835,94

Solução 3	Contratação de serviços ofertados pelas próprias nuvens.
Alternativa Viável	() SIM (X) NÃO

Descrição: A Solução 3 implica na utilização do contrato com o integrador de multi-nuvem (Serpro) para ativação de funcionalidades de gestão de acesso e proteção de credenciais da(s) nuvem(ns) contratada(s). Com o contrato assinado recentemente, o Tribunal tem flexibilidade para selecionar o provedor que melhor atender às necessidades para migração dos sistemas e aplicações. Haveria, assim, a possibilidade de se transferir o orçamento da aquisição de uma solução para ampliação dos créditos do referido contrato visando a ativação das funcionalidades citadas. Justificativa da Solução não ser considerada viável para a presente contratação: Embora se apresente como uma opção atrativa pela possível redução na complexidade burocrática pelo aproveitamento de um contrato vigente, algumas limitações dessa opção a inviabilizam como solução, dentre elas: * Insuficiência de requisitos: as funcionalidades ofertadas não atendem todos os requisitos identificados na avaliação de uma solução de PAM, pois recursos importantes como monitoramento e gravação de sessão, 'proxy' de banco de dados e 'failover onprem', dentre outros, estão ausentes nesse tipo de oferta. * Limitação de ambiente: são voltadas para proteção de acessos a ativos e recursos alocados na própria nuvem, inexistindo integração (ou com integração limitada) para gestão de ambiente em outra nuvem ou data-centers próprios. * Duplicação de esforço e complexidade de gestão operacional e contratual: dada a limitação de ambiente de atuação, seria necessária a contratação das mesmas funcionalidades em cada nuvem contratada, dificultando o gerenciamento de acesso aos recursos, propiciando incorreções de permissionamento e exposição indevida à exploração maliciosa por terceiros. * Adequação contratual: por não terem sido parte integrante do escopo inicial da contratação do integrador multi-nuvem, a inclusão das funcionalidades necessárias poderia incorrer em impactos contratuais não dimensionadas anteriormente. Ante o exposto, a Solução 3 foi considerada não viável para a presente contratação por não atender a todos os requisitos técnicos e de negócio.	
Fornecedor	
Valor Estimado Anual	

Solução 4	Licenciamento de nova solução via ofertas nos <i>marketplaces</i> das nuvens.
Alternativa Viável	() SIM (X) NÃO
Descrição: A Solução 4 implica em uma segunda forma de utilização do contrato com o integrador de multi-nuvem (Serpro), com a aquisição de uma solução diretamente pelo <i>marketplace</i> das nuvens disponibilizadas pelo contrato. Com o contrato assinado recentemente, o Tribunal tem flexibilidade para selecionar o provedor que melhor atender às necessidades para migração dos sistemas e aplicações. Haveria, assim, a possibilidade de se transferir o orçamento da aquisição de uma solução para ampliação dos créditos do referido contrato visando a ativação das funcionalidades citadas. Justificativa da Solução não ser considerada viável para a presente contratação: Além da questão de adequação contratual citada na Solução 3, essa modalidade de contratação apresenta outras intercorrências: * inexistência de contratos: na pesquisa de preços em portais públicos não foi identificado nenhum caso de contratação por essa modalidade, fato confirmado pelos próprios fabricantes, que não apresentaram nenhum caso vigente. * falta de maturidade do modelo: os fabricantes demonstraram não estar familiarizados com esse modelo de contratação no mercado brasileiro, no momento inexistindo critérios definidos para disponibilização desse tipo de oferta. Ante o exposto, a Solução 4 foi considerada não viável para a presente contratação por não atender a todos os requisitos técnicos e de negócio.	
Fornecedor	
Valor Estimado Anual	

2. Alternativas Viáveis:

Solução 2	Licenciamento de nova solução via licitação.
Descrição: A Solução 2 implica na seleção de empresa especializada para o fornecimento de nova solução com licenças no modelo por subscrição, incluindo serviços de instalação, configuração, repasse de conhecimento, garantia e suporte técnico. Desta forma, há necessidade de se realizar a contratação de novas licenças pela modalidade de subscrição considerando o quantitativo total desejado, além de suporte técnico e atualização em um único ambiente integrado, provendo recursos atualizados para proteção de credenciais privilegiadas em uso no TJDF.	

Fornecedor	A ser definido por pregão eletrônico.
Valor estimado	R\$ 7.526.835,94

2.1. **Análise e Comparação entre os Custos Totais de Propriedade das Soluções (Total Cost Ownership - TCO)**

Dicas:

- Nesta análise, considerar apenas as soluções técnica e funcionalmente viáveis, de todo o rol levantado.
- Observar os custos inerentes ao ciclo de vida dos bens e serviços de cada solução, a exemplo dos valores de aquisição dos ativos, insumos, garantia, manutenção.

Dado que a Solução 2 apresentou-se como a única opção viável, foi a única contemplada na análise de custos. O Custo Total de Propriedade (TCO) para a Solução 2 foi estimado considerando um cenário de licenciamento por subscrição com garantia e suporte técnico por 36 meses. Não são previstos custos adicionais para o projeto. Além disso, todos os custos de implementação e transferência de conhecimento serão de responsabilidade do fornecedor.

Os cálculos estimados são apresentados na seção V - Estimativas do Valor da Contratação.

2.2. **Quadro comparativo entre as soluções viáveis:**

Itens de comparação	Solução 2
Necessidade de capacitação	Sim. Transferência de conhecimento via manuais e demonstração formal das funcionalidades e recursos de acordo com as especificações técnicas requeridas nesse estudo.
Necessidade de adequação do ambiente	Não há
Condições para garantia adicional	Não há
Requisitos para suporte (manutenções) após término do contrato	Não há
Custo total de propriedade	R\$ 7.526.835,94
Adequações de acessibilidade existentes	Não há
Racionalização de recursos	Sim
A solução atende plenamente às necessidades de segurança da informação?	Sim
Os quantitativos estão de acordo com as necessidades dos usuários do TJDFT?	Sim
Racionalização de recursos	Sim
Resultado	Atende

3. **Análise Comparativa das Soluções Viáveis com Base no Quadro Resumo Acima**

A Solução 2 emergiu como a única opção viável, pois atende de forma ótima às necessidades atuais deste Tribunal, sem ser insuficiente ou excessiva. Ela possibilita uma implantação gradual do serviço, o que favorece o desenvolvimento contínuo da equipe e a evolução dos processos. Adicionalmente, a Solução 2 apresentou um custo vantajoso, reforçando sua escolha ao combinar eficiência operacional com economia para o Tribunal.

3.1. **Contratações Públicas Similares**

Cumprе registrar que, conforme o Relatório da Pesquisa de Preços de Contratações Públicas (4773742), a pesquisa de preços públicos retornou vários resultados cujo objeto refere-se à contratação de solução de PAM.

Contudo, pelos motivos expostos no documento, a diferença para o estudo atual em diversas variáveis que impactam na precificação -

tipo de licenciamento, prazo de contratação, diluição do licenciamento e serviço em vários itens, módulos diferentes precificados conjuntamente, quantitativos de cada módulo, entre outros - inviabilizam sua utilização em na composição da cesta de preços.

3.2. Disponibilidade de solução no Portal do Software Público Brasileiro

Dica: Legislação pertinente (Portaria STI/MP nº 46/2016)

Em consulta ao Catálogo de Software Público Brasileiro não foram encontradas soluções similares ao objeto em referência, pois não se trata de adoção de soluções de software desenvolvidas e disponibilizadas livremente e sem ônus.

4. Conclusão da Análise do Mercado

Pelas análise apresentada, a **Solução 2 -Licenciamento de nova solução via licitação**, mostrou-se aderente a todos os requisitos aplicáveis à contratação. Conclui-se pela escolha da única alternativa viável, Solução 2, que atende aos interesses do TJDF. Existem diversos fabricantes que fornecem a solução no país, garantindo, assim, a competitividade. O custo da aquisição para o período de 36 meses será de **R\$ 7.526.835,94 (sete milhões quinhentos e vinte e seis mil oitocentos e trinta e cinco reais e noventa quatro centavos)**.

5. Parcelamento do Objeto

É possível o parcelamento do bem e/ou serviço a ser contratado?	Sim () Não (X)
Em caso afirmativo, justifique se o objeto pode ser adjudicado a uma ou a várias empresas, se por itens ou por grupo de itens, bem como respondendo e justificando as indagações abaixo.	
A opção pelo parcelamento se configura quando todas as respostas das questões a seguir forem verdadeiras: a) <u>É tecnicamente viável</u> dividir a solução? A possibilidade de parcelamento do objeto foi estudada na presente contratação; entretanto, por tratar-se de fornecimento de solução de gestão de acessos privilegiados com licenciamento por subscrição, incluindo serviços de instalação, configuração, repasse de conhecimento e garantia pelo período de 36 (trinta e seis) meses, é fundamental, para a garantia da qualidade do serviço, que sejam fornecidos por um mesmo fabricante/fornecedor, em virtude da necessidade da devida integração dos componentes fornecidos pela solução, além de otimizar custos e reduzir o tempo de atendimento em caso de problemas. A adjudicação dos Itens que compõem cada lote a empresas distintas, além de aumentar seu custo administrativo, abre margem para que as empresas deixem de prestar o serviço contratado, alegando que a falha de um componente sob sua responsabilidade foi causada por falha de componente sob responsabilidade de outra CONTRATADA. De modo a impedir que esse cenário se torne realidade, comprometendo a disponibilidade de todos os serviços de TIC deste Tribunal, é fundamental o não parcelamento da presente contratação. b) <u>É economicamente viável</u> dividir a solução? Por se tratar de licenciamento de um única solução com respectivo suporte técnico e garantia, não vislumbra-se cenário de economicidade com a divisão dos itens. c) <u>Não existe perda da economia de escala</u> ao dividir a solução? Cabe consignar ainda a possível perda da economia de escala, visto que o mercado usualmente oferta menores valores visando abarcar um maior volume, podendo diferir no valor do lote, custos inerentes a operação própria e outros advindos da contratação, traduzindo-se em um menor custo da contratação almejado pela Administração. d) <u>Há o melhor aproveitamento do mercado e ampliação da competitividade</u> ao dividir a solução? Além dos fatores supracitados, pode-se elencar as seguintes vantagens pelo não parcelamento da presente contratação: • Maior nível de controle pela Administração na execução dos serviços, pelo fato da existência de apenas um software de gerenciamento; • Maior interação entre as diferentes fases da implantação/implementação; • Redução de custos no que se refere ao Custo Total de Propriedade – TCO; • Maior facilidade no cumprimento do cronograma preestabelecido; • Diminuição da quantidade de servidores públicos a serem alocados para atividades de fiscalização e gestão do contrato, tendo em vista que cada equipe é composta por no mínimo 4 servidores (gestor, fiscal técnico, fiscal requisitante e fiscal administrativo), exigindo a alocação de recursos humanos para composição de equipes de gestão e fiscalização em função da celebração de inúmeros contratos de objetos altamente relacionados. • Na observância dos prazos, concentração da responsabilidade pela execução em uma equipe de gestão e fiscalização; • Concentração da garantia dos resultados. Considerando o arcabouço de justificativas acima, decidiu-se pelo não parcelamento da presente contratação.	

