INSTITUTO NACIONAL DO SEGURO SOCIAL

ESTUDO TÉCNICO PRELIMINAR

Processo Administrativo nº 35014.048537/2021-19

Proteção Avançada Contra Ameaças Cibernéticas

Brasília, 01/01/2022
Histórico de Revisões

Data	Versão	Descrição	Autor
13/01/2022	1.0	Finalização da primeira versão do documento	• Rafael Roque Leite • Jullyano Lino da Silva • Edir Vargas Coelho

INTRODUÇÃO

O Estudo Técnico Preliminar tem por objetivo identificar e analisar os cenários para o atendimento da demanda que consta no Documento de Oficialização da Demanda, bem como demonstrar a viabilidade técnica e econômica das soluções identificadas, fornecendo as informações necessárias para subsidiar o respectivo processo de contratação, conforme Art. 11 da IN SGD/ME nº 1/2019.

O enquadramento dessa contratação foi redefinido como solução de TI, segundo a Instrução Normativa SGD/ME nº 01/2019. Trata-se de um conjunto de serviços comuns de informática, em consonância com o DECRETO Nº 7.174, DE 12 DE MAIO DE 2010, quer descreve no art 2° *"A aquisição de bens e serviços de tecnologia da informação e automação deverá ser precedida da elaboração de planejamento da contratação, incluindo projeto básico ou termo de referência contendo as especificações do objeto a ser contratado, vedando-se as especificações que:"*

- *I – direcionem ou favoreçam a contratação de um fornecedor específico;*
- *II – não representem a real demanda de desempenho do órgão ou entidade; e*
- *III – não explicitem métodos objetivos de mensuração do desempenho dos bens e serviços de informática e automação.*

Ressalta-se que aplica-se ao presente estudo as normas específicas para contratação dos objetos descritos art. 8º, § 2º, da IN SGC/ME nº 01, de 2019 - Anexo, quais sejam, **licenciamento de software e serviços agregados**, seguindo-se todas as determinações e inclusões de cláusulas necessárias a este tipo de contratação.

Não se aplica, considerando o mesmo instrumento supracitado, serviços de autenticação para serviços públicos digitais; serviços de desenvolvimento, sustentação e manutenção de software; infraestrutura de centro de dados, serviços em nuvem, sala-cofre e sala segura.

Adicionalmente, o objeto da presente contratação não se enquadra aos ditames do Decreto nº 9507/2018, inclusive quanto às proibições do seu art. 3º.

Este Estudo Técnico Preliminar tem por objetivo identificar e analisar a viabilidade técnica e econômica da contratação, em acordo com o DOD, documento SEI (2905217), de empresa para provimento de licenças de Solução de Segurança Integrada de Proteção de E*ndpoints* (estações de trabalho e servidores de rede) e Proteção de Dados (criptografia e anti-exfiltração), Detecção e Resposta de Endpoint (Endpoint Detection and Response - EDR), incluindo capacitação e serviço especializado de implantação

O objeto da pretendida contratação tem a natureza de **serviço comum de caráter continuado**, pois pode ser objevamente especificado por meio de padrões usuais no mercado. Podendo, portanto, ser contratado por meio de processo licitatório na modalidade pregão em sua forma eletrônica.

JUSTIFICATIVA DA CONTRATAÇÃO

O Instituto Nacional do Seguro Social – INSS, caracterizado como prestador de serviços previdenciários para a sociedade, busca alternativas de melhoria contínua, com programas de modernização e excelência operacional, ressaltando a otimização de resultados e de ferramentas. Atua de forma bastante descentralizada, disponibilizando seus sistemas a diversas organizações, como a OAB, tribunais, cooperativas de trabalhadores, o cidadão brasileiro – através do site "Meu INSS". Recentemente o Instituto passou a oferecer aos seus servidores a possibilidade do teletrabalho – Portaria Nº 1.182/PRES/INSS, de 20 de novembro de 2020 – e começou a utilizar serviço de nuvem privada para hospedar seus sistemas, realizando vários projetos e investimentos em Tecnologia da Informação e Comunicações (TIC), buscando melhoria da qualidade e eficiência dos serviços prestados a toda a sociedade.

Com esse intuito de avançar nas políticas previdenciárias concomitante ao atendimento crescente da demanda por TI, o INSS necessita implantar segurança em toda sua cadeia de atendimento. Agindo tempestivamente com a intenção de evitar que ameaças digitais como a inserção de dados fraudulentos em sistemas, o roubo de dados previdenciários, o roubo de credenciais de acesso de seus servidores, ataques de *ransomware* nas estações dos servidores, ataques lógicos e físicos de *keyloggers*, dentre outras, possa por em risco as suas operações.

Esta demanda visa dotar o arcabouço tecnológico que o INSS utiliza para desenvolvimento e continuidade de seu trabalho, através da prospecção de um produto ou serviço que ofereça uma estratégia de proteção para os seus ativos computacionais.

O último contrato celebrado entre o INSS com fornecedor de antivírus se encerrou em 2015. Desde então, as técnicas utilizadas por pessoas mal intencionadas, com o objetivo de explorar as vulnerabilidades das instituições, evoluíram a par e passo com o desenvolvimento tecnológico, permitindo o surgimento de uma nova geração de ameaças, desenhadas para roubar dados em vez de causar prejuízo em arquivos digitais. Ferramentas antigas de combate a vírus não protegem mais contra essa nova geração, pois ameaças podem passar despercebidas por sistemas de proteção que verificam somente a assinatura de arquivos, e não comportamento ou circunstâncias.

As soluções de antivírus mudaram sua forma de atuação para abranger as novas abordagens de detecção e prevenção de ameaças, como as tecnologias de aprendizado de máquina e de inteligência artificial, que podem identificar padrões de comportamento fraudulento em meio à utilização convencional dos recursos tecnológicos.

No cenário atual, onde constantes e crescentes ameaças têm como alvo os ativos de tecnologia da informação, assim como a imagem da organização e de seus colaboradores perante a sociedade, é imprescindível propiciar um ambiente de trabalho mais integrado a fim de que os usuários em teletrabalho sejam alcançados pelas mesmas ferramentas de proteção e de segurança disponíveis no órgão, aumentando a segurança, a produtividade e criando mecanismos eficiente de gestão.

Uma vez que as rotinas de trabalho também devem se adequar à aprovação de regulamentos na área tecnológica, como a Lei Geral de Proteção dos Dados (LGPD) qualquer solução adotada para a proteção dos *Endpoints* (estações de trabalho, notebooks, servidores virtuais em nuvem, impressoras, dispositivos USB de armazenamento e conexões de rede, inclusive com a Internet) também deve estar em conformidade com os marcos regulatórios.

A solução de proteção deve abranger o ambiente interno, de Intranet, com suas estações de trabalho, notebooks, servidores virtuais em nuvem, impressoras, dispositivos USB de armazenamento e conexões de rede, inclusive com a Internet, sob atualização constante em relação à proteção contra ameaças.

Como dito anteriormente, muitos servidores do órgão trabalham em regime de teletrabalho (*home office)*, assim, este contexto também deve ser avaliado em estudo técnico para a solução de proteção e segurança a ser adquirida.

Também destacou-se algumas entre as diversas metodologias de proteção que podem interessar ao INSS, e que também será algo de estudo:

- Gerenciamento de permissões de acesso a dispositivos USB;
- Gerenciamento de atualizações de aplicativos;
- Controle do acesso à rede e à Internet;
- Técnicas de prevenção contra a perda de dados;
- Detecção e resposta de ameaças com assinatura ainda não catalogada;
- Proteção *anti-malware*, evitando sua propagação na Intranet;
- Detecção de tráfego malicioso na Intranet;
- Detecção e proteção contra *phishing* vindo de sites fraudulentos;
- Proteção contra links maliciosos recebidos por e-mail;
- Proteção contra roubo de senha e de credenciais de acesso a aplicativos;
- Controle de acesso irregular (em horário não permitido, em estação de trabalho não permitida, etc.)
- Detecção de alto volume de trafego em contexto irregular (fora do horário, em estação de trabalho não permitida, múltiplos acessos simultâneos);
- Bloqueio da ação de *Bots*;
- Detecção de comportamentos irregulares de usuários, aplicativos ou serviços;
- Capacidade de identificar arquivos ou processos maliciosos;
- Reversão de dados para um estado anterior no caso de um ataque de *ransomware*;
- Isolamento de estações e processos suspeitos.

Em 2017 o Centro de Tratamento de Incidentes de Redes do Governo (CTIR Gov) por meio do "Alerta nº 07/2017-Ataques de Ransomware Bad Rabbi" reforçou a necessidade de manutenção dos softwares de antivírus para todos os órgãos e entidades da administração pública, tal medida visa mitigar as ameaças de sequestro de dados.

Por último, mas não menos importante, destaca-se a NOTA TÉCNICA Nº 1/2021/CGIN/DTI-INSS da Coordenação Geral de Infraestrutura de TIC - CGIN/DTI, documento SEI (4651370), da qual expõe medidas e propõe ações de tratamento e resposta a incidentes cibernéticos, além de atividades diversas concernentes à Segurança da Informação e Comunicação no âmbito do INSS.

Neste documento, registrou-se o modus operandi mais reiteradamente identificado - com base na compreensão atual - consiste no ingresso do(s) atacante(s) em alvos de rede **(equipamentos servidores)** do INSS instalados em Agências da Previdência Social ou em datacenters da Dataprev, podendo ser de propriedade do INSS (serviço de colocation) ou da própria Dataprev (serviço de hosting).

Dessa forma, toran-se indispensável a implantação de solução para proteção, ainda que básica, dos endpoints do INSS.

