

Estudo Técnico Preliminar 10/2025

1. Informações Básicas

Número do processo: 23034.039474/2024-35

2. Descrição da necessidade

. Descrição da necessidade

2.1 Contratação de subscrição de solução de segurança da informação para proteção de ameaças online, bem como da gestão de acesso remoto a rede do FNDE e de acessos privilegiados a infraestrutura crítica de processamento de dados por doze (12) meses, incluindo serviços de implantação, garantia de suporte e atualização.

2.2 Contextualização

2.2.1 O FNDE, autarquia Federal vinculada ao Ministério da Educação (MEC), instituída pela Lei nº 5.537, de 21 de novembro de 1968, com sede e foro em Brasília – DF, tem por finalidade captar recursos financeiros e canalizá-los para o financiamento de projetos educacionais nas áreas de ensino, pesquisa, alimentação escolar, material escolar e bolsas de estudo em observância às diretrizes estabelecidas pelo MEC. Sua missão é prover recursos e executar ações para o desenvolvimento da educação de qualidade a todos os brasileiros, missão essa, assentada na transparência, na cidadania e no controle social, na inclusão social, na avaliação de resultados e na excelência na gestão.

2.2.2 Os principais programas de governo executados sob a responsabilidade do FNDE, têm sua operação suportada por soluções de TI cujo objetivo é promover a liberação de recursos aos diversos programas e projetos vinculados às ações educacionais, a exemplo de:

- Programa Nacional de Alimentação Escolar (PNAE);
- Programa Nacional do Livro Didático (PNLD);
- Programa Dinheiro Direto na Escola (PDDE);
- Programa Nacional de Apoio ao Transporte do Escolar (PNATE);
- Programa Caminho da Escola (Transporte Escolar);
- Programa Nacional de Reestruturação e Aquisição de Equipamentos para a Rede Escolar e Pública da Educação Infantil (PROINFÂNCIA);
- Programa de Ações Articuladas (PAR);
- Programa Brasil Alfabetizado;
- Educação de Jovens e Adultos;
- Educação Especial;
- Ensino em Áreas Remanescentes de Quilombolas;
- Educação Escolar Indígena;
- Financiamento Estudantil – FIES, dentre outros

2.2.3 Esse cenário requisita que a Diretoria de Tecnologia e Inovação - DIRTi disponha e mantenha soluções especializadas em Tecnologia da Informação e principalmente de segurança garantindo o atendimento das necessidades informacionais dos programas por meio das soluções tecnológicas,

sem as quais seria impossível atingir os compromissos institucionais de prover serviços públicos à sociedade.

2.2.4 Através da Portaria SGD/MGI Nº 852, de 28 de março de 2023 a Secretaria do Governo Digital instituiu o **Programa de Privacidade e Segurança da Informação (PPSI)**, sob a Diretoria de Privacidade e Segurança da Informação. O PPSI é caracterizado como um conjunto de projetos e processos de adequação nas áreas de privacidade e segurança da informação e tem como valores: a **maturidade**; a **resiliência**; a **efetividade**; a **colaboração** e a **inteligência**.

2.2.5 O PPSI implementa ações de Privacidade e Segurança da Informação no âmbito dos órgãos e entidades da administração pública federal direta, autárquica e fundacional, que possuem unidades que compõem o Sistema de Administração dos Recursos de Tecnologia da Informação (SISP), conforme art. 3º do Decreto nº 7.579, de 11 de outubro de 2011.

2.2.6 Os controles, segundo o PPSI, é orientado principalmente a dimensão Privacidade e Segurança. Na dimensão Segurança os controles são conjuntos prescritivos relacionado as práticas recomendadas de segurança cibernética e ações defensivas com finalidade de ajudar a prevenir os ataques generalizados e perigosos, dando suporte à conformidade com o Decreto nº 10.222/2020 (Estratégia Nacional de Segurança Cibernética (E-CIBER)), Decreto nº 10.748/2021 (Rede Federal de Gestão de Incidentes Cibernéticos), Portaria GSI/PR nº 93/2021 (Glossário de Segurança da Informação), demais Instruções Normativas (INs) ou Normas Complementares (NCs) estabelecidas pelo GSI/PR bem como o CIS Controls V8 e NIST Cybersecurity Framework e ABNT NBR ISO/IEC séries 27000.

2.2.27 Na dimensão Segurança do PPSI a ênfase dos controles é voltado entre outras a gestão de contas, gestão do controle de acesso, gestão de registros de auditoria, proteções de e-mail e navegador web, defesas contra malware, gestão da infraestrutura de rede, monitoramento e defesa da rede, segurança de aplicações, etc.

2.2.8 Tendo em vista que o FNDE é um órgão seccional do SISP, a autarquia tem participado desde o início do PPSI nas avaliações para as adequações dos controles de segurança conforme os processos do programa definidos pelo SGD/MGI.

2.2.9 Em 2024 o FNDE participou no Programa Nacional de Proteção do Conhecimento Sensível (PNPC), consultoria de segurança com foco na prevenção de espionagem, sabotagem e vazamento de informações conduzido pela ABIN (Agência Brasileira de Inteligência). O foco principal do PNPC é promover a proteção de conhecimentos sensíveis em instituições nacionais, públicas ou privadas.

2.2.10 O PNPC atuou na sensibilização da equipe do FNDE, na identificação de ameaças e vulnerabilidades nos sistemas de proteção da Autarquia e na apresentação de recomendações para redução de risco de incidentes, através de um relatório encaminhado em Janeiro de 2025.

2.2.11 Para a adequação aos objetivos do PPSI, bem como as demais normas de segurança a exemplo do Decreto 9.637/2018 de 26 de dezembro de 2018, que institui a Política Nacional de Segurança da Informação, dispõe sobre a governança da segurança da informação, foi publicado a portaria nº 757, de 5 de setembro de 2024, que dispõe sobre a Política de Segurança da Informação no âmbito do Fundo Nacional de Desenvolvimento da Educação – PSI-FNDE, no qual trouxe várias diretrizes para aprimorar a segurança institucional do órgão. A Portaria revogou a antiga PSI-FNDE instituído conforme a Portaria FNDE n. 250, de 24 de abril de 2018.

2.2.12 Conforme o Art. 2º do PSI-FNDE

“Art. 2º. A PSI-FNDE compreende os domínios de segurança da informação, defesa cibernética, segurança física e proteção de dados organizacionais e tem por escopo as

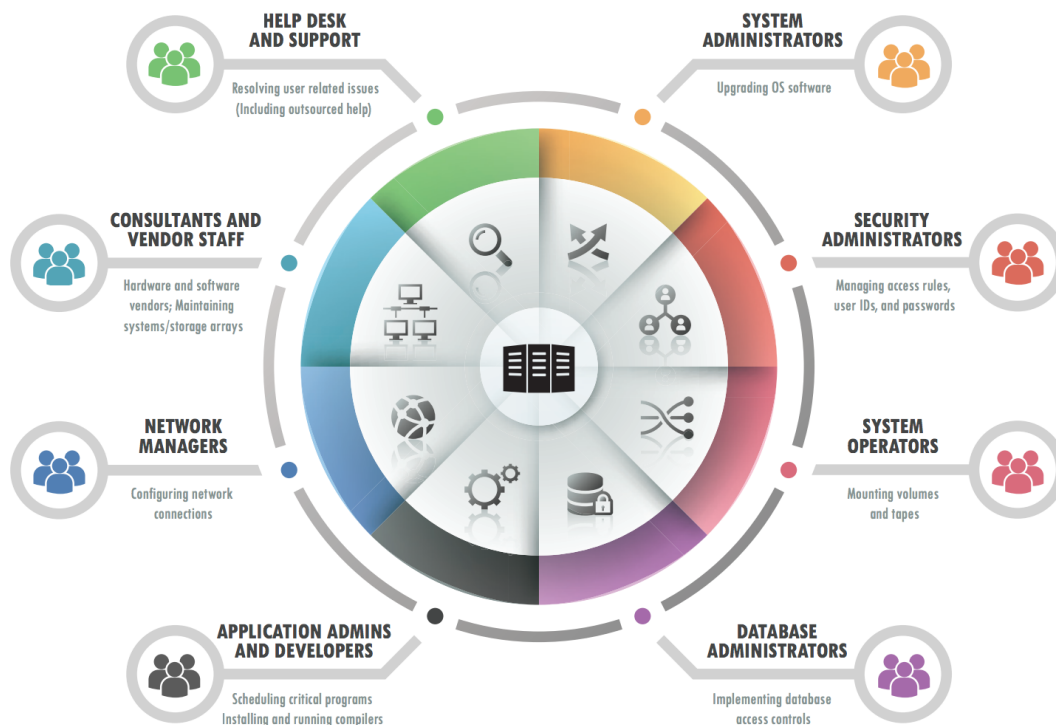
ações destinadas à preservação da disponibilidade, integridade, confidencialidade e autenticidade das informações e dados – bem como a proteção de dados pessoais e a privacidade ...”

2.2.13 Tendo em vista a necessidade de aprimoramento no controle de acesso a rede de dados da autarquia bem como a infraestrutura crítica de processamento para atendimento aos controles do PPSI e PNPC.

2.2.14 Dentre esses aprimoramentos, foi identificado que a autarquia carece de: um gerenciamento para controle dos credenciais de acesso seguro aos recursos privilegiados, melhoria nas ferramentas e procedimentos de segurança para proteção de ameaças online, bem como da gestão de acesso remoto e seguro a rede do FNDE.

2.3.15 Em relação a classificação do controle de credenciais de acesso seguro aos recursos privilegiados é necessário considerar a natureza do controle em relação ao uso dos Serviços e Infraestrutura de Tecnologia da Informação, no qual é possível identificar quatro (04) tipos de usuários no contexto das organizações:

- **Cliente ou Usuário Final (End-User):** São indivíduos que utilizam as soluções de TI da organização. Usuários Normais ou Padrões com Uso Individual, com pouco acesso e com informações restritas, e privilégios restritos. Geralmente estão em maior número na empresa. Ainda podem ser classificados com Internos ou Externos.
- **Administradores (Admin):** Administradores ou Super Usuários, do inglês Super Users, com uso compartilhado, existente para realizar mudanças de configuração (planejadas ou não) e que possui acesso elevado a informações, e privilégios elevados. São exemplos deste tipo de conta: Administrator, Local Admin, Root, db2admin e sysadmin.
- **Desenvolvedores (Devs):** São especialistas que tem acesso a recursos específicos que subsidiam o desenvolvimento de software e projetos no contexto da organização. Precisam de privilégios específicos a depender da sua especialidade. A exemplo de programadores, administradores de Banco de Dados, entre outros.
- **Aplicações e Serviços (Application):** Contas de Serviço são contas para execução, manutenção ou permissão de acesso referentes a aplicações e serviços específicos. Geralmente de uso compartilhado, e dependente de uma aplicação específica, que necessita de privilégio elevado para desempenhar sua tarefa (Aplicações – A2A, Banco de Dados – A2DB, Monitoração de Desempenho, Backup, entre outros).



2.3.16 Para contas dos tipos Administradores, Desenvolvedores e de Aplicações e Serviços existem no mercado recursos de **Gestão de Acessos Privilegiados (Privilege Account Management – PAM)**. São soluções que realizam a Gestão de Credenciais, Monitoramento de Sessão, Autorização de Comandos, entre outros.

2.3.17 A gestão de privilégios possibilita armazenar informações detalhadas sobre cada permissão concedida, gerar diagnósticos precisos para a conformidade de todos os aplicativos utilizados, documentos e registros acessados, conferindo para o FNDE, o controle necessário para regular o uso dos dados.

2.3.18 Visto isso, vale destacar que uma solução de Gestão de Acesso Privilegiados serve tanto para o gerenciamento de acesso para os usuários não institucionais, aqueles que de alguma forma utilizam sistemas da instituição, para prestação de serviços de manutenção de infraestrutura de processamento de dados, quanto para gerenciamento de acesso dos servidores e prestadores de serviços no acesso ao ambiente de processamento de dados.

2.2.19 Neste sentido não existe no órgão uma solução específica para o gerenciamento de acesso privilegiados em que as credencias ficam sob o controle dos terceiros e/ou servidores trazendo riscos para a segurança. Inevitavelmente o comprometimento de uma credencial de acesso privilegiado haverá exploração de toda a infraestrutura crítica de processamento de dados, deixando o Órgão vulnerável a incidentes de segurança que podem afetar o funcionamento da instituição e trazendo prejuízos

2.2.20 Além disso, é importante citar outro ponto crítico, que trata-se dos acessos remotos providos aos usuários do FNDE que necessitam de uma conexão segura, no qual acontece por meio de Virtual Private Network (VPN) nos quais são disponibilizados aos servidores/colaboradores, nos seguintes casos:

- o acesso ao servidor de arquivos;

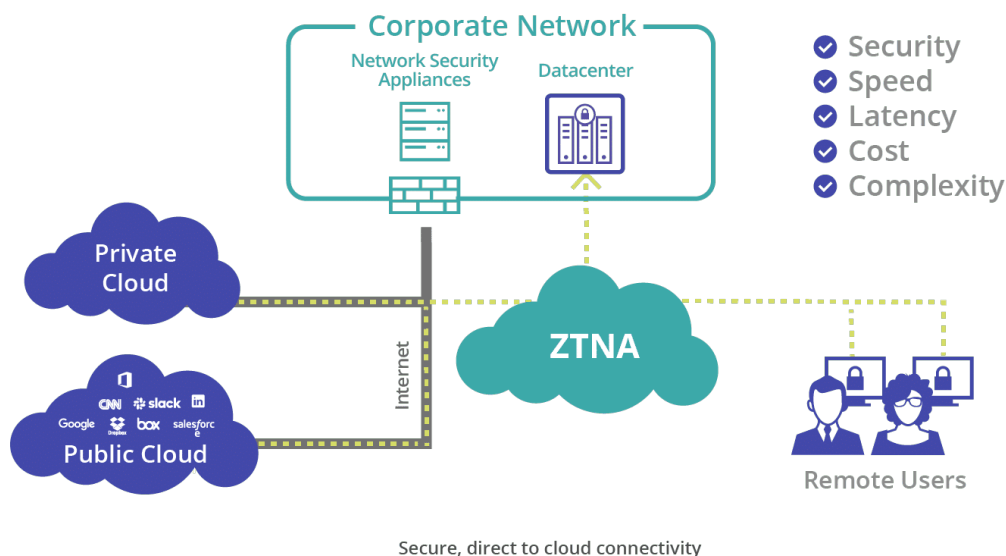
- acesso à aplicações disponíveis apenas na rede interna;
- acesso ao ambiente de desenvolvimento, homologação e produção (fábrica de software – desenvolvedor externo);
- acesso privilegiado as equipes de sustentação e operação de serviços de infraestrutura.

2.2.21 As VPNs possuem, reconhecidamente, problemas que afetam os aspectos de Segurança da Informação, conforme ALERTA 08/2022 do CTIR GOV - Centro de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos de Governo (<https://www.gov.br/ctir/pt-br/assuntos/alertas-e-recomendacoes/alertas/2022/alerta-08-2022>):

"...O acesso via VPN provê autenticação, integridade e confidencialidade dos dados em trânsito. Entretanto, ao mesmo tempo em que o acesso via VPN permite e flexibiliza o trabalho organizacional, o abuso deste recurso pode também ser usado como vetor para ações maliciosas ou mesmo ataques direcionados as Redes Internas das Instituições".

2.2.22 É neste sentido que surge a necessidade da contratação de solução de **gestão de acesso remoto a rede do tipo Zero Trust Network Access (ZTNA)** que é uma tecnologia de segurança que implementa o modelo de segurança Zero Trust. Esse modelo assume que ameaças podem estar tanto dentro quanto fora da rede, portanto, verifica rigorosamente cada usuário e dispositivo antes de conceder acesso a recursos internos. "Zero Trust" é uma estratégia de segurança de rede baseada na filosofia de que nenhuma pessoa ou dispositivo, dentro ou fora da rede de uma organização, deve receber acesso para se conectar aos sistemas ou cargas de trabalho de TI a menos que seja explicitamente necessário.

ZTNA flow for Remote Users

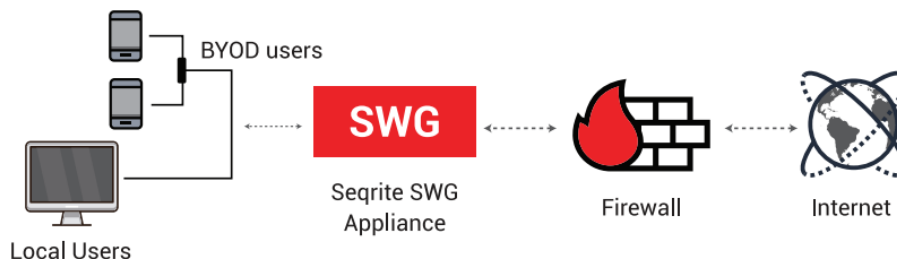


2.2.22.1 O uso de ZTNA permite :

- Proteção do acesso remoto a aplicativos privados;
- Substituindo as conexões VPN;
- Limitando o acesso do usuário;
- Visibilidade profunda da atividade do usuário;
- Avaliação da postura do endpoint.

