



FUNDAÇÃO NACIONAL DE SAÚDE
ESTUDO TÉCNICO PRELIMINAR DA CONTRATAÇÃO

Processo nº 25100.000386/2021-95

1. **INTRODUÇÃO**

- 1.1. 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.
- 1.2. Esse estudo técnico irá analisar a melhor forma de lidar com as duas demandas existentes no *Data center* da Funasa, aquisição de uma nova solução de armazenamento e a aquisição de servidores de redes, visto que são projetos que se complementam.
- 1.3. Referência: Art. 11 da IN SGD/ME nº 1/2019.

2. **DEFINIÇÃO E ESPECIFICAÇÃO DAS NECESSIDADES E REQUISITOS**

2.1. **DESCRIÇÃO DA DEMANDA**

2.1.1. Trata-se de demanda da Coordenação-Geral de Modernização e Tecnologia da Informação - CGMTI para analisar viabilidade de contratação/renovação de licenças de software, serviços de manutenção e suporte da solução de backup da Fundação Nacional de Saúde - Funasa, e garantia da proteção dos dados desta fundação por 36 meses.

2.2. **IDENTIFICAÇÃO DAS NECESSIDADES DE NEGÓCIO**

2.2.1. 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.

2.2.2. 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.

2.2.3. A solução de backup é um serviço de fundamental importância para a Organização, pois suporta a função de salvaguarda das informações que apoiam a execução das atividades finalísticas da Funasa, de forma a garantir o atingimento de sua missão institucional.

2.2.4. Hoje, é fundamental manter as áreas de negócio do órgão com recursos tecnológicos que garantam o acesso às informações de sua propriedade ou sob sua custódia, protegendo-as de acessos não autorizados, conforme a Política de Segurança da Informação.

2.2.5. A contratação em tela visa atender à necessidade de continuidade dos serviços de *backup* da Funasa, permitindo:

- 2.2.5.1. Prover maior capacidade de armazenamento, gravação, recuperação, segurança e disponibilidade das informações para atender às demandas atuais e futuras da Funasa, além de regularizar as pendências de licenciamento, manutenção e suporte técnico da atual solução de *backup*;
- 2.2.5.2. Criar um plano de continuidade para recuperar um sistema ou serviço de TI em caso de falha ou em caso de ataque cibernético à rede de tecnologia da Funasa;
- 2.2.5.3. Criar redundâncias de recuperação de desastres que possa recuperar, no mínimo, 24 horas de dados, serviços e sistemas críticos da instituição;

- 2.2.5.4. Implementar alta disponibilidade no processo de restauração e recuperação de dados; e
- 2.2.5.5. Manter um serviço de *backup* de longa retenção.
- 2.2.5.6. 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.

2.2.6. O processo de backup é parte dos procedimentos de Segurança da Informação que a CGMTI tem como obrigação de executar e garantir a disponibilidade dos dados salvaguardados pelo backup, devendo proporcionar uma grande capacidade de acondicionamento de arquivos digitais, estabelecendo política de proteção e recuperação de dados, mantendo a informação intacta e acessível para a recuperação em caso de desastres. Esclarece-se ainda que, por tratar-se de uma solução de apoio à gestão da política de segurança da informação e comunicação da FUNASA, existe o entendimento de que a manutenção desta infraestrutura deve ser considerada serviço contínuo, demandando.

2.3. IDENTIFICAÇÃO DAS NECESSIDADES TECNOLÓGICAS E ANÁLISE DO CENÁRIO ATUAL

2.3.1. A solução atual de *backup* da Funasa foi adquirida através do Contrato 08/2017 que teve vigência de 03/04/2017 até 03/04/2019 (Processo SEI nº 25100.036154/2014-46, documento 0075541 pág. 97 à 102). A seguir, ilustração demonstrativa da distribuição:

DESCRIÇÃO	QUANTIDADE
Módulo controlador modelo Veritas NetBackup 5240	1
Gavetas de discos Veritas NetBackup 5240	1
Licença NetBackup Enterprise — Frontend Terabyte (Renovação)	20 TB
Licença NetBackup Enterprise — Frontend Terabyte (Adicional)	10 TB
Suporte BCS (Business Critical - 12 Meses)	1
Suporte Essencial (12 meses)	1

Tabela 01 - Contrato Legado Funasa.