Além da solução de proteção avançada para Endpoints, o presente ETP visa a avaliar a necessidade de serviço agregado, como treinamento especializado e suporte técnico.

CONTEXTO DE SEGURANÇA ATUAL DO INSS

Neste tópico será apresentado o contexto de soluções de segurança vigentes no INSS, ou que estão em processo de estudo e projetização, com a finalidade de subsidiar e contextualizar as diretrizes básicas para a definição dos itens da contratação, bem como a sua futura implantação.

Iniciativas da DTI:

Projeto: Realização de hardening nos servidores linux

Sob a justificativa de mapear as ameaças, planejar os controles e mitigar os riscos relacionados a uma superfície de ataque, a saber os servidores GNU/Linux distribuídos pelas unidades da Autarquia, responsável pela exploração de vulnerabilidades que têm, promovido o roubo de credenciais, será realizado o processo de fortalecimento dos controles de segurança nos servidores por meio das seguintes ações que estão em fase de planejamento, dentre elas a atualização das versões dos servidores web hospedadas nestes servidores; atualização de bibliotecas, pacotes e ferramentas, bem como atualização do Sistema Operacional destes equipamentos.

Projeto: Desenvolver dashboard de SIC

Sob a justificativa de, no contexto de segurança cibernética, trazer maior visibilidade dos ativos de rede do Instituto, um painel único está em fase de planejamento, prospecção e desenho a fim de ser implantado como um concentrador de informações de segurança oriundas de bases de dados de diversas ferramentas, também em processo de implantação.

Projeto: Mapear processos de monitoramento de SIC (Outlook, EPS, Observador)

Sob a justificativa de aprimorar a segurança cibernética dos processos de mensageria contratada pela Autarquia, processos de monitoramento e controle de segurança, nativos e integrados em um painel único na própria solução, serão implantados, configurados e operacionalizados pela equipe de segurança do INSS.

Contrato nº 28/2020:

Contrato de prestação de serviços de tecnologia da informação e comunicação, de subscrição de licenças de uso de softwares Microsoft, do tipo suíte de escritório. Este contrato oferece solução de subscrição de licenças de suite de aplicações das quais, dentre elas, é o serviço de correio eletrônico Outlook 365, que conta com módulo de proteção nativa contra mensagens maliciosas e phishing dentro da própria suíte Microsoft.

GLOSSÁRIO

Considerando a necessidade de definir um **glossário**, ficam estabelecidos os seguintes termos:

- **EndPoint Security:** O Endpoint Security atua na interrupção de ameaças, no monitoramento da integridade geral do sistema e na geração de relatórios com informações sobre detecção e status. Em outras palavras, o sistema protege servidores, sistemas de computadores, laptops e tablets contra ameaças conhecidas e desconhecidas.
- **Data Loss Prevention (DLP)**: solução de prevenção à perda de dados que entrega funcionalidades como criptografia e mecanismos de anti-exfiltração. Ela também automatiza alguns processos de adequação da organização à LGPD (Lei Geral de Proteção de Dados).
- **Endpoint Detection and Response (EDR)**: a detecção e resposta a ameaças contra computadores monitora ameaças e permite a resposta contínua contra a exploração de vulnerabilidades por essas ameaças.
- **Endpoint and Server Security**: conjunto de soluções de segurança de estações de trabalho e servidores composta por módulos, configurados através de políticas e resumidos em painel único, como controle de dispositivos periféricos, controle de navegação web, proteção contra malware por meio da identificação de assinaturas conhecidas ou da identificação heurística de comportamentos de artefatos maliciosos.
- **Extended Detection and Response (XDR)**: ferramenta de detecção de ameaças de segurança e resposta a incidentes baseada em SaaS, específica do fornecedor, que nativamente integra vários produtos de segurança em um sistema de operações de segurança coeso que unifica todos os componentes licenciados.
- **Global Threat Intelligence Exchange Cloud**: nuvem global de compartilhamento de inteligência de ameaças que permite o compartilhamento de informações sobre ameaças e dados de segurança relevantes para a corporação. Solução que nivela as soluções de segurança com dados mais recentes sobre ameaças mapeadas e orienta de forma assertiva a equipe de segurança, de prevenção e de resposta a incidentes de segurança cibernética.
- **Zero-Trust:** modelo de segurança que desfaz o conceito de perímetro de segurança e aplica a abordagem de "nunca confiar, mas sempre verificar", ou seja, qualquer dispositivo nunca é considerado seguro por padrão e, uma vez que estejam conectados à rede corporativa, devem ser submetidos à avaliação de conformidade de segurança corporativa.
- **Zero-Trust Network Access (ZTNA)**: estratégia de composição de políticas granulares, adaptativas e sensíveis ao contexto a fim de fornecer acesso Zero-Trust, seguro e contínuo a aplicativos corporativos hospedados em nuvem ou em Data Centers locais por dispositivos remotos de qualquer local.

1. DEFINIÇÃO E ESPECIFICAÇÃO DAS NECESSIDADES E REQUISITOS

1.1. A seguir serão elencados os requisitos necessários à contratação definidos pela área requisitantes (Diretoria de Operações - DIOP), bem como pela área de tecnologia da informação do INSS (Diretoria de Tecnologia da Informação e Inovação - DTI), de acordo com suas competências e responsabilidades, obtidos a partir do DOD e de reuniões realizadas durante a elaboração deste ETP. Estes requisitos têm por fundamento estabelecer o que a solução contratada deverá atender, incluindo os requisitos mínimos de qualidade, e aqueles requisitos indispensáveis ao atendimento à necessidade de negócio e garantindo-se a economicidade da contratação.

1.2. Identificação das Necessidades de Negócio

1.2.1. As licenças fornecidas devem ser por subscrição e deverão permanecer ativas na vigência do contrato;

1.2.2. A solução deverá fornecer Console de Gerenciamento para controle e operacionalização, além de controle de políticas, para cada tipo de módulo de segurança contratado.

1.2.2.1. O console de gerenciamento de permitir a criação de políticas de segurança por perfis autorizados pela contratada;

1.2.2.2. Deverá permitir a instalação das licenças ou agentes em servidores, estações de trabalho e máquinas virtualizadas, via console de gerenciamento, com opção de remoção de soluções antivírus previamente instaladas;

1.2.2.3. Deverá possui painel de controles dashboard com acompanhamento e monitoramento em tempo real do status de cada endpoint.

1.2.3. Além do console de gerenciamento mencionado no item anterior, a Contratada deverá encaminhar mensalmente, em até 10 dias úteis após o fechamento do ciclo de faturamento, Relatório Mensal de Execução dos Serviços contendo no mínimo:

1.2.3.1. Mês/Ano de Referência;

1.2.3.2. Data de início e fim do ciclo de faturamento apurado;

1.2.3.3. Quantitativo de licenças/agentes efetivamente instalados no período apurado;

1.2.3.4. Logs e informações de quarentena gerados no período apurado;

1.2.3.5. Ocorrências geradas a partir de abertura de chamados pelo Contratante ou pela Contratada, com detalhamento de sua resolução, conforme Níveis Mínimos de Serviços Acordados;

1.2.3.6. Demais métricas que permitam a avaliação da efetividade dos serviços.

1.2.4. O pagamento relativo ao fornecimento do serviço será realizado mensalmente considerando o quantitativo de licenças efetivamente instaladas e comprovadas via relatório mensal de faturamento a ser encaminhado pela Contratada.

1.2.5. As faturas serão mensais ou por período estabelecido em contrato, conforme o quantitativo de licenças/agentes efetivamente instalados e apresentados no relatório mensal de serviços e atestados pelo gestor do contrato;

1.2.6. Em conformidade com o que versa a IN 01/2019, item 1.6, Anexo, a implantação de licenças e serviços agregados, deverão ocorrer de forma gradual, seguindo cronograma de implantação, cabendo o pagamento apenas sobre os quantitativos demandados, fornecidos e efetivamente implantados.

1.3. **Identificação das Necessidades Tecnológicas**

1.3.1. As especificações técnicas das licenças contendo maior nível de detalhamento se encontram anexadas ao processo, documento SEI (6581336), e **atualizadas** pelo documento SEI (7478553).

1.3.2. Cumpre ressaltar que o documento de Especificações Técnicas da Solução foi trabalhado no sentido de manter a ampla concorrência do certame e evitar especificações por demais criteriosas que pudessem restringir ou direcionar a participação de candidatos licitantes. Dessa forma, o mercado foi **amplamente consultado** acerca do que as soluções e suas tecnologias podem oferecer ou não, sempre mantendo o interesse da demanda de segurança cibernética do INSS como prioridade.

1.3.3. Tal consulta se fez imprescindível visando reduzir ao máximo os riscos relacionados à implantação das soluções em momento posterior, evitando-se assim, a inclusão de especificações que poderiam não estar de acordo com a infraestrutura de TI do órgão ou com as capacidades das tecnologias prospectadas junto ao mercado.

1.3.4. Todas as troca de e-mails, contendo questionamento formalizados pelo mercado se encontram compilados e anexados a este ETP, documento SEI (7473487).

1.4. **Alinhamento Institucional com essa contratação**

1.4.1. A contratação objeto deste estudo está alinhada com os seguintes alinhamentos institucionais:

I - Plano Diretor de Tecnologia da Informação e Comunicação - PDTIC

PDTI do INSS - 2020/2022 *RESOLUÇÃO Nº 13/CEGOV/INSS, DE 14 DE OUTUBRO DE 2020*		
5. Alinhamento com a Estratégia da Organização		
ID	**Objetivo**	**Ação Estratégica**
	Atualização e normalização da infraestrutura	Contratação de produtos e serviços de Tecnologia da Informação
6. Necessidades de TI Consolidadas		
ID	**Necessidade de TI**	**Descrição**
N1	Provimento, manutenção e atualização do parque de equipamentos e da infraestrutura de redes	O parque tecnológico contempla duas categorias: (1) Equipamentos de utilização direta pelos colaboradores e visitantes; (2) Equipamentos e soluções necessários para suportar a infraestrutura de TIC, mantidos diretamente pela DTI.