2.2.23 Deestaca-se que, com o crescimento do trabalho remoto, tanto dos servidores bem como os colaboradores do FNDE, bem como a utilização de serviços em nuvem a exemplo da plataforma Microsoft Office e o aumento no uso de dispositivos pessoais (BYOD) para conexão no ambiente da

autarquia, a superfície de ataque no âmbito do FNDE cresceu significativamente. Embora a autarquia possua soluções tradicionais de segurança, a exemplo de firewalls de perímetro, atualmente não é mais suficiente para proteção dos usuários e os dados corporativos, especialmente em um cenário onde o acesso à internet ocorre de qualquer lugar. É nesse contexto que seria viável a implementação de solução do tipo **Secure Web Gateway (SWG)**.



2.2.24 Neste sentido, para a aplicação de mais camadas de segurança ao acesso e, conseqüentemente, aos serviços providos, entende-se como necessária a implementação das soluções citadas acima.

2.2.25 - Destaca-se que tais soluções são complementares e não substituem outros ativos e ferramentas de Segurança da Informação já em uso no Órgão e nem elimina a necessidade futura de outras soluções e serviços de segurança, considerando a grande abrangência de controles essencialmente necessários para a proteção e guarda das informações de uma instituição crítica tal como o FNDE.

2.2.25.1 Em comparação com o firewall e o ZTNA, no ZTNA o acesso é concedido apenas ao recurso específico necessário, enquanto os firewalls atualmente no FNDE monitoram e controlam o tráfego entre os diferentes segmentos e inspecionam o tráfego para identificar e bloquear atividades maliciosas.

2.2.25.2 Em comparação com o firewall e o SWG, enquanto o firewall protege a rede como um todo, o SWG foca especificamente no tráfego de navegação, inspecionando e bloqueando ameaças em nível de aplicação. O firewall pode segmentar a rede, enquanto o SWG garante que cada segmento tenha acesso controlado à internet, permitindo uma abordagem baseada em "confiança zero". Ambos trabalham juntos para inspecionar tráfego HTTPS de maneira eficiente, garantindo que ameaças escondidas em conexões criptografadas sejam detectadas.

2.2.26 - Desta forma, o presente documento demonstrará os cenários e demais informações que subsidiam a necessidade e as condições e as alternativas viáveis ou compatíveis para a pretensa contratação.

2.3 Da Justificativa da Necessidade

2.3.1 Ao longo dos anos, o FNDE tem investido em recursos de tecnologia da informação e comunicação, principalmente de segurança, de forma a assegurar o desempenho de suas atividades institucionais, possibilitando a melhoria de processos de segurança.

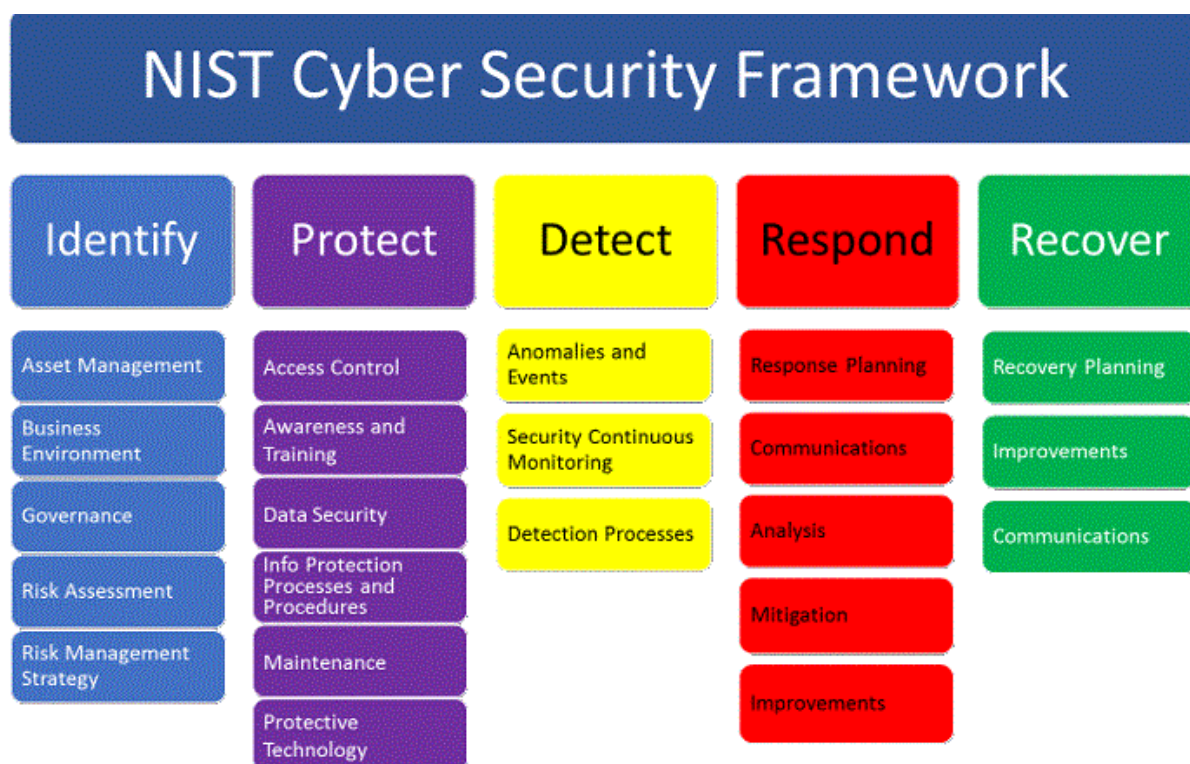
2.3.2 Um exemplo é a contratação de solução de redes, bem como de soluções de aplicativos de escritórios e de segurança baseado na plataforma Microsoft, solução de Firewall e de balanceamento de carga e outros, além diversas ações que vem sendo implementadas ou planejadas para o aperfeiçoamento da Segurança Cibernética do Órgão.

2.3.3 Assim, a presente contratação faz parte dessa estratégia de evolução e não criará sobreposição com a infraestrutura de segurança hoje em produção no âmbito da Autarquia,

considerando algumas lacunas e grande abrangência dos controles de Segurança que devem ser adotados em qualquer instituição.

2.3.4 Como exemplo dessa abrangência e conforme já exposto, existem vários frameworks de segurança da informação que auxiliam as organizações a estabelecer a sua estratégia, adaptando-se às suas necessidades específicas e ao cenário de ameaças em constante evolução. Nesse contexto podemos citar:

- **NIST Cybersecurity Framework:** Desenvolvido pelo National Institute of Standards and Technology (NIST) dos Estados Unidos, este framework se concentra em cinco áreas principais: Identificar, Proteger, Detectar, Responder e Recuperar. Ele oferece uma abordagem baseada em risco que permite que organizações de todos os tamanhos adaptem as melhores práticas de segurança cibernética de acordo com suas necessidades específicas



- **CIS Controls:** Os Controls da Center for Internet Security (CIS) são um conjunto de 18 (dezoito) controles de segurança desenvolvidos para fornecer uma abordagem prática e eficaz contra ameaças comuns. Eles são frequentemente atualizados para se alinhar com as tendências e ameaças emergentes no cenário cibernético. O Tribunal de Contas da União e o Ministério da Gestão e Inovação, por exemplo, tem utilizado em suas ações os controles referenciados neste framework.



2.3.4 O Acórdão 2430/2024 - Plenário no qual o TCU realizou a auditoria operacional na Casa Civil da Presidência da República e no Gabinete de Segurança Institucional da Presidência da República com o objetivo de avaliar em que medida a Política Nacional de Cibersegurança (PNCiber) está de acordo com as boas práticas, em especial comparada ao previsto no Referencial de Controle de Políticas Públicas do TCU, o Tribunal informa

"As atividades de segurança cibernética no país estão insuficientes, como ocorre, por exemplo, nas 254 organizações do Sisp que não implementam completamente o conjunto básico de medidas de segurança de defesa cibernética esperado de uma organização de pequeno a médio porte ..."

2.3.5 O Acórdão 2387/2024 - Plenário no qual o TCU realizou a auditoria operacional na Secretaria de Governo Digital do Ministério da Gestão e da Inovação em Serviços Públicos e as demais 253 organizações que compõem o Sistema de Administração dos Recursos de Tecnologia da Informação (Sisp), tomadas como amostra: Agência Espacial Brasileira; Banco Central do Brasil; Comando da Marinha; Conselho de Controle de Atividades Financeiras; Empresa Brasileira de Infraestrutura Aeroportuária; Ministério da Defesa; e Universidade Federal do Rio Grande do Sul com o objetivo de avaliar os controles de cibersegurança e de segurança da informação implementados pelas organizações do Sistema de Administração dos Recursos de Tecnologia da Informação (Sisp), o Tribunal solicita

9.2. recomendar a cada uma das organizações do Sisp relacionadas no apêndice E do relatório de peça 200 que:

9.2.1. adotem medidas para implementar os controles de segurança cibernética necessários para reduzir o risco de ataques cibernéticos ao nível aceitável para as políticas públicas que executam, utilizando como referencial as diretrizes

expedidas pela SGD/MGI por meio do PPSI, de acordo com o art. 8º da Portaria-SGD/MGI nº 852/2023;

9.2.2. enviem esforços para que o processo de gestão de riscos decorrentes de ataques cibernéticos seja liderado explicitamente pela sua alta administração, alinhado ao previsto no art. 17 do Decreto nº 9.203/2017;

2.3.6 A presente contratação atenderá, tanto os acórdãos acima quanto os controles constante no PPSI e PNPC bem como o Direcionador Estratégico - DRE – 1 - Elevação da maturidade em governança, gestão ágil e cibersegurança, bem como a Iniciativa Estratégica - INI-1.03: Aprimorar instrumentos de cibersegurança constante no Plano Diretor de Tecnologia da Informação do FNDE.

2.3.7 Conforme já exposto, visa o atendimento de controles básicos de forma a implementar **Gestão de Acessos Privilegiados, gestão de acesso remoto a rede do tipo Zero Trust Network Access (ZTNA) e do Secure Web Gateway (SWG)**, controles estes essenciais para a Segurança da rede.

2.3.8 Registra-se ainda a relevância de gestão de acessos no Cenário de Segurança Cibernética, ao passo de que maior parte dos incidentes estão relacionados ao vazamento de credenciais de acessos conforme pode se observado em vários estudos e publicações e entidades e organismos que tratam dessa temática, a exemplo do resultado do estudo da Verizon da 2024:

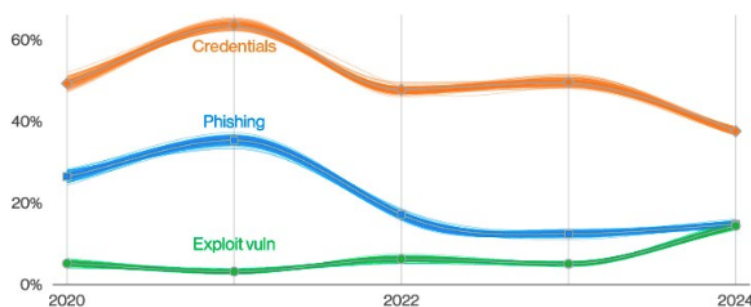


Figure 6. Select ways-in enumerations in non-Error, non-Misuse breaches over time

<https://www.cybersecuritydive.com/news/valid-credentials-most-intrusions/689118/>

Credenciais de conta válidas estão por trás da maioria das intrusões cibernéticas, conclui CISA

A taxa de sucesso dessas técnicas ressalta o poder de permanência dos métodos mais comuns que os agentes ameaça usam para obter acesso inicial a sistemas direcionados.

<https://outpost24.com/blog/credential-theft-the-business-impact-of-stolen-credentials/>

2.3. Desta forma a pretensa contratação proporcionará um maior controle de cibersegurança referente a gestão de acessos, em complemento a outras soluções já adotadas considerando o atendimento as recomendações e orientações direcionadas aos Órgãos da Administração Pública. Desta forma, visamos a eventual contratação das seguintes soluções/serviços:

- **Gestão de Acessos Privilegiados**
- **Armazenamento de Credenciais**

- **Gestão de Acesso Remoto e Seguro (ZTNA e SWG)**

3. Área requisitante

Área Requisitante	Responsável
Coordenação-Geral de Infraestrutura e Serviços da Tecnologia da Informação - CGINF	Karen de Sousa Costa
Coordenação de Operações e Cibersegurança - COPEC	Belmiro da Graça Soares

4. Necessidades de Negócio

4. Necessidades de Negócio

4.1 As necessidades de negócio, também chamadas de requisitos do negócio, refletem as necessidades e expectativas de uma organização para alcançar seus objetivos estratégicos e operacionais. Nesse para o FNDE a contratação visa proporcionar, dentre outros:

- **Confidencialidade, integridade e disponibilidade:** A solução deve garantir uma barreira contra acessos não autorizados e garantir a precisão e consistência dos dados, bem como a alta disponibilidade dos serviços.
- **Proteção dos Dados do FNDE:** A solução deve garantir a limitação de acesso indevido aos dados e sistemas contra violações bem como a proteção dos acessos privilegiados da infraestrutura crítica de processamento de dados.
- **Acesso remoto seguro:** Garante que os servidores e prestadores de serviços possam acessar os recursos de tecnologia da informação de forma segura independente da sua localização.
- **Conformidade regulatória:** Atendimento aos requisitos de proteção de dados e segurança da informação bem como, no mínimo, os controles do PPSI e PNPC.
- **Transferência de conhecimento:** A solução deverá ter ainda em sua composição um item para treinamento, para garantir que ocorra a transferência do conhecimento para os servidores e colaboradores que atuam na infraestrutura de TI do FNDE.
- **Implementação assistida:** Todos os serviços de instalação e configuração deverão ser executados pela Contratada, de modo a não sobrecarregar a equipe de servidores e colaboradores da autarquia, porém as atividades deverão ser acompanhadas pelos servidores e colaboradores que atuarão na operação da solução após entregue pela Contratada.

5. Necessidades Tecnológicas

5. Necessidades Tecnológicas

5.1 As necessidades tecnológicas, também chamadas de requisitos da solução de tecnologia, descrevem as características de uma solução que atendam aos requisitos do negócio.

5.2 Necessidades Tecnológicas para Soluções de Gestão de Acessos Privilegiados

- 5.3.1. Prover meios de auditar os acessos administrativos realizados nos ativos de rede do FNDE;
- 5.3.2 Registrar os eventos realizados nas sessões privilegiadas;
- 5.3.3 Registrar as ações realizadas em posse de conta privilegiada com possibilidade de gravação de sessão (gravação de telas);
- 5.3.4 Melhorar controle sobre a utilização de recursos privilegiados do ambiente computacional;
- 5.3.5 Obter o monitoramento das ações de servidores e prestadores de serviços com o uso de credenciais privilegiadas;
- 5.3.6 Melhorar qualidade na prestação de informações na investigação de incidentes de segurança;
- 5.3.7 Rastrear o uso de contas privilegiadas no ambiente computacional;
- 5.3.8 Aprimorar a segurança da informação e comunicação do FNDE.

5.3 Necessidades Tecnológicas para Soluções de Gestão de Acesso Remoto (ZTNA)

- 5.3.1 Controle de acesso granular que garanta que os usuários acessem apenas os recursos necessários para suas funções.
- 5.3.2 Automação do provisionamento e desprovisionamento de acessos.
- 5.3.3 Integração com sistemas de gestão de acessos privilegiados e outras infraestruturas existentes no âmbito do FNDE.
- 5.3.4 Implementação de medidas de segurança contra-ataques cibernéticos, como detecção de anomalias, resposta a incidentes e inspeção SSL/TLS.
- 5.3.5 Criptografia de dados em trânsito para proteger as comunicações durante a navegação na web, bem como entre dispositivos e aplicativos.

5.5 Necessidades Tecnológicas para Soluções de Gestão de Acesso Seguro (SWG)

- 5.5.1 Bloqueio de sites maliciosos e prevenção de downloads perigosos.
- 5.5.2 Filtragem de conteúdo e políticas de acesso para proteger os usuários durante a navegação na internet.
- 5.5.3 Proteção contra ameaças da web, como malware, phishing e ataques de dia zero.
- 5.5.4 Integração com sistemas de gestão de acessos privilegiados e outras infraestruturas existentes no âmbito do FNDE.
- 5.5.5 Implementação de medidas de segurança contra-ataques cibernéticos, como detecção de anomalias, resposta a incidentes e inspeção SSL/TLS.

5.6 Necessidades Tecnológicas para Soluções de Gestão e Armazenamento de Credenciais

- 5.6.1 Prover de forma segura o armazenamento centralizado das credenciais de acesso dos ativos de rede em alta disponibilidade;
- 5.6.2 Melhorar qualidade na prestação de informações na investigação de incidentes de segurança;
- 5.6.3 Aprimorar a segurança da informação e comunicação do FNDE.

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

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

Os requisitos aqui informados são padrões e comumente adotados em contratações similares e em processos de contratações em andamento.

6.1 Requisitos de Continuidade do Negócio

6.1.1 Para possibilitar o controle de suporte e manutenção, deverá ser previsto que a execução de suporte técnico seja através da abertura de chamados técnicos com prazos de atendimento e solução em conformidade com os níveis de serviços requeridos pelo FNDE.

