INSTITUTO NACIONAL DO SEGURO SOCIAL

Processo Administrativo nº 35014.048551/2021-12

ESTUDO TÉCNICO PRELIMINAR

CONTRATAÇÃO DE SOLUÇÃO PARA GERENCIAMENTO E CONTROLE DE ACESSO A RECURSOS DE TIC

Data	Versão	Descrição	Autor
28/06/2021	1.0	Inicialização da primeira versão do documento	Integrantes Requisitante e Técnicos
12/11/2021	1.1	Atualização do documento segundo solicitações da CGIN/DTI	Integrantes Requisitante e Técnicos
31/01/2022	1.3	Finalização da 1ª versão completa do documento	Integrantes Requisitante e Técnicos
12/09/2022	1.4	Finalização da 2ª versão completa do documento	Integrantes Requisitante, Técnico e Administrativo
20/10/2022	1.5	Finalização da 3ª versão completa do documento	Integrantes Requisitante, Técnico e Administrativo
17/11/2022	1.6	Finalização da 4ª versão completa do documento	Integrantes Requisitante, Técnico e Administrativo

Brasília/DF, 17 de novembro de 2022

INTRODUÇÃO

O Estudo Técnico Preliminar - ETP tem por objetivo identificar e analisar os cenários para o atendimento da demanda que consta no Documento de Oficialização da Demanda - DOD (id. SEI nº 2905260), bem como demonstrar a viabilidade técnica e econômica das soluções identificadas, fornecendo as informações necessárias para subsidiar o respectivo processo de contratação.

Durante a elaboração do ETP diversos aspectos foram levantados para que os gestores se certificassem que existe uma necessidade de negócio claramente definida, quais as soluções capazes de atendê-la, vantagens e desvantagens e se os resultados pretendidos com a contratação possuem retorno frente ao valor a ser investido.

A presente análise tem por objetivo verificar a viabilidade técnica e econômica da contratação de Solução para Gerenciamento e Controle de Acesso a Recursos de TIC Active Directory - AD, com base nos parâmetros definidos no art. 11 da Instrução Normativa SGD/ME nº 01/2019 e considerando os requisitos definidos pela Diretoria de Tecnologia da Informação e Inovação - DTI constantes no DOD.

Diante da manifestação da CGIS no despacho (id. SEI nº 9344550**)**, a demanda originalmente identificada no DOD teve seu escopo alterado, de forma que passe a estudar a viabilidade de contratar as licenças da mesma solução (mesmo objeto), como subscrição, sendo estas as disponíveis no modelo comercial da Fabricante Microsoft, bem como pelos motivos explicitados no referido despacho acerca da orientação da DTI no sentido de se levar em conta a urgente necessidade de modernização do parque de ativos de TI do INSS.

No que se refere aos servidores Linux instalados nas unidades do INSS, os requisitos da Solução para Controle de Acesso a Recursos de TIC deverão ser limitados a fim de que não haja a necessidade de soluções distintas para as plataformas Linux e Windows.

1. DEFINIÇÃO E ESPECIFICAÇÃO DAS NECESSIDADES E REQUISITOS

1.1. Identificação das necessidades de negócio

1.1.1. Controlar o acesso a todos os recursos de TIC

1.1.1.1. Em alinhamento com os seguintes objetivos do PDTI INSS 2020-2022:

a) Gestão e controle de ativos de TIC que possibilite auditoria no uso dos equipamentos (CORREGEDORIA);

b) Controlar o acesso dos usuários aos recursos de TIC, permitindo gerenciar e controlar o acesso aos equipamentos e recursos do Instituto, bem como auditar as ações realizadas(DTI).

1.1.1.2. O INSS precisa controlar o acesso a todos os seus recursos de TIC. Esse controle precisa ser feito de forma eficiente e segura, e incluir todos que utilizam desses recursos, sejam servidores da Autarquia ou não.

1.1.1.3. Esse controle envolve, entre outras coisas, a capacidade do INSS definir quem, quando e a partir de que dispositivo o recurso pode ser acessado, definir que uso de cada recurso é permitido a cada usuário.

1.1.1.4. Esse mesmo nível de controle deve ser possível de ser aplicado a um único usuário ou a grupos de usuários. Para isso. é necessária que os recursos de agrupamento de usuário atendam todas as necessidades de negócio do INSS.

1.1.1.5. Além disso, é preciso incluir neste controle, o acesso não só a partir de dispositivos de propriedade do INSS, mas também a partir de dispositivos de particulares, sejam estes os servidores do Instituto ou não.

1.1.1.6. Em um contexto de incremento do trabalho remoto e de crescente disponibilização de recursos na Internet, esse controle deve se estender para além da rede do INSS, alcançando qualquer acesso aos recursos, a partir de qualquer lugar e onde quer que os recursos estejam hospedados.

1.1.1.7. Também em um contexto em que os recursos podem ser acessados de variados dispositivos (desktops, notebooks), é preciso que o controle de acesso se estenda a todas as plataformas de hardware com capacidade de acessar os recursos de TIC.

1.1.2. **Auditar o acesso aos recursos de TIC do INSS**

1.1.2.1. Ainda em alinhamento aos objetivos do PDTIC 2022, além de controlar o acessos aos recursos de TIC, em todas as dimensões, o INSS precisa auditar esses acessos, ou seja, identificar quem acessou o recurso, quando acessou, de onde acessou e o que fez durante esse acesso.

1.1.3. **Individualizar o acesso aos recursos de TIC**

1.1.3.1. Atualmente, no âmbito das redes internas do INSS, o acesso aos recursos de TIC não é feito de forma individualizada pelas pessoas que se utilizam desses recursos. Na verdade, esta possibilidade está disponível apenas nos dispositivos (desktops e notebooks) que se conectam diretamente nas redes de acesso instaladas nas dependências da Direção Central do INSS em Brasília/DF, e registrados no serviço de controle de acesso (controle de domínio) provido pela DATAPREV. Ressalte-se que esse serviço não é alvo de objeto contratual, não se podendo garantir, ou se exigir, qualquer qualidade sobre o serviço.

1.1.3.2. O acesso remoto a recursos hospedados na rede interna é feito atualmente através de serviço VPN, provido pela Dataprev. Nesse acesso há autenticação de usuários, no qual a pessoa que pretende acessar remotamente o recurso precisa informar ao serviço credenciais individualizadas (usuário e senha e/ou certificado digital), a fim de se obter o acesso. As credenciais são individualizadas, ou seja, o conjunto usuário/senha/certificado digital pertence apenas a uma pessoa.