7. Plano de Metas e Ações			
Necessidades de TI Consolidadas	**Meta Descrição**	**Metas / Indicador**	**Ações**
N1 Provimento, manutenção e atualização do parque de equipamentos e da infraestrutura de redes	M1 Prover equipamentos e soluções para atender às necessidades dos usuários de TI	% de projetos concluídos conforme Plano Anual de Execução de Projetos (indicador anual)	A3 Prover ferramentas tecnológicas e licenças de software de uso corporativo

ANEXO I - NECESSIDADES DE TI				
Id	**Necessidade (oportunidade/problema)**	**Expectativa De Solução**	**Área Requisitante**	**Necessidades De TI Consolidadas**
110	Gestão dos processos de segurança da informação	Fomentar as ações de SIC e implementar processo	DTI	Aperfeiçoamento das iniciativas de segurança de tecnologia da informação

III - Plano Anual de Contratação 2022 - PAC 2022 (TI)

ITEM	**CÓDIGO DO ITEM**	**DESCRIÇÃO**	**DESCRIÇÃO SUSCINTA DO OBJETO**
297	26077	Software como Serviço - SaaS	Subscrição de suíte de software antivírus, antimalware, proteção contra ameças avançadas, outros.

2. **ESTIMATIVA DA DEMANDA – QUANTIDADE DE BENS E SERVIÇOS**

2.1. Neste tópico foi feito o registro do quantitativo de licenças necessárias para a composição da solução a ser contratada, de forma detalhada, motivada e justificada, inclusive quanto à forma de cálculo.

2.2. A estimativa de demanda foi realizada considerando o parque computacional do INSS (desktops), servidores hosts, servidores virtuais e equipamentos móveis (notebooks), bem como foi realizado levantamento do quantitativo de servidores públicos ativos no INSS, aplicando-se filtros sobre o valor glbola no intuito de chegar a um número mais preciso, considerando que o INSS possui quantidade relevante de servidores em regime de teletrabalho, instituido pela INSTRUÇÃO NORMATIVA Nº 65, DE 30 DE JULHO DE 2020.

2.3. A composição da solução, foi considerado o histórico de incidentes nos últimos 3 anos ocorridos no INSS, conforme anexo.

2.4. **Parque de Ativos Computacionais do INSS**

2.4.1. Visando subsidiar e embasar a estimativa definida neste item, optou-se pelo levantamento do parque de ativos computacionais do INSS, levando em consideração o aspecto de heterogeneidade do parque como um todo, além de buscar fontes de informação diversas no intuito consolidar o quantitativo da forma mais precisa, dentro da realidade do INSS. Considera-se o parque como "heterogêneo, devido à relevante discrepância entre a idade das máquinas, entre os pregões de compras de Desktops ocorridos nos últimos 10 anos, além dos próprios sistemas operacionais instalados compor-se de, principalmente, windows 7.

2.4.2. Conforme disposto acima, o parque de ativos computacionais do INSS é muito grande e não possui, além do cadastro patrimonial, um serviço de gestão de ativos contratado, de forma que sua composição, estado de conservação, equipamentos em processo de alienação, além de outros detalhes pertinentes, estejam bem controlados e mapeados. Desta forma, considerou-se o levantamento de fontes que pudessem expor um panorama mais completo possível do parque para que fosse possível calcular uma estimativa de demanda coerente com as necessidades do INSS.

2.4.3. O levantamento de ativos computacionais do INSS cosiderou as seguintes fontes para levantamento:

- Estações de Trabalho (desktops) patrimoniados;
- Equipamentos Móveis (notebooks) patrimoniados;
- Pregão nº 8/2020 de compra de computadores;
- Pregão nº 00009/2016 de compras de computadores;
- Pregão 013/2013 de compras de computadores, ano 2013;
- Consulta de quantitativos de Servidores Hosts;
- Consulta de quantitativos de Servidores Virtuais;
- Consulta de Servidores Públicos ativos no INSS;
- Consulta ao software público Configurador Automático e Coletor de Informações Computacionais, CACIC, mantido pela da Dataprev;
- Consulta ao número de licenças de suíte de escritório Microsoft Office 365 por perfil atribuído.

2.4.4. Além dos levantamentos patrimoniais, e das contratações que visaram a compra de micro computadores e notebooks, foram considerados mapear o quantitativo de servidores públicos ativos no INSS para se obter comparação destes com o quantitativo de estações de trabalho registradas pelo patrimônio, considerando que o número de pessoas utilizando as estações de trabalho pode fornecer uma perspectiva mais concreta, em face da provida pelo patrimônio. Foi aplicado filtro sobre o quantitativo levantado de servidores públicos ativos no INSS para os que estão em regime de teletrabalho do Programa de Gestão, tendo vista que estes servidores não estão utilizando as estações de trabalho do INSS.

2.4.5. Considerou-se mapear o contrato nº 28/2020 para subscrição de licenças de suite de escritório Microsoft Office 365, tendo em vista a similaridade da metodologia utilizada para aferição do quantitativo de licenças instaladas em cada estação de trabalho, para fins de comparação com os resultados encontrados nos outros levantamentos deste item.

2.4.6. Visando obter elementos para implantação de possível solução de proteção remota aos usuários que necessitam acessar a rede interna do INS via VPN, foi realizado levantamento do quantitativo de assinaturas de VPN ativas dentro de um determinado período.

2.4.7. Os demais levantamentos foram realizados consultando as demais áreas da DTI para se obter números de servidores de arquivos (hosts) físicos e virtuais, para finalização do cálculo de quantitativo dos endpoints a serem abarcados pelas soluções de proteção.

2.4.8. Os levantamentos realizados encontram-se distribuídos na tabela abaixo:

LEVANTAMENTO PATRIMONIAL	QUANTITATIVO
Computadores Desktop	65.876
Notebooks	3.681

Fonte: DSMAT/DGPA/INSS, ADMPER, anexo documento SEI (6581050)

PREGÕES	PROCESSO SEI	COMPUTADORES DEKTOPS	NOTEBOOKS
Pregão 013/2013 (Windows 7)	Anexo Homologação Nº 00013/2013 (SRP)	34.940	2.951
Pregão Nº 00009/2016 (Windows 10)	Anexo Homologação Nº 00009/2016 (SRP)	18.229	-
Pregão nº 8/2020 (Windows 10)	35014.075314/2020-43	2.980	127
TOTAL		**56.149**	**3.078**

Fonte: Aquisição Pregões 2013 e 2016, documento SEI (6581139)

TOTAL DE SERVIDORES PÚBLICOS ATIVOS - INSS (A)	PERITOS MÉDICOS FEDERAIS	TRABALHO PRESENCIAL (A-B)	TELETRABALHO PARCIAL	TELETRABALHO INTEGRAL (B)
27.947	3.249	24.676	1.752	3.271

Fonte: SIAPE, planilha documento SEI (6581157)

LICENÇAS SUITE MICROSOFT OFFICE 365- PERFIL ATRIBUÍDO	
Licenças F3	25.739
Licenças E1	2.848
Licenças E3	194
TOTAL	**28.781**

Fonte: Contrato 28/2020, dezembro/2021, documento SEI (6581193)

SERVIDORES COM ACESSO À VPN	QUANTITATIVO
Usuários Únicos Diários	6.000
Média de Usuários Simultâneos	4.200

*Fonte: informações dos contratos nº 19 e 20 de 2020,*Volumetria de Usuários (janeiro 2022). Volumetria de Usuários (janeiro 2022), documento SEI (5799543)

SISLAT - FORMULÁRIO WEB BASEADO EM REDMINE	QUANTITATIVO
Computadores Desktop	28.818
Servidores Linux	1.626

Fonte: NOTA TÉCNICA Nº 3/2021/DIOP/CSIT/CGIN/DTI, documento SEI (5617429) /Zabbix/ Planilha Extraída, documento SEI (6581260)

SERVIDORES VIRTUAIS	QUANTITATIVO
Servidoresde de Arquivo Virtuais - GovCloud	256
Servidores Virtuais - AWS	351

Fonte: Dataprev, Contrao 19/2020, anexo documento SEI (6581283)

2.4.9. Considerando as fontes consultadas e detalhadas nas tabelas acimas, percebe-se que as informações coletadas não são precisas, fato que se explica tendo em vista o INSS não possuir um contrato de Gestão de Ativos do parque computacional da Autarquia. Observa-se que, de acordo com levantamento patrimonial, têm-se mais microcomputadores do que o quantitativo de servidores ativos no INSS.

2.4.10. Considerando o que versa a IN 01/2019, item 1.5, Anexo, onde o volume de licenças e de serviços agregados a serem contratados deve refletir a necessidade do órgão, a Equipe de Planejamento da Contratação optou pelo quantitativo que mais se aproximasse da realidade do INSS, e considerou o número de servidores ativos, que efetivamente utilizam os equipamentos relacionados no objeto desta contratação por melhor refletir o quantitativo de licenças a serem adquiridas.