6.2 Requisitos Sociais, Ambientais e Culturais da solução de TIC

6.2.1 O idioma a ser utilizado na documentação dos serviços técnicos vinculados a solução a ser entregue pela Contratada deve ser em formato digital e estar em língua portuguesa ou inglesa.

6.2.2 O idioma a ser utilizado no processo de gerenciamento de chamados deve ser a língua portuguesa, podendo eventualmente ser utilizado o inglês, desde que autorizado pelo FNDE, e que a equipe técnica seja informada previamente de que o atendimento será realizado em inglês.

6.2.3 A Contratada deverá adotar práticas de sustentabilidade ambiental na execução do objeto, no que couber, conforme disposto na Instrução Normativa SLTI/MP nº 1/2010 e Decreto nº 7.746/2012, da Casa Civil, da Presidência da República.

6.2.4 Os serviços prestados pela Contratada deverão pautar-se sempre pelo uso racional de recursos e equipamentos, de forma a evitar e prevenir o desperdício de insumos e material consumidos, bem como a geração excessiva de resíduos, a fim de atender às diretrizes de responsabilidade ambiental adotadas pelo FNDE

6.2.5 Os resíduos dos processos de manutenção deverão ser recolhidos pela Contratada para fins de destinação adequada conforme legislação ambiental

6.3 Requisitos da Capacitação

6.3.1 A CONTRATADA deverá repassar à CONTRATANTE todas as informações solicitadas e documentação da solução, além de disponibilizar treinamento conforme especificações a serem fornecidas conforme o presente documento.

6.3.2 O treinamento será demandado à CONTRATADA pela CONTRATANTE após a efetiva implementação e estruturação da solução de segurança em seu parque tecnológico, quando acordarão cronograma para realização do treinamento.

6.3.3 O treinamento deverá ser em Brasília – DF, para a equipe técnica do CONTRATANTE.

6.3.4 Todos os custos relativos à realização do treinamento são de exclusiva responsabilidade da CONTRATADA.

6.3.5 O treinamento deverá capacitar as equipes técnicas do CONTRATANTE a operarem, configurarem, administrarem e resolverem problemas usuais na solução adquirida.

6.3.6 Quando o treinamento for ofertado remotamente (modalidade Educação à Distância), deverá ser ministrado de forma síncrona. Não computando na carga horária cursos assíncronos, materiais multimídia, voucher e similares.

6.3.7 Deverá ser ofertada para uma (01) turma com no mínimo cinco (05) alunos /participantes e com carga horária mínima de vinte (20) horas por item contratado.

6.3.8 Deverá ser fornecido certificado de conclusão emitido pelo fabricante.

6.3.9 Os horários do curso deverão seguir a conveniência do CONTRATANTE, podendo sua realização ocorrer apenas em um dos períodos do dia (manhã ou tarde).

6.3.10 Deverá ser fornecido material didático completo e com conteúdo oficial do fabricante, podendo ser fornecido por meio de manuais/documentos em PDF.

6.3.11 É de responsabilidade da CONTRATADA registrar em ata todas as etapas do treinamento. De forma a apresentar ao final desta fase registros de data de realização da(s) sessão(ões), o conteúdo abordado e a assinatura dos participantes.

6.4 Requisitos Legais e de Segurança da Informação

6.4.1 Cabe destacar alguns preceitos legais e direcionamentos do Governo Federal quanto à contratação e prestação de serviços de TIC, a saber:

6.4.1.1 Lei nº 12.527, de 18 de novem de 2011, que regula o acesso à informações previsto em lei

6.4.1.2 Lei nº 13.709, de 14 de agosto de 2018 (Lei Geral de Proteção de Dados).

6.4.1.3 Lei 14.133, de 01 abril de 2021 – Lei de Licitações e Contratos Administrativos;

6.4.1.4 Decreto Nº 7.174, de 12 de maio de 2010 – regulamenta a contratação de bens e serviços de informática e automação pela administração pública federal, direta ou indireta, pelas fundações instituídas ou mantidas pelo Poder Público e pelas demais organizações sob o controle direto ou indireto da União;

6.4.1.5 Decreto nº 7.724, de 16/05/2012, que regulamenta a lei Lei 12.527, de 18/11/2011;

6.4.1.6 Decreto nº 7.845, de 14/11/2012, que trata do credenciamento de segurança e tratamento de informação classificada em qualquer grau de sigilo;

6.4.1.7 Decreto nº 9.637, de 26 de dezembro de 2018, que, entre outras coisas, institui a Política Nacional de Segurança da Informação e dispõe sobre a governança da segurança da informação;

6.4.1.8 Decreto nº 10.024, de 20 de setembro de 2019 – Regulamenta a licitação, na modalidade pregão, na forma eletrônica, para a aquisição de bens e a contratação de serviços comuns, incluídos os serviços comuns de engenharia, e dispõe sobre o uso da dispensa eletrônica, no âmbito da administração pública federal;

6.4.1.9 Instrução Normativa nº 05/2017, da Secretaria de Logística e Tecnologia da Informação do Ministério do Planejamento, Orçamento e Gestão que dispõe sobre as regras e diretrizes do procedimento de contratação de serviços sob o regime de execução indireta no âmbito da Administração Pública federal direta, autárquica e fundacional;

6.4.1.10 Instrução Normativa (IN) nº 65, de 07 de julho de 2021, que dispõe sobre o procedimento administrativo para a realização de pesquisa de preços para a aquisição de bens e contratação de serviços em geral, no âmbito da administração pública federal direta, autárquica e fundacional.

6.4.1.11 Instrução Normativa SGD/ME Nº 94, de 23 de dezembro de 2022 - Dispõe sobre o processo de contratação de soluções de Tecnologia da Informação e Comunicação - TIC pelos FNDEs e entidades integrantes do Sistema de Administração dos Recursos de Tecnologia da Informação - SISP do Poder Executivo Federal.

6.4.1.12 Portaria SGD/ME nº 778, de 04 de abril de 2019, que dispõe sobre a implantação da Governança de Tecnologia da Informação e Comunicação nos órgãos e entidades pertencentes ao Sistema de Administração dos Recursos de Tecnologia da Informação do Poder Executivo Federal - SISP.

6.4.1.13 Portaria SGD/MGI Nº 852, DE 28 de março de 2023, que dispõe sobre o Programa de Privacidade e Segurança da Informação - PPSI

6.4.1.14 Portaria SGD/MGI nº 5.950, de 26 de outubro de 2023 e seus anexos, que estabelece modelo de contratação de software e de serviços de computação em nuvem, no âmbito dos órgãos e entidades integrantes do Sistema de Administração dos Recursos de Tecnologia da Informação - SISP do Poder Executivo Federal.

6.4.1.15 Portaria FNDE nº 757, de 5 de setembro de 2024, que dispõe sobre a Política de Segurança da Informação no âmbito do Fundo Nacional de Desenvolvimento da Educação – PSI-FNDE

6.5 Requisitos Temporais

6.5.1 Os serviços devem ser prestados conforme definido neste documento e no Termo de Referência, a contar do recebimento da Ordem de Serviço (OS), emitida pela Contratante, podendo ser prorrogada, excepcionalmente, por até igual período, desde que justificado previamente pelo Contratado e autorizado pela Contratante.

6.5.2 Para os serviços de instalação e configuração das soluções, treinamento e o serviço de suporte para as soluções disponibilizadas será considerada como hora útil, aquela compreendida entre 08h e 18h em dias úteis, podendo também ser denominado como horário útil.

6.5.3 Para o serviço de monitoramento deverá ser considerada a janela de atendimento 24 x 7, ou seja, todos os dias (segunda a domingo) 24 horas diárias, sendo realizado de forma contínua.

6.6 Requisitos de Privacidade e Segurança da Informação

6.6.1 A Contratada deve executar o objeto do certame em estreita observância aos ditames estabelecido pela Lei 13.709/2018 (Lei Geral de Proteção de Dados Pessoais - LGPD).

6.6.2 A Contratada deverá submeter-se aos procedimentos contidos nas normas de segurança corporativa do FNDE, em todos os eventos em que for necessária a presença de seus prepostos e /ou funcionários nas dependências da Autarquia.

6.6.3 A Contratada deverá submeter-se aos procedimentos contidos na Política de Segurança da Informação do FNDE (PSI-FNDE) instituída conforme a Portaria FNDE nº 757, de 5 de setembro de 2024 disponível no endereço https://www.gov.br/fnde/pt-br/aceso-a-informacao/legislacao/portarias/2024/PORTARIA_757_5_DE_SETEMBRO_DE_2024.pdf/view bem como as Normas Operacionais e Processos de Segurança

6.6.4 A Contratada deve guardar sigilo dos dados e das informações postas à sua disposição, não podendo cedê-los a terceiros ou divulgá-los de qualquer forma sem anuência expressa da Autarquia, devendo entregar assinados o Termo de Manutenção de Sigilo e o Termo de Ciência.

6.6.5 A Contratada deverá assinar e entregar, na Reunião Inicial, o Termo de Compromisso de Manutenção de Sigilo (TCMS) e providenciar a assinatura do Termo de Ciência por todos os seus colaboradores que estejam relacionados com a execução do objeto.

6.6.6 A Contratada deverá obedecer aos critérios, padrões, normas e procedimentos operacionais adotados pelo FNDE.

6.6.7 A Contratada deve manter sigilo, sob pena de responsabilidades civis, penais e administrativas, sobre todo e qualquer assunto de interesse da Autarquia ou de terceiros de que tomar conhecimento em razão da execução do objeto deste Contrato devendo orientar seus empregados nesse sentido.

6.6.8 A Contratada deve responsabilizar-se pelos materiais, produtos, ferramentas, instrumentos equipamentos disponibilizados para a execução dos serviços, não cabendo ao FNDE qualquer responsabilidade por perdas decorrentes de roubo, furto ou outros fatos que possam vir a ocorrer.

6.6.9 A Contratada não poderá transferir a outrem no todo ou em parte o objeto do presente contrato sem prévia e expressa anuência da Autarquia, exceto aqueles que se refiram a ativos sob garantia de terceiros. Em caso de atendimento efetuado por terceiros nas dependências do FNDE, a Contratada deverá disponibilizar técnico(s) do seu quadro funcional próprio para acompanhar todos os procedimentos.

6.6.10 A Contratada não poderá veicular publicidade acerca dos serviços contratados, sem prévia autorização, por escrito, da Autarquia.

6.6.11 A Contratada deve manter em caráter confidencial, mesmo após o término do prazo de vigência ou rescisão do contrato, as informações relativas as configurações de hardware e de softwares existente no Ambiente do FNDE.

6.6.12 A Contratada deve executar todos os testes de segurança necessários e definidos na legislação pertinente;

6.6.7.13 A Contratada deve garantir o cumprimento:

6.6.7.13.1 Dos normativos vigentes editados pelo Gabinete de Segurança Institucional (GSI/PR) sobre Segurança da Informação, bem como, suas atualizações e demais normativos complementares, encontrados em: <https://www.gov.br/gsi/pt-br/assuntos/dsi>.

6.6.7.13.2 Dos normativos internacionais de boas práticas da família ISO/IEC 27000, em especial, quanto às normas ABNT NBR ISO/IEC 27001:2013; 27002:2013; e, 27005:2019;

6.6.7.13.3 De boas práticas do Center for Internet Security (CIS) e do National Institute of Standards and Technology (NIST), a critério do FNDE

6.6.7.13.4 Das diretrizes da Lei Geral de Proteção de Dados – LGPD (Lei Federal nº 13.709/18).

6.6.7.14 Promover a implementação de controles de segurança da informação conforme as práticas dispostas nos normativos citados.

6.6.15 A execução dos serviços de forma remota, fora das dependências do FNDE, é permitida, desde que cumpridas as diretrizes de segurança estabelecidas pelo FNDE.

6.6.16 Na hipótese dos colaboradores da CONTRATADA trabalharem remotamente, os seguintes requisitos devem ser cumpridos:

6.6.16.1 Todo acesso ao ambiente do FNDE deve ser realizado por meio do ambiente corporativo da CONTRATADA, considerando os mecanismos de segurança obrigatórios pontuados neste item;

6.6.16.2 Os colaboradores devem ser capacitados quanto às boas práticas de segurança da informação, não excluindo as certificações exigidas no presente documento;

6.6.16.3 A CONTRATADA deve prover recursos suficientes e com a adequada segurança para seus colaboradores.

6.6.17 Prospectar e implementar soluções de segurança da informação aplicando, sempre que possível, um modelo de segurança *Zero Trust*.

6.6.18 Definir, apresentar e executar processo de gestão de riscos de segurança da informação nos ambientes gerenciados sob sua responsabilidade técnica.

6.6.9 Garantir a rastreabilidade das ações realizadas nos ambientes gerenciados sob sua responsabilidade técnica, mantendo trilhas de auditoria de segurança da informação.

6.7 Requisitos de Implantação

6.7.1 Para a implantação da solução a contratada deve apresentar a documentação de projeto contendo:

6.7.1.1 Sumário acerca do cenário existente;

6.7.1.2 Descritivo da(s) ferramenta(s) implementadas;

6.7.1.3 Plano de comunicação;

6.7.1.4 Plano de riscos;

6.7.1.5 Especificidades de cada solução;

6.7.1.6 Meios de contato para suporte da contratada e da fabricante;

6.7.1.7 Sugestão de melhorias futuras;

6.8 Requisitos de Metodologia de Trabalho

6.8.1 A metodologia de trabalho será baseada no conceito de delegação de responsabilidade, onde o FNDE é responsável pela gestão e fiscalização do contrato e pela atestação da aderência aos padrões de qualidade exigidos, e a CONTRATADA como responsável pela execução dos serviços e gestão dos seus recursos humanos.

6.8.2 A execução dos serviços está condicionada ao recebimento pelo Contratado de Ordem de Serviço (OS) emitida pelo FNDE.

6.8.3 A OS indicará o serviço, a quantidade e a localidade na qual os serviços deverão ser prestados.

6.8.4 A execução do serviço deve ser acompanhada pelo CONTRATADO, que dará ciência de eventuais acontecimentos ao FNDE.

6.8.5 A CONTRATADA deverá executar os serviços seguindo os processos, padrões e procedimentos indicados pelo FNDE.

6.8.6 Todas as atividades devem estar de acordo com as especificações e melhores práticas dos fabricantes dos equipamentos/software e com as recomendações de organizações padronizadoras do segmento, desde que não entrem em conflito com os padrões, procedimentos e documentação definidos pelo FNDE.

6.8.7 Também, no que couber, na execução dos serviços a CONTRATADA deve manter observância às políticas, regulamentações, especificações técnicas e orientações definidos pelos padrões de GOVERNO.

6.9 Outros requisitos

6.9.1 Durante o planejamento da contratação outros requisitos poderão vir a se definir bem como a revisão dos inicialmente descritos acima.

7. Estimativa da demanda - quantidade de bens e serviços

7. Estimativa da demanda - quantidade de bens e serviços

7.1 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.

7.2 Assim, estima-se a eventual contratação dos seguintes itens:

Grupo	Item	Especificação	CATSER	Métrica
1	1	Subscrição de gestão de acessos privilegiados.	27502	Usuários
	2	Subscrição para solução de Segurança para Armazenamento de Credenciais.	27502	Usuários

	3	Serviços de Instalação e Configuração das Soluções (por item / módulo)	26972	Serviço
	4	Serviço de treinamento / capacitação por (item / módulo)	3840	Turma
2	5	Serviço de acesso remoto confiança zero (ZTNA)	27502	Usuários
	6	Serviço de acesso seguro interno/externo (SWG)	27502	Usuários
	7	Serviços de Instalação e Configuração das Soluções (por item / módulo)	26972	Serviço
	8	Serviço de treinamento / capacitação (por item / módulo)	3840	Turma

7.3 Para o dimensionamento da demanda da **Solução de Gestão de Acessos Privilegiados** (item 01 da tabela) foi considerado de forma preliminar os seguintes volumes:

7.3.1 O atual contrato de sustentação de infraestrutura que possui 26 prestadores de serviços (com previsão de acréscimo de mais 6 colaboradores), bem como os da central de serviços com atualmente com 11 colaboradores totalizando 43 (quarenta e três usuários) usuários com privilégios administrativos.

7.3.2 Além disso, estima-se a alocação de mais 15 licenças aos servidores do FNDE bem como 20 licenças para a equipe de desenvolvimento e 10 licenças aos eventuais prestadores de serviços que necessitam de acesso ao ambiente para prestação de suporte e garantia as soluções no ambiente do FNDE e uma reserva de 12 licenças para eventualidades no decorrer da vigência, estimando-se o quantitativo total de 100 usuários, conforme abaixo:

Contrato de sustentação de infraestrutura de TIC	32 usuários
Central de Serviços	11 usuários
Equipe de Desenvolvimento de Soluções	20 usuários
Prestadores de Serviço de Manutenção e Suporte	10 usuários
Servidores do FNDE	15 usuários
Licenças reservas	12 usuários
TOTAL ESTIMADO	100 usuários

7.4 Para o dimensionamento da demanda da **Solução de Gestão de Armazenamento de Credenciais** (item 02) bem como de **Acesso Seguro** (item 06 da tabela), foi efetuado levantamento em que obteve-se as seguintes informações:

7.4.1 Atualmente o FNDE possui 1528 usuários que acessam a rede do FNDE. Estes são os usuários aptos utilizar estações de trabalho, rede de computadores e sistemas institucionais, a exemplo do SEI (Sistema Eletrônico de Informações).