2.3.2. A solução de *Backup* é composta por 01 Appliance (Hardware) Netbackup 5240, que possui capacidade de 103 Terabytes de área líquida de armazenamento, conforme ilustração demonstrativa da distribuição:

NetBackup Appliance					
UID	Hostname	Appliance Model	Software Version	Capacity	Capacity Utilization
VTAS0002530		5240	3.1.1	102.77 TB	 33.16%

2.3.2.1. Foi consultado o site da fabricante da solução e constatado que o hardware 5240 possui garantia até o mês 10 de 2025. No quadro abaixo está descrito o período de garantia do hardware.

NETBACKUP APPLIANCE HARDWARE			
MODEL	START OF SALE	END OF SALE	END OF SUPPORT LIFE (EOSL)
5240	04/07/2016	30/09/2020	31/10/2025

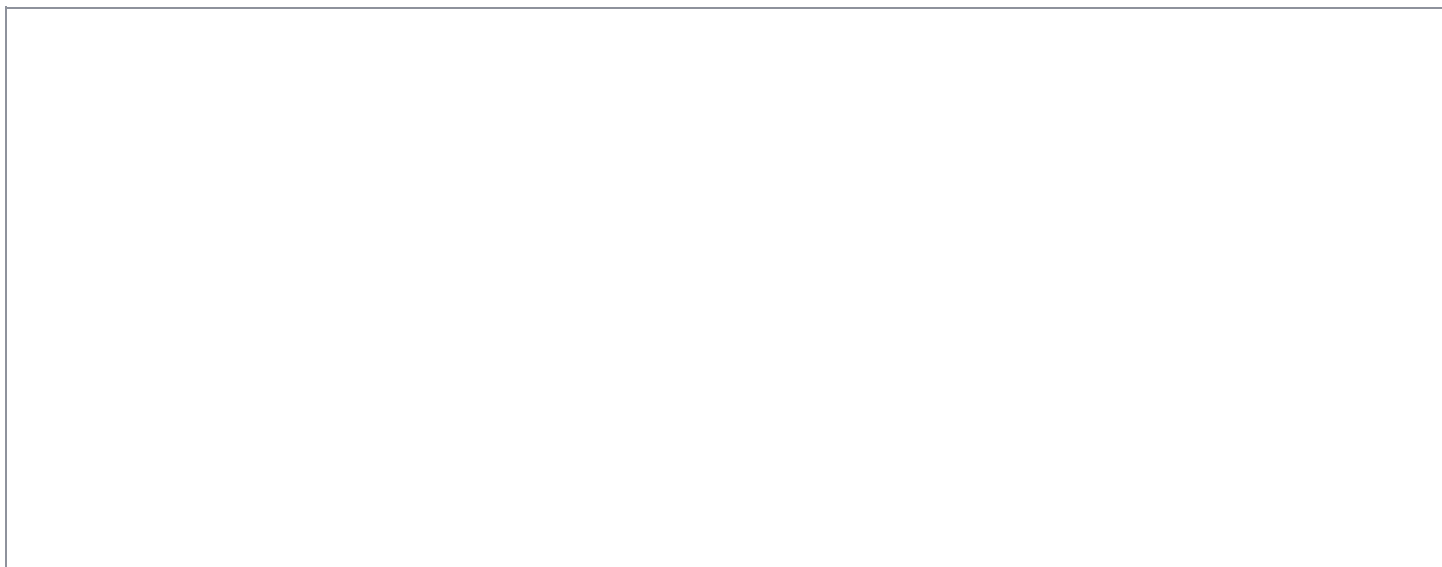
Tabela 02 - Garantia do hardware. Fonte: https://www.veritas.com/support/en_US/article.100045773.