2.4.11. Diante do quantitativo impreciso, optou-se pela referência do quantitativo de servidores públicos ativos no INSS para base de cálculo do quantitativo de licenças a serem adquiridas sob demanda, adicionando-se a este valor os quantitativos de servidores de arquivo físicos e servidores de arquivo virtuais. Aplicou-se redutor sobre o valor global dos servidores inscritos no Programa de Gestão do INSS em regime de teletrabalho integral. O resultado encontra-se na tabela abaixo:

LEVANTAMENTO DO PARQUE	QUANTITATIVO ENDPOINTS
Servidores Públicos Ativos SIAPE	27.947
Peritos Médicos Federais	3.249
Servidores Físicos	1.626
Servidores Virtuais - GovCloud	256
Servidores Virtuais - AWS	351
TOTAL	**33.429**

2.4.12. Será acrescido ao resultado encontrado na tabela acima, um percentual de 10 % de licenças sob demanda, chegando-se ao quantitativo de **36.771 endpoints**, considerando que as licenças serão pagas sob demanda e pela imprevisibilidade no acréscimo de pessoal, a constante movimentação de pessoal, aposentados e servidores cedidos e oriundos de outros órgãos ou de novas aquisições de endpopints no âmbito do INSS.

2.4.13. O processo administrativo de contratação, documento SEI 35014.040622/2022-10, que trata da adesão às Atas de Registro de Preços nº 34/2021 e 39/2021 do Ministério da Economia - ME, cuja estimativa de aquisições estão detalhadas no Termo de Referência, documento SEI (6704517), também poderá impactar no quantitativo de estações de trabalhos e notebooks a serem utilizadas no ambiente do INSS, ainda que a justificativa de adesão à ata seja a de promover a substituição de parte do parque, não se pode ignorar a possibilidade de novas adesões para acréscimo de novos equipamentos, incluindo servidores de arquivo e rede físicos. Dessa forma, considerando que o pagamento pelas licenças ocorrem sob demanda, decidiu-se acrescentar **3.427** endpoints ao quantitativo final para se chegar a um valor fechado de 40.000 licenças a serem contemplados durante todo o período de vigência contratual.

2.4.14. Foi considerado também, o processo de contratação do contrato número 28//2020, firmado com a empresa Teltec para fornecimento de serviços de tecnologia da informação e comunicação, de subscrição de licenças de uso de softwares Microsoft, do tipo suíte de escritório, onde a previsibilidade para o quantitativo de licenças foi similar, chegando-se à quantitativo semelhante, conforme contrato documento SEI 2512467.

2.5. **Histórico de Incidentes Cibernéticos do INSS**

2.5.1. Com a finalidade de compreender o cenário de vulnerabilidade, os registros de reclamações e indicações de ataques de vírus ao parque computacional do INSS, foi solicitado à SSEG/DTI, um histórico de incidentes relacionados a ataques diretos a endpoints. Importante ressaltar que os chamados relacionados sobre ataques de vírus, phishing e malware dependem de abertura de chamados pelos usuários, tornando o quantitativo apurado aproximado. O levantamento se encontra relacionado na tabela abaixo:

Canal	Quantidade de Chamados Abertos	Período	Observações
suporte.inss.gov.br	30	01/21 - 17/01/22	Desde o início da utilização.
SDM	1.335	01/18 - 03/02/22	4 anos
E-mail ETIR - Vírus	40	01/21 - 17/01/22	Desde o início da utilização.
E-mail ETIR - Phishing	500	01/21 - 04/02/22	Desde o início da utilização.
E-mail ETIR - Malware	5	01/21 - 04/02/22	Desde o início da utilização.

F*onte: e-mail SSEG/DTI, documento SEI (6581348)*

2.6. Considerando os levantamento realizado, bem como as demais informações pertinentes levantadas, estabeleceu-se as soluções tecnológicas e demais intens agregados para a contratação. As informações estão dispostas na tabela abaixo:

ITENS	CATSER	DESCRICAO	DESCRIÇÃO DETALHADA	UNIDADE	QUANTIDADE
1	24333	Serviço de Subscrição de Licença de Software	Solução de Proteção de Endpoints - Computadores Desktops, Notebooks, Servidores de Arquivo Físicos e Virtuais, e Solução de	Unidade	40.000

			Detecção e Resposta de Ameaças de Computadores - Endpoint Detection and Response - EDR, incluindo gerenciamento centralizado, instalação dos agentes nas máquinas e suporte técnico e garantia pelo período contratual.		
2	16918	Serviços Técnicos Especializados de Implantação da Solução	Implantação dos componentes da console de gerenciamento central da solução no ambiente do INSS, bem como disponibilização das licenças ou agentes.	Serviço	1
3	3840	Treinamento Customizado da Solução	Treinamento especializado para prover conhecimento necessário à equipe para operação, monitoramento das soluções e criação das políticas de segurança.	Aluno	20

2.7. **Justificativa detalhada para as aquisições da licenças**

2.7.1. Solução de Proteção de Endpoints

2.7.1.1. A Solução de Proteção de Endpoints consiste na proteção básica do parque de ativos computacionais do INSS, que atualmente é inexistente. O último contrato de solução de Anti-Vírus no âmbito do INSS se encerrou em 2015, tendo a autarquia ficado sem a proteção básica de proteção às estações de trabalho e demais endpoints.

2.7.1.2. Ainda que os chamados abertos nos incidentes registrados desde o início do suporte INSS sejam razoavelmente baixos, conforme tabela do Item 2.5, não se justifica a ausência de proteção básica contra ataques diretos às estações de trabalho do INSS, considerando a abrangência do parque bem como a quantidade de servidores públicos que atuam no órgão, deixando uma ampla margem de vulnerabilidade em se tratando de órgão tão relevante como o INSS.

2.7.1.3. No mundo da segurança da informação contra ataques cibernéticos, a grande maioria dos ataque se aproveitam do fato de que a maior parte dos endpoints são usados e mantidos por usuários comuns, que não costumam ter a habilidade para reconhecer que o endpoint está sendo atacado, muito menos protegê-lo, fazendo com que o usuário final seja o elo mais fraco na segurança abrindo possibilidades para violações de dados.

2.7.1.4. A solução visa assegurar que todos os serviços e terminais conectados a uma rede estejam protegidos contra vários tipos de ataques cibernéticos como worms, cavalos de troia, spywares, adwares, rootkits e ataques de vulnerabilidades de software, sendo considerada a proteção básica e essencial para qualquer organização que possui terminais conectados a uma rede corporativa.

2.7.2. Solução de Detecção e Resposta de Ameaças de Computadores - *Endpoint Detection and Response* - EDR

2.7.2.1. O EDR é uma parte importante que compõe a segurança para endpoints, e é responsável por proteger de forma proativa a rede contra ameaças de endpoint. A segurança de EDR é composta de práticas e tecnologias que monitoram constantemente e proativamente a atividade de endpoints, identifica ameaças e é capaz de iniciar respostas e tratamentos automáticos contra ataques.

2.7.2.2. As soluções de EDR fornecem visibilidade em tempo real para a rede de endpoints, assim como capacidades proativas para identificar e responder às ameaças de endpoint. Para tornar possível essas capacidades, as soluções de EDR fazem uso de mecanismos como, coleta e armazenamento de Dados, detecção e análise de comportamento, que estabelecem um padrão normal de atividade no endpoint e identifica quais anomalias representam atividade maliciosa.

2.7.2.3. Considerando o cenário atual, no âmbito do INSS, a solução se justifica pelo fortalecimento dos controles de segurança no tratamento de incidentes de segurança cibernéticas relacionadas ao vazamento de credenciais, facilita a a atuação guiada e automatizada no tratamento e correlação de incidentes de segurança cibernética focados nos endpoints e servidores pelo SOC, e promove a condução das ações de segurança conforme o planejamento de segurança para 2022, a saber, criação de um SOC e de um painel de segurança centralizado.

3. ANÁLISE DAS SOLUÇÕES

3.1. Conforme inciso II do art. 11, deve-se verificar para composição da análise comparativa: A disponibilidade de solução similar em outro órgão ou entidade da Administração Pública; As alternativas do mercado; A existência de software público brasileiro; As políticas, os modelos e os padrões de governo, a exemplo do ePing, eMag, ePwg, ICP-Brasil e e-ARQ Brasil, quando aplicáveis; As necessidades de adequação do ambiente do órgão ou entidade para viabilizar a execução contratual (exemplo: mobiliário, instalação elétrica, espaço adequado para prestação do serviço, etc); A possibilidade de aquisição na forma de bens ou contratação como serviço; Os diferentes modelos de prestação do serviço; Os diferentes tipos de soluções em termos de especificação, composição ou características dos bens e serviços integrantes; A ampliação ou substituição da solução implantada.

3.2. **Disponibilidade de solução similar em outro órgão ou entidade da Administração Pública**

3.2.1. No âmbito da Administração Pública, o serviço de subscrição de licenças de software de Proteção de Endpoints é amplamente utilizada, dada a sua relevância no cenário atual, onde as ameaças cibernéticas são crescentes, diferenciadas e apresentam elevado grau de sofisticação, exigindo dos governos ações efetivas de prevenção e combate às práticas maliciosas no uso de Tecnologia da Informação, por meio de ações transversais, integradoras, interdisciplinares e multi-setoriais.

3.2.2. Os diferentes tipo de tecnologia disponíveis no mercado oferecem diversas técnicas e módulos de proteção tornando as opções disponíveis bastante abrangentes. Dessa forma, a pesquisa de preços e de mercado considerou os filtros que inclui-se os termos "Proteção de Endpoints", "antivírus", de forma genérica, e as soluções encontradas em contratações em outras entidades da Administração Pública, foram analisadas conforme o contexto e, posteriormente, foram incluídas no item 5 deste ETP - Análise da Pesquisa de Preços.

3.2.3. A Equipe de Planejamento da Contratação realizou pesquisa de mercado para posterior formação da cesta de preços, além de registro das fontes consultadas, como os portais oficiais do Governo Federal, mídias especializadas, contratações similares em outros entes públicos e pesquisa direta com fornecedores da solução, conforme pode-se verificar no item 5 deste estudo preliminar.

