FUNDAÇÃO NACIONAL DE SAÚDE

ESTUDO TÉCNICO PRELIMINAR DA CONTRATAÇÃO

Processo nº 25100.006254/2021-77

1. INTRODUÇÃO

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

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

2. DESCRIÇÃO DA NECESSIDADE

2.1. Descrição da Solução de Tecnologia da Informação

2.1.1. Trata-se de demanda da Coordenação-Geral de Modernização e Tecnologia da Informação - CGMTI para analisar viabilidade de aquisição de licenças de solução de gateway de segurança de e-mails (AntiSpam) para a FUNASA, com fornecimento de serviço de instalação e configuração, suporte, manutenção especializada e garantia de toda a solução por 12 (doze) meses, e ainda treinamento, conforme especificações constantes no Termo de Referência.

2.1.2. Bens e serviços que compõem a solução

ITEM	DESCRIÇÃO	MÉTRICA	QUANTIDADE
1	Solução de software de gateway de segurança de e-mails (AntiSpam), com fornecimento de serviços especializados por 12 meses	Caixas Postais	4500
2	Serviço de Instalação e Configurações da Solução de gateway e segurança de e-mails.	Unidade	1
3	Treinamento	Pessoa	3

Tabela 1 – Descrição da Solução.

2.2. Motivação/Justificativa

2.2.1. Atualmente, há aproximadamente 4.500 (quatro mil e quinhentos) caixas de e-mail ativas na Funasa enviando e recebendo uma média de 8.000 (oito mil) e-mails por dia. Pode-se observar que o e-mail é uma ferramenta de extrema importância para o desempenho das atividades desta autarquia.

2.2.2. Ainda, houve um investimento no licenciamento da plataforma Office 365, que tem trazido aos usuários da Funasa a possibilidade de utilização de soluções de tecnologia como plataforma, sem a necessidade de especificação e automatização pela área de tecnologia, o que garante agilidade aos processos de negócio e uniformidade nos procedimentos e serviços utilizados. Atualmente, a Funasa obtém de 3.190 licenças na plataforma Office 365, utilizando o pacote Office, exchange, Teams, Armazenamento OneDrive, etc.

2.2.3. Neste sentido, a aquisição de solução do tipo AntiSpam visa proporcionar maior segurança aos usuários deste serviço tanto no sentido de se evitar os spams recebidos diariamente quanto mitigar o crescente número de tentativas de roubo de senhas e dados. A ferramenta pretendida proporcionará, também, certo nível de inteligência propiciando a atualização, em tempo real, de acordo com o surgimento de novas ameaças à segurança e integridade do serviço de e-mail no ambiente da Funasa. É importante destacar também que se trata não apenas de um incremento na segurança, mas uma necessidade.

2.2.4. Essa solução é mais uma camada de segurança utilizada para detectar e remover as mais variadas formas de ameaças virtuais, tanto para ambientes domésticos quanto para, sobre tudo, redes corporativas. Em um mundo caótico onde a sofisticação dos ataques cibernéticos está em evidência, é fundamental a adoção de modernas soluções de antispam e antivírus com capacidade de proteger contra ameaças dos tipos “objetos maliciosos" Browser Helper (BHOs), sequestradores de navegador, ransomware, keyloggers, backdoors, rootkits, cavalos de tróia, worms, PEL maliciosos, dialers, fraudtools, adware e spyware, dentre outros. Além disso, incluem ainda proteção contra URLs maliciosas infectadas, fraude e ataques de phishing, roubo de identidade digital, ataques bancários on-line, técnicas de engenharia social, ameaças persistentes avançadas (APT), botnets e ataques DDoS, sendo capazes de atuar sobre as inúmeras variantes de sistemas operacionais disponíveis no mercado. O foco da solução é evitar a disseminação dessas ameaças no serviço de e-mail corporativo.

3. DEFINIÇÃO E ESPECIFICAÇÃO DAS NECESSIDADES E REQUISITOS

3.1. Identificação das necessidades de negócio

3.1.1. A Fundação Nacional de Saúde (FUNASA), órgão executivo do Ministério da Saúde, é uma das instituições do Governo Federal responsável por promover a inclusão social por meio de ações de saneamento para prevenção e controle de doenças. É também a instituição responsável por formular e implementar ações de promoção e proteção à saúde relacionadas com as ações estabelecidas pelo Subsistema Nacional de Vigilância em Saúde Ambiental.

3.1.2. No que se refere à gestão de tecnologia da informação, os princípios e os fundamentos formulados pela FUNASA têm como sustentação a correta utilização de recursos de infraestrutura e o planejamento de informatizar seus processos, nesse sentido, existe a necessidade de um aporte tecnológico (hardware e software) capaz de manter a integridade, confidencialidade e disponibilidade das informações.

3.1.3. A contratação faz-se indispensável pois visa prover segurança e proteção, de forma a minimizar e em grande parte coibir a contaminação dos serviços e sistemas informatizados por programas ou atividades digitais maliciosas, contribuindo para a garantia do nível mínimo adequado e desejado de proteção dos dados e informações da Funasa.

3.1.4. Esta contratação também possui o objetivo de atender as exigências sobre a proteção de dados apoiando demandas da Lei Geral de Proteção de Dados - LGPD, bem como auxiliar a CGMTI na análise e proteção dos dados e informações que transitam por e-mail, através da solução de gateway de segurança de e-mails.

3.1.5. O projeto em questão está em conformidade e encontra-se alinhado ao Plano Diretor de Tecnologia da Informação – PDTIC da FUNASA e proposta orçamentária de 2022, bem como ao Planejamento Institucional 2018 - 2023.

ALINHAMENTO AOS PLANOS ESTRATÉGICOS	
ID	**OBJETIVOS ESTRATÉGICOS**

N4	Implantar e atualizar controles que promovam a Segurança da Informação e Comunicações
N9	Melhorar a prestação de serviços à sociedade através da transformação digital

Tabela 2 - Alinhamento aos Planos Estratégicos.

ALINHAMENTO AO PDTIC DA FUNASA			
ID	**META**	**ID**	**AÇÃO**
M5	Implementar ações de Segurança da Informação e Proteção de Dados (adequação tecnológica à LGPD)	A5.3	Implementação de controles para conformidade com a LGPD
		A5.9	Aquisição de nova ferramenta de Anti-Spam

Tabela 3 – Alinhamento da Demanda ao PDTIC da Funasa

ALINHAMENTO AO PLANEJAMENTO INSTITUCIONAL 2018 - 2023		
ID	**CÓD. DA INICIATIVA**	**TÍTULO DA INICIATIVA**
OE11	IE11.3A	Implementar o Plano de Transformação Digital como Plano Estratégico, em consonância com a Política de Gestão da Informação

Tabela 4 – Alinhamento da Demanda ao Planejamento Institucional da Funasa.

ALINHAMENTO AO PAC 2022		
Nº ITEM	**TIPO DE ITEM**	**DESCRIÇÃO**
261	Serviços de TIC	LICENCIAMENTO DE DIREITOS PERMANENTES DE USO DE SOFTWAREPARA SERVIDOR

Tabela 5 – Alinhamento da Demanda ao PAC 2022 da Funasa.

ALINHAMENTO À ESTRATÉGIA DE GOVERNO DIGITAL
A presente aquisição também guarda alinhamento à Estratégia de Governo Digital (EGD) para o período de 2020 a 2022, instituída pelo Decreto nº 10.332, de 28 de Abril de 2020, no tocante ao Objetivo Estratégico OE 16 "**Otimização das infraestruturas de tecnologia da informação**". Para alcance desse objetivo estratégico, a EGD enuncia como iniciativa (Iniciativa nº 16.1) a realização de, no mínimo, seis compras centralizadas de bens e serviços comuns de TIC, até 2022.

Tabela 6 - Alinhamento da demanda à Estratégia de Governo Digital.

3.2. **Requisitos Tecnológicos e Demais Requisitos**

3.2.1. **REQUISITOS DE CAPACITAÇÃO**

3.2.1.1. A CONTRATADA deverá repassar à CONTRATANTE todas as informações solicitadas e documentação da solução;

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

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

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

3.2.1.5. O treinamento deverá capacitar as equipes técnicas do CONTRATANTE a operar, configurar, administrar e resolver problemas usuais na solução adquirida, englobando tanto os componentes de hardware quanto de software;

3.2.1.6. Deverá ser ofertada para 3 (três) pessoas e com carga horária mínima de 40 (quarenta) horas;

3.2.1.7. Deverá ser fornecido certificado de conclusão emitido pelo fabricante;

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

3.2.1.9. Deverá ser fornecido material didático completo e com conteúdo oficial do fabricante.

3.2.2. **REQUISITOS LEGAIS**

3.2.3. A contratação do objeto deste Estudo tem amparo legal nos seguintes dispositivos legais:

3.2.4. Lei nº 8.666, de 21 de junho de 1993, que regulamenta o art. 37, inciso XXI, da Constituição Federal, institui normas para licitações e contratos da Administração Pública e dá outras providências;

3.2.5. Lei 12.349, altera as de 21 de junho de 1993, 8.958, de 20 de dezembro de 1994, e 10.973, de 2 de dezembro de 2004; e revoga o §1° do art. 2° da Lei no 11.273, de 6 de fevereiro de 2006.