7.4.2 Conforme Despacho SEI nº 4455190 da área de pessoas, há a previsão de ingresso de mais 99 servidores de contratos temporários da União (CTU's), além da nomeação de mais 25 servidores da Carreira do FNDE. Também foi informado o início de um processo de contratação de serviço de apoio administrativo com a previsão de 99 postos de trabalho.

7.4.3 Atualmente a atual fábrica de software possui 112 prestadores de serviços e na futura contratação ainda há previsão de contratação de 200 prestadores de serviços o que reflete em um aumento estimado de 88 pessoas.

7.4.3 Além disso encontra-se em andamento no FNDE outros processos de contratação para a reposição de postos e novos serviços, a exemplo da contratação de apoio a gestão e de BI, o que direciona para a necessidade de reversa de aproximadamente 149 usuários.

7.4.3 Segue abaixo o resumo dos quantitativos da **solução de gestão de armazenamento de credenciais** bem como de acesso seguro:

Número de usuários de rede do FNDE	1528 usuários
Servidores - Contrato Temporário da União	99 usuários
Novos servidores, terceiros, consultores	124 usuários
Outros - Fabrica de Software e Contratos de Apoio a Gestão de TIC e BI	149 usuários
TOTAL ESTIMADO	1900 usuários

7.5 Para o dimensionamento da demanda da **Solução de Gestão de Acesso Remoto** confiança zero (item 05 da tabela), foi efetuado o estudo de informações de forma a contemplar os usuários da futura fábrica de software bem como os demais usuários que necessitam de acesso específicos a ambientes e serviços internos, não publicados. Dessa forma considerou-se 400 usuários.

7.5.1 Registra-se que apesar da quantidade de usuários que atuam remotamente e de forma híbrida ser superior ao quantitativo acima, entende-se que usuários comuns utilizam serviços publicados externamente, sem a necessidade de VPN's para acesso ao ambiente interno e restrito, sendo o número acima suficiente para o atendimento dessa demanda.

7.6 Ainda, considerando que tratam-se de soluções novas e que não estão no escopo de conhecimento dos atuais perfis e colaboradores do Órgão, faz-se necessária a previsão de **serviços de implantação/configuração** da solução por parte do fornecedor para garantir o funcionamento e uso de todos os recursos da solução. Além disso é necessário o **repasse de conhecimento** (treinamento) para a equipe que após a implantação irá sustentar e operar a solução. Assim para o dimensionamento dessa demanda estimou-se a quantidade de um serviço de instalação e treinamento para cada solução que for contratada. Ou seja, por item/modulo conforme os itens 03 e 07, 04 e 08 da tabela acima.

7.7 Por fim, é importante registrar que as quantidades informadas acima tratam-se de meras estimativas considerando o cenário atual e as informações recebidas. É possível que até que ocorra a contratação possa existir variações tanto dos itens como dos volume informados, levando a necessidade de novos ajustes da demanda, considerando o ambiente dinâmico a qual estamos expostos bem como diversos fatos supervenientes que possam ocorrer durante o processo de contratação.

7.8 Tal situação viabilizaria o Órgão para uma contratação através de Registro de Preço, a fim de que possa haver compra futura considerando a flexibilidade deste procedimento para Administração

Pública em comprar ou contratar quando quiser, na quantidade que quiser, desde que dentro dos quantitativos máximos licitados e dentro do prazo de validade da ata, não se obrigando ainda a contratação de todos os itens.

8. Levantamento de soluções

8. Levantamento de Soluções

8.1 O levantamento e a análise comparativa de soluções, nos termos do inc. II do art. 11 da IN-94 /2022 – SGD/ME, visa a elencar as alternativas de atendimento à demanda proposta considerando, além do aspecto econômico, os aspectos qualitativos em termos de benefícios para o alcance dos objetivos da contratação.

8.2 Existem várias opções de soluções as quais são possíveis se considerar para atender às necessidades de um órgão da administração pública federal. Assim, se faz importante observar Critérios para Seleção, a exemplo de:

- Conformidade e Segurança
- Funcionalidades e Integração
- Escalabilidade e Desempenho
- Usabilidade e Experiência do Usuário
- Suporte e Manutenção

8.3 Além dos critérios de seleção expostos acima, durante o planejamento de uma contratação, antes mesmo da externalização e formalização de processos existem ações que são realizadas para a análise de melhor forma de implantação da estratégia, considerando prazos, prioridades, e outras análises.

8.4 Sob as soluções elencadas neste documento, registra-se que desde o ano de 2022 foram iniciadas ações para a contratações de soluções de segurança, a exemplo de Gestão de Acesso Privilegiado, que atenderiam parte das necessidades apresentadas nesse documento. Por questões internas e considerando que na mesma época foi lançado o PPSI (Programa de Privacidade e Segurança da Informação) com a necessidade de implementação de diversas medidas de segurança, em que também houve a expectativa do próprio Ministério da Gestão e Inovação para a contratação de soluções e serviços gerenciados de segurança da informação, foi necessária a reavaliação da demanda.

8.5 Além das questões pontuadas acima e de outras, registra-se que naquele mesmo período outros processos tiveram que ser priorizados considerando a criticidade e o encerramento dos contratos vigentes, a exemplo do Licenciamento Microsoft (2023), Outsourcing de impressão (2022 /2023), Central de Atendimento ao Usuário (2023), Substituição dos Switches Datacenter e Departamentais, (2022/2023), Oracle (2023) dentre várias outras ações e projetos que requereram o amplo acompanhamento desta Coordenação-Geral, composta até então de somente 4 (quatro) servidores dentro de toda a sua estrutura.

8.6 Assim, com a necessidade de implementação de controles conforme já exposto, em meados de 2024 as tratativas relacionadas a projetos de segurança foram retornadas, estando no escopo atenção especial a contratação de serviços de SOC e análises de Soluções de Gestão de Acesso Privilegiado e ZTNA sendo que durante as tratativas o Órgão foi informado sobre o planejamento

realizado pelo Ministério da Cultura para a contratação de parte das soluções que seriam de interesse do FNDE, em que a contratação daquele Órgão seria realizada mediante Registro de Preço, com a publicação de IRP para a registro de interesse dos demais Órgãos.

8.7 Desta forma, considerando outras dificuldades relacionadas a condução dos processos licitatórios em que, considerando todos os fluxos e tramitações e validações internas no FNDE, historicamente tem demorado mais de 1 ano para a conclusão, foi registrada de forma preliminar a participação em Órgão em alguns itens previstos na Intenção de Registro de Preço - IRP 12 /2024 Registro de Preço nº 12/2024 - UASG 420001 - SPOA/SE/MINC, gerenciada pelo Ministério da Cultura.

8.8 Ressalta-se que por se tratar de um IRP não faz-se obrigatória a contratação futura de todos os itens e quantidades registradas pelo FNDE que poderá, inclusive, vir a dar continuidade ao seu próprio processo na ocorrência de alguma eventualidade da contratação, considerando os termos deste Estudo Técnico Preliminar, bem como ajustes que podem vir a ocorrer neste documento até a efetivação da contratação.

8.9 Em contrapartida sabe-se que a contratação via Registro de Preços de soluções de natureza comum proporciona benefícios para a Administração Pública, como por exemplo: Economia de Tempo, Redução de Custos diretos e indiretos, flexibilidade.

8.9.1 Assim, considerando o exposto acima e a necessidade de maior eficiência, agilidade e celeridade nos processos de contratações de objetos similares e que atenderiam a requisitos básicos e comuns, registra-se que as informações e levantamentos constantes nesse tópico levou em consideração grande parte dos estudos realizados por outros órgãos da Administração Pública Federal, em especial pelo Ministério da Cultura, no qual vem planejando a contratação de soluções de controle e gestão de acesso desde 2023 também por equipe competente igualmente composta por servidores públicos.

8.10 Sob este aspecto destaca-se que a equipe de planejamento focou na análise da compatibilidade da contratação com as necessidades do FNDE e na confirmação dos preços mediante realização de nova pesquisa de preço, a fim de confirmar o atendimento do mercado às especificações do processo e aos preços estimados, com vistas a análise de viabilidade da contratação via o registro de preço proposto, bem como o formato da contratação.

8.4 Gestão de Acessos Privilegiados

8.4.1 *Quanto a análise de disponibilidade de solução similar no portal do software público.*

8.4.1.1 Por meio da pesquisa realizada não foram identificadas soluções de softwares públicos que atenda a essa necessidade.

8.4.1.2 Palavras-chave utilizadas na pesquisa Gestão de Identidade, SSO, PAM, MFA, autenticação. (Fonte: https://softwarepublico.gov.br/social/search/software_infos)

8.4.2 *Quanto a disponibilidade de solução no Catálogo de Soluções de TI da SGD.*

8.4.2.1 Por meio de consulta junto ao portal, não foi identificada a existência de Catálogo de Soluções de TIC contendo acordo de plataforma ou solução similar para o objeto em estudo.

8.4.2.2 Também foi não foi encontrado projeto similar no Cronograma de Projetos.

(Fonte: <https://www.gov.br/governodigital/pt-br/contratacoes/catalogo-de-solucoes-de-tic>)

8.4.3 *Quanto a uso em outros órgãos públicos similares.*

8.4.3.1 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 atendidos com as soluções de mercado identificadas neste estudo técnico.

8.4.3.2 Necessidades similares em outros órgãos ou entidades da Administração Pública e as soluções adotadas/contratações similares.

ÓRGÃO	PREGÃO	DESCRIÇÃO
Superintendência Estadual de Licitações - SUPEL /RO	820/2021	Solução de Gerenciamento de Acessos Privilegiados (Privileged Access Management - PAM)
Agência Nacional de Telecomunicações – ANATEL	25/2021	Solução de PAM (Gerenciamento de Acesso Privilegiado) e Solução de auditoria de serviços Microsoft
Conselho da Justiça Federal	37/2021	Solução, serviços e transferência de conhecimento
Ministério Público do Distrito Federal e Territórios – MPDFT	72/2021	Solução, serviços e transferência de conhecimento
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
Tribunal Superior do Trabalho	58/2021	Registro de preços para aquisição de soluções de segurança, auditoria e prevenção de ameaças.
Tribunal Superior Eleitoral	02/2022	Registro de preços para eventual aquisição de Solução de Gerenciamento de Acessos Privilegiados para dispositivos (ativos de rede, servidores físicos e virtuais e outros sistemas tecnológicos), com capacidade para armazenar, proteger, controlar, gerenciar, auditar e monitorar o acesso privilegiado incluindo serviço de instalação e transferência de conhecimento, consoante especificações, condições, quantidades e prazos constantes do Termo de Referência – Anexo I do Edital.

8.4.4 Disponibilidade de solução disponível no mercado

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

8.4.4.2 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 e possui diversos fabricantes de soluções que podem ser capazes de atender à demanda identificada pela área requisitante, com funcionalidades e modelos distintos.

8.4.4.3 Foram identificadas algumas ferramentas gratuitas e/ou open-source (software livre) para o contexto das soluções, mas, durante análise técnica, elas se mostraram insuficientes para atender a demanda. Seja pela falta de funcionalidades, compatibilidade com requisitos técnicos necessários para o atendimento das demandas ou por requererem demasiado esforço técnico-operacional para customização, dessa forma, foi concluído que há vantagem para o FNDE se as soluções descritas sejam adquiridas nos moldes deste estudo, que para este fim não foram identificadas ferramentas gratuitas/públicas que atendessem a necessidade do FNDE.

8.4.4.4 Um ponto crítico para o sucesso deste projeto é que as revendas das soluções tenham capacidade de entregar os serviços solicitados para o perfeito funcionamento do software.

8.4.4.5 Dessa forma, foi identificada uma grande quantidade de revendas com capacidade e aptidão de fornecer o objeto e prestar os serviços técnicos especializados exigidos e necessários, foram consideradas as seguintes premissas para esta análise:

8.4.4.5.1 Os bens e serviços que compõem a solução pretendida são do segmento de segurança da informação.

8.4.4.5.2 Desta forma, apenas soluções que sejam capazes de monitorar e controlar identidades são capazes de atender plenamente as necessidades identificadas.

8.4.4.5.3 Com objetivo de viabilizar a maior participação de fabricantes e garantir a ampla concorrência concluímos que o processo deve considerar a possibilidade de as revendas ofertarem soluções tecnologias compostas por múltiplos fabricantes.

8.4.4.6 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.

8.4.4.7 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, que atende as necessidades de forma mais eficiente.

8.4.4.8 Diante dos argumentos apresentados, esta equipe de planejamento da contratação entende que a plataforma tecnológica objeto do presente estudo deve ser baseada nos pilares tecnológicos elencados a seguir.

8.4.4.9 Essa orientação tem como objetivo o direcionamento correto das características fundamentais da solução de modo a permitir a contratação de solução de segurança para gerenciamento de identidades e acesso, dos integrantes do SISP.

- **Gerenciamento e proteção para contas privilegiadas com gerenciamento de sessões (PASM):** As contas privilegiadas devem ser protegidas com o cofre de suas credenciais e o acesso a essas contas é então intermediado para usuários humanos, serviços e aplicativos por meio da ferramenta PAM. As funções de gerenciamento de sessão privilegiada (PSM)

estabelecem sessões, geralmente com injeção de credenciais e gravação de sessão completa. As senhas e outras credenciais, como certificados e tokens para contas privilegiadas, são gerenciadas ativamente (por exemplo, sendo alternadas em intervalos definíveis ou na ocorrência de eventos específicos). Opcionalmente, as soluções PASM também podem fornecer gerenciamento de senha de aplicativo para aplicativo (AAPM) e/ou recursos de acesso remoto privilegiado sem instalação para equipe de TI externa e terceiros que não exigem uma VPN.

- **Gerenciamento e proteção de elevação e delegação de privilégios (PEDM):** Os agentes baseados em host no sistema gerenciado concedem privilégios específicos a usuários conectados. As ferramentas PEDM fornecem controle de comando baseado em host (filtragem), controles de permissão/negação/isolamento de aplicativos e/ou elevação de privilégios, o que permite que processos específicos sejam executados com um nível mais alto de privilégios. As ferramentas PEDM devem ser executadas no sistema operacional real (no nível do kernel ou do processo). O controle de comando por meio de filtragem de protocolo é explicitamente excluído dessa definição porque o ponto de controle é menos confiável. As ferramentas PEDM também podem opcionalmente fornecer controles de aplicativos e recursos de monitoramento de integridade de arquivos. As ferramentas PEDM são frequentemente um requisito obrigatório para indústrias regulamentadas e onde a conformidade com PCI-DSS, SOX e outros controles regulatórios e financeiros são estipulados. Ambientes de defesa e governo também exigem a remoção de privilégios de administrador local.
- **Gerenciamento e proteção de segredos:** Credenciais (como senhas, tokens OAuth e chaves SSH) e segredos para software e máquinas são gerenciados, armazenados e recuperados programaticamente por meio de APIs e SDKs. A confiança é estabelecida e intermediada com a finalidade de trocar segredos e gerenciar autorizações e funções relacionadas entre diferentes entidades não humanas, como máquinas, contêineres, aplicativos, serviços, scripts, processos e pipelines de DevSecOps. O gerenciamento de segredos é frequentemente usado em ambientes dinâmicos e ágeis, como IaaS, PaaS e plataformas de gerenciamento de contêineres. Os produtos de gerenciamento de segredos também podem fornecer AAPM.

8.4.5 Identificação das soluções:

8.4.5.1 Foram identificadas algumas soluções open-source (softwares 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.

8.4.5.2 Observando-se as necessidades e os requisitos tecnológicos após o levantamento realizado obteve-se como resultado as seguintes das soluções relacionadas ao gerenciamento de acessos privilegiados:

ID SOLUÇÃO	NOME DA SOLUÇÃO
01	Cyberark
02	Beyond Trust

03	Senha Segura
----	--------------

8.4.5.2.1 Solução de Mercado 01 – Cyberark: A plataforma de segurança de identidade da CyberArk permite acesso seguro para qualquer identidade — humana ou máquina — a qualquer recurso ou ambiente de qualquer lugar, utilizando qualquer dispositivo. 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. (Fonte: <https://www.cyberark.com/products/>)

8.4.5.2.2 Solução de Mercado 02 – Beyond Trust: O fabricante Beyond Trust possui as soluções Password Safe e Privilege Management. Afirma que a plataforma oferece visão completa de todas as identidades, privilégios e acessos para revelar pontos cegos e bloquear ataques em todo o seu ambiente de identidades. (Fonte: <https://www.beyondtrust.com/pt>)

8.4.5.2.3 Solução de Mercado 03 - Senha Segura: O Senha Segura possui as soluções Account and Session PAM Core, Domum acesso remoto, Endpoint PAM Senha Segura Go. Oferece um conjunto abrangente de recursos de PAM. A plataforma PAM se integra perfeitamente a várias tecnologias e sistemas, garantindo acesso. (Fonte: <https://senhasegura.com/pt-br>)

8.4.6 Todo o “estudo dos requisitos tecnológicos” foi considerado para a definição do Caderno de Especificações Técnicas, anexo ao presente documento.