3.3. **Quanto à Existência de Software Público Brasileiro**

3.3.1. A solução objeto deste estudo preliminar não se trata de software público brasileiro e não consta em seus catálogos, pois trata-se de solução privada que consiste em fornecimento de Subscrição de Software de Proteção Avançada de Endpoints, que permite estabelecer soluções de segurança de estações de trabalho e servidores composta por módulos, configurados através de políticas aplicadas através de um console de gerenciamento centralizado, incluindo suporte técnico especializado.

3.4. **Necessidades de Adequação do Ambiente do Órgão ou Entidade**

3.4.1. Não foram identificadas necessidades de adequação aos ambientes do INSS para implantação da solução.

3.5. **Possibilidade de Aquisição na Forma de Bens ou Contratação como Serviço**

3.5.1. A solução objeto deste estudo preliminar deverá ser contratada enquanto Software como Serviço - SaaS, considerando que não se trata aquisição de bens, e sim de serviços de subscrição de licenças de software, não necessitando da aquisição de quaisquer equipamentos ou bens agregados para seu funcionamento.

3.6. **Diferentes Modelos de Prestação do Serviço**

3.6.1. Foram identificados 2 modelos de faturamento para a prestação do serviço, conforme abaixo:

3.6.1.1. Aquisição e subscrição de licença de software com pagamento mensal (aluguel);

3.6.1.2. Aquisição e subscrição de licença de software com pagamento único por licença;

3.6.2. O formato mais viável para a contratação será que a apresentar melhor custo benefício ao INSS, a ser confirmado pelo resultado da Pesquisa de Preços, item 5 - Análise da Pesquisa de Preços deste Estudo Preliminar.

3.6.3. Demais modelos de contratação fornecida pelo tipo de solução foi analisada e comparada no item 3.10 - Análise Comparativa das Soluções.

3.6.4. Sobre as formas de hospedagem para as soluções, foram identificados os seguintes modelos

3.6.4.1. Hospedagem física local *on premisse*;

3.6.4.2. Hospedagem em nuvem.

3.6.5. O modelo de hospedagem a ser adotado, conforme disposto na tabela comparativa de soluções, item 3.11. deste ETP, será o modelo de Gerência Centralizada **hospedada em nuvem**, diante das seguintes vantagens identificadas

3.6.5.1. Gerenciamento centralizado;

3.6.5.2. Redução de custos e investimentos com infraestrutura local;

3.6.5.3. Padronização das aplicações para todo o Instituto;

3.6.5.4. Maior disponibilidade e facilidade na recuperação e arquivamento;

3.6.5.5. Facilidade de acesso ás aplicações considerando-se a estrutura altamente capilar do Instituto;

3.6.5.6. Facilidade de migração de ambientes.

3.7. **Da Substituição da Solução**

3.7.1. A solução analisada neste ETP poderá ser avaliada a sua substituição, considerando o prazo contratual a ser definido, bem como as mudanças de cenário de infraestrutura do INSS, e em conformidade com o que versa o item 1.4.1 da IN 01/2019, Anexo, a saber:

3.7.1.1. Serviço de Diretório - AD, gerido pelo INSS;

3.7.1.2. Link de Dados de Internet, gerido pelo INSS;

3.7.1.3. Serviço de gestão de Ativos de Parque Computacional e de Rede, gerido pelo INSS;

3.7.1.4. Custo benefício amparado por pesquisa de preços em momento oportuno.

3.8. **Do Suporte Técnico Especializado**

3.8.1. O suporte técnico necessário para a execução dos serviços consiste na manutenção e disponibilidade da solução do serviço dentro dos parâmetros a ser definidos dentro do Termo de Referência, e em conformidade com o que versa a IN 01/2019, item 1.4.5, Anexo.

3.8.2. O Suporte Técnico não constituirá item apartado do objeto da contratação considerando que a solução é atrelada aos serviços subscrição de licenças providas pelas fabricantes das soluções, cujo suporte técnico remoto precisar ser prestado e gerenciado pelos mesmos fornecedores da solução a ser contratada.

3.8.3. A Contratada deverá prestar o Suporte Técnico e Especializado, pelo período de vigência do contrato e da validade das subscrições, para sanar os problemas relacionados com as soluções e funcionamento pleno das licenças/agentes instaladas nos computadores (endpoints e servidores), bem como pela manutenção da plataforma de console de gerenciamento online indicado no item 4.1.2.

3.8.4. Os serviços de suporte deverão ser corretivos, proativos e consultivos, envolvendo atividades como auxílio na configuração de políticas e administração da solução, instalação de novas versões, patches e hotfixes, análise de dúvidas sobre melhores práticas de configuração, entre outros;

3.8.5. A Contratada deverá realizar o suporte técnico on-site ou de maneira remota.

3.8.6. Entende-se por Suporte Técnico Remoto as seguintes atividades:

3.8.6.1. Esclarecimento e resolução de quaisquer falhas identificadas na:

3.8.6.2. Suporte à instalação das licenças/agentes;

3.8.6.3. Operacionalização da console de gerenciamento;

3.8.6.4. Indisponibilidade do serviço contratados;

3.8.6.5. Quaisquer outros suportes correlatos ao serviço contratado;

3.8.7. Deverão ser fornecidas obrigatóriamente todas as atualizações de versão que ocorrerem durante toda a vigência das subscrições.

3.8.8. A Contratada deve garantir que novas versões de software ou atualizações dos produtos em garantia tenham a perfeita compatibilidade com o ambiente operacional em uso nas instalações do Contratante.

3.8.9. Os chamados deverão ser abertos pela Contratante através de canais disponibilizados pela Contratada, sem ônus ao Contratante, respeitando-se os Acordos Mínimos de Serviços;

3.8.10. A Contratada deverá manter ferramentas de monitoramento contra incidentes que afetem as soluções contratadas e a console de gerenciamento, independente da abertura de chamados feito pela Contratante, conforme o item anterior;

3.8.11. Durante o período contratual, os serviços de suporte técnico remoto serão prestados por técnicos credenciados pela Contratada e devidamente habilitados e certificados nas soluções adquiridas. .

3.8.12. O suporte técnico será realizado 24 (vinte e quatro) horas por dia, 07 (sete) dias por semana, incluindo feriados, conforme Instrumento de Medição de Resultado.

3.8.13. Toda e qualquer despesa decorrente do suporte realizado durante o período contratual do serviço prestado será de responsabilidade da Contratada.

3.8.14. As informações sobre os canais de atendimento para abertura dos chamados deverão ser apresentadas à Contratante na reunião inicial, após a assinatura do Contrato.

3.8.15. A Contratada deverá providenciar o registro de toda e qualquer solicitação de suporte técnico, independentemente de sua natureza, cabendo à Contratante, o devido acompanhamento.

3.8.16. Deverão ser disponibilizados canais de atendimento para abertura dos chamados à Contratante conforme segue:

3.8.16.1. Website ou;

3.8.16.2. Telefone ou;

3.8.16.3. Portal web.

3.8.17. O Portal referido deverá estar formatado para a lingua portuguesa.

3.8.18. O início do Suporte será considerado a partir do chamado registrado e entregue à contratada pelos meios disponibilizados pela mesma.

3.8.19. O Suporte deverá ser tratado por técnico especializado e certificado pelo fabricante da solução. A certificação deverá ser apresentada conforme Modelo de Execução do Contrato, item 6 deste Termo de Referência.

3.8.20. Cada chamado deverá conter, no mínimo, o registro das informações abaixo:

3.8.20.1. Número único do chamado;

3.8.20.2. Data e hora da abertura do chamado;

3.8.20.3. Descrição do problema a ser solucionado;

3.8.20.4. Data e hora do início do atendimento;

3.8.20.5. Data e hora do encerramento do atendimento.

3.8.21. Entende-se por resolução do chamado o tempo total desde a abertura do chamado até a solução do problema.

3.9. Identificação das Soluções

3.9.1. A tabela abaixo consta os itens a serem utilizados para a Análise Comparativa das Soluções e seus respectivos quantitativos, baseados nos levantamentos feitos anteriormente:

ITENS	CATSER	DESCRICAO	DESCRIÇÃO DETALHADA	UNIDADE	QUANTIDADE
1	27502	Serviço de Subscrição de Licença de Software	Solução de Proteção de Endpoints - Computadores Desktops, Notebooks, Servidores de Arquivo Físicos e Virtuais, e Solução de Detecção e Resposta de Ameaças de Computadores - Endpoint Detection and Response - EDR, incluindo gerenciamento centralizado, instalação dos agentes nas máquinas e suporte técnico e garantia pelo período contratual.	Unidade	40.000
2	26972	Serviços Técnicos Especializados de Implantação da Solução	Implantação dos componentes da console de gerenciamento central da solução no ambiente do INSS, bem como disponibilização das licenças ou agentes.	Serviço	1
3	3840	Treinamento Customizado da Solução	Treinamento especializado para prover conhecimento necessário à equipe para operação, monitoramento das soluções e criação das políticas de segurança.	Aluno	20

3.10. Análise Comparativa das Soluções

3.10.1. Conforme descrito nos itens anteriores, não foram identificadas outras soluções ou outros modelos de prestação de serviços para provimento de internet patrocinada, sendo a reversão dos dados móveis ao INSS a única solução disponível nas fontes consultadas, conforme verificado no item 5 deste ETP.

