FUNDAÇÃO NACIONAL DE SAÚDE

# ESTUDO TÉCNICO PRELIMINAR DA CONTRATAÇÃO

Processo nº 25100.005982/2021-61

## 1. INTRODUÇÃO

1.1. Este 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 da solução identificada, fornecendo as informações necessárias para subsidiar o respectivo processo de contratação.

1.2. O presente documento visa oferecer subsídios à elaboração do Termo de Referência, estabelecer parâmetros para uma boa execução contratual e está alinhado com o disposto na Instrução Normativa nº 01, de 04 de abril de 2019, emitida pela Secretaria de Governo Digital do Ministério da Economia - SGD/ME.

## 2. DESCRIÇÃO DA NECESSIDADE

### 2.1. Descrição da Solução de Tecnologia da Informação

2.1.1. Contratação de empresa especializada no fornecimento de licenças de software de solução de prevenção contra vazamento de informações em meio digital (Data Loss Prevention - DLP) incluindo implantação da solução, treinamento, manutenção especializada e suporte técnico pelo período de 36 (trinta e seis) meses.

| ITEM | DESCRIÇÃO | MÉTRICA | QUANTIDADE |
|---|---|---|---|
| 1 | Aquisição de licenças de software de solução de prevenção contra vazamento de dados - Data Loss Prevention - DLP. | Unidade | 3190 |
| 2 | Treinamento | Pessoa | 3 |

Tabela 1 – Descrição da Solução.

### 2.2. Motivação/Justificativa

2.2.1. Ao longo dos últimos anos houve um considerável crescimento no número de ataques e riscos associados a dados sensíveis. Em um mundo cada vez mais digitalizado, a informação atualmente acabou se tornando um ativo extremamente valioso para as organizações, no mundo todo, os casos relacionados à violação de dados já atingiram grandes varejistas, instituições financeiras, provedores de aplicações e órgãos do governo.

2.2.2. Em 14 de agosto de 2018 foi sancionada a Lei nº 13.709. A Lei Geral de Proteção de Dados (LGPD) dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direitos público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade. Essa Lei cria uma regulamentação para o uso, proteção e transferência de dados pessoais no Brasil, nos âmbitos privado e público.

2.2.3. Segundo o artigo 46 da LGPD, os agentes de tratamento devem adotar medidas de segurança, técnicas e administrativas aptas a proteger os dados pessoais. Isso inclui protegê-los de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito.

2.2.4. Para atendimento e alinhamento aos normativos que regem a matéria, a Funasa adquiriu licenças de software da solução da plataforma de produtos Symantec, através do contrato nº 46/2018, cuja vigência expirou em 17/04/2020, tendo a área técnica-requisitante optado pela não renovação do contrato em referência à época, portanto, desde então a Funasa não dispõe desta solução de segurança.

2.2.5. A Coordenação Geral de Modernização e Tecnologia da Informação - CGMTI entende que a informação, em qualquer dos seus formatos, é o principal ativo das instituições, públicas ou privadas e, considerando o cenário globalizado, está cada vez mais exposta a riscos de segurança. A Segurança da Informação e Comunicações compreende um conjunto de ações que buscam proteger e preservar os ativos de informação, assegurando-lhes disponibilidade, integridade, confidencialidade e autenticidade.

2.2.6. A informação tornou-se um recurso de importância crescente para qualquer setor e atividade do Estado brasileiro. Informação e conhecimento são fatores determinantes para a gestão governamental, e os órgãos e entidades da Administração Pública Federal utilizam grande volume de informações para promover, de forma eficiente, a prestação de serviço público ao cidadão, bem como para a tomada de decisões estratégicas.

2.2.7. Em linhas gerais, o processo de prevenção à perda de dados é apoiado por uma ferramenta/aplicação, que adequadamente configurada, é capaz de atuar de maneira preventiva - ao monitorar as mensagens e arquivos transitados. Caso seja identificado algum conteúdo que não deve ser transitado, a ferramenta pode alertar o usuário que este conteúdo é sensível ou mesmo bloquear o trâmite, baseado em filtros de conteúdo que demandam uma configuração detalhada. A ferramenta DLP também tem o potencial de auxiliar no processo de investigação de incidentes de vazamento da informação.

2.2.8. As configurações e políticas devem contemplar a capacidade da FUNASA de prevenir, detectar e reduzir a vulnerabilidade a incidentes relacionados ao ambiente cibernético, demandando reavaliação de procedimentos e controles internos à luz dos objetivos definidos. Considerando os avanços da tecnologia digital, a natureza das operações e a complexidade dos produtos, serviços, atividades e processos, o atendimento pleno desta exigência regulatória torna-se grande desafio. Os procedimentos e controles existentes, bem como aqueles a serem construídos, vão implicar em reavaliação de tecnologias, novos investimentos e, principalmente, necessidade de pessoal qualificado.