2.3.3. Quanto ao licenciamento do software, a Funasa atualmente utiliza o modelo de licenciamento permanente por volumetria de Armazenamento de Frontend. Neste tipo de licenciamento, cobra-se um valor por Terabyte (TB) de dados que será protegido. Neste contexto, há uma diferenciação importante a saber:

1. **Armazenamento de Backend:** leva-se em consideração a quantidade total de dados protegida pelo *backup* durante toda a política de retenção da sua Organização, ou seja, em um servidor de arquivos é considerada a soma do volume dos arquivos atuais e todas as versões de modificações efetuadas nestes arquivos, desde que ainda não tenham expirado.
2. **Armazenamento de Frontend:** leva-se em consideração somente o volume do dado protegido, sendo independente do tempo de retenção da política da sua Organização, ou seja, em um servidor de arquivos irá considerar somente o volume dos arquivos atuais, não importando o tamanho das versões modificadas salvas que ainda estejam válidas.

2.3.4. A volumetria contratada através do contrato 08/2017 e aditivos, foi de 30 TB Frontend, no qual inclui implementação ilimitada de agentes, proteção de servidores de arquivos, bancos de dados, aplicativos e archive para ambientes locais. Além de gerenciamento centralizado de servidores de backup para locais ramificados.


- I. **Observação:** O licenciamento atual da solução de backup não contempla os serviços do Office 365. É necessário pontuar que a proteção dos dados do Office 365 é uma necessidade importante da Funasa para se adequar às exigências da LGPD e Acórdão 1109/2021 do TCU com foco no atendimento aos 5 subcontroles:



10.1	Realize cópias de segurança (<i>backups</i>) de todos os dados da organização, de forma regular e automática
10.2	Realize cópias de segurança (<i>backups</i>) integrais dos sistemas críticos da organização, de modo a permitir sua rápida recuperação em caso de necessidade
10.3	Realize, periodicamente, testes de restauração (<i>restore</i>) das cópias de segurança (<i>backups</i>) da organização, de modo a atestar seu funcionamento em caso de necessidade
10.4	Proteja adequadamente as cópias de segurança (<i>backups</i>) da organização, por meio de mecanismos de controle de acesso físico e lógico
10.5	Armazene as cópias de segurança (<i>backups</i>) da organização em ao menos um destino não acessível remotamente

FONTE: https://pesquisa.apps.tcu.gov.br/#/documento/acordao-completo/*/NUMACORDAO%253A1109%2520ANOACORDAO%253A2021%2520COLEGIADO%253A%2522Plen%25C3%25A1rio%2522/DTRELEVANCIA%2520desc%252C%2520NUMACORDAOINT%2520desc/0/%2520

II. **Observação:** Outro ponto importante é que no contrato público do fabricante Microsoft Office 365 fica claro que a responsabilidade da proteção dos dados será da FUNASA, conforme apresentado a seguir:



Disponibilidade dos Serviços

6. Disponibilidade dos Serviços.

a. Os Serviços, os Aplicativos e Serviços de Terceiros ou materiais ou produtos oferecidos por meio dos Serviços podem estar indisponíveis periodicamente ou poderão ser oferecidos apenas por tempo limitado ou podem variar dependendo da sua região ou dispositivo. Se você alterar o local associado à sua conta da Microsoft, poderá precisar readquirir material ou aplicativos que estavam disponíveis a você e pagos na região anterior. Você concorda em não acessar ou usar material ou Serviços que são ilícitos ou não licenciados para uso no país a partir do qual você acessa ou usa tais materiais ou Serviços ou para ocultar ou falsificar seu local ou identidade a fim de acessar ou usar tais materiais ou Serviços.

b. Trabalhamos para manter os Serviços em funcionamento; entretanto, todos os serviços online sofrem interrupções e paradas ocasionais, e a Microsoft não é responsável por nenhuma interrupção ou perda que você possa sofrer em decorrência disso. Em caso de uma interrupção, você não poderá recuperar Seu Conteúdo nem os Dados que você tinha armazenado. Recomendamos que você faça backup regularmente do Seu Conteúdo e dos Dados armazenados nos Serviços ou que os armazene usando Aplicativos e Serviços de Terceiros.

FONTE: <https://www.microsoft.com/pt-br/servicesagreement>

III. **Observação:** Proteção contra ataques cibernéticos, por exemplo Ransomware, novamente o contrato público do fabricante Microsoft Office 365 fica claro que a responsabilidade da proteção dos dados será da FUNASA, conforme apresentado a seguir:

Mesmo que você tome todas as precauções para proteger sua organização, ainda poderá ser vítima de um ataque de **ransomware**. O ransomware é uma grande empresa e os ataques são muito sofisticados.