8.4.7 Diante dos levantamentos realizados , pode-se observar que foram apresentadas diversas soluções presentes no mercado para atender a demanda do FNDE.

8.5 Controle de Acesso (ZTNA e SWG)

8.5.1 Selecionar a solução adequada dependerá das necessidades específicas do FNDE, incluindo requisitos de segurança, orçamento e infraestrutura existente.

8.5.2 *Quanto a análise de disponibilidade de solução similar no portal do software público.*

8.5.2.1 Por meio da pesquisa realizada não foram identificadas soluções de softwares públicos que atenda a essa necessidade.

8.5.2.2 Palavras-chave utilizadas na pesquisa Gestão de Acesso, Controle de Acesso, ZTNA, SWG, Acesso remoto. (Fonte: https://softwarepublico.gov.br/social/search/software_infos)

8.5.3 *Quanto a disponibilidade de solução no Catálogo de Soluções de TI da SGD.*

8.5.3.1 Por meio de consulta junto ao portal, não foi identificada a existência de Catálogo de Soluções de TIC contendo acordo de plataforma ou solução similar para o objeto em estudo.

8.5.3.2 Também foi não foi encontrado projeto similar no Catálogo de Soluções de TIC com condições padronizadas do Governo Federal.

(Fonte: <https://www.gov.br/governodigital/pt-br/contratacoes/catalogo-de-solucoes-de-tic>)

8.5.4 *Quanto a uso em outros órgãos públicos similares.*

8.5.4.1 A equipe de planejamento da contratação, mais uma vez, buscou junto ao mercado, contratações, com as seguintes características: Escopo similar ao objeto, similaridades de requisitos negociais e tecnológicos, publicados recentemente e que foram atendidos com as soluções de mercado identificadas neste estudo técnico.

8.5.4.2 Verifica-se que há a prática de contratação destes serviços de subscrição de licenças por outros órgãos conforme exemplos listados a seguir.

ÓRGÃO	PREGÃO	DESCRIÇÃO
Agência Nacional de Transportes Terrestres – ANTT	20/2023	Registro de Preços para eventual contratação de plataforma integrada para proteção de usuários e visibilidade da superfície estendida de ataques, com resolução contínua de vulnerabilidades e priorização e correlação dos eventos de segurança, conforme condições, quantidades e exigências estabelecidas no Edital e seus anexos.
Ministério das Comunicações	10/2023	Contratação de Solução integrada de Segurança Cibernética, contando com gestão de vulnerabilidade, defesa cibernética, resposta incidentes de segurança, incluindo os serviços de segurança da informação especializados em sustentação e implementação de soluções de cibersegurança.
Postal Saúde	09/2023	Contratação de plataforma única para segurança e controle de acesso à internet, aplicações SaaS e privadas, contemplando monitoramento constante da experiência do usuário.

8.5.5 Disponibilidade de solução disponível no mercado

8.5.5.1 Por meio de consulta aos portais dos fabricantes de soluções de gestão de acesso, foram encontradas as seguintes informações de fabricantes de soluções disponíveis no mercado.

ID SOLUÇÃO	NOME DA SOLUÇÃO
01	ZScaler
02	CloudFlare
03	Fortinet
04	Palo Alto Network
05	NetSkope

06

Forcepoint

8.5.5.1.1 Solução de Mercado 01 – Zscaler: Zscaler Private Access (ZPA) é uma solução ZTNA baseada em nuvem que oferece acesso seguro a aplicativos internos sem expor a rede à internet. Utiliza a abordagem de confiança zero para fornecer conexões seguras entre usuários e aplicativos. Zscaler Internet Access (ZIA) é uma plataforma SWG de segurança em nuvem que oferece proteção abrangente contra ameaças web, inspeção SSL e filtragem de conteúdo para garantir uma navegação segura. Baseado em nuvem, segurança web abrangente, inspeção SSL, proteção contra ameaças avançadas. (Fonte: <https://www.zscaler.com.br/products-and-solutions>)

8.5.5.1.2 Solução de Mercado 02 – Cloudflare: A solução ZTNA verifica e protege o acesso de funcionários e terceiros em todos os seus aplicativos auto-hospedados, SaaS e não web, ajudando a mitigar riscos e garantir uma experiência do usuário tranquila. Ele verifica o contexto granular, como a identidade e a postura do dispositivo, para cada solicitação, fornecendo acesso rápido e confiável em toda a sua empresa. Já a solução SWG visibilidade de aproximadamente 20% da web, a escala de rede incomparável da Cloudflare protege a navegação dos funcionários na internet e bloqueia ameaças que causam violações. Simplifique a criação e auditoria de políticas com categorias predefinidas. (Fonte: <https://www.cloudflare.com/pt-br/zerotrust/products/>)

8.5.5.1.3 Solução de Mercado 03 – Fortinet: A Solução ZTNA proporciona acesso seguro e controlado a aplicativos internos e em nuvem, aplicando os princípios de segurança de Zero Trust. A solução é projetada para substituir VPNs tradicionais, oferecendo uma abordagem mais segura e eficiente para o acesso remoto. O SWG oferece proteção abrangente contra ameaças da web, controle de conteúdo e políticas de acesso para proteger os usuários durante a navegação na internet. A solução é projetada para garantir uma navegação segura, prevenindo acessos a sites maliciosos e protegendo contra malware e outras ameaças online. (Fonte: <https://www.fortinet.com/br/solutions/enterprise-midsize-business/unified-sase>)

8.5.5.1.4 Solução de Mercado 04 – Palo Alto Networks: Uma plataforma de segurança em nuvem que fornece acesso seguro e escalável a aplicativos e dados corporativos. Integra-se com outras soluções de segurança da Palo Alto Networks para uma proteção abrangente. Abordagem unificada de segurança, integração com outros produtos Palo Alto, proteção abrangente. (Fonte: <https://www.paloaltonetworks.com.br/sase>)

8.5.5.1.5 Solução de Mercado 05 – Netskope: Projetada para fornecer acesso seguro e contínuo a aplicativos internos, sem a necessidade de VPNs tradicionais. Utiliza a abordagem de confiança zero para garantir que apenas usuários e dispositivos autorizados possam acessar recursos específicos. Solução baseada em nuvem que oferece segurança abrangente para navegação na web e uso de aplicativos na nuvem. Proporciona visibilidade e controle sobre o tráfego web, protegendo contra ameaças cibernéticas e garantindo conformidade com as políticas de segurança. Facilita implementação e escalabilidade sem necessidade de hardware adicional. Minimiza o impacto na produtividade dos usuários. (Fonte: <https://www.netskope.com/pt/products/next-gen-swg>)

8.5.5.1.6 Solução de Mercado 06 – Forcepoint: Oferece acesso seguro a aplicativos internos e na nuvem, eliminando a necessidade de VPNs tradicionais. Baseada nos princípios do modelo de segurança de Zero Trust, a solução garante que o acesso seja concedido apenas a usuários e dispositivos autenticados e autorizados. Fornece proteção contra ameaças avançadas e análise de comportamento para identificar e mitigar riscos. Oferece políticas granulares de controle de acesso e filtragem de conteúdo. Análise de comportamento, proteção contra ameaças avançadas, políticas granulares de controle de acesso.

(Fonte: <https://www.forcepoint.com/product/ztna-zero-trust-network-access> e <https://www.forcepoint.com/product/forcepoint-one-web-security>)

8.5.6 Diante dos levantamentos realizados na pesquisa apresentada acima, pode-se observar que existem diversas soluções presentes no mercado para atender de forma preliminar a necessidade do FNDE.

9. Análise comparativa de soluções

9. Análise Comparativa de soluções

9.1 A análise comparativa de soluções, nos termos do inc. II do art. 11 da IN SGD/ME Nº 94, de 23 de dezembro de 2022 visa a elencar as alternativas de atendimento à demanda considerando, além do aspecto econômico, os aspectos qualitativos em termos de benefícios para o alcance dos objetivos da contratação.

9.2 Em relação às possibilidades em alinhamento ao inciso II do art. 11 da Instrução Normativa SGD /ME nº 94, de 23 de dezembro de 2022, tem-se que:

9.2.1 O Software Público brasileiro não atende o objeto desta contratação.

9.2.2 As políticas, os modelos e os padrões da arquitetura e-PING de Interoperabilidade de Governo Eletrônico não se aplicam nessa contratação, visto que o objeto não abrange serviços disponibilizados pelo governo eletrônico que trabalham conjuntamente com interação e troca de informações.

9.2.3 Não há necessidade de adequação do ambiente do FNDE para viabilizar a execução contratual.

9.2.4 Existe a viabilidade de adesão a uma ata de registro de preços, considerando que há vários produtos disponíveis no mercado e ainda considerando que as contratações de soluções similares são frequentemente realizadas por Órgãos Federais, cabe a realização de pesquisa quanto a disponibilidade de uma Ata de Registro de Preços vigente para adesão, desde que atenda aos requisitos demandados.

9.2.4.1 Sob este aspecto não foi identificada atas da firmadas para os itens da contratação. No entanto, o FNDE encontra-se como partícipe na IRP 12/2024 do Ministério da Cultura.

9.3 Para a realização de análise comparativa entre as soluções, considerando aquelas foram levantadas neste estudo, foram consideradas viáveis as soluções:

- A. Contratação de subscrição de licença software (Software as a Service - SaaS);
- B. Licenciamento por Aquisição/Perpétuo;
- C. Solução gratuita e/ou open-source (Software Livre)

9.4. Assim, considerando as opções apresentadas, são apresentadas as análises referentes às Necessidade de Negócio e Tecnológicas.

9.4.1 Para as Necessidades de Negócio

	Soluções
--	----------

Necessidades de Negócio	A	B	C
Automação e centralização da administração: A TI perde muito tempo revendo o privilégio de acesso dos funcionários para garantir que cada um visualize apenas o permitido.	Atende	Atende	Atende
Acesso remoto seguro: Garante que os colaboradores possam acessar os recursos de forma segura, independentemente da localização.	Atende	Atende	Atende
Prevenção contra malware e ataques cibernéticos: Como órgão do governo, o FNDE pode ser alvo de ataques cibernéticos por diferentes motivos, incluindo espionagem, roubo de informações ou interrupção de serviços, desta forma espera-se que a solução ajude a prevenir infecções por malware e ataques de ransomware, protegendo os dispositivos e a rede contra ameaças cibernéticas. Mitigando dentre outros riscos, os associados a ameaças internas, limitando o acesso dos usuários apenas ao necessário para suas funções.	Atende	Atende	Não Atende
Conformidade regulatória: Considerando que o FNDE está sujeito a regulamentações específicas relacionadas à proteção de dados e segurança da informação, espera-se que a Gestão de Contas e Acessos possa ajudar a garantir a conformidade com essas regulamentações, fornecendo recursos de segurança necessários para limitar o acesso indevido aos dados e sistemas contra violações.	Atende	Atende	Atende
Transferência de conhecimento: A solução deverá ter ainda em sua composição um item para treinamento, para garantir que ocorra a transferência do conhecimento para os servidores e colaboradores que atuam na infraestrutura de TI do FNDE.	Atende	Atende	Não Atende
Implementação assistida: Todos os serviços de instalação e configuração deverão ser executados pela CONTRATADA, de modo a não sobrecarregar a equipe de servidores e colaboradores do FNDE, porém as atividades deverão ser acompanhadas pelos servidores e colaboradores que atuarão na operação da solução após entregue pela CONTRATADA.	Atende	Atende	Não Atende
Escalabilidade: A implantação de uma solução eficiente de Gestão de Acessos torna-se ainda mais crucial com o crescimento do Órgão. A necessidade de acompanhar o aumento do número de usuários, dispositivos e aplicativos, bem como a manutenção e possível ampliação do trabalho remoto por meio do Programa de Gestão do Desempenho (PGD). Assim, solução escolhida deve ser capaz de acompanhar a expansão do Órgão e se adaptar às novas demandas	Atende	Atende	Atende

de segurança, garantindo que todos os acessos sejam devidamente controlados e protegidos.			
Resultado da Análise	Atende	Atende	Não Atende

9.4.2 Necessidades Tecnológicas para Soluções de Gestão de Acessos Privilegiados

Necessidades de Negócio	Soluções		
	A	B	C
Proteção das Informações: <ul style="list-style-type: none"> • Proteção das informações sensíveis e confidenciais contra acessos não autorizados. • Implementação de medidas de segurança contra ataques cibernéticos. • Criptografia de dados em repouso e em trânsito. 	Atende	Atende	Atende
Conformidade e Governança: <ul style="list-style-type: none"> • Atender às exigências das legislações e normas aplicáveis, como LGPD, Lei de Acesso à Informação, e outras. • Ferramentas de verificação de conformidade com regulamentos e normas. • Implementação de políticas de conformidade e governança de identidade. • Capacidade de gerar relatórios de conformidade para auditorias e revisões regulatórias. 	Atende	Atende	Atende
Gestão de Identidades e Acessos: <ul style="list-style-type: none"> • Controles específicos para a gestão de acessos privilegiados. • Implementação e gestão de políticas de acesso baseadas em funções e riscos. • Gestão de permissões e perfis de acesso, inclusive os privilegiados. • Controle de acesso baseado em função (RBAC) e em atributos (ABAC). 	Atende	Atende	Atende

<ul style="list-style-type: none"> • Capacidade de proteção de identidades não humanas em plataformas de containerização 				
Eficiência Operacional: <ul style="list-style-type: none"> • Integração com LDAP, Active Directory, e outros diretórios. • Suporte para integração com sistemas legados e aplicações modernas (via APIs, conectores, etc.). • Integração com serviços de nuvem e ambientes híbridos. • Capacidade de suportar um grande número de usuários e transações. • Suporte técnico contínuo e atualizações regulares. 		Atende	Atende	Atende
Monitoramento e Auditoria: <ul style="list-style-type: none"> • Possibilitar o controle e auditoria dos acessos aos sistemas e dados da instituição. • Relatórios detalhados de acessos e atividades dos usuários. • Prover registros de uso de privilégios e trilhas de auditoria • Capacidade de auditoria completa e geração de logs. 		Atende	Atende	Atende
Segurança Avançada: <ul style="list-style-type: none"> • Suporte para autenticação multifator (Multiple Factor Authentication - MFA). • Autenticação baseada em riscos e contexto. 		Atende	Atende	Atende
Infraestrutura de Identidade: <ul style="list-style-type: none"> • Repositório centralizado de identidades. • Alta disponibilidade e resiliência. 		Atende	Atende	Não Atende
Resultado da Análise		Atende	Atende	Não Atende

9.4.3 Necessidades Tecnológicas para Soluções de Gestão de Acesso (ZTNA e SWG)

	Soluções
--	----------

Necessidades de Negócio	A	B	C
<p>Segurança de Acesso Remoto:</p> <ul style="list-style-type: none"> Proteção das informações sensíveis e confidenciais contra acessos não autorizados. Autenticação contínua e baseada em contexto, verificando a identidade do usuário e a integridade do dispositivo. 	Atende	Atende	Não Atende
<p>Proteção contra Ameaças da Web:</p> <ul style="list-style-type: none"> Bloqueio de sites maliciosos e prevenção de downloads perigosos. Filtragem de conteúdo e políticas de acesso para proteger os usuários durante a navegação na internet. Proteção contra ameaças da web, como malware, phishing e ataques de dia zero. 	Atende	Atende	Não Atende
<p>Visibilidade e Monitoramento:</p> <ul style="list-style-type: none"> Monitoramento contínuo das atividades na web, fornecendo visibilidade completa do tráfego. Relatórios detalhados das atividades de navegação dos usuários. Capacidade de auditoria completa e geração de logs. 	Atende	Atende	Não Atende
<p>Conformidade e Governança:</p> <ul style="list-style-type: none"> Atender às exigências das legislações e normas aplicáveis, como LGPD, Lei de Acesso à Informação, e outras. Ferramentas de verificação de conformidade com regulamentos e normas. Capacidade de gerar relatórios de conformidade para auditorias e revisões regulatórias. 	Atende	Atende	Não Atende
<p>Gestão de Acessos:</p> <ul style="list-style-type: none"> Implementação e gestão de políticas de acesso baseadas em funções e riscos. Controle de acesso granular que garante que os usuários acessem apenas os recursos necessários para suas funções. Automação do provisionamento e desprovisionamento de acessos. 	Atende	Atende	Não Atende

<p>Monitoramento e Auditoria:</p> <ul style="list-style-type: none"> • Possibilitar o controle e auditoria dos acessos aos sistemas e dados da instituição. • Monitoramento contínuo das atividades dos usuários e dispositivos. • Capacidade de auditoria completa e geração de logs detalhados. 	Atende	Atende	Não Atende
<p>Eficiência Operacional:</p> <ul style="list-style-type: none"> • Melhoria da eficiência operacional através da automação de processos de acesso. • Suporte técnico contínuo e atualizações regulares. • Centralização da gestão das políticas de segurança web. • Integração com outros sistemas de segurança e infraestrutura existente. • Interface intuitiva e amigável para administração. 	Atende	Atende	Não Atende
<p>Segurança Avançada:</p> <ul style="list-style-type: none"> • Implementação de medidas de segurança contra-ataques cibernéticos, como detecção de anomalias, resposta a incidentes e inspeção SSL/TLS. • Criptografia de dados em trânsito para proteger as comunicações durante a navegação na web, bem como entre dispositivos e aplicativos. • Suporte para padrões de segurança como SAML, OAuth, OpenID Connect. 	Atende	Atende	Não Atende
<p>Escalabilidade e Desempenho:</p> <ul style="list-style-type: none"> • Capacidade de suportar muitos usuários e transações. • Alta disponibilidade e resiliência. • Desempenho otimizado para minimizar latências e garantir uma experiência de usuário positiva. 	Atende	Atende	Não Atende
<p>Flexibilidade e Customização:</p> <ul style="list-style-type: none"> • Capacidade de personalização para atender às necessidades específicas da instituição. 	Atende	Atende	Não Atende

<ul style="list-style-type: none"> Suporte para workflows personalizados de acesso e políticas de segurança. 			
Resultado da Análise	Atende	Atende	Não Atende

9.5 Considerando, ainda, as informações elencadas no quadro supracitado, de imediato identificamos que as alternativas atendem os requisitos básicos. Dessa maneira além desses quesitos iremos prosseguir na análise dos demais pontos.