3.2.6. Decreto nº 3.555, de 08 de agosto de 2000, que aprova o Regulamento para a modalidade de licitação denominada pregão, para aquisição de bens e serviços comuns;

3.2.7. Lei nº 10.520, de 17 de julho de 2002, que institui, no âmbito da União, Estados, Distrito Federal e Municípios, nos termos do art. 37, inciso XXI, da Constituição Federal, modalidade de licitação denominada pregão, para aquisição de bens e serviços comuns, e dá outras providências;

3.2.8. Decreto nº 5.450, de 31 de maio de 2005, que regulamenta o pregão, na forma eletrônica, para aquisição de bens e serviços comuns, e dá outras providências;

3.2.9. Lei Complementar nº 123, de 14 de dezembro de 2006, que institui o Estatuto Nacional da microempresa e da Empresa de Pequeno Porte, altera dispositivos das Leis nºs 8.212 e 8.213, ambas de 24 de julho de 1991, da Consolidação das Leis do Trabalho – CLT, aprovada pelo Decreto-Lei nº 5.452, de 1º de maio de 1943, da Lei nº 10.189, de 14 de fevereiro de 2001, da Lei Complementar nº 63, de 11 de janeiro de 1990; e revoga as Leis nºs 9.317, de 5 de dezembro de 1996, e 9.841, de 5 de

3.2.10. Instrução Normativa nº 05 do MPOG, de 26 de maio de 2017, que dispõe sobre as regras e diretrizes do procedimento de contratação de serviços sob o regime de execução indireta no âmbito da Administração Pública federal direta, autárquica e fundacional;

3.2.11. Instrução Normativa Nº 1, de 4 de abril de 2019. 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.

3.2.12. Instrução Normativa SEGES /ME nº 65, de 7 de julho de 2021, que dispõe sobre o procedimento administrativo para a realização de pesquisa de preços para aquisição de bens e contratação de serviços em geral, no âmbito da administração pública federal direta, autárquica e fundacional;

3.2.13. A referida contratação deve assegurar os princípios da Lei Geral de Proteção de Dados Pessoais (LGPD - Lei nº 13.709/2018), descritos no Artigo 6º. da Lei. Toda informação trafegada, por meio dos equipamentos de tecnologia da informação e comunicação, que fazem parte do objeto de contratação devem atender às exigências da Lei Geral de Proteção de Dados Pessoais.

3.3. REQUISITOS DE MANUTENÇÃO E GARANTIA

3.3.1. A garantia de funcionamento das licenças adquiridas, bem como o suporte técnico serão pelo período de 36 (trinta e seis) meses.

3.3.2. O serviço de assistência técnica em GARANTIA deverá cobrir todos os procedimentos técnicos destinados ao reparo de eventuais falhas apresentadas nos equipamentos, de modo a restabelecer seu normal estado de uso e dentre os quais se incluem a substituição de peças, ajustes e reparos técnicos em conformidade com manuais e normas técnicas especificadas pelo fabricante.

3.3.3. Durante o prazo de garantia será substituída sem ônus para o CONTRATANTE, a parte ou peça defeituosa, após a conclusão do respectivo analista de atendimento de que há a necessidade de substituir uma peça ou recolocá-la no sistema;

3.3.4. Para efeitos de certificar a garantia, a CONTRATADA deve possuir recurso disponibilizado via web, site do próprio fabricante, que permita verificar a garantia do equipamento através da inserção do seu número de série;

3.3.5. A substituição de componentes ou peças decorrentes da garantia não gera quaisquer ônus para o CONTRATANTE. Toda e qualquer peça ou componente consertado ou substituído, fica automaticamente garantido até o final do prazo de garantia técnica do contrato;

3.3.6. Os serviços de suporte técnico abrangem:

3.3.6.1. Manutenção preventiva, manutenção corretiva, esclarecimento de dúvidas e reparação de problemas na solução;

3.3.6.2. Elaboração de relatórios, estudos e diagnósticos sobre o ambiente;

3.3.6.3. Transferência de conhecimento aos técnicos da CONTRATANTE referente aos problemas vivenciados e às soluções aplicadas, na forma a ser determinada pelas partes;

3.3.6.4. Realização de instalação, atualização e configuração de novas versões dos produtos após a disponibilização das atualizações tecnológicas pelo fabricante.

3.3.7. O suporte técnico contempla o atendimento para sanar dúvidas relacionadas com instalação, configuração e uso do software ou para correção de problemas, em especial na configuração de parâmetros, falhas, erros, defeitos ou vícios identificados no funcionamento da solução.

3.3.8. O suporte técnico deve contemplar, quando for o caso, atendimento a eventual problema de instalação ou configuração de softwares básicos e de infraestrutura de TIC (sistemas operacionais, servidores de banco de dados, servidores de aplicação, etc.) necessários ao funcionamento da solução;

3.3.9. Deve contemplar também a atualização de versões do software aplicativo, as quais incorporam correções de erros ou problemas registrados e melhorias implementadas pela fabricante, num empacotamento estável do sistema. O serviço de atualização de versão tem por finalidade assegurar a devida atualização da solução durante o período de vigência da garantia. Refere-se ao fornecimento de novas versões e releases da solução lançados no período. A cada nova liberação de versão e release, será disponibilizada em formato digital manuais e demais documentos técnicos, bem como nota informativa das funcionalidades implementadas. Em caso de lançamento de patch de correção, a CONTRATADA deverá comunicar o fato ao CONTRATANTE e indicar a forma de obtenção e os defeitos que serão corrigidos pelo patch. Em ambos os casos, a comunicação deve ser feita no prazo de até 30 (trinta) dias, a contar do lançamento de nova versão ou solução de correção;

3.3.10. A CONTRATADA será responsável pelos serviços de implantação das novas versões e releases dos produtos por ela fornecidos como partes do objeto, bem como pela aplicação dos patches de correção e pacotes de serviço (service packs) relativos a esses produtos. Para a implantação das novas versões/releases, bem como para a aplicação dos patches, deverá ser aberto chamado de suporte técnico com nível de severidade adequado e a prestação dos serviços deve ser agendada com os responsáveis pela solução na CONTRATANTE;

3.3.11. Deverá ser prestado suporte técnico remoto com atendimento mediante registro de chamados em página de website, em sistema fornecido pela CONTRATADA e/ou pelo fabricante; e também através de contato telefônico. Esse serviço destina-se a esclarecimento de dúvidas e resolução de problemas relacionados à configuração e uso dos componentes da solução CONTRATADA;

3.3.12. As peças substitutas deverão apresentar padrões de qualidade e desempenho iguais ou superiores aos das peças utilizadas na fabricação do equipamento e devem integrar a garantia da solução;

3.3.13. A CONTRATADA auxiliará o CONTRATANTE na reinstalação das ferramentas, caso seja necessário, ao longo do tempo de garantia da ferramenta;

3.3.14. A CONTRATADA deverá disponibilizar os seguintes canais de acesso ao suporte técnico: Portal Web, E-mail, Central 0800 e/ou telefone fixo;

3.3.15. O atendimento deve ser 24x7x365, ou seja, 24 (vinte e quatro) horas por dia em 7 (sete) dias da semana por 365 (trezentos e sessenta e cinco) dias por ano, em língua portuguesa;

3.3.16. O recebimento dos equipamentos/serviços será efetivado pela equipe designada pelo CONTRATANTE, e dar-se-á da forma provisória e definitiva. A forma provisória será no ato da entrega dos equipamentos/serviços e a forma definitiva será após a instalação, configuração e teste da solução.

3.4. REQUISITOS TEMPORAIS

3.4.1. O prazo de início de atendimento para os chamados de suporte técnico e manutenção pela garantia deverá estar de acordo com o especificado no acordo de nível de serviço do Termo de Referência;

3.4.2. O prazo de entrega e instalação deverá estar de acordo com o especificado no Termo de Referência, caso não seja especificado um prazo diferente na ordem de serviço.

3.4.3. Os equipamentos e as licenças de softwares devem ser entregues em Brasília, no endereço descrito na tabela abaixo:

UF	ENDEREÇO
DF	SAUS QUADRA 04 , BL- N. Cidade: Brasília. UF: Distrito Federal - DF. CEP: 70070040. - Brasília/DF - CEP: 70.719-040 - Telefone: (61) 3314-6466/6442 Fax: (61) 3314-6253

Tabela 7 - Endereço de entrega da solução.

3.4.4. A entrega dos equipamentos deverá acontecer no horário compreendido entre as 09:00 as 17:00 e poderá ser agendada em data e hora previamente com a CONTRATANTE;

3.4.5. Caberá ao CONTRATANTE rejeitar no total ou em parte, os materiais entregues em desacordo com o objeto do Termo de Referência.