IV - Demanda x Qtde de Itens

Dica:

Incluir memórias de cálculo e documentos pertinentes, considerando interdependência com outras contratações, visando a economia de escala, a estimativa deve ser justificada com levantamentos concretos.

Relação entre a demanda prevista e a quantidade de cada Item do objeto

Considerando a natural ampliação do número de sistemas, usuários, bases de dados e equipamentos advinda: das ações de transformação digital de serviços, integração de canais digitais e interoperabilidade de sistemas do Plano de Transformação Digital 2021-2026 do objetivo estratégico de incrementar as políticas e os processos de segurança como previsto no Plano Estratégico 2021-2026 e da obrigatoriedade de implementação da gestão de usuários de sistemas informatizados por meio do gerenciamento de identidades, acessos e privilégios definida pela Resolução nº 396/2021 do CNJ (ENSEC-PJ), verifica-se a necessidade de provisionamento adicional do número de dispositivos, aplicações e usuários de credenciais a serem protegidos.

Além da necessidade atual pelas equipes da área de tecnologia, com a inclusão do "Programa de Migração para Nuvem Corporativa" no Portfólio Estratégico do TJDF, considerou-se a ampliação da necessidade de proteção, além do planejamento de ampliação do uso da solução por servidores de outras áreas para proteção de credenciais sensíveis, como em contas corporativas de mídias sociais, por exemplo.

Durante o estudo, foi realizado o levantamento do quantitativo de administradores de sistemas com necessidade de uso da solução nos últimos 12 meses, estimado em cerca de 260 (duzentos e sessenta) usuários, evidenciando um déficit de mais de 70%, uma vez que atualmente existem apenas 150 licenças contratadas. Dessa forma, considerando a utilização atual, a projeção de ampliação e uma reserva técnica para uso emergencial, identificou-se a necessidade de dobrar o quantitativo de usuários licenciados, totalizando 300 (trezentas) licenças.

Para usos adicionais, levantou-se também a necessidade de ampliação da quantidade de sistemas e aplicações usuárias de credenciais privilegiadas a serem integradas com a solução para uso seguro automatizado dessas credenciais. Nesse quesito, identificou-se o quantitativo de 1.000 (hum mil) aplicações a utilizar, aproximadamente, 5.000 (cinco mil) credenciais ou segredos. Ainda, optou-se pela aquisição de 5 (cinco) licenças de usuário externo, para o caso de acessos esporádicos de terceiros, como fornecedores e prestadores de serviço, em tarefas de configuração, atualização, manutenção, análises, etc. E, a partir do incremento na segurança e da experiência adquirida no último contrato, optou-se por um prazo de 36 (trinta e seis) meses de contratação, de forma a possibilitar a ampliação gradativa da utilização da ferramenta evitando impactos bruscos nas atividades operacionais das equipes usuárias ou mesmo indisponibilidade de sistemas críticos.

Assim, a presente contratação foi dimensionada da seguinte forma para atender às necessidades do TJDF:

Descrição do Serviço	Quantidade	Unidade
Solução de gestão de acessos privilegiados com licenciamento por subscrição, incluindo serviços de instalação, configuração, repasse de conhecimento e garantia pelo período de 36 (trinta e seis) meses	1	UN
Suporte técnico.	36	MENSAL

V - Estimativas do Valor da Contratação

Dica: Colocar as memórias de cálculo e documentos pertinentes, incluir como anexos caso opte por manter o sigilo das informações de origem que devem ser preservadas.

1. Estimativas Preliminares de Preço

1.1. Contextualização

Cumprir registrar que foi realizada ampla pesquisa de preços públicos pela Equipe de Planejamento da Contratação. A pesquisa está em consonância com a [Portaria GPR 1583](#) de 08 de agosto de 2024, especialmente no que tange ao artigo 4º, *in verbis*:

"Art. 4º A pesquisa de preços para fins de determinação do preço estimado em processo licitatório para a aquisição de bens ou a contratação de serviços em geral, bem como para as alterações e prorrogações contratuais, será realizada mediante a utilização das seguintes fontes, empregadas de forma combinada ou não:

I - sistemas oficiais de governo, observado o índice de atualização de preços correspondente;

II - contratações similares feitas pela Administração Pública, em execução ou concluídas no período de 1 (um) ano anterior à data da pesquisa de preços, inclusive mediante sistema de registro de preços, observado o índice de atualização de preços correspondente, bem como Atas de Registro de Preços - ARP dentro do prazo de validade;

III - dados de pesquisa publicada em mídia especializada, sítios eletrônicos especializados ou de domínio amplo, desde que o documento de preço anexado ao processo administrativo contenha a data, o horário de acesso e o endereço do sítio eletrônico, devendo ser considerado, para obtenção do preço do item, o valor para pagamento à vista, sem desconto adicional e sem considerar custo de frete, vedada a utilização de preços provenientes de consultas a sítios eletrônicos de intermediação de vendas e leilão;

IV - tabela oficial, como do Sistema de Orçamento de Obras de Sergipe - ORSE, do Sistema de Custos Referenciais de Obras - SICRO, do Sistema Nacional de Pesquisa de Custos e Índices da Construção Civil - SINAPI, e de sítios eletrônicos especializados ou

de domínio amplo, desde que contenha a data, o horário de acesso e o endereço do sítio eletrônico;

V - pesquisa direta, mediante solicitação formal de cotação, em que constem o Cadastro Nacional de Pessoa Jurídica - CNPJ da empresa e o nome do responsável pela elaboração do orçamento, desde que não tenham sido obtidos orçamentos com mais de 6 (seis) meses de antecedência da data de divulgação do edital;

VI - pesquisa na base nacional de notas fiscais eletrônicas, desde que a data das notas fiscais esteja compreendida no período de até 1 (um) ano anterior à data da pesquisa de preços."

Saliente-se que, conforme o documento Relatório da Pesquisa de Preços de Contratações Públicas (4773742), a pesquisa de preços públicos retornou objetos semelhantes ao da presente contratação. Contudo, apesar do objeto semelhante, a precificação realizada nas referidas contratações possuem tipo de licenciamento, composição de módulos e quantitativos diferentes do desejado nesse estudo, não sendo possível definir qual seria o valor a ser utilizado no cálculo de preço.

Desta forma, para a formação da cesta de preços foram utilizados os valores de propostas de preços de fornecedores via pesquisa direta (inciso V).

1.2. Análise Comparativa de Custos

Conforme previsto no inciso III do art. 11º da Instrução Normativa SGD/ME nº 94, de 23 de dezembro de 2022, a análise comparativa de custos, in verbis:

"III - análise comparativa de custos, que deverá considerar apenas as soluções técnica e funcionalmente viáveis, incluindo:"

Ademais, conforme o § 1º do art. 11º da Instrução Normativa SGD/ME nº 94, de 23 de dezembro de 2022, são dispensados os cálculos de custo total de propriedade (TCO) das soluções consideradas inviáveis, in verbis:

"§ 1º As soluções identificadas no inciso II consideradas inviáveis deverão ser registradas no Estudo Técnico Preliminar da Contratação, dispensando-se a realização dos respectivos cálculos de custo total de propriedade."

Desta forma, para a presente contratação foi realizada a análise comparativa de custos e os cálculos de custo total de propriedade somente para as solução técnica e funcionalmente viável: Solução 2.

1.3. Aquisições e Contratações Similares de Outros Entes Públicos (inciso II do art 4º da Portaria GPR 1583):

Não foram utilizados valores de Pregões Eletrônicos, conforme indicado na seção '1.1. Estimativas Preliminares de Preço'.

1.4. Propostas de preços de fornecedores (inciso V do art 4º da Portaria GPR 1583)

Conforme o E-mail – Solicitação de Propostas Comerciais (4773729), as seguintes empresas foram contactadas a apresentar proposta comercial: **7 Secure, Approach, Arvvo, Asper, Blue Eye, Carbon IT, Infosafe, Petacorp, Vilti**.

Registra-se que somente as empresas abaixo encaminharam suas respectivas propostas comerciais de forma tempestiva até o fechamento dos estudos técnicos. Desta forma, essas propostas foram utilizadas para a elaboração da estimativa do valor da contratação. Os preços estão arrolados e detalhados na Planilha de Custos e Formação de Preços (4773743).

- Proposta Comercial 1 - Blue Eye (4773733)
- Proposta Comercial 2 - Carbon IT (4773736)
- Proposta Comercial 3 - Infosafe (4773738)
- Proposta Comercial 4 - Vilti (4778558)

1.5. Metodologia

Inicialmente, para a obtenção do **VALOR UNITÁRIO MÉDIO** dos respectivos itens da presente contratação, foi utilizada a metodologia da **mediana** combinada com a metodologia da **média aritmética**, ambas modalidades previstas no art. 6º da Instrução Normativa ME nº 65, de 07 de julho de 2021, in verbis:

"Art. 6º Serão utilizados, como métodos para obtenção do preço estimado, a **média**, a **mediana** ou o menor dos valores obtidos na pesquisa de preços, desde que o cálculo incida sobre um conjunto de três ou mais preços, oriundos de um ou mais dos parâmetros de que trata o art. 5º, desconsiderados os valores inexequíveis, inconsistentes e os excessivamente elevados."

Após o cálculo da **mediana** do respectivo item, foram calculados limites inferiores (-25% do valor da mediana) e limites superiores (+25% do valor da mediana) a fim de desconsiderar os tanto os valores excessivamente elevados quanto os excessivamente reduzidos. Para o cálculo do **VALOR UNITÁRIO MÉDIO** foi realizada a **média aritmética** dos valores que ficaram dentro do limite inferior e do limite superior da mediana.

Inicialmente, após a aplicação da metodologia de cálculo, as proposta das empresas Blue Eye e Carbon IT foram desconsideradas por enquadramento, respectivamente, acima e abaixo da variação de 25% da mediana, restando apenas dois preços válidos.

Contudo, ao se analisar detalhadamente a proposta da Carbon IT, verificou-se que apenas o item 1 ficou fora da faixa e com uma mínima diferença para o valor considerado. Ademais, a grande diferença de preços entre as propostas apresentadas de fabricantes diversos, evidenciando uma grande variação de precificação pelos fabricantes, deve ser considerada na análise para o descarte de valores considerados inexequíveis, inconsistentes e excessivamente elevados. Por esses motivos, optou-se pela manutenção da proposta da Carbon IT na composição da cesta, atingindo-se o mínimo de três preços válidos.

Pelo exposto, solicitamos ao NUPEP a ampliação da pesquisa realizada nesse estudo a fim de aumentar o quantitativo de preços válidos, bem como avaliar a manutenção das três propostas de preço citadas e, caso necessário, encaminhar solicitação à SEG para permitir a continuidade do processo com os critérios e preços válidos aqui considerados, a fim de minimizar o risco de sobrepreço ou licitação deserta por valor divergente da média do mercado.

2. Análise e Comparação entre os Custos Totais de Propriedade das Soluções (Total Cost Ownership - TCO)

A presente seção registra a comparação de Custos Totais de Propriedade para as soluções técnica e funcionalmente viáveis, nos termos do inciso III do art. 11. da IN SGD-ME nº 01/2019. Conforme exposto no **Item 1.2. Análise Comparativa de Custos**, para a presente contratação foi realizada a análise comparativa de custos e os cálculos de custo total de propriedade somente para a solução técnica e funcionalmente viável, a citar: **Solução 2.**

Para o cálculo do TCO da Solução 2, elaborou-se um cálculo utilizando os valores das propostas de preços de fornecedores. O detalhamento do cálculo encontra-se na Planilha de Custos e Formação de Preços (4773743).