9.6 Examina-se nesta seção, para cada solução, os aspectos previstos na IN SGD/ME nº 94/2022 que devem ser avaliados em uma contratação de TIC.

Requisito	Solução	Sim	Não	Não se aplica
A solução encontra-se implantada em outro órgão ou entidade da Administração Pública?	Solução A	X		
	Solução B		X	
	Solução C		X	
A solução está disponível no Portal do Software Público Brasileiro?	Solução A			X
	Solução B			X
	Solução C			X
A solução é composta por software livre ou software público?	Solução A		X	
	Solução B		X	

	Solução C	X		
A solução é aderente às políticas, premissas e especificações técnicas definidas pelos Padrões de governo ePing, eMag e ePWG?	Solução A			X
	Solução B			X
	Solução C			X
A solução é aderente às regulamentações da ICP-Brasil?	Solução A			X
	Solução B			X
	Solução C			X
A solução é aderente às orientações, premissas e especificações técnicas e funcionais do e-ARQ Brasil?	Solução A			X
	Solução B			X
	Solução C			X

9.7 Considerando que as soluções em estudo possuem possibilidade de atender a demanda, foi verificado os cenários relacionados aos tipos de licenciamentos praticados no mercado, conforme os pontos positivos e negativos a seguir:

9.7.1 Licenciamento Perpétuo:

9.7.1.1 Pontos Positivos:

- **Custo Único:** O pagamento é feito uma vez, e a solução pode ser usada indefinidamente, o que pode ser mais econômico a longo prazo, especialmente para organizações que planejam usar a solução por muitos anos.
- **Propriedade Permanente:** A organização possui a licença permanentemente, o que pode proporcionar maior controle sobre os custos e o ciclo de vida da solução.

- **Flexibilidade:** Pode ser mais flexível em termos de implantação e integração com outras ferramentas de segurança, pois não está vinculado a um contrato de assinatura.

9.7.1.2 Pontos Negativos:

- **Custo Inicial Elevado:** o custo inicial de aquisição pode ser significativamente maior do que o licenciamento anual ou por subscrição, o que pode ser um desafio para esta Pasta, além disso corre-se o risco de haver um pagamento por produtos que não sejam necessários depois de algum tempo, caso ocorra uma redução do parque ou migração de soluções.
- **Atualizações e Suporte:** normalmente, o suporte e as atualizações estão disponíveis por um período limitado após a compra inicial, e podem exigir custos adicionais para estender esses serviços.
- **Menos Flexibilidade de Atualização:** Pode ser mais difícil e caro atualizar para versões mais recentes da solução, pois pode exigir a compra de atualizações ou migrações adicionais.

9.7.2 Licenciamento Anual/ Subscrição por doze (12) meses:

9.7.2.1 Pontos Positivos:

- **Custo Anual Previsível:** O custo é distribuído ao longo do tempo, facilitando o planejamento financeiro e eliminando o alto custo inicial associado ao licenciamento perpétuo.
- **Atualizações e Suporte Incluídos:** Geralmente inclui suporte técnico e atualizações de software
- **Maior Flexibilidade:** Permite uma maior flexibilidade para ajustar o número de licenças conforme as necessidades da organização mudam ao longo do tempo.

9.7.2.2 Pontos Negativos:

- **Custo Total a Longo Prazo:** Pode ser mais caro a longo prazo do que o licenciamento perpétuo, especialmente se a solução for usada por muitos anos.
- **Dependência Contínua:** A organização fica continuamente dependente do fornecedor para suporte e atualizações, e a interrupção do pagamento pode resultar na perda de acesso à solução.
- **Falta de Propriedade:** A organização não possui a licença permanentemente e pode perder o acesso à solução se não renovar a licença anualmente.

9.8 Considerando que ambas as soluções em estudo possuem possibilidade de atender a demanda, após a análise dos tipos de licenciamentos praticados no mercado, esta equipe de planejamento da contratação, entende razoável a escolha da contratação no modelo de **subscrição de licenças** por doze (12) meses.

Destaca-se que este modelo de licenciamento tem sido o mais praticado pela Administração Pública, a exemplo de quase todos os contratos de soluções da DIRT/CGINF que tem sido no formato de Subscrição.

10. Registro de soluções consideradas inviáveis

10. Registro de soluções consideradas inviáveis

10.1 Com base na análise anterior foram consideradas com inviáveis considerando aspectos econômicos e/ou técnicos.

10.1.1 SOLUÇÃO B: Licenciamento por Aquisição/Perpétuo

10.1.1.1 A proposta dessa alternativa representa a modalidade de licenciamento em que se adquire de forma vitalícia a solução de software.

10.1.1.2 Nesta modalidade o Contratante adquire as licenças de software de forma perpétua, porém verifica-se como prática que não há o fornecimento perpétuo das atualizações das licenças, ou seja, mesmo que se tenha as licenças perpétuas, necessitam de atualizações, para que funcionem de forma correta, neste sentido os riscos de: dependência de um único fornecedor; limitação da concorrência quando da análise de renovações contratuais, tornam este tipo de licenciamento inviável.

10.1.1.3 Neste sentido, as características do modelo de licenciamento por aquisição são extremamente rígidas e não permitem modificações.

10.1.1.4 Resumidamente, nesse tipo de contratação, há o risco de aquisição de licenças e de serviços agregados, que podem ser ou não utilizados, afetando com isso a economicidade da contratação, além de gerar gastos com produtos não utilizados, uma vez que essas licenças são pagas de forma antecipada e na modalidade à vista. Nesse sentido, trecho do entendimento esposado pelo TCU, no Acórdão 2569/2018 – Plenário, no qual recomenda a aquisição de licenças pontuais que atendam a demanda do órgão, visando a redução dos riscos na contratação, senão vejamos:

“...adquiram quantitativo de licenças estritamente necessário, vedando-se o pagamento antecipado por licenças de software, vinculando o pagamento dos serviços agregados às licenças efetivamente utilizadas, principalmente em projetos considerados de alto risco ou de longo prazo, nos quais o quantitativo deve ser atrelado à evolução do empreendimento, e devidamente documentado nos estudos técnicos preliminares, podendo ser utilizado o Sistema de Registro de Preço, que viabiliza o ganho de escala na compra ao mesmo tempo que proporciona a aquisição no momento oportuno”

10.1.1.5 Desta forma conclui-se que a presente alternativa é tecnicamente inviável.

10.1.2 SOLUÇÃO C: Solução gratuita e/ou open-source (Software Livre)

10.1.2.1 Não há disponibilidade de solução de software livre capaz de Software Livre atender aos requisitos técnicos nesse contexto. Esta solução apresenta alta complexidade, pois necessita de capacitação permanente da equipe de informática, falta de suporte técnico, baixa. Assim, esta opção está aos poucos sendo substituída por ferramentas pagas com suporte, gerenciamento unificado e garantia de funcionamento.

11. Análise comparativa de custos (TCO)

11. Análise Comparativa de Custos (TCO)

11.1 Da Pesquisa de Preço

11.1.1 Estando, portanto, dispensada a realização dos respectivos cálculos de custo total de propriedade - TCO (§1º do art. 11 da IN 94/2022 da SGD/ME) para as soluções B e C, conforme registrado no item 10 (Registro de Soluções Consideradas Inviáveis), passa-se, agora, para a pesquisa de mercado, que segue as determinações da Instrução Normativa nº 65 (IN 65/2021), de 07 de julho de 2021, sobre o procedimento administrativo para a realização de pesquisa de preços para aquisição de bens e contratação de serviços em geral, no âmbito da administração pública federal direta, autárquica e fundacional, e que trata dos aspectos da nova lei de licitações, Lei nº 14.133, de 1º de abril de 2021.

11.1.2 Conforme a IN 65/2021, a pesquisa deve prioritariamente ser realizada pelo Painel de Preços disponível no endereço eletrônico e/ou <http://paineldeprecos.planejamento.gov.br>, previsão do art. 5º da referida IN:

"Art. 5º A pesquisa de preços para fins de determinação do preço estimado em processo licitatório para a aquisição de bens e contratação de serviços em geral será realizada mediante a utilização dos seguintes parâmetros, empregados de forma combinada ou não:

I - composição de custos unitários menores ou iguais à mediana do item ou banco de correspondente nos sistemas oficiais de governo, como Painel de Preços preços em saúde, observado o índice de atualização de preços correspondente;

II - contratações similares feitas pela Administração Pública, em execução ou, inclusive concluídas no período de 1 (um) ano anterior à data da pesquisa de preços mediante sistema de registro de preços, observado o índice de atualização de preços correspondente;

III - dados de pesquisa publicada em mídia especializada, de tabela de referência formalmente aprovada pelo Poder Executivo federal e de sítios eletrônicos especializados ou de domínio amplo, desde que atualizados no momento da pesquisa e compreendidos no intervalo de até 6 (seis) meses de antecedência da data de divulgação do edital, contendo a data e a hora de acesso;

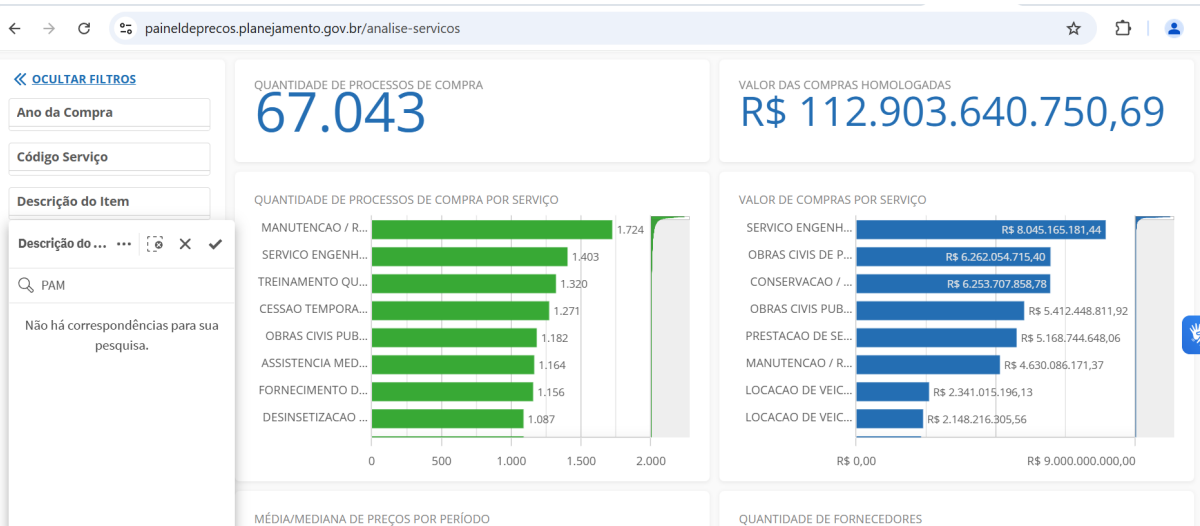
IV - pesquisa direta com, no mínimo, 3 (três) fornecedores, mediante solicitação formal de cotação, por meio de ofício ou e-mail, desde que seja apresentada justificativa da escolha desses fornecedores e que não tenham sido obtidos os orçamentos com mais de 6 (seis) meses de antecedência da data de divulgação do edital; ou

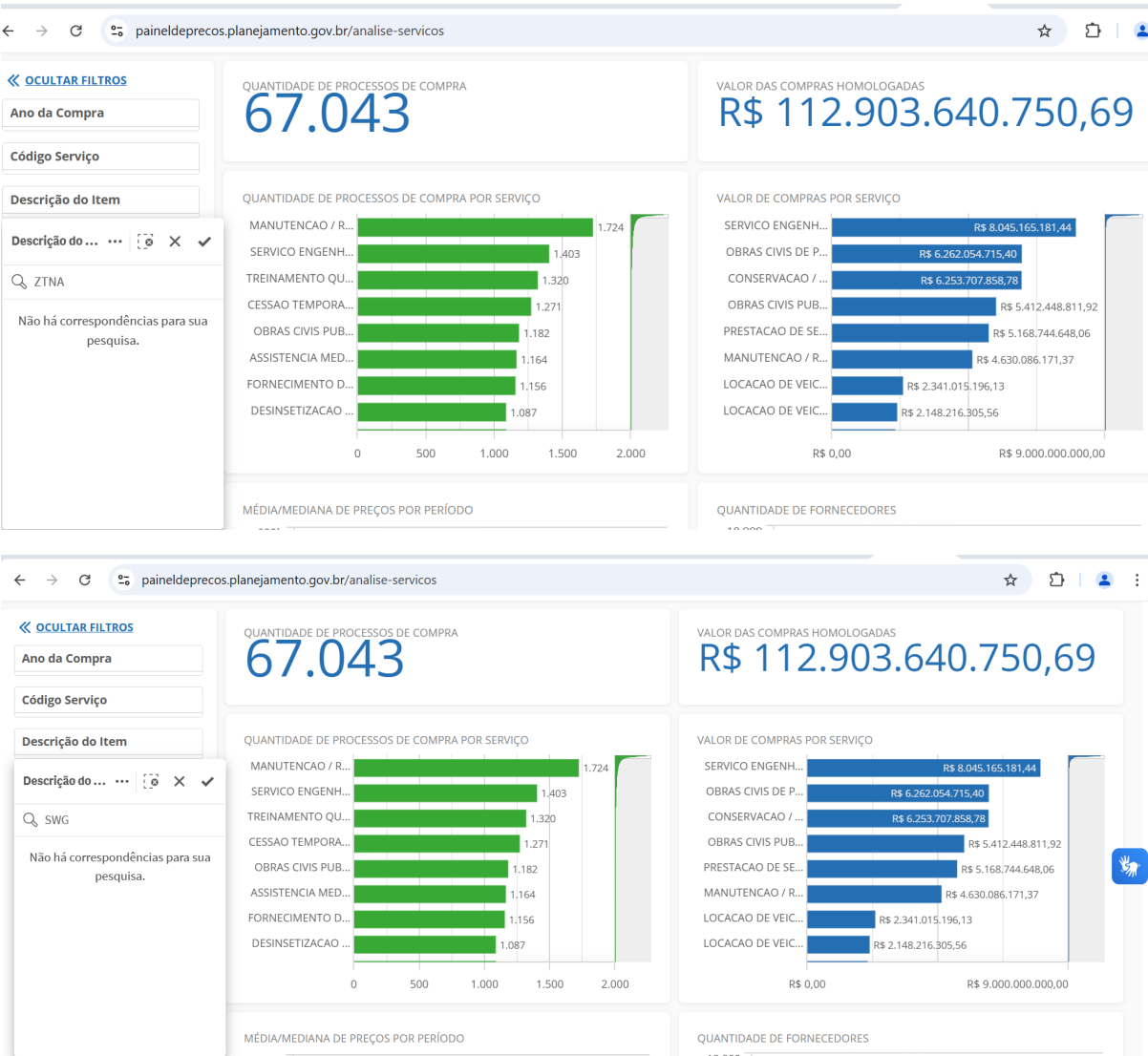
V - pesquisa na base nacional de notas fiscais eletrônicas, desde que a data das notas fiscais esteja compreendida no período de até 1 (um) ano anterior à data de divulgação do edital, conforme disposto no Caderno de Logística, elaborado pela Secretaria de Gestão da Secretaria Especial de Desburocratização, Gestão e Governo Digital do Ministério da Economia.

§ 1º Deverão ser priorizados os parâmetros estabelecidos nos incisos I e II, devendo, "em caso de impossibilidade, apresentar justificativa nos autos

11.2. - Do Painel de Preços e Contratações Similares

11.2.1 Em atendimento ao presente disposto no inciso I e II do Art. 5 da referida IN, foi realizada pesquisa de preços no Painel de Preços da Administração Pública Federal para verificar contratações similares em execução ou concluídos nos 12 (doze) meses anteriores à data da pesquisa de preços utilizando seguintes filtros aplicados: Palavras Chaves: Solução de Gestão de Acessos. Código Material 27502, Ano da Compra 2024 e 2025, Esfera Federal, Objeto da Compra: Solução de Gestão de Acesso Privilegiados; PAM, ZTNA, SWG, após isso, foram consideradas apenas as contratações na Modalidade Pregão. Da pesquisa realizada não foi encontrado o contratações similares.