3.4.6. O recebimento dos equipamentos será efetivado pela equipe designada pelo CONTRATANTE, e dar-se-á da forma provisória e definitiva. A forma provisória será no ato da entrega dos equipamentos e a forma definitiva será após a instalação, configuração e teste da solução.

3.5. **REQUISITOS DE SEGURANÇA**

3.5.1. A empresa CONTRATADA para prestação dos serviços deverá observar os seguintes requisitos quanto à Segurança da Informação e Comunicações:

3.5.1.1. Deverão ser observados os regulamentos, normas e instruções de segurança da informação e comunicações adotadas pela FUNASA, incluindo, mas não se limitando, ao definido na Política de Segurança da Informação e Comunicações e suas Normas Complementares, durante a execução dos serviços nas instalações da FUNASA;

3.5.1.2. Deverá ser garantida a disponibilidade, integridade, confidencialidade e sigilo dos documentos e informações inerentes ao contrato e seus serviços, podendo ser responsabilizado legalmente quem porventura causar perdas e danos à FUNASA e a terceiros;

3.5.1.3. Toda informação confidencial gerada e/ou manipulada em razão desta contratação, seja ela armazenada em meio físico, magnético ou eletrônico, deverá ser devolvida nas seguintes hipóteses, mediante formalização entre as partes:

a) Término ou rompimento do Contrato; ou

b) Solicitação da FUNASA.

3.5.1.4. Devem ser utilizadas ferramentas de proteção e segurança de informações, a fim de evitar qualquer acesso não autorizado aos sistemas e softwares, seja em relação ao que eventualmente estejam sob sua responsabilidade direta ou que foram disponibilizados a FUNASA, ainda que por meio de link;

3.5.1.5. Quando solicitado formalmente pela FUNASA, deverão ser realizadas, prioritária e concomitantemente, alterações para sanar possíveis problemas de segurança ou de vulnerabilidade nos referidos sistemas ou softwares utilizados para execução do serviço contratado;

3.5.1.6. A CONTRATADA deverá informar à FUNASA, formalmente e tempestivamente, sobre quaisquer necessidades de atualização ou mudança na configuração dos serviços prestados;

3.5.1.7. Prestar os esclarecimentos necessários à FUNASA, bem como informações concernentes à natureza e andamento dos serviços executados, ou em execução;

3.5.1.8. Garantir a integridade e disponibilidade dos documentos e informações que, em função do Contrato, estiverem sob a sua guarda, sob pena de responder por eventuais perdas e/ou danos causados a FUNASA e a terceiros;

3.5.1.9. A empresa CONTRATADA não poderá divulgar, mesmo que em caráter estatístico, quaisquer informações originadas na FUNASA, sem prévia autorização;

3.5.1.10. O acesso às instalações da CONTRATADA onde serão realizados os serviços deverá ser controlado e permitido somente às pessoas autorizadas;

3.5.1.11. A CONTRATADA deverá manter os seus profissionais identificados por crachás, quando em trabalho, devendo substituir imediatamente aquele que seja considerado inconveniente à boa ordem ou que venha a transgredir as normas disciplinares da FUNASA;

3.5.1.12. A CONTRATADA deverá manter os seus profissionais informados quanto às normas disciplinares da FUNASA, exigindo sua fiel observância, especialmente quanto à utilização e segurança das instalações;

3.5.1.13. Deverá ser celebrado TERMO DE COMPROMISSO entre a CONTRATADA e a FUNASA para garantir a segurança das informações da FUNASA, assim como, celebrado o TERMO DE CIÊNCIA a todos envolvidos na prestação dos serviços;

3.5.1.14. Não transferir a terceiros os serviços contratados;

3.5.1.15. Manter sigilo absoluto sobre todas as informações provenientes dos serviços realizados, documentos elaborados e informações obtidas dentro da FUNASA.

3.6. **REQUISITOS SOCIAIS, AMBIENTAIS E CULTURAIS**

3.6.1. Aderência aos padrões definidos pelo Modelo de Acessibilidade em Governo Eletrônico – e-MAG, conforme a Portaria Normativa SLTI nº 03, de 7 de maio de 2007, quando houver necessidades de acessibilidade ao aplicativo para solicitações de suporte técnico;

3.6.2. Os serviços prestados pela Contratada deverão pautar-se sempre no uso racional de recursos e equipamentos, de forma a evitar e prevenir o desperdício de insumos e materiais consumidos bem como a geração excessiva de resíduos, a fim de atender às diretrizes de responsabilidade ambiental adotadas pela Contratante; e

3.6.3. A Contratada deverá instruir os seus empregados quanto à necessidade de racionalização de recursos no desempenho de suas atribuições, bem como das diretrizes de responsabilidade ambiental adotadas pela Contratante, autorizando a participação desses em eventos de capacitação e sensibilização promovidos pela Contratante, quando for o caso.

3.7. **REQUISITOS DE PAGAMENTO**

3.7.1. As Ordens de Serviço somente serão validadas e liberadas para pagamento quando as condições a seguir forem satisfeitas:

3.7.1.1. As licenças forem entregues e instaladas pela CONTRATADA atendendo às especificações contidas no Termo de Referência;

3.7.1.2. O fornecedor emitir certificado de garantia de 12 (doze) meses para as licenças entregues;

3.7.1.3. A qualidade do serviço tiver sido avaliada e aceita pela CONTRATANTE.

3.7.2. O pagamento deverá ser efetuado mediante a apresentação de Nota Fiscal ou Fatura pela CONTRATADA, que deverá conter as informações necessárias à conferência do objeto fornecido, incluindo o prazo de validade, a data da emissão, os dados do contrato e do órgão contratante, o período de prestação dos serviços, o valor a pagar e eventual destaque do valor de retenções tributárias cabíveis.

3.7.3. O objeto será recebido provisoriamente, pelo responsável pelo seu acompanhamento e fiscalização para efeito de posterior verificação de sua conformidade com as especificações constantes no Termo de Referência, no prazo de até 05 (cinco) dias úteis.

3.7.4. Em até 15 (quinze) dias corridos após a emissão do Termo de Recebimento Provisório, salvo a inexistência de pendências a serem saneadas, sendo confirmada sua operação e desempenho a contento, nos termos do Termo de Referência, a CONTRATANTE emitirá o Termo de Recebimento Definitivo;

3.7.5. Antes do pagamento, a CONTRATANTE verificará a regularidade fiscal da CONTRATADA através de consulta “on-line” ao Sistema de Cadastramento Unificado de Fornecedores - SICAF, ou na impossibilidade de acesso ao referido sistema, mediante consulta aos sítios oficiais.

3.7.6. À CONTRATANTE fica reservado o direito de retenção ou glosa no pagamento, sem prejuízo das sanções cabíveis quando a CONTRATADA:

3.7.6.1. Não produzir os resultados, deixar de executar, ou não executar com a qualidade mínima exigida as atividades contratadas; ou

3.7.6.2. Deixar de utilizar materiais e recursos humanos exigidos para a execução do serviço, ou utilizá-los com qualidade inferior à demandada.

3.8. **REQUISITOS DE ACEITAÇÃO DO OBJETO**

3.8.1. A aceitação do objeto ocorrerá apenas se a empresa vencedora apresentar todos os critérios de habilitação;

3.8.2. A descrição do objeto na Nota Fiscal deverá ser idêntica à descrição do edital e da Nota de Empenho, caso contrário o serviço executado deverá ser recusado para correção da documentação por parte da contratada.

3.9. **DA INSTALAÇÃO E CONFIGURAÇÃO**

3.9.1. A CONTRATADA deverá instalar a solução ofertada nas instalações da CONTRATANTE;

3.9.2. A empresa que realizar a implantação deverá ter técnicos treinados em toda a solução ofertada;

3.9.3. Os serviços que eventualmente acarretem risco para os sistemas em produção ou requeiram parada de servidores, equipamentos e rede elétrica, somente poderão ser executados fora de expediente, em horários previamente acordados com a área de TI do local de instalação.

4. METAS DO PLANEJAMENTO ESTRATÉGICO A SEREM ALCANÇADAS

4.1. Evitar, mitigar e conter a propagação de pragas digitais facilitando o tratamento destes incidentes com a administração centralizada da solução de proteção;

4.2. Oferecer maior agilidade e eficácia no tratamento de incidentes devidos a Spam e lixo eletrônico;

4.3. Garantir segurança, disponibilidade e estabilidade;

4.4. Aumentar a proteção contra ataques originados no correio eletrônico;

4.5. Conformidade com a Lei Geral de Proteção de Dados Pessoais - LGPD (Lei nº 13.709/2018).

5. LEVANTAMENTO DAS ALTERNATIVAS

5.1. IDENTIFICAÇÃO E ANÁLISE DAS POSSÍVEIS SOLUÇÕES

ID	DESCRIÇÃO DA SOLUÇÃO (OU CENÁRIO)
1	Adoção de solução baseada em software open source
2	Aquisição de nova ferramenta de AntiSpam (software proprietário)

Tabela 8 - Descrição das soluções/cenários.