Os investimentos acima realizados são fundamentais para a sustentação tecnológica dos serviços providos pelo Tribunal. Importante ressaltar que não se descartarão esses investimentos, pelas seguintes necessidades estratégicas do Tribunal: Continuidade dos contratos de suporte e manutenção vigentes, recém renovados/firmados; datacenter é necessário para a arquitetura de serviços do TJDFT, que contém serviços legados que podem não conseguir ser migrados para nuvem sem serem refatorados, o que pode tomar um tempo proibitivo; por fim, conforme o normativo vigente, é necessário avaliar o sigilo das informações e somente migrar cargas de trabalho com sigilo adequado ao tipo de nuvem. Por exemplo, não migrar sigilosos para nuvem pública, salvo as exceções descritas na legislação.

3. Orçamento Estimado da Contratação

A pesquisa de preço foi realizada de maneira ampla mas, apesar de serem encontrados pregões em que parte do objeto contemplam os mesmos itens desta contratação, a composição dos itens, quantitativos, prazos e forma de precificação divergentes impossibilitou a definição dos valores correspondentes. Dessa forma, foram usados preços obtidos a partir de propostas comerciais fornecidas por empresas representantes das fabricantes.

Por fim, conforme o cálculo detalhado na Planilha de Custos e Formação de Preços (4773743), o orçamento estimado da contratação é de **R\$ 7.526.835,94 (sete milhões quinhentos e vinte e seis mil oitocentos e trinta e cinco reais e noventa quatro centavos).**

SOLUÇÃO 2 - Seleção de empresa especializada para o fornecimento de solução de gestão de acessos privilegiados com licenciamento por subscrição, incluindo serviços de instalação, configuração, repasse de conhecimento, garantia e suporte técnico pelo período de 36 (trinta e seis) meses, conforme as especificações técnicas do Termo de Referência e seus anexos.						
Lote	Item	Descrição do Serviço	Quantidade	Unidade	Valor Unitário Médio	Valor Total Médio
1	1	Solução de gestão de acessos privilegiados com licenciamento por subscrição, incluindo serviços de instalação, configuração, repasse de conhecimento e garantia pelo período de 36 (trinta e seis) meses	1	UN	R\$ 6.776.982,94	R\$ 6.776.982,94
1	2	Suporte técnico.	36	MES	R\$ 20.829,25	R\$ 749.853,00
VALOR TOTAL						R\$ 7.526.835,94

4. Contratações Correlatas ou Interdependentes

Não há contratações correlatas ou interdependentes em relação à presente contratação.

VI - Descrição Completa da Solução Alvo

1. Solução Escolhida

Nome	Licenciamento de nova solução via licitação.
------	--

Descrição dos Bens e Serviços	1. Solução de gestão de acessos privilegiados com licenciamento por subscrição, incluindo serviços de instalação, configuração, repasse de conhecimento e garantia pelo período de 36 (trinta e seis) meses. 2. Suporte técnico.
Valor estimado	R\$ 7.526.835,94

2. Descrição Completa

2.1. Definição da Solução Pretendida

Seleção de empresa especializada para fornecimento de solução de gestão de acessos privilegiados com licenciamento por subscrição, incluindo serviços de instalação, configuração, repasse de conhecimento e garantia pelo período de 36 (trinta e seis) meses.

2.2. Descrição Completa:

Lote 1 – Item 1: Solução de gestão de acessos privilegiados com licenciamento por subscrição, incluindo serviços de instalação, configuração, repasse de conhecimento e garantia pelo período de 36 (trinta e seis) meses, conforme especificações técnicas contidas no Termo de Referência.

Quantidade: 1 (um).

Período: 36 (trinta e seis) meses a partir da emissão do Termo de Recebimento Definitivo (TRD).

CATSER / NBS: 27502 / 1.1103.22.00 Licenciamento de direitos de uso de programas de computador (software)

Lote 1 – Item 2: Suporte técnico.

Quantidade: 36 (trinta e seis).

Período: 36 (trinta e seis) meses a partir da emissão do Termo de Recebimento Definitivo (TRD).

CATSER / NBS: 26792 / 1.1501.30.00 - Serviços de suporte em tecnologia da informação (TI)

Recursos Disponibilizados:

- Caso sejam necessárias, a instalação de novos módulos ou reinstalação de módulos atualmente utilizados na solução deverão ser realizadas preferencialmente em máquinas virtuais no parque VMware ESXi do CONTRATANTE.
- Será disponibilizado ambiente virtualizado em plataforma VMware para instalação do produto em máquina virtual com sistema operacional Microsoft Windows Server ou Linux RedHat em versão mais recente e recursos (memória, processamento, armazenamento e rede) disponibilizados conforme requisitos da solução.
- Caso a solução requeira o uso de banco de dados externo, sistemas operacionais, sdks, APIs ou qualquer outra aplicação integrada, deverá a CONTRATADA fornecer o(s) licenciamento(s) necessário(s) para o funcionamento da solução, durante a vigência do suporte/garantia da solução.
- Não será aceita solução que utilize de software ou sistema operacional obsoleto, sem suporte ativo do seu fabricante ou mantenedor.

Especificação dos requisitos e necessidades mínimas:

1. Escopo e Licenciamento

- 1.1. As licenças fornecidas para toda a solução e todos seus módulos deverão ser por subscrição, com validade trienal, possibilitando o uso durante o período de contratação da subscrição e do suporte. A arquitetura poderá ser híbrida ou totalmente on-premises, física ou virtual, desde que o cofre digital (local de armazenamento das credenciais e políticas) esteja inteiramente sob custódia do CONTRATANTE, com possibilidade de replicação local para contingência.
- 1.2. Caso a solução possua componentes SaaS ou em nuvem para armazenamento das credenciais, será obrigatória a disponibilidade de failover local, garantindo o funcionamento ininterrupto das operações críticas localmente (gestão de credenciais, autenticação, auditoria, proxy e workflows locais).
- 1.3. A CONTRATADA deverá garantir suporte técnico, atualizações de segurança e correções por, no mínimo, 36 (trinta e seis) meses após o aceite da entrega definitiva, com possibilidade de renovação contratual mediante cláusulas específicas.
- 1.4. Todos os componentes da solução (inclusive agentes, SDKs, APIs, SOs, BDs, módulos de integração etc.) deverão estar devidamente licenciados para uso ilimitado no contexto da organização, respeitando as exigências previstas de alta disponibilidade, ambientes segregados (produção/homologação/testes) e integração com sistemas legados ou críticos.
- 1.5. No momento da apresentação das propostas, todos os componentes de hardware e software constantes da Solução deverão possuir Fim de Vida (End-of-Life - EOL) e Fim de Suporte (End-of-Support - EOS) ainda não definidos ou anunciados publicamente para um prazo superior a 36 (trinta e seis) meses.
- 1.6. O licenciamento deverá permitir acesso a atualizações (updates) e novas versões (upgrades) do(s) produto(s) e funcionalidades, durante todo o período de vigência da licença e suporte.
- 1.7. As licenças deverão permitir acesso ilimitado e irrestrito a todos os recursos licenciados durante o período contratado.

- 1.8. As licenças deverão estar em nome do “Tribunal de Justiça do Distrito Federal e dos Territórios” pelo período de vigência do suporte e/ou garantia, legalizado, não sendo admitidas versões “shareware”, “trial”, NFR “not for resale” ou semelhantes.
- 1.9. Caso o produto ofertado seja descontinuado pelo FABRICANTE, a CONTRATADA deverá fornecer à CONTRATANTE, sem custo adicional, outra solução que atenda a todas as exigências deste termo pelo período restante do contrato firmado.
- 1.10. A critério da CONTRATANTE as licenças não utilizadas/inativas poderão ser movimentadas para novos usuários sem que isso possa ser considerada quebra contratual ou extrapolação dos limites definidos.

2. Gestão de Acessos Privilegiados

- 2.1. A solução deverá permitir a gestão de acessos privilegiados de, no mínimo, 2.600 dispositivos (600 servidores + 2000 ativos de rede), incluindo instâncias de sistemas operacionais em provedores de nuvem pública (AWS, Azure, GCP).
- 2.2. A solução deverá permitir o acesso seguro de, no mínimo, 300 (trezentos) usuários privilegiados simultaneamente, com todas as funcionalidades habilitadas.
- 2.3. A solução deve possuir um motor de fluxos de trabalho (workflow) robusto e configurável para a aprovação de acesso privilegiado. Este mecanismo deve suportar, no mínimo, as seguintes capacidades:
 - 2.3.1. Configuração de Múltiplos Níveis de Aprovação: Capacidade de criar fluxos de aprovação com múltiplos estágios e/ou múltiplos aprovadores por estágio (e.g., a solicitação requer a aprovação do gestor do solicitante e, em seguida, do proprietário do sistema).
 - 2.3.2. A solução deverá ser capaz de exigir Justificativa Obrigatória a cada solicitação de sessão privilegiada ou obtenção de senhas.
 - 2.3.3. A solução deve permitir a integração com sistemas de Gerenciamento de Serviços de TI (ITSM), como ServiceNow ou Jira, para que o número de um ticket de incidente ou mudança possa ser exigido e validado como parte da solicitação.
 - 2.3.4. Notificações e Escalonamento (Escalation): A solução deve notificar automaticamente os aprovadores designados sobre solicitações pendentes.
 - 2.3.5. Auditoria Completa do Fluxo: Cada passo do workflow, incluindo a solicitação, cada aprovação ou negação, comentários dos aprovadores e eventuais escalonamentos, deve ser registrado em uma trilha de auditoria detalhada e imutável.
- 2.4. A solução deverá suportar o processo de "check-out" e "check-in" de credenciais privilegiadas. Este processo deve garantir que:
 - 2.4.1. O "check-out" (retirada da credencial do cofre) por um usuário autorizado seja um evento totalmente auditado, com registro de justificação.
 - 2.4.2. O "check-in" (devolução da credencial) obrigatoriamente acione um processo automático de rotação (alteração) da senha no sistema de destino, invalidando a senha que foi exposta ao usuário.
- 2.5. A solução deverá permitir o acesso privilegiado transparente, sem que o usuário visualize ou insira a senha.
- 2.6. A solução deve fornecer funcionalidades robustas para implementar uma estratégia de Zero Standing Privileges (ZSP), onde o acesso privilegiado é concedido dinamicamente e revogado automaticamente após o uso. Para tal, a plataforma deve suportar, no mínimo, a concessão de acesso Just-in-Time (JIT), permitindo a elevação temporária de privilégios em contas existentes, o acesso a credenciais por um período limitado, ou ainda a criação e remoção de credenciais efêmeras para uso durante o período de sessão privilegiada concedido ao usuário, com fluxos de trabalho de aprovação e auditoria completa.
- 2.7. O controle de acesso deve estar baseado em papéis (RBAC).
- 2.8. Todos os acessos realizados via solução deverão ser auditáveis, com geração automática de logs.
- 2.9. A solução deverá oferecer dashboard gerencial com visão consolidada.
- 2.10. A arquitetura do sistema deverá evitar que credenciais privilegiadas sejam expostas ou trafeguem fora da infraestrutura da solução.
- 2.11. A solução deve ter a capacidade de gerenciar credenciais que estejam em sistemas localizados em múltiplas localidades geográficas ou domínios, independentemente de sua quantidade.

