FUNDAÇÃO NACIONAL DE SAÚDE

ESTUDO TÉCNICO PRELIMINAR DA CONTRATAÇÃO

Processo nº 25100.000334/2020-38

1. INTRODUÇÃO

1.1. O Estudo Técnico Preliminar tem por objetivo identificar e analisar os cenários para o atendimento da demanda que consta no Documento de Oficialização da Demanda, bem como demonstrar a viabilidade técnica e econômica das soluções identificadas, fornecendo as informações necessárias para subsidiar o respectivo processo de contratação.

Referência: Art. 11 da IN SGD/ME nº 1/2019.

2. TERMOS E DEFINIÇÕES UTILIZADAS

2.1. Resumo

2.2. As contas privilegiadas fornecem acesso elevado, muitas vezes irrestrito, aos sistemas e tecnologias de informação subjacentes de uma organização, tornando-as alvos valiosos para agentes mal-intencionados internos e externos. Frequentemente essas contas são usadas em ataques bem-sucedidos para obter acesso a recursos corporativos e sistemas críticos (por exemplo, SEI e SIGA), resultando em violações de dados.

2.3. Organizações complexas, incluindo Governo e e instituições privadas, enfrentam desafios ao gerenciar contas privilegiadas, o que representa um risco significativo para seus negócios. Se usadas incorretamente, essas contas podem causar danos operacionais significativos, incluindo roubo de dados, espionagem, sabotagem, resgate ou contornar controles importantes.

2.4. Para enfrentar esses desafios, instituições como National Cybersecurity Centre of Excellence (NCCoE), Gartner e Kuppinger recomendam a utilização de uma solução de segurança para proteger e aplicar políticas organizacionais de maneira adequada para o uso de contas com privilégios. O exemplo de implementação destaca como as organizações podem adicionar uma camada de segurança entre os usuários e as contas privilegiadas que eles acessam.

Gartner Magic Quadrant 2020 - Pág. 2

O Gartner cobre três categorias distintas de ferramentas que evoluíram com o foco predominante para líderes de gerenciamento de segurança e risco (SRM) e outros líderes da TI considerando o investimento em ferramentas PAM:

■ **Gerenciamento de sessões e contas privilegiadas (PASM).** Contas privilegiadas são protegidas pela guarda de suas credenciais em cofre. O acesso a essas contas é então intermediado para usuários humanos, serviços e aplicativos. As funções de gerenciamento de sessão privilegiada (PSM) estabelecem sessões com possível injeção de credencial e gravação de sessão completa. Senhas e outras credenciais para contas privilegiadas são gerenciadas ativamente, como sendo alteradas em intervalos definíveis ou após ocorrência de eventos específicos. As soluções PASM podem, opcionalmente, também fornecer gerenciamento de senhas de aplicações para aplicações (AAPM) e / ou acesso remoto privilegiado sem necessidade de instalação para equipe de TI e terceiros que não requer VPN.

■ **Gerenciamento de elevação e delegação de privilégios (PEDM)**. Privilégios específicos são concedidos no sistema gerenciado por agentes baseados em host para usuários conectados. As ferramentas PEDM fornecem controle de comando (filtragem), controles de permitir / negar / isolar aplicativos e / ou elevação de privilégios, o último na forma de permitir que comandos específicos sejam executados com um nível mais alto de privilégios.

As ferramentas PEDM devem ser executadas no sistema operacional real (kernel ou nível de processo). Controle de comandos por meio de filtragem de protocolo é explicitamente excluído desta definição, porque o ponto de controle é menos confiável. As ferramentas PEDM também podem fornecer recursos de monitoramento de integridade de arquivos.

■ **Gerenciamento de segredos: credenciais (como senhas, tokens OAuth, chaves SSH, etc.)** e segredos para software e máquinas são gerenciados de forma programática, armazenados e recuperados por meio de APIs e SDKs. A confiança é estabelecida e negociada com o objetivo de trocar segredos e para gerenciar autorizações e funções relacionadas entre diferentes entidades não humanas, como máquinas, contêineres, aplicativos, serviços, scripts, processos e pipelines DevSecOps.

O gerenciamento de segredos é frequentemente usado em ambientes dinâmicos e ágeis, como IaaS, PaaS e plataformas de gerenciamento de contêineres.

2.5. ***Gerenciamento de identidade:*** é um termo que se refere de forma abrangente à administração de identidades individuais no contexto de um sistema, como uma companhia, uma rede de dados ou até mesmo um país. Em tecnologia da informação, gerenciamento de identidade é um conceito utilizado para estabelecer e manter papéis e privilégios de acesso de usuários de uma determinada rede. O Gerenciamento de identidade provê, aos administradores de TI e aos gestores, ferramentas e tecnologias para controlar o acesso a informações críticas da organização.

2.5.1. O principal objetivo de um sistema de gerenciamento de identidade em um ambiente corporativo é definir uma identidade única para cada indivíduo da organização. Uma vez estabelecida a identidade única, ela deverá ser mantida, modificada e monitorada durante todo o ciclo de vida do acesso. Gerenciamento de identidade em TI permite que essa identidade única seja administrada de forma eficaz, garantindo que as políticas e regulamentações da entidade sejam aplicadas.

2.6. ***Gerenciamento de acessos:*** *T*em como objetivo garantir o direito de usuários autorizados acessarem um determinado serviço, enquanto proíbe o acesso a usuários não autorizados. Esses acessos estão definidos nas políticas de segurança da organização.

2.7. ***Solução de PAM*** (Privileged Access Management): é uma solução que restringe e controla o acesso privilegiado em um ambiente de redes, sistemas e banco de dados.

3. JUSTIFICATIVA DA CONTRATAÇÃO

3.1. *Problema*

3.1.1. As organizações, incluindo a Funasa, contam com contas privilegiadas para permitir que usuários autorizados desempenhem suas funções com pouca ou nenhuma supervisão direta ou controle técnico de suas ações.

3.1.2. A CGMTI tem dificuldade em gerenciar essas contas, o que, por sua vez, abre um risco significativo para o negócio. Se usados de forma inadequada, estas contas podem causar danos operacionais substanciais, incluindo roubo de dados, espionagem, sabotagem ou resgate.

3.1.3. Atores externos mal-intencionados podem obter acesso não autorizado a contas privilegiadas por meio de uma variedade de técnicas, como o aproveitamento de credenciais roubadas ou esquemas de engenharia social. Além disso, existem casos raros de funcionários descontentes que abusam de suas contas, bem como funcionários honestos que cometem erros.

3.1.4. O uso indevido e os erros podem afetar os aplicativos de alto valor (por exemplo, sistemas de banco de dados com dados sensíveis, SEI e SIGA entre outros).

3.1.5. Gerenciar contas privilegiadas é uma tarefa importante, mas complicada. O Data Center da Funasa opera uma infraestrutura altamente complexa e possui sistemas distintos que são executados em vários sistemas operacionais. Gerenciar e controlar o acesso a essas contas privilegiadas é ainda mais complicado pelo ritmo significativo de mudanças na força de trabalho e nas responsabilidades ao longo do tempo.

3.1.6. Por último, as alterações feitas no nível do sistema podem ser usadas para ter controles de desvio, para ocultar a atividade ou fazer com que as instituições violem seus rigorosos requisitos de conformidade.

3.1.7. Como caso de uso, temos o caso do Superior Tribunal de Justiça (STJ) que foi vítima de um ataque de ransomware em novembro de 2020, onde a instituição confirmou ter sido alvo de um ataque hacker que criptografou dados e forçou o tribunal a suspender sessões e tirar seus sistemas e site do ar durante dias.

Fonte: //www.uol.com.br/tilt/noticias/redacao/2020/11/05/site-do-stj-sai-do-ar-apos-ataque-hacker-saude-tambem-investiga-invasao.htm?

https://www.conjur.com.br/2020-nov-04/stj-sofre-ataque-hacker-suspende-prazos-segunda-911

3.1.8. Ademais, com a nova Lei Geral de Proteção de Dados brasileira, todas as empresas e órgãos públicos deverão investir em segurança e implementar processos e tecnologias efetivos para prevenir, detectar e remediar violações de dados pessoais.