3.10.2. A Portaria STI/MP nº 46, de 28 de setembro de 2016 de políticas, modelos e os padrões de governo, a exemplo dos Padrões de Interoperabilidade de Governo Eletrônico - ePing, Modelo de Acessibilidade em Governo Eletrônico - eMag, Padrões Web em Governo Eletrônico - ePwg, Infraestrutura de Chaves Públicas Brasileira - ICP-Brasil e Modelo de Requisitos para Sistemas Informatizados de Gestão Arquivística de Documentos - e-ARQ Brasil, quando aplicáveis:

Requisito	Solução	Sim	Não	Não se Aplica
A Solução encontra-se implantada em outro órgão ou entidade da Administração Pública?	Solução 1	X		
A Solução está disponível no Portal do Software Público Brasileiro? (quando se tratar de software)	Solução 1		x	
A Solução é composta por software livre ou software público? (quando se tratar de software)	Solução 1		x	x
A Solução é aderente às políticas, premissas e especificações técnicas definidas pelos Padrões de governo ePing, eMag, ePWG?	Solução 1			x
A Solução é aderente às regulamentações da ICP-Brasil? (quando houver necessidade de certificação digital)	Solução 1			x
A Solução é aderente às orientações, premissas e especificações técnicas e funcionais do e-ARQ Brasil? (quando o objetivo da solução abranger documentos arquivísticos)	Solução 1			x

3.11. **Matriz Comparativa de Soluções**

3.12. Neste item buscou-se compararas soluções levando-se em conta os aspectos funcionais das tecnologias disponíveis no mercado e as mais utilizadas em outros órgãos da Adminstração Pública, em função dos requisitos de tecnologia, do cenário de infraestrutura e de governança do INSS, para avaliar a viabilidade de cada uma dessas soluções.

Apectos Funcionais e Requisitos da Solução	Solução 1	Solução 2	Solução 3	Solução 4	Solução 5
	Solução de Proteção de Endpoints	Solução de Proteção de Dados e Anti-Exfiltração de Dados, *Data Loss Protection* - DLP	Solução de Detecção e Resposta de Ameaças de Computadores - *Endpoint Detection and Response* - EDR	Solução de Nuvem Compartilhada de Inteligência contra Ameaças e análise avançada de malware	Solução de Acess Rede *Zero-Trust* p computadores - *Trust Network Acc* ZTNA
Descrição Sucinta	Proteção de computadores composta pelos módulos básicos: prevenção a ameaças baseada em assinaturas bem conhecidas, firewall, controle web, controle de aplicações e proteção baseada em comportamento malicioso.	Proteção de dados classificáveis por políticas a fim de garantir a confidencialidade e exfiltração de informações sensíveis.	Detecção de incidentes cibernéticos conforme políticas estabelecidas de forma a permitir o seu tratamento de forma orquestrada e automatizada a fim de embasar uma resposta.	Compartilhamentos de informações de Inteligência de Ameaças a fim de orientar o SOC e gerenciar campanhas de segurança.	Controle de acess aplicavos. ZTN estende os princípiosde Zero Access(ZTA) pa verificarusuário dispositivosantes eles acessem aplicavo. Issoper validar queele atendem à polí segurança daemp para acessar a aplicação.
Modalidade de Hospedagem	• Software hospedado localmente; • Gerência centralizada majoritariamente hospedada em nuvem, conforme tendências do mercado.	• Software hospedado localmente; • Gerência centralizada majoritariamente hospedada em nuvem, conforme tendências do mercado.	• Software hospedado localmente; • Gerência centralizada majoritariamente hospedada em nuvem, conforme tendências do mercado.	• Software hospedado em infraestrutura local com acesso a nuvens privadas, públicas e híbridas, conforme tendências do mercado.	• Software hospedado infraestrut local com acesso a nu privadas, públicas e híbridas, conforme tendências mercado.
Vantagens	• Ausência de solução de segurança para endpoints no ambiente do INSS.	• Facilita a adequação à LGPD • Tem conformidade com tratamento de perda de dados; • Promove automatização do mapeamento e proteção de dados sensíveis; • Possibilita a catalogação de dados conforme classificação institucional.	• Promove insumos para a atuação de equipe de SOC; • Alimenta o Dashboard de SIC com o objetivo de alertar e conduzir as ações de resposta dos analistas do SOC.	• Possibilita o nivelamento das soluções de segurança com os dados consumidos de forma que operem orquestradamente ante a iminentes e mapeados riscos de segurança; • Promove informação para os analistas do SOC e orienta assertivamente sua atuação.	• Otimização custo e desempenh em relação VPN; • Solução complemer no estabelecim de controle segurança p estações alienígenas modalidade trabalho re e trabalho híbrido; • Solução baseada em Infraestrut como servi IaaS; • Concessão acessos granulares aplicativos usuários de

					forma a iso diminuir a exposição c informaçõe sobre a infraestrutu de rede.
Desvantagens	• Possível elevação do consumo de recursos (CPU, RAM e disco) das estações e servidores.	• Possível elevação do consumo de recursos (CPU, RAM e disco) das estações e servidores. • Incompatibilidades com os servidores GNU/Linux do INSS.	• Armazenamento local nas estações e servidores de dados de incidentes de segurança; • Possível limitação de funcionalidades em servidores GNU/Linux; • Possível elevação do consumo de recursos (CPU, RAM e disco) das estações e servidores.	• Baixa maturidade de segurança do INSS para consumo de tais informações.	• Ausência de funcionalid homogênea entre os fornecedor • Necessidad instalação c agentes e d integração soluções ge exclusivam pela Datapr • Largura de banda de re adequada e gerenciável INSS.
Riscos da Contratação	• Ausência de solução de Service Desk para a implantação, operação e manutenção da solução; • Ausência de serviço de diretório; • Ausência de Gestão de Ativos; • Capacidade de banda limitada nos links disponíveis nas unidades do INSS; • Hospedagem em nuvem majoritariamente praticada pelo mercado; • Necessidade de adequação à INSTRUÇÃO NORMATIVA Nº 5 DO GSI, DE 30 DE AGOSTO DE 2021.	• Ausência de solução de Service Desk para a implantação, operação e manutenção da solução; • Ausência de serviço de diretório; • Ausência de Gestão de Ativos; • Ausência de classificação da informação madura para o embasamento das políticas de criptografia anti-exfiltração; • Capacidade de banda limitada nos links disponíveis nas unidades do INSS; • Hospedagem em nuvem majoritariamente praticada pelo mercado; • Necessidade de adequação à INSTRUÇÃO NORMATIVA Nº 5 DO GSI, DE 30 DE AGOSTO DE 2021.	• Ausência de solução de Service Desk para a implantação, operação e manutenção da solução; • Ausência de serviço de diretório; • Ausência de Gestão de Ativos; • Capacidade de banda limitada nos links disponíveis nas unidades do INSS; • Hospedagem em nuvem majoritariamente praticada pelo mercado; • Necessidade de adequação à INSTRUÇÃO NORMATIVA Nº 5 DO GSI, DE 30 DE AGOSTO DE 2021.	• Riscos de implantação e manutenção com baixo impacto.	• Envolve nov contratação • Custo de entrada em produção m do que a solução atualmente uso (VPN).

4. REGISTRO DE SOLUÇÕES CONSIDERADAS INVIÁVEIS

4.1. Conforme § 1º do art. 11 da IN 01/2019, as soluções identificadas e consideradas inviáveis deverão ser registradas no Estudo Técnico Preliminar da Contratação (breve descrição e justificativa), dispensando-se a realização dos respectivos cálculos de custo total de propriedade.

4.2. Considerando a Matriz Comparativa das Soluções do item 3.11, as soluções consideradas inviáveis, bem como suas justificativas encontram-se resumidas na tabela abaixo:

SOLUÇÃO	NOME DA SOLUÇÃO
2	Solução de Proteção de Dados e Anti-Exfiltração de Dados, *Data Loss Protection* - DLP
5	Solução de Acesso de Rede *Zero-Trust* para computadores - *Zero Trust Network Access* - ZTNA

6	Solução de Correlacionamento de Comportamento entre estações, servidores e ativos de rede (eXtended Detection and Response – XDR)
7	Microssegmentação de Processos, Aplicativos, Usuários, Atividades de Rede e Computadores
8	Solução de Prevenção, Detecção e Mitigação Lógica de Keylogger Físico

4.3. As soluções a seguir foram desconsideradas levando-se em conta o que versa a IN 01/2019 em seu Anexo, item 1 - CONTRATAÇÃO DE LICENCIAMENTO DE SOFTWARE E SERVIÇOS AGREGADOS, a saber, a necessidade de se alinhar a aquisição de licenças de software e seus serviços agregados às reais necessidades do órgão para evitar gastos com produtos e serviços não utilizados;

4.4. Foi considerado neste mesmo tópico, oque versa o item 1.4.3 da mesma IN 01/2019, Anexo, a compatibilidade de produtos alternativos que viabilizem a utilização da solução, de modo a não aceitar que se condicione o fornecimento de produto ou de serviço ao fornecimento de solução específica. Desta forma, o cenário dos sistemas operacionais disponíveis no parque computacional e dos servidores de arquivo, físicos e virtuais, foi apresentado de forma clara e objetiva nas especificações técnica anexa a este ETP, bem como em reuniões com diversos fabricantes e fornecedores para expor ao mercado as necessidades de compatibilidade disponíveis no INSS no momento atual, de modo que a sua futura implantação seja viabilizada com minimização de riscos.

4.5. Solução de DLP: A demanda pela solução de proteção de dados veio do DOD e foi prospectada neste ETP pela Equipe de Planejamento, considerando que o INSS mantém uma grande quantidade de dados considerados sensíveis sob sua guarda.

4.5.1. A solução de DLP foi incluída na lista de itens para contratação em um primeiro momento, bem como foi realizada pesquisa de preços públicos para se chegar a uma cesta de preços. No entanto, a maioria dos fornecedores das soluções encaminharam manifestações desfavoráveis ao uso do DLP no ambiente do INSS, através de análise das especificações técnicas, devido a fatores de incompatibilidade desta solução com o servidores físicos GNU/Linux.