5.1.1. SOLUÇÃO 1 - ADOÇÃO DE SOFTWARE OPEN SOURCE

5.1.1.1. De acordo com opensource.com, o software open source é aquele que qualquer um pode inspecionar, modificar e melhorar. Além dessas características, segundo o opensource.org, os termos de distribuição do software open source devem seguir alguns critérios, como, por exemplo, redistribuição livre e distribuição do código junto com o software.

5.1.1.2. As tabelas abaixo apresentam o estudo de algumas soluções open source de antispam disponíveis:

Solução	**MailScanner**
Descrição	MailScanner é um sistema de segurança de e-mail open source desenvolvido para gateways de e-mail baseados em Linux. O programa analisa e-mails procurando por vírus, spams e outros malwares. De acordo com o manual da solução, o software controla uma variedade de aplicações open source para analisar e-mails e detectar spam e vírus, quais sejam: • ClamAV Antivírus; • BitDefender Antivírus; • SpamAssassin; • Pyzor; • Razor2; • DCC. A última versão do software é a 5.0.3-7, de 14 de agosto de 2016

Tabela 9 - Análise da solução open source MailScanner.

Solução	**RadicalSpam**
Descrição	De acordo com o site da solução, o pacote RadicalSpam é distribuído sob GPL v2, incluindo produtos como Postfix, SpamAssassin, Amavisd-new, ClamAV, Razor, DCC, Postgrey e Bind, provendo SMTP seguro e funcionalidades anti-spam, antivírus, MTA, DNS, Greylisting etc. Uma das inovações do software é forma como é desenvolvido, o que resulta em independência relativa ao sistema hospedeiro. O RadicalSpam permite que o administrador se livre de restrições de instalações que são frequentemente encontradas em soluções open source, especialmente o gerenciamento de dependências.

	RadicalSpam pode ser executado nas distribuições Linux mais comuns, como, por exemplo, Redhat, Suse, Gentoo, Debian. A sustentabilidade do sistema é assegurada pela comunidade de usuários, mas também pelas respectivas comunidades de cada produto incluído no pacote.

Tabela 10 - Análise da solução open source RadicalSpam.

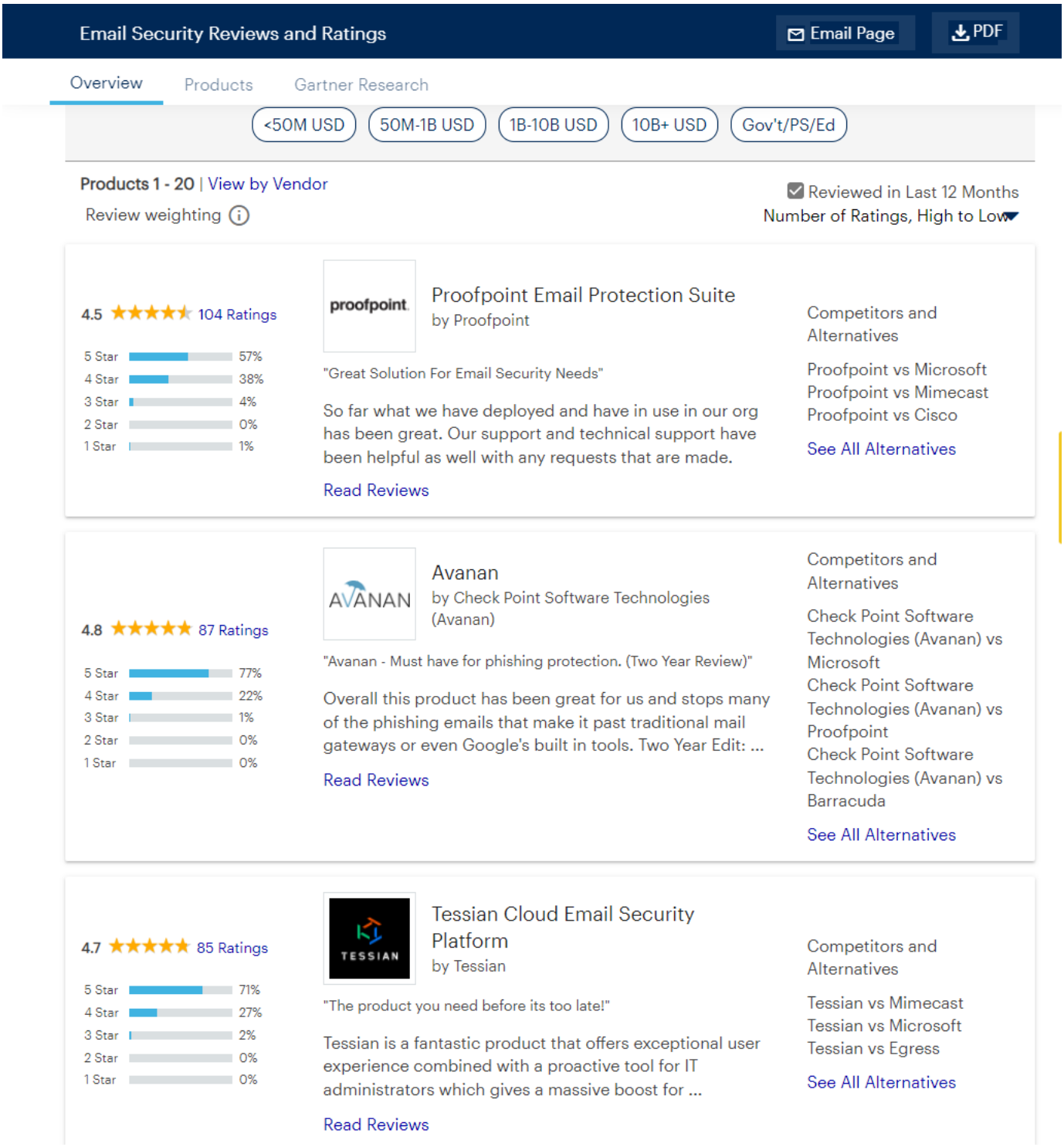
5.2. **SOLUÇÃO 2 - AQUISIÇÃO DE SOFTWARE DE GATEWAY DE SEGURANÇA DE E-MAILS**

5.2.1. Compreende a contratação de empresa especializada no fornecimento de licenças de software de solução de AntiSpam incluindo implantação da solução, treinamento, manutenção especializada e suporte técnico pelo período de 12 (doze) meses.

5.2.2. O software promove o aumento dos níveis de segurança no ambiente de e-mail institucional. Refere-se ao objetivo de identificar e bloquear, em tempo real, ataques, invasões ou abusos direcionados ao ambiente de e-mail, de forma a reduzir os riscos relacionados à imagem institucional, perda de informações e descumprimento de normas e regulamentos. Visa também atender a necessidade de possuir uma infraestrutura mais robusta, necessária para atender às demandas de envio e recebimento de mensagens institucionais, internas e externas, através da implementação de recursos de segurança da informação.

5.2.3. Softwares proprietários são programas licenciados, com direitos exclusivos para o produtor. O software, normalmente, é abrangido por patentes e direitos autorais. Os programas de anti-spams, em sua maioria, são softwares desenvolvidos por empresas especializadas em segurança e que fornecem suporte técnico.

5.2.4. Para fins de levantamento de soluções disponíveis no mercado, considerando a solução de id 02, utilizou-se como parâmetro a pesquisa efetuada pelo GARTNER (empresa com atuação no ramo de pesquisas, consultorias, eventos e prospecções acerca do mercado de TI), o mercado de soluções de segurança para prevenção contra vazamento de informações apresenta diversos fabricantes e soluções conforme pode ser visto em levantamento anual acerca de soluções de AntiSpam.