2.2.9. Destaque-se, ainda, o Decreto nº 10.222, de 5 de fevereiro de 2020, do Governo Federal, que aprova a Estratégia Nacional de Segurança Cibernética. Entre requisitos e controles definidos no documento, a seção 1.3, “Proteção Estratégica”, define uma proteção para infraestruturas críticas, no qual a FUNASA se insere, o que envolve institucionalizar processos, procedimentos e soluções de prevenção a vazamentos de informações pessoais ou institucionais.

2.2.10. O mesmo Decreto nº 10.222 cita o Decreto nº 9.637, de 26 de dezembro de 2018, que instituiu a Política Nacional de Segurança da Informação e dispõe sobre princípios, objetivos, instrumentos, atribuições e competências de segurança da informação para os órgãos e entidades da Administração Pública Federal, sob o prisma da governança. Nessa temática, destaca-se que o Decreto nº 9.637 pontua a relevância da segurança de informações sigilosas e a proteção contra vazamento de dados.

2.2.11. A pretensa contratação visa a proteção do ambiente da FUNASA, pois a ferramenta de DLP propiciará, dentre outros, proteção e autenticidade dos dados, maximizando a proteção contra ameaças da web. Ainda, a solução é parte de um conjunto essencial de funcionalidades necessárias para a gestão efetiva dos ativos de negócios desta Fundação.

2.2.12. Assim, a aquisição da solução de DLP é necessária para que a FUNASA 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 e ficar sem a solução é algo inimaginável. Neste sentido, medidas precisam ser tomadas visando manter esta infraestrutura adequada aos novos desafios que se apresentam.

## 3. DEFINIÇÃO E ESPECIFICAÇÃO DAS NECESSIDADES E REQUISITOS

3.1. **Identificação das necessidades de negócio**

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

- Proteção das informações sensíveis ao negócio da FUNASA;
- Aumentar a eficiência da segurança, proteção e autenticidade dos dados e acessos;
- Redução da probabilidade de ocorrência de incidentes de segurança;
- Controle da saída de dados sensíveis, seja via transferência de arquivos ou publicação em páginas da internet;
- Amplificação da camada de proteção e visibilidade de informações sensíveis;
- Fluxo automatizado de descoberta de informações sensíveis em todos os pontos do ambiente;
- Garantir a disponibilidade e continuidade dos serviços de TI;
- Prevenir a perda de dados por meio de adoção de uma estratégia de monitoramento e observância às diretivas constantes na Lei Geral de Proteção de Dados, LGPD, de 21 de Agosto de 2020, que dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural.

3.1.2. O projeto em questão está em conformidade e encontra-se alinhada 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 |
| | | A5.7 | Aquisição de nova ferramenta para prevenção contra perda de dados (DLP - Data Loss Prevention) |

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** |
| 308 | Soluções de TIC | SERVICO DE LICENCA PELO USO DE SOFTWARE |

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 36 (trinta e seis) 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. LEVANTAMENTO DAS ALTERNATIVAS

### 4.1. IDENTIFICAÇÃO DAS POSSÍVEIS SOLUÇÕES

| ID | DESCRIÇÃO DA SOLUÇÃO (OU CENÁRIO) |
|---|---|
| 1 | Adoção de solução baseada em software livre. |
| 2 | Aquisição de solução de prevenção contra vazamento de informações em meio digital (Data Loss Prevention - DLP), incluindo implantação da solução, treinamento, manutenção especializada e suporte técnico pelo período de 36 (trinta e seis) meses. |
| 3 | Renovação de solução Data Loss Prevention - DLP da plataforma de produtos Symantec existente na Funasa. |

Tabela 8 - Descrição das soluções/cenários.

### 4.2. ANÁLISE COMPARATIVA DAS SOLUÇÕES

#### 4.2.1. SOLUÇÃO 1

4.2.1.1. A primeira solução a ser avaliada consiste na adoção de software livre. Por “software livre” devemos entender aquele software que respeita a liberdade e senso de comunidade dos usuários, à grosso modo, isso significa que os usuários possuem a liberdade de executar, copiar, distribuir, estudar, mudar e melhorar o software.

4.2.1.2. Ao mesmo tempo que tal fato pode ser encarado de forma positiva, há que se levar em consideração que este cenário apresenta uma grande fragilidade de segurança, tendo em vista que as customização são feitas livremente sem levar em consideração aspectos importantes de padronização, escalabilidade e consistência.

4.2.1.3. Outro ponto muito importante na adoção de software livre é que estes não possuem suporte ou garantia, ficando os dados desta FUNDAÇÃO, a mercê de comunidades livres, sem SLA ou qualquer tipo de garantia.