1.1.3.3. A individualização do acesso é condição necessária para se fazer auditoria de utilização dos recursos de TIC.

1.1.3.4. Também é necessária para que sejam definidos perfis de acesso aos recursos ao nível de cada usuário, provendo eficiência e segurança na utilização dos mesmos, além de possibilitar um gerenciamento mais eficiente da utilização dos recursos por parte dos usuários.

1.1.3.5. A individualização do acesso também vai permitir que vários usuários compartilhem com mais segurança o mesmo dispositivo.

1.1.3.6. É desejável ainda que os usuários utilizem as mesmas credenciais para acesso a qualquer recurso de TIC, de qualquer dispositivo e lugar, estejam acessando a partir da rede interna do INSS ou não.

1.1.3.7. Existe, portanto, a necessidade de que o acesso individualizado aos recursos de TIC esteja disponível a todos os usuários.

1.2. **Identificação das Necessidades Tecnológicas**

1.2.1. **Requisitos de Arquitetura tecnológica**

1.2.1.1. Os componentes centrais da Solução devem ser hospedados e executados em ambiente, virtualizado ou não, externo ao INSS, seja em datacenter,

em nuvem ou em ambos.

1.2.1.2. Os componentes centrais da Solução devem ser implementados em arquitetura de alta disponibilidade , em cluster de componentes hospedados em ambientes físicos segregados entre si.

1.2.1.3. A Solução deve otimizar a utilização das redes locais do INSS na execução de todas as funcionalidades requeridas.

1.2.1.4. A Solução deve privilegiar a utilização de técnicas que otimizem o uso das funcionalidades requeridas.

1.2.1.5. A Solução deve permitir a auditoria dos acessos e configurações de todos os serviços computacionais que a compõem.

1.2.1.6. A distribuição e implantação de agentes de software, necessários ao funcionamento da solução nos dispositivos e recursos de TIC, deve ter todo seu fluxo automatizado.

1.2.1.7. O ingresso de computadores (exceto servidores) nos domínios controlados pelo serviço deve ter todo seu fluxo automatizado.

1.2.1.8. O serviço deve prover portal web para gerenciamento completo e consulta, de forma centralizada e consolidada, on line, em tempo real, a partir de dentro ou de fora da rede do INSS, seja de computadores ou dispositivos móveis.

1.2.1.9. A solução deve ter funcionalidade de criação de workflows para automatização de tarefas. Os workflows devem cobrir o ciclo completo das tarefas, inclusive retornando à plataforma de gerenciamento o resultado da execução.

1.2.1.10. A solução deve atender computadores com sistema operacional Windows a partir da versão 7, caso necessário.

1.2.1.11. Todas as interfaces de usuário, resultados de consultas e relatórios da Solução devem estar em idioma Português brasileiro.

1.2.1.12. A Solução deve ser capaz de atender os dispositivos e recursos de TIC de interesse do INSS:

a) Computadores conectados nas redes das unidades do INSS;

b) Impressoras conectadas nas redes das unidades do INSS;

c) Equipamentos ativos de rede local conectados nas redes das unidades do INSS;

d) Dispositivos dedicados de áudio e vídeo, que tenham endereço IP e estejam conectados nas redes das unidades do INSS;

e) Dispositivos dedicados à digitalização de imagens, que tenham endereço IP e estejam conectados nas redes das unidades do INSS.

1.2.2. **Requisitos de Segurança**

1.2.2.1. Deve-se assegurar, por meio de cláusulas contratuais, que os serviços a serem contratados permitirão a portabilidade de dados e softwares, no que couber, e que as informações do contratante estarão disponíveis para transferência de localização, em prazo adequado.

1.2.2.2. Todos os dados trafegados para funcionamento da solução devem ser criptografados.

1.2.2.3. Todas as informações pessoais armazenadas em nuvem deverão ser armazenadas com criptografia.

1.2.2.4. A Solução deverá observar todas as normas pertinentes relacionadas à segurança da informação, dados pessoais e privacidade.

1.2.2.5. Além das políticas que a provedora deverá estabelecer, esta deverá ainda observar, no que couber, a Política de Segurança da Informação do Instituto Nacional do Seguro Social - POSIN-INSS (RESOLUÇÃO Nº 9, DE 31 DE AGOSTO DE 2020 - Ministério da Economia/Instituto Nacional do Seguro Social/Presidência), destacadamente quanto ao que se refere a:

a) Tratamento de incidentes de SI;
b) gestão de riscos de segurança;
c) gestão de continuidade;
d) controles de acesso;
e) gestão de mudanças de TI;
f) computação em nuvem;
g) segurança física e do ambiente.

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

1.2.3.1. A Solução deverá ser provida com suporte técnico e em níveis de atendimento compatíveis com a criticidade e necessidade à sustentação da solução.

2. ESTIMATIVA DA DEMANDA - QUANTIDADE DE BENS E SERVIÇOS

2.1. A Solução deverá contemplar todos os servidores, empregados públicos, bem como os demais colaboradores em exercício no INSS.

2.2. Assim, tendo em vista o processo de contratação da Solução Integrada de Colaboração, Produtividade e Comunicação (Id. SEI 35000.002467/2019-97), que contempla exatamente este mesmo público, o quantitativo para esta Solução terá por base os quantitativos daquela Solução.

2.3. Dessa forma, em consulta à ferramenta de Gerenciamento de Licenças do Microsoft 365, realizada em **19/11/2021**, o quantitativo a ser utilizado neste processo se encontra na Tabela do item 6 deste ETP.

3. ANÁLISE DE SOLUÇÕES

3.1. Identificação das soluções

3.1.1. Baseado nos requisitos de negócios e tecnológicos, entende-se que a Solução que os atenderá trata-se de **Solução de Serviço de Diretório**.

3.1.2. Um diretório é uma estrutura hierárquica que armazena informações sobre objetos na rede. Um serviço de diretório fornece os métodos para armazenar dados de diretório e disponibilizá-los para usuários e administradores de rede. Por exemplo, pode-se armazenar informações sobre contas de usuário, como nomes, senhas, números de telefone etc., permitindo-se que outros usuários autorizados acessem essas informações.

3.1.3. O Serviço de Diretório armazena informações sobre objetos na rede e torna essas informações fáceis de serem encontradas e usadas por administradores e usuários, a partir do armazenamento de dados estruturado como base para uma organização lógica e hierárquica de informações de diretório.

3.1.4. Esse armazenamento de dados, também conhecido como diretório, contém informações sobre objetos do diretório. Esses objetos normalmente incluem

recursos compartilhados, como servidores, arquivos compartilhados, impressoras e as contas de usuário e computador de rede.

3.1.5. A segurança é integrada ao Serviço de Diretório por meio da autenticação de logon e do controle de acesso a objetos no diretório. Com um logon de rede único, os administradores podem gerenciar dados de diretório e da organização em toda a rede e os usuários de rede autorizados podem acessar recursos em qualquer lugar da rede. A administração baseada em política facilita igualmente o gerenciamento de redes mais complexas.