3.2. Justificativa da Contratação

3.2.1. O contrato nº 35/2018 celebrado entre a Funasa e a empresa 3BM IT Solutions Serviços e Tecnologia LTDA-ME (razão social alterada através do Termo Aditivo n ° 6/2019 (SEI 1095735) para Visionset Segurança em Tecnologia LTDA) tem como objeto a prestação de serviços de atividades de execução continuada, na modalidade SaaS (Software as a Service), com valor global de R$ 4.664.484,00, assinado no dia 23 de abril de 2018 e renovado em 2019, com o objetivo de melhorar a gestão de identidade da Funasa, manter as contas privilegiadas em um único repositório seguro, implementar regras de autorização para uso de contas privilegiadas, gerar senhas automatizada com tempo definido de validade, registrar as ações realizadas em posse de contas privilegiadas (gravação de sessão), monitorar as ações de funcionários e terceiros que possuam contas privilegiadas, melhorar a

qualidade na prestação de informações na investigação de incidentes de segurança e na prestação às informações aos órgãos de controle, além de obter resultados relacionados à eficiência, efetividade, economicidade e isonomia.

3.2.2. Seguindo determinação do item 9.7.1 do Acórdão 2.2017/2018 TCU - Plenário, determina que a Funasa realize a revisão de todos os contratos de TIC, esta Coordenação Geral inicia novo processo de planejamento da contratação, que através deste Estudo Técnico Preliminar, avaliará o grau de obtenção de sucesso no alcance dos objetivos acima mencionados através do Contrato nº 35/2018.

3.2.3. Como mencionado, atualmente já existe na instituição uma solução de Gerenciamento de Acesso Privilegiado (PAM - Privileged Access Management), que inclui a funcionalidade de Cofre de Senhas, solução que permite, quando corretamente implantada, controle de acesso aos sistemas e seus dados, mantendo alinhamento às normas de Segurança da Informação, inclusive à Lei Geral de Proteção de Dados - LGPD, já que permite a rastreabilidade dos acessos privilegiados, controlando qualquer tipo de acesso aos dados sensíveis. Assim sendo, a manutenção de uma solução de gerenciamento de identidades e cofre de senhas pode proporcionar ao órgão a capacidade de controle dos acessos realizados em seus sistemas, com auditoria e customização necessária para garantir o privilégio mínimo necessário às atividades de cada servidor e colaborador, conforme o controle descritos na Norma Complementar nº 07 da IN01/GSIPR (1878040), a exemplo do item 6.3.2 - *Respeitar o princípio do menor privilégio para configurar as credenciais ou contas de acesso dos usuários aos ativos de informação*.

3.2.4. As soluções a serem estudadas devem então atender às necessidades da Funasa para estabelecimento e aprimoramento de controles de segurança relacionadas à gestão de riscos e de segurança da informação, inclusive no que tange ao atendimento à Lei Geral de Proteção de Dados - LGPD, de acordo com as deliberações do Comitê de Governança, Riscos e Controles e Subcomitê de Governança, Riscos e Controles da Funasa, refletidos no Plano Diretor de Tecnologia da Informação e Comunicações 2021 - PDTIC, aprovado em conformidade com o Planejamento Estratégico da Funasa pelo seu Comitê Gestor de Tecnologia da Informação.

3.2.5. A intenção desse planejamento da contratação é realizar Estudo Técnico Preliminar de forma a avaliar a solução atualmente adotada na Funasa, comparando com outras ferramentas, outros modelos de implementação e diferentes formas de fornecimento do serviço, e caso seja encontrada no mercado soluções mais vantajosas, o ETP deverá direcionar a um novo processo licitatório em substituição à renovação contratual, atendendo às recomendações do Tribunal de Contas da União - TCU.

3.2.6. Esta contratação também possui o objetivo de atender aos novos decretos e leis de segurança da informação:

3.3. **Atender as exigências sobre a proteção dos acessos privilegiados apoiando demandas da LGPD**

3.3.1. **Artigos 6º e 46º - Determinar como os dados deverão ser tratados, mantidos e protegidos e a quem responsabilizar caso o descumprimento.**

3.3.1.1. Proteção de acesso a dados pessoais sensíveis - Gestão dos Privilégios em Servidores e Estações, Proteção de Credenciais na Infraestrutura e nas Aplicações, Repositório Seguro de Credenciais e Monitoramento das Sessões Privilegiadas.

3.3.2. **Artigos 42º, 43º e 48º - Responsabilização pessoal e resposta a incidentes**

3.3.2.1. Detecção e Resposta Rápida a Incidentes logo no início do ciclo de ataque - Identificação das Ações nas Sessões Privilegiadas e Respostas Automáticas a Comportamentos de Alto Risco nos Acessos Privilegiados.

3.3.3. **Artigo 50º - Boas práticas de governança, através de regras que deverão respeitar os preceitos da lei, de maneira a mitigar os riscos inerentes ao tratamento de dados e Implementar e demonstrar a efetividade da políticas de segurança relacionados ao tratamento de dados.**

3.3.3.1. Avaliar o Risco e testar a efetividade dos processos de proteção de dados - Relatórios com Status de Risco do Ambiente Privilegiado e Classificação do Risco das Ações Monitoradas nas sessões privilegiadas.

3.3.3.2. Demonstrar Conformidade e provar que os controles de segurança necessários estão no lugar certo - Trilha de Auditoria das Ações Privilegiadas, Relatórios de Conformidade das Credenciais Críticas e Análise e Histórico dos Acessos Privilegiados.

3.4. **Atender as exigências da estratégia nacional de segurança cibernética - e-ciber - Decreto nº 10.222, de 5 de fevereiro de 2020.**

3.4.1. Item 2.3.1. Fortalecer as ações de governança cibernética: criar controles para o tratamento de informações com restrição de acesso.

4. CRONOGRAMA DO ESTUDO TÉCNICO PRELIMINAR

4.1. Considerando a existência de uma ferramenta de Gerenciamento de Acessos Privilegiados (PAM - Privileged Access Management), é importante que o Estudo Técnico seja detalhado, a fim de avaliar tanto a viabilidade da utilização da ferramenta atualmente instalada, quanto para avaliar outras ferramentas disponíveis no mercado que possam atender

às necessidades da Funasa. Por esse motivo, a equipe da CGMTI seguirá um plano de ação para a realização do Estudo Técnico.

	descrição	Objetivo	atividades
Fase 1	Análise da Situação atual	Avaliação de viabilidade técnica e jurídica para renovação do contrato vigente (contrato nº 35/2018).	Compreensão do cenário atual Detalhamento do modelo atualmente adotado para licenciamento da solução. Detalhamento dos desembolsos ocorridos durante 24 meses de vigência do contrato
	Cotação preliminar	Avaliação a respeito da vantajosidade da manutenção da solução.	Definição de uma especificação prévia, sujeita a ajustes após manifestação do mercado. Envio de pedido de cotação da ferramenta, especialmente de PAM, para análise de vantajosidade da solução atual. Envio de solicitação de propostas de ajustes no escopo das funcionalidades pre definidas, com o objetivo de ampliação da competição.
	Decisão sobre a manutenção da Solução	Avaliação de todos os aspectos e decisão a respeito da manutenção da solução	Análise dos aspectos jurídicos, técnicos e de custos para decisão de manutenção da solução. Produção de Nota Técnica no processo 25100.014566/2017-78 justificando a viabilidade para renovação ou motivando nova contratação.
	Final da Fase 1 - Análise de Viabilidade da solução atualmente adotada		
Fase 2 Em caso de condução de novo processo licitatório	Prova de Conceito das ferramentas	Prova de conceito (POC) com ferramenta Beyond Trust Prova de Conceito com ferramenta Senha Segura Prova de conceito com outra solução que venha a se mostrar competitiva para o certame	Envio de convite para realização de POC Termo de Início de POC Teste "on the job" de cada solução
	Avaliação das ferramentas testadas	Relatórios a respeito das ferramentas testadas	Emissão de relatório atestando pontos fortes e fracos para cada solução Relatório sobre os requisitos importantes não atendidos ou requisitos dispensáveis não atendidos.
	Recebimento das	Solicitação de ajustes de especificação pelos	Realização de reuniões com as empresas para

	contribuições de fabricantes para ajuste da especificação	diversos fabricantes e integradores de solução	conclusão da especificação do produto.
	Ajuste na especificação das ferramentas	Refinamento da especificação das ferramentas considerando a contribuição de diversos integradores e fabricantes de soluções com o objetivo de ampliar a competição	Conclusão dos requisitos da solução a ser licitada
	Cotação final	Com o escopo fechado após consulta aos fabricantes e integradores de solução, realização de nova consulta de preços, além de consulta de mercado.	Envio para nova cotação, além de cotação pelo painel de preços
	Encaminhamento do processo licitatório para a CPL e análise da PFE	Realização de reunião com a PFE para apresentação do ETP e TR	Realização de reunião com a PFE para apresentação do ETP e TR, coletando informações que possam subsidiar e acelerar o processo de ajustes presentes no parecer da Procuradoria
Final do Planejamento da Contratação			