4.2.1.4. Pelas razões supracitadas, a equipe de planejamento da contratação não encontrou elementos objetivos que justifiquem a utilização desse cenário/solução.

### 4.3. SOLUÇÃO 2

4.3.1. A solução 2 consiste na contratação de nova solução de mercado compreendendo a contratação de empresa especializada no fornecimento de licenças de software de solução de prevenção contra vazamento de informações em meio digital (Data Loss Prevention - DLP), incluindo implantação da solução, treinamento, manutenção especializada e suporte técnico pelo período de 36 (trinta e seis) meses.

4.4. Considerando o ambiente atual da Funasa, esta solução possibilitará o atendimento das necessidades atuais da fundação, 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.

4.5. Para subsidiar a análise deste cenário, levando em consideração não apenas os aspectos técnicos, mas também considerando o custo para a Administração, em pesquisa de preços realizada pela equipe de planejamento da contratação, o custo total de propriedade (TCO) deste cenário para atender às necessidades da Funasa por 36 meses foi estimado em **R$ 3.516.472,79 (três milhões, quinhentos e dezesseis mil quatrocentos e setenta e dois reais e setenta e nove centavos)**.

4.6. Se comparado com custo total estimado da solução de id 3, a solução 2 se apresenta como a mais vantajosa do ponto de vista financeiro. Portanto, considerando os aspectos técnicos e financeiros mencionados, a solução 2 se apresentou como um cenário completamente viável.

4.7. Portanto, a equipe de planejamento da contratação não encontrou justificativa técnica ou econômica para não seguir o recomendado neste cenário.

4.8. **SOLUÇÃO 3**

4.8.1. A solução 3 considera a renovação de solução DLP da plataforma de produtos Symantec existente na Funasa. Em 2016 a Funasa adquiriu solução DLP da plataforma de produtos Symantec através do contrato nº 27/2016, o qual teve a vigência finalizada em fevereiro de 2018.

4.8.2. Em 17/04/2018 foi realizada a contratação de empresa para renovação da solução de proteção DLP. Em 17/04/2019 o contrato foi renovado por mais 12 meses e teve sua vigência expirada em 17/04/2020. Na época a área técnica-requisitante optou pela não renovação do contrato, pois através da Nota Técnica (SEI 1968150) a equipe de gestão e fiscalização do contrato informou que o valor praticado pelo contrato 46/2018, quando comparado aos valores praticados em outros contratos vigentes para objeto semelhante, para o período de 12 meses, poderia ser considerado elevado e **não representava vantajosidade econômico financeira para a Administração.**

4.8.3. Na época a CGMTI sugeriu a renovação do contrato 46/2018, desde que fosse realizada a inclusão de cláusula rescisória a qualquer tempo, até que fosse possível a conclusão do processo licitatório em andamento (25100.000191/2020-64).

4.8.4. O processo mencionado refere à contratação de solução EDR, cujo contrato não contemplou ferramenta de DLP, pois através da Nota Técnica (SEI 2517984) a equipe planejamento decidiu pela exclusão do Lote 2 (Solução de Data Loss Prevention – DLP) do processo licitatório, deixando para momento posterior a contratação de solução mais robusta que possa implementar os requisitos previstos na Lei Geral de Proteção de Dados Pessoais – LGPD.

4.8.5. Para subsidiar a análise deste cenário, levando em consideração não apenas os aspectos técnicos mas também o custo da solução para a Administração, foi solicitado orçamento à fornecedores para o cenário 3 (renovação), no período de 18 de maio a 12 de julho de 2022, conforme pedido de cotação em anexo (SEI nº 3990025), onde, até a data deste documento, foram recebidas as propostas comerciais das empresas FAST HELP (SEI 3903999) e Fullpar (SEI 4024064), apresentando os valores abaixo:

| Item | Descrição | Qtd | Valor Proposta 1 | Valor Proposta 2 | Média |
|---|---|---|---|---|---|
| 1 | Licenças de Software de Solução de Prevenção de Vazamento de Dados – Data Loss Prevention - DLP. | 3190 | R$ 4.536.180,00 | R$ 2.902.900,00 | R$ 3.719.540,00 |
| 2 | Treinamento | 1 | R$ 44.428,00 | R$ 43.500,00 | R$ 43.964,00 |
| **Total** | | | | | **R$ 3.763.504,00** |

Tabela 9 - Estimativa de Custos para o Cenário 3.

4.8.6. Nesse sentido, foi elaborado o mapa comparativo dos custos para as soluções (Tabelas 10 e 11 deste ETPC), no qual observa-se que a **contratação de nova solução DLP é mais vantajosa financeiramente**, ou seja, no valor obtido com base na pesquisa de preços há uma diferença de **R$ 247.031,21** (duzentos e quarenta e sete mil trinta e um reais e vinte e um centavos) **a mais** para o cenário de renovação de Solução DLP.

