MINISTÉRIO DA ECONOMIA
Secretaria Especial de Desburocratização, Gestão e Governo Digital
Secretaria de Governo Digital
Departamento de Plataformas

ESTUDO TÉCNICO PRELIMINAR

Processo Administrativo nº 19974.100683/2022-39

AQUISIÇÃO CENTRALIZADA DE SOLUÇÃO DE SEGURANÇA PARA GERENCIAMENTO DE IDENTIDADES E ACESSOS

0.0.1.

HISTÓRICO - REVISÕES			
Data	**Versão**	**Descrição**	
21/04/2022	1.0	Criação do Documento	
	1.1	Revisão e Ajustes	
	2.0	Revisão e Ajustes após IRP	
	2.1	Revisão e ajustes após interações com o mercado e órgão de controle	
	2.2	Revisão e ajustes após análise da PGFN	

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 (SEI-ME n° 24189586), bem como demonstrar a viabilidade técnica e econômica das soluções identificadas, fornecendo as informações necessárias para subsidiar o processo de contratação, em consonância com o art. 11 da Instrução Normativa SGD-ME nº 01/2019.

1.2. O objeto do estudo é a **aquisição de solução de segurança para gerenciamento de identidades e acessos, para atender o Ministério da Economia e órgãos integrantes do Sistema de Administração dos Recursos de Tecnologia da Informação – SISP**.

2. MOTIVAÇÃO/JUSTIFICATIVA

2.1. O Ministério da Economia é um provedor de serviços e recursos para os órgãos integrantes do Sistema de Administração dos Recursos de Tecnologia da Informação – SISP.

2.2. Atualmente, a maioria dos serviços e atividades das áreas econômicas e negociais do governo federal, são processadas com o emprego de soluções e sistemas. Com o advento do emprego da tecnologia, migrando diversos serviços públicos para os meios digitais, elevam os riscos relacionados à segurança, compreendendo dados e informações de bases armazenadas nos mais diversos órgãos públicos, quanto a acessos não autorizados que podem resultar em vazamento de dados, afetando toda a estrutura governamental.

2.3. Os órgãos integrantes do SISP possuem infraestruturas complexas, variadas e robustas, que contam com diversos tipos de soluções e sistemas, construídos com os mais diversos tipos de tecnologias e linguagens. Para uma gestão e governança de todo esse conjunto de dados, informações e serviços digitais corporativos, visando o reuso, controle, monitoramento, segurança e alinhamento com o negócio, a Secretaria de Governança Digital - SGD/ME está propondo uma contratação centralizada desse tipo de serviço, de forma a mitigar riscos relacionados à segurança da informação.

2.4. A iniciativa dessa contratação esta intrinsecamente relacionada com o Programa de Privacidade e Segurança da Informação da Secretaria de Governo Digital:

> "O Programa de Privacidade e Segurança da Informação (PPSI) é constituído por um conjunto de ações de adequação nas áreas de privacidade e segurança da informação, desenvolvidas dentro do escopo das disciplinas de governança, pessoas, metodologia, tecnologia e gestão de maturidade, implementadas deforma concomitante e incremental. Tais ações são voltadas para aumento do grau de maturidade e de resiliência dos órgãos e das entidades integrantes do Sistema de Administração dos Recursos de Tecnologia da Informação (SISP) do Poder Executivo Federal."
> .

2.5. O PPSI é uma importante ferramenta para o aprimoramento das ações relacionadas a proteção de dados e segurança da informação " *O PPSI objetiva elevar o grau de maturidade dos órgãos e das entidades do SISP em termos de proteção de dados pessoais e ações de segurança da informação. Consequentemente, o PPSI também aumenta a proteção dos sistemas críticos de governo no ambiente cibernético."*

2.6. A pretensa contratação está diretamente ligada a torre de tecnologia que é uma das cinco torres que compõe o modelo de atuação do PPSI (Governa, Pessoas, Metodologia, Tecnologia e Gestão de maturidade):

> ***"Na torre de tecnologia , mantém-se o enfoque nas seguintes frentes:***
> ***- Soluções em segurança cibernética, contemplando avaliação e fomento da adoção de ferramentas de diagnósticos dos sistemas críticos que permitam a aplicação de testes como PENTEST, SAST, DAST, bem como prospecção conjunta com os órgãos do SISP de soluções SOC (Security Operations Center), SIEM (Security Information and Event Management) e NOC (Network Operations Center), dentre outras; e***
> ***- Desenvolvimento de plataforma de consentimento do cidadã o para atendimento aos princípios preconizados na Lei nº 13.709, de 14 de agosto de 2018 (LGPD), além de outras ferramentas."***

2.7. A disponibilização dessa solução de gerenciamento de identidades e acessos nos mais diversos órgãos, possibilitará:

- A integração de vários sistemas e aplicações de órgãos que fazem uso de diversas bases de usuários, nem sempre sincronizadas e consistentes (estejam estas baseadas em bancos de dados corporativos ou serviços de diretórios – *Active Diretory*), a uma solução de gerenciamento de identidade com um repositório de usuários sincronizado e consistente no âmbito da Administração Pública;
- Mapeamento de processos, a definição de perfis e a definição de políticas de controle de acesso adequadas a cada tipo de negócio e usuário, em vários órgãos;
- A consolidação do provisionamento de identidades para as diversas bases de autenticação utilizadas pelos recursos conectados à solução por meio de interfaces de uma única solução;
- A centralização e automatização da administração de identidades, ou seja, uma única interface administrativa, com um repositório central de usuários, aumentando assim a segurança e reduzindo os custos através da administração, controle e auditoria, que são necessidades comuns em diversos órgãos;
- O controle e a concessão de acesso para os serviços e sistemas críticos disponibilizados e definidos para cada tipo de perfil.

- Melhorar a eficiência operacional por meio de automações de segurança para tratamento das identidades, acelerando a transformação digital por meio da modernização dos acessos aos sistemas e apoiando o cumprimento dos requisitos de auditoria e conformidade.

2.8. Desse modo, o presente estudo é motivado pela necessidade de proteger a administração pública no cenário atual, onde a identidade é considerada o novo perímetro de segurança, gerenciando e monitorando contas e senhas, habilitando os trabalhos presenciais e remotos de maneira segura, resguardando as identidades críticas por meio do monitoramento dos comportamentos de maneira abrangente, evitando abusos de privilégios em portais e sistemas e a exploração do vetor mais comum de ataques cibernéticos na atualidade. Melhorar a eficiência operacional por meio de automações de segurança para tratamento das identidades, acelerando a transformação digital por meio da modernização dos acessos aos sistemas e apoiando o cumprimento dos requisitos de auditoria e conformidade, conforme destacam os renomados institutos do mercado no que tange a tecnologia da informação.

3. DEFINIÇÃO E ESPECIFICAÇÃO DAS NECESSIDADES E REQUISITOS

3.1. Identificação das necessidades de negócio

3.1.1. As necessidades de negócio, também chamadas de requisitos do negócio, segundo o Corpo de Conhecimento de Análise de Negócios (Guia BABOK v. 2.0), são metas de mais alto nível, objetivos ou necessidades da organização. Descrevem as razões pelas quais um projeto foi iniciado, os objetivos que o projeto vai atingir e as métricas que serão utilizadas para medir o seu sucesso. Nesse sentido, a presente seção visa descrever as necessidades de negócios que conduzirão as análises de soluções e definição daquela considerada mais adequadas a tais objetivos organizacionais, conforme relação a seguir:

Tabela 1 - Requisitos de negócio

REQUISITOS DE NEGÓCIO	JUSTIFICATIVA
Atender às demandas registradas nos Planos Anuais de Contratações (PAC) relacionadas à contratação de solução de segurança.	Verificou-se que a demanda pode ser atendida por ferramentas de diferentes fabricantes, desde que atuem no segmento pretendido, e diversos órgãos já licitaram objetos semelhantes. Nesse sentido, um dos direcionadores desses estudos é avaliar as diferentes formas de fornecimento e prestação desse tipo de objeto, que atende diferentes realidades e infraestruturas distintas.
Viabilizar a segurança e controle das identidades e seus acessos relacionados aos sistemas e soluções de TIC.	Considerando as ações estratégicas voltadas à segurança e proteção de dados e acessos não autorizados, relacionados ao Governo Federal e decorrentes da iniciativa 11.2 (Implementar controles de segurança da informação e privacidade em trinta sistemas críticos do Governo federal, até 2022) e Iniciativa 11.3 (Definir padrão mínimo de segurança cibernética a ser aplicado nos canais e nos serviços digitais, até 2022), do objetivo 11 - Garantia da segurança das plataformas de governo digital e de missão crítica, prevista na Estratégia de Governo Digital para o período de 2020 a 2022, anexo ao Decreto n°10.332 de 28 de abril de 2020, com redação dada pelo Decreto nº 10.996, de 14 de março de 2022.
Assegurar a proteção de dados armazenados e trafegados em soluções e sistemas governamentais	Definir padrão de identidade do órgão, definição de níveis de acesso com privilégio mínimo e de segregação de funções, estabelecendo processo e de responsáveis por solicitação, gerenciamento e revogação de contas de acesso e criando processos de verificação de identidade, com monitoramento de comportamentos das mesmas e trilhas de auditoria que vise ao registro dos acessos a sistema de informação.
Minimizar riscos de segurança da informação decorrentes de vulnerabilidades em Sistemas Operacionais	Segundo o relatório "*Operating System Security and Secure Operating Systems*", publicado pela GIAC (*Global Information Assurance Certification)*, 2013, a segurança dos sistemas operacionais é uma peça central para se assegurar a segurança dos softwares em execução e de todos os sistemas de informação que rodam sobre a infraestrutura de datacenter, além de estar relacionado com a segurança de outros elementos de rede tais como switches, firewalls, servidores, entre outros.
Melhores práticas	Garantir que o Ministério da Economia esteja aderente às melhores práticas nacionais e internacionais da área de Segurança da Informação, e em consonância com as normas vigentes.
Expansão	Proporcionar a expansão da capacidade atual, promovendo a proteção das identidades e seus acessos à infraestrutura tecnológica e áreas de negócio sustentadas pelo Ministério da Economia por meio das funcionalidades de rede e segurança presentes e habilitadas de acordo com a solução a ser contratada.
Diretrizes Governamentais e jurisprudenciais	Observar todas as diretrizes proferidas pelo Governo Federal e pelos Órgãos de Controle no que tange às orientações quanto às contratações de serviços públicos de TIC.

3.2. Identificação das necessidades tecnológicas

3.2.1. As necessidades tecnológicas, também chamadas de requisitos da solução de tecnologia, descrevem as características de uma solução que atenda aos requisitos do negócio. São desenvolvidos e definidos neste documento os seguintes requisitos tecnológicos.

3.2.2. A disciplina de segurança para identidades e acessos é a que permite que as pessoas certas acessem os recursos certos nos momentos certos e pelos motivos certos através de um plano de controle e monitoramento para determinar uma raiz de confiança para todas as identidades digitais.

3.2.3. Uma segurança para identidades e acessos eficaz deve validar identidades, proteger e monitorar os acessos, gerenciar privilégios de negócio e da tecnologia da informação aos recursos em ambientes de tecnologia cada vez mais heterogêneos e ser otimizado para segurança reforçada, prover boa experiência do usuário e eficiência operacional em todas as populações de usuários — sua força de trabalho, parceiros, clientes e identidades de máquina atendendo aos requisitos de conformidade cada vez mais rigorosos.

3.2.4. Processos e tecnologias de proteção das identidades eficazes e eficientes também podem desempenhar um papel central nos esforços de transformação digital de uma organização, aumentar a produtividade e o engajamento dos funcionários e fornecer uma base para fornecer relacionamentos confiáveis com clientes e parceiros.

3.2.5. As organizações que desenvolvem recursos de proteção e gerenciamento de acessos e identidades maduros podem reduzir seus custos e, mais importante, tornar-se significativamente mais ágeis no suporte a novas iniciativas de negócios.