3.1.6. Servidor de Diretório é o software que permite a execução de todas as funcionalidades descritas para o Serviço de Diretório.

3.1.7. O Servidor de Diretório fornece os meios para o controle centralizado de acesso a todos os recursos de TIC que estejam registrados nos domínios controlados por ele.

3.1.8. O Servidor de Diretório permite ainda que sejam definidos usuários, grupos de usuários e dispositivos, e políticas centralizadas de acesso e utilização dos recursos de TIC por parte desses usuários.

3.1.9. O Servidor de Diretório registra os acessos aos objetos do diretório, permitindo que esse acesso seja auditado.

3.1.10. O Servidor de Diretório requer para seu funcionamento uma infraestrutura local de softwares básicos (sistema operacional, banco de dados, gerenciadores de sistemas de arquivos, virtualizadores etc.), hardware (servidores, armazenamento etc.), e rede (acesso dos usuários aos serviços providos pelos Servidores que compõem a solução). Além de ambiente físico compatível e que atenda aos requisitos ambientais, de energia e segurança que o serviço requer.

3.2. **Soluções disponíveis do mercado**

3.2.1. Com o objetivo de identificar possíveis provedores deste tipo de solução, foram realizadas diversas pesquisas na internet, bem como reuniões com representantes de diversos produtos de soluções de TIC, destacadamente, os fornecedores que estiveram melhor posicionados segundo o grupo de aconselhamento Gartner, em novembro de 2021, na linha “Gerenciamento de Acesso” (link disponível em https://www.forgerock.com/resources/analyst-report/2021-gartner-mq-access-management, acesso em 13/01/2022), tema que mais se aproximou ao buscado pela Autarquia.

3.2.2. Assim, foram identificadas os seguintes provedores: JumpCloud; IBM; Micro Focus; Okta; Auth0 (Okta); Ping Identity; ForgeRock; Oracle; CyberArk; Ilantus; Thales; e Microsoft.

3.2.2.1. ***Sobre a JumpCloud***

Conforme Anexo Memória de Reunião (id. SEI nº 6359553), o INSS se reuniu em 18/11/2021 com a Inteligence Partner, parceira no Brasil da Jumpcloud.

Segundo a Empresa, a solução da JumpCloud é um Serviço de Diretório na Nuvem, ***hospedado em território dos Estados Unidos da América***, o qual pode controlar, através de conectores nativos, o acesso a qualquer sistema que utilize os protocolos LDAP ou SAML, permitindo-se ainda a gestão integrada e centralizada de acesso dos usuários a vários sistemas, aplicativos e redes.

Na JumpCloud, para se controlar dispositivos com Sistemas Operacionais Windows, Linux ou Mac, no entanto, é necessária ***a instalação manual de um agente no dispositivo***. Particularmente quanto à Windows 7, foi informado não haver certeza de que a solução apresentada o suporta.

A Inteligence Partner informou que a solução da Jumpcloud permite ainda controlar quem pode ter acesso a um dispositivo, e com que privilégio de acesso, bem como aplicar políticas por dispositivo, exemplificando a aplicação em dispositivos Mac, inclusive demonstrando a possibilidade de aplicar políticas por Sistema Operacional, bem como por grupo de usuários.

Não soube informar se a solução da Jumpcloud poderia se integrar, para autenticação, ao cliente de VPN utilizado pelo INSS para acesso remoto à rede interna.

Relatou que não há nenhum órgão público utilizando a solução da Jumpcloud. Informou ainda que o maior cliente da Jumpcloud no Brasil deve ter cerca de 5 mil usuários.

Informou que a solução da Jumpcloud ***não provê um serviço LDAP, ou qualquer base, para autenticação de usuários***. Disse que não é o objetivo da solução.

Assim, entendeu-se que a solução da Jumpcloud apresentada não atende aos principais requisitos da contratação, principalmente quanto a prover uma base para autenticação de usuários, instalação remota de agente em dispositivos, além da hospedagem da Solução em território nacional (em atendimento à determinações normativas de segurança da informação).

3.2.2.2. ***Sobre a IBM***

Conforme Anexo Memória de Reunião (id. SEI nº 6359553), o INSS se reuniu com a IBM em 29/11/2021, tendo sido apresentado um panorama do Gerenciamento de Identidade e Acesso, nos seus vários aspectos: Gerenciamento de Identidade, de Acesso e de Privilégios.

Em seguida, a IBM apresentou as principais funcionalidades dos componentes das suas soluções que tratam dos referidos aspectos do Gerenciamento de Identidade.

A Empresa informou também que **não está no escopo das suas soluções, o controle de acesso a dispositivos**, como computadores ou impressoras, nem de recursos compartilhados nas redes, como arquivos em servidores. Nem está no escopo a definição de políticas de acesso a esses dispositivos, por qualquer critério.

Assim, entendeu-se que as soluções apresentadas pela IBM não atendem alguns dos principais requisitos desta contratação.

3.2.2.3. ***Sobre a Micro Focus***

O INSS se reuniu com a Micro Focus em 30/11/2021, tendo esta explicado de forma breve como as Soluções de Gestão de Identidades atualmente funcionam e qual o seu propósito. Segundo a Empresa, o alcance de soluções de identidades atualmente estão arquiteturalmente acima de um serviço de diretório, sendo este, na verdade, um importante componente.

A Empresa informou que possui um serviço de diretório – *edirectory* – em sua solução, mas não a ponto de substituir o *Active Directory* da Microsoft, afirmando ser possível e comum a integração deste com sua solução. Como exemplo da não substituição do *Active Directory* pelo *edirectory*, citou a **falta de capacidade de ingressar uma máquina num domínio, requisito essencial para o INSS.**

Assim, entendeu-se que a solução da Micro Focus é mais voltada para uma solução mais ampla de gerenciamento de identidades, e não um serviço de diretório propriamente dito que seja apto a atender as necessidades do INSS. Assim, esta alternativa foi tida por inapropriada para o atendimento à Autarquia.

3.2.2.4. ***Sobre a Okta, Auth0 (Okta), Ping Identity e ForgeRock***

Conforme Anexo Memória de Reunião (id. SEI nº 6359553), o INSS se reuniu com a NETBR, parceira no Brasil das empresas *Okta, Auth0 (Okta), Ping Identity e ForgeRock,* em 30/11/2021, tendo esta explicado de forma breve como as Soluções de Gestão de Identidades atualmente funcionam e qual o seu propósito, e apresentou os provedores parceiros para cada tipo de gestão.