4.8.7. Portanto, a equipe de planejamento da contratação não encontrou elementos objetivos que justifiquem a utilização/escolha desse cenário/solução.

4.9. **MAPA COMPARATIVO DOS CÁLCULOS TOTAIS DE PROPRIEDADE (TCO)**

| **Estimativa de TCO** | |
|---|---|
| **Descrição da solução** | **Custo Total da Solução (36 meses)** |
| **SOLUÇÃO 2**: Aquisição de solução de prevenção contra vazamento de informações em meio digital (Data Loss Prevention - DLP), incluindo implantação da solução, treinamento, manutenção especializada e suporte técnico pelo período de 36 (trinta e seis) meses. | **R$ 3.516.472,79** |
| **SOLUÇÃO 3**: Renovação de solução Data Loss Prevention - DLP da plataforma de produtos Symantec existente na Funasa. | **R$ 3.763.504,00** |

Tabela 10 - Estimativa de TCO.

| Estimativa de custo para a SOLUÇÃO 2 (A) | Estimativa de custo para a SOLUÇÃO 3 (B) | Diferença entre os custos Solução 1 e 2 (B) - (A) |
|---|---|---|
| R$ 3.516.472,79 | R$ 3.763.504,00 | **R$ 247.031,21** |

Tabela 11 - Mapa Comparativo TCO.

4.9.1. Observa-se no mapa comparativo acima que a solução mais econômica para a Administração é a solução de id 2 (Contratação de nova solução DLP) a qual apresentou uma diferença de **R$ 1.064.135,21** (um milhão, sessenta e quatro mil cento e trinta e cinco reais e vinte e um centavos) **a menor** em relação ao cenário de renovação de solução DLP existente (Solução 3).

4.10. **SOLUÇÕES DISPONÍVEIS NO MERCADO**

4.10.1. Consoante análise de mercado realizada 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 informaçõe**s** apresenta diversos fabricantes e soluções conforme pode ser visto em levantamento anual acerca de soluções DLP (Data Loss Prevention).