4.5.2. As empresas que manifestaram formalmente os problemas relacionados ao DLP no ambiente do INSS se encontram consolidadas no documento SE (7473487):

4.5.3. Além das considerações formalizadas pelos fornecedores, foi feita consulta à Divisão de Segurança em TI, DSEG/DTI no sentido de saber se a DTI já possui alguma política e/ou projeto que trate acerca do tema de proteção de dados sensíveis no âmbito do INSS, onde foi respondido através de e-mail, documento SEI (6581373).

4.5.4. A DSEG informou no e-mail acerca da ferramenta de proteção de dados integrada MIP. Faz parte desta suíte de aplicativos alguns recursos da Proteção de Informações da Microsoft (MIP). Os recursos de MIP estão incluídos na Conformidade do Microsoft 365 e fornecem as ferramentas para que se possa conhecer, proteger e evitar a perda de dados. Um dos recursos do MIP permite a criação de políticas de DLP. No Microsoft 365, com uma política de DLP, pode-seidentificar, monitorar e proteger automaticamente itens confidenciais em:

- Microsoft 365 serviços como Teams, Exchange, SharePoint e OneDrive
- Office aplicativos como Word, Excel e PowerPoint
- Windows 10, Windows 11 e pontos de extremidade macOS (Catalina 10.15 e superior)
- aplicativos de nuvem que não são da Microsoft
- Compartilhamentos de arquivos locais e SharePoint.

4.5.5. Desta forma, entende-se que a exclusão da solução de DLP, considerando as limitações e problemas de compatibilidade colocadas, não vão trazer prejuízos ao INSS. A implantação da solução, bem como das demais soluções excluidas desta contratação poderão ser estudadas novamente em outra oportunidade, quando as limitações apresentadas forem superadas.

4.6. Solução de ZTNA: Conforme quadro comparativo, embora a solução possa prover proteção para os acessos remotos no ambiente do INSS, ela exige um link de dados com largura de banda mais robusta do que existe de disponível na autarquia. Existe a previsão de contratação de link de dados em andamento, no entanto, considerando-se o risco desta contratação não ocorrer, optou-se por descartar a solução a fim de se evitar problemas com a implementação da solução.

4.6.1. Na tabela do item 3.12 deste ETP contém maior detalhamento das limitações desta solução no ambiente de TI do INSS.

4.7. Solução de XDR: Embora a solução avançada de detectação e resposta - XDR possa prover respostas robustas de segurança, foi identificado gargalos e limitações para sua implantação no ambiente do INSS, conforme detalhado no quadro comparativo de soluções. A solução ainda é recente no mercado sendo a oferta consideravelmente heterogênea, dependendo de equipe de SOC e gestão de ativos de rede gerenciado pelo próprio INSS, o que não é a realidade atual da Autarquia.

4.7.1. Na tabela do item 3.12 deste ETP contém maio detalhamento das limitações desta solução no ambiente de TI do INSS.

4.8. Microsegmentação de Rede: A solução, conforme demonstrado na tabela comparativa de soluções, embora promova uma melhor visibilidade às atividades ativas na rede do INSS, demonstrou baixa relevância para o escopo do projeto, considerando que o INSS ainda não possui um controle básico de atividades maliciosas no ambiente de rede, sendo o controle granular uma solução avançada que dependeria de equipe de SOC sedimentada com necessidade de controle administrativo, bem como a dependência de uma gestão de ativos de rede gerenciado pelo próprio INSS. A solução também dependerá de largura de banda de rede mais robusta do que disponível no ambiente atual do INSS.

4.8.1. Na tabela do item 3.12 deste ETP contém maio detalhamento das limitações desta solução no ambiente de TI do INSS.

4.9. Solução de Prevenção e Detecção de Keylogger Físico: Os ataques relacionados a keylogger Físicos foram abordados no DOD do projeto, sendo considerado relevante a busca por soluções que possam prover proteção adequada a este tipo de ameaça. No entanto, as soluções apresentadas pelos fornecedores, registradas no item 5 deste ETP, bem como em todas as reuniões realizadas pela Equipe de Planejamento, não atendem a demanda levantada no DOD, bem como não foi encontrada em pesquisas em mídia especializada, soluções que possam atender a demanda, sendo que as demais soluções demonstraram atender parcialmente este cenário de ameaça, gerando incerteza para a sua inclusão no escopo do projeto.

4.9.1. Não foi possível encontrar referências, ou soluções que atendessem plenamente a demanda levantada no DOD em nenhuma fonte para a pesquisa de preços.

5. ANÁLISE DA PESQUISA DE PREÇOS

5.1. Normativos aplicados na pesquisa de preço

5.2. A equipe de planejamento da contratação realizou pesquisa de mercado com objetivo de encontrar o valor de mercado do item, para posterior cálculo dos Custos Totais de Propriedade.

5.3. A pesquisa segue as seguintes orientações:

5.3.1. INSTRUÇÃO NORMATIVA Nº 1, DE 4 DE ABRIL DE 2019 da SGD/ME que dispõe sobre o processo de contratação de soluções de Tecnologia da Informação e Comunicação - TIC pelos órgãos e entidades integrantes do Sistema de Administração dos Recursos de Tecnologia da Informação - SISP do Poder Executivo Federal.

5.3.2. INSTRUÇÃO NORMATIVA Nº 73, DE 5 DE AGOSTO DE 2020. 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.

5.4. **Identificação do agente responsável pela cotação**

5.4.1. Foram analisadas contratações por entes públicos, sites especializados, e diretamente com os fornecedores, sendo descrito o resultado da análise, e quando considerado pela equipe, entrou para o cálculo da cesta de preço do item.

5.4.2. A pesquisa foi realizada no painel de preços, mídia e com os fornecedores entre o período 09/03/2022 e 18/03/2022, pelos responsáveis: Rafael Roque Leite <rafael.leite@inss.gov.br>, matrícula SIAPE 1221311 e Edir Vargas Coelho <edir.vargas@inss.gov.br>, matrícula SIAPE 3195239.

5.5. **Parâmetros e fontes da pesquisa de preços**

5.5.1. A pesquisa de preços foi realizada mediante a utilização dos seguintes parâmetros:

5.5.1.1. **Painel de Preços**, disponível no endereço eletrônico gov.br/painel de preços, desde que as cotações refiram-se a aquisições ou contratações firmadas no período de até 1 (um) ano anterior à data de divulgação do instrumento convocatório;

5.5.1.2. Dados de pesquisa publicada em **mídia especializada,** 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 instrumento convocatório, contendo a data e hora de acesso;

5.5.1.3. Pesquisa com **contratações similares com outros entes públicos**.

5.5.1.4. Pesquisa direta com **fornecedores**, mediante solicitação formal de cotação, desde que os orçamentos considerados estejam compreendidos no intervalo de até 6 (seis) meses de antecedência da data de divulgação do instrumento convocatório.

5.6. **Filtros utilizados no Painel de Preços**

5.6.1. Identificação do CATSER

5.6.2. CATSER 27502

5.6.2.1. Item: 1

5.6.2.2. Descrição: Cessão Temporária de Direitos Sobre Programas de Computador Locação de Software

5.6.2.3. Unidade: Unidade

5.6.2.4. Natureza Despesa: 33904006, 33909240, 33914006

5.6.3. CATSER 26972

5.6.3.1. Item: 2

5.6.3.2. Descrição: Serviços de Instalação, Transição e Configuração / Parametrização de Software

5.6.3.3. Unidade: Unidade

5.6.3.4. Natureza Despesa: 33903657, 33904021, 33909236, 33909240, 33914021, 44903657, 44904003, 44904005, 44909236, 44909240

5.6.4. CATSER 3840

5.6.4.1. Item: 3

5.6.4.2. Descrição: Treinamento Informática - Sistema / Software

5.6.4.3. Unidade: Unidade

5.6.4.4. Natureza Despesa: 33904020, 33909240, 33914020

5.7. **Pesquisa em Mídia Especializada**

5.7.1.

5.8. **Pesquisa de contratações similares com outros entes públicos**

5.8.1. A pesquisa de contratações similares com outros entes públicos apresentou resultados cujos parâmetros foram aceitos pela Equipe de Planejamento da Contratação. Os contratos e respectivos anexos encontram-se no anexo Pesquisa de Preços com Outros Entes, documento SEI (6581410).

5.9. **Pesquisa de Preços junto aos fornecedores da solução**

5.10. A pesquisa realizada junto aos fornecedores do mercado foi realizada através do e-mail conforme modelo de proposta de preços documento SEI (7475643).

5.11. O INSS solicitou às empresas para incluir na propostas as seguintes informações:

5.11.1. Informações da empresa (timbre, razão social, CNPJ, endereço, telefone, e-mail, site);

5.11.2. Assinatura do responsável pela elaboração da proposta;

5.11.3. Número e data da proposta;

5.11.4. Validade da proposta;

5.11.5. Informações do objeto ofertado (descrição do objeto, unidade, valor unitário mensal, valor total para um período de 12 meses de contrato.)

5.12. Adicionalmente, foi incluso o registro nos autos da contratação correspondente da relação de fornecedores que foram consultados e não enviaram propostas como resposta à solicitação de que trata o inciso IV do caput art 5° da IN nº 73/2020 bem como o § 2º, inciso III do mesmo artigo.