3.2.6. Com o aumento das ameaças cibernéticas, regulamentações financeiras e de privacidade mais rígidas, as iniciativas de gerenciamento e segurança de identidades e seus acessos continuam crescendo. Fornecer serviços eficazes diante dos desafios atuais exige várias mudanças, muitas vezes interdependentes. Para

garantir o sucesso, é fundamental que os gestores de segurança e gerenciamento de riscos responsáveis gerenciem essas mudanças por meio de um programa bem estruturado e alinhado as áreas de negócio.

3.2.7. O desafio se torna complexo ao ter que suportar várias opções de acesso de usuários e dispositivos, bem como várias gerações de ativos digitais em uma infraestrutura de identidade moderna e flexível objetivando reduzir o risco, é necessário que se implemente as melhores práticas, como autenticação multifator (MFA) variada e adaptável, políticas de privilégio mínimo por meio de arquitetura de confiança zero.

3.2.8. Se não bastasse a heterogeneidade de identidades humanas ainda temos que lidar com o aumento de processos automatizados por robôs, assim como novos sistemas e de integrações sistemas de terceiros, os quais deixam uma trilha grande de credenciais de serviços (não humanas), que podem ser exploradas, trazendo um grande dano as corporações.

3.2.9. Outro aspecto relevante que temos que considerar é a crescente utilização de ambientes em nuvem, no qual em muitas vezes nos deparamos com um único sistema se encontrar operacional em mais de uma nuvem, trazendo uma grande complexidade operacional e de segurança.

3.2.10. O gerenciamento de segurança identidades e acessos necessita de um processo de aperfeiçoamento contínuo. Assim como um iceberg há grande quantidade de atividades sob a superfície das iniciativas propostas. Quando subestimamos a escala e o impacto da mudança pode levar a uma falha no planejamento.

3.2.11. O Gartner em seu estudo sobre IAM (*Identity and Access Management* - Gerenciamento e Identidades e Acessos) de 2021 aponta que “alguns líderes de segurança e gerenciamento de riscos acreditam que uma grande iniciativa de IAM pode ser implantada como um projeto” e “Alguns clientes planejam adquirir e implantar essa tecnologia em um prazo irreal e estão prontos para escolher um produto sem antes passar pelos estágios de planejamento adequados e configurar um programa formal de IAM. Esta é uma receita clássica para o fracasso...”

3.2.12. O Gartner projeta que, até 2021, as organizações sem um programa formal gastarão 40% a mais em recursos de IAM e alcançarão menos do que as organizações com esses programas. Os líderes de segurança e gerenciamento de risco responsáveis pelo IAM (líderes do IAM) devem trabalhar em estreita colaboração com as partes interessadas para garantir que os desenvolvimentos estejam alinhados às metas de negócios e que as mudanças sejam faseadas em tempo hábil. Ao empacotar e governar iniciativas em um único programa, os líderes podem gerenciar interações e agregar valor aos negócios durante todo o ciclo de vida do programa.

3.2.13. O Gartner ainda define que empregar as iniciativas embaixo de um programa único e bem governado de IAM garante:

- Benefícios planejados alinhados às necessidades do negócio;
- Os requisitos de recursos são totalmente compreendidos e gerenciados;
- As prioridades concorrentes são gerenciadas;
- Os benefícios são entregues como um fluxo contínuo de acordo com o plano; e
- O orçamento é usado de forma mais eficiente, minimizando o retrabalho e a duplicação de esforços.

3.2.14. O Forrester research em sua pesquisa denominada “*Evolve your IAM strategy*” (Evolua sua estratégia de IAM) apresenta quatro estágios fundamentais para programas de IAM:

- Determinar a responsabilidade por todas as áreas funcionais do IAM identificar e analisar os riscos do IAM criar orçamentos e construir parcerias em toda a organização;
- Atribuir e gerenciar privilégios e autorizações de usuários, fornecer autoatendimento ao usuário e aplicar políticas e fluxos de trabalho adaptáveis, respeitando o princípio de privilégio mínimo;
- Autenticação do acesso do usuário, inclusive para usuários privilegiados e identidades não humanas, com monitoramento contínuo para identificar atividades anômalas do usuário; e
- Gerar eficiências operacionais por meio de automação, configuração, melhoria de processos, rastreamento de ROI e do custo total de propriedade (TCO) para determinar o sucesso do projeto e ajustes orçamentários.

3.2.15. Para viabilizar a proteção da identidade fim-a-fim identificamos através dos estudos que o mercado está passando por uma convergência onde as soluções de segurança para identidades, gestão e controle dos seus acessos, sessões, contas e privilégios associados se unem garantido o controle da identidade, provendo auditoria, monitoramento comportamental com a habilitação de privilégios sob demanda.

3.2.16. Diante dos estudos realizados e das necessidades internas foram elencados os requisitos tecnológicos necessários para o desenvolvimento de um projeto robusto de segurança para identidades para suportar as inciativas do Ministério da Economia.

Tabela 2 - Requisitos Tecnológicos

REQUISITOS TECNOLÓGICOS	JUSTIFICATIVA
Prover mecanismos de segurança da informação	Com uma solução de gerenciamento de identidades e acessos, poderemos aplicar políticas de segurança eficientes e eficazes nos mais diversos contextos da instituição e seus mais diversos serviços, assim possuindo a capacidade de aplicar as diretrizes internas que garantam uma rastreabilidade e auditoria de registros.
Abranger todos os tipos de acessos e identidades	Partindo do preceito que qualquer identidade pode se tornar privilegiada através de movimentos laterais e escalação de privilégios, ou mesmo as próprias informações de negócio que esta identidade tem acesso podem possuir um alto grau de confidencialidade, faz se necessário assegurar o controle de identidade, acessos seguros e autorizados garantindo a segurança de credenciais (logins e senhas) sejam elas humanas (servidores públicos, terceiros, parceiros da administração pública ou cidadãos) ou não humanas (segredos no ciclo de desenvolvimento de softwares/serviços, robôs e credenciais de aplicações). Para isso é necessária uma solução que consiga manter segura esta gama heterogênea de identidades.
Assegurar mecanismos de gerenciamento de privilégios elevados	As identidades com privilégios elevados são responsáveis pelos acessos a sistemas e infraestruturas em nuvem, datacenter local e híbrida. Estas identidades têm um alto poder de comprometimento do ambiente tecnológico, estas sendo ativos tecnológicos de alto valor, faz se necessário a utilização de soluções especializadas de mercado que garantam a segurança destas identidades.
Prover registros de uso de privilégios e trilhas de auditoria	Possuir capacidade de informar dados e registros de acessos, de igual forma tais registros podem ser requisitados visando o atendimento de ocorrências referentes a Lei Geral de Proteção de Dados Pessoais (LGPD)
Detectar e mitigar incidentes de forma mais eficaz através de mecanismos de inteligência artificial	Este tipo de solução é a principal forma de prevenir impersonificação de identidades, abusos nos acessos, violações de privilégios, conseguindo conter ataques internos e externos. Ter a capacidade de controlar todos os serviços no âmbito digital por meio de um sistema consolidado trás uma enorme vantagem operacional. Sendo assim, além de conseguir definir quais aplicações determinado colaborador pode usar, também destacamos os ganhos em ter capacidade de monitorar e gerar alertas de atividades de risco e suspeitas no ambiente computacional, suspender e mitigar tais atividades, além de produzir relatórios detalhados sobre cada identidade e cada acesso privilegiado. Com a evolução tecnológica as soluções passaram a utilizar de inteligência artificial em seus motores analíticos que realizam o monitoramento, facilitando a detecção de atividades promíscuas, viabilizando a correlação dos eventos e acelerando o tempo de reação na identificação de incidentes de segurança.

Ganhar agilidade e eficiência no tratamento de incidentes e na criação de relatórios.	A falta de um relatório gerado automaticamente com todas as ações realizadas através das identidades e dos acessos privilegiados dificulta o tratamento de eventos e dos incidentes e possui esta capacidade facilitará a identificação de brechas de segurança e pontos de melhorias.
Prover políticas para acessos adaptativos baseados em riscos e contextos conhecidos de uma autenticação.	Através de políticas de acesso condicional será possível aplicar o conceito de confiança zero (Zero Trust), oferecendo aos usuários exatamente os acessos que necessitam para cumprir sua atividade fim. Mantendo o equilíbrio entre a prática de segurança e produtividade. Importante que estes acessos condicionais estejam aliados a mecanismos de inteligência artificial supracitados para detectar desvios de comportamento das identidades antes de realizar o início de uma sessão, oferecendo uma capacidade proativa e evitando o comprometimento do ambiente tecnológico antes da materialização do mesmo. Este conceito deve ser aplicado para todos os tipos de identidades sejam elas privilegiadas ou não.
Prover múltiplo fator de autenticação para diversos casos de uso com capacidade de interpretação de risco adaptativo	Ter a capacidade de prover autenticação autoajustada baseada no contexto de risco e segurança aprendido, permite a criação de um perfil de comportamento para cada usuário, aproveitando atributos históricos e situacionais específicos do mesmo, como localização, dispositivo, rede, horário, dia da semana, geo velocidade e índice de risco de comportamento. O risco atrelado ao comportamento do usuário deve fazer o uso de um motor de inteligência artificial baseado em algoritmos de aprendizado de máquina afim de conhecer desvios de comportamento individual de cada identidade, este risco deve ser utilizado para automação de processos antifraude, relatórios e durante a autenticação de início de sessão, este último com a finalidade de requisitar os métodos multifatoriais baseando-se no risco intrínseco a cada autenticação, ajudando no conceito do equilíbrio entre a prática de segurança e produtividade. Este conceito deve ser aplicado para todos os tipos de identidades sejam elas privilegiadas ou não. Os casos de uso para autenticação multifatorial não devem estar restritos somente para aplicações web, mas também para VPNs, estações de trabalho, servidores e infraestrutura de TI em geral.
Prover capacidade de acesso remoto a infraestrutura privilegiada e aplicações web de negócio sem VPN	Ser capaz de conceder acesso remoto aos ativos críticos e aplicações sem a necessidade de uma solução de VPN quando fora do ambiente tecnológico ou rede local do órgão. Este acesso deve obedecer a todos os preceitos de segurança e tipos de identidade supracitados, tais como, início de sessão com verificação de risco atrelado a Inteligência artificial e multifatorial.
Prover ganhos operacionais para recuperação de acessos e senhas	Aumentar a velocidade de atendimento de demandas de recuperação de acesso e reset de senhas, oferecendo capacidade de autosserviço e autenticação sem senha *(passwordless)*.
Gravação e proteção de sessões de aplicações do tipo web de negócio de forma não intrusiva.	Prover meios de auditar os acessos providos e as sessões web dos usuários finais para fins de auditoria e segurança
Possuir a capacidade de disparar gatilhos de gravação em vídeo relacionado a ações do usuário na estação de trabalho que estejam cumprindo atividades críticas	Partindo do preceito que qualquer identidade pode se tornar privilegiada através de movimentos laterais e escalação de privilégios, ou mesmo as próprias informações de negócio que esta identidade tem acesso pode possuir um alto grau de confidencialidade, faz-se necessário a gravação de sessões de aplicações web de negócio, conceitualmente não privilegiadas, a fim de prevenir o vazamento destas informações ou mesmo criar trilhas de auditorias detalhadas com evidências visuais das ações além de todas as modificações realizadas nestas sessões web. Importante que para o usuário final isto seja transparente, não seja necessário nenhum tipo de modificação de proxy de internet, utilização de VPN ou passagem por um servidor de acesso intermediário (servidor proxy / jump server). Tudo deve ser local na estação do usuário e enviado para um armazenamento em nuvem.
Proteger identidades, credenciais e acessos de forma fim-a-fim	Uma mesma solução que adeque as abordagens de PASM e PEDM junto da solução de IAM com o objetivo de fornecer visibilidade e controle em todas as etapas, facilitando também a implementação de controles específicos para cada nicho de proteção.
Proteger silos de armazenamento de credenciais em servidores e estações.	Deve proteger contra roubo de credenciais vulneráveis armazenadas em navegadores, aplicativos, ferramentas de acesso remoto, S.O. Windows e ações suspeitas; permitir a criação de armadilhas de credenciais para detecção antecipada de comportamentos de atacantes, diminuindo o tempo de permanência e o impacto de um ataque; Deve proteger as senhas de credenciais administrativas locais de todas as estações de trabalho Windows em um repositório central seguro de credenciais, permitindo a aplicação de políticas granulares de rotações e trocas automáticas das senhas, trilha de auditoria dos acessos às mesmas, mitigando situações de roubo, perda e exploração de credenciais; Deve permitir elevação de privilégios com acesso sob demanda - Just In Time - e validação de identidade via MFA passwordless integrado, permitindo provisionamento temporário do acesso de administrador local a estações de trabalho e servidores mediante solicitação, com base no tempo e removendo o acesso quando o tempo acabar, sendo o processo totalmente aditável e prover painel de inteligência de ameaças com relatórios.
Possuir capacidade de definição de políticas granulares para cada Etapa da proteção de identidades	Para cada etapa, entenda-se: Desde controle granular por usuário, até definições de acesso a recursos nos servidores e estações.
Deve se comunicar com outras ferramentas de segurança e ampla capacidade de integrações	A Solução deve permitir comunicação via API e Syslog para outros componentes de segurança da estratégia, como SIEM, SOAR, por exemplo, com o objetivo de participar diretamente da estratégia de segurança possuindo recursos nativos para que seja possível acelerar a implementação e adição de novos dispositivos, identidades em tempo de projeto.
Confiança zero (Zero Trust) orientado às Identidades	A solução deve apoiar o conceito de confiança zero (Zero Trust) com foco nas identidades e seus dispositivos utilizados durante o início de uma sessão. O primeiro passo é verificação de cada identidade utilizando conceitos multifatoriais de autenticação (alguma coisa que você sabe, tenha ou é) atrelados a um motor de inteligência artificial com algoritmos de aprendizado de máquina supracitados, para conhecer comportamentos desconhecidos que não são possíveis de serem configurados em regras de acessos condicionais (baseados em atributos de uma autenticação). O segundo passo é a verificação da identidade e se dispositivo utilizado é confiável, ou seja, é um dispositivo confiado pelo órgão.