5. DEFINIÇÃO E ESPECIFICAÇÃO DAS NECESSIDADES E REQUISITOS

5.1. Identificação das necessidades de negócio

5.1.1. Realizar a gestão de contas privilegiadas em sistemas, dispositivos e aplicativos sob responsabilidade desta coordenação;

5.1.2. Automatizar de forma aleatória, o gerenciamento e armazenamento de senhas e outras credenciais para contas administrativas, de serviço e de aplicativo;

5.1.3. Controlar o acesso a contas privilegiadas, incluindo as compartilhadas e as “chamadas de emergência” (acesso de emergência);

5.1.4. Isolar, monitorar, registrar, indexar, armazenar e auditar sessões, comandos e ações de acesso privilegiado;

5.1.5. Fornecer conexão única (SSO) para sessões, comandos e ações privilegiados de forma segura para não revelar credenciais de conta (senhas, chaves criptográficas, etc.);

5.1.6. Delegar, controlar e filtrar operações privilegiadas que um administrador pode executar;

5.1.7. Garantir níveis exigidos de confiança e responsabilidade pelo acesso privilegiado, fornecendo autenticação ou integração com produtos ou serviços de autenticação externos;

5.1.8. Prover conformidade com a LGPD (Lei Geral de Proteção de Dados).

5.1.8.1. A Lei Geral de Proteção de Dados (LGPD) foi promulgada em agosto de 2018 e, com isso, há mudanças fundamentais em como os dados dos cidadãos brasileiros podem ser tratados. Assim como o Regulamento Geral de Privacidade de Dados da União Européia (GDPR), os infratores enfrentarão penalidades monetárias, no caso da LGPD, até 2% do volume de negócios, ou um máximo total de cinquenta milhões de reais (R$ 50.000.000) por infração, se a lei for violada.

5.2. Identificação das necessidades tecnológicas

5.2.1. As soluções devem atender a necessidade da Funasa para o aprimoramento de controles de segurança apontados pelas iniciativas da autarquia relacionadas à gestão de riscos e de segurança da informação, de acordo com as deliberações do Comitê de Governança, Riscos e Controles e Subcomitê de Governança, Riscos e Controles da Funasa,

refletidos no Plano Diretor de Tecnologia da Informação e Comunicações 2021 - PDTIC, aprovado em conformidade com o Planejamento Estratégico da Funasa pelo seu Comitê Gestor de Tecnologia da Informação.

5.2.2. Considerando que, segundo o Relatório "The Forrester Wave^{TM}: Privileged Identity Management" de 2016, 80% das das violações são resultado de abuso ou uso indevido das contas privilegiadas, podemos verificar que contas e privilégios não gerenciados representam uma vulnerabilidade e podem ser alvos de ataques. Por isso, uma solução adequada para gestão desses acessos deve fazer parte da solução de Segurança da Informação no parque tecnológico da Funasa.

5.2.3. Ainda, segundo o relatório "Gartner, Magic Quadrant for Privileged Access Management" de Dezembro de 2018, as ferramentas de Gerenciamento de Acessos Privilegiados, ou PAM (Privileged Access Management), ajudam as organizações a fornecerem acesso privilegiado seguro a ativos críticos e a atenderem aos requisitos de conformidade, gerenciando e monitorando contas e acessos privilegiados.

5.2.4. A aquisição das soluções subsidiará os setores que lidam direta e indiretamente com segurança da informação, por isso, a equipe técnica da Funasa compreende não só a importância de uma solução que permita o gerenciamento, monitoramento e auditoria das contas e sessões privilegiadas, com controle de privilégios excessivos em dispositivos, em acessos locais, mas também que ofereça proteção, gerenciamento e auditoria das sessões de acesso privilegiado realizados remotamente, considerando a grande quantidade de prestadores de serviços atuando no ambiente Funasa, como por exemplo, servidores em teletrabalho além dos colaboradores da Fábrica de Software, de Suporte à Infraestrutura de TIC e da Central de Serviço ao Usuário.

5.2.5. A pandemia vivida atualmente, exigiu o amplo acesso remoto dos servidores aos ambientes de trabalho, trazendo à tona a necessidade da realização de estudos a respeito da implementação de acessos remotos seguros, já que muitos chamados de suporte ao usuário são atendidos através de acesso remoto à estação de trabalho do colaborador, por um técnico, para atendimento.

5.2.6. As soluções que possam oferecer os serviços necessários à organização **não têm vinculação tecnológica**, o que dispensa a contratação de todas como uma solução conjunta. Em contrapartida, visto que o objetivo é avaliar a viabilidade das ferramentas existentes, e se for o caso, licitar nova solução em substituição à atual, é interessante para a Funasa que sejam adquiridas no mesmo processo licitatório e que a empresa vencedora forneça não só a solução completa (hardware e software), mas também o suporte técnico necessário para a utilização da solução completa.

5.2.7. A solução de Gerenciamento de Acesso Privilegiado (PAM – Privileged Access Management), deve conter, pelo menos, funcionalidades de Gerenciamento de Contas e Sessões Privilegiadas (*Privileged Account and Session Management -PASM*) e Gerenciamento de Elevação e delegação de Privilégios (*Privilege Elevation and Delegation Management - PEDM*), além de funcionalidades para Acesso Remoto Privilegiado Seguro e Suporte Remoto Privilegiado, essas últimas, motivadas pela gestão de riscos em casos de ocorrência de novo ciclo de Pandemia, como o da COVID-19, que obrigou grande parte dos servidores a exercerem suas atividades de forma remota.

5.3. **Demais requisitos necessários e suficientes à escolha da solução de TIC.**

5.3.1. Interface padrão Web multiplataforma, sem agentes.

5.3.2. Solução com banco de dados próprio sem a necessidade de licenças adicionais de outros fabricantes.

5.3.3. Realizar a gravação, indexação e armazenamento da sessão em vídeo e logs de textos em repositório seguro, criptografado e protegido contra qualquer alteração que comprometa a integridade dessas evidências.

5.3.4. Opção de conexão direta via cliente (Jump Server, RDP, SQL Manager e etc.), sem exibir a senha para o usuário (Proxy RDP e SSH).

5.3.5. Prover autenticação transparente no sistema-alvo ou dispositivo de rede sem exibir a senha aos administradores da rede ou terceiros.