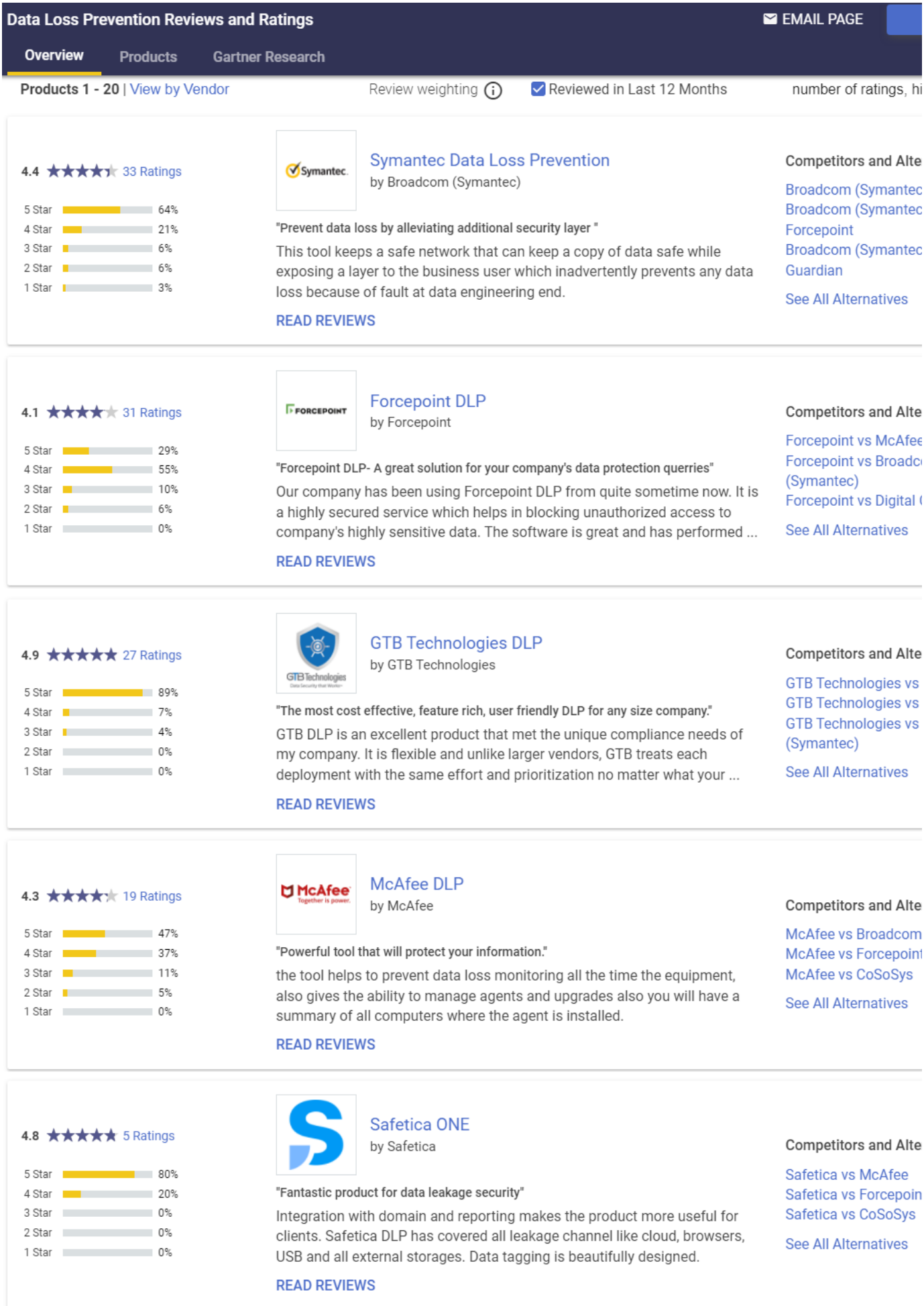


Imagem 1. Levantamento anual de solução DLP realizado pelo Gartner.

4.10.2. **Definição**: Conjunto de tecnologias e técnicas de inspeção usadas para classificar o conteúdo de informações contido em um objeto – como um arquivo, e-mail, pacote, aplicativo ou armazenamento de dados – enquanto em repouso (em armazenamento), em uso (durante uma operação) ou em trânsito (através de uma rede). As ferramentas DLP também têm a capacidade de aplicar dinamicamente uma política — como registrar, relatar, classificar, realocar, marcar e criptografar — e/ou aplicar proteções de gerenciamento de direitos de dados corporativos.

4.10.3. O Gartner avalia soluções DLP 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.

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

| ESTUDO DE MERCADO | |
|---|---|
| **Solução para Investigação e Prevenção Contra Vazamento de Informações** | **SYMANTEC**<br>• Descoberta de onde os dados estão armazenados na nuvem, em dispositivos móveis e em ambientes locais da empresa;<br>• Monitoramento de como os dados estão sendo usados quando os funcionários estiverem conectados ou não à rede;<br>• Proteção dos dados contra vazamento ou roubo, independentemente de onde estiverem armazenados ou como estiverem sendo usados;<br>• Ampliação do alcance dos recursos de prevenção contra a perda de dados para incluir ambientes na nuvem e dispositivos móveis;<br>• Ampliação das políticas de segurança e conformidade para além dos limites da rede;<br>• Fornece o menor custo total de propriedade, com metodologias de implementação comprovadas, políticas intuitivas e ferramentas para o gerenciamento de incidentes, além de uma cobertura abrangente de todos os canais de alto risco;<br>• Proteção contra gravação de arquivos ou pastas em dispositivos móveis;<br>• Integração com a Solução de Antispam – SMG. |
| | **GTB TECHNOLOGIES**<br>• Descoberta de dados, descoberta eletrônica e classificação de dados – automática, em tempo real – com detecção de OCR;<br>• Descobrir, identificar, classificar, inventariar, indexar, redigir, corrigir, indexar, controlar e proteger dados, incluindo PII, PCI, PHI, IP, dados estruturados e não estruturados, FERC, NERC, SOX, GLBA e etc;<br>• Gerenciamento de direitos digitais com reconhecimento de conteúdo integrado;<br>• Reconhecimento de conteúdo e contexto que fornece às organizações um controle de acesso abrangente a dados confidenciais para constituintes internos e externos;<br>• Impedir a sincronização de dados confidenciais com nuvens privadas ou não autorizadas. |
| | **MCAFEE**<br>• Obtenção de proteção proativa à perda de dados;<br>• Implementação de políticas rapidamente para um valor imediato;<br>• Simplificação do gerenciamento de política. |
| | **FORCEPOINT**<br>• Reconhecimento dos dados confidenciais ocultos em imagens, documentos digitalizados e capturas de tela;<br>• Implementa com segurança os serviços na nuvem, como Microsoft Office 365 e Box, mantendo visibilidade e controle sobre dados confidenciais;<br>• O Drip DLP considera a transmissão cumulativa de dados para identificar pequenas quantidades de vazamentos de dados;<br>• Identificação de funcionários de alto risco, identificando atividades que indicam furto de dados;<br>• Detecção de dados com impressões digitais em dispositivos de ponto de extremidade dentro e fora da rede corporativa;<br>• Suporte para dispositivos de ponto de extremidade Mac OS X e Microsoft Windows;<br>• Detecção de envio de dados confidenciais para fora da empresa por e-mail, uploads na web, mensagens instantâneas e clientes de serviços em nuvem. Inclui descriptografia SSL quando usado com Forcepoint Web Security. |

Tabela 12 – Estudo de Mercado.