Na Governança e Administração de Identidade (*IGA - Identity Governance and Administration),* que cuida do ciclo de vida das identidades na organização (criação, manutenção, exclusão etc.), informou que trabalha com a solução da SailPoint.

Apresentou a Ping Identity e a ForgeRock como parceiros nas soluções de Gerenciamento de Identidade e Acesso de Clientes *(CIAM – Costumer Identity and Access Management),* informando que a primeira é líder mundial nesse segmento. Explicou que o serviço possui as mesmas funcionalidades do IAM - *Identity and Access Management* (Gerenciamento de Identidade e Acesso), mas voltado para o Cliente externo, consumidor, público em geral.

O INSS informou que o CIAM está fora do escopo da contratação, pois ela é voltada para os colaboradores, a serviço do órgão.

Em seguida, a NETBR falou sobre a OKTA, que é a parceira no segmento IAM. Informou que a empresa é a líder no segmento, posição que, segundo a NetBr, fora recentemente fortalecida, com a aquisição da Auth0, também umas das líderes mundiais do segmento. Em seguida falou que a solução da Okta/Auth0, faz o gerenciamento de acesso e identidade dos colaboradores da organização, que é uma plataforma na nuvem, provida no modelo SaaS. Esclareceu que devido à quantidade de usuários que precisaria atender para o INSS, a variável performance de qualquer solução deveria ser bastante considerada. Por fim, disse que a solução **não atende todos os requisitos apresentados pelo INSS, principalmente aqueles referentes ao controle de acesso aos *endpoints* (estações de trabalho), impressoras de rede e compartilhamentos na rede interna**.

Informou ainda que a solução da OKTA/Auth0, **não se integraria a solução de gerenciamento de acesso aos Sistemas Corporativos, utilizados atualmente pelo INSS, sendo este serviço é um dos requisitos da contratação**.

Assim, entendeu-se que as soluções apresentadas pela NetBR, são mais voltadas para uma solução mais ampla de gerenciamento, governança e administração de identidades, e não um serviço de diretório propriamente dito que seja apto a atender as necessidades do INSS.

3.2.2.5. ***Sobre a Oracle***

Em reunião realizada em com representantes da Oracle, após o INSS apresentar suas demandas, estes entenderam que a Oracle não poderia atendê-las plenamente, mas que possivelmente apenas a Microsoft poderia fazê-lo. Assim, os produtos deste fabricante foram desconsiderados como possível candidato à solução a ser contratada pelo INSS.

3.2.2.6. ***Sobre a CyberArk***

Após reunião realizada em 27/08/2021 com a Oakmont Group, foi possível entender o foco da Cyberark.

A Solução da Cyberark atua sobre a proteção de identidades e acessos privilegiados através de proteção de acesso baseada em análise comportamentos,

resposta rápida a incidentes, avaliação de riscos relacionados à proteção de dados, verificação de conformidades etc.

Assim, percebeu-se que a Cyberark atua em uma camada superior e complementar ao desejado neste momento pelo INSS, sendo este necessário àquele.

Dessa forma, entendeu-se que a solução da Cyberark não é atua na linha de soluções buscadas pelo INSS.

3.2.2.7. ***Sobre a Ilantus e Thales***

Não foram identificados representante no Brasil que pudessem apresentar ao INSS esta soluções.

Apesar desta situação, diante das várias reuniões com outros representantes, restou configurado que atualmente apenas as soluções da Microsoft irão atender plenamente as necessidades do INSS.

3.2.2.8. ***Sobre a Microsoft***

Dentre todas as empresas consultadas pelo INSS, a Microsoft, foi a única tida por possuir a solução que o INSS necessita, inclusive, sendo assim reconhecida pela grande maioria dos demais fabricantes consultados.

Além de atender as **necessidades de negócio e tecnológicas**, o Azure AD com o Active Directory, ao contrário das demais soluções identificadas, de forma integral: 1) pode ser hospedado em território nacional (caso se opte pela sua versão em nuvem - Azure Active Directory); 2) permite a instalação automatizada de agentes; 3) provê uma base apropriada para autenticação de usuários; 4) permite o controle de acesso a computadores, impressoras, recursos compartilhados em rede etc.; e 5) é capaz de se integrar a soluções de gerenciamento de acesso aos Sistemas Corporativos do INSS.

O Azure Active Directory é tido pela Microsoft como a "próxima evolução das soluções de gerenciamento de identidade e acesso para a nuvem", pois reúne melhorias no gerenciamento de acesso a recursos de TIC se comparadas ao Active Directory, não se limitando a ambiente locais, mas também contemplando os serviços baseados em nuvem tão presentes nos dias atuais. O link https://docs.microsoft.com/pt-br/azure/active-directory/fundamentals/active-directory-compare-azure-ad-to-ad traz distinções de conceitos utilizados entre os produtos, bem como deixa claro as melhorias funcionais realizadas na abordagem em nuvem.

Por ser provisionado em ambiente de nuvem do próprio fabricante, o Azure Active Directory fornece outros benefícios intrínsecos aos serviço de nuvem, como a abstração para o cliente das tarefas de manutenção da infraestrutura necessário ao funcionamento da Solução, o que não ocorre com o Active Directory cujas manutenções deverão ser objeto de ação por parte da Autarquia.

Uma vez que o cenário Híbrido – Com Azure AD é voltado para ambientes Microsoft, esta solução permite uma melhor integração com o atual parque tecnológico do INSS, que se constitui, no que se refere a computadores e notebook, em sistema operacionais Windows. Ressalta-se ainda que o INSS possui a solução de colaboração Microsoft 365 já contratada (inclusive, sendo esta a base para se definir os quantitativos para Solução objeto deste estudo), o que vêm a contribuir para uma melhor integração entre as soluções, e assim, oferecendo funcionalidades e recursos mais seguros e de menor esforço operacional em sua manutenção.

No entanto, relevante observar que a Microsoft também informou que dentre os requisitos para utilização da solução baseada em nuvem, encontra-se a

necessidade de o parque de computadores possuir como sistema operacional o Windows 10, o que não é o caso do INSS, que possui cerca de 90% de seus dispositivos com o Windows 7.

Assim, configura-se como impossibilidade a integração do Azure Active Directory ao parque legado do INSS. Cogitou-se a possibilidade de aquisição de Azure Active Directory para os novos dispositivos com Windows 10, formando-se uma solução "híbrida", no entanto, entendeu-se que diante da implantação do Active Directory, os ganhos pretendidos com o Azure Active Directory seriam consideravelmente minimizados, uma vez que todo o esforço operacional para manutenção e sustentação dos dispositivos com Windows 7 já estaria sido realizado.