5.3.6. Auditoria com trilha inalterável para qualquer operação.

5.3.7. Utilizar algoritmo AES-256 para criptografia do tráfego de informações.

5.3.8. Guarda compartilhada de senha mestra (Master-key parted).

5.3.9. Alta disponibilidade (HA).

5.3.10. Ambiente virtualizado x86.A

5.3.11. Autenticação em dois fatores.

5.3.12. Integração com Active Directory.

5.3.13. Compatível com navegadores Mozilla Firefox, Chrome, Safari, Internet Explorer e Edge.

5.3.14. Suporte a sistemas operacionais Microsoft, Linux (Debian / Ubuntu Server / CentOS / Red Hat) ou do tipo Unix.

5.3.15. Bloqueio de comandos em sessões SSH, Telnet e bancos de dados.

6. ANÁLISE DA SOLUÇÃO ATUAL

6.1. Atualmente, para atendimento aos requisitos do contrato nº 35/2018 são fornecidas, como serviço (Software as a Service - SaaS), licenças das ferramentas CyberArk (Acesso Privilegiado Seguro) e Dynatrace (Gerenciamento de Desempenho de Aplicação - APM). Por ser um contrato de fornecimento como serviço, as licenças não estão registradas em nome da Funasa, **e por isso, caso não seja renovado o contrato, todos os produtos decorrentes do monitoramento, seja por qualquer das ferramentas supramencionadas, não poderão ser recuperadas futuramente. Assim, esse modelo de contratação não atende às necessidades da Administração Pública Federal, por representar dependência tecnológica que obriga sucessivas renovações do contrato para manutenção dos resultados pelos quais já houve remuneração. Isso quer dizer que, ao término do período de vigência do contrato, os serviços serão interrompidos, e não mais haverá histórico dos resultados dos serviços prestados que já tenham sido remunerados.**

6.1.1. Ainda, é importante mencionar que devido à falta de maturidade e problemas internos de gestão de Tecnologia da Informação, **a ferramenta Dynatrace foi pouco utilizada**, pelo menos durante o último ano de vigência do contrato, o que direciona para a não renovação do contrato para o fornecimento da solução. Por outro lado, a ferramenta CyberArk, considerada líder de mercado segundo o relatório "Gartner, Magic Quadrant for Privileged Access Management" de Dezembro de 2018, tem sido muito utilizada como solução para Gerenciamento de Acessos Privilegiados (PAM).

6.1.2. Houve uma proposta enviada por e-mail pela empresa Visionset no dia 03/04/2020 para tentativa de renovação, com o seguinte formato:

1 - Transformar a licença em perpetua para que não seja mais uma dependência.

2a - Substituição da Ferramenta de APM Dynatrace por outra de funcionalidades semelhantes chamada AppDynamics, com redução de 38% do valor do contrato, totalizando 2.316.000,00, podendo ser pago em 12 parcelas fixas; ou

2b - Renovação apenas da solução CyberArk, **transformando a mesma e licenciamento perpetuo** pelo valor de 768.000 dividido em 12 parcelas iguais de R$ 64.000,00; ou

2c - Renovação só da solução CyberArk, transformando a mesma e licenciamento perpetuo – R$ 696.000,00 pagamento único.

6.1.3. Ocorre que a qualquer uma das alternativas propostas pelo fornecedor deve ser interpretado como alteração de escopo contratual, e por isso entendemos que a alteração do escopo contratual no momento da renovação não é viável juridicamente, considerando as regras do edital que culminou na contratação da solução composta pelas duas ferramentas supramencionadas não traz critérios objetivos para avaliar quais requisitos devem ser cumpridos por cada uma das ferramentas, e assim, impossível mensurar qual o valor adequado para pagamento considerando a redução de um conjunto de serviços. Assim, ao aceitar tal proposta estaríamos incorrendo em atentado ao princípio básico da vinculação ao instrumento convocatório.

6.1.4. Outro ponto a ser analisado é a aparente vantajosidade da renovação de apenas uma das soluções, já que ainda que o valor se mostre mais vantajoso para a Administração Pública quando comparado o valor vigente com o valor proposto para renovação, não é possível afirmar que, com um escopo reduzido de funcionalidades (necessidades), outras soluções de mercado não possam atender às novas especificações com condições ainda mais vantajosas para a Administração, e por isso, caso seja decidido pela renovação, existe o risco de que se atente ao princípio da isonomia e em restrição à competição, e consequentemente, fuga da busca da solução mais vantajosa e da economicidade.

6.1.5. Durante os últimos 24 meses, foram gastos um total de R$ 8.706.030,65 (oito milhões, setecentos e seis mil trinta reais e sessenta e cinco centavos) , tendo sido gastos na solução o valor de R$ 4.445.768,96 no primeiro ano de vigência e R$ 4.260.261,69 no segundo ano de vigência, restando até o momento a apuração do último mês. Importante mencionar que o valor reduzido em comparação com o ano anterior é resultado da redução gradativa de abertura de novas Ordens de Serviços nos últimos meses de vigência contratual.

6.1.6. O quadro abaixo demonstra o desembolso por mês dos últimos 24 meses:

Especificação do serviço	Mês de ocorrência	Valor de pagamento	Somatório

Licença de Software	maio	3.768.990,00	3.768.990,00
Suporte	maio	86.260,86	676.778,96
Suporte	junho	93.320,32	
Suporte	julho	94.867,60	
Suporte	agosto	89.097,54	
Suporte	setembro	36.933,57	
Suporte	outubro	29.335,13	
Suporte	novembro	23.069,94	
Suporte	dezembro	20.630,40	
Suporte	janeiro	55.705,95	
Suporte	fevereiro	77.844,95	
Suporte	março	36.224,40	
Suporte	abril	33.488,30	
Licença de Software	maio	3.768.990,00	3.768.990,00
Suporte	maio	54.910,39	516.221,58
Suporte	junho	50.137,03	
Suporte	julho	76.556,83	
Suporte	agosto	97.301,99	
Suporte	setembro	45.176,71	
Suporte	outubro	35.150,33	
Suporte	novembro	51.810,67	
Suporte	dezembro	34.285,14	
Suporte	janeiro	18.264,35	

Suporte	fevereiro	13.950,01	
Suporte	março	13.728,24	
Suporte	abril	24.949,89	
Desembolso Total em 24 meses			**8.730.980,54**

6.1.7. Pelos motivos expostos acima, a equipe de Planejamento da Contratação, através do resultado do estudo de viabilidade, **optou pela não renovação do contrato contrato nº 35/2018**, e por isso, é dada continuidade a este Estudo Técnico Preliminar para a aquisição de solução mais vantajosa para a Administração.

7. ESTIMATIVA DA DEMANDA – QUANTIDADE DE BENS E SERVIÇOS

7.1. As licenças fornecidas para toda a solução e todos seus eventuais módulos deverão ser perpétuas, possibilitando o uso mesmo após eventual vencimento da garantia e/ou suporte. Para fins de dimensionamento do serviço técnico, considerar-se-á inicialmente os seguintes dispositivos:

Descrição	QTD
Usuários para acesso privilegiado (admin segurança/rede/Root/DomainAdmin/DBadmin/SysDBA, VMadmin, outros).	50
Estações de Trabalho de outros tipos (Tablets, Smartphones, etc.)	231
Domínios LDAP	1
Servidores físicos	79
Servidores virtuais	234 (79 Linux e 155 Windows)
Storages corporativos	25
Unidades de leitura/gravação de fitas de backup	2
Switches Core, Tor ou SAN	16
Switches de distribuição	201
Controladora WiFi	2
Appliances de segurança da informação	11
Instâncias de banco de dados	23
Instâncias servidor WEB (IIS, Apache, outros)	50

Instâncias servidor de aplicação (J2EE, .NET, Zope, etc.)	40
Instâncias servidor de correio eletrônico (MS Exchange, Postfix, Sendmail, Expresso, etc.)	4
Servidores Hipercorvergentes	8
Instâncias de servidor de gerenciamento e monitoramento de TI	1
Instâncias de servidor de gerenciamento de processos	3
Sistemas aplicativos	50
Sites WEB (Internet, intranet e extranets)	3

Tabela - Descrição e quantidade de serviços do parque computacional (3103646).

Grupo	Item	Descrição	Unidade de medida	Quantidade	Justificativa / Memória de cálculo
1	1	Solução de gerenciamento de gestão de acessos privilegiados, armazenamento de credenciais, que possibilite o isolamento, gravação e o monitoramento de sessões de ativos de TIC com serviço de garantia pelo período de 36 (trinta e seis) meses	Solução	1	Esse quantitativo foi estipulado considerando o número de usuários de recursos de TIC e uma expectativa de crescimento dado o Recrutamento do Cade e novos contratos administrativos
	2	Serviço de instalação e configuração para a solução de gestão de acessos privilegiados, armazenamento de credenciais	Serviço	1	Esse quantitativo foi estipulado considerando a instalação e a configuração da Solução de gerenciamento de identidade no ambiente da Funasa.
		Suporte Técnico Mensal	Serviço	36	Suporte técnico mensal para a instituição. Auxiliando na customização e na resolução de demandas diárias do órgão.
	3	Treinamento oficial com o fabricante da ferramenta de gerenciamento de identidade	Pessoa	5	Esse quantitativo foi estipulado considerando o número de servidores da CGMTI envolvidos da gestão da solução e fiscalização técnica do

					contrato. Atualmente a CGMTI possui 11 servidores.