As etapas deste artigo darão a você a melhor chance de recuperar dados e interromper a propagação interna da infecção. Antes de começar, considere os seguintes itens:

- Não há garantias de que pagar o resgate retornará o acesso aos arquivos. Na verdade, pagar o resgate pode torná-lo um alvo para mais ransomware.

Se você já pagou, mas se recuperou sem usar a solução do invasor, entre em contato com seu banco para ver se ele pode bloquear a transação.

Também recomendamos que você reporte o ataque de ransomware à aplicação da lei, aos sites de relatórios de fraude e à Microsoft, conforme descrito posteriormente neste artigo.

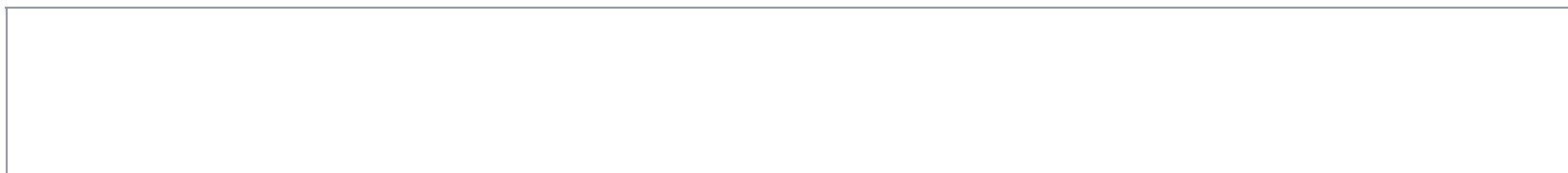
- É importante que você responda rapidamente ao ataque e suas consequências. Quanto mais tempo você esperar, menor será a probabilidade de recuperar os dados afetados.

Etapa 1: Verificar seus backups

Se você tiver backups offline, provavelmente poderá restaurar os dados criptografados depois de remover a carga de ransomware (malware) do seu ambiente.

FONTE: <https://docs.microsoft.com/en-us/microsoft-365/security/office-365-security/recover-from-ransomware?view=o365-worldwide>

2.3.5. Foram extraídos os relatórios de consumo de backup (documento sei nº 2760757) de cada unidade da Funasa para obter o valor assertivo de consumo de dados, segue o resultado abaixo:



Soluções Veritas Existentes

- 1x Appliances 5240 103TB
- 30 TB de NetBackup Complete Edition

Uso NetBackup atual

NetBackup Software

- 52,75 FETB

Site	Standard	Oracle	MS-Windows	MS-SQL-Server	MS-Exchange-Server	Total
FARINA	3,54	7,40	21,70	0,21	2,95	35,78
FARINAAC			0,45			0,45
FARINAAL			0,40			0,40
FARINAAM			0,77			0,77
FARINAAP						-
FARINABA			0,91			0,91
FARINACE			0,77			0,77
FARINAE			0,59			0,59
FARINAGO			0,61			0,61
FARINAMA			0,50			0,50
FARINAMG			0,97			0,97
FARINAMS			1,24			1,24
FARINAMT			0,88			0,88
FARINAPA			0,64			0,64
FARINAPB						-
FARINAPE			0,91			0,91
FARINAPI			0,52			0,52
FARIPAPR			0,76			0,76
FARINARJ			0,86			0,86
FARINARN			1,14			1,14
FARINARO			0,70			0,70
FARINARR			0,66			0,66
FARINARS			0,34			0,34
FARINASC			1,05			1,05
FARINASE			0,79			0,79
FARINASP			0,52			0,52
FARINATO						-
						52,75

2.3.6. Analisando o contexto do relatório citado acima, é possível identificar que o hardware de backup está utilizando 45% da sua capacidade total de 103 TB de armazenamento. A massa de dados de backup é de 52,75 TB, incluindo Presidência-Brasília e todas as unidades das Superintendências Estaduais - Suest's.