Dentre os cenários levantados junto a Microsoft o Híbrido – Com Azure AD (em nuvem) e Active Directory (on premise), com modernização do ambiente operacional de toda rede interna, especialmente a cerca da necessidade do INSS seguir uma política de implantação de soluções para modernização do parque de TI, conforme Despacho CGIS (Id. 9344550).

Dessa forma, diante de todo o exposto, a solução da Microsoft Híbrido – Com Azure AD (em nuvem) e Active Directory (on premise) será a escolhida para atendimento às necessidades da Autarquia.

3.3. Análise comparativa de soluções

3.3.1. Em contato com a Microsoft, visando prospectar os cenários das soluções demandadas, foi apresentado à Equipe de Planejamento da Contratação, os seguintes cenários tecnológicos conforme as tabelas abaixo, excluindo-se o cenário de licenciamento perpétuo considerando que o mesmo já fora analisado anteriormente no projeto original, Estudo Técnico Preliminar , bem como a determinação exarada no despacho CGIS (Id. SEI 9344550) orientando pela contratação via subscrição:

Cenário 1 - On Premise		
Type	**SKU**	**Product Description**
Subscrição	W06-00445	Core CAL ALng LSA UCAL (Windows Server, System Center Configuration Manager, Exchange Server, Sharepoint Server e Skype for Business Server)
Infraestrutura e Dados		
Subscrição	9EA-00039	Win Server DC Core ALng LSA 2L

3.3.2. Este cenário inclui as licenças do Windows Server para implantação do Active Directory, alem das User Cal, licenças de usuários para ter acesso aos serviços implantados no servidor. Contudo, este cenário além de ser totalmente on premise, demandando um esforço maior de sustentação, não atende aos requisito de modernização tecnológica do INSS, visto que é uma solução defasada em termos de arquitetura de serviço, de padrões de acesso seguros, e não provê upgrade do ambiente das estações para uma configuração atualizada, em conformidade com padrões modernos de funcionamento, integração de ambientes e segurança. **Desta forma, este cenário está descartado, por não atender os requisitos postos neste documento.**

Cenário 2 - Híbrido - Com Azure AD		
Type	**SKU**	**Product Description**

Subscrição	JFX-00003	M365 F3 FUSL Sub Per User (Licença de Office 365 F3, Upgrade de Windows, CAL Bridge, EMS - Azure AD Premium P1, Endpoint Manager/Intune e Information Protection)
Subscrição	AAA-12414	CCAL Bridge O365 Sub Per User (Windows Server e System Center Configuration Manager - depende de licenças O365 E1 ou E3)
Infraestrutura e Dados		
Subscrição	9EA-00039	Win Server DC Core ALng LSA 2L

3.3.3. Este cenário , além das licenças do Windows Server para implantação do Active Directory, para implantação em infraestrutura local, on premise, e das User Cal, licenças de usuários para ter acesso ao serviços, também inclui licenças de uso do serviço em nuvem de controle e gerenciamento de acesso de usuários e dispositivos. Esse serviço provê funcionalidades como logon único, autenticação multifator e acesso condicional, rastreamento de atividades de usuários, além de serviço de proteção à informação. Por ser provisionado em ambiente de nuvem do próprio fabricante, possui outros benefícios intrínsecos aos serviço de nuvem, como a abstração para o cliente das tarefas de manutenção da infraestrutura necessário ao funcionamento da Solução, não onerando a equipe de suporte do órgão, com a sustentação do serviço. No entanto, neste cenário, uma parte dos usuários não teriam acesso ao serviço em nuvem. Ou seja, uma parte dos usuários teria de ingressar em domínio local, a fim de ser possível controlar o acesso à rede, não podendo inclusive acessar dispositivos que tiverem ingressados no serviço em nuvem. Ou seja, neste cenário, órgão teria de lidar com dois ambientes tecnológicos distintos, não integrados entre si. **Assim, este cenário não atende aos requisitos da solução.**

Cenário 3 - Híbrido – Com Azure AD		
Type	**SKU**	**Product Description**
Subscrição	JFX-00003	M365 F3 FUSL Sub Per User (Licença de Office 365 F3, Upgrade de Windows, CAL Bridge, EMS - Azure AD Premium P1, Endpoint Manager/Intune e Information Protection)
Subscrição	AAA-10732	EMS E3 ALng Sub Per User (Azure AD Premium P1, Endpoint Manager/Intune, Azure Information Protection e CAL Bridge)
Infraestrutura e Dados		
Subscrição	9EA-00039	Win Server DC Core ALng LSA 2L

3.3.4. Este cenário , além das licenças do Windows Server para implantação do Active Directory, para implantação em infraestrutura local, on premise, e das User Cal, licenças de usuários para ter acesso ao serviços, também inclui licenças de uso do serviço em nuvem de controle e gerenciamento de acesso de usuários e dispositivos. Esse serviço provê funcionalidades como logon único, autenticação multifator e acesso condicional, rastreamento de atividades de usuários, além de serviço de proteção à informação. Por ser provisionado em ambiente de nuvem do próprio fabricante, possui outros benefícios intrínsecos aos serviço de nuvem, como a abstração para o cliente das tarefas de manutenção da infraestrutura necessário ao funcionamento da Solução, não onerando a equipe de suporte do órgão, com a sustentação do serviço. E diferentemente do cenário 2, este atende a toda a demanda prevista para a solução, a todos os usuários. **Assim, esse cenário foi o escolhido pela Equipe de Planejamento da Contratação para provimento da solução.**

3.3.5. Há que se considerar que o item 1 do Grupo 1 da presente contratação, inclui o pacote do MS 365 contendo licenciamento do tipo F3 para todos os usuários que se enquadrem nessa categoria, sendo um dos itens dos objetos do Contrato 28/2020 Id. SEI 35014.327974/2020-15).

3.3.6. Desse modo, a presente contratação, especificamente quanto a ativação das licenças do Office 365 F3, somente será realizada após a finalização do contrato acima, com previsão de término para 28/12/2022.