7.2. A solução deve prover auditoria e gestão de acessos privilegiados por meio de credenciais privilegiadas para pelo menos 1.086 (mil e oitenta e seis) dispositivos que estão operando no parque tecnológico da Funasa.

7.3. Para o cálculo da quantidade de pessoas que realizarão treinamento de operação, utilizou-se como referência o número de analistas na COINF e COINT, sendo 05 (cinco) o número de pessoas que irão realizar o treinamento.

7.4. Em razão de existir diversos mecanismos de precificação no mercado e devido à complexidade de delimitar a quantidade de licenças, adotar-se-á a opção de compra por Unidade de Medida "Solução" e quantidade "01". Assim o quantitativo de dispositivos e usuários que a solução deve atender serão os que estão descritos na Tabela - Descrição e quantidade de serviços do parque computacional., acima. Dessa forma, entende-se que o modelo adotado representa uma forma justa de participação no processo licitatório.

8. ANÁLISE DE SOLUÇÕES

8.1. Como é possível depreender da análise apresentada na introdução deste estudo, o ambiente tecnológico da Funasa é extremamente complexo e sensível. A pluralidade e rotação de servidores e técnicos pode ser um perigo concreto para a continuidade da gestão. Assim sendo, foram levantados alguns cenários possíveis neste estudo técnico, que se alinham com as necessidades e diretrizes estratégicas existentes, os quais serão abaixo apresentados como eventuais alternativas.

8.1.1. **Alternativa 01 - Não aquisição da solução**

8.1.2. Permanecer sem uma solução de gestão de acessos privilegiados colocaria esta Coordenação e ao órgão em não conformidade com a LGPD e com estratégia nacional de segurança cibernética - e-ciber - decreto nº 10.222, de 5 de fevereiro de 2020.

8.1.3. Os riscos e perigos atrelados pela não utilização desta solução são extremamente altos e podem impactar negativamente em todos os serviços da Fundação.

8.1.4. Atualmente a gestão e salvaguarda destas a credencias estão a cargo de empresas e funcionários terceirizados sem vínculo que por ventura possam ter seus contratos findados ou serem desligados de suas funções. Este desligamento, passível nas relações de trabalho, poderia ensejar uma interrupção na prestação dos serviços à comunidade, uma vez que aquele funcionário/servidor, detentor de elevados privilégios, tenha saído insatisfeito e resolva prejudicar o funcionamento de um serviço ou sistema.

8.1.5. Além disso, é importante salientar a complexidade do ambiente e a quantidade de ativos de rede (usuários, switch, firewall, roteadores, balanceadores de carga, storage, servidores físicos e virtuais e aplicações diversas) existentes no parque atualmente e que estão sob administração desta Coordenação.

8.1.6. Assim, a segurança e integridade dos dados de toda a Fundação poderiam ser comprometidos, seja através de um desligamento de pessoas, um ataque cibernético ou mesmo um usuário malicioso dentro da própria rede, que ao obter sucesso em seu ataque poderia escalonar privilégios e assumir total controle do de dados sensíveis ou sistema.

8.2. **Alternativa 02 - Utilização de Software Livre ou código aberto**

8.2.1. Não foi encontrado nenhum software no portal https://softwarepublico.gov.br compatível com as necessidades da Funasa.

8.2.2. Já em relação a softwares livres de código aberto mantidos pela comunidade foi possível verificar a existência de algumas ferramentas para gerenciamento de identidade e acesso.

8.2.3. Entretanto, as ferramentas livres apesar de oferecem diversos benefícios, como a possibilidade de custo zero na aquisição de licenças e customização sob demanda, apresentam vários desafios, dentre eles:

8.2.3.1. Possuir equipe exclusiva para aprender, entender, dominar, customizar e manter sua operação;

8.2.3.2. Entender e mitigar os riscos de segurança envolvidos;

8.2.3.3. Não ter suporte sob demanda em caso de problemas;

8.2.3.4. Não haver garantia de qualidade do software, nem de continuidade de evolução técnica;

8.2.3.5. A Funasa não tem pessoas suficiente para ficar dedicado na operação de softwares livres. Introduzi-los num ambiente crítico como o desta Fundação, sem a devida atenção, representaria um enorme risco para a segurança de todo o parque computacional.

8.2.3.6. Para se ter noção do impacto que uma brecha de segurança em código aberto pode representar, utilizou-se o exemplo da empresa americana Equifax[1], que através de uma violação de segurança no Apache Struts[2], teve o vazamento dos dados de 143 milhões de clientes nos Estados Unidos, com um prejuízo estimado de U$ 439 milhões.

[1] - Por que a segurança em software open source ainda é um desafio. - https://computerworld.com.br/2018/04/03/por-que-seguranca-em-software-open-sourceainda-e-um-desafio/

[2] - Apache Struts. - https://pt.wikipedia.org/wiki/Apache_Struts

8.3. **Alternativa 03 - Aquisição de solução de gestão de acessos privilegiados (Privileged Access Management - PAM)**

8.3.1. Depreendendo-se das análises anteriores fica evidente a importância da aquisição de uma solução de gestão de acessos privilegiados ser, no atual cenário, a melhor opção para a Funasa. Poder contar com uma solução testada e homologada em diversos ambientes ao redor do mundo, com garantia e suporte técnico especializado é o diferencial esperado com essa contratação. A criticidade do ambiente e falta de pessoal, anteriormente mencionadas, aumentam significativamente a necessidade de auxílio de empresas tecnológicas com conhecimento e expertise na área, para que a implementação e continuidade dos serviços ocorram de forma segura e transparente para o usuário final.

8.4. **Identificação das soluções**

8.4.1. No contexto da presente contratação, existe o quadrante "Privileged Access Management".

8.4.2. Os documentos sei nº 2319585 e nº 2319581 possuem o comparativo detalhado das soluções de PAM. Espera-se que esta contratação consiga trazer para participar do certame, as melhores soluções do mercado e conseguir os menores preços da APF, conforme demonstração do quadrante mágico do Gartner e The Forrester Wave, abaixo:

Figura - Magic Quadrant for Privileged Access Management

Figura - Quadrante Forrester Wave

8.4.3. O estudo técnico irá focar nas soluções que se encontram no quadrante "Leaders";

8.5. **Análise das Alternativas existentes**

Requisito	Sim	Não	Não se aplica	Justificar quando não aplicável

A Solução encontra-se implantada em outro órgão ou entidade da Administração Pública Federal?	X			
A Solução está disponível no Portal do Software Público Brasileiro?		X		
A Solução é um software livre ou software público?		X		Os softwares livres encontrados não atendem a necessidade da Funasa conforme exposto no item .1.2.
A Solução é aderente às políticas, premissas e especificações técnicas definidas pelos Padrões e-PING, e-MAG?			X	O objeto dessa contratação não se enquadra nos padrões de acessibilidade e interoperabilidade do SISP.
A Solução é aderente às regulamentações da ICP-Brasil? (quando houver necessidade de certificação digital)			X	O objeto dessa contratação não se enquadra nos padrões do ICP-Brasil, porém adotam parcialmente práticas no padrão x509
A Solução é aderente às orientações, premissas e especificações técnicas e funcionais do – e-ARQ Brasil?			X	O objeto dessa contratação não se enquadra nos padrões do e-ARQ por não se tratar de solução arquivística.