Portal de Login Único Seguro para aplicações (SSO, Single Sign-On Seguro)	Necessidade de um portal único para acesso as aplicações através de SSO protegido pelos métodos de autenticação multifatoriais com risco adaptativo supracitados. Este portal deve ter suporte aos protocolos estândares mais modernos de mercado como também protocolos mais legados. Este portal de SSO com acesso as aplicações deve suportar de forma geral o autosserviço dos usuários para diversas funcionalidades da solução, tais como, reset de senha, registro dos métodos multifatoriais, aprovações, configurações de atributos da identidade dentre outros. Importante que este portal vise facilitar o acesso para as aplicações e ao mesmo tempo assegurar o acesso do mesmo somente para a identidade autenticada e autorizada, visando melhorar a experiência do usuário e também ganhos operacionais do órgão.
Gestão de senhas de aplicações de negócio que não suportam Single Sign-On (login único).	A solução deve incluir no seu portal de login único web (SSO, single sign-on) a capacidade de guardar senhas e usuários de aplicações de negócio que não estão sincronizadas com o repositório centralizado de identidades e/ou não suportam protocolos de SSO, com a finalidade de melhorar a segurança destas credenciais e também a experiência do usuário final. A segurança através do armazenamento destas credenciais diretamente na identidade corporativa do funcionário evitando que o mesmo utilize outras formas de armazenamento como planilhas, cadernos e soluções não corporativas para gestão de senhas. A experiência através da automação do autopreenchimento dos campos de usuário, senha e envio do formulário de login destas aplicações web. Deve também suportar o armazenamento de credenciais de aplicações não web, através de itens seguros. Importante que a solução não realize nenhum tipo de cache local destas credenciais, sempre consultando a nuvem da solução durante um preenchimento automatizado ou visualização destas credenciais, evitando assim o roubo das mesmas por malwares e atores não autorizados.
Diretório em nuvem IDP (*Identity Provider*)	Necessidade de um diretório em nuvem que possa fornecer identidades para autenticação e autorização as quais existam somente neste diretório, com a finalidade de flexibilizar a criação de identidades externas que não estão criadas nos repositórios de identidades tradicionais do órgão. Adicionalmente este diretório deve se conectar com os repositórios tradicionais de identidades com a finalidade de ser um concentrador de todos os repositórios de identidades, ondem possam ser aplicadas regras de autenticação e autorização adicionais supracitadas suportando o conceito de confiança zero (Zero Trust) para qualquer identidade que seja autenticada e autorizada pela solução. Importante que o diretório em nuvem possua APIs abertas para operações de criação, leitura, atualização e remoção de identidades e grupos.
Prover licenciamento em modalidade simples, preferencialmente, por identidade.	Prover licenciamento em modalidade simples, preferencialmente, por identidade.
Capacidade de gestão de senhas para usuários de negócio, com armazenamento em cofre de senhas	Prover ao usuário de negócio uma extensão no browser para retirar credenciais automaticamente do cofre e realizar a injeção nos campos de usuário e senha nas aplicações web com credenciais armazenadas para cada identidade, trazendo assim a experiência de SSO. Capacidade de armazenar também credenciais não web ou notas seguras no cofre de senhas. Adicionalmente não deve realizar nenhum tipo de cache local destas credenciais, sempre removendo do cofre sempre que utilizado. Dar a opção de não permitir o usuário não visualizar a senha durante a injeção das credenciais. Capacidade para os usuários de negócio compartilhem credenciais e automações de SSO com outros usuários.
Capacidade de controle de autenticação e autorização em nível granular para identidades não humanas	Permitir acesso em múltiplos ambientes, conseguindo assim diminuir a superfície de exposição e comprometimento.
Capacidade de proteção para chaves de API	Ter a capacidade de proteger chaves de API através do armazenamento seguro em estrutura centralizada (cofre) visando entrega para processos automatizados ou scripts que sejam sempre mascarados.
Capacidade de proteção de identidades não humanas em plataformas de conteinerização	Proteger credenciais não humanas através da capacidade de proteção e gerenciamento de segredos que atenda as demandas de segurança de credenciais e suas subcategorias, onde entende-se como segredos uma estrutura de dados que possa conter senhas, chaves privadas, tokens e chaves de APIs e ser entregue de maneira segura e criptografada para aplicações, contêineres e serviços, atuando como gerador e intermediário (broker) de segredos para diversos clientes, como aplicações, contêineres e clientes de criptografia possibilitando o armazenamento de múltiplas versões de um mesmo segredos. O fornecimento de segredos deve oferecer meios de controle de solicitante com múltiplos fatores, incluindo minimamente Tempo de vida (TTL) e restrições de IP/range
Disponibilizar pacote de desenvolvimento para proteção de identidades não humanas	Proteger identidade não humanas através da disponibilização de SDK (Software Development Kit) que pode ser configurado para permitir que aplicações possam solicitar as credenciais sob demanda ao invés de utilizar credenciais estáticas, atualizar informações de contas automaticamente no banco de dados de senhas e inscrever automaticamente em sistemas alvo sem aguardar por atualizações dinâmicas;
Capacidade de proteção de identidade não humanas para aplicações tracionais	Ter a capacidade de proteger credenciais não humanas através de suporte a utilização de integração com servidores WebSphere, WebLogic, JBoss e Tomcat, para fornecimento de credenciais via datasources, ou de funcionalidade semelhante, mantendo um cache atualizado das credenciais utilizadas localmente no servidor da aplicação, a fim de prevenir falhas na comunicação com o cofre digital e trazer velocidade às consulta, além de suportar redundância de credenciais, oferecendo mais de um usuário e senha à aplicação em questão de maneira transparente, de forma que se evite qualquer possível indisponibilidade mínima durante o processo de troca de senhas.

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

3.3.1. Além dos requisitos de negócio e tecnológicos, a presente seção destaca aqueles requisitos que devem ser considerados ao longo do planejamento da contratação para se assegurar o alcance dos objetivos pretendidos com a aquisição, conforme a seguir:

Tabela 3 - Requisitos complementares

REQUISITOS	JUSTIFICATIVA
Suportar requisitos da LGPD	Buscando apoiar nas iniciativas de conformidade com a lei geral de proteção de dados a solução deverá suportar os artigos 6, 42, 43, 46, 48 e 50.
Requisitos Sociais, Ambientais e Culturais	Deverá fornecer as licenças de software de forma eletrônica, evitando a confecção e transporte de mídias.
Requisitos de implementação	Deverá ser elaborado conjuntamente o projeto de implementação da solução.
Requisitos de transferência de	Deverá ser elaborado conjuntamente o conteúdo referente a transferência de conhecimento da solução.

conhecimento	
Requisitos de suporte técnico	Devido a complexidade operacional e a necessidade de recursos especializados consideramos como necessário serviço de suporte técnico para apoiar as demandas de operação e evolução da solução.

4. ESTIMATIVA DA DEMANDA – QUANTIDADE DE BENS E SERVIÇOS

4.1. A presente seção contém o registro do quantitativo estimado de bens e serviços necessários para a composição da solução a ser contratada, de forma detalhada, motivada e justificada, inclusive quanto à forma de cálculo. Busca-se descrever também os métodos, as metodologias e as técnicas de estimativas que foram utilizados, nos termos do inciso I do art. 11 da IN SGD-ME n.º 01/2019.

4.2. Inicialmente, apenas para efeitos de uma cotação para obtenção de valores unitários, a SGD/ME apresenta a seguinte quantidade inicial:

Tabela 4 - Estimativa da Demanda

DESCRIÇÃO	QUANTIDADE
Segurança para identidades - Proteção de acesso do usuário final adaptado ao risco comportamental	1000
Segurança para identidades – Monitoramento e proteção da sessão do usuário final	1000
Segurança para identidades – Proteção e gestão de credenciais do usuário final em browser	1000
Segurança para identidades – Proteção e monitoramento de ameaças ao usuário da TI	200
Segurança para identidades – Segurança para identidades – Proteção e monitoramento de ameaças a credenciais em servidores	100
Segurança para identidades – Segurança para identidades – Proteção e monitoramento de ameaças a credenciais em estações de trabalho	1000
Segurança para identidades – Proteção de secrets em aplicações nativas em nuvem/contêiner	2
Segurança para identidades – Proteção de secrets em aplicações tradicionais/legado	100
Serviço Técnico Especializado - Operação Assistida (até 3.000 subscrições)	1
Treinamento (até 6 pessoas)	Quantidade: 1

4.3. No momento da realização deste estudo técnico não foi possível estimar o quantitativo necessário para o atendimento do Ministério da Economia, em função da dificuldade de coletar as informações necessárias, uma vez que o órgão encontra-se em processo de segregação de seus usuários de rede dos usuários de rede do Ministério da Previdência e Trabalho (órgão criado recentemente e cuja as atribuições eram executadas pelo Ministério da Economia).

4.4. Verifica-se que as quantidades acima são meramente aleatórias, com o objetivo de obter valores unitários de cada item. Após a abertura da IRP todos os órgãos do SISP interessados em participar, juntamente com o Ministério da Economia encaminharão os quantitativos reais para que possa ser consolidado a estimativa da demanda e posteriormente seja realizada uma nova cotação de preço a qual integrará a pesquisa de preço e consequentemente a definição do orçamento da licitação.

5. ANÁLISE DO MERCADO FORNECEDOR

5.1. Nesta seção, pretende-se apresentar os aspectos relacionados ao mercado fornecedor, apontando suas principais características e especificidades relacionadas às compras de governo nesse segmento.

5.2. A equipe de planejamento seguiu uma ordem lógica, que permitiu registrar todo o esforço empreendido até a escolha da solução que atende a demanda de forma mais eficiente.