Cenário 4 - Azure AD		
Type	**SKU**	**Product Description**
Subscrição	WL6-00002	AzureActvDrctryP1K ShrdSvr ALNG SubsVL MVL PerUsr
Subscrição	U5U-00016	Intune USL Sub AP Per User
Subscrição	3R2-00002	AzureActvDrctryPremP1 ShrdSvr ALNG SubsVL MVL PerUsr

3.3.7. Este cenário inclui licenças de uso do serviço em nuvem de controle e gerenciamento de acesso de usuários e dispositivos. Esse serviço provê funcionalidades como logon único, autenticação multifator e acesso condicional, rastreamento de atividades de usuários, além de serviço de proteção à informação. Por ser provisionado em ambiente de nuvem do próprio fabricante, possui outros benefícios intrínsecos aos serviço de nuvem, como a abstração para o cliente das tarefas de manutenção da infraestrutura necessário ao funcionamento da Solução, não onerando a equipe de suporte do órgão, com a sustentação do serviço. Este cenário também atende a toda a demanda prevista para o serviço em nuvem, no entanto, não provê as licenças do Windows Server para implantação do Active Directory, em infraestrutura local, on premise, requisito da solução. **Assim, este cenário não atende aos requisitos da solução.**

3.3.8. Escolhido o modelo de arquitetura da Solução, registra-se será utilizado, para a parte local, on premise, da solução, o ambiente de armazenamento em **nuvem** um vez que o INSS não dispõe de infraestrutura física (Datacenter ou outro ambiente físico) adequada para suportar a Solução.

3.3.9. **Formas de aquisição do Active Directory (on-premise)**

3.3.9.1. O Active Directory é formado por dois componente: 1) licenças de acesso para clientes (chamadas de *Client Access Licenses* - CALs) e; 2) licenças de sistemas operacionais voltadas para servidores que fornecerão o serviço.

3.3.9.2. ***Quanto às Cals:***

3.3.9.3. CALs são licenças (não softwares) que dão direito de acesso a serviços da Microsoft providos através do Windows Server.

3.3.9.4. Registra-se ainda que uma cal é vinculada a cada usuário que participará/utilizará o serviço de diretório. Assim, será necessário adquirir tantas CALs quanto forem o número de usuários.

3.3.9.5. Ainda há a opção de se adquirir CAL vinculados a dispositivos (*Device CAL*), mas esta escolha é mais indicada quando o número de dispositivos é menor que o número de usuário, ou seja, quando dispositivos são compartilhados com usuários, o que não é o caso do INSS.

3.3.9.6. ***Quanto às licenças Windows Server:***

3.3.9.7. Além das CALs, conforme mencionado anteriormente, será necessário adquirir licenças de Windows Server para os servidores que fornecerão o serviço.

3.3.9.8. Após conversa com a Microsoft, esta informou que atualmente é possível adquirir duas versões de Windows Server: 2.1) Windows Server Standard e; 2.2) Windows Server Datacenter.

3.3.9.9. Ambas versões do Windows Server possuem direitos de uso temporal ilimitado ou pérpetuas (mas, assim como as CALs, vinculados à versão adquirida) e subscrição.

3.3.9.10. A diferença entre estas duas versões encontra-se no tipo de ambiente em que serão utilizados. Enquanto o Windows Server Standard é voltado para ambientes físicos, ou minimamente virtualizados, o Windows Server Data Center é indicado para Datacenter e ambientes em nuvem altamente virtualizados.

3.3.9.11. Uma vez que o serviço será provido através de **nuvem já contratada pelo INSS** , entende-se como mais indicado a aquisição da versão **Windows Server Datacenter**. Além disto, o Windows Server Datacenter possui recursos não presentes na versão Standard, que poderão ser úteis ao Instituto, como, a utilização de máquinas virtuais em número ilimitado, definição e controle de rede por software etc.

3.3.9.12. O Windows Server Datacenter, assim como o Windows Server Standard, possui modelo de licenciamento baseado em núcleos. Assim, para a estimativa do número de licenças necessárias ao serviço de diretório, foram realizadas consultas no mercado, onde se apontou a necessidade de servidores com processador de pelo menos 32 núcleos. Visto que para atender o requisito de alta disponibilidade da Solução, os servidores devem ser implementados em cluster de no mínimo 2 servidores, cada um com 32 núcleos, totalizando 64 núcleos, serão necessárias **32 licenças**, uma vez que cada licença cobre até dois núcleos.

3.3.9.13. ***Sobre o Software Assurance - SA da Microsoft***

3.3.9.14. As licenças acima, tanto das CAL como do Windows Server, para o cenário escolhido (cenário 3), inclui o *Software Assurance* - SA.

3.3.9.15. A adição deste recurso não acrescenta novas funcionalidades às licenças, mas apenas dá direito a um conjunto de benefícios, como garantia de atualização para novas versões de upgrade, utilização híbrida com nuvem Azure, mobilidade de licenças etc.

3.3.9.16. Ainda sobre atualização, registra-se que a aquisição do Windows Server CAL sem SA não impede o acesso a atualizações de correções (*update*), mas apenas não dá direito a novas versões (*upgrade*). Historicamente, as versões do Windows Server (atrelado/vinculado às Cals) são lançadas no mínimo a cada 03 (três) anos, e assim, não se vislumbra a necessidade desta atualização, ainda mais diante da possibilidade de atualização do parque computacional do INSS neste período, o que levaria a uma revisão de toda solução a ser escolhida.

3.3.10. **Do Serviço de Implantação, Customização, Suporte Técnico e Treinamento da Solução**

3.3.10.1. Além da aquisição das licenças citadas acima, será necessário adquirir os serviços de implantação, customização, suporte e treinamento.

3.3.10.2. Diferentemente dos itens anteriores (Licenças), que necessariamente serão fornecidos pela Microsoft, estes serviços poderão ser prestados por terceiros além da fabricante do Windows.

3.3.10.3. O serviço de implantação consistirá na preparação do ambiente central da Solução, na nuvem do fabricante e em infraestrutura a ser provida pelo INSS, onde serão instalados e provisionadas as licenças adquiridas.

3.3.10.4. Atrelado ao serviço de implantação, encontra-se a customização da Solução, que consiste em personalizá-la segundo ambiente e necessidades do INSS, sempre em observância das recomendações do fabricante da Solução.

3.3.10.5. Para se garantir uma adequada utilização e sustentação da Solução é necessário se adquirir suporte técnico apropriado, uma vez que a Solução a ser contratada constitui-se em novo serviço a ser prestado pela Equipe de TIC do INSS, além de sua criticidade natural em sendo um sistema estruturante que poderá ser utilizado por diversos outros sistemas.

3.3.10.6. O Treinamento deverá ser utilizado para que o INSS consiga prestar suporte técnico aos seus usuários, bem com realizar as configurações necessárias à operacionalização da Solução. Apesar deste treinamento, registra-se a necessidade de aquisição do suporte técnico, diante de novos problema que não poderiam ser contemplados no treinamento, além da já citada criticidade da Solução.