3. Gestão Avançada de Credenciais e Senhas

- 3.1. A solução deverá permitir o gerenciamento completo do ciclo de vida de credenciais privilegiadas, técnicas e de serviço, abrangendo, no mínimo, as seguintes fases:
 - 3.1.1. Descoberta e Registro (Onboarding): Capacidade de descobrir contas privilegiadas existentes nos sistemas de destino e registrá-las no cofre para gerenciamento.
 - 3.1.2. Armazenamento Seguro: Garantia de que todas as credenciais são armazenadas de forma segura e criptografada.
 - 3.1.3. Uso Controlado: Aplicação de políticas de acesso, fluxos de trabalho de aprovação e mediação de todo o uso das credenciais.
 - 3.1.4. Manutenção (Rotação): Capacidade de alterar (rotacionar) as senhas e chaves automaticamente com base em políticas.
 - 3.1.5. Desativação (Offboarding): Capacidade de remover a credencial do gerenciamento e, quando aplicável, desativar a conta no sistema de destino.
- 3.2. A ferramenta deverá ser capaz de gerar senhas aleatórias fortes com comprimento de até 127 caracteres configuráveis.
- 3.3. A rotação de credenciais deverá ocorrer de forma automática e programável, com base em múltiplos gatilhos (triggers), incluindo, no mínimo: em intervalos de tempo agendados, após cada uso (check-in/check-out), ou sob demanda por um administrador ou usuário com devidas permissões.
- 3.4. A solução deverá permitir o gerenciamento centralizado de contas locais, de diretórios, de serviço, chaves SSH, certificados e contas privilegiadas em nuvem.
- 3.5. Todas as credenciais gerenciadas devem ser armazenadas em cofre seguro com criptografia AES-256 (ou superior) e conformidade com o padrão FIPS 140-2 (ou superior).
- 3.6. A solução deverá permitir o controle e rastreamento de onde as credenciais são utilizadas.
- 3.7. O cofre deverá possuir política de alta disponibilidade e replicação automática.
- 3.8. O acesso ao cofre deverá estar protegido por autenticação multifator.
- 3.9. A solução deverá oferecer mecanismos de verificação automática da integridade e consistência das senhas, garantindo que a senha armazenada no cofre corresponde à do sistema de destino. Caso a senha seja diferente, a solução deve ser capaz de gerar relatórios e alertas notificando este evento.
- 3.10. A solução deverá possuir interface de administração de credenciais via web, API REST, SDK e CLI.
- 3.11. A solução deverá ser capaz de descobrir e alterar credenciais em uma ampla gama de sistemas, incluindo, no mínimo:
 - 3.11.1. Contas Windows (locais, de domínio, de serviço).
 - 3.11.2. Contas em ambientes Linux e Unix.
 - 3.11.3. Contas em Bancos de Dados, incluindo Oracle, SQL Server, PostgreSQL, InterSystems Cache e MySQL.
 - 3.11.4. Contas do Active Directory (AD) e outros serviços de diretório compatíveis com LDAP.
 - 3.11.5. Contas de serviço utilizadas em aplicações web (e.g., Application Pools do Microsoft IIS).

- 3.11.6. Processos interdependentes e credenciais de serviço, incluindo credenciais em ambientes em cluster.
- 3.11.7. Contas em ambientes multicloud (pelo menos AWS, Azure, GCP).
- 3.12. A solução deve permitir a utilização de scripts ou tarefas personalizadas antes e/ou depois de cada tarefa de mudança de senhas para lidar com dependências complexas.
- 3.13. A solução deve ser capaz de exportar a chave de criptografia principal do cofre (ou artefato equivalente) de forma segura, para ser utilizada em cenários de recuperação de desastres, garantindo o acesso às credenciais gerenciadas.
- 3.14. Gestão de Credenciais de Aplicação e Scripts (AAPM)
 - 3.14.1. Escopo e Descoberta: A solução deve ser capaz de integrar (onboard) e gerenciar de forma centralizada as credenciais utilizadas por aplicações, serviços e scripts (identidades não-humanas), eliminando a necessidade de senhas, chaves de API ou tokens embutidos (hard-coded). A solução deve suportar, no mínimo, 20 (vinte) aplicações ou servidores de aplicações distintos.
 - 3.14.2. Padrões de Recuperação de Credenciais: A solução deve suportar, no mínimo, um dos seguintes padrões arquiteturais para a entrega segura de credenciais às aplicações:
 - a) Padrão Agentless (API/SDK): Fornecimento de APIs RESTful e SDKs documentados que permitam a aplicações e scripts requisitarem credenciais diretamente do cofre de forma segura; ou
 - b) Padrão Baseado em Agente: Fornecimento de um provedor de credenciais local (agente) que possa ser instalado no servidor da aplicação, mantendo um cache seguro para alta disponibilidade e desempenho.
 - 3.14.3. Autenticação de Identidades Não-Humanas: A solução deve prover múltiplos métodos para autenticar a aplicação requisitante antes de liberar uma credencial. Deve suportar, no mínimo, uma combinação de 2 (dois) dos seguintes atributos para definir a identidade da aplicação:
 - a) Endereço de rede (IP/DNS/CIDR) da máquina de origem.
 - b) Contexto do usuário do sistema operacional que executa o processo da aplicação.
 - c) Assinatura criptográfica (hash) do executável da aplicação.
 - d) Apresentação de um certificado de cliente TLS válido.

4. Acesso Privilegiado, Gravação e Proxy de Sessões

- 4.1. A solução deverá fornecer múltiplos métodos de acesso seguro e transparente a sistemas e dispositivos alvo, garantindo que o usuário final não precise visualizar ou manusear diretamente as credenciais privilegiadas. A solução deve atender aos requisitos de acesso das duas categorias abaixo:
 - 4.1.1. Modelos de Acesso Obrigatórios (Ambos devem ser suportados)
 - Para garantir a cobertura de casos de uso de alta segurança e acesso universal, a solução deve obrigatoriamente suportar os dois seguintes modelos:
 - 4.1.1.1. Acesso via Servidor de Salto (Jump Server / Bastion Host): Capacidade de o usuário estabelecer uma sessão RDP para um servidor de proxy seguro (o "jump server"), a partir do qual a solução lança clientes nativos (e.g., PuTTY, DBEaver, SSMS) para se conectar ao sistema de destino. Neste modelo, a autenticação no servidor final é automatizada pelo servidor de proxy, e toda a interação dentro da sessão RDP é gravada para todos os usuários contratados.
 - 4.1.1.2. Acesso via Navegador Web (HTML5): Capacidade de renderizar sessões gráficas (RDP, VNC) e de terminal (SSH) diretamente em um navegador web padrão, sem a necessidade de software cliente ou plugins na estação de trabalho do usuário.
 - 4.1.2. Modelo de Acesso com Cliente Nativo
 - Para atender às necessidades de administradores e usuários avançados que utilizam ferramentas nativas em suas próprias estações de trabalho, a solução deve suportar, ao menos, a seguinte arquitetura:
 - 4.1.2.1. Acesso via Proxy de Protocolo Nativo: Capacidade de a solução atuar como um proxy transparente para protocolos específicos, permitindo que os usuários utilizem seus clientes nativos diretamente de suas estações de trabalho. A string de conexão é modificada para apontar para o proxy, que injeta as credenciais e grava a sessão. Este modelo deve suportar, no mínimo:
 - a) Proxy SSH: (exemplo: 'ssh usuario_pam@usuario_alvo@servidor_alvo@servidor_proxy_pam').
 - b) Proxy de Banco de Dados: Para os principais protocolos de banco de dados (Oracle, PostgreSQL, Microsoft SQL Server, MySQL, MariaDB), permitindo o uso de ferramentas como DBEaver ou SQL Developer diretamente da máquina do usuário através do proxy.
 - 4.1.3. Acesso via Lançador de Aplicações com Agente Cliente: Capacidade de iniciar aplicações nativas instaladas na estação de trabalho do usuário (e.g., clientes SQL, clientes RDP/SSH nativos) e injetar as credenciais do cofre de forma automática e transparente na sessão. Este método pode fazer uso de um agente cliente local para facilitar a automação e a injeção segura de credenciais e auditoria/monitoramento da sessão.
 - 4.2. Todos os acessos realizados através dos métodos descritos acima deverão ter suas sessões registradas integralmente em vídeo e/ou texto, conforme aplicável ao protocolo.
 - 4.3. A gravação das sessões deverá incluir indexação, busca textual e proteção contra adulteração.
 - 4.4. As sessões devem ser acessíveis apenas a perfis autorizados.
 - 4.5. O proxy de banco de dados deverá ser capaz de injetar credenciais, encerrar sessões automaticamente e aplicar políticas de bloqueio de comandos específicos, de forma granular, a fim de evitar o uso de comandos SQL potencialmente danosos (e.g., DROP TABLE).
 - 4.6. A arquitetura da solução deverá ser escalável, com suporte a múltiplos nós em balanceamento de carga ou failover automático.
 - 4.7. A solução deverá permitir a criação de "Zonas de Controle" distintas, ou seja, a implantação de componentes de proxy em diferentes segmentos de rede (e.g., DMZ, redes de produção, nuvem) para otimizar o desempenho e reforçar a segurança.
 - 4.8. A solução deverá prover ferramentas de análise automatizada para as gravações de sessão, capazes de identificar e marcar comandos ou ações específicas.

5. DevOps, Containers e APIs

- 5.1. Arquitetura e Integração:
 - 5.1.1. A solução deve prover um componente ou módulo específico para o gerenciamento de segredos em pipelines de CI/CD e ambientes de contêineres, projetado para alta velocidade, baixa latência e escalabilidade massiva.
 - 5.1.2. Deve haver integração nativa ou via plugins com as principais ferramentas de automação, CI/CD e orquestração, incluindo, no mínimo: Kubernetes, OpenShift, Ansible, GitLab, Terraform e Jenkins.
 - 5.1.3. A solução deverá ser compatível com ambientes híbridos e multicloud (AWS, GCP, Azure).
 - 5.1.4. A solução deve possibilitar integração com dispositivos de Hardware Security Module (HSM) devidamente homologados pelo fabricante.
- 5.2. Gestão de Segredos e Políticas:
 - 5.2.1. A plataforma deve permitir a definição de políticas de acesso a segredos como código (Policy as Code),

permitindo que as políticas sejam versionadas, auditadas e gerenciadas.

5.2.2. A solução deve suportar a geração de segredos dinâmicos e de curta duração (just-in-time) para acesso a bancos de dados e plataformas de nuvem.

5.2.3. A solução deverá permitir a guarda de múltiplas versões de um mesmo segredo.

5.2.4. A solução deverá realizar a rotatividade de segredos, quando cabível, tanto em sua complexidade quanto em tempo de expiração, conforme as políticas definidas.

5.2.5. A solução deve fornecer meios de revogar completamente o acesso a um segredo sob demanda ou por meio de definição de políticas.

5.2.6. As secrets deverão ser armazenadas de forma segura e serem disponibilizadas para a aplicação por meio de conexão criptografada.