5.3. Em primeiro lugar, a equipe de planejamento buscou entender o objeto junto ao segmento de mercado. Posteriormente, buscou avaliar as alternativas que se encontram disponíveis e por fim buscou avaliar qual o melhor modelo de fornecimento do objeto. A partir desses insumos, a equipe analisou todos os prós e contras dos insumos provenientes das análises acima e cotejou com a demanda identificada pela Área Requisitante, o que permitiu concluir pelo cenário que atende às necessidades de forma mais eficiente.

5.4. **Segmentos de Mercado**

5.4.1. O mercado de segurança da informação é amplo e possui diversos fabricantes de soluções que podem, a princípio, atender às demandas identificadas pela área requisitante.

5.4.2. Foram identificadas algumas soluções livres para o objeto proposto, tais como: KleycloaK e OpenIAM, contudo em função de não contemplar todas as funcionalidades almejadas, incompatibilidade com alguns requisitos técnicos necessários para o atendimento das demandas e principalmente pela ausência de suporte técnico, essas soluções não foram incluídas no comparativo de soluções viáveis, por considerar que o suporte técnico de um fabricante nos assuntos relacionados a segurança da informação é de suma importância para a administração.

5.4.3. O Segmento de soluções de gerenciamento de identidades e acessos compreende um tipo de objeto de extrema relevância para proteção do ambiente tecnológico. Esse segmento de mercado é amplo, existindo ferramentas de diversos fabricantes com funcionalidades e modelos distintos, os quais passaremos a analisar no tópico a seguir.

5.5. **Produtos e Soluções de Mercado**

5.5.1. Observando-se as necessidades e os requisitos tecnológicos elencados nesse estudo técnico, bem como a análise do mercado, realizamos o levantamento das soluções relacionadas ao gerenciamento de identidades e acesso e apresentamos uma descrição sucinta de cada uma delas.

5.5.2. Solução de Mercado 01 – Delinea

5.5.2.1. O fabricante Delinea possui às soluções Delinea Privileged Behavior Analytics, Cpnnection Manager, Server Suite, Cloud Suite, Privilege Manager, Cloud Access Controller.

5.5.3. Solução de Mercado 02 – Microsoft

5.5.3.1. O fabricante Microsoft possui a solução na sua suite de Identity and Access Management o Azure AD Premium P2 e o Azure AD Privileged Identity Management

5.5.4. Solução de Mercado 03 – Cyberark

5.5.4.1. O fabricante Cyberark possui a solução CyberArk Workforce Identity - Single Sign-on, Adaptive Multi-Factor Authentication, Directory Services, Endpoint Authentication, App Gateway, User Behavior Analytics e Secure Web Sessions, Privileged Access Manager, DevSecOps e Endpoint Privilege Manager.

5.5.5. Solução de Mercado 04 – Google

5.5.5.1. O fabricante Google possui a solução Google Cloud Identity Premium - Multi-Factor Authentication, Endpoint management, Single sign-on.

5.5.6. Solução de Mercado 05 – Micro Focus

5.5.6.1. O fabricante Micro Focus possui as soluções NetIQ Access Manager e Privileged Access Manager, Risk Service e Self service Password Reset.

5.5.7. Solução de Mercado 06 – Beyond Trust

5.5.7.1. O fabricante Beyond Trust possui as soluções Password Safe e Privilege Management.

5.5.8. Solução de Mercado 07 – Senha Segura

5.5.8.1. O fabricante Senha Segura possui as soluções Account and Session PAM Core, Domum acesso remoto, Endpoint PAM SenhaSegura Go.

5.6. **Análise de contratações com similaridade**

5.6.1. A equipe de planejamento da contratação buscou junto ao mercado, contratações, com as seguintes características: Escopo similar ao objeto, similaridades de requisitos negociais e tecnológicos, publicados recentemente e que foram antedidos com as soluções de mercado identificadas no item 5.5 deste estudo técnico, e o resultado encontra-se abaixo:

Tabela 5 - Contratações similares

UASG	ÓRGÃO	PREGÃO	PRODUTO	DATA	QUANTIDADE	VALOR
927353	Superintendência Estadual de Licitações - SUPEL/RO	820/2021	Solução de Gerenciamento de Acessos Privilegiados (*Privileged Access Management – PAM*)	27/01/2022	Solução	669.750,00
413001	Agência Nacional de Telecomunicações - ANATEL	25/2021	Solução	21/12/2021	Solução de PAM (Gerenciamento de Acesso Privilegiado) (5)	2.967.065,33
					Solução de auditoria de serviços Microsoft (3)	5.132.277,44
Total						8.099.342,77
90026	Conselho da Justiça Federal – CJF	37/2021	Solução, serviços e transferência de conhecimento	09/12/2021	Vários	1.004.933,33
200009	Ministério Público do Distrito Federal e Territórios – MPDFT	72/2021	Solução, serviços e transferência de conhecimento	29/11/2021	Vários	1.530.421,57
154215	UNIFAP	15/2020	Solução de Segurança da informação para Sistemas Críticos com Monitoramento Comportamental, Repositório Seguro, Proteção de Aplicações dentro ou fora de containers, Proteção para Servidores e Estações de Trabalho, entre outros	30/12/2020	Vários	13.942.930,00
303001	CADE	08/2018	Contratação de soluções de gerenciamento de identidade, gerenciamento de acessos privilegiados e correlacionamento de eventos, provendo ao Conselho Administrativo de Defesa Econômica - CADE	27/11/2018	Vários	4.360.645,00

5.7. **Análise geral das ferramentas identificadas**

5.7.1. De modo geral, as ferramentas acima possuem características específicas provenientes de cada fabricante. A grande quantidade identificada junto ao mercado exigiu uma análise especialmente de ordem técnica, apreciando se as características de cada uma são capazes de atender a demanda, especialmente em relação aos requisitos previamente identificados. Algumas funcionalidades são comuns e abaixo listamos os resultados dessa análise.

5.7.2. Prover mecanismos de segurança da informação

5.7.2.1. Todas as soluções possuem as características mínimas de segurança da informação com automações e auditorias mais simplificadas, porém a maioria das soluções não possuem profundidade no que diz respeito a mecanismos inteligentes proativos de detecção e mitigação de ameaças às identidades e credenciais, como roubo de senhas e abuso de privilégios com identidades de negócios e máquinas/serviços.

5.7.3. Abranger todos os tipos de acessos e identidades

5.7.3.1. Este requisito de proteção de acessos e identidades de usuários de negócio não foi identificado junto às soluções dos fabricantes Delinea e BeyondTrust, já os requisitos de proteção a acessos e identidades de administradores da TI foi identificado junto às soluções Delinea, Microsoft, CyberArk, Google, MicroFocus, Beyond Trust e Senha Segura. No caso das soluções da Microsoft e Google foi identificado que atendem parcialmente esta necessidade.

5.7.3.2. Apesar das soluções Microsoft e Google endereçarem proteções para identidades e acessos de administradores da TI, eles se limitam aos seus ambientes providos em nuvem, deixando de atender demandas de soluções de mercado amplamente utilizadas nos ambientes tecnológicos, como Bancos de Dados Oracle, sistemas Unix/Linux, ativos de rede, entre outros.

5.7.4. Assegurar mecanismos de gerenciamento de privilégios elevados

5.7.4.1. Este requisito não foi identificado junto as soluções Google e Senha Segura

5.7.4.2. A solução da Microsoft atende parcialmente esta necessidade, uma vez que está limitado ao universo Microsoft.

5.7.4.3. Esse requisito é plenamente atendido pelas soluções da Delinea, Cyberark, Micro Focus e Beyond Trust.

5.7.5. Prover registro de uso de privilégio e trilhas de auditoria

5.7.5.1. Este requisito não foi identificado para identidades e acessos de negócio junto as soluções Delinea, Microsoft, Google, MicroFocus, Beyond Trust e Senha Segura.

5.7.5.2. Este requisito é atendido pela solução da Cyberark tanto para identidades e acessos privilegiados de usuários de negócio quanto de administradores da TI.

5.7.5.3. As soluções, no geral, possuem características para gerar trilhas de auditoria limitadas aos acessos privilegiados de administradores da TI.

5.7.6. Detectar e mitigar incidentes de forma mais eficaz através de mecanismos de inteligência artificial

5.7.6.1. As soluções Delinea, Microsoft, Google, Beyond Trust e Senha Segura dispõem de capacidades limitadas a algumas detecções de ameaças/comportamentos anômalos das identidades de administradores das TI.

5.7.6.2. As soluções Google, Microsoft e CyberArk dispõem de capacidades de detecções de ameaças/comportamentos anômalos das identidades de negócios.

5.7.6.3. A solução CyberArk dispõe das capacidades de detecção e mitigação de incidentes envolvendo todos os tipos de identidades demandadas.

5.7.7. Ganhar agilidade e eficiência no tratamento de incidentes e na criação de relatórios

5.7.7.1. Esse requisito não foi identificado junto as soluções Delinea, Google, Beyond Trust e Senha Segura.

5.7.7.2. As que atendem parcialmente esta necessidade são as soluções da Microsoft e MicroFocus.

5.7.7.3. A solução Microsoft não possui a abrangência necessária para identidades privilegiadas e a MicroFocus possui módulos limitados, que não realizam para todos os tipos de identidades.

5.7.7.4. Este requisito é atendido pela solução da Cyberark.

5.7.8. Confiança zero (zero trust) para identidades

5.7.8.1. O requisito não foi identificado junto as soluções Delinea, Beyond Trust e Senha Segura

5.7.8.2. As que atendem parcialmente esta necessidade são as soluções da Microsoft, Google e MicroFocus

5.7.8.3. A soluções Microsoft e Google não possuem a abrangência necessária para identidades privilegiadas e a MicroFocus possui módulos limitados, que não realizam para todos os tipos de identidades

5.7.8.4. Este requisito é atendido pela solução da Cyberark

5.7.9. Prover políticas para acessos adaptativos baseados em riscos e contextos conhecidos de uma autenticação

5.7.9.1. Este requisito não foi identificado junto as soluções Delinea, Beyond Trust, MicroFocus e Senha Segura

5.7.9.2. As que atendem parcialmente esta necessidade são as soluções da Microsoft e Google.

5.7.9.3. Este requisito é atendido pela solução da Cyberark

5.7.9.4. As soluções que cumprem parcialmente possuem módulos de Inteligência Artificial, porém estão limitados a alguns tipos de identidades e, especificamente as soluções da Microsoft e do Google não realizam a avaliação do comportamento temporal para logins de risco baseados neste comportamento.

5.7.10. Prover múltiplo fator de autenticação para diversos casos de uso com capacidade de interpretação de risco adaptativo

5.7.10.1. Este requisito não foi identificado junto as soluções Delinea, Beyond Trust e Senha Segura

5.7.10.2. As que atendem parcialmente esta necessidade são as soluções da Microsoft e Google.

5.7.10.3. A solução Microsoft se limita a conhecer localidades e novos dispositivos para verificar o comportamento histórico de uma identidade.

5.7.10.4. Este requisito é plenamente atendido pelas soluções da Cyberark e Micro Focus.

5.7.11. Prover capacidade de acesso remoto a infraestrutura privilegiada e aplicações web de negócio sem VPN

5.7.11.1. Este requisito não foi identificado junto as soluções Google e Micro Focus

5.7.11.2. As que atendem parcialmente esta necessidade são as soluções da Delinea, Microsoft, Beyond Trust e Senha Segura

5.7.11.3. Este requisito é plenamente atendido pela solução da Cyberark.

5.7.11.4. As soluções que cumprem parcialmente se limitam a realizar tal acesso somente para alguns tipos de identidades (em geral privilegiadas de administradores da TI).

5.7.12. Prover ganhos operacionais para em recuperação de acessos e senhas

5.7.12.1. Este requisito não foi identificado junto as soluções Delinea, Google, Beyond Trust e Senha Segura

5.7.12.2. Este requisito é plenamente atendido pelas soluções da Microsoft, Cyberark e Micro Focus

5.7.13. Gravação e proteção de sessões de aplicações do tipo web de negócio de forma não intrusiva.

5.7.13.1. Este requisito não foi identificado junto as soluções Delinea, Microsoft, Google, MicroFocus, Beyond Trust e Senha Segura

5.7.13.2. Este requisito é atendido pela solução Cyberark

5.7.13.3. As soluções que não cumprem com esta funcionalidade se limitam a realizar o requisito para identidades privilegiadas de administradores de TI.