8.6. **PROJETOS SIMILARES REALIZADOS POR OUTROS ÓRGÃOS OU ENTIDADES DA ADMINISTRAÇÃO PÚBLICA**

1- Tribunal de Justiça do DF e Territórios - TJDFT

UASG: 100001

PREGÃO ELETRÔNICO: Nº 065/2019 - PA: 0026940/2018

Descrição do Objeto: contratação de empresa para aquisição, suporte e atualização de solução de segurança da informação para a gestão de acessos privilegiados, armazenamento de credenciais, que possibilite o isolamento, gravação e o monitoramento de sessões de ativos de TIC do TJDFT por um período de até 36 meses, incluindo serviço de instalação e repasse de conhecimento, nos termos do presente edital e dos seus anexos

Valor Homologado/Negociado: R$ 4.300.000,00

Fornecedor: CARBONIT – FABRICANTE: CYBERARK

>A solução contratada contempla: Cofre Digital, Gravação de Acessos, Análise Comportamental em 2 Sites em Alta Disponibilidade para 14.000 dispositivos-alvo gerenciados e 150 usuários, Proteção para 20 aplicações, 2 (dois) clusters de orquestradores de contêineres com 60 hosts / 80 aplicações, Proteção local (agentes) para 4 controladores de domínio e 700 servidores, com 3 anos de garantia, instalação e treinamento.

***Não contempla: Proteção Local (agentes) para estações trabalho.*

2- Ministério da Justiça e Segurança Pública- MJSP

Conselho Administrativo de Defesa Econômica - CADE

UASG: 303001

PREGÃO ELETRÔNICO: Nº 08/2018

Descrição do Objeto: Contratação de soluções de gerenciamento de identidade, **gerenciamento de acessos privilegiados [GRUPO 2]** e correlacionamento de eventos, provendo ao Conselho Administrativo de Defesa Econômica - Cade - capacidade de gerenciamento de privilégios mínimos, autenticação transparente, múltiplos fatores de autenticação e adoção de provisionamento de acessos; geração de relatórios sobre eventos, otimização nas rotinas de identificação, detecção e análise de eventos e incidentes, armazenamento de registros de ativos de rede unificado, com resposta e remediação de incidentes de rede

Valor Homologado/Negociado: R$ 1.235.497,00

- TECHBIZ FORENSE DIGITAL LTDA – FABRICANTE: CYBERARK

>A solução contratada contempla: Cofre Digital, Gravação de Acessos, Análise Comportamental em 1.000 dispositivos alvo gerenciados, Proteção para 15 aplicações, Proteção local (agentes) para 350 servidores e 550 estações de trabalho, Site em Alta Disponibilidade, com 5 anos de garantia, instalação e treinamento.

**Não contempla: Proteção para Controladores de Domínio e credenciais em aplicações conteinerizadas.*

3- BANCO DO ESTADO DO PARÁ S.A.

UASG: 925803

Pregão Eletrônico Nº 40/2018

Descrição do Objeto: AQUISIÇÃO DE SOLUÇÃO DE AUDITORIA, GESTÃO E CONTROLE DE ACESSOS PRIVILEGIADOS

Valor Homologado/Negociado: R$ 5.293.183,00

- LICITANTE: VISION SET – FABRICANTE: CYBERARK

>A solução contratada contempla: Cofre Digital, Gravação de Acessos, Análise Comportamental em 4.000 sistemas alvo gerenciados, Proteção para 120 aplicações e 3 Controladores de Domínio, local (agentes) para 390 servidores e 3.500 estações de trabalho, 2 sites em Alta Disponibilidade, com 2 anos de garantia, instalação e treinamento.

**Não contempla: Proteção para credenciais em aplicações conteinerizadas.*

4- Ministério das Cidades

UASG: 560010

Pregão eletrônico nº: **10/2017**

Descrição do Objeto: O objeto da presente licitação é o registro de preços para contratação de empresa especializada para fornecimento de solução de segurança de gerenciamento de credenciais de altos privilégios e Firewall de nova geração, com garantia de 36 (trinta e seis) meses, contemplando serviços técnicos especializados de instalação, configuração e treinamento, conforme condições, quantidades e exigências estabelecidas neste Edital e seus anexos.

Valor Homologado/Negociado: R$ 1.470.210,00

- LICITANTE: DISRUPTEC BRASIL LTDA – FABRICANTE: LIEBERMAN SOFTWARE

> A solução contratada contempla: Cofre Digital para 3.000 dispositivos alvo gerenciados, Site em Alta Disponibilidade, com 3 anos de garantia, instalação e treinamento.

**Não contempla: Gravação de Acessos, Análise Comportamental, agentes para servidores e estações de trabalho, Proteção para Controladores de Domínio e credenciais em aplicações conteinerizadas.*

9. ANÁLISE E COMPARAÇÃO ENTRE OS CUSTOS TOTAIS DE PROPRIEDADE

9.1. Pesquisa de Preço

9.1.1. Quanto à pesquisa de preços de mercado, utilizou-se a metodologia prevista na Instrução Normativa Nº 73 de agosto de 2020, que dispõe sobre o procedimento administrativo para a realização de pesquisa de preços para a aquisição de bens e contratação de serviços em geral, no âmbito da administração pública federal direta, autárquica e fundacional.

9.1.2. O Art. 5º da IN 73/2020 determina que a pesquisa de preços será realizada mediante a utilização dos seguintes parâmetros, empregados de forma combinada ou não:

- *I - Painel de Preços, disponível no endereço eletrônico **http://paineldeprecos.planejamento.gov.br**;*
- *II - Contratações similares de outros entes públicos, em execução ou concluídos nos 180 (cento e oitenta) dias anteriores à data da pesquisa de preços;*
- *III - Pesquisa publicada em mídia especializada, sítios eletrônicos especializados ou de domínio amplo, desde que contenha a data e hora de acesso; ou*
- *IV - Pesquisa com os fornecedores, desde que as datas das pesquisas não se diferenciem em mais de 180 (cento e oitenta) dias.*

9.1.3. Em 01 de novembro de 2020, ao realizar a pesquisa no referido portal utilizando as expressões “*Gestão de identidade*” e "Gestão de acesso" e "Cofre de Senha" como parâmetro de pesquisa para o campo “Descrição do Serviço”, o resultado final das pesquisa não obteve êxito na pesquisa.