5.3. Autenticação de Identidades de Máquinas e Aplicações

5.3.1. A solução deve prover múltiplos métodos de autenticação para identidades não-humanas (máquinas, workloads, contêineres), eliminando a necessidade de segredos estáticos pré-configurados. A solução deve suportar, no mínimo, os seguintes métodos de autenticação:

a) Baseado em Identidade Nativa de Nuvem: Capacidade de autenticar um workload com base em sua identidade nativa do provedor de nuvem (e.g., AWS IAM Roles, Azure Managed Identities, GCP Service Accounts).

b) Baseado em Identidade de Orquestrador: Capacidade de autenticar um contêiner com base em seus atributos da plataforma de orquestração (e.g., Kubernetes Namespace e Service Account).

c) Baseado em Certificado: Autenticação mútua via TLS (mTLS), onde o workload apresenta um certificado de cliente válido.

d) Baseado em Token: Capacidade de validar um JSON Web Token (JWT) ou um token OIDC emitido por um provedor de identidade confiável.

5.4. Administração, Auditoria e Licenciamento:

5.4.1. A solução deverá prover uma interface web e uma API REST de administração para gerenciamento do cluster, componentes, usuários, segredos e políticas.

5.4.2. A solução deverá prover auditoria e log de todos os eventos de segurança (solicitação, revogação, acesso, alterações de permissão) de forma aderente à RFC 5424 (Syslog) e com garantia de imutabilidade.

5.4.3. A solução deve garantir alta disponibilidade por meio da replicação de secrets entre diferentes nós.

5.4.4. A solução deverá atender um ambiente composto por, no mínimo, 2 (dois) clusters de orquestradores de containers com 60 (sessenta) hosts distribuídos e 1.000 (um mil) aplicações consumindo 5.000 (cinco mil) segredos armazenados.

6. Gestão de Identidade e Autenticação

6.1. Arquitetura de Bastião com Autenticação Local: A solução deve, obrigatoriamente, ser capaz de operar com um diretório de utilizadores local e independente, desacoplado de serviços de diretório externos como Active Directory ou Microsoft Entra ID. A plataforma deve ser capaz de autenticar os seus próprios administradores e contas de emergência ("break-glass") utilizando exclusivamente este diretório local, que deve suportar, no mínimo, políticas de senha granulares e a imposição de Autenticação Multifator (MFA) nativa.

6.2. Capacidade de Federação como Provedor de Serviço (SP): Para fins de integração com a infraestrutura corporativa, a solução deve também ser capaz de atuar como um Provedor de Serviço (SP) padrão, integrando-se com IdPs externos via SAML 2.0 ou OIDC para autenticação de usuários operacionais.

6.3. É obrigatório o suporte à autenticação multifator (MFA) com múltiplos mecanismos, incluindo, no mínimo:

6.3.1. senhas de uso único baseadas em tempo (TOTP);

6.3.2. notificações push;

6.3.3. certificados X509; e

6.3.4. padrões FIDO2/WebAuthn:

6.3.4.1. Suportar minimamente Windows Hello ou Yubikey.

6.3.4.2. Permitir cadastro e alteração de dispositivo FIDO2 por usuário.

6.4. A autenticação deverá suportar mecanismos de adaptação baseados em risco e contexto.

6.5. A solução deve ser extensível, oferecendo um framework ou APIs que permitam o desenvolvimento de integrações com mecanismos de autenticação personalizados ou legados.

6.6. A interface de administração deverá prover um painel de monitoramento em tempo real que exiba as sessões privilegiadas ativas, permitindo a intervenção de um administrador (e.g., visualização ao vivo e término forçado da sessão).

6.7. A solução deverá oferecer conectores para diretórios LDAP, AD e provedores de identidade em nuvem.

6.8. Para casos de delegação de identidade, como em cenários de duplo salto (double-hop), a solução deverá suportar o encaminhamento da identidade federada original (via token forwarding ou técnica similar).

6.9. A solução deverá permitir a assunção de identidade delegada por prazo determinado e sob fluxo de autorização.

6.10. A solução deverá prover auditoria completa da cadeia de autenticação e delegação, registrando de forma clara quem acessou qual recurso em nome de quem.

7. Alta Disponibilidade e Arquitetura

7.1. A solução deverá ser implantada em arquitetura de alta disponibilidade (HA).

7.2. É obrigatório que a solução principal (onde são armazenadas as secrets) funcione, ao menos, em duas localidades físicas do CONTRATANTE, com replicação ativa-ativa ou ativa-passiva com Disaster Recovery Automático em caso de indisponibilidade do nó originalmente ativo.

7.3. Os nós secundários deverão assumir automaticamente as funções dos nós primários em caso de falha, com tempo de resposta inferior a 5 minutos.

7.4. A solução deverá manter a consistência dos dados replicados.

7.5. A arquitetura deverá permitir escalabilidade horizontal (adição de mais nós ao cluster para aumentar a capacidade) e suportar uma topologia híbrida (componentes on-premises e na nuvem gerenciados de forma centralizada).

7.6. A solução deverá prover ambiente espelho completo para testes, treinamento e homologação.

7.7. O CONTRATANTE irá prover a infraestrutura (servidores/software em ambiente virtualizado, camada de balanceamento/redirecionamento de tráfego) para implantação e uso da solução em ambiente on-premises.

7.7.1. Caso a solução fornecida faça uso de hardware próprio (appliances), estes devem ser fornecidos pela CONTRATADA, no quantitativo necessário para atender aos requisitos de arquitetura e alta disponibilidade, com todas as licenças válidas, com garantia igual ao do objeto desta contratação e sem custos adicionais para o CONTRATANTE.

7.8. A solução deve permitir o Backup e Recovery de seu Banco de Dados e de todas as configurações de software, com as seguintes capacidades:

7.8.1. Permitir a execução de tarefas de backup sem a necessidade de agentes de terceiros e com criptografia do arquivo de backup.

7.8.2. Permitir a execução de Backups automatizados, com agendamento de horários.

7.9. A solução deverá prover mecanismos para controle e otimização da carga de trabalho interna, de modo a possibilitar o ajuste de parâmetros de desempenho de acordo com as características do ambiente.

8. Monitoramento e Análise Comportamental

8.1. A solução deverá incluir módulo nativo de análise de comportamento (UBA – User Behavior Analytics) ou se integrar com solução de SIEM/SOAR/UEBA externa em uso no Tribunal, atualmente Microsoft Sentinel.

8.1.1. Caso a funcionalidade seja atendida por meio de integração com solução externa, a CONTRATADA será responsável por efetuar todas as configurações necessárias na solução externa.

8.2. O sistema deverá identificar automaticamente padrões comportamentais suspeitos.

8.3. A ferramenta deverá permitir a classificação de eventos por níveis de risco e resposta automática.

8.4. As detecções deverão suportar a correlação entre múltiplos eventos para identificar o encadeamento de ações.

8.5. A análise deverá permitir a associação entre usuários e ativos comprometidos.

8.6. É mandatório que o motor de análise detecte tentativas de evasão de controles, escalonamento de privilégios e movimentação lateral.

8.7. A interface de monitoramento deverá incluir dashboards personalizáveis e histórico completo de alertas.

8.8. O mecanismo de análise comportamental deverá suportar customização de regras e aprendizado supervisionado.

9. Gestão de Privilégios em Nuvem

9.1. Preferencialmente, a solução deverá implementar o uso de credenciais efêmeras para atribuição de privilégios em nuvem, mitigando os riscos de acesso em ambientes de nuvem.

9.1.1. Deve permitir acesso operacional efêmero com privilégios temporários, eliminando acessos permanentes a ambientes sensíveis.

9.1.2. A solução deve gerar identidades temporárias, como usuários ou certificados efêmeros, para cada conexão autorizada.

9.1.3. A identidade efêmera deve ser criada automaticamente no início da sessão e removida após encerramento.

9.1.4. Certificados, usuários ou tokens criados devem ser efêmeros e não reutilizáveis entre sessões.

9.2 Caso a solução não implemente credenciais efêmeras, deverá ser capaz de gerenciar os riscos de acesso em ambientes de nuvem. Esta capacidade deverá incluir, no mínimo:

9.2.1. Análise e Otimização de Direitos:

9.2.1.1. Analisar os direitos para identificar riscos como excesso de privilégios, direitos dormentes e combinações tóxicas.

9.2.1.2. Utilizar Machine Learning (ML) ou tecnologia apropriada para recomendar o dimensionamento correto dos direitos (right-sizing).

9.2.1.3. Apresentar um indicador ou score de risco quantificável.

9.2.2. Remediação e Aplicação de Políticas:

9.2.2.1. Permitir a criação de políticas de segurança ("guardrails") para prevenir a atribuição de permissões de alto risco.

9.2.3. Acesso Just-in-Time (JIT) para Nuvem:

9.2.3.1. Orquestrar o acesso temporário e sob demanda (JIT) para consoles de gerenciamento de nuvem e workloads, provisionando e 'desprovisionando' dinamicamente as permissões necessárias para a sessão.

9.2.4. Auditoria e Conformidade Específica para Nuvem:

9.2.4.1. Gerar relatórios detalhados sobre o estado dos direitos na nuvem para fins de auditoria e conformidade.

10. Acesso Remoto

No que se refere ao acesso remoto privilegiado (prestadores/usuários externos), a solução deverá:

10.1. Possuir funcionalidade que permita a conexão segura de usuários pela Internet, sem a necessidade de instalação e configuração de clients ou VPN (VPN-less) suportando, no mínimo, 5 usuários concorrentes.

10.2. Disponibilizar todos os recursos para as sessões remotas, incluindo gravação de sessão, acompanhamento em tempo real, bloqueio de comandos, análise de comportamento e registro de auditoria, entre outros.

10.3. Tratar usuários terceiros e servidores do tribunal de forma diferenciada, permitindo que os servidores tenham acesso total à ferramenta, enquanto terceiros tenham acesso restrito à console, sem opções de configuração da ferramenta.

10.4. Permitir a liberação granular do acesso externo, usuário a usuário, para que o administrador possa definir exatamente quais credenciais e dispositivos poderão ser acessados.

10.5. Possibilitar a definição do período de validade da liberação de acesso.

10.6. Permitir a revogação de acessos previamente liberados.

10.7. Permitir a liberação de acesso mediante aprovação, onde o usuário pode solicitar o acesso a uma credencial, que será concedido apenas com uma justificativa e a aprovação de, pelo menos, um aprovador.

11. Auditoria, Relatórios e Conformidade

11.1. A solução deverá oferecer auditoria completa e contínua de todas as atividades realizadas em seus módulos.

11.2. Todos os registros de auditoria deverão estar em conformidade com a RFC 5424 (Syslog) e serem imutáveis.

11.3. Os relatórios deverão abranger diferentes dimensões (operacionais, gerenciais, conformidade) e serem exportáveis.

11.4. A solução deverá incluir uma interface de consulta de dados de auditoria que suporte buscas complexas e interativas, permitindo que analistas e auditores gerem relatórios para análise de incidentes e conformidade de forma eficiente, sem a necessidade de conhecimento em linguagens de consulta de banco de dados (e.g., SQL).

11.5. A solução deve integrar-se diretamente, sem codificação adicional ou adição de scripts, com as principais soluções de SIEM do mercado, enviando logs formatados sobre, no mínimo: atividades administrativas, recuperação e alteração de senhas, e atividades dos usuários na aplicação.