5.7.14. Possuir a capacidade de disparar gatilhos de gravação em vídeo relacionado a ações do usuário na estação de trabalho que estejam cumprindo atividades críticas.

5.7.14.1. Esse requisito não foi identificado junto as soluções Delinea, Microsoft, Google e MicroFocus

5.7.14.2. As que atendem esta necessidade são as soluções Beyond Trust, CyberArk e Senha Segura

5.7.15. Proteger identidades, credenciais e acessos de forma fim-a-fim.

5.7.15.1. Esse requisito de proteção de acessos e identidades de usuários de negócio não foi identificado junto às soluções dos fabricantes Delinea, BeyondTrust, já os requisitos de proteção a acessos e identidades de administradores da TI foi identificado junto às soluções Delinea, Microsoft, CyberArk, Google, MicroFocus, Beyond Trust e Senha Segura.

5.7.15.2. As soluções Microsoft e Google atendem parcialmente esta necessidade.

5.7.15.3. Apesar das soluções Microsoft e Google endereçarem proteções para identidades e acessos de administradores da TI, os mesmos se limitam aos seus ambientes providos em nuvem, deixando de atender demandas de soluções de mercado amplamente utilizadas nos ambientes tecnológicos, como Bancos de Dados Oracle, sistemas Unix/Linux, ativos de rede, entre outros.

5.7.15.4. Esse requisito é plenamente atendido pela solução da Cyberark

5.7.16. Proteger silos de armazenamento de credenciais em servidores e estações

5.7.16.1. Os requisitos de proteções contra roubo de credenciais vulneráveis armazenadas em navegadores, aplicativos, ferramentas de acesso remoto, S.O. Windows e criação de armadilhas de credenciais não foram identificados junto as soluções, Delinea, Microsoft, Google, MicroFocus, Beyond Trust e Senha Segura.

5.7.16.2. As que atendem parcialmente às necessidades de proteção das senhas de credenciais administrativas locais de todas as estações de trabalho Windows e permisão de elevação de privilégios com acesso sob demanda - Just In Time são as soluções Delinea, BeyondTrust e Senha Segura.

5.7.16.3. Este requisito é plenamente atendido pela solução da Cyberark.

5.7.17. Possuir capacidade de definição de políticas granulares para cada etapa da proteção de identidades

5.7.17.1. Este requisito é atendido parcialmente junto as soluções Google e Senha Segura, as soluções referenciadas não atendem todas as etapas da proteção de identidades por todos os pontos necessários.

5.7.17.2. Este requisito é plenamente atendido pelas soluções da Delinea, Microsoft, Cyberark, Microfocus e Beyond Trust

5.7.18. Deve se comunicar com outras ferramentas de segurança e ampla capacidade de integrações.

5.7.18.1. Esse requisito não foi identificado junto as soluções Google e Senha Segura

5.7.18.2. As que atendem parcialmente esta necessidade são as soluções Microsoft e Micro Focus

5.7.18.3. Microsoft, possui comunicação limitada ao universo Microsoft em sua plenitude. Para outros casos, a integração com outros fabricantes é limitada. A Micro Focus possui API para soluções de IDM, não a qualificando para a ampla capacidade de integrações.

5.7.18.4. Este requisito é plenamente atendido pelas soluções da Delinea, Cyberark e Beyond Trust

5.7.19. Portal de Login Único para aplicações (SSO, Single Sign-On)

5.7.19.1. O requisito não foi identificado junto as soluções Delinea, Beyond Trust e Senha Segura.

5.7.19.2. Este requisito é plenamente atendido pelas soluções da Microsoft, Cyberark, Google e Micro Focus

5.7.20. Gestão de senhas de aplicações de negócio que não suportam Single Sign-On (login único).

5.7.20.1. O requisito não foi identificado junto as soluções Delinea, Microsoft, Google, Beyond Trust e Senha Segura

5.7.20.2. A que atende parcialmente esta necessidade é a solução da Micro Focus.

5.7.20.3. Micro Focus não realiza este armazenamento para aplicações que não são web no mesmo portal de SSO.

5.7.20.4. Este requisito é plenamente atendido pela solução da Cyberark.

5.7.21. Diretório em nuvem IDP (Identity Provider)

5.7.21.1. O requisito não foi identificado junto as soluções Delinea, MicroFocus, Beyond Trust e Senha Segura

5.7.21.2. O requisito é plenamente atendido pelas soluções da Microsoft, Cyberark e Google

5.7.21.3. As Soluções que não cumprem esse requisito é porque não possuem um IDP nativo.

5.7.22. Prover licenciamento em modalidade simples, preferencialmente, por identidade.

5.7.22.1. O requisito foi identificado junto a todas as soluções analisadas.

5.7.23. Capacidade de gestão de senhas para usuários de negócio, com armazenamento em cofre de senhas

5.7.23.1. O requisito não foi identificado junto as soluções Microsoft, Beyond Trust e Senha Segura

5.7.23.2. As que atendem parcialmente esta necessidade são as soluções Google e Micro Focus, essas soluções não possuem características de autosserviço para o compartilhamento das credenciais de negócio. Especialmente a solução do Google trabalha via cache local que não é considerado seguro por haver o risco de manipulação local do silo de credenciais.

5.7.23.3. Este requisito é plenamente atendido pelas soluções da Cyberark e Delinea

5.7.24. Capacidade de controle de autenticação e autorização em nível granular para identidades não humanas

5.7.24.1. O requisito não foi identificado junto as soluções Dilinea, MicroFocus e Beyond Trust

5.7.24.2. A que atende parcialmente esta necessidade são as soluções da Google e SenhaSegura. A solução da Google atende mediante a utilização das funções inerentes ao Google IAM, consequentemente a integração ocorre somente com produtos e serviços da própria google, com relação a solução da senha segura, ela só atende parcialmente pois em ambiente de plataforma de orquestação de contêneir ela não utiliza todas as caracteristícas do ambiente.

5.7.24.3. Esse requisito é plenamente atendido pelas soluções da Cyberark e Microsoft

5.7.25. Capacidade de proteção para chaves de API

5.7.25.1. O requisito não foi identificado junto a solução MicroFocus

5.7.25.2. Este requisito é plenamente atendido pelas soluções da Cyberark, Delinea, Microsoft, Google, Beyond Trust e SenhaSegura

5.7.25.3. Capacidade de proteção de identidades não humanas em plataformas conteinerização

5.7.25.4. o requisito não foi identificado junto a solução MicroFocus

5.7.25.5. As que atendem parcialmente esta necessidade são as soluções da Delinea, Microsoft, Google, Beyond Trust e SenhaSegura. Todas as soluções seguem o mesmo critério , não atendendo granularidade de identificação de recursos como exemplo: Namespace e serviceaccount

5.7.25.6. Este requisito é plenamente atendido pelas soluções da Cyberark

5.7.26. Disponibilizar pacote de desenvolvimento para proteção de identidades não humanas

5.7.26.1. O requisito não foi identificado junto a solução MicroFocus.

5.7.26.2. As que atendem parcialmente esta necessidade são as soluções da Delinea, Microsoft, Beyond Trust e SenhaSegura. A Solução da Microsoft entrega somente para .Net, as demais apresentam escopo limitado de linguagens de desenvolvimento.

5.7.26.3. Este requisito é plenamente atendido pelas soluções Google e Cyberark.

5.7.27. Capacidade de proteção de identidade não humanas para aplicações tracionais (Não conteinerizadas ou não nativas em nuvem)

5.7.27.1. O requisito não foi identificado junto as soluções Microsoft, Google e MicroFocus

5.7.27.2. As que atendem parcialmente esta necessidade são as soluções da Delinea, Beyond Trust e SenhaSegura. As soluções que atendem parcialmente, atendem via API, mas não oferecem possibilidade de armazenamento local do tipo cache nem oferecem drive proxy.

5.7.27.3. Esse requisito é plenamente atendido pela solução da Cyberark

5.7.28. Após análise detalhada de todos os requisitos mínimos indispensáveis, elaboramos uma tabela comparativa entre as soluções identificadas, cotejando todas as características quanto ao atendimento pleno, parcial ou não atende, sendo:

Plenamente

Parcialmente
Não atende

Tabela 6 - Tabela comparativa de requisitos tecnológicos

Requisitos	Delinea	Microsoft	Cyberark	Google	Microfocus	Beyond Trust	Senha Segura
Prover mecanismos de segurança da informação							
Abranger todos os tipos de acessos e identidades							
Assegurar mecanismos de gerenciamento de privilégios elevados							
Prover registro de uso de privilégio e trilhas de auditoria							
Detectar e mitigar incidentes de forma mais eficaz através de mecanismos de inteligência artificial							
Ganhar agilidade e eficiência no tratamento de incidentes e na criação de relatórios							
Confiança zero (zero trust) para identidades							
Prover políticas para acessos adaptativos baseados em riscos e contextos conhecidos de uma autenticação							
Prover múltiplo fator de autenticação para diversos casos de uso com capacidade de interpretação de risco adaptativo							
Prover capacidade de acesso remoto a infraestrutura privilegiada e aplicações web de negócio sem VPN							
Prover ganhos operacionais para em recuperação de acessos e senhas							
Gravação e proteção de sessões de aplicações do tipo web de negócio de forma não intrusiva							
Possuir a capacidade de disparar gatilhos de gravação em vídeo relacionado a ações do usuário na estação de trabalho que estejam cumprindo atividades críticas							
Proteger identidades, credenciais e acessos de forma fim-a-fim							
Proteger silos de armazenamento de credenciais em servidores e estações							
Possuir capacidade de definição de políticas granulares para cada etapa da proteção de identidades							
Deve se comunicar com outras ferramentas de segurança e ampla capacidade de integrações							
Portal de Login Único para aplicações (SSO, Single Sign-On)							
Gestão de senhas de aplicações de negócio que não suportam Single Sign-On (login único)							
Diretório em nuvem IDP (Identity Provider)							
Prover licenciamento em modalidade simples, preferencialmente, por identidade							
Capacidade de gestão de senhas para usuários de negócio, com armazenamento em cofre de senhas							
Capacidade de controle de autenticação e autorização em nível granular para identidades não humanas							
Capacidade de proteção para chaves de API							
Capacidade de proteção de identidades não humanas em plataformas de conteinerização							
Disponibilizar pacote de desenvolvimento para proteção de identidades não humanas							
Capacidade de proteção de identidade não humanas para aplicações tracionais (não conteinerizadas ou não nativas em nuvem							

5.7.29. Agrupando o resultado da análise dos requisitos tecnológicos referente a cada uma das soluções, temos o seguinte quantitativo:

Tabela 7 - Tabela comparativa resumida

Requisitos	Delinea	Microsoft	Cyberark	Google	Micro Focus	Beyond Trust	Senha Segura
Plenamente atendido	7	8	27	6	7	7	5
Parcialmente atendido	8	13	0	11	8	8	10
Não atendido	12	6	0	10	12	12	12

5.8. Em paralelo a análise dos requisitos tecnológicos foi verificado o modelo de licenciamento das soluções, nesse ponto foram identificados as seguintes opções:

- Aquisição de licenças perpétuas, serviços agregados e serviços técnicos especializados; e

- Subscrição da solução e serviços técnicos especializados.

5.8.1. Sobre os modelos apresentados, realizamos a análise conforme tabela abaixo:

Tabela 8 - Tabela comparativa de modelos de licenciamento

Modelo	Análise
Perpétuo	1. Exige um alto desembolso financeiro inicial 2. Obriga a contratação de serviços complementares 3. Gera dependência tecnológica 4. Alto risco de descontinuidade 5. Exige renovação anual de licenças
Subscrições	1. Pagamentos anuais, desembolso fracionado 2. Possibilidade de substituição da ferramenta a qualquer momento 3. Dispensa a necessidade de contratação de serviços complementares 4. Redução de riscos de interrupção

5.8.2. Durante análise comparativa do modelo de licenciamento das soluções, identificamos uma convergência dos fabricantes dos softwares de gestão de identidades e acessos, alternando do modelo de licenciamento perpétuo, com contratos adjacentes de manutenção, suporte e garantia para modelo de licenciamento de subscrição de licenças.