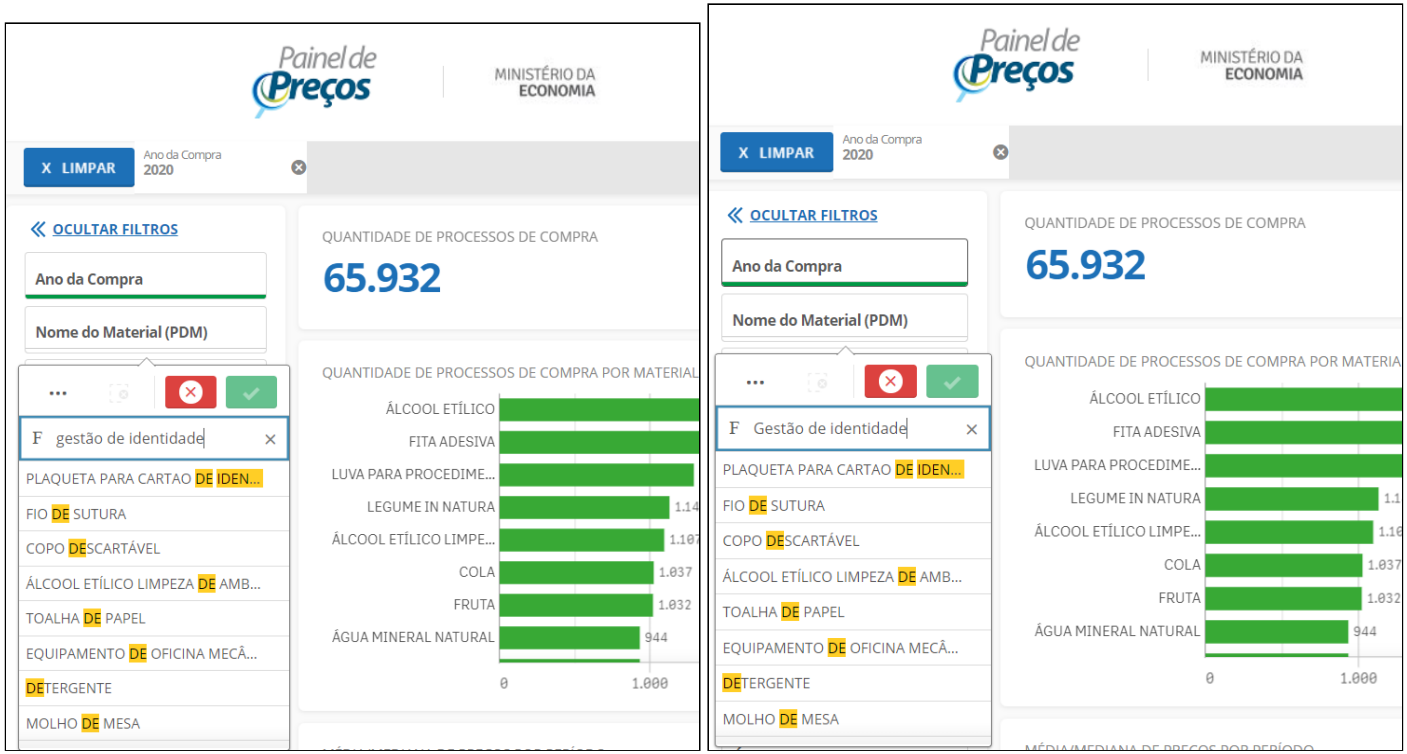

Imagem - Resultado da pesquisa de preço no sistema paineldepreços.gov.br

9.1.4. Concluindo, como não foi localizado nenhum objeto similar ao da Funasa no painel de preços, nem consultando outros órgãos da administração pública, a pesquisa de preço será composta com propostas de fornecedores conforme o item *IV - pesquisa direta com fornecedores, mediante solicitação formal de cotação, desde que os orçamentos considerados estejam compreendidos no intervalo de até 6 (seis) meses de antecedência da data de divulgação do instrumento convocatório.*

9.2. **CÁLCULO DOS CUSTOS TOTAIS DE PROPRIEDADE**

9.2.1. Análise e comparação entre os custos totais de propriedade das soluções identificadas, levando-se em conta os valores de aquisição dos ativos, insumos, garantia e manutenção. Foi solicitado aos fabricantes descritos no Gartner que enviasse à equipe de planejamento da contratação um preço estimado para que fosse possível dimensionar o impacto orçamentário da contratação (e-mail SEI 0496223).

I - Empresa 1 (2540310);

II - Empresa 2 (2540319);

III - Empresa 3 (2540328);

IV - Empresa 4 (2540343).

9.2.2. **Custo Total de Propriedade – Memória de Cálculo -** A planilha abaixo descreve os valores da pesquisa de preço com os fabricantes.

Grupo	Item	Descrição	Unidade de medida	Quantidade	Empresa 01		Empresa 02		Empresa 03		Empresa		Valor Médio Unitário (Média Aritmética)	Valor médio total (Média Aritmética)
					Valor Unitário	Valor Total	Valor Unitário	Valor Total	Valor Unitário	Valor Total	Valor Unitário	Valor Total		

1	1	Solução de gerenciamento de gestão de acessos privilegiados, armazenamento de credenciais, que possibilite o isolamento, gravação e o monitoramento de sessões de ativos de TIC com serviço de garantia pelo período de 36 (sessenta) meses	Solução	1	2.751.149,00	2.751.149,00	1.184.715,93	1.184.715,93	1.785.000,00	1.785.000,00	1.151.340,12	1.151.340,12	1.585.893,55	1.585.893,55
	2	Serviço de instalação e configuração para a solução de gestão de acessos privilegiados, armazenamento de credenciais	Serviço	1	50.000,00	50.000,00	89.833,33	89.833,33	34.000,00	34.000,00	61.476,74	61.476,74	54.302,40	54.302,40
	3	Suporte Técnico Mensal	Serviço	36	3.500,00	126.000,00	4.578,05	164.809,80	6.000,00	216.000,00	15.460,44	556.575,84	7.384,62	265.846,41
	4	Treinamento Técnico	Pessoa	5	10.000,00	50.000,00	5.600,00	28.000,00	5.600,00	28.000,00	10.200,00	51.000,00	16.908,08	84.540,38
Valor Total						**2.977.149,00**		**1.467.359,06**		**2.063.000,00**		**1.820.392,70**		**1.990.582,75**

9.3. **Custo Total de Propriedade – Memória de Cálculo - Estimativa de 03 Pontos (PERT):**

9.3.1. O valor estimado para início do pregão foi estimado utilizando a técnica de estimativa conhecida como Estimativa de Três Pontos, utilizada para estimativas de custos de projetos, de acordo com o Guia PMBOK.

9.3.2. A estimativa de 3 pontos, também conhecida como PERT (Técnica de Revisão e Avaliação de Programa), considera os riscos para aprimorar a estimativa de custo e orçamentação do projeto, e utiliza três estimativas para definir o valor aproximado de custos de um projeto:

- **Pessimista (E_p)**: os custos de determinada atividade são baseados na avaliação do pior cenário.
- **Otimista (E_o)**: os custos de determinada atividade são baseados na análise do melhor cenário.
- **Mais Provável (E_m)**: os custos de determinada atividade são baseados em uma análise realista para o objeto a ser adquirido considerando os valores praticados no mercado.

9.3.3. A estimativa de custos resultante da análise PERT é chamada de Custo Esperado da Atividade (Ce) e é calculada através de uma média ponderada das três estimativas:

$Ce = (E_o + 4*E_m + E_p)/6$

Utilizando a mesma técnica, calcula-se também o Desvio Padrão (DP):

$DP = \pm(Ep- Eo)/6$

Obs: Para a obtenção do valor Mais Provável, consideramos a média aritmética dos dois valores intermediários, ou seja, aqueles que não foram considerados estimativa otimista ou pessimista.

					Otimista		***Mais Provável***		***Pessimista***		***Estimativa de 3 Pontos (O+4MP+R)/6***	***Estimativa de 3 Pontos (O+4MP+R)/6***
Grupo	***Item***	***Descrição***	***Unidade de medida***	***Quantidade***	***Valor Unitário***	***Valor Total***	***Valor Unitário***	***Valor Total***	***Valor Unitário***	***Valor Total***	***Unitário***	***Total***
1	1	Solução de gerenciamento de gestão de acessos privilegiados, armazenamento de credenciais, que possibilite o isolamento, gravação e o monitoramento de sessões de ativos de TIC com serviço de garantia pelo período de 36 (sessenta) meses	Solução	1	1.151.340,12	1.151.340,12	1.484.857,97	1.484.857,97	2.751.149,00	2.751.149,00	1.640.320,16	1.640.320,16
	2	Serviço de instalação e configuração para a solução de gestão de acessos privilegiados, armazenamento de credenciais	Serviço	1	34.000,00	34.000,00	55.738,37	55.738,37	89.833,33	89.833,33	57.797,80	57.797,80
	3	Suporte Técnico Mensal	Serviço	36	3.500,00	126.000,00	5.289,03	190.404,90	15.460,44	556.575,84	6.686,09	240.699,24
	4	Treinamento Técnico	Pessoa	5	5.600,00	28.000,00	7.800,00	39.000,00	10.200,00	51.000,00	7.833,33	39.166,67
Valor Total						**1.339.340,12**						**1.977.983,87**

		1.770.001,24	**3.448.558,17**			

9.4. Considerando que a Média Ponderada do valor total obtida através da estimativa de 3 Pontos resultou ligeiramente inferior à média aritmética do valor total, adotando uma posição conservadora, utilizaremos o menor valor como valor estimado inicial para o Pregão.

9.5. Ainda, é importante mencionar que o custo total estimado anual, contemplando licenciamento, serviço de suporte mensal e treinamento se aproxima do valor pago apenas pelo serviço de suporte do contrato anterior, demonstrado no item 6.1.6 desde documento, ignorando o valor do licenciamento, treinamento e outros componentes do Custo Total de Operação.

9.6. **MAPA COMPARATIVO DOS CÁLCULOS TOTAIS DE PROPRIEDADE (TCO)**

Solução Viável 1	**Estimativa de TCO ao longo dos anos**		
Alternativa 03 - Aquisição de solução de gestão de acessos privilegiados (Privileged Access Management - PAM)	**1º ano**	**2º ano**	**3º ano**
	659.327,96	1.318.655,91	1.977.983,87

10. **DESCRIÇÃO DA SOLUÇÃO DE TIC A SER CONTRATADA**

10.1. Tendo como base a análise exposta nas **alternativas** dos Item 9, que apresentou as ressalvas e considerações quanto a não utilização de uma solução de gestão de acessos privilegiados ou a utilização de uma solução de código aberto, é possível inferir que uma eventual economia financeira advinda da escolhas de um dos itens retromencionados, poderá não representar uma vantagem diante do risco corporativo e operacional, além da possibilidade de interrupção e não entrega de serviços com a qualidade esperada na implementação desta solução.