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

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

12. Requisitos Operacionais e de Usabilidade

12.1. A solução deve prover uma 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.

12.2. A solução deve disponibilizar uma interface única e centralizada para administração de todos os recursos, acessos, usuários, políticas, auditorias e relatórios.

13. Requisitos de Instalação, Configuração, Manutenção, Atualização e Migração

13.1. Responsabilidade Integral: A CONTRATADA será integralmente responsável pela prestação de todos os serviços profissionais necessários para a completa implantação, configuração, manutenção, atualização e operacionalização da solução

ofertada, em conformidade com todos os requisitos estabelecidos neste documento.

- 13.1.1. A proposta deve contemplar o serviço de instalação e configuração padrão da solução contratada.
- 13.1.2. A instalação e configuração deverá ser planejada e documentada previamente pela CONTRATADA em conjunto com a equipe técnica da CONTRATANTE, onde devem ser definidos todos os passos necessários para a instalação, incluindo o cronograma e plano de testes.
- 13.1.3. A instalação e configuração deverá ser executada por profissional com conhecimento certificado na plataforma ofertada.
- 13.1.4. A instalação e configuração deverá ser realizada em conformidade com as melhores práticas e guias de deployment do FABRICANTE da solução adquirida, em conjunto com a equipe técnica da CONTRATADA.
- 13.1.5. Deverá realizar todas as configurações de políticas, tarefas, automações, zonas de exclusão, relatórios, entre outros.
- 13.1.6. A CONTRATADA deverá fornecer documentação da configuração da solução após execução dos serviços (as-built).
- 13.1.7. Toda documentação deverá ser fornecida em formato digital.
- 13.1.8. A CONTRATADA deverá realizar os testes de instalação de toda a solução, específicos para o produto que está sendo instalado, verificação do funcionamento do produto e verificação de que os softwares em uso estejam na versão mais recente disponibilizada (versão estável recomendada).
- 13.1.9. A realização dos serviços deve ser planejada de acordo com disponibilidade de ambas as partes. O planejamento anterior ao serviço pode ser realizado remotamente através de videoconferência.
- 13.1.10. Todos os parâmetros a serem configurados deverão ser alinhados entre as partes em reuniões de pré-projeto, devendo a CONTRATADA sugerir as configurações de acordo com normas técnicas e boas práticas de mercado e do FABRICANTE, cabendo à CONTRATANTE a sua aceitação expressa ou recusa nos casos de não atendimento das condições estabelecidas.
- 13.1.11. Para os itens que exigirem paradas ou risco de parada do equipamento em produção, a instalação, manutenção e atualização deverá ser planejada junto à equipe técnica da CONTRATANTE e ocorrer em horário definido por esta, inclusive fora do horário comercial.
- 13.1.12. A instalação, configuração, manutenção e atualização deverão ser efetuadas de forma a não comprometer o funcionamento dos sistemas, recursos ou equipamentos atualmente em operação.
- 13.1.13. A instalação, configuração, manutenção e atualização deverão ser realizadas de tal forma que as interrupções no ambiente de produção sejam as mínimas possíveis e estritamente necessárias, devidamente planejadas e, ainda, não causem transtornos aos usuários finais da CONTRATANTE.
- 13.1.14. É de responsabilidade da CONTRATADA a instalação de todos os produtos e a integração destes ao ambiente da CONTRATANTE sem prejuízo às operações.
- 13.2. Migração da Solução Existente: Caso a solução seja diferente da atualmente em uso (Core PAS/PAM Self Hosted CyberArk), a CONTRATADA será responsável por planejar e executar a migração completa para a nova plataforma. Este processo deve incluir, no mínimo:
 - 13.2.1. A migração de todos os cofres (safes), contas, conectores, políticas e configurações existentes.
 - 13.2.1.1. Para mensuração de esforço, considerar, no mínimo: 330 cofres, 3300 contas, 30 políticas de gerenciamento de contas (complexidade de senha, periodicidade de rotação etc.), 50 conectores [RDP, SSH, WinSCP, conectores de BDs (SQL ServerMgmtStudio, DBeaver), Web, Snap-in MMC.exe, entre outros].
 - 13.2.2. A migração do histórico de gravações de sessão, na medida em que for tecnicamente viável e compatível entre as plataformas.
 - 13.2.3. A reconfiguração ou desenvolvimento de todas as integrações e plugins atualmente em uso para garantir a continuidade operacional.
 - 13.2.4. Plano de Migração: A CONTRATADA deverá apresentar um Plano de Migração detalhado em até 15 (quinze) dias após a emissão da Ordem de Serviço inicial. Este Plano deve conter o cronograma de atividades, a alocação de recursos, a metodologia de migração e os critérios de aceite, e deverá ser formalmente aprovado pelo CONTRATANTE antes do início da execução.
- 13.3. Cronograma de Implantação: A implantação da solução, incluindo a migração descrita no item 13.2, se necessária, deverá ser concluída no prazo máximo de 3 (três) meses a contar da data de aprovação do Plano de Migração.

14. Requisitos de Garantia e Suporte Técnico:

- 14.1. O serviço de suporte será executado pela CONTRATADA, durante todo o período de vigência do contrato, que corresponde ao prazo mínimo de garantia dos softwares, devendo ser iniciado no primeiro dia útil após o aceite definitivo da solução, na seguinte forma:
 - 14.1.1. Promover atualização de módulos e novas versões do software conforme disponibilização pela fabricante.
 - 14.1.2. Promover instalação de releases e patches de manutenção desenvolvidos durante o período.
 - 14.1.3. Fornecer conectores, plugins e/ou quaisquer integradores existentes ou que vierem a ser necessários à adequação aos sistemas da contratante, atuais e futuros, tanto do executável quanto do código-fonte correspondente, bem como a documentação de todas modificações e configurações realizadas, quando não fornecidos pela fabricante.
 - 14.1.4. Avaliar, sugerir e promover mudanças de arquitetura da solução, mediante solicitação da equipe do TJDFT.
 - 14.1.5. Oferecer suporte via canais digitais (telefone, chat, e-mail) para atendimento de chamados em regime de 24 horas por dia e 7 dias por semana, garantindo atendimento em no máximo 2h para eventos com indisponibilidade da solução por completo, 24h para eventos com indisponibilidade em funcionalidades específicas/pontuais e 72h para eventos eventos não enquadrados nos anteriores.
 - 14.1.6. Acompanhar toda solicitação de chamado de suporte remoto através dos canais de atendimento da fabricante quando necessário.
 - 14.1.7. Disponibilizar base de conhecimentos de solução de problemas e documentos técnicos.
 - 14.1.8. Auxiliar o TJDFT no seu registro junto ao site de licenciamento da fabricante.
 - 14.1.9. Auxiliar o TJDFT na ativação e consumo dos benefícios relacionados às licenças contratadas.

15. Repasse de conhecimento

- 15.1. A CONTRATADA deverá realizar repasse de conhecimento *hands-on* da solução para equipe técnica indicada pela CONTRATANTE, com as seguintes características:
 - 15.1.1. Deverá ser realizado por um técnico com conhecimento certificado na solução ofertada.
 - 15.1.2. Deverá possuir carga horária mínima de 20 horas.
 - 15.1.3. Deverá fornecer uma comprovação de repasse de conhecimento (certificado de conclusão/participação).
 - 15.1.4. Deverá disponibilizar material didático, manuais técnicos ou qualquer outro material que auxilie no repasse de conhecimentos.
 - 15.1.5. Deverá fornecer o treinamento para, no mínimo, uma turma com 10 (dez) servidores do TJDFT.

- 15.1.6. Deverá ser realizado nas dependências da CONTRATANTE ou de forma remota, conforme alinhamento prévio.
- 15.1.7. Poderá ser realizado em horário de expediente do TJDF, ou em horário diverso, em dias úteis, conforme alinhamento prévio entre o CONTRATANTE e a CONTRATADA.
- 15.1.8. O CONTRATANTE não assumirá os custos de licenças e/ou softwares extras, diárias e transporte dos instrutores, assim como outros custos relativos a esta capacitação. Todos os custos devem ser previstos pela CONTRATADA da solução na elaboração de suas propostas.
- 15.1.9. Ao término do processo de Repasse de Conhecimento, a CONTRATADA deverá realizar uma avaliação de satisfação em relação ao curso, como conteúdo, instalações, material didático e de aplicação à prática profissional, bem como do(s) instrutor(es).
- 15.1.10. Caso seja considerado insatisfatório, a CONTRATADA deverá realizar um novo Repasse de Conhecimento, com a finalidade de atender às demandas não supridas inicialmente.

VII - Alinhamento Estratégico

1. Alinhamento entre a Contratação e os Planos da Administração e da Área de TIC

1.1. Alinhamento com o Plano Estratégico do Tribunal - [PE](#)

Alinhamento com o Plano Estratégico do Tribunal – PE 2021-2026

- **Perspectiva:** Processos Internos
 - PI.8: Incrementar as políticas e os processos de segurança.
 - PI.8.E1: Incrementar a segurança da informação e a proteção de dados pessoais.

1.2. Congruência com a Estratégia Nacional de TIC do Poder Judiciário - [ENTIC-JUD](#)

Congruência com os objetivos da Estratégia Nacional de Tecnologia da Informação e Comunicação - ENTIC-JUD 2021-2026

- **Perspectiva:** Processos Internos
 - Objetivo Estratégico 7 - Aprimorar a Segurança da Informação e a Gestão de Dados: Melhorar os avanços voltados para a Segurança da Informação e dados pessoais frente aos mais diversos desafios, fazendo-se valer principalmente das vantagens oriundas da utilização de Inteligência Artificial e demais soluções disruptivas de TIC.

1.3. Aderência com as seguintes ações do [PDTIC](#)

Aderência com as seguintes ações do Plano Diretor de Tecnologia da Informação e Comunicação - PDTIC 2025

- Ação SI40.1: Estudo para contratação ou expansão de solução de gestão de acessos privilegiados (PAM).

1.4. Conformidade com o Plano de Contratações Anual - [PCA](#)

- Iniciativa SETI_013 - Renovação de garantia, atualização e ampliação de licenças de uso de solução de gestão de acessos privilegiados.

VIII - Justificativa da Solução Escolhida

Dica: A Justificativa deve ser clara, precisa e suficiente para demonstrar as reais necessidades da contratação.

1. Fundamentação:

A presente contratação visa atender às demandas do TJDF relacionadas a solução de gestão de acessos privilegiados com licenciamento por subscrição, incluindo serviços de instalação, configuração, repasse de conhecimento e garantia pelo período de 36 (trinta e seis) meses.

Conforme exposto, neste presente estudo, apenas a Solução 2 foi considerada viável para a presente contratação, tendo em vista que as soluções 1, 3 e 4 não atendem plenamente as necessidades do órgão.