2.3.7. Dessa forma, a Funasa possui o seguinte cenário:

1. Renovação dos 30 TB existentes;
2. Licenciamento dos 23 TB novos, no mínimo, para regularizar o ambiente atual;
3. Estimar o crescimento do ambiente de backup para os próximos 03 ou 05 anos;
4. Avaliar a aquisição de um novo Appliance para criar o ambiente de recuperação de desastres e aumentar a maturidade de segurança de dados da Funasa.
5. Estudar a necessidade de aquisição para proteção dos dados do Office365

2.3.8. Taxa de crescimento de armazenamento de backup

2.3.8.1. Para estimar uma taxa de crescimento de armazenamento anual do ambiente, foi considerada a soma da massa total de dados de 2017 e multiplicado por 15,17%, ou seja, 30 * 1,1517. Desse modo, encontramos o valor aproximado de crescimento por ano, conforme descrito na tabela abaixo:

TAXA DE CRESCIMENTO AO ANO

TB	ANO
30	2017
34,551	2018
39,7923867	2019
45,82889176	2020
52,78113464	2021
60,78803277	2022
70,00957734	2023

Tabela 03 - Estimativa de crescimento da massa de backup.

2.3.8.2. Com estes dados, podemos estimar que a taxa mínima de crescimento médio nos últimos cinco anos foi de aproximadamente 15%. Com isso, o valor estimado de dados para a renovação e expansão do licenciamento de backup da Funasa ficaria em torno de 4.5 TB por ano, somando o montante de 70 TB para os próximos três anos.

2.3.9. **Justificativa para a expansão da solução:** Aquisição de um segundo repositório de dados para criar um ambiente de Recuperação de desastres.

2.3.9.1. Diante do cenário de constante evolução de ataques cibernéticos, a presente contratação pretende melhorar a maturidade da segurança de dados da Funasa.

2.3.9.2. Observando o ataque hacker que ocorreu no dia 03 de novembro de 2020 ao ambiente de tecnologia do STJ e que paralisou todas as atividades do Superior Tribunal de Justiça por semanas, no qual afetou o ambiente de backup da instituição, esta equipe técnica entende que é necessário ampliar o ambiente de backup da Funasa para aumentar a proteção dos dados da instituição.

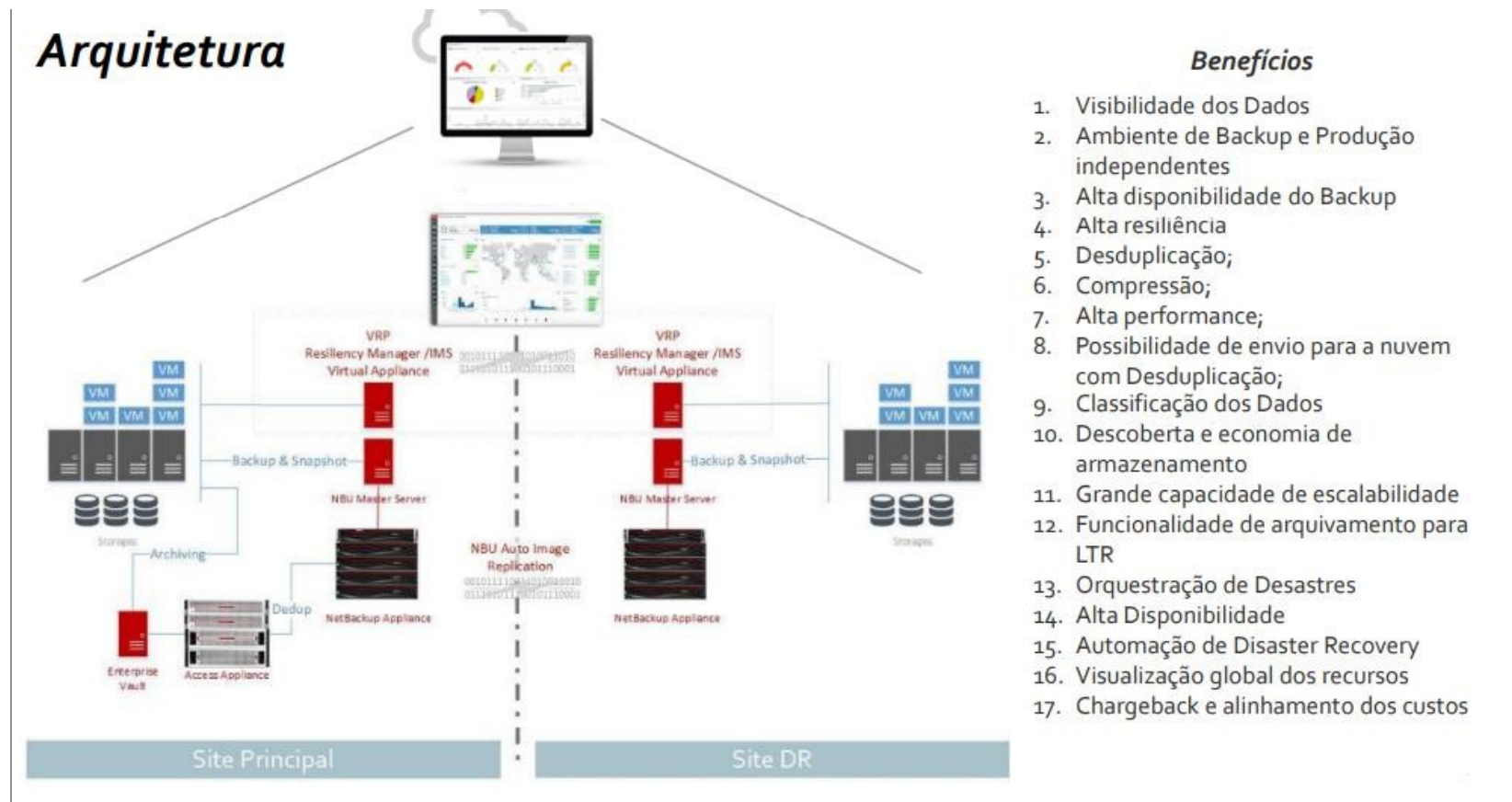
1. <https://www.cisoadvisor.com.br/stj-mais-de-1200-servidores-congelados-backups-destruidos/>
2. <https://www.conjur.com.br/2020-nov-15/stj-continua-restaurando-backup-servidores-ajustando-sistema>