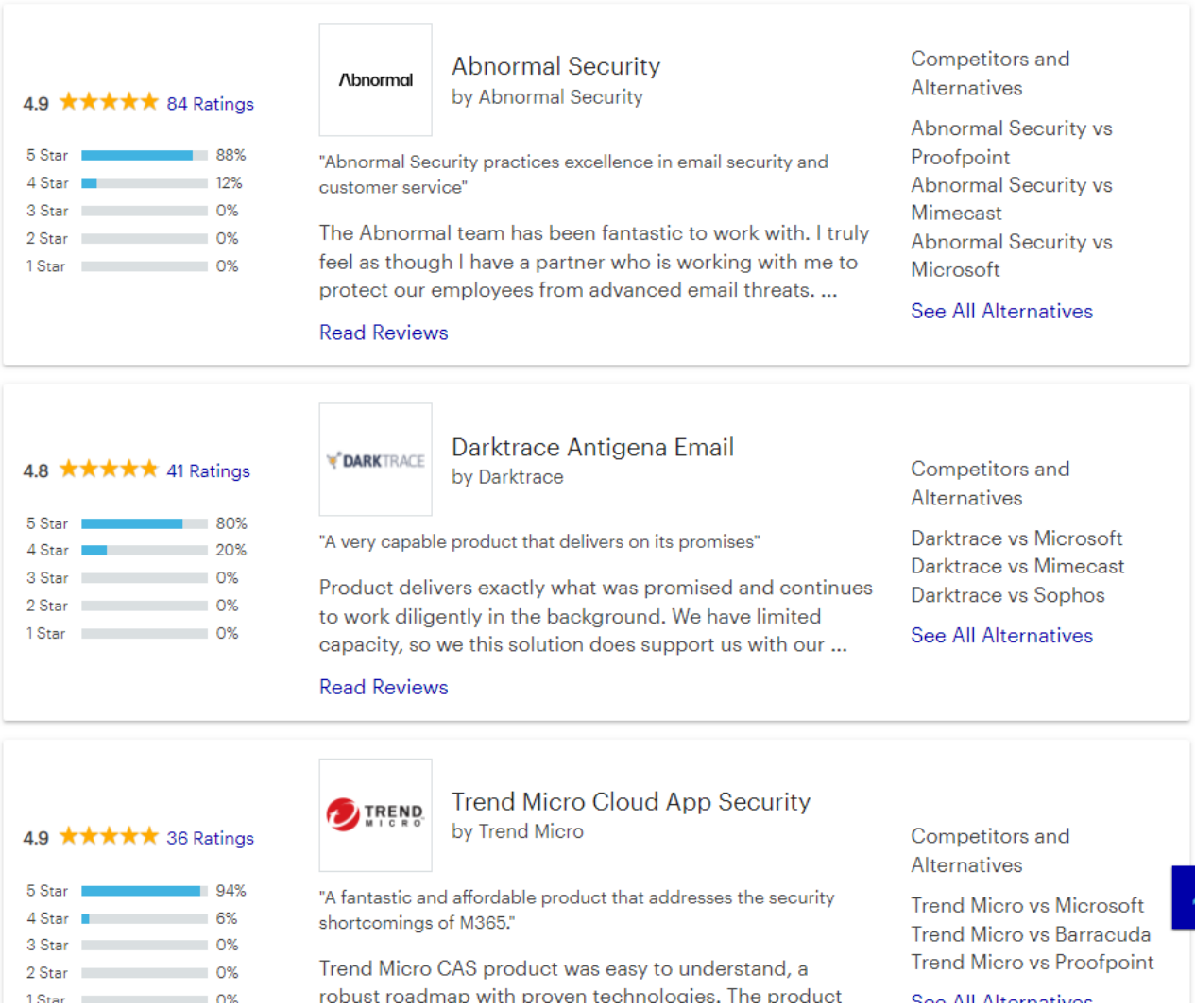


Imagem 1. Levantamento anual de solução AntiSpam pelo Gartner.

5.2.5. **Definição**: Conjunto de tecnologias e técnicas de inspeção usadas para bloquear a entrada de spams em um sistema, por exemplo, a caixa de email. Fazendo uso de diversos protocolos e parâmetros para identificar mensagens indesejadas e não solicitadas – como um arquivo, e-mail, pacote, em uso (durante uma operação) ou em trânsito (através de uma rede). As ferramentas AntiSpam também têm a capacidade de aplicar dinamicamente uma política — como registrar, relatar, classificar, e/ou aplicar proteções de gerenciamento.

5.2.6. O Gartner avalia soluções AntiSpam que fornecem visibilidade do uso de dados em uma organização para um amplo conjunto de casos de uso e a aplicação dinâmica de políticas com base no conteúdo e contexto no momento de uma operação, abordando ameaças relacionadas a dados, incluindo os riscos de perda de dados inadvertida ou acidental, e a exposição de dados confidenciais usando monitoramento, filtragem, bloqueio e outros recursos de correção.

5.2.7. O estudo abaixo relaciona as alternativas existentes no mercado que se enquadram nas necessidades/benefícios elencadas pela Instituição:

ESTUDO DE MERCADO	
Solução de AntiSpam	**TRENDMICRO** • Proteção em camadas defendendo contra ataques persistentes e direcionados de ransomware e outros tipos malware de zero day; • Monitoramento e filtragem de remetentes maliciosos com diversas abordagem; • Proteção contra comprometimento de e-mail corporativo (BEC); • Análise dinâmica de sandbox para arquivos e URL / detecção de exploits; • Análise de conteúdo do e-mail usando uma variedade de técnicas para filtrar spam e phishing.
	DARKTRACE • Descoberta de dados, descoberta eletrônica e classificação de dados – automática, em tempo real ; • Uso de inteligência artificial central para impedir as ameaças de e-mail mais avançadas, intervindo para proteger os funcionários de toda a gama de ameaças direcionadas à caixa de entrada; • Interrompe o spear phishing avançado e as falsificações digitais.
	BARRACUDA

	• Proteção contra malware, spam, phishing e ataques DoS bem como DDoS; • Filtragem com opções de quarentena, podendo aplicar regras para e-mail e anexos para garantir que cada e-mail enviado esteja em conformidade com as políticas corporativas de DLP; • Integração com um serviço de criptografia de e-mail baseado em nuvem para e-mail de saída.
	PROOFPOINT • Segurança de e-mail detectam e-mails com URLs ou anexos maliciosos; • Bloqueio de ransomware e malware polimórfico; • Reescreve URLs protege seus usuários em qualquer rede e dispositivo e detecta se uma mensagem foi armada após a entrega; • Identificação de funcionários de alto risco, identificando atividades que indicam furto de dados; • Remove e-mails de phishing contendo URLs envenenados após a entrega de e-mails indesejados de contas internas comprometidas; • Defesa BEC avançada e também oferece visibilidade granular dos detalhes das ameaças BEC.

Tabela 11 – Estudo de Mercado.

5.2.8. Destaque-se que foi realizada prova de conceito (POC) no ambiente da FUNASA em que foram habilitados os filtros de spam abaixo, e conforme Nota Técnica - Prova de Conceito (POC) Antispam (SEI nº 4113475), foi realizado um comparativo entre as ferramentas relacionadas a seguir:

5.2.9. **InterScan Messaing Security Virtual Appliance - Trend Micro;**

5.2.10. **Fortimail da Fortigate; e**

5.2.10.1. **ProofPoint.**

5.2.11. As ferramentas acima possuem funções de detecção e bloqueio de spam, de anti-malware, de antivírus, proteção contra perda de dados, detecção de ameaças, Sandboxing, portal de gerenciamento centralizado entre outras. As referidas ferramentas também possibilitam criar regras customizadas, restauração de mensagens em quarentena e executam atualizações diárias de definições associadas a antispam e antivírus em suas respectivas bases de conhecimento.

5.2.12. O anexo (SEI nº 4113475) apresenta um comparativo no qual, após análise da performance das ferramentas, concluiu-se que em relação ao uso das mesmas, o InterScan Messaing Security Virtual Appliance, Fortimail e Proofpoint tiveram performances semelhantes, porém, na análise dentro do ambiente da Funasa, a ferramenta Proofpoint, apresentou um melhor resultado nas funções de heurística e na detecção de spam, phishing e malware.

5.2.13. A ferramenta Proofpoint detectou os sinais do ataque de phishing e Assunto - Qintess/Funasa: Contrato 070/2020 – Infraestrutura malware nos logs das mensagens que já haviam sido analisadas pelas ferramentas da Fortimail e do InterScan Messaing Security Virtual Appliance e que não foram detectados por ambas, promovendo, desta forma, um melhor bloqueio desse tipo de mensagem em comparação com o filtro de spam da Fortimal e do InterScan Messaing Security Virtual Appliance, conforme demonstrado no anexo (SEI nº 4113475).

5.2.14. De modo geral, a ferramenta da Prooftpoint apresentou o melhor desempenho, promovendo também uma redução de chamados referentes à problemas de envio e recebimento de mensagens e, consequentemente, das tratativas necessárias para bloqueio ou liberação de falsos positivos que passavam ou ficavam retidos na quarentena das ferramentas da Fortimail e do InterScan Messaing Security Virtual Appliance.

5.3. **Da existência de software público brasileiro**

5.3.1. De acordo com a busca realizada no dia 30 de junho de 2022, às 10:30, com as palavras chaves "AntiSpam", o portal: softwarepublico.gov.br, retornou que não havia encontrado nenhum software correspondente.

Imagem 2. Pesquisa de solução AntiSpam no portal de software público.

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

ÓRGÃO	Nº PREGÃO	SOLUÇÃO
MINISTÉRIO DA INFRAESTRUTURA	21/2021	Objeto: Pregão Eletrônico - O objeto da presente licitação é a contratação de empresa especializada para prestação de Serviço de Solução de Filtragem de Conteúdo de E-mail na Nuvem (**Antispam** Corporativo), para proteção de caixas postais, contemplando serviços de instalação, manutenção, atualização e suporte técnico especializado da plataforma ofertada, nos termos, condições, quantidades e exigências estabelecidas neste Edital e seus anexos.
DEPARTAMENTO NACIONAL DE INFRAESTRUTURA DE TRANSPORTES	505/2021	Registro de Preço de Registro de preço para eventual aquisição de Solução de **Antispam** incluindo o licenciamento, instalação, configuração, garantia e transferência de conhecimento para a operação da ferramenta com console de gerenciamento centralizado., em conformidade com as condições e especificações estabelecidas neste Termo de Referência

Tabela 12 - Análise de Projetos Similares.