Tabela 9 - Modelo de licenciamento das soluções analisadas

Id	Soluções	Modelo de Licenciamento
1	Delinea	Subscrição da solução e serviços técnicos especializados
2	Microsoft	Subscrição da solução e serviços técnicos especializados
3	Cyberark	Subscrição da solução e serviços técnicos especializados
4	Google	Subscrição da solução e serviços técnicos especializados
5	Micro Focus	Subscrição da solução e serviços técnicos especializados
6	Beyond Trust	Subscrição da solução e serviços técnicos especializados
7	Senha Segura	Subscrição da solução e serviços técnicos especializados

6. MODELOS DE PRESTAÇÃO DE SERVIÇOS TÉCNICOS ESPECIALIZADOS

6.1. Os serviços técnicos especializados se mostraram necessários para a garantia da efetiva implantação e continuidade da utilização da solução adquirida.

6.2. A CONTRATADA deverá suportar operacionalmente a solução, disponibilizando pelo menos um profissional para até 3.000 mil subscrições de usuários finais contratadas conforme perfil de Analista de Segurança descrito abaixo.

6.3. Os serviços deverão ser executados de segunda a sexta, das 08:00 as 18:00, ou seja, em horário comercial.

6.4. Os serviços deverão ser executados nas dependências da CONTRATADA a qual deverá disponibilizar toda a infraestrutura física e tecnológica para a execução dos serviços, não havendo dedicação de mão de obra exclusiva.

6.5. Até o dia 5 (cinco) do mês subsequente à realização do serviços a CONTRATADA deverá apresentar um relatório de atividades referente à execução dos serviços, o qual servirá de base para a fiscalização atestar e efetuar o pagamento.

6.6. Descrição dos serviços técnicos especializados – operação assistida

6.7. As atividades de operação assistida objetivam otimizar a utilização dos produtos adquiridos, o desenvolvimento ou aperfeiçoamento de competências, além da sustentação da operação como um todo. Estas atividades são continuadas e devem permanecer ativas durante toda a execução do contrato.

6.8. As atividades compreendem toda a sustentação do ambiente, interação com as equipes multidisciplinares, execução de revisões de configurações e verificações proativas do ambiente.

6.9. Buscam, ainda, contribuir em projetos técnicos e desenvolvimento de documentações, sessões de orientações das equipes do cliente e apoio na resolução de incidentes de segurança;

6.10. Os serviços técnicos especializados se mostraram necessários devido a complexidade tecnológica que envolve o objeto e a necessária especialização para atender as demandas e seus produtos resultantes.

6.11. Perfil do Profissional da Operação Assistida

6.11.1. A seguir são definidos os requisitos mínimos obrigatórios para o perfil profissional a ser alocado na execução dos serviços:

6.11.2. Analista de segurança da informação

6.11.2.1. Profissional com graduação ou pós-graduação na área de Tecnologia da Informação.

6.11.2.2. O profissional deve ter no mínimo 2 anos de experiência na área de Segurança da informação.

6.11.2.3. O profissional deverá apresentar certificado oficial do fabricante Cyberark Certified Delivery Engineer (CDE).

6.11.2.4. Este profissional especializado é necessário para execução de tarefas relacionada a tecnologia de forma abrangente, sendo responsável por cuidar de forma operacional das demandas de sustentação do ambiente, além da interação com as equipes multidisciplinares, execução de revisões de configurações, verificações proativas do ambiente e contribuir em projetos técnicos e desenvolvimento de documentações.

7. SERVIÇOS DE SUPORTE TÉCNICO E GARANTIA DO FABRICANTE

7.1. O FABRICANTE deverá fornecer o serviço de garantia e suporte para solução durante o período de vigência do contrato contados a partir da emissão do Termo de Recebimento Definitivo da implantação para garantia de atualizações de versão e acionamento em nível de resolução de problemas pelo próprio fabricante, e apoiar o CONTRATANTE na resolução de incidentes junto ao fabricante;

7.2. O atendimento para identificação e correção de falhas ou inconsistências detectadas nos produtos da solução de forma a garantir o perfeito funcionamento e utilização dos softwares, de acordo com o estabelecido nos manuais que acompanham o produto;

7.3. A FABRICANTE deverá fornecer correções de bugs ou alternativa para corrigir defeitos nos softwares indicados que façam com que eles não operem de acordo com a documentação publicada para os usuários dos softwares;

7.4. Os serviços de suporte técnico deverão ser prestados em escala 24 (vinte e quatro) horas por dia, 7 (sete) dias da semana, durante o período de vigência do contrato, em português brasileiro;

7.5. Para operacionalização do suporte técnico, o FABRICANTE deverá disponibilizar uma área em sítio da Web voltada para a abertura dos chamados técnicos. Como forma de atendimento paliativo a comunicação poderá ser através de uma central de atendimento telefônica 0800 e/ou endereços de correio eletrônico (e-mail);

7.6. Todo e qualquer chamado feito pela CONTRATANTE deverá ser registrado em sistema informatizado para acompanhamento e controle de sua execução;

7.7. A FABRICANTE será responsável pelo fornecimento de informações sobre novas versões dos sistemas, bem como sua respectiva documentação técnica;

7.8. Todos os prazos para atendimento da garantia começarão a ser contados a partir da abertura o chamado independentemente de este ter sido feito via telefone, e-mail ou site da FABRICANTE;

7.9. O serviço de suporte técnico e garantia deve incluir o acompanhamento do fabricante durante todo o período do contrato com objetivo de prestar consultoria especializada na solução.

7.10. Níveis de serviços

7.10.1. Os serviços de suporte técnico deverão ser executados conforme níveis de serviços abaixo descritos:

Tabela 10 - Níveis de criticidade

Criticidade	**Descrição**	**Prazo para início de atendimento**
Severidade 1 (Alta)	Sistema parado ou produto inoperante com impacto nas operações críticas de negócio. **Exemplos:** Servidor de produção ou outro sistema inicial está inativo. Parte substancial dos dados essenciais corre risco de perda ou corrupção. Operações relacionadas ao negócio foram afetadas, falha que compromete a integridade geral do sistema ou dos dados.	Em até 2 horas
Severidade 2 (Média/Alta)	Alto impacto no ambiente de produção ou grande restrição de funcionalidade. **Exemplo:** Ocorreu um problema no qual um recurso importante foi gravemente danificado. As operações podem continuar de forma limitada, embora a produtividade a longo prazo possa ser afetada negativamente.	Em até 4 horas
Severidade 3 (Média)	O defeito não gera impacto ao negócio. **Exemplo:** Ocorreu um erro que causou impacto negativo limitado nas operações.	Em até 6 horas uteis
Severidade 4 (Baixa)	O problema é pequeno, ou de documentação. **Exemplos:** O problema não afetou as operações da contratante negativamente. Encaminhamento de solicitações e ou sugestões para novos recursos ou aprimoramento do software licenciado.	Em até 12 horas uteis

8. ANÁLISE E IDENTIFICAÇÃO DE SOLUÇÕES VIÁVEIS DE MERCADO

8.1. Considerando a análise realizada no tópico 5 - ANÁLISE DO MERCADO FORNECEDOR, a equipe de planejamento da contratação entende que a solução da fornecedora **Cyberark** mediante o fornecimento de subscrições e serviços técnicos especializados, conforme comumente é contratado no âmbito dos órgãos públicos, é a única solução que atende em sua completude os requisitos levantados nesse estudo técnico preliminar da contratação.

8.2. Conforme demonstrado na Tabela 6 - Tabela comparativa de requisitos tecnológicos e Tabela 7 - Tabela comparativa resumida, diversas soluções atendem itens específicos dos requisitos tecnológicos definidos neste estudo, contudo isso implicaria na realização de diversos contratos o que no entendimento da equipe de planejamento da contratação não é vantajoso tecnicamente.

8.3. Um cenário envolvendo mais de uma ferramenta pode resultar em falhas de funcionamento, risco à vulnerabilidade e segurança, além de dificultar o acompanhamento, fiscalização e gerenciamento de mais de um fornecedor.

8.4. Desta forma, temos que uma divisão em mais de uma solução implicaria em perda de garantia de integridade referencial de dados caso duas ferramentas de desenvolvedores distintos começassem a se intercomunicar, alterando concomitantemente importantes bases de dados que seriam distintas. Haveria sério entrave técnico, tornando mais onerosa e menos confiável a contratação, ademais em uma auditoria ou investigação de evento dificultaria tanto a identificação da causa como do responsável pela eventual perda de dados ou de outros aspectos relacionados a segurança.

8.5. No decorrer da elaboração desse estudo técnico, nota-se que que o mercado está passando para uma convergência de necessidades, aliando soluções de acesso privilegiado e segurança para identidades sob um mesmo conceito, denominado gerenciamento de acesso provendo segurança para identidades. Nesse contexto, concluímos que as iniciativas isoladas nessas frentes devem convergir em uma necessidade única, considerando soluções que possuem a maior abrangência em proteção de identidades fim-a-fim, pensando não somente no cenário atual, bem como nos cenários futuros.

8.6. Outro aspecto relevante é a capacidade de integrações da solução com o portfólio de soluções já existentes, desta forma viabilizando ganhos imediatos após a implementação da solução promovendo aumento de segurança, confiabilidade e auditoria, além da capacidade de resposta em caso de incidentes.

8.7. Outro ponto relevante é a manifestação do Gartner no documento de 2021, intitulado "*Magic Quadrant for Acess Management* - Quadrante Mágico para Gerenciamento de Acessos" , cujo texto transcrevemos abaixo:

Um fabricante de Access Management deve prover minimante as seguintes capacidades:

- Administração de identidade internas e externas, incluindo serviços de sincronização de diretórios
- *Self-service* de usuários, incluindo para interface para usuários finais e de administração com registro, gerenciamento de senhas, gerenciamento de perfil e delegação de administração
- Catálogo de aplicações da sua força de trabalho com login único (SSO)
- Autorização e acesso adaptativo com suporte para protocolos modernos como oAuth 2.0
- Gerenciamento de sessões
- Métodos de autenticação dos usuários incluindo múltiplo fator de autenticação e login único (SSO)

- Integração com políticas de traga seu próprio dispositivo (BYOD) e uso de identidades publicas como contas de média social para acesso.
- API de controle de acesso para controlar autenticação e autorização para APIs alvo
- Suportar aplicações padrões, incluindo capacidades para acesso rápido, SSO e MFA para SaaS e Aplicações Web através de protocolos modernos como SAML e OpenID Connect
- Suportar aplicações customizadas, incluindo capacidade para acesso rápido, SSO e MFA para aplicações web legadas que não suportam protocolos de SSO.
- Capacidade analítica, incluindo relatórios, logs e informações analíticas de identidades sobre administração e acesso em tempo de execução.

8.8. É importante frisar que a solução identificada neste estudo como solução viável para o Ministério da Economia é a única que atende todos os requisitos elencandos acima. considerando a utilização de uma única plataforma.

8.9. O atendimento dos requisitos desse estudo técnico mediante a utilização de uma solução proveniente de um único fornecedor permitirá a utilização de uma única plataforma para a gestão de identidades e acessos, economizando-se com manutenção, treinamentos, dentre outros gastos.

8.10. Por fim, cabe ressaltar que a solução da Cyberark para Gestão de Identidades e Acessos possui a melhor colocação no documento "*Magic Quadrant for Acess Management* - Quadrante Mágico para Gerenciamento de Acessos", publicado em 2021:

Source: Gartner (July 2021)

8.11. Segue abaixo a análise referente aos aspectos previstos na IN SGD-ME n. 01/2019 que devem ser avaliados em uma contratação de TIC.