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

4.10.5.1. De acordo com a busca realizada no dia 20 de Janeiro de 2022, às 14:45, com as palavras chaves "data loss prevention", o portal: softwarepublico.gov.br, retornou que não havia encontrado nenhum software correspondente.


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

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

| ID | SOLUÇÃO | ORGÃO/UNIDADE | Nº PREGÃO | ÓRGÃO/UNIDADE |
|---|---|---|---|---|
| 01 | Escolha da proposta mais vantajosa para a contratação solução integrada de segurança para estação de trabalho e servidores em ambiente corporativo de acordo com as especificações, registro de preços, conforme condições, quantidades e exigências estabelecidas neste Edital e nos anexos. | MINISTERIO DA SAÚDE | 34/2021 | 250110 COORDENAÇÃO GERAL DE MATERIAL E PATRIMÔNIO |
| 02 | Registro de preços para a Aquisição de licenças de software para solução de prevenção contra vazamento de informações em meio digital, contemplando suporte, instalação, configuração, treinamento, garantia e atualização irrestrita para a última versão existente do fabricante por 36 meses a contar da assinatura do contrato, a fim de atender as demandas do PRODERJ, dos Órgãos Participantes e demais órgãos que futuramente aderirem a ATA de Registro de Preços, conforme as especificações contidas no Termo de Referência. | GOVERNO DO ESTADO DO RIO DE JANEIRO | 03/2021 | CENTRO DE TECNOLOGIA DE INFORMAÇÃO E COMUNICAÇÃO DO ESTADO DO RIO DE JANEIRO - PRODERJ |

Tabela 13 - Análise de Projetos Similares.

4.11.1. 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.

4.11.2. 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 | | X | |

Tabela 14 - Análise das Alternativas Existentes.

## 5. REGISTRO DE SOLUÇÕES CONSIDERADAS INVIÁVEIS

5.1. A **Solução de Id. 1** 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.

5.2. A **Solução de Id. 3** se apresentou inviável do ponto de vista econômico, tendo em vista o custo elevado da solução em relação ao cenário de contratação de nova solução de mercado, conforme evidenciado no item 4.9 deste estudo.

## 6. DESCRIÇÃO DA SOLUÇÃO ESCOLHIDA

### 6.1. Bens e serviços que compõem a solução

| ITEM | DESCRIÇÃO | MÉTRICA | QUANTIDADE |
|---|---|---|---|
| 1 | Aquisição de licenças de software de solução de prevenção contra vazamento de dados - Data Loss Prevention - DLP | Unidade | 3190 |
| 2 | Treinamento | Pessoa | 3 |

Tabela 15 - Bens e serviços que compõem a solução.

### 6.2. Justificativa da solução escolhida

6.3. 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 prevenção contra vazamento de informações em meio digital (Data Loss Prevention - DLP) incluindo implantação da solução, treinamento, manutenção especializada e suporte técnico pelo período de 36 (trinta e seis) meses,

6.4. 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.

6.5. A contratação será 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.

6.5.1. A contratação da solução escolhida se faz necessária em razão da necessidade

6.5.2. Assim, a contratação da solução de Data Loss Prevention - DLP 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 solução de prevenção contra vazamento de dados 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, armazenados em meio digital, seja comprometida, garantindo a disponibilidade, integridade, confidencialidade e autenticidade dos dados nas redes e sistemas computacionais da Funasa.

## 7. ESTIMATIVA DE VOLUME DA DEMANDA

### 7.1. Item 1 - Aquisição de licenças de software de solução de prevenção contra vazamento de dados - Data Loss Prevention - DLP

7.1.1. Para a definição da demanda de volume de licenciamento da solução, foi realizado um levantamento do quantitativo de usuários ativos desta Funasa, conforme Anexo - Levantamento de usuários ativos da Funasa. (SEI 3403340).

7.1.2. Atualmente há uma média de 3.034 contas ativas**,** e considerando as mudanças passíveis de ocorrem no cenário da Funasa e Superintendências Estaduais - SUEST's, especificamente quanto a expectativa de alteração do quadro de pessoal da Fundação, abarcando os servidores da casa, os terceirizados e estagiários, foi adicionada uma margem de 5% ao quantitativo mencionado, portanto o volume de licenciamento estimado para os próximos 03 anos é de 3190 licenças.