2.3.9.3. Atualmente, a Funasa possui somente 01 (um) repositório de backup, e esta solução opera no mesmo ambiente do dado de produção. Caso ocorra algum desastre físico ou um ataque cibernético que venha comprometer a solução de backup atual, a instituição terá bastante dificuldades para recuperar os seus dados.

2.3.10. Neste caso, a ação de expandir o local de armazenamento de backup possui o objetivo de criar um segundo ambiente segregado do ambiente de produção para recuperação de desastre. Com isso, caso o backup principal venha a ser comprometido, a Funasa terá um segundo local para salvar e recuperar os dados e os sistemas após um desastre ou ataque cibernético.

2.3.10.1. A imagem abaixo descreve o modelo simplificado da arquitetura pretendida pela Funasa:





2.4. JUSTIFICATIVA PARA AQUISIÇÃO DE UM NOVO APPLIANCE

2.4.1. Atualmente, a Funasa possui apenas 01 (um) appliance para armazenamento do backup de todos os serviços, situado dentro da sala cofre, identificando-se, portanto, a necessidade de aquisição de um novo appliance, que possibilite a criação de um ambiente de recuperação de desastres com vistas a aumentar a maturidade de segurança de dados da Fundação.

2.4.2. Para tanto, com a aquisição de renovação dos serviços de backup, faz-se necessária a definição de um local de segurança onde deve ser instalado um novo appliance para redundância dos dados armazenados que não seria afetado por um desastre no local de dados primário (Funasa).

2.4.3. Partindo desta premissa, foram definidos pela área técnica 02 cenários para alocação da solução, conforme a seguir:

2.4.4. **Opção 01** - Instalação do novo appliance na estrutura de datacenter do Departamento de Informática do Sistema Único de Saúde (DATASUS), neste sentido, cumpre ressaltar que já está tramitando o Processo SEI (25100.003913/2021-13), no qual foi formalizada a presente demanda junto ao Diretor do DATASUS.

2.4.5. **Opção 02** - Caso não seja possível a alocação da solução no Cenário 01, o novo appliance poderá ser alocado na Superintendência de Goiânia - SUEST-GO com as devidas especificações de segurança e energia recomendadas pelo fabricante. A escolha pela SUEST-GO considera a sua proximidade caso ocorra um eventual problema em que haja a necessidade de intervenção presencial.