113.2.2 Dessa forma, de forma a ampliar a pesquisa de pesquisa, optou-se para pesquisa ampla junto ao mercado privado.

11.3 - Da pesquisa de preço no mercado

11.3.1 Devido à particularidade deste objeto e visando justificar um preço mais adequado ao objeto a ser contratado pelo FNDE, foi necessário realizar a pesquisa com fornecedores, seguindo o determinado pela INSEGES/ME nº 65, de 7 de julho de 2021 que dispõe sobre o procedimento administrativo para a realização de pesquisa de preços para aquisição de bens e contratação de serviços em geral, no âmbito da administração pública federal direta, autárquica e fundacional, a pesquisa de preços será realizada via pesquisa direta com fornecedores, conforme determina o inciso IV do art.5º:"

Art. 5º A pesquisa de preços para fins de determinação do preço estimado em processo licitatório para a aquisição de bens e contratação de serviços em geral será realizada mediante a utilização dos seguintes parâmetros, empregados de forma combinada ou não:

I - composição de custos unitários menores ou iguais à mediana do item correspondente nos sistemas oficiais de governo, como Painel de Preços ou banco de preços em saúde, observado o índice de atualização de preços correspondente;

II - contratações similares feitas pela Administração Pública, em execução ou concluídas no período de 1 (um) ano anterior à data da pesquisa de preços, inclusive mediante sistema de registro de preços, observado o índice de atualização de preços correspondente;

III - dados de pesquisa publicada em mídia especializada, de tabela de referência

IV - pesquisa direta com, no mínimo, 3 (três) fornecedores, mediante solicitação formal de, desde que seja apresentada justificativa da escolha cotação, por meio de ofício ou e-mail desses fornecedores e que não tenham sido obtidos os orçamentos com mais de 6 (seis) meses de antecedência da data de divulgação do edital; ou

V - pesquisa na base nacional de notas fiscais eletrônicas, desde que a data das notas fiscais esteja compreendida no período de até 1 (um) ano anterior à data de divulgação do edital, conforme disposto no Caderno de Logística, elaborado pela Secretaria de Gestão d a Secretaria Especial de Desburocratização, Gestão e Governo Digital do Ministério (grifo nosso)

11.3.2 Ainda de acordo com a IN 65/2021, a pesquisa com os fornecedores deverá se atentar ao §2º do art. 5º:

"Art. 5º

(...)§ 2º Quando a pesquisa de preços for realizada com fornecedores, nos termos do inciso IV, deverá ser observado:

I - prazo de resposta conferido ao fornecedor compatível com a complexidade do objeto a ser licitado;

II - obtenção de propostas formais, contendo, no mínimo:

a) descrição do objeto, valor unitário e total;

b) número do Cadastro de Pessoa Física - CPF ou do Cadastro Nacional de Pessoa Jurídica- CNPJ do proponente;

c) endereços físico e eletrônico e telefone de contato;

d) data de emissão; e

e) nome completo e identificação do responsável.

III - informação aos fornecedores das características da contratação contidas no art. 4º, com vistas à melhor caracterização das condições comerciais praticadas para o objeto a ser contratado; e

IV - registro, nos autos do processo da contratação correspondente, da relação de

11.3.3. Visando realizar a pesquisa de preços com os fornecedores se baseando na IN 65/2021, foi realizado uma pesquisa direta mediante solicitação formal via e-mail, com 10 (dez) fornecedores, dos quais, todos os 7 (sete) responderam, a citar: 3Structure IT Ltda, 5IT Instituto Tecnológico, CLM Software Comércio Importação e Exportação Ltda, Dfense Security Tecnologia da Informação Ltda

Garage Tech, Global Sec. Tecnologia & Informação Ltda, Shield Security Tecnologia Ltda., conforme o processo 23034.039474/2024-35.

11.3.4. A tabela a seguir apresenta a compilação das propostas recebidas dos fornecedores visando calcular o TCO das propostas:

Parâmetro	Empresa	Grupo	Item	Especificação	CATSER	Métrica	Qtde	Valor Unitário	Valor Total
IV	3Structure IT Ltda	1	1	Subscrição para solução de segurança para identidades e acessos - Monitoramento comportamental e mitigação de riscos das identidades privilegiadas.	27502	Usuários	100	R\$ 8.204,00	R\$ 820.400,00
			2	Subscrição para solução de Segurança para Armazenamento de Credenciais.	27502	Usuários	1900	R\$ 421,00	R\$ 799.900,00
			3	Serviços de Instalação e Configuração das Soluções (por item / módulo)	26972	Serviço	2	R\$ 104.300,00	R\$ 208.600,00
			4	Serviço de treinamento / capacitação por (item / módulo)	3840	Turma	2	R\$ 130.280,00	R\$ 260.560,00
		2	5	Serviço de acesso remoto confiança zero (ZTNA)	27502	Usuários	400	R\$ 958,00	R\$ 383.200,00
			6	Serviço de acesso seguro interno/externo (SWG)	27502	Usuários	1900	R\$ 2.900,00	R\$ 5.510.000,00
			7	Serviços de Instalação e Configuração das Soluções (por item / módulo)	26972	Serviço	2	R\$ 208.035,00	R\$ 416.070,00
			8	Serviço de treinamento / capacitação (por item / módulo)	3840	Turma	2	R\$ 286.739,00	R\$ 573.478,00
									R\$ 8.972.208,00
Parâmetro	Empresa	Grupo	Item	Especificação	CATSER	Métrica	Qtde	Valor Unitário	Valor Total
		1	1	Subscrição para solução de segurança para identidades e acessos - Monitoramento comportamental e mitigação de riscos das identidades privilegiadas.	27502	Usuários	100	R\$ 9.805,35	R\$ 980.535,00
			2	Subscrição para solução de Segurança para Armazenamento de	27502	Usuários	1900	R\$ 474,02	R\$ 900.638,00

IV	5IT Instituto Tecnológico	2		Credenciais.					
			3	Serviços de Instalação e Configuração das Soluções (por item / módulo)	26972	Serviço	2	R\$ 148.000,00	R\$ 296.000,00
			4	Serviço de treinamento / capacitação por (item / módulo)	3840	Turma	2	R\$ 125.000,00	R\$ 250.000,00
			5	Serviço de acesso remoto confiança zero (ZTNA)	27502	Usuários	400		
		6	Serviço de acesso seguro interno/externo (SWG)	27502	Usuários	1900			
		7	Serviços de Instalação e Configuração das Soluções (por item / módulo)	26972	Serviço	2			
		8	Serviço de treinamento / capacitação (por item / módulo)	3840	Turma	2			
									R\$ 2.427.173,00
Parâmetro	Empresa	Grupo	Item	Especificação	CATSER	Métrica	Qtde	Valor Unitário	Valor Total
IV	CLM Software Comércio Importação e Exportação Ltda	1	1	Subscrição para solução de segurança para identidades e acessos - Monitoramento comportamental e mitigação de riscos das identidades privilegiadas.	27502	Usuários	100		
			2	Subscrição para solução de Segurança para Armazenamento de Credenciais.	27502	Usuários	1900		
			3	Serviços de Instalação e Configuração das Soluções (por item / módulo)	26972	Serviço	2		
			4	Serviço de treinamento / capacitação por (item / módulo)	3840	Turma	2		
		2	5	Serviço de acesso remoto confiança zero (ZTNA)	27502	Usuários	400	R\$ 1.420,00	R\$ 568.000,00
			6	Serviço de acesso seguro interno/externo (SWG)	27502	Usuários	1900	R\$ 1.930,00	R\$ 3.667.000,00
			7	Serviços de Instalação e Configuração das Soluções (por item / módulo)	26972	Serviço	2	R\$ 350.000,00	R\$ 700.000,00
			8	Serviço de treinamento / capacitação (por item / módulo)	3840	Turma	2	R\$ 305.200,00	R\$ 610.400,00
									R\$ 5.545.400,00
		Parâmetro	Empresa	Grupo	Item	Especificação	CATSER	Métrica	Qtde

IV	Dfense Security Tecnologia da Informação Ltda	1	1	Subscrição para solução de segurança para identidades e acessos - Monitoramento comportamental e mitigação de riscos das identidades privilegiadas.	27502	Usuários	100		
			2	Subscrição para solução de Segurança para Armazenamento de Credenciais.	27502	Usuários	1900		
			3	Serviços de Instalação e Configuração das Soluções (por item / módulo)	26972	Serviço	2		
			4	Serviço de treinamento / capacitação por (item / módulo)	3840	Turma	2		
		2	5	Serviço de acesso remoto confiança zero (ZTNA)	27502	Usuários	400	R\$ 1.189,45	R\$ 475.780,00
			6	Serviço de acesso seguro interno/externo (SWG)	27502	Usuários	1900	R\$ 1.789,32	R\$ 3.399.708,00
			7	Serviços de Instalação e Configuração das Soluções (por item / módulo)	26972	Serviço	2	R\$ 279.250,90	R\$ 558.501,80
			8	Serviço de treinamento / capacitação (por item / módulo)	3840	Turma	2	R\$ 279.890,35	R\$ 559.780,70
									R\$ 4.993.770,50
Parâmetro	Empresa	Grupo	Item	Especificação	CATSER	Métrica	Qtde	Valor Unitário	Valor Total
IV	Garage Tech	1	1	Subscrição para solução de segurança para identidades e acessos - Monitoramento comportamental e mitigação de riscos das identidades privilegiadas.	27502	Usuários	100	R\$ 9.014,48	R\$ 901.448,00
			2	Subscrição para solução de Segurança para Armazenamento de Credenciais.	27502	Usuários	1900	R\$ 462,67	R\$ 879.073,00
			3	Serviços de Instalação e Configuração das Soluções (por item / módulo)	26972	Serviço	2	R\$ 128.777,63	R\$ 257.555,26
			4	Serviço de treinamento / capacitação por (item / módulo)	3840	Turma	2	R\$ 162.485,91	R\$ 324.971,82
			5	Serviço de acesso remoto confiança zero (ZTNA)	27502	Usuários	400		
			6	Serviço de acesso seguro interno/externo (SWG)	27502	Usuários	1900		
				Serviços de Instalação e					

		2	7	Configuração das Soluções (por item / módulo)	26972	Serviço	2		
			8	Serviço de treinamento / capacitação (por item / módulo)	3840	Turma	2		
									R\$ 2.363.048,08
Parâmetro	Empresa	Grupo	Item	Especificação	CATSER	Métrica	Qtde	Valor Unitário	Valor Total
IV	Global Sec. Tecnologia & Informação Ltda	1	1	Subscrição para solução de segurança para identidades e acessos - Monitoramento comportamental e mitigação de riscos das identidades privilegiadas.	27502	Usuários	100		
			2	Subscrição para solução de Segurança para Armazenamento de Credenciais.	27502	Usuários	1900		
			3	Serviços de Instalação e Configuração das Soluções (por item / módulo)	26972	Serviço	2		
			4	Serviço de treinamento / capacitação por (item / módulo)	3840	Turma	2		
		2	5	Serviço de acesso remoto confiança zero (ZTNA)	27502	Usuários	400	R\$ 1.254,40	R\$ 501.760,00
			6	Serviço de acesso seguro interno/externo (SWG)	27502	Usuários	1900	R\$ 1.845,90	R\$ 3.507.210,00
			7	Serviços de Instalação e Configuração das Soluções (por item / módulo)	26972	Serviço	2	R\$ 274.500,00	R\$ 549.000,00
			8	Serviço de treinamento / capacitação (por item / módulo)	3840	Turma	2	R\$ 293.550,00	R\$ 587.100,00
									R\$ 5.145.070,00
Parâmetro	Empresa	Grupo	Item	Especificação	CATSER	Métrica	Qtde	Valor Unitário	Valor Total
		1	1	Subscrição para solução de segurança para identidades e acessos - Monitoramento comportamental e mitigação de riscos das identidades privilegiadas.	27502	Usuários	100		
			2	Subscrição para solução de Segurança para Armazenamento de Credenciais.	27502	Usuários	1900		
			3	Serviços de Instalação e Configuração das Soluções (por item /	26972	Serviço	2		

IV	Shield Security Tecnologia Ltda			módulo)					
		4	Serviço de treinamento / capacitação por (item / módulo)	3840	Turma	2			
		2	5	Serviço de acesso remoto confiança zero (ZTNA)	27502	Usuários	400	R\$ 1.098,50	R\$ 439.400,00
			6	Serviço de acesso seguro interno/externo (SWG)	27502	Usuários	1900	R\$ 1.881,90	R\$ 3.575.610,00
			7	Serviços de Instalação e Configuração das Soluções (por item / módulo)	26972	Serviço	2	R\$ 233.567,00	R\$ 467.134,00
			8	Serviço de treinamento / capacitação (por item / módulo)	3840	Turma	2	R\$ 282.350,00	R\$ 564.700,00
									R\$ 5.046.844,00

11.3.4.5 Os documentos da pesquisa de preço realizada pelo FNDE e a planilha consolidada das respostas encontram-se nos Anexos III e IV

11.4 Da identificação da Intenção de Registro de Preços compatível

11.4.1 Conforme já exposto, considerando a Intenção de Registro de Preço nº 12/2024 - UASG 420001 - SPOA/SE/MINC, gerenciada pelo Ministério da Cultura, tem-se que os itens **03, 04, 10 e 11 do Grupo 1** (itens 01, 02, 03 e 04 constante na tabela acima) bem como os **itens 12, 13, 14 e 15 do Grupo 2** (itens 05, 06, 07 e 08 constante na tabela acima) supririam as necessidades e requisitos do FNDE.

11.4.2 Verifica-se que há compatibilidade do objeto da intenção de registro de preço do Ministério da Cultura. Neste sentido o FNDE, deliberou na conveniência da sua participação conforme preconiza o art. 10 do Decreto 11.462/2023 abaixo.

Art. 10. Os órgãos e as entidades de que trata o art. 1º, antes de iniciar processo licitatório ou contratação direta, consultarão as IRPs em andamento e deliberarão a respeito da conveniência de sua participação.

11.4.3 Diante dos valores a serem registrados passamos a verificação da vantajosidade econômica na adesão, conforme descrito abaixo.

11.5 Da Metodologia do Preço Estimado

11.5.1 Conforme orienta o §3º do Art. 1º e Art. 6º da IN nº 65, de 07 de julho de 2021, na metodologia para obtenção do preço estimado deve-se observar os seguintes métodos:

"Art. 1º Esta Instrução Normativa dispõe sobre o procedimento administrativo para a realização de pesquisa de preços para aquisição de bens e contratação de serviços em geral, no âmbito da administração pública federal direta, autárquica e fundacional.

(...)

§ 3º Para aferição da vantagem econômica das adesões às atas de registro de preços, bem como da contratação de item específico constante de grupo de itens em atas de registro de preços, deverá ser observado o disposto nesta Instrução Normativa."

(...)

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

11.5.2 No presente caso, foi utilizada como método para obtenção do preço estimado o menor dos valores obtidos na pesquisa de preços, visto que o cálculo incide sobre um conjunto de três ou mais preços, oriundos de um dos parâmetros de que trata o art. 5º da IN nº 65, de 07 de julho de 2021, conforme metodologia abaixo:

11.5.2.1 Coleta de preços unitários utilizando contratações similares consultadas nos sistemas oficiais de governo;

11.5.2.2 Coleta de preços unitários utilizados em contratações similares com a administração pública;

11.5.2.3 Coleta de preços unitários de fornecedores.

11.5.2.4 Montagem de planilha contendo os preços unitários obtidos nos passos acima, conforme apresentado no Mapa Comparativo de Preços (Anexo IV);

11.5.2.5 Análise crítica dos preços unitários obtidos em cada item que compõem as planilhas, a fim de tratar as variações de preços encontradas na pesquisa, nos termos do §4º, do artigo 6º, da IN nº 65, de 07 de julho de 2021. Neste caso, conforme demonstrado, foram encontradas variações nos custos dos serviços de instalação e configuração das soluções bem como de treinamento / capacitação, que classificam os objetos como consistentes em relação ao objeto da contratação, os quais foram considerados tendo em vista os procedimentos técnicos utilizadas pelas empresas.