### 7.2. Item 2 - Treinamento

7.2.1. O quantitativo do item 2 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.

## 8. ANÁLISE COMPARATIVA DE CUSTOS (TCO)

### 8.1. CÁLCULO DOS CUSTOS TOTAIS DE PROPRIEDADE

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

| ITEM | DESCRIÇÃO | MÉTRICA | QUANTIDADE |
|---|---|---|---|
| 1 | Aquisição de licenças de software de solução de prevenção contra vazamento de dados - Data Loss Prevention - DLP | Unidade | 3190 |
| 2 | Treinamento | Pessoa | 3 |

Tabela 16 - Itens considerados para construção do TCO.

### 8.2. TCO PARA O ITEM 1

8.2.1. 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.

8.2.2. Para o item 1, a pesquisa traz em sua cesta de preços 04 (quatro) valores, sendo 1 (um) no parâmetro II (contratações públicas) e 03 (três) no parâmetro IV (fornecedores). Não houve êxito na obtenção de preços pelo parâmetro I, conforme análise detalhada constante dos itens 3.4 e 3.5 da Nota Técnica (SEI nº 3594251).

| Item | Descrição | Parâmetro | Fonte de consulta | Valor Unitário | Média | Desvio Padrão | Limite Superior (Média + Desvio) | Limite Inferior (Média -Desvio) | Análise de Exequibilidade de Preços |
|---|---|---|---|---|---|---|---|---|---|
| 1 | Aquisição de licenças de software de solução de prevenção contra vazamento de dados - Data Loss Prevention - DLP | II | Governo do Estado do RJ | R$ 1.055,00 | R$ 1.082,12 | 32,90 | 1.115,02 | 1.049,22 | ACEITÁVEL |
| | | IV | Fornecedor 1 (Arvvo) | R$ 1.112,20 | | | | | ACEITÁVEL |
| | | IV | Fornecedor 3 (ISH) | R$ 1.117,28 | | | | | EXC.ELEVADO |
| | | IV | Fornecedor 4 (A2B) | R$ 1.044,00 | | | | | INEXEQUÍVEL |
| 2 | Treinamento | IV | Fornecedor 1 (Arvvo) | R$ 15.000,00 | R$ 21.503,33 | 4.603,26 | 26.106,60 | 16.900,07 | INEXEQUÍVEL |
| | | IV | Fornecedor 3 (ISH) | R$ 24.500,00 | | | | | ACEITÁVEL |
| | | IV | Fornecedor 4 (A2B) | R$ 25.010,00 | | | | | ACEITÁVEL |

Tabela 17 - Preços coletados para o item 1.

8.2.3. Conforme exposto acima, após a exclusão dos valores elevados e inexequíveis, restou apenas 2 (dois) valores considerados aceitáveis para cada item e, considerando que para a definição do indicador a ser adotado para utilização do preço de referência o cálculo deve incidir sobre um **conjunto de três ou mais preços,** utilizou-se como parâmetro a média dos 4 (quatro) os preços coletados para o item 1.

| Item | Descrição | Parâmetro | Fonte de consulta | Valor Unitário | Média |
|---|---|---|---|---|---|
| 1 | Aquisição de licenças de software de solução de prevenção contra vazamento de dados - Data Loss Prevention - DLP | II | Governo do Estado do RJ | R$ 1.055,00 | R$ 1.082,12 |
| | | IV | Fornecedor 1 (Arvvo) | R$ 1.112,20 | |
| | | IV | Fornecedor 3 (ISH) | R$ 1.117,28 | |
| | | IV | Fornecedor 4 (A2B) | R$ 1.044,00 | |

Tabela 18 - Média de preços aceitáveis para o item 1.

8.3. **TCO PARA O ITEM 2**

8.3.1. 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.

8.3.2. Para o item 2, a pesquisa traz em sua cesta de preços 03 (três) valores no parâmetro IV. Não houve êxito na obtenção de preços pelos parâmetros I, e II conforme análise detalhada constante dos itens 3.4 e 3.5 da Nota Técnica (SEI nº 3594251).

| Item | Descrição | Parâmetro | Fonte de consulta | Valor Unitário | Média | Desvio Padrão | Limite Superior (Média + Desvio) | Limite Inferior (Média -Desvio) | Análise de Exequibilidade de Preços |
|---|---|---|---|---|---|---|---|---|---|
| 2 | Treinamento | IV | Fornecedor 1 (Arvvo) | R$ 15.000,00 | R$ 21.503,33 | 4.603,26 | 26.106,60 | 16.900,07 | INEXEQUÍVEL |
| | | IV | Fornecedor 3 (ISH) | R$ 24.500,00 | | | | | ACEITÁVEL |
| | | IV | Fornecedor 4 (A2B) | R$ 25.010,00 | | | | | ACEITÁVEL |

Tabela 19 - Preços coletados para o item 2.