5.4.1. As soluções adquiridas em contratações recentes da Administração Pública utilizados como referência, possuem configurações aproximadas ou similares a aquisição pretendida pela Funasa. Portanto a contratação pode ser caracterizada como bem comum, pois as padronizações de suas configurações são comumente encontradas no mercado e em contrações da Administração Pública.

5.4.2. A tabela a seguir apresenta a análise quanto as políticas, os modelos e os padrões de governo, a exemplo do ePing, eMag, ePwg, ICP-Brasil e e-ARQ Brasil, quando aplicáveis:

Requisito	Entidade	Sim	Não	Não se Aplica
A Solução encontra-se implantada em outro órgão ou entidade da Administração Pública?	1, 2	X		
A Solução está disponível no Portal do Software Público Brasileiro?	1, 2		X	
A capacidade e alternativas do mercado, inclusive existência de software livre ou software público?	1, 2		X	
A Solução é aderente às políticas, premissas e especificações técnicas definidas pelos Padrões e-PING, e-MAG?	1, 2	X		
A Solução é aderente às regulamentações da ICP-Brasil? (Quando houver necessidade de certificação digital)	1, 2			X
A Solução é aderente às orientações, premissas e especificações técnicas e funcionais do – e-ARQ Brasil?	1, 2	X		
A Solução é aderente às necessidades técnicas do órgão?	1, 2	X		
A análise de projetos similares foi utilizada para realização do orçamento estimado?	1, 2	2	1	

Tabela 13 - Análise das Alternativas Existentes.

6. REGISTRO DE SOLUÇÕES CONSIDERADAS INVIÁVEIS

6.1. A **Solução de Id. 01** compreende o uso de solução baseada em software livre. Devido à falta de suporte técnico especializado, possuir código fonte, ausência de garantias e necessidade de composição com vários produtos para entrega aproximada da necessidade, fica evidente que esta solução não atenderia as necessidades da Funasa.

7. DESCRIÇÃO DA SOLUÇÃO ESCOLHIDA

7.1. Justificativa da Solução Escolhida

7.1.1. Entre as opções de soluções open source e proprietárias, **optou-se pelo software proprietário** (Solução de Id 02) pelos seguintes motivos:

- Os softwares proprietários analisados possuem uma série de funcionalidades que atenderão as necessidades de segurança da informação da FUNASA;
- As soluções estudadas reduzem o tempo de resposta a incidentes de segurança da informação;
- As soluções possuem suporte especializado em segurança da informação.

7.1.2. A solução a ser contratada é a de **Id 02** que compreende a contratação de empresa especializada no fornecimento de licenças de software de solução de AntiSpam incluindo implantação da solução, treinamento, manutenção especializada e suporte técnico pelo período de 12 (doze) meses.

7.1.3. Através da referida contratação será possível atender as necessidades da Funasa, com ganho em qualidade e eficiência, além de prover o atendimento aos requisitos de segurança da informação, garantindo a disponibilidade e continuidade dos serviços de TI, bem como para atender às constantes evoluções dos recursos de TIC, desse modo, a contratação da solução escolhida irá fornecer o suporte adequado às necessidades do negócio desta FUNASA, que necessita de soluções de segurança que sejam proativas e inteligentes, buscando preservar um dos maiores ativos existentes atualmente nas organizações que é a informação.

7.1.4. A contratação da solução escolhida se faz necessária em razão da necessidade de aquisição de solução robusta, eficaz e confiável de filtragem de conteúdo a fim de proteger a rede de computadores de ataques e conteúdos maliciosos e garantir a segurança, integridade e confidencialidade dos dados, devido ao grande volume de mensagens que transitam nos diversos endereços de e-mail da fundação, sendo um alto percentual destas Spam e lixo eletrônico.

7.1.5. Assim, a contratação da solução de AntiSpam também é necessária para que a fundação possa cumprir a sua missão, atendendo com qualidade e segurança às expectativas dos usuários dos seus serviços, uma vez que a sua infraestrutura de segurança de tecnologia da informação necessita de melhorias contínuas. Neste sentido, a aquisição de licenças de software de AntiSpam torna-se imprescindível, visando manter esta infraestrutura adequada aos novos desafios que se apresentam, com o fito de evitar que a segurança dos dados da FUNASA, seja comprometida, garantindo a disponibilidade, integridade e autenticidade dos e-mails nas redes e sistemas computacionais da Funasa.

7.2. **Solução escolhida**

7.3. Considerando as soluções analisadas neste processo, as justificativas apresentadas no item anterior e os valores apresentados, optou-se por manter a licitação abordada com ampla concorrência de mercado e menor preço global, auferindo a proposta com o valor mais vantajoso para a administração, desde que atendam aos requisitos mínimos tecnológicos elencados no Termo de Referência.

8. ESTIMATIVA DE VOLUME DA DEMANDA

8.1. **Item 1 - Aquisição de Licenças AntiSpam**

8.1.1. A demanda de volume de licenciamento da solução para o item 1 foi definida com base na média atual de caixas de e-mail ativas na Fundação, conforme Relação de Usuários Ativos com Contas de E-mail, extraída do Active Directory - AD (SEI nº 4113519).

8.1.2. De acordo com o levantamento acima mencionado, atualmente há 4649 (quatro mil seiscentos e quarenta e nove) caixas postais ativas, no entanto, este quantitativo pode sofrer oscilações, de acordo com a entrada/saída de funcionários e colaboradores usuários da rede Funasa. Desta forma foi definido o quantitativo médio de 4500 (quatro mil e quinhentos) contas de e-mail.

8.2. **Item 2 - Serviço de Instalação e Configurações da Solução de gateway e segurança de e-mails**

8.2.1. O quantitativo do item 2 foi estimado em 1 (um), considerando que o objeto da contratação pleiteada é constituído de uma solução única, que deverá ser entregue e instalada em conjunto.

8.3. **Item 3 - Treinamento**

8.3.1. O quantitativo do item 3 foi estimado em 03 (três) pessoas, com base no número de Técnicos da Funasa atualmente lotados na Coordenação Geral de Modernização e Tecnologia da Informação - CGMTI que possuem conhecimento das normas de Segurança da Informação da Fundação.

9. ANÁLISE COMPARATIVA DE CUSTOS (TCO)

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

9.1.1. Para construção do TCO de cada um dos itens foi levado em consideração os seguintes itens:

ITEM	DESCRIÇÃO	MÉTRICA	QUANTIDADE
1	Solução de software de gateway de segurança de e-mails (AntiSpam), com fornecimento de serviços especializados por 12 meses	Caixas Postais	4500
2	Serviço de Instalação e Configurações da Solução de gateway e segurança de e-mails.	Unidade	1
3	Treinamento	Pessoa	3

Tabela 14 - Itens considerados para construção do TCO.

9.2. **TCO PARA O ITEM 1**

9.2.1. Para realização deste TCO, realizou-se pesquisa de preço seguindo as orientações contidas na INSTRUÇÃO NORMATIVA SEGES /ME Nº 65, DE 7 DE JULHO DE 2021, que dispõe sobre o procedimento administrativo para a realização de pesquisa de preços para aquisição de bens e contratação de serviços em geral, no âmbito da administração pública federal direta, autárquica e fundacional.

9.2.2. Conforme demonstra a tabela abaixo, para o item 1, a pesquisa traz em sua cesta de preços 8 (oito) valores, sendo 1 (um) no parâmetro I e 7 (sete) no parâmetro IV.

Item	Descrição	Parâmetro	Fonte de consulta	Valor Unitário	Média	Desvio Padrão	Limite Superior (Média + Desvio)	Limite Inferior (Média -Desvio)	Análise de Exequibilidade dos Preços
1	Solução de software de gateway de segurança de e-mails (AntiSpam), com fornecimento de serviços especializados por 12 meses	I	PE 505/2021 - DNIT	R$ 80,13	R$ 378,87	197,39	576,26	181,48	INEXEQUÍVEL
		IV	Fornecedor 1	R$ 620,00					EXC.ELEVADO
		IV	Fornecedor 2	R$ 580,80					EXC.ELEVADO
		IV	Fornecedor 3	R$ 655,05					EXC.ELEVADO
		IV	Fornecedor 4	R$ 235,00					ACEITÁVEL
		IV	Fornecedor 5	R$ 300,00					ACEITÁVEL
		IV	Fornecedor 6	R$ 260,00					ACEITÁVEL
		IV	Fornecedor 7	R$ 300,00					ACEITÁVEL

Tabela 15 - Preços coletados para o item 1.

9.2.3. Após a apuração dos preços excessivamente elevados ou excessivamente baixos, a coleta de dados resultou em uma cesta composta por 4 (quatro) valores considerados aceitáveis., na forma como segue.