5.13. O registro da relação de fornecedores que foram consultados e a relação das respostas dadas ao INSS estão indicadas na tabela abaixo:

Pesquisa	Empresa	A empresa entregou Proposta Comercial?	Respondeu ao INSS por e-mail?	A empresa manifestou interesse em participar do processo?	A empresa comercializa todos os itens (serviços, suporte e exigências do TR)?	Solicitou esclarecimentos?	Sugeriu adequações nas especificações?	Apresentou algum teste do serviço a ser contratado ?	Apresent algum IF ou ATA vigente
FORNECEDORES	Guardicore								Não
	NetSafe	Sim	Sim	Sim	Sim	Sim	Sim	Não	Não
	Oi	Sim	Sim	Sim	Sim	Sim	Sim	Não	Não
	NetSecurity		Sim	Sim	Sim	Sim	Sim	Não	Não
	Future		Sim			Sim	Sim	Não	Não
	Acorp								Não
	Kaspersky		Sim	Sim	Sim	Sim	Sim	Não	Não
	Xsite								Não
	Aboutnet	Sim	Sim	Sim	Sim				Não
	Brasoftware		Sim	Sim	Sim	Sim	Sim	Não	Não
	Network	Sim	Sim	Sim	Sim			Não	Não
	Teletex	Sim	Sim	Sim	Sim			Não	Não
	Inbtec								Não

5.14. **Série de preços coletados**

5.14.1. **Critérios -** A pesquisa de preços, sempre que possível, deverão ser observadas as condições comerciais praticadas, incluindo prazos e locais de entrega, instalação e montagem do bem ou execução do serviço, formas de pagamento, fretes, garantias exigidas, podendo ser de qualquer marcas e modelos, desde que atendam as exigências da contratação.

5.14.2. **Parâmetros -** Conforme determinado no Inciso I do art. 5º da Instrução Normativa nº 73 de 5 de agosto de 2020 da Secretaria de Gestão / Secretaria Especial de Desburocratização, Gestão e Governo Digital / Ministério da Economia, foram priorizadas as pesquisas de mercado realizadas no Painel de Preços do Governo e Contratações realizadas por outros Entes Públicos. Além das fontes citadas, foram efetuadas coleta de preços em mídias especializadas e sites comerciais de diversos fornecedores de certificados digitais existentes no mercado, bem como consulta direta junto a esses fornecedores.

5.14.3. **Metodologia** - A definição do Método matemático aplicado para a definição do valor estimado e as Justificativas para a metodologia utilizada, bem com a definição dos valores estimados para cada item da contratação.

5.15. Foi elaborada a pesquisa de preços e anexado ao processo, com a finalidade de comparar os preços coletados e inseridos em uma cesta de preços, considerando as fontes pesquisadas, conforme orientação da INSTRUÇÃO NORMATIVA Nº 1, DE 4 DE ABRIL DE 2019 da SGD/ME e INSTRUÇÃO NORMATIVA Nº 73, DE 5 DE AGOSTO DE 2020.

5.16. Como parâmetro de comparação de preços, optou-se pela utilização da **média saneada** dos preços encontrados, tendo em vista os preços coletados apresentarem variação excessiva.

5.17. Em cumprimento ao § 2º, Art. 2º, da Instrução Normativa N° 5/2014 da SLTI/MPOG, foram utilizados **mais de 3 preços**, de diferentes fontes para compor a cesta de preços.

5.18. O rol de preços coletados na pesquisa encontram-se no Anexo III - Planilha Pesquisa de Preços Consolidada, documento SEI (7472451).

5.19. As propostas de preços e os termos de homologação desses pregões e demais evidências encontram-se nos seguintes anexos:

5.19.1. Anexo - Pesquisa de Preços Painel de Preços documento SEI (7473226);

5.19.2. Anexo - Pesquisa de Preços Mídia Especializada documento SEI (6581391);

5.19.3. Anexo - Pesquisa de Preço Outros Entes documento SEI (6581410);

5.19.4. Anexo - Pesquisa de Preços Fornecedores documento SEI (7473487).

5.20. **Resultado obtido da Cesta de Preços**

5.20.1. **Metodologia de cálculo**

5.20.1.1. A cesta de preços foi obtida a partir da **média aritmética simples** de todos os preços encontrados nas fontes pesquisadas, desconsiderado os preços excessivamente elevados, bem como, os excessivamente baixos, mas que compuseram o subconjunto para obtenção do preços com os valores mais homogêneos.

5.20.1.2. Abaixo, segue-se o resultado da cesta de preços considerando a média aritmética dos preços coletados. A memória de cálculo contendo detalhamento do método matemático aplicado na obtenção da cesta de preços pode ser verificada no anexo, **documento SEI** (7472451).

6. ANÁLISE COMPARATIVA DE CUSTOS (TCO)

6.1. A análise do TCO foi realizada considerando-se o quantitativo de licenças no primeiro ano contemplando as Estações de Trabalho (31.196), Servidores Virtuais - GovCloud (256) e Servidores Virtuais - AWS (351) - totalizando 31.803 licenças, conforme tabela abaixo:

Item	Descrição do Item	Quantidade	1º ANO	2º ANO	3º ANO	4º ANO	5º ANO
1	Subscrição de Licenças	40.000 (un)	R$ 5.036.005,05	R$ 6.334.000,00	R$ 6.334.000,00	R$ 6.334.000,00	R$ 6.334.000,00
2	Implantação	1 (un)	R$ 416.253,27	-	-	-	-

3	Treinamento	20 (alunos)	R$ 98.240,00	-	-	-	-

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

7.1. As soluções optadas pela Equipe de Planejamento da contratação estão dispostas na tabela a seguir.

ITENS	CATSER	DESCRICAO	DESCRIÇÃO DETALHADA	UNIDADE	QUANTIDADE	VALOR DE REFERÊNCIA UNITÁRIO	VALOR DE REFERÊNCIA TOTAL
1	24333	Serviço de Subscrição de Licença de Software	Solução de Proteção de Endpoints - Computadores Desktops, Notebooks, Servidores de Arquivo Físicos e Virtuais, e Solução de Detecção e Resposta de Ameaças de Computadores - Endpoint Detection and Response - EDR, incluindo gerenciamento centralizado, instalação dos agentes nas máquinas e suporte técnico e garantia pelo período contratual.	Unidade	40.000	R$ 158,35	R$ 6.334.000,00
2	16918	Serviços Técnicos Especializados de Implantação da Solução	Implantação dos componentes da console de gerenciamento central da solução no ambiente do INSS, bem como disponibilização das licenças ou agentes.	Serviço	1	R$ 416.253,27	R$ 416.253,27
3	3840	Treinamento Customizado da Solução	Treinamento especializado para prover conhecimento necessário à equipe para operação, monitoramento das soluções e criação das políticas de segurança.	Aluno	20	R$ 4.912,00	R$ 98.240,00

7.2. Convém ressaltar que a solução escolhida neste presente estudo não contem item presente nos Catálogos de Soluções de TIC com Condições Padronizadas publicados pelo Órgão Central do SISP, portanto, não existindo os elementos constantes do respectivo Catálogo, tais como: especificações técnicas, níveis de serviços, códigos de catalogação, PMC-TIC, entre outros.

7.3. Por fim, a Equipe de Planejamento da Contratação atesta expressamente que este Estudo Técnico Preliminar da Contratação atendeu a todas as orientações contidas no Anexo I, item 1.4 da IN SGD nº 01/2019, conforme descrito nos itens anteriores.

8. **ESTIMATIVA DE CUSTO TOTAL DA CONTRATAÇÃO**

8.1. De acordo com a cesta de preços encontrada, o valor global da contratação é de R$ **6.848.493,27** (seis milhões, oitocentos e quarenta e oito mil quatrocentos e noventa e três reais e vinte e sete centavos), para o período de 12 meses iniciais**.**

9. **DECLARAÇÃO DE VIABILIDADE DA CONTRATAÇÃO**

9.1. Diante deste Estudo Técnico Preliminar, entende-se como **VIÁVEL**, técnica e economicamente, a contratação da demanda, mediante procedimento licitatório sob o critério de "menor preço". Esta contratação trata de bens comuns, sendo comumente adquiridos por muitos órgãos públicos, e de grande oferta pelo mercado, o que garantirá ampla concorrência e, consequentemente, economia ao Instituto.

10. **APROVAÇÃO E ASSINATURA**

10.1. A Equipe de Planejamento da Contratação foi instituída pela **PORTARIA DGPA/INSS Nº 342, DE 03 DE DEZEMBRO DE 2021**, documento SEI (5771121)**.**

10.2. Em conformidade com § 2º do Art. 11 da IN SGD/ME nº 01, de 2019, o Estudo Técnico Preliminar deve ser assinado pelos Integrantes Técnicos e Requisitantes e pela Autoridade Máxima da Área de TIC:

INTEGRANTE TÉCNICO	INTEGRANTE REQUISITANTE	INTEGRANTE ADMINISTRATIVO	APOIO

Rafael Roque Leite	Jullyano Lino da Silva	Ana Carolina Mateus Borges	Edir Vargas Coelho
Matrícula SIAPE: 1221311	Matrícula SIAPE: 1786967	Matrícula/SIAPE: 3234387	Matrícula: 3195239

AUTORIDADE MÁXIMA DA ÁREA DE TIC
JOÃO RODRIGUES DA SILVA FILHO Matrícula SIAPE: 1561845 Diretor de Tecnologia da Informação

Documento assinado eletronicamente por **Rafael Roque Leite**, **Integrante Técnico**, em 26/10/2022, às 19:05, 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 **EDIR VARGAS COELHO**, **Empregado Público Cedido**, em 26/10/2022, às 19:05, 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 26/10/2022, às 19:05, 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 **JULLYANO LINO DA SILVA**, **Coordenador(a) Geral de Infraestrutura e Operações**, em 26/10/2022, às 19:08, 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 31/10/2022, às 14:14, 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 **9462971** e o código CRC **1516321B**.

Referência: Processo nº 35014.048537/2021-19 SEI nº 9462971

Criado por rafael.leite, versão 2 por edir.vargas em 26/10/2022 18:41:39.