8.3.3. Conforme exposto acima, após a exclusão dos valores elevados e inexequíveis, restou apenas 2 (dois) valores considerados aceitáveis para cada item e, considerando que para a definição do indicador a ser adotado para utilização do preço de referência o cálculo deve incidir sobre um **conjunto de três ou mais preços,** utilizou-se como parâmetro a média dos 3 (três) preços coletados para o item 2.

| Item | Descrição | Parâmetro | Fonte de consulta | Valor Unitário | Média |
|---|---|---|---|---|---|
| 2 | Treinamento | IV | Fornecedor 1 (Arvvo) | R$ 15.000,00 | R$ 21.503,33 |
| | | IV | Fornecedor 3 (ISH) | R$ 24.500,00 | |
| | | IV | Fornecedor 4 (A2B) | R$ 25.010,00 | |

Tabela 20 - Média de preços aceitáveis para o item 2.

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

9.1. 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 prevenção contra vazamento de dados (DLP) que atenda às necessidades da Funasa por 36 meses, o custo total da contratação foi estimado em **R$ 3.516.472,79 (três milhões, quinhentos e dezesseis mil quatrocentos e setenta e dois reais e setenta e nove centavos)** na forma como segue.

| ITEM | DESCRIÇÃO | QUANTIDADE | VALOR UNITÁRIO | VALOR TOTAL |
|---|---|---|---|---|
| 1 | Aquisição de licenças de software de solução de prevenção contra vazamento de dados - Data Loss Prevention - DLP | 3190 | R$ 1.082,12 | R$ 3.451.962,80 |
| 2 | Treinamento | 3 | R$ 21.503,33 | R$ 64.509,99 |
| **Custo Estimado Total** | | | | **R$ 3.516.472,79** |

Tabela 21 - Custo Estimado Total da Contratação.

9.2. O detalhamento da pesquisa de preços encontra-se na Nota Técnica de Elaboração de Pesquisa de Preços (SEI nº 3594251) e **P**lanilha de Estimativa de Custos (SEI nº 3980625).

## 10. BENEFÍCIOS ESPERADOS

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

10.1.1. Proteção das informações sensíveis ao negócio da FUNASA;

10.1.2. Identificação eficaz de violações de políticas e atividades suspeitas em tempo real, através dos servidores físicos e virtuais.

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

10.1.4. Controle da saída de dados sensíveis, seja via transferência de arquivos ou publicação em páginas da internet;

10.1.5. Redução dos danos/perdas causados por incidentes de segurança.

## 11. NECESSIDADES DE ADEQUAÇÃO DO AMBIENTE PARA EXECUÇÃO CONTRATUAL

Não se aplica

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

### 12.1. Recursos Materiais

12.1.1. 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.

### 12.2. Recursos Humanos

12.2.1. 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.

12.2.2. 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.

## 13. ESTRATÉGIA DE CONTINUIDADE CONTRATUAL

### 13.1. Requisitos de Continuidade Contratual

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

13.1.1.1. **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.

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

13.1.2.1. **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.

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

13.1.3.1. **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.

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

13.1.4.1. **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.

### 13.2. Continuidade do fornecimento da solução de tecnologia da informação em eventual interrupção contratual

13.2.1. 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;

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

13.2.3. 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;

13.2.4. 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;

13.2.5. 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;

13.2.6. 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.

### 13.3. Atividades de transição contratual e encerramento do contrato

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

13.3.2. 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;

13.3.3. 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.

13.3.4. 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.

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

13.4.1. 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

13.5. **Transferência de conhecimento**

13.5.1. 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.

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

13.6.1. 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;

13.6.2. 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.

## 14. APROVAÇÃO E ASSINATURAS

14.1. A Equipe de Planejamento da Contratação foi instituída pela Portaria nº 5424, de 26 de outubro de 2021 (SEI nº 3340533).

14.2. 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 |
|---|---|
| TELVIO MARTINS DE MELLO<br>**Coordenador-Geral de Modernização e de Tecnologia da Informação**<br>SIAPE: 1.425.456 | ANDRÉ WILSON PIMENTA SANTANA<br>**Coordenador de Inovação e Infraestrutura Tecnológica**<br>SIAPE: 1.347.001 |

Tabela 22 - Equipe de Planejamento da Contratação.

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

14.3.1. 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<br>**Diretor do Departamento de Administração**<br>SIAPE 3.278.934 |

Tabela 23 - Autoridade Máxima da Área de TIC.

Documento assinado eletronicamente por **Andre Wilson Pimenta Santana**, **Coordenador de Inovação e Infraestrutura Tecnológica**, em 16/08/2022, às 11:30, 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 **Telvio Martins de Mello**, **Coordenador-Geral de Modernização e de Tecnologia da Informação**, em 16/08/2022, às 12:30, 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 31/08/2022, às 11:20, 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 **3980626** e o código CRC **8729FBE1**.

**Referência:** Processo nº 25100.005982/2021-61 SEI nº 3980626