Tabela 11 - Análise conforme IN n.º 01/2019

Requisito	Solução	Sim	Não	Não se aplica
A Solução encontra-se implantada em outro órgão ou entidade da Administração Pública?	Solução - Cyberark	X		
A Solução está disponível no Portal do Software Público Brasileiro? (quando se tratar de software)	Solução - Cyberark		X	
A Solução é composta por software livre ou software público? (quando se tratar de software)	Solução - Cyberark		X	
A Solução é aderente às políticas, premissas e especificações técnicas definidas pelos Padrões de governo ePing, eMag, ePWG?	Solução - Cyberark			X
A Solução é aderente às regulamentações da ICP-Brasil? (quando houver necessidade de certificação digital)	Solução - Cyberark			X
A Solução é aderente às orientações, premissas e especificações técnicas e funcionais do e-ARQ Brasil? (quando o objetivo da solução abranger documentos arquivísticos)	Solução - Cyberark			X

8.12. Complementamos o quadro acima com as seguintes informações acerca da solução considerada viável para o Ministério da Economia:

8.12.1. Necessidade de adequação do ambiente do órgão ou entidade para viabilizar a execução contratual.

8.12.1.1. Não é necessário nenhuma adequação no ambiente do Ministério da Economia.

8.12.2. Possibilidade de aquisição na forma de bens ou contratação como serviço.

8.12.2.1. Foi definido pela equipe de planejamento da contratação que a aquisição ocorrerá mediante contratação como serviço desonerando o Ministério da Economia da necessidade de aquisição de software com licenciamento perpétuo; a contratação de subscrição cresceu exponencialmente e é considerada uma boa prática de mercado, conforme identificamos mediante a Tabela 8 - Tabela comparativa de modelos de licenciamento e Tabela 9 - Modelo de licenciamento das soluções analisadas, destaca-se como benefícios as atualizações(correção de bugs e falhas de segurança), upgrades (novas versões) e suporte técnico.

8.12.2.2. Os serviços a serem contratados enquadram-se nos pressupostos do Decreto n.° 9.507/2018 constituindo-se serviços auxiliares, instrumentais ou acessórios de que tratam os incisos do caput que poderão ser executados de forma indireta, vedada a transferência de responsabilidade para a realização de atos administrativos ou a tomada de decisão para o contratado e não inerentes às categorias funcionais abrangidas por seu respectivo plano de cargos.

8.12.3. Parcelamento ou não da solução.

8.12.3.1. Conforme já mencionado nos parágrafos 8.3, 8.4, 8.5 e 8.6, a contratação de licenças de um mesmo fornecedor é o cenário tecnicamente mais viável, desta forma a possibilidade de parcelamento da solução, consistiria em:

- Contratação de subscrição de software; e
- Contratação de serviço de operação assistida

8.12.3.2. A possibilidade de divisão ou não dos componentes de uma solução em itens para serem licitados em separado está relacionada com o grau de interdependência técnica entre os seus componentes, o que não é possível no caso da solução avaliada por este estudo técnico.

8.12.3.3. A presente contratação é uma a solução integrada que perfaz um conjunto de software e serviços que se interoperam para o atendimento das necessidades apontadas e justificadas neste documento. Trata-se de um conjunto de softwares e serviços integrando um único objeto com um alto grau de especialização, não sendo viável tecnicamente a sua separação.

8.12.3.4. Caso, em uma situação hipotética o Ministério da Economia optasse por parcelar a presente solução (cujo parcelamento é considerado inviável), poderia causar grandes prejuízos a instituição, uma vez que havendo alguma intercorrência em um dos contratos o órgão poderia ter a subscrição sem o serviço técnico especializado ou o cenário inverso, em ambos os casos o objetivo da contratação seria prejudicado.

8.12.3.5. O parcelamento das contratações de soluções de TI pelo Ministério da Economia é sempre ponderado em função do poder discricionário da Administração Pública, que lhe dá a prerrogativa de fazê-lo até o limite da coerência, da viabilidade técnica e da capacidade interna de gestão.

8.12.3.6. Neste caso, como já citado, o objeto em questão é uma solução concebida sob a forma de uma plataforma integrada tecnicamente indivisível uma vez que todos os componentes de softwares e serviços são intrínsecos à mesma solução, não sendo possível o seu desmembramento.

8.12.4. Diferentes Modelos de Prestação de Serviço

8.12.4.1. Conforme explicitado na Tabela 8 - Tabela comparativa de modelos de licenciamento, a contratação como serviço se mostrou mais vantajosa, nessa modalidade foi identificada apenas um modelo de prestação de serviço que é a contratação de subscrição

8.12.5. Diferentes Tipos de Soluções em Termos de Especificação, Composição ou Características dos Bens e Serviços Integrantes

8.12.5.1. Não foram identificados outros tipos de solução relevantes além do exposto neste Estudo Técnico Preliminar.

8.12.6. Ampliação ou Substituição da solução implantada

8.12.6.1. Atualmente o Ministério da Economia não possui uma solução implantada que contemple o escopo dessa contratação, não cabendo ampliação ou substituição de solução.

8.12.7. Catálogos de Soluções de TIC com Condições Padronizadas

8.12.7.1. Ao analisar o Catálogo de Soluções de TIC com Condições Padronizadas (atualizado em 26/05/2022) "https://www.gov.br/governodigital/pt-br/contratacoes/catalogo-de-solucoes-de-tic, não foi identificado nenhum catálogo ativo com a fornecedora Cyberark ou qualquer outra solução analisada nesse ETPC.

8.13.

9. REGISTRO DE SOLUÇÕES CONSIDERADAS INVIÁVEIS NO MOMENTO DA REALIZAÇÃO DO ESTUDO

9.1. Considerando a análise realizada no tópico 5 - ANÁLISE DO MERCADO FORNECEDOR, as soluções Delinea, Microsoft, Google, Micro Focus, Beyond Trust e Senha Segura são consideradas inviáveis em função de não atender todos os requisitos tecnológicos definidos nesse estudo técnico.

10. ANÁLISE COMPARATIVA DE CUSTO TOTAL (TCO)

10.1. A equipe de planejamento da contratação não realizou a análise comparativa de custos em virtude do estudo técnico preliminar da contratação identificar somente uma solução/cenário viável, conforme disciplina o inciso III do art. 11 da IN SGD/ME nº 01/2019:

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

11. DESCRIÇÃO DA SOLUÇÃO DE TIC A SER CONTRATADA

11.1. Diante da análise de mercado, alinhando-se aos objetivos de negócio e ao perfil de demanda registrada, foi constatado que o fabricante Cyberark através de subscrições e serviços técnicos especializados, conforme comumente contratado no âmbito de órgãos públicos, atende integralmente a necessidade do ME.

11.2. A escolha da fabricante Cyberark é fundamentada por sua maior capacidade de atendimento dos itens especificados nos requisitos tecnológico que são julgados como essenciais para atendimento das necessidades do ME. O atendimento dos objetivos e resultados pretendidos somente é possível por meio do atendimento pleno aos requisitos mínimos necessários, sendo a Cyberark a única fabricante com total capacidade de atendimento aos requisitos. Abaixo destacamos os principais requisitos tecnológicos:

- Proteger identidades, credenciais e acessos de forma fim-a-fim
- Confiança zero (zero trust) para identidades
- Gravação e proteção de sessões de aplicações do tipo web de negócio de forma não intrusiva
- Gestão de senhas de aplicações de negócio que não suportam Single Sign-On (login único)
- Prover registro de uso de privilégio e trilhas de auditoria
- Ganhar agilidade e eficiência no tratamento de incidentes e na criação de relatórios
- Prover políticas para acessos adaptativos baseados em riscos e contextos conhecidos de uma autenticação

11.3. A justificativa do cenário escolhido é resultante de todas as análises realizadas no âmbito deste estudo. A Lei Geral de Licitações - 8.666/1993, em seu § 5°do art. 7°, prevê que nos casos em que for tecnicamente justificável, é possível construir o objeto indicando características e especificações exclusivas.

11.4. Dsta forma, entemos que Essa questão interfere também no funcionamento de forma integrada da solução, pois um cenário envolvendo mais de uma ferramenta pode resultar e falhas de funcionamento, risco à vulnerabilidade e segurança, além de dificultar o acompanhamento, fiscalização e gerenciamento de mais de um fornecedor.

11.5. Em face do exposto, entendemos que a contratação de subscrições de solução tecnológica para gerenciamento de identidades e acesso do fabricante Cyberark, por 24 meses, com suporte, garantia, fornecimento de serviços técnicos especializados e treinamento, conforme quantidade estabelecida na tabela x.

Tabela 11 - Estimativa da Demanda (Descrição da solução de TIC a ser contratada).

Item	Part Number	Descrição	Unidade de medida	Quantidade	Valor Unitário	Valor Anual	Valor Total
1	-	Segurança para Identidades	usuários	-			
1.1	IAMFA-B2E-USER-SASS	Segurança para identidades – Proteção de acesso do usuário final adaptado ao risco comportamental	usuários	1000			
1.2	WORKFORCE-ENTERPRISE-USER-SAAS	Segurança para identidades – Monitoramento e proteção da sessão do usuário final	usuários	1000			
1.3	IWPM-B2E-USER-SAAS	Segurança para identidades – Proteção e gestão de credenciais do usuário final em browser	usuários	1000			
1.4	PRIV-STANDARD-USER-SUBS	Segurança para identidades – Proteção e monitoramento de ameaças ao usuário da TI	usuários	200			
1.5	EPM-TARGET-SVR-SAAS	Segurança para identidades – Proteção e monitoramento de ameaças a credenciais em servidores	servidores	100			
1.6	EPM-TARGET-WRK-SAAS	Segurança para identidades – Proteção e monitoramento de ameaças a credenciais em estações de trabalho	Estações de Trabalho	1000			
1.7	APP-DYN-REGION-T1-SUBS	Segurança para identidades – Proteção de secrets em aplicações nativas em nuvem/contêiner	Cluster	2			
1.8	APP-STATIC-SUBS	Segurança para identidades – Proteção de secrets em aplicações tradicionais/legado	Aplicações	100			
1.9		Serviços Técnicos Especializados – Operação Assistida (até 3.000 subscrições)	Mensal	1			
1.10		Treinamento específico para utilização da solução tecnológica	Turma	1			

12. ANÁLISE DA INTENÇÃO DE REGISTRO DE PREÇO

13. ESTRATÉGIA DA CONTRATAÇÃO

13.1. A presente seção descreve os estudos e justificativas que fundamentaram decisões na modelagem de diferentes aspectos e condições do Termo de Referência.

13.2. Vigência e modalidade da licitação

13.2.1. Por se tratarem de serviços comuns, o objeto da presente licitação deve ser licitado na modalidade PREGÃO ELETRÔNICO, com adjudicação pelo valor global.

13.2.2. O contrato deverá ter vigência de 24 meses podendo ser prorrogado por igual período conforme estabelece o art.57º da lei 8.666.93.

13.3. Justificativa para vigência superior a 12 meses

13.3.1. O artigo 57 da Lei Federal nº 8.666/93 disciplina a duração dos contratos administrativos, bem como as possíveis hipóteses de prorrogação de seu prazo de vigência.

> *Art. 57. A duração dos contratos regidos por esta Lei ficará adstrita à vigência dos respectivos créditos orçamentários, exceto quanto aos relativos:*
> *I - aos projetos cujos produtos estejam contemplados nas metas estabelecidas no Plano Plurianual, os quais poderão ser prorrogados se houver interesse da Administração e desde que isso tenha sido previsto no ato convocatório;*
> *II - à prestação de serviços a serem executados de forma contínua, que poderão ter a sua duração prorrogada por iguais e sucessivos períodos com vistas à obtenção de preços e condições mais vantajosas para a administração, limitada a sessenta meses;*
> *III - (Vetado).*
> *IV - ao aluguel de equipamentos e à utilização de programas de informática, podendo a duração estender-se pelo prazo de até 48 (quarenta e oito) meses após o início da vigência do contrato.*
> *V - às hipóteses previstas nos incisos IX, XIX, XXVIII e XXXI do art. 24, cujos contratos poderão ter vigência por até 120 (cento e vinte) meses, caso haja interesse da administração.*

13.3.2. A regra estabelecida pelo artigo 57 se mostra bem clara: a duração dos contratos, em regra, deve se restringir à vigência dos respectivos créditos orçamentários, restando vedado o contrato administrativo com prazo de vigência indeterminado.