No Tribunal, além das rotinas já estabelecidas que são imprescindíveis para manter a segurança da informação, as necessidades que surgiram devido as novas formas de trabalho a distância também se tornaram indispensáveis. Segundo o Tribunal de Contas da União (TCU), o Brasil foi o quinto país do mundo com maior incidência de ataques de *ransomware* (“sequestro” de dados). Com a nova realidade de teletrabalho, o acesso aos sistemas corporativos disponíveis na rede interna do Tribunal passou a necessitar do acesso externo de forma extensiva. Essa nova situação aumenta a

exposição do ambiente de TIC, que agora está mais vulnerável às ameaças cibernéticas vindas do ambiente externo. Dessa forma, novos desafios de segurança de informação surgem, demandando ações e ferramentas que ainda não fazem parte da realidade do TJDF. Logo, a aquisição de soluções TIC focadas em segurança de informações, é estritamente necessária para mitigar os riscos advindos do novo ambiente de trabalho e da sofisticação crescente das ameaças digitais.

A adoção da Solução 2 - Seleção de empresa especializada para o fornecimento de solução de gestão de acessos privilegiados com licenciamento por subscrição, incluindo serviços de instalação, configuração, repasse de conhecimento e garantia para utilização pelo TJDF pelo período de 36 (trinta e seis) meses - faz-se necessária tendo em vista que a ausência de tal ferramenta poderá permitir que usuários internos ou externos mal intencionados possam explorar ameaças não detectadas previamente, resultando em possíveis ataques cibernéticos que comprometam a integridade, confidencialidade ou disponibilidade de sistemas críticos para o Tribunal, como o Processo Judicial Eletrônico (PJe), o Sistema Eletrônico de Informações (SEI), os sistemas de gestão de pessoas ou qualquer outro sistema eletrônico essencial.

Os benefícios acima relacionados remetem à garantia de confidencialidade, integridade e disponibilidade da informações armazenadas por este Tribunal, tendo em vista os novos cenários de ameaças à segurança da informação.

IX - Planejamento e Sustentação da Contratação

1. Identificação dos benefícios a serem alcançados com a solução escolhida em termos de eficácia, eficiência, economicidade, efetividade e padronização

A solução de gestão de acessos privilegiados pretendida por este projeto de aquisição visa, sobretudo:

- Ampliar os mecanismos de segurança da informação existentes no TJDF;
- Prover confidencialidade, integridade e disponibilidades das informações;
- Atender aos planejamentos da administração e da área de TIC;
- Atender aos requisitos da Estratégia Nacional de Segurança Cibernética do Poder Judiciário (ENSEC-PJ) e demais normativos de gestão de segurança da informação, no que tange ao gerenciamento de identidades, acessos e privilégios;
- Atender aos requisitos de Segurança da Informação contidos na ENSEC-JUD e demais normativos de gestão de segurança da informação.
- Aprimorar o nível de maturidade em segurança cibernética no âmbito do TJDF.
- Proteção de dados e ativos de informação.
- Modernizar os recursos de proteção de identidades e credenciais privilegiadas acrescentando funcionalidades não disponibilizadas pela solução atual.
- Possibilitar a ampliação do escopo de utilização da solução para áreas além da SETI.
- Ampliar o quantitativo de usuários e credenciais privilegiadas protegidas.
- Aumentar a eficiência operacional.

2. Os resultados pretendidos em efetividade e desenvolvimento nacional sustentável:

Os manuais técnicos, documentação e outros materiais porventura produzidos no escopo do contrato deverão ser entregues, preferencialmente, em formato digital aberto;

3. Observância aos requisitos do Modelo Nacional de Interoperabilidade (MNI):

Dica:

[CNJ TACT 058/2009](#) - Estabelecimento de padrões para intercâmbio de informações de processos judiciais e assemelhados entre os diversos órgãos de administração da justiça.

O Modelo Nacional de Interoperabilidade (MNI) definiu-se pelas equipes técnicas dos órgãos (STF - CNJ - STJ - CJF - TST - CSJT - AGU - CNMP e PGR), de acordo com as metas do Termo de Cooperação Técnica nº 58/2009. Visa estabelecer os padrões para intercâmbio de informações de processos judiciais e assemelhados entre os diversos órgãos de administração de justiça, além de servir de base para implementação das funcionalidades pertinentes no âmbito do sistema processual. Elabora e implementa o padrão nacional de integração de sistemas de processo eletrônico, por meio da tecnologia de Webservice.

Este modelo não é aplicável a esta contratação, por não se tratar de desenvolvimento de software.

4. Aderência às regulamentações da Infraestrutura de Chaves Públicas Brasileira (ICP-Brasil) :

Dica: Link [Legislação](#) - Para soluções que necessitem de utilização de certificação digital.

A Infraestrutura de Chaves Públicas Brasileira (ICP-Brasil) é uma cadeia hierárquica e de confiança que viabiliza a emissão de certificados digitais para identificação virtual do cidadão. Observa-se que o modelo adotado pelo Brasil foi o de certificação com raiz única, sendo que o Instituto Nacional de Tecnologia da Informação (ITI), além de desempenhar o papel de Autoridade Certificadora Raiz (AC – Raiz), também tem o papel de credenciar e descredenciar os demais participantes da cadeia, supervisionar e fazer auditoria dos processos.

A fim de garantir a compatibilidade com a ICP-Brasil, é fundamental que toda contratação que necessite trabalhar com certificados digitais esteja a ela alinhada.

Embora certificados ICP-Brasil possam ser utilizados no escopo de funcionalidades da solução, não são requisito necessário ao seu funcionamento e emprego.

Declaramos que este modelo não é aplicável a esta contratação, por não possuir necessidade do uso de Certificados Digitais ICP-Brasil.

5. Alinhamento com o Modelo de Requisitos para Sistemas Informatizados de Gestão de Processos e Documentos do Judiciário Brasileiro (MoReq-Jus)

Dica: [CNJ RES. Nº 91 de 29/09/2009](#) - Regras mínimas para garantir, dentre outros requisitos, a confiabilidade, autenticidade e acessibilidade de documentos geridos pela solução.

O Modelo de Requisitos para Sistemas Informatizados de Gestão de Processos e Documentos do Poder Judiciário (MoReq-Jus) apresenta os requisitos que os documentos digitais produzidos pelo Judiciário e os sistemas informatizados de gestão documental deverão cumprir, no intuito de garantir a segurança e a preservação das informações, assim como a comunicação com outros sistemas.

A motivação está na criação de um padrão uniforme de elaboração de sistemas processuais e de gestão documental capazes de atender às necessidades e de se adaptar às particularidades dos diferentes órgãos da Justiça brasileira.

Ao adotar o MoReq-Jus, o CNJ efetiva as recomendações da Carta da Organização das Nações Unidas para a Educação, a Ciência e a Cultura (Unesco) para a Preservação do Patrimônio Arquivístico Digital, que incentiva o estabelecimento de políticas públicas, metodologias e normas que minimizem a fragilidade de softwares e assegurem, ao longo do tempo, a autenticidade, a integridade e o acesso contínuo de documentos por todos os segmentos da sociedade.

A Resolução nº 91, de 29 de setembro de 2009, publicada no DOU, Seção 1, em 9/10/09, p. 242, e no DJ-e nº 172/2009, em 9/10/09, p. 5- 6, e Anexo publicado no DJ-e nº 178/2009, em 21/10/09, p. 5-167, institui o MoReq-Jus e disciplina a obrigatoriedade da sua utilização no desenvolvimento e manutenção de sistemas informatizados para as atividades judiciais e administrativas no âmbito do Poder Judiciário.

Para esta contratação, o MoReq-Jus não é aplicável, pois não trata de desenvolvimento ou aquisição de software relacionado a processos eletrônicos.

6. Avaliação das necessidades e adequação do ambiente para execução contratual:

Infraestrutura tecnológica	Não haverá necessidade de adequação da infraestrutura tecnológica física, as principais soluções analisadas ofertam appliances virtuais. Para implantar adequadamente as licenças adquiridas, podem ser necessárias atualizações de menor impacto nos ambientes operacionais do TJDFT.
Infraestrutura elétrica	Não há necessidade de adequação da infraestrutura elétrica.
Logística de implantação	Para instalação de appliances virtuais não há necessidade de adequação relacionada à logística de implantação.
Espaço físico e mobiliário	Não há necessidade de adequação do espaço físico.
Impacto ambiental	Não são esperados impactos ambientais.

7. Recursos Necessários à Continuidade do Negócio

7.1. Recursos Materiais

Recurso 1	Link de conectividade entre TJDFT e ambiente de nuvem utilizados	Qtde	2
Disponibilidade	A SETI conta com link de conectividade à Internet, necessário à comunicação com ambiente em nuvem da solução vencedora para fornecimento de recursos de proteção, caso possua algum módulo nessa modalidade.		
Ação	Monitorar utilização do link atual e validar se há necessidade de contratação de links dedicados adicionais.		
Resp. pela ação	COINF		

7.2. Recursos Humanos

Recurso 1	Profissionais com experiência em segurança da informação e com conhecimento nas rotinas e políticas de infraestrutura de TI do TJDFT.
Formação	Servidores do quadro do TJDFT lotados na SETI/COSEC.
Atribuições	Atuação efetiva no acompanhamento, na gestão, na fiscalização e na absorção do conhecimento previstos nesta contratação.

Recurso 2	Fiscal Requisitante
Formação	Servidores do quadro do TJDFT lotados na COSEC.
Atribuições	Atuação efetiva no acompanhamento, na gestão, na fiscalização e na absorção do conhecimento das áreas de especialidade dos serviços previstos nesta contratação.

Recurso 3	Fiscal Técnico
Formação	Servidores do quadro do TJDFT lotados nos núcleos subordinados a COSEC.
Atribuições	Servidor do TJDFT responsável pela fiscalização técnica do contrato.

Recurso 4	Fiscal Administrativo
Formação	Servidores do quadro do TJDFT.
Atribuições	Servidor do TJDFT responsável pela fiscalização do contrato quanto aos aspectos administrativos.

Recurso 5	Gestor do Contrato
Formação	Servidores do quadro do TJDFT lotados na COACTI/NUACTI.
Atribuições	Servidor do TJDFT responsável pela coordenação do processo de gestão e fiscalização da execução contratual.

8. Estratégia de Continuidade Contratual

Evento 1	Descontinuidade na prestação do objeto durante ou após a vigência contratual.
Ações Preventivas ou de Contingência	Sector Responsável
Proceder com a aplicação das cláusulas contratuais estipuladas para o caso	NUACTI
Reativação do ambiente Cyberark com licenças perpétuas	COSEC

Planejar nova contratação junto a outro fornecedor	COSEC
--	-------

9. Ações para Transição e Encerramento Contratual

Dica: Informações como entrega de versões finais dos produtos, passagem de know-how, devolução de recursos materiais, revogação de perfis de acesso, eliminação de caixas postais, etc.

Ação 1	Fornecer backup criptografado de todos os dados, configurações e informações relevantes para o funcionamento da solução.
Início	30 dias antes do término do contrato
Término	Ao término do contrato
Responsável	CONTRATADA

Ação 2	Eliminar todos os dados da CONTRATANTE do ambiente do(s) provedor(es).
Início	30 dias antes do término do contrato
Término	De acordo com o Plano de Transição.
Responsável	CONTRATADA e CONTRATANTE.