Item	Descrição	Parâmetro	Fonte de consulta	Valor Unitário	Média	Mediana	Menor Preço	Desv.Padrão	Coef de Variação
1	Solução de software de gateway de segurança de e-mails (AntiSpam), com fornecimento de serviços especializados por 12 meses	IV	Fornecedor 4	R$ 235,00	R$ 273,75	R$ 280,00	R$ 235,00	27,70	10%
		IV	Fornecedor 5	R$ 300,00					
		IV	Fornecedor 6	R$ 260,00					
		IV	Fornecedor 7	R$ 300,00					

Tabela 16 - Preços aceitáveis para o item 1.

9.3. **TCO PARA O ITEM 2**

9.3.1. Para realização deste TCO, realizou-se pesquisa de preço seguindo as orientações contidas na INSTRUÇÃO NORMATIVA SEGES /ME Nº 65, DE 7 DE JULHO DE 2021, que dispõe sobre o procedimento administrativo para a realização de pesquisa de preços para aquisição de bens e contratação de serviços em geral, no âmbito da administração pública federal direta, autárquica e fundacional.

9.3.2. Conforme demonstra a tabela abaixo, para o item 2 a pesquisa traz em sua cesta de preços 7 (sete) valores no parâmetro IV.

Item	Descrição	Parâmetro	Fonte de consulta	Valor Unitário	Média	Desvio Padrão	Limite Superior (Média + Desvio)	Limite Inferior (Média -Desvio)	Análise de Exequibilidade dos Preços
2	Serviço de Instalação e Configurações da Solução de gateway e segurança de e-mails	IV	Fornecedor 1	R$ 80.000,00	R$ 61.288,23	9.476,25	70.764,48	51.811,98	EXC.ELEVADO
		IV	Fornecedor 2	R$ 62.617,60					ACEITÁVEL
		IV	Fornecedor 3	R$ 64.400,00					ACEITÁVEL
		IV	Fornecedor 4	R$ 50.000,00					INEXEQUÍVEL
		IV	Fornecedor 5	R$ 52.000,00					ACEITÁVEL
		IV	Fornecedor 6	R$ 55.000,00					ACEITÁVEL
		IV	Fornecedor 7	R$ 65.000,00					ACEITÁVEL

Tabela 17 - Preços coletados para o item 2.

9.3.3. Após a apuração dos preços excessivamente elevados ou excessivamente baixos, a coleta de dados resultou em uma cesta composta por 5 (cinco) valores considerados aceitáveis, na forma como segue.

Item	Descrição	Parâmetro	Fonte de consulta	Valor Unitário	Média	Mediana	Menor Preço	Desv.Padrão	Coef de Variação
2	Serviço de Instalação e Configurações da Solução de gateway e segurança de e-mails	IV	Fornecedor 2	R$ 62.617,60	R$ 59.803,52	R$ 62.617,60	R$ 52.000,00	5.291,86	9%
		IV	Fornecedor 3	R$ 64.400,00					
		IV	Fornecedor 5	R$ 52.000,00					
		IV	Fornecedor 6	R$ 55.000,00					
		IV	Fornecedor 7	R$ 65.000,00					

Tabela 18 - Preços aceitáveis para o item 2.

9.4. **TCO PARA O ITEM 3**

9.4.1. Para realização deste TCO, realizou-se pesquisa de preço seguindo as orientações contidas na INSTRUÇÃO NORMATIVA SEGES /ME Nº 65, DE 7 DE JULHO DE 2021, que dispõe sobre o procedimento administrativo para a realização de pesquisa de preços para aquisição de bens e contratação de serviços em geral, no âmbito da administração pública federal direta, autárquica e fundacional.

9.4.2. Conforme demonstra a tabela abaixo, para o item 3 a pesquisa traz em sua cesta de preços 7 (sete) valores no parâmetro IV.

Item	Descrição	Parâmetro	Fonte de consulta	Valor Unitário	Média	Desvio Padrão	Limite Superior (Média + Desvio)	Limite Inferior (Média -Desvio)	Análise de Exequibilidade dos Preços
3	Treinamento	IV	Fornecedor 1	R$ 12.500,00	R$ 17.038,14	4.412,62	21.450,77	12.625,52	INEXEQUÍVEL
		IV	Fornecedor 2	R$ 16.942,00					ACEITÁVEL
		IV	Fornecedor 3	R$ 15.325,00					ACEITÁVEL
		IV	Fornecedor 4	R$ 15.000,00					ACEITÁVEL
		IV	Fornecedor 5	R$ 22.000,00					EXC.ELEVADO
		IV	Fornecedor 6	R$ 12.500,00					INEXEQUÍVEL
		IV	Fornecedor 7	R$ 25.000,00					EXC.ELEVADO

Tabela 19 - Preços coletados para o item 3.

9.4.3. Após a apuração dos preços excessivamente elevados ou excessivamente baixos, a coleta de dados resultou em uma cesta composta por 3 (três) valores considerados aceitáveis, na forma como segue.

Item	Descrição	Parâmetro	Fonte de consulta	Valor Unitário	Média	Mediana	Menor Preço	Desv.Padrão	Coef de Variação
3	Treinamento	IV	Fornecedor 2	R$ 16.942,00	R$ 15.755,67	R$ 15.325,00	R$ 15.000,00	849,29	5%
		IV	Fornecedor 3	R$ 15.325,00					
		IV	Fornecedor 4	R$ 15.000,00					

Tabela 20 - Preços aceitáveis para o item 3.

10. ESTIMATIVA DE CUSTO TOTAL DA CONTRATAÇÃO

10.1. Com base em pesquisa elaborada de acordo com a INSTRUÇÃO NORMATIVA SEGES /ME Nº 65, DE 7 DE JULHO DE 2021, que dispõe sobre o procedimento administrativo para a realização de pesquisa de preços para aquisição de bens e contratação de serviços em geral, no âmbito da administração pública federal direta, autárquica e fundacional, considerando a configuração de uma solução de AntiSpam que atenda às necessidades da Funasa por 12 (doze) meses, o custo total da contratação foi estimado em **R$ 1.338.945,53** (um milhão, trezentos e trinta e oito mil novecentos e quarenta e cinco reais e cinquenta e três centavos).

ITEM	DESCRIÇÃO	QUANTIDADE	VALOR UNITÁRIO	VALOR TOTAL
1	Solução de software de gateway de segurança de e-mails (AntiSpam), com fornecimento de serviços especializados por 12 meses	4500	R$ 273,75	R$ 1.231.875,00
2	Serviço de Instalação e Configurações da Solução de gateway e segurança de e-mails	1	R$ 59.803,52	R$ 59.803,52
3	Treinamento	3	R$ 15.755,67	R$ 47.267,01
Custo Estimado Total				**R$ 1.338.945,53**

Tabela 21 - Custo Estimado Total da Contratação.

10.2. O detalhamento da pesquisa de preços encontra-se na Nota Técnica (SEI 4112829) e Planilha de Estimativa de Custos (SEI nº 4111986).

11. DECLARAÇÃO DE VIABILIDADE DA CONTRATAÇÃO

11.1. O presente Estudo Técnico Preliminar foi elaborado em harmonia com a Instrução Normativa nº 01/2019 da Secretaria de Governo Digital do Ministério da Economia – SGD/ME, além das orientações do Tribunal de Contas da União previstas nos acórdãos TCU 2207/2018 e 2037/2019, e Relatório de Monitoramento TC 037.11/2018-3 bem como em conformidade com os requisitos técnicos necessários ao cumprimento das necessidades e objeto da aquisição.

11.2. No mais, atende adequadamente às demandas de negócio formuladas, os benefícios pretendidos são adequados, os custos previstos são compatíveis e caracterizam a economicidade, os riscos envolvidos são administráveis e a área requisitante priorizará o fornecimento de todos os elementos aqui relacionados necessários à consecução dos benefícios pretendidos, pelo que recomendamos a aquisição proposta.

12. BENEFÍCIOS ESPERADOS

12.1. Com a presente contratação são esperados os seguintes benefícios:

12.1.1. Proteção das informações sensíveis ao negócio da FUNASA;

12.1.2. Redução da probabilidade de ocorrência de incidentes de segurança;

12.1.3. Controlar, monitorar e filtrar as páginas web visitadas;

12.1.4. Aumentar a proteção da rede interna da FUNASA contra incidentes de segurança originados nas estações de trabalho.

12.1.5. Aumentar a proteção contra ataques originados no correio eletrônico.

13. NECESSIDADES DE ADEQUAÇÃO DO AMBIENTE PARA EXECUÇÃO CONTRATUAL

Não se aplica

14. RECURSOS NECESSÁRIOS À CONTINUIDADE DO NEGÓCIO DURANTE E APÓS A EXECUÇÃO DO CONTRATO

14.1. Recursos Materiais

14.1.1. Os equipamentos e materiais utilizados, bem como a prestação dos serviços deverão estar rigorosamente dentro das normas vigentes e das especificações estabelecidas pela FUNASA, sendo que a inobservância desta condição implicará a sua recusa, bem como a sua devida adequação/substituição, sem que caiba à CONTRATADA qualquer tipo de reclamação ou indenização.