3.3.11. **Outros pontos analisados para escolha da Solução**

3.3.11.1. Em atendimento às recomendações normativas para contratação de Solução de TIC, para a escolha da solução foram ainda considerados:

3.3.11.2. **Necessidades similares de outro órgão ou entidade da Administração Pública**

3.3.11.3. Não foram identificadas necessidades similares de outros órgãos.

3.3.11.4. **Alternativas do Mercado: tipos de soluções disponíveis**

3.3.11.5. As alternativas de solução disponíveis pelo mercado foram relacionadas e apresentadas anteriormente.

3.3.11.6. **A ampliação ou substituição da solução implantada**

3.3.11.7. Não existe solução implantada no INSS, de forma que não há que se falar em “ampliação” ou mesmo “substituição”, sendo necessária, então, uma nova contratação.

3.3.11.8. **Possibilidade de aquisição na forma de bens ou contratação como serviço**

3.3.11.9. Os itens que compõem a Solução estão descritos no tópico 6, de forma que além das licenças de subscrição, se encontram também as contratações de serviços.

3.3.12. **Parcelamento ou não da solução**

3.3.12.1. Entendeu-se ser possível a separação de itens por dois agrupamentos (Grupo 1 - Licenças e Grupo 2 - Serviços), conforme tópico 6 deste Estudo, de forma que estão separadas as licenças dos serviços.

3.3.12.2. As licenças devem ser adquiridas de forma conjunta, diante da expectativa de ganho de escala, uma vez que o produtos serão oriundos da mesma fabricante Microsoft.

3.3.12.3. Quanto aos serviços, entende-se que devam ser adquiridos por meio de um único fornecedor, uma vez que existem dependências técnicas entre eles, além de se trazer mais benefícios para a administração.

3.3.12.4. **A Solução encontra-se implantada em outro órgão ou entidade da Administração Pública?**

3.3.12.5. Sim. A aquisição de direito de uso de software, bem como serviços técnicos são comuns na Administração Pública.

3.3.12.6. **A Solução está disponível no Portal do Software Público Brasileiro?**

3.3.12.7. Para os casos que poderiam se aplicar, não estão.

3.3.12.8. **A Solução é aderente às políticas, premissas e especificações técnicas definidas pelos Padrões de governo ePing, eMag, ePWG?**

3.3.12.9. No que couber, entende-se que sim.

3.3.12.10. **A Solução é aderente às regulamentações da ICP-Brasil? (quando houver necessidade de certificação digital)**

3.3.12.11. Atualmente, não se vislumbra que a Solução a ser contratada seja utilizada para certificação digital.

3.3.12.12. **A Solução é aderente às orientações, premissas e especificações técnicas e funcionais do e-ARQ Brasil? (quando o objetivo da solução abranger documentos arquivisticos)**

3.3.12.13. Não se aplica.

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

3.3.13.1. A seguir encontram-se os principais pontos observados durante a Fase de Planejamento da Contratação para que o INSS, destacadamente através da DTI, consiga implantar e utilizar de forma apropriada a Solução.

3.3.13.2. **1 - Suporte técnico aos usuários**. O INSS deverá possuir pessoal capaz de prestar suporte técnico aos seus usuários. São esperadas demandas por parte destes relacionadas a atualização cadastral, *reset* de senha, acesso a documentos armazenados em seu computadores, acesso a impressoras, perfis de acesso etc. Parte destas demandas é atualmente atendida pela Dataprev, assim, sugere-se que o INSS consulte a referida empresa para que se possa estimar o número de demandas de usuários e assim se certificar que possuirá capacidade de atendê-los, devendo esta verificação ser realizada antes da celebração de qualquer contrato referente aos itens deste Estudo. Sugere-se que o INSS crie ainda um Plano de Comunicação para seus usuários quando da entrada do serviço no ar para que se minimize demandas de possíveis problema.

3.3.13.3. **2 - Intermediação junto à Dataprev**. A DTI deverá realizar a intermediação entre os fornecedoras da Solução e a Dataprev para viabilizar a implantação da Solução, destacadamente, no processo de migração/sincronização de dados entre os domínios existente e o que será criado. Ainda relacionado à Dataprev, deverá o INSS estabelecer com a Empresa um Plano de Alteração de Acesso de Sistemas, em que o novo serviço de diretório passará a ser usado pelos sistemas que atualmente se autenticam utilizando-se da base da Estatal. Naturalmente, essas mudanças deverão observar a capacidade de sustentação e atendimento dos usuários. Registra-se ainda que os sistemas a serem integrados ao novo serviço poderão requisitar adaptações.

3.3.13.4. **3 - Infraestrutura necessária**. O INSS deverá providenciar o ambiente para implantação da Solução, inclusive que atenda os **requisitos específicos de**

segurança da solução. Além do ambiente em si, o INSS deverá possuir pessoal técnico para sustentação e operação desse ambiente que deverá ser capacitado conforme item de contratação presente neste Estudo.

3.3.13.5. **Catálogos de Soluções de TIC com Condições Padronizadas**

3.3.13.6. Contratações de itens de Tecnologia da Informação e Comunicação - TIC. Em consulta aos Catálogos de Soluções de TIC com Condições Padronizadas (disponíveis em https://www.gov.br/governodigital/pt-br/contratacoes/catalogo-de-solucoes-de-tic), acesso em 06/10/2022, foi verificado que o objeto da contratação consta do catálogo de produtos a Microsoft.

4. REGISTRO DE SOLUÇÕES CONSIDERADAS INVIÁVEIS

4.1. Conforme informado anteriormente, foram tidas por inviáveis as soluções providas por fornecedores diferente da Microsoft, pois acabam por não atender requisitos de negócio e tecnológicas de forma integral, como ser hospedado em território nacional (casos de soluções nuvem), capacidade de gerenciamento de dispositivos, integração com esquemas legados de autenticação, como LDAP etc

4.2. Quanto às CALs, foram descartadas a possibilidade de aquisição vinculada a dispositivos (*Device* CAL), diante desta escolha ser mais indicada quando o número de dispositivos é menor que o número de usuário, ou seja, quando dispositivos são compartilhados com usuários, o que não é o caso do INSS.

4.3. Quando ao Windows Server, a versão Standard foi descartada devido ser voltada para ambientes físicos, ou minimamente virtualizados. Uma vez que o serviço será provido através de **nuvem já contratada pelo INSS** , entende-se como mais indicado a aquisição da versão Windows Server Datacenter, que é indicada para Datacenter e ambientes em nuvem altamente virtualizados.

5. ANÁLISE COMPARATIVA DE CUSTOS (TCO)

5.1. Uma vez que há apenas uma única alternativa para cada componente da Solução o custo total da Solução encontra-se presente no tópico 8 – ESTIMATIVA DE CUSTO TOTAL DA CONTRATAÇÃO.