13.3.3. Não existe vedação nenhuma quanto a definição da vigência contratual no Art. 57 da Lei 8.666/1993 estar acima de 12 meses. Pelo contrário, ele autoriza que um contrato de serviço continuado seja vigente por até 60 meses.

13.3.4. Quanto a adoção de prazo de vigência da contratação ser de 24 (vinte e quatro) meses, prorrogável até o limite de 60 (sessenta) meses, esclarecermos que um período de vigência contratual ampliado contribui para que a contratação em tela possa ser considerada mais atrativa pelo mercado por meio de uma maior diluição dos custos com depreciação e manutenção dos equipamentos ou investimentos, o que pode, inclusive, ter impactos sobre o preço final proposto pela licitante vencedora do certame, favorecendo a Administração em termos de economicidade e ampliação da competitividade.

13.3.5. Seguindo esta lógica, a jurisprudência do TCU sustenta a possibilidade da fixação do prazo de vigência estendido com a finalidade de obter preços e condições mais vantajosos para a Administração, como o Acórdão 3.320/2013-Segunda Câmara:

"O prazo de vigência de contratos de serviços contínuos deve ser estabelecido considerando-se as circunstâncias de forma objetiva, fazendo-se registrar no processo próprio o modo como interferem na decisão e quais suas consequências. Tal registro é especialmente importante quando se fizer necessário prazo inicial superior aos doze meses entendidos como regra pelo TCU. Há necessidade de se demonstrar o benefício decorrente do prazo estabelecido (Acórdão 3320/2013-Segunda Câmara)."

13.3.5.1. No caso em questão a contratação com previsibilidade de vigência acima dos 12 meses é econômica e tecnicamente mais vantajosa para a Administração, conforme vantagens elencadas abaixo:

- Evitar o acionamento da máquina pública a cada prorrogação;
- Evitar gastos administrativos nessas autuações a cada 12 meses;
- Possibilidade de diluir investimentos ou de custos por parte do particular (amortização), facilitando o dimensionamento do investimento, afetando significativamente os valores mensais do contrato;
- Atender às características específicas da contratação;
- Reduzir a complexidade de implementação da solução para um período de vigência maior;
- Alterar a cultura diária dos usuários da instituição envolvendo alteração de processos e curva de aprendizado, que nos casos de 12 meses gera um impacto ainda mais oneroso;
- Aumento da capacidade de segurança através da integração com as demais soluções da instituição que irão demandar maior esforço, pois perpetuando por um período maior, reduz riscos elevados à segurança; e
- Ganhos de economicidade.

13.4. Estimativa da Demanda

13.4.1. A estimativa de demanda será realizada após consulta a todos os órgãos integrantes do SISP.

13.4.2. Não existe, neste primeiro momento, possibilidade de definir com elevado grau de precisão, qual o quantitativo exato a ser contratado. De qualquer forma, como o objetivo desse projeto é a disponibilização da solução para os integrantes do SISP, sugere-se a adoção do sistema de registro de preços para satisfazer a presente demanda.

13.4.3. A adoção do sistema de registro de preço justifica-se pela forma de aquisição dos bens e serviços, que terá previsão de entregas parceladas, segundo a nossa necessidade, conforme as disponibilidades orçamentárias, uma vez que segundo Decreto nº 7.892/2013:

"Art. 2º Será adotado, preferencialmente, o SRP nas seguintes hipóteses:
I - quando, pelas características do bem ou serviço, houver necessidade de contratações frequentes;
II - quando for mais conveniente a aquisição de bens com previsão de entregas parceladas ou contratação de serviços necessários à Administração para o desempenho de suas atribuições;
[...]
IV - quando pela natureza do objeto não for possível definir previamente o quantitativo a ser demandado pela Administração."

14. ESTIMATIVA DE CUSTO TOTAL DA CONTRATAÇÃO

14.1. A estimativa de custos da contratação considerou a contratação de 100% do volume projetado no Item 4 - ESTIMATIVA DA DEMANDA - QUANTIDADE DE BENS E SERVIÇOS. Dessa forma, tem-se a seguinte estimativa de custos:

Tabela 12 - Estimativa de custo da contratação

ITEM	PART NUMBER	DESCRIÇÃO	MEDIDA	QUANTIDADE	VALOR UNITÁRIO	VALOR ANUAL	VAI
1	IAMFA-B2E-USER-SAAS	Proteção de acesso do usuário final adaptado ao risco comportamental	Usuários	1.000	R$ 290,93	R$ 290.930,00	R$
2	WORKFORCE-ENTERPRISE-USER-SAAS	Monitoramento e proteção da sessão do usuário final	Usuários	1.000	1.390,50	R$ 1.390.500,00	R$
3	IWPM-B2E-USER-SAAS	Proteção e gestão de credenciais do usuário final em browser	Usuários	1.000	R$ 289,00	R$ 289.000,00	R$
4	PRIV-STANDARD-USER-SUBS	Proteção e monitoramento de ameaças ao usuário da TI	Usuários	200	R$ 5.005,40	R$ 1.001.080,00	R$
5	EPM-TARGET-SVR-SAAS	Proteção e monitoramento de ameaças a credenciais em servidores	Servidores	100	R$ 665,90	R$ 66.590,00	R$
6	EPM-TARGET-WRK-SAAS	Proteção e monitoramento de ameaças a credenciais em estações de trabalho	Estações de trabalho	1.000	R$ 249,47	R$ 249.470,00	R$
7	APP-DYN-REGION-T1-SUBS	Proteção de secrets em aplicações nativas em nuvem/contêiner	Clusters	2	R$ 299.650,50	R$ 599.301,00	R$
8	APP-STATIC-SUBS	Proteção de secrets em aplicações tradicionais/legado	Aplicações	100	R4 4.180,80	R$ 418.080,00	R$
9	N/A	Serviços Técnicos Especializados – Operação Assistida	Mensal	1	R$ 59.200,00	R$ 710.400,00	R$

10	N/A	Treinamento específico para utilização da solução tecnológica	Turma	1	R$ 59.400,00	R$ 59.400,00	R$ 1
					R$ 430.322,50	R$ 5.074.751,00	**R$** 1

14.2. Conforme Tabela 12 - Estimativa de custo da contratação, o valor de referência total para esta contratação é de **R$ 10.149.502,00 (Dez milhões, cento e quarenta e nove mil, quinhentos e dois reais).**

14.3. Esta estimativa será melhor detalhada após a finalização da Intenção de Registro de Preço (IRP). Após isso, será realizada pesquisa de preços e a estimativa será consolida com os volumes finais e os valores unitários na versão final do Termo de Referência.

15. DO MODO DE DISPUTA DO PREGÃO

15.1. A presente seção define e justifica o modo de disputa a ser adotado no Pregão, em atenção ao Decreto 10.024, de 20 de setembro de 2019. Inicialmente, destaca-se que o referido Decreto introduziu a figura do modo de disputa a ser adotado no pregão, podendo ser aberto (descrito no art. 32 desse Decreto) ou aberto e fechado (descrito no art. 33 desse Decreto).

15.2. Os modos de disputa definem como se dará o envio de lances no pregão eletrônico. No modo aberto, os licitantes apresentarão lances públicos e sucessivos, com prorrogações, conforme o critério de julgamento adotado no edital. Já no modo Aberto e Fechado, os licitantes apresentarão lances públicos e sucessivos, com lance final fechado.

15.3. Para se definir o modo de disputa mais apropriado para a presente contratação, observou-se as seguintes características inerentes à Teoria do Leilões, conforme descrita em vasta bibliografia relacionada a essa Teoria, em específico na obra de Paul Klemperer, "What Really Matters in Auction Design", publicação realizada no Journal of Economic Perspectives -Volume 16, Number 1 páginas 169–189 (Disponível neste link):

a. Propensão à colusão; e
b. Prevenção ao comportamento predatório.

15.4. Ressalta-se, inicialmente, que cada modo de disputa possui características específicas que os tornam mais ou menos vantajosos a depender das condições relacionadas à estrutura do mercado, à natureza do objeto e ao arranjo local de fornecimento dos bens e serviços. Note que a vantajosidade a ser perseguida relaciona-se a maior quantidade de incentivos que o modo de disputa é capaz de fornecer para que o desenho do mecanismos de seleção do fornecedor possibilite o alcance do melhor resultado para a administração, mitigando-se o risco da ocorrência de disfunções entre os agentes participantes que afetem a ampla concorrência e o melhor preço à administração pública.

15.5. Sobre a propensão à colusão, verificou-se no presente estudo que a solução pertence a um único fabricante, consequentemente o setor de venda para o governo desse tipo de produto acompanha um nível de concentração elevado. Em mercados altamente concentrados, a probabilidade da ocorrência da colusão explícita ou tácita é maior. Nesse sentido, a utilização de uma fase de lances selados, segundo Klemperer, é mais apropriada para mitigar o risco de colusão, principalmente porque evita a chamada sinalização de propostas (Bid Signaling).

15.5.1. Outro aspecto a ser considerado é o grau de padronização ou homogeneização do produto objeto da contratação. Isso porque produtos diversificados permitem que diferentes fornecedores assumam um comportamento prejudicial à concorrência, denominado de comportamento predatório, ou seja, assumam lances próximos à inexequibilidade com o intuito de criar artificialmente barreiras à entrada de novos participantes. Por se tratar de uma solução nomeada, o modelo de disputa mais adequado é aquele que possua uma fase de propostas seladas, uma vez que o risco de ocorrência da chamada maldição do fornecedor ou de eventual risco moral é menor do que em casos de produtos muitos diversificados.

15.5.2. Pelo exposto, e considerando ainda o número não expressivo de prestadores dos serviços em vendas para o governo devido ao grau de concentração, o modo de disputa do Pregão deverá ser ABERTO E FECHADO, conforme rito estabelecido no artigo 33 do Decreto nº 10.024, de 2019, que regulamenta a licitação, na modalidade de pregão, na forma eletrônica, para a aquisição de bens e a contratação de serviços comuns de engenharia, e dispõe sobre o uso da dispensa eletrônica, no âmbito da Administração Pública Federal.

16. DECLARAÇÃO DE VIABILIDADE DA CONTRATAÇÃO

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

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

- Economia no valor da licitação em função do ganho de escala e na forma agrupada de contratação;
- Eficiência com a redução do custo administrativo em função do agrupamento de itens em uma solução única;
- Efetividade com a padronização dos itens previstos, subscrições e aumento da qualidade das especificações técnicas; e
- . Eficácia com o atendimento das necessidades de diversas instituições referente a solução de Gerenciamento de Identidades e Acessos.

16.3. Além disso, frisa-se que a presente contratação 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.

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

17. APROVAÇÃO E ASSINATURA

17.1. Equipe de Planejamento da Contratação instituída pelo Documento de Oficialização de Demanda (SEI-ME 24189586) e Despacho SGES-CNTRAL-CGTIC (SEI-ME 24473275) .

17.2. Estudo Técnico Preliminar aprovado e assinado pelos Integrantes Técnicos e Requisitantes e pela autoridade máxima da área de TIC, conforme o § 2º do Art. 11 da IN SGD-ME nº 01, de 2019.

Documento assinado eletronicamente

FÁBIO MORETH MARIANO

Integrante Técnico

Matrícula/SIAPE: 1793489

Documento assinado eletronicamente

GUSTAVO NASCIMENTO FRADIQUE

Integrante Requisitante

Matrícula/SIAPE: 1277598

Aprovo.

Documento assinado eletronicamente

LARA BRAINER MAGALHÃES TORRES DE OLIVEIRA

Diretora

Matrícula/SIAPE 1503583