11.5.3 Considerando os métodos estatísticos média simples e mediana, a Tabela a seguir apresenta os resultados.

Grupo	Item	Especificação	CATSER	Métrica	Qtde	Média	Mediana	Menor Preço
1	1	Subscrição para solução de segurança para identidades e acessos - Monitoramento comportamental e mitigação de riscos das identidades privilegiadas.	27502	Usuários	100	R\$ 9.007,94	R\$ 9.014,48	R\$ 8.204,00
	2	Subscrição para solução de Segurança para Armazenamento de Credenciais.	27502	Usuários	1900	R\$ 452,56	R\$ 462,67	R\$ 421,00

	3	Serviços de Instalação e Configuração das Soluções (por item / módulo)	26972	Serviço	2	R\$ 127.025,88	R\$ 128.777,63	R\$ 104.300,00
	4	Serviço de treinamento / capacitação por (item / módulo)	3840	Turma	2	R\$ 139.255,30	R\$ 130.280,00	R\$ 125.000,00
2	5	Serviço de acesso remoto confiança zero (ZTNA)	27502	Usuários	400	R\$ 1.184,07	R\$ 1.189,45	R\$ 958,00
	6	Serviço de acesso seguro interno/externo (SWG)	27502	Usuários	1900	R\$ 2.069,42	R\$ 1.881,90	R\$ 1.1789,32
	7	Serviços de Instalação e Configuração das Soluções (por item / módulo)	26972	Serviço	2	R\$ 269.070,58	R\$ 274.500,00	R\$ 208.035,00
	8	Serviço de treinamento / capacitação (por item / módulo)	3840	Turma	2	R\$ 289.545,87	R\$ 286.739,00	R\$ 279.890,35

11.5.4 Considerando os valores unitários exibidos, a Tabela a seguir consolida os valores totais da propensa contratação para 12 meses levando em consideração os valores constante na Intenção de Registro de Preço nº 12/2024 - UASG 420001 - SPOA/SE/MINC, gerenciada pelo Ministério da Cultura.

Grupo	Item	Especificação	CATSER	Métrica	Qtde	Valor Unitário	Valor Total
1	1	Subscrição para solução de segurança para identidades e acessos - Monitoramento comportamental e mitigação de riscos das identidades privilegiadas.	27502	Usuários	100	R\$ 8.204,00	R\$ 820.400,00
	2	Subscrição para solução de Segurança para Armazenamento de Credenciais.	27502	Usuários	1900	R\$ 397,06	R\$ 754.414,00

	3	Serviços de Instalação e Configuração das Soluções (por item / módulo)	16972	Serviço	2	R\$ 104.300,00	R\$ 208.600,00
	4	Serviço de treinamento / capacitação por (item / módulo)	3840	Turma	2	R\$ 125.000,00	R\$ 250.000,00
2	5	Serviço de acesso remoto confiança zero (ZTNA)	27502	Usuários	400	R\$ 1.046,00	R\$418.400,00
	6	Serviço de acesso seguro interno /externo (SWG)	27502	Usuários	1900	R\$ 1.617,00	R\$ 3.072.300,00
	7	Serviços de Instalação e Configuração das Soluções (por item / módulo)	16972	Serviço	2	R\$ 208.035,00	R\$ 416.070,00
	8	Serviço de treinamento / capacitação (por item / módulo)	3840	Turma	2	R\$ 183.723,40	R\$ 367.446,80
							R\$ 6.307.630,80

11.5.5. Conforme consta no Mapa de Pesquisa de Preço (Anexo IV) o Menor Preço apresenta valores compatíveis com os preços de mercado e estão de acordo com os constantes na Intenção de Registro de Preço nº 12/2024 - UASG 420001 - SPOA/SE/MINC, a ser gerenciada pelo Ministério da Cultura.

11.5.6 Por meio da análise dos resultados da pesquisa de preços é possível inferir que há mais de um fabricante capaz de atender a demanda e que não há exclusividade para a venda de qualquer um dos produtos dos fabricantes, fato que torna clara a viabilidade da realização de um pregão para a realização da licitação.

11.5.7 Destaca-se que foi mantido o menor preço obtido na pesquisa.

12. Descrição da solução de TIC a ser contratada

12. Descrição da solução de TIC a ser contratada

12.1 A contratação da solução constante do objeto dar-se-á por meio de Intenção de Registro de Preço nº 12/2024 - UASG 420001 - SPOA/SE/MINC, gerenciada pelo Ministério da Cultura de Preço nº 12/2024. Os itens do objeto serão licitados e adjudicados por grupo pelo Órgão Gerenciador considerando indivisibilidade deles, uma vez que os serviços são de uma mesma

natureza, que guardam correlação entre si, seja por similaridade técnica ou de tecnologia, fatores que os tornam partes de uma solução de tecnologia da informação.

12.2 Nos levantamentos realizados constatou-se como conveniente e/ou oportuna a contratação da solução no formato de serviço (SaaS/Subscrição) tendo como características positivas e premissas:

- *Toda a necessidade atual e futura de licenças de software precisa estar descrita na formalização do contrato;*
- *O pagamento é feito quando do aceite da entrega dos produtos em parcela única para a vigência de doze (12) meses;*
- *O dimensionamento pode ser ajustado ao longo dos anos;*
- *Qualquer atualização tecnológica já está contemplada neste modelo de licenciamento*
- *Todas as soluções tecnológicas disponíveis no modelo de licenciamento perpétuo também estão disponíveis para o modelo de subscrição;*
- *O gasto no processo de assinatura é de custeio; e*
- *Gestão simplificada.*

12.3 O presente modelo se notabiliza por pagar pelo serviço da licença durante o período que o FNDE julgar necessário obtendo os benefícios e entregáveis planejados. Caso chegue o momento que determinada solução está defasada e/ou não faça mais sentido o FNDE poderá deixar este licenciamento de lado visto que a contratação se dá por um modelo de prestação de serviços. Desta forma conclui-se que a presente alternativa é tecnicamente viável.

12.4 É importante registrar a necessidade de contratação do serviço de instalação, implantação dos softwares, garantia técnica e transferência de conhecimento necessários à plena operação da solução considerando as etapas já mapeadas pelo Órgão Gerenciador e demais condições de atendimento, incluindo-se os tempos de suporte, em que este FNDE encontra-se de acordo com o planejado.

13. Estimativa de custo total da contratação

Valor (R\$): 6.307.630,80

13. Estimativa de custo Total da Contratação

13.1 Diante do levantamento das informações por meio da pesquisa de preços, restou verificado que o custo estimado dos serviços no primeiro período de doze (12) meses é de R\$ **6.307.630,80 (seis milhões e trezentos e sete mil e seiscentos e trinta reais e oitenta centavos)**, conforme informações ilustradas na tabela a seguir:

Grupo	Item	Especificação	CATSER	Métrica	Qtde	Valor Unitário	Valor Total
	3	Subscrição para solução de gestão de acessos privilegiados.	27502	Usuários	100	R\$ 8.204,00	R\$ 820.400,00

1	4	Subscrição para solução de Segurança para Armazenamento de Credenciais.	27502	Usuários	1900	R\$ 397,06	R\$ 754.414,00
	10	Serviços de Instalação e Configuração das Soluções (por item / módulo)	16972	Serviço	2	R\$ 104.300,00	R\$ 208.600,00
	11	Serviço de treinamento / capacitação por (item / módulo)	3840	Turma	2	R\$ 125.000,00	R\$ 250.000,00
2	12	Serviço de acesso remoto confiança zero (ZTNA)	27502	Usuários	400	R\$ 1.046,00	R\$418.400,00
	13	Serviço de acesso seguro interno/externo (SWG)	27502	Usuários	1900	R\$ 1.617,00	R\$ 3.072.300,00
	14	Serviços de Instalação e Configuração das Soluções (por item / módulo)	16972	Serviço	2	R\$ 208.035,00	R\$ 416.070,00
	15	Serviço de treinamento / capacitação (por item / módulo)	3840	Turma	2	R\$ 183.723,40	R\$ 367.446,80
Total Geral							R\$ 6.307.630,80

14. Justificativa técnica da escolha da solução

14. Justificativa Técnica da escolha da solução

14.1 Com relação aos requisitos técnicos, a solução foi especificada para prover as funcionalidades mínimas para atendimento das necessidades de cibersegurança e infraestrutura tecnológica do FNDE.

14.2 Após análise técnica das soluções levantadas a subscrição e implantação se mostra a mais vantajosa do ponto de vista técnico.

14.3 A especificação do objeto também considerou os critérios de sustentabilidade ambiental previstos no Decreto nº 7.746, de 05 de junho de 2012, da Casa Civil da Presidência da República, no que couber.

14.4 A escolha pela contratação, foi baseada na análise com mais vantajosidade dos aspectos técnicos e econômicos da solução, se mostrando ser a mais viável, quer sob a perspectiva técnica, econômica e, especialmente, sob a ótica da segurança da informação.

14.5 Uma vez que se busca uma solução que, além de garantir a economicidade, reduza a indisponibilidade e garanta a eficiência do serviço público, o licenciamento perpétuo de software não se configura como uma escolha tecnicamente e economicamente viável, tendo em vista os riscos apontados na análise da solução, seção 11 deste documento, bem como o fato de ser uma opção que usualmente é mais onerosa para a Administração do que quando o bem é contratado na modalidade Subscrição, modelo que vem sendo adotado por grande parte das soluções.

14.6 Pelas razões acima delineadas, pelo já exposto tecnicamente neste estudo técnico preliminar, o cenário escolhido e os requisitos da contratação são compatíveis com a necessidade do FNDE, sendo que esta equipe de planejamento declara viável a contratação para viabilizar o incremento da maturidade da Segurança da Informação e a melhoria dos recursos tecnológicos do FNDE.

15. Justificativa econômica da escolha da solução

15. Justificativa Econômica da escolha da solução

15.1 Quanto a viabilidade de parcelamento da solução de TIC (Inciso I, § 2º, art. 12, da IN SGD/ME nº 94/2022), o parcelamento foi proposto bem como os itens foram enumerados à medida que se mostraram tecnicamente viável e economicamente vantajoso, considerando:

15.1.1 Viabilidade Técnica:

15.1.1.1 Integração e Interoperabilidade: A aquisição de integrada pode simplificar a melhoria na gestão e garantir uma maior interoperabilidade entre as diferentes soluções, proporcionando uma infraestrutura de segurança mais coesa e eficiente.

15.1.1.2 Desempenho e Escalabilidade: Ao adquirir solução integrada, será possível que o FNDE garanta que todas as partes do sistema sejam otimizadas para trabalhar em conjunto, proporcionando um desempenho consistente e com escalabilidade conforme as necessidades da autarquia.

15.1.1.3 Características dos recursos de Hardware e Software: Com soluções de um único fabricante, há uma maior probabilidade de que a solução atenda as características de hardware e software do parque computacional, simplificando a implementação e a gestão.

15.1.1.4 Facilidade de Gerenciamento: Soluções integradas de um único fabricante geralmente oferecem uma interface de gerenciamento unificada, o que facilita o monitoramento e o gerenciamento de todas as soluções a partir de uma única plataforma, neste sentido caso opte pela aquisição de vários fabricantes, certamente a gerência destes recursos será mais complexa exigindo que os servidores e colaboradores tenham que aprender a trabalhar em mais de uma plataforma de gerência.

15.1.1.5 Suporte Técnico e Atualizações: Ao adquirir soluções de um único fabricante, o FNDE poderá contar com um único ponto de contato para suporte técnico e atualizações, o que simplifica que o processo de resolução de problemas será mais simplificado garantindo que as soluções estejam sempre atualizadas com as últimas correções de segurança com menor esforço dos operadores da solução.

15.1.2 Viabilidade Econômica:

15.1.2.1 Economia a longo prazo: A longo prazo, atuar com produtos padronizados, pode resultar em economias significativas devido a uma melhor integração e eficiência operacional.

15.1.2.2 Custo Total de Propriedade (TCO): A consolidação de um sistema de um único fabricante pode reduzir o TCO ao longo do tempo, pois simplifica o gerenciamento, reduz os custos de treinamento e suporte, e minimiza a complexidade operacional.

15.1.2.3 ROI (Retorno sobre o Investimento): A implementação de soluções integradas de um único fabricante pode resultar em um ROI mais rápido, devido a uma melhor eficiência operacional, redução de incidentes de segurança e custos evitados associados a paralisações ou perdas de dados.

15.2 Considerando os benefícios em termos de integração, desempenho, gerenciamento simplificado, suporte unificado e potenciais economias financeiras, recomenda-se fortemente a aquisição da Solução de Tecnologia da Informação para proteção de ameaças online, bem como da gestão de acesso remoto a rede do FNDE e de acessos privilegiados a infraestrutura crítica de processamento de dados. Isso não apenas impactará a infraestrutura de tecnológica do FNDE, mas também os serviços providos a Sociedade Brasileira, podendo, inclusive, resultar em uma melhor eficiência operacional e custos reduzidos ao longo do tempo.

15.3 O prazo de garantia de doze (12) meses permite que a equipe de tecnologia da informação tenha apoio durante o processo de incorporação da solução na realidade organizacional, continuando com foco na atuação, com aplicação de métodos e procedimentos que agreguem valor aos recursos tecnológicos e serviços ofertados servidores e colaboradores da rede do FNDE e para os cidadãos que utilizam os serviços ofertados.

16. Benefícios a serem alcançados com a contratação

16. Benefícios a serem alcançados com a contratação

16.1 De acordo com a Necessidades de Negócio e Tecnológicas apontadas neste estudo, como por exemplo:

- **Acesso remoto seguro:** Fornecer acesso fácil e seguro para colaboradores que exerçam atividades fora da sede do FNDE.
- **Prevenção contra malware e ataques cibernéticos:** Mitigando dentre outros riscos, os associados a roubo ou utilização indevida de credenciais de acesso privilegiadas limitando o acesso dos usuários apenas ao necessário para suas funções bem como, ter maior controle sobre acessos remotos originados de dispositivos pessoais, evitando acesso de cibercriminosos ao ambiente tecnológico do FNDE.
- **Conformidade regulatória:** Aplicar políticas de segurança no contexto de Controle de Acesso e, consequentemente, buscar aderência ao Programa de Privacidade e Segurança da Informação (PPSI) e Programa Nacional de Proteção do Conhecimento Sensível (PNPC).

17. Providências a serem Adotadas

17. Providências a serem tomadas

17.1 O FNDE deverá instituir Grupo de Trabalho por intermédio da DIRTl composta por servidores da área técnica de Tecnologia da Informação para mapear necessidades referentes à gestão de acessos privilegiados visando a correta implementação da solução, em concordância com item “e”, Inciso I, Art. 11, da IN SGD/ME nº 94/2022.

17.2 Todas as adequações necessárias, incluindo instalação e configuração da solução, serão de responsabilidade da CONTRATADA.

17.3 A prestação dos serviços deverá ocorrer, preferencialmente, nos dias e horários de expediente, nada impedindo, porém, que ajustes que impactam na operação de infraestrutura se realizem fora do expediente, desde que haja necessidade e haja comunicado prévio da Contratada e anuência do FNDE.

18. Instrumentos de Planejamento

18. Dos Instrumentos de Planejamento

18.1 A contratação pretendida encontra-se alinhada conforme listado abaixo:

18.1.1 Do alinhamento ao Plano Diretor de Tecnologia da Informação

18.1.1.1 O objeto da contratação está previsto no Plano Diretor de Tecnologia da Informação do FNDE no Direcionador Estratégico - DRE – 1 - Elevação da maturidade em governança, gestão ágil e cibersegurança, bem como a Iniciativa Estratégica - INI-1.03: Aprimorar instrumentos de cibersegurança.

18.1. 2 Do alinhamento ao Plano de Contratações Anual de 2025

18.1.2.1 O objeto da contratação está previsto no Plano de Contratações Anual de 2025, conforme detalhamento a seguir:

18.1.2.1.1 Título da Contratação: DFD 38/2025 - Segurança para proteção de ameaças online, da gestão de acesso remoto e de acessos.

18.1.2.1.2 Número da Contratação: 153173-55/2025

19. Fonte Orçamentária

21. Da Fonte Orçamentária

21.1 Fonte orçamentária: Ação 2000 - Administração da unidade.

21.2 Plano Orçamentário: 000A - Modernização da Estrutura de Informática.

20. Declaração de Viabilidade

Esta equipe de planejamento declara **viável** esta contratação.

20.1. Justificativa da Viabilidade

Consoante o inciso V do art. 11 da Instrução Normativa SGD/ME nº 94 de 23 de dezembro de 2022, esta equipe de planejamento, declara viável esta contratação com base neste Estudo Técnico Preliminar.

Considerando o inciso II do § 1º do art. 18 da Lei nº 14.133, de 2021, a pretensa contratação se encontra no Plano de Contratações Anual - PCA, de modo a indicar o seu alinhamento com o planejamento da Administração, sob o Processo SEI nº 23034.039474/2024-35.

21. Responsáveis

Todas as assinaturas eletrônicas seguem o horário oficial de Brasília e fundamentam-se no §3º do Art. 4º do [Decreto nº 10.543, de 13 de novembro de 2020](#).

BELMIRO DA GRACA SOARES

Integrante Técnico



Assinou eletronicamente em 18/02/2025 às 10:07:30.

KAREN DE SOUSA COSTA

Integrante Requisitante



Assinou eletronicamente em 18/02/2025 às 14:55:22.

DELSON PEREIRA DA SILVA

Diretor de Tecnologia e Inovação

Lista de Anexos

Atenção: Apenas arquivos nos formatos ".pdf", ".txt", ".jpg", ".jpeg", ".gif" e ".png" enumerados abaixo são anexados diretamente a este documento.

- Anexo I - Anexo I - Caderno de Especificações Técnicas.pdf (328.56 KB)
- Anexo II - Anexo II - Solicitação de Propostas.zip (1.63 MB)
- Anexo III - Anexo III - Propostas.zip (1.73 MB)
- Anexo IV - Anexo IV - Mapa Comparativo de Preço.xlsx (24.71 KB)
- Anexo V - Anexo V - Política de Segurança da Informação - PSI-FNDE - Portaria757_2024_FNDE.pdf (473.65 KB)