6. DESCRIÇÃO DA SOLUÇÃO A SER CONTRATADA

6.1. Diante do exposto, o INSS deverá adquirir:

RESUMO ITENS A SEREM ADQUIRIDOS			
Grupo	**ITEM**	**OBJETO**	**Quantidade**
Grupo 1 - Licenças	01	Windows Server CAL Bridge per User (M365 F3 FUSL- EMS - Azure AD Premium P1, Endpoint Manager/Intune e Information Protection)	26.769
	02	Windows Server CAL Bridge per User (EMS E3- Azure AD Premium P1, Endpoint Manager/Intune e Information Protection)	3.253
	03	Windows Server Datacenter 2022 Core ALng LSA 2L	32
Grupo 2 - Serviços	04	Implantação e customização	1
	05	Suporte técnico	12 meses
	06	Treinamento	1

7. ESTIMATIVA DE CUSTO TOTAL DA CONTRATAÇÃO

7.1. A Equipe de Planejamento da Contratação realizou a pesquisa de preços para esta contratação conforme preconiza à Instrução Normativa nº 73/2020/SEGES/ME.

7.2. A pesquisa de preços da solução considerada técnica e funcionalmente viável encontra-se no ANEXO DSC Id. SEI nº 8950837.

7.3. Assim, de forma resumido, as estimativas para a contratação estão reproduzidas abaixo, cujo valor total estimado para 12 (doze) meses é de **R$ 18.455.075,73 (dezoito milhões, quatrocentos e cinquenta e cinco mil, setenta e cinco reais e setenta e três centavos).**

RESUMO ITENS A SEREM ADQUIRIDOS						
GRUPO	**ITEM**	**ITEM**	**QUANT**	**VALOR UNITÁRIO**	**TOTAL MENSAL**	**VALOR GLOBAL 12 MESES**
Grupo 1 - Licenças	01	Windows Server CAL Bridge per User (M365 F3 FUSL-EMS - Azure AD Premium P1, Endpoint Manager/Intune e Information Protection)	26.769	R$ 50,11	R$ 1.341.394,59	R$ 16.096.735,08
	02	Windows Server CAL Bridge per User (EMS E3- Azure AD Premium P1, Endpoint Manager/Intune e Information Protection)	3.253	R$ 42,31	R$ 137.634,43	R$ 1.651.613,16
	03	Windows Server Datacenter 2022 Core ALng LSA 2L	32	R$ 1.573,00	-	R$ 50.336,00
Grupo 2 - Serviços	04	Implantação e customização	1	R$ 428.901,91	-	R$ 428.901,91
	05	Suporte técnico	1	R$ 7.311,33	R$ 7.311,33	R$ 87.735,96
	06	Treinamento	1	R$ 139.753,62		R$ 139.753,62
CUSTO TOTAL DA CONTRATAÇÃO					**R$ 1.486.340,35**	**R$ 18.455.075,73**

8. DECLARAÇÃO DE VIABILIDADE DA CONTRATAÇÃO

8.1. Diante do Estudo Técnico Preliminar realizado, a Equipe de Planejamento da Contratação entende ser viável a presente contratação, desde que observadas os apontamentos deste Estudo, destacadamente quanto ao "NECESSIDADES DE ADEQUAÇÃO DO AMBIENTE", bem como dos riscos registrados no Mapa de Gerenciamento de Riscos (id. SEI nº 8962357).

9. ASSINATURA

9.1. A Equipe de Planejamento da Contratação foi instituída pela Portaria nº 266/DGPA/INSS, de 03 de agosto de 2021, tendo sido alterada pela Portaria DIROFL/INSS Nº 70, DE 19 DE abril DE 2022

9.2. Conforme o §6º do art. 12 da IN SGD/ME nº 01, de 2019, o Estudo Técnico Preliminar deverá ser aprovado e assinado pelos Integrantes Técnicos e Requisitantes e pela autoridade máxima da área de TIC:

9.3.

INTEGRANTE TÉCNICO	INTEGRANTE ADMINISTRATIVA	INTEGRANTE REQUISITANTE
_____ Carlos Alexandre Gusmão Negrão Matrícula SIAPE: 3.195.483	_____ Mônica Cristina Quibáo Matrícula SIAPE: 2.263.327	_____ Rafael Roque Leite Matrícula SIAPE: 2.221.311

10. APROVAÇÃO E DECLARAÇÃO DE CONFORMIDADE

10.1. Aprovo este Estudo Técnico Preliminar e atesto sua conformidade às disposições da Instrução Normativa SGD/ME nº 1, de 4 de abril de 2019.

AUTORIDADE MÁXIMA DA ÁREA DE TIC (OU AUTORIDADE SUPERIOR, SE APLICÁVEL – § 3º do art. 11)
_____ JOÃO RODRIGUES DA SILVA FILHO DIRETOR DE TECNOLOGIA DA INFORMAÇÃO E INOVAÇÃO9SUBSTITUTO) Matrícula/SIAPE: 1.561.845

Documento assinado eletronicamente por **Rafael Roque Leite**, **Chefe de Divisão de Suporte a Contratações de Tecnologia da Informação**, em 17/11/2022, às 17:26, conforme horário oficial de Brasília, com o emprego de certificado digital emitido no âmbito da ICP-Brasil, com fundamento no art. 6º, caput, do Decreto nº 8.539, de 8 de outubro de 2015.
Nº de Série do Certificado: 538023739757699980862416162 41

Documento assinado eletronicamente por **TAREK IBRAHIM CHAMCHAUM**, **Empregado Público Cedido**, em 17/11/2022, às 17:26, conforme horário oficial de Brasília, com fundamento no § 3º do art. 4º do Decreto nº 10.543, de 13 de novembro de 2020.

Documento assinado eletronicamente por **Carlos Alexandre Gusmão Negrão**, **Analista Técnico Administrativo**, em 17/11/2022, às 17:27, conforme horário oficial de Brasília, com fundamento no § 3º do art. 4º do Decreto nº 10.543, de 13 de novembro de 2020.

Documento assinado eletronicamente por **MONICA CRISTINA QUIBAO**, **Analista do Seguro Social**, em 17/11/2022, às 17:28, conforme horário oficial de Brasília, com fundamento no § 3º do art. 4º do Decreto nº 10.543, de 13 de novembro de 2020.

Documento assinado eletronicamente por **JOAO RODRIGUES DA SILVA FILHO**, **Diretor(a) de Tecnologia da Informação**, em 17/11/2022, às 17:58, conforme horário oficial de Brasília, com fundamento no § 3º do art. 4º do Decreto nº 10.543, de 13 de novembro de 2020.

A autenticidade deste documento pode ser conferida no site https://sei.inss.gov.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0, informando o código verificador **9667808** e o código CRC **12FEF8B7**.

Referência: Processo nº 35014.048551/2021-12 SEI nº 9667808

Criado por tarek.chamchaum, versão 5 por tarek.chamchaum em 17/11/2022 17:25:28.