14.2. Recursos Humanos

14.2.1. O modelo de prestação de serviços prevê que a CONTRATADA seja integralmente responsável pela gestão de seu pessoal em todos os aspectos, sendo vedado à equipe da FUNASA, formal ou informalmente, qualquer tipo de ingerência ou influência sobre a administração da mesma, ou comando direto sobre seus empregados, fixando toda negociação na pessoa do preposto da CONTRATADA ou seu substituto.

14.2.2. Neste sentido, se torna indispensável a transferência de conhecimento à equipe técnica da FUNASA de todos os novos procedimentos e/ou serviços implantados ou modificados pela CONTRATADA, mediante documentação técnica em repositório adotado pela Fundação para esse fim, dando plena capacidade ao mesmo de acompanhar, executar e gerenciar os serviços contratados em caso de descontinuidade do contrato.

15. ESTRATÉGIA DE CONTINUIDADE CONTRATUAL

15.1. Requisitos de Continuidade Contratual

15.1.1. **Haver falhas na legislação aplicada ou nas especificações/qualidade da solução:**

15.1.1.1. **Ações de Contingência e seus respectivos responsáveis:** Ter certeza que a equipe de planejamento tenha capacidade e conhecimento do assunto técnico, bem como da parte administrativa e jurídica, estando tudo isso transcrito nos documentos – Equipe de Planejamento.

15.1.2. **Questões Relacionadas a Defeitos e Reparações**

15.1.2.1. **Ações de Contingência e seus respectivos responsáveis:** Caso a empresa CONTRATADA não providencie a troca ou reparação de algum produto com defeito, haverá a aplicação de advertência, multa, notificação, sanções, abatimento das custas do depósito em garantia. O custo do retrabalho dos serviços ocorrerá a expensas da empresa, o que poderá ser cobrado judicialmente– Comissão executora.

15.1.3. **Serviço de Manutenção Fora do Prazo**

15.1.3.1. **Ações de Contingência e seus respectivos responsáveis:** Caso a empresa CONTRATADA não providencie a instalação e/ou a manutenção em um prazo hábil estipulado, causando prejuízo ao Erário, haverá aplicação de advertência, multa, notificação, sanções, abatimento das custas do depósito em garantia – Comissão executora.

15.1.4. **Garantia de Qualificação Econômico-Financeira**

15.1.4.1. **Ações de Contingência e seus respectivos responsáveis:** A empresa CONTRATADA deverá apresentar qualificação econômico-financeira que minimize ocorrência do risco de insubsistência da empresa – Setor de compras.

15.2. **Continuidade do fornecimento da solução de tecnologia da informação em eventual interrupção contratual**

15.2.1. A futura transição contratual decorrente de nova contratação para o mesmo objeto e a eventual interrupção do contrato por qualquer motivo são riscos inerentes a pretendida contratação, para os quais concorrem como ações planejadas para favorecer a continuidade dos serviços, reduzir os impactos e prover maior segurança institucional;

15.2.2. A empresa CONTRATADA deverá apresentar, sempre que solicitado pela FUNASA, qualificação econômico-financeira que minimize o risco de insubsistência da mesma;

15.2.3. Também com o intuito de minimizar os impactos no caso de insubsistência/falência da CONTRATADA, todo material ou produto da FUNASA mantido, produzido ou atualizado pela CONTRATADA deverá estar sob total controle da Fundação;

15.2.4. É admissível a fusão, cisão ou incorporação da CONTRATADA com/em outra pessoa jurídica, desde que sejam observados pela nova pessoa jurídica todos os requisitos de habilitação exigidos na licitação original; sejam mantidas as demais cláusulas e condições do contrato; não haja prejuízo à execução do objeto pactuado e haja a anuência expressa da Administração à continuidade do contrato;

15.2.5. A empresa CONTRATADA repassará à FUNASA, todo o conhecimento técnico e capacitação necessária para a manutenção e suporte técnico, visando manter a solução em funcionamento em caso de interrupção por transição contratual ou outro motivo, o termo de Direito de Propriedade Intelectual da FUNASA no que concerne à parte de customização desenvolvida com base nas definições de requisitos próprios da Fundação;

15.2.6. A CONTRATADA devolverá os recursos disponibilizados, terá os perfis que lhe foram atribuídos revogados, bem como a eliminação das caixas postais de correio eletrônico caso seja necessário.

15.3. **Atividades de transição contratual e encerramento do contrato**

15.3.1. A empresa CONTRATADA deverá apresentar periodicamente, qualificação econômico-financeira que minimize ocorrência do risco de insubsistência da empresa;

15.3.2. Em caso de venda da empresa CONTRATADA ou incorporação por novos controladores, a empresa CONTRATADA deverá assegurar a CONTRATANTE, mediante cláusula contratual, transferência de todas as obrigações contratuais ao sucessor;

15.3.3. No caso de interrupção contratual a empresa deverá devolver todos os equipamentos encontrados em sua posse. A CONTRATANTE poderá rescindir o contrato por razões supervenientes, assegurados os direitos da CONTRATADA. Nesse caso, a CONTRATANTE comunicará à CONTRATADA com antecedência de 90 (noventa) dias do término do contrato para que ela elabore o Plano de Transição e realize a passagem do contrato. Neste caso, a CONTRATADA deverá devolver os equipamentos encontrados em sua posse reparados e os serviços abertos do momento da comunicação de rescisão do contrato e não finalizadas devem ser finalizadas antes do término do contrato. Especialmente no encerramento do contrato, a Área Administrativa deverá assegurar-se da adequada liquidação de todas as obrigações contratuais.

15.3.4. A CONTRATADA deve devolver todos os recursos de propriedade da CONTRATANTE, tais como:

- Licenças de softwares;
- Manuais e documentos, classificados ou que devam permanecer com a CONTRATANTE.

15.4. **A estratégia de independência da CONTRATANTE com relação à CONTRATADA**

15.4.1. A estratégia de independência tem como garantia o Termo de Recebimento Provisório, o qual deverá ser assinado pelos respectivos fiscais técnico e requisitante, e o Termo de Recebimento Definitivo, o qual deverá ser assinado pelo fiscal requisitante e pelo Gestor, que irá subsidiar a emissão do Termo de Encerramento do Contrato

15.5. **Transferência de conhecimento**

15.5.1. A transferência de conhecimento deve ser ofertada à equipe técnica da FUNASA, precisamente à equipe técnica da Informática. A referida transferência compreende, necessariamente, demonstração prática de cada funcionalidade dos equipamentos/produtos adquiridos, informações técnicas, em plena compatibilidade com o ambiente computacional da FUNASA e em conformidade com a proposta técnica previamente apresentada no Plano Executivo.

15.6. **Direitos de propriedade intelectual (LEI Nº. 9.610/1998)**

15.6.1. Os direitos de propriedade intelectual do software e projetos não necessitam ser transferidos ao contratante por tratar-se de solução proprietária e produtos de uso exclusivo para esta solução;

15.6.2. Entretanto, a entrega deverá incluir a licença de uso de todo o software fornecido para operacionalização do equipamento durante todo o seu período de atividade, independentemente da expiração da garantia e do contrato.

16. **APROVAÇÃO E ASSINATURAS**

16.1. A Equipe de Planejamento da Contratação foi instituída pela Portaria nº 5274, de 14 de outubro de 2022 (SEI nº 4176480).

16.2. Conforme o §2º do Art. 11 da IN SGD/ME nº 1, de 2019, o Estudo Técnico Preliminar da Contratação será aprovado e assinado pelos Integrantes Técnico e Requisitante da Equipe de Planejamento da Contratação e pela autoridade máxima da Área de TIC.

Integrante Requisitante	Integrante Técnico
ANDRÉ WILSON PIMENTA SANTANA **Coordenador-Geral de Modernização e de Tecnologia da Informação** SIAPE: 1.347.001	GLEICY KELLEN DOS SANTOS FAUSTINO **Coordenadora de Sistema de Informação - COINF** SIAPE: 1.320.942

Tabela 22 - Equipe de Planejamento da Contratação.

16.3. **Aprovação da Autoridade Máxima da Área de TIC**

16.3.1. Conforme o §3º do Art. 11 da IN SGD/ME nº 1, de 2019, caso a autoridade máxima da Área de TIC venha a compor a Equipe de Planejamento da Contratação, a autoridade que assinará o Estudo Técnico Preliminar da Contratação será aquela superior à autoridade máxima da Área de TIC.

Autoridade Máxima da Área de TIC
ALAN OLIVEIRA LIMA **Diretor do Departamento de Administração** SIAPE 3.278.934

Tabela 23 - Autoridade Máxima da Área de TIC.

Documento assinado eletronicamente por **Andre Wilson Pimenta Santana**, **Integrante Requisitante**, em 17/10/2022, às 14:45, 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 **Gleicy Kellen dos Santos Faustino**, **Integrante Técnico**, em 18/10/2022, às 09:42, 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 **Alan Oliveira Lima**, **Diretor do Departamento de Administração**, em 19/10/2022, às 11:39, 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.funasa.gov.br/consulta, informando o código verificador **3885510** e o código CRC **49FC6919**.

Referência: Processo nº 25100.006254/2021-77 SEI nº 3885510