10.2. Dessa forma, é razoável que a enorme responsabilidade imputada à equipe da CGMTI, responsável por salvaguardar e administrar a Rede Corporativa do Data center da Funasa, com sua atual dimensão exemplificada através do documento (3103646), poderia ser amenizada utilizando-se a solução pleiteada.

10.3. Os bens que constituem o objeto deste termo de referência enquadram-se no conceito de bem comum onde os requisitos técnicos são suficientes para determinar o conjunto da solução escolhida e ainda verificou-se que este objeto é fornecido comercialmente por mais de uma empresa no mercado.

Grupo	**Item**	**Descrição**	**Unidade de medida**	**Quantidade**
1	1	Solução de gerenciamento de gestão de acessos privilegiados, armazenamento de credenciais, que possibilite o isolamento, gravação e o monitoramento de sessões de ativos de TIC com serviço de garantia pelo período de 36 (trinta e seis) meses	Solução	1
	2	Serviço de instalação e configuração para a solução de gestão de acessos privilegiados, armazenamento de credenciais	Serviço	1
	3	Suporte Técnico Mensal	Serviço	36
	4	Treinamento oficial com o fabricante da solução	Pessoa	5

10.4. Os itens dos Lote 01 deverão ser licitados e adjudicados por grupo considerando a indivisibilidade dos mesmos, pois as soluções e os serviços são de uma mesma natureza, que guardam correlação entre si, seja por similaridade técnica ou de tecnologia.

10.5. O fornecimento de itens por meio de CONTRATADAS distintas trariam enormes riscos ao projeto. Um grande risco viria da necessidade continua de comunicação entre os diferentes fornecedores o quê, historicamente, não ocorre com fluidez nem de forma satisfatória, sendo a parte mais lesada o CONTRATANTE. Além disso, há necessidade de

ocorrer perfeita integração técnica entre os itens do objeto. Dessa forma, o fornecimento parcial dos itens por diferentes fornecedores traria não apenas maior complexidade, como maiores custos de integração e riscos de não execução adequada.

11. ESTIMATIVA DE CUSTO TOTAL DA CONTRATAÇÃO

11.1. Diante do exposto e com base na presente pesquisa de mercado, elaborada de acordo com a INSTRUÇÃO NORMATIVA Nº 73, DE 5 DE AGOSTO DE 2020, considerando a configuração de uma solução de segurança que atenda as necessidades da Funasa por 36 meses, conclui-se que a valor da contratação está estimado em **R$ 1.977.983,85** (um milhão, novecentos e setenta e sete mil novecentos e oitenta e três reais e oitenta e cinco centavos) , estão discriminados por itens nas tabelas a seguir:

Grupo	Item	Descrição	Unidade de medida	Quantidade	Valor Unitário	Valor total
1	1	Solução de gerenciamento de gestão de acessos privilegiados, armazenamento de credenciais, que possibilite o isolamento, gravação e o monitoramento de sessões de ativos de TIC com serviço de garantia pelo período de 36 (sessenta) meses	Solução	1	1.640.320,16	1.640.320,16
	2	Serviço de instalação e configuração para a solução de gestão de acessos privilegiados, armazenamento de credenciais	Serviço	1	57.797,80	57.797,80
	3	Suporte Técnico Mensal	Serviço	36	6.686,09	240.699,24
	4	Treinamento Técnico da solução	Pessoa	5	7.833,33	39.166,65
Valor Total						1.977.983,85

11.2. Os preços estimados da planilha serão considerados como valor máximos para aceitação da proposta pela Funasa.

12. DECLARAÇÃO DE VIABILIDADE DA CONTRATAÇÃO

12.1. A declaração da viabilidade da contratação expressa nessa seção apresenta a justificativa da solução escolhida, abrangendo a identificação dos benefícios a serem alcançados em termos de eficácia, eficiência, efetividade e economicidade.

12.2. Nesse sentido, o planejamento em tela almeja os seguintes resultados:

a) Economia no valor da aquisição da solução pretendida para substituir o Contrato 28/2018;

b) Eficiência com a redução do custo administrativo;

c) Efetividade com a padronização dos produtos e oferta de uma solução que objetiva maior produtividade e colaboração entre as equipes;

d) Eficácia com o atendimento das necessidades da instituição de está aderente com as normas de segurança da informação.

12.3. No mais, atende adequadamente às demandas de negócio formuladas, os benefícios a serem alcançados são adequados, os custos previstos são compatíveis e caracterizam a economicidade, os riscos envolvidos são administráveis.

12.4. Considerando as informações do presente estudo, entende-se que a presente contratação se configura tecnicamente **VIÁVEL.**

13. APROVAÇÃO E ASSINATURA

Conforme o § 2º do Art. 11 da IN SGD/ME nº 01, de 2019, o Estudo Técnico Preliminar deverá ser aprovado e assinado pelos Integrantes Técnicos e Requisitantes e pela autoridade máxima da área de TIC:

13.1. Integrante Requisitante

13.1.1. O presente planejamento atende adequadamente às demandas de negócio formuladas, os benefícios pretendidos são adequados, a viabilidade da contratação e os custos previstos são compatíveis e caracterizam a economicidade, os riscos envolvidos são administráveis e a área requisitante priorizará o fornecimento de todos os elementos aqui relacionados necessários à consecução dos benefícios pretendidos, pelo que recomendamos a aquisição proposta.

13.2. Integrante Técnico

13.2.1. O presente planejamento foi elaborado em harmonia com a Instrução Normativa n° 1 de 4 de abril de 2019, emitida pela Secretaria de Governo Digital do Ministério da Economia, bem como a viabilidade da contratação, que está em conformidade com os requisitos técnicos necessários ao cumprimento das necessidades e objeto da aquisição.

13.3. Responsável da Área Técnica e Requisitante

13.3.1. O presente planejamento está de acordo com as necessidades técnicas, operacionais e estratégicas do órgão e em conformidade com o Art. 10°, da Instrução Normativa n° 1 de 4 de abril de 2019, emitida pela Secretaria de Governo Digital do Ministério da Economia.

13.4. Integrante Administrativo

13.4.1. O presente planejamento está em conformidade com os requisitos administrativos necessários ao cumprimento do objeto, atendendo Instrução Normativa n° 1 de 4 de abril de 2019, emitida pela Secretaria de Governo Digital do Ministério da Economia.

13.5. Aprovação da Autoridade Competente

13.5.1. O presente documento está em conformidade com os requisitos administrativos necessários ao cumprimento do objeto e aprovo o Termo de Referência, cujos fundamentos passam a integrar a presente decisão por força do art. 50, §1º, da Lei nº. 9.784/99. Diante disso, decido motivadamente pelo prosseguimento da contratação em conformidade com o Art. 10°, §2º da Instrução Normativa n° 1 de 4 de abril de 2019, emitida pela Secretaria de Governo Digital do Ministério da Economia.

Documento assinado eletronicamente por **Andre Wilson Pimenta Santana**, **Coordenador(a)**, em 09/08/2021, às 10:27, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do Decreto nº 8.539, de 8 de outubro de 2015.

Documento assinado eletronicamente por **Telvio Martins de Mello**, **Coordenador-Geral de Modernização e de Tecnologia da Informação**, em 09/08/2021, às 14:43, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do Decreto nº 8.539, de 8 de outubro de 2015.

Documento assinado eletronicamente por **Marcio Biage da Silveira**, **Chefe do Serviço de Compras e Contratos**, em 09/08/2021, às 15:22, conforme horário oficial de Brasília, com

fundamento no art. 6º, § 1º, do Decreto nº 8.539, de 8 de outubro de 2015.

A autenticidade deste documento pode ser conferida no site https://sei.funasa.gov.br/consulta, informando o código verificador **3107526** e o código CRC **929E9E0A**.

Referência: Processo nº 25100.000334/2020-38 SEI nº 3107526