Ação 3	Transferência de conhecimento para equipe técnica do TJDFT por meio de: base de conhecimento e documentação disponibilizada; relatórios; chamados atendidos; solicitações formais de atendimentos (telefônico, ferramenta online ou correio eletrônico), orientações e acompanhamento de procedimentos; arquitetura utilizada, implantações e ajustes realizados, consultorias prestadas.
Início	Início da vigência contratual.
Término	Encerramento da vigência contratual.
Responsável	CONTRATADA

10. Regras para Estratégia de Independência com Relação à Contratada

10.1. Forma de Transferência de Conhecimento

Seq	Descrição do item a ser transferido	Forma de transferência
1	Documentação descritiva dos recursos utilizados, modificações implementadas e configurações e adequações realizadas.	Meio digital
2	A CONTRATADA deverá realizar o repasse de conhecimento de operacionalização da plataforma para as equipes do TJDFT após a assinatura do contrato e sem custos adicionais para O TJDFT.	Transferência de conhecimentos para equipe técnica do TJDFT por meio de: base de conhecimento e documentação disponibilizada; relatórios; chamados atendidos; solicitações formais de atendimento (telefônico, ferramenta on-line ou correio eletrônico), orientações e acompanhamento de procedimentos; consultorias especializadas; atualizações e correções realizadas.

10.2. Direitos de Propriedade Intelectual e Autorais da Solução:

Dica: Relacionar e justificar aqui também, caso alguns produtos decorrentes da contratação sejam de direito exclusivo da contratada.

O direito patrimonial, de propriedade intelectual e autoral dos produtos gerados em decorrência da execução do objeto contratado serão de exclusiva e permanente propriedade do TJDFT, constituindo segredo comercial, ficando a CONTRATADA impedida, sob pena da lei, de utilização para outros fins que não aqueles previstos no contrato.

11. Adequação Orçamentária e Cronograma Físico-financeiro

a) Fonte de recursos e classificação orçamentária

Plano Orçamentário	0006 - Manutenção de Sistemas de Tecnologia da Informação
Plano Orçamentário	SEG0 - Segurança da Informação nas Unidades do Poder Judiciário
Plano Orçamentário	TISI - Capacitação de Servidores Efetivos e Comissionados das Unidades de TI

b) Estimativa de Impacto Orçamentário

Valor estimado	R\$ 7.526.835,94
Exercício financeiro	item 1 - solução: 2025 (R\$ 6.776.982,94) item 2 - suporte técnico: 2026 (249.951,00) e 2027(249.951,00) e 2028 (249.951,00)
Percentual do orçamento	100%
Análise e conclusão	A presente contratação faz parte das contratações previstas no PAC 2025, sob a ação SETI_013 , compatível com o valor estimado para a contratação (R\$ 2.500.000,00/ano)*.

* Cumpre salientar que o valor informado no Plano de Contratações Anual - PCA 2025 foi estimado considerando-se a perspectiva do **custo anual** da contratação, uma vez que o período de contratação ainda não fora determinado.

c) Cronograma de Execução Físico-financeira

Marco	Prazo máximo (em dias)	Evento	Responsável	Previsão de Desembolso*
Dia D0	-	Assinatura do contrato entre o CONTRATANTE e a empresa licitante vencedora.	TJDFT e CONTRATADA	0%
Dia D1	D0 + 5	Reunião inicial do contrato.	TJDFT e CONTRATADA	0%
Dia D2	-	Emissão da Ordem de Serviço pelo CONTRATANTE.	TJDFT	0%
Dia D3	D2 + 15	Apresentação do Plano de Migração, caso necessário.	CONTRATADA	0%
Dia D4	D3 + 15	Aprovação do Plano de Migração, caso necessário.	TJDFT	0%
Dia D5	D2 + 30	Entrega dos documentos que comprovem o fornecimento e a ativação das licenças contratadas, da solução as-built' e instalação dos appliances.	CONTRATADA	0%
Dia D6	D5 + 7	Emissão do Termo de Recebimento Provisório, para conferência dos produtos e serviços entregues e autorização para emissão de faturamento.	TJDFT	50%
Dia D7	D4+90	Conclusão da Migração, caso necessária.	CONTRATADA	0%
Dia D8	D7 + 14	Emissão do Termo de Recebimento Definitivo, autorização para emissão de faturamento e início do período de garantia e de execução do serviço de suporte técnico.	TJDFT	50%

* A previsão de desembolso considera o valor do item 1 (solução), uma vez que o item 2(suporte técnico) será realizado mensalmente após a Emissão do Termo de Recebimento Definitivo.

X - Declaração de Viabilidade da Contratação

Dica:

Na contextualização, referenciar principalmente o conteúdo dos itens:

- A descrição e a justificativa da solução escolhida. (VI e VIII)

- Identificação dos benefícios a serem alcançados em termos de eficácia, eficiência, economicidade, efetividade e padronização (IX.1).

1. Contextualização:

Com base nas informações levantadas neste ETP, a equipe de planejamento deste projeto declara explicitamente que a contratação é viável para a:

Seleção de empresa especializada para o fornecimento de solução de gestão de acessos privilegiados com licenciamento por

subscrição, incluindo serviços de instalação, configuração, repasse de conhecimento, garantia e suporte técnico pelo período de 36 (trinta e seis) meses, conforme as especificações técnicas do Termo de Referência e seus anexos.

A necessidade da contratação é clara e adequadamente justificada.

O alinhamento da contratação com os planos do TJDFT está devidamente demonstrado nas etapas anteriores deste documento.

As quantidades de itens a contratar estão coerentes com as demandas previstas, considerando que a estimativa de consumo foi informada pela área técnica responsável e devidamente demonstrada em seção anterior deste documento.

A análise de mercado foi adequadamente realizada e demonstrou haver ampla capacidade do mercado em atender à necessidade do negócio. Tal questão é sustentada pelo fato de que o fornecimento de solução de gestão de acessos privilegiados é um serviço comum ao TJDFT e a vários órgãos da Administração Pública.

A escolha do tipo de solução a contratar está devidamente justificada no corpo deste Estudo Técnico Preliminar e a contratação se dará por licitação na modalidade pregão, em observância ao inciso I do Art. 28 e Art. 29 da Lei 14.133/2021.

A solução de TI a contratar está devidamente descrita, incluindo todos os elementos necessários para alcançar os resultados pretendidos e atender à necessidade da contratação.

Não há justificativa para o parcelamento da solução por se tratar de solução integrada com respectivo suporte técnico.

Os resultados pretendidos com a contratação foram devidamente expostos, em termos de economicidade, eficácia, eficiência, de melhor aproveitamento dos recursos humanos, materiais e financeiros disponíveis, inclusive com respeito a impactos ambientais positivos, bem como a melhoria da qualidade da prestação dos serviços de suporte a usuários, de forma a atender a necessidade da contratação.

Os impactos esperados com a implantação e operação da solução foram identificados e as providências para adequar o ambiente do órgão foram planejadas e são viáveis, inclusive aquelas relativas ao impacto ambiental da solução e à disponibilidade de pessoal qualificado para gerir o contrato na área de TI e na área requisitante.

Os riscos relevantes foram adequadamente levantados e realizadas propostas para sua mitigação.

A relação custo-benefício da contratação é considerada favorável e vantajosa para o TJDFT.

Há evidências de que a área requisitante se comprometeu com o planejamento preliminar da solução (elaboração dos estudos técnicos preliminares) e há expectativa de que apoiará a construção do Termo de Referência ou do projeto básico e apoiará o esforço de gestão do contrato.

Foram realizadas estimativas preliminares dos preços do objeto a ser contratado, com a pesquisa de mercado para precificação, a fim de que a administração superior do TJDFT possa disponibilizar o orçamento adequado para a contratação do objeto escopo deste projeto no exercício corrente, bem como poder se programar adequadamente para que sejam providos os recursos necessários ao longo dos diversos exercícios caso a contratação seja estendida.

2. Decisão

Por todo o exposto, declara-se a viabilidade da contratação, sugerindo o seu prosseguimento.

XI - Equipe de Planejamento da Contratação

Função	Nome	Matrícula	Email	Telefone
Integrante requisitante	Raymundo Avelino Aben-athar	317.161	raymundo.vieira@tjdft.jus.br	(61)3103-4200
Subst. integrante requisitante	Eduardo da Silva Sousa	318.205	eduardo.ssousa@tjdft.jus.br	(61)3103-7676
Integrante técnico 1	Marcelo Soares Mota	321.048	marcelo.mota@tjdft.jus.br	(61)3103-7676
Integrante técnico 2	Cristiano Rodrigues Pereira Junior	319.657	cristiano.junior@tjdft.jus.br	(61)3103-7676
Subst. integrante técnico	Sávio Levy Rocha	319.212	savio@tjdft.jus.br	(61)3103-7600
Integrante administrativo 1	Álvaro Cesário César Cordeiro Couto	319.817	alvaro.couto@tjdft.jus.br	(61)3103-4990
Subst. Integr. Administrativo 1	Elaine Brandão de Souza	317.386	elaine.souza@tjdft.jus.br	(61)3103-4990
Integrante administrativo 2	Michelle Rocha Ferreira	320.154	michelle.ferreira@tjdft.jus.br	(61)3103-4625
Subst. Integr. Administrativo 2	Ednaldo José de Araújo Junior	318.475	ednaldo.junior@tjdft.jus.br	(61)3103-4625

XII - Unidade Superior Responsável

Nome da unidade	SETI - SECRETARIA DE TECNOLOGIA DA INFORMAÇÃO
Nome do responsável	Luiz Fernando Sirotheau Serique Junior - Secretário de TI

=====

Sequência lógica dos tópicos do ETP:

	Tópico
I	Necessidade da Contratação
II	Descrição Resumida do Objeto
III	Análise de Mercado
IV	Demanda x Qtde de Itens
V	Estimativas do Valor da Contratação
VI	Descrição Completa da Solução
VII	Alinhamento Estratégico
VIII	Justificativa da Solução Escolhida
IX	Planejamento e Sustentação da Contratação
X	Declaração de Viabilidade da Contratação
XI	Equipe de Planejamento da Contratação
XII	Unidade Superior Responsável



Documento assinado eletronicamente por **Marcelo Soares Mota, Analista Judiciário**, em 05/11/2025, às 17:41, conforme art. 1º, III, "b", da Lei 11.419/2006.



Documento assinado eletronicamente por **Eduardo Da Silva Sousa, Coordenador(a)**, em 06/11/2025, às 13:14, conforme art. 1º, III, "b", da Lei 11.419/2006.



Documento assinado eletronicamente por **Cristiano Rodrigues Pereira Junior**, **Analista Judiciário**, em 06/11/2025, às 14:31, conforme art. 1º, III, "b", da Lei 11.419/2006.



Documento assinado eletronicamente por **Luiz Fernando Sirotheau Serique Junior**, **Secretário(a)**, em 06/11/2025, às 14:51, conforme art. 1º, III, "b", da Lei 11.419/2006.



Documento assinado eletronicamente por **Raymundo Avelino Aben-athar**, **Subsecretário(a)**, em 06/11/2025, às 16:47, conforme art. 1º, III, "b", da Lei 11.419/2006.



Documento assinado eletronicamente por **Ana Paula Rezende Costa**, **Supervisor(a)**, em 12/11/2025, às 17:28, conforme art. 1º, III, "b", da Lei 11.419/2006.



A autenticidade do documento pode ser conferida no site https://sei.tjdft.jus.br/sei/controlador_externo.php?acao=documento_conferir&acao_origem=documento_conferir&lang=pt_BR&id_orgao_acesso_externo=0 informando o código verificador **4643493** e o código CRC **6C1403BC**.