2.4.6. Nota Técnica - Requisitos da Suest para receber a solução appliance (3082854)

2.5. **JUSTIFICATIVA DA FUNCIONALIDADE DE BACKUP E ARCHIVE PARA SOLUÇÃO DO OFFICE365**

2.5.1. A Funasa atualmente utiliza a suíte de automação de escritório Microsoft Office 2016, o servidor de e-mail corporativo Exchange Server 2013, a ferramenta de mensageria instantânea Skype for Business (antigo Lync Server) 2016 e a plataforma de aplicações web SharePoint 2016. Após mais de 5 anos de uso, esse conjunto de softwares encontra-se desatualizado e precisa ser renovado.

2.5.2. O processo (25100.002748/2020-00) trata da contratação do licenciamento das soluções Microsoft, no qual a Funasa adotou e já implantou o licenciamento do Office365 E1.

2.5.3. Os serviços do licenciamento Office365 possuem diversas ferramentas de colaboração e serviços on-line, por exemplo, o sistema de armazenamento online de arquivos OneDrive, que permite que os arquivos de determinado servidor ou unidade estejam armazenados em computadores seguros da nuvem e o serviço de e-mail na nuvem. Vale ressaltar que a utilização do serviço de e-mail na nuvem irá resultar na redução drástica do volume de dados que permanecem sendo alvo dessa tecnologia, reduzindo-se, também drasticamente, a economia em volume de armazenamento advinda da aplicação das rotinas de arquivamento.

2.5.4. Diante dessa contratação de solução Office365, surge a necessidade de proteção dos dados institucionais que estarão no ambiente de nuvem, visto que os dados, em qualquer modelo de implementação (on-prem, IaaS, Paas ou SaaS), sempre será responsabilidade do cliente, a equipe técnica da CGMTI entende que o modelo de proteção de dados da nuvem Microsoft não atende completamente as necessidades de salvaguarda de informações da Funasa. Nesse cenário, a equipe entende que é necessária uma solução complementar para proteger os dados da Funasa e atender algumas disposições da LGPD e Acórdão 1109/2021 do TCU.

2.5.4.1. Vale pontuar que atualmente a Funasa não possui nenhuma solução de proteção de dados ou backup para o ambiente Microsoft 365, por isso, essa necessidade será tratada como uma nova aquisição ou expansão da solução atual.

2.5.5. O documento (SEI Nº 2748617) possui a descrição e comparação das funcionalidades de proteção de dados da nuvem Microsoft.

2.6. **IDENTIFICAÇÃO DAS NECESSIDADES TECNOLÓGICAS**

2.6.1. A solução deve permitir a automatização de processos para recuperação de desastres com a fácil integração, promovida por técnicas de replicação, nativas do sistema de armazenamento.

2.6.2. A solução deve garantir integração com outros recursos do data center de forma a garantir o desempenho das aplicações e demais serviços que garantem a continuidade do negócio da Funasa.

2.6.3. Deve operar com arranjos e configurações que garantam a alta disponibilidade do sistema de armazenamento de dados. Disponibilidade em 99.999% ao ano, Downtime de 5min 15s.

2.6.4. Deve prover soluções para garantir integridade e segurança dos dados armazenados.

- 2.6.5. Deve ser instalado de forma a reaproveitar recursos no data center, garantindo o mínimo de tempo possível para instalação e migração de dados.
- 2.6.6. Deve possuir funcionalidades operacionais que devem garantir o gerenciamento, provisionamento de ambientes, replicação de dados, deduplicação de dados e backup e restore de dados.
- 2.6.7. Deve possuir funcionalidade de proteção de informação das soluções relativas ao Office365 que representarem profunda alteração na forma com que os dados são armazenados e protegidos.
- 2.6.7.1. Deve possuir proteção para caixas postais no Office365.
- 2.6.7.2. Para correio eletrônico, devem ser consideradas, para dimensionamento da proteção inicial de 5.000 caixas postais.
- 2.6.7.3. Deve ser configurado backup do Office365 com dupla abordagem de proteção, ou seja, armazenado em duas localidades diferentes na nuvem provida pela CONTRATADA, sendo uma delas com localização física no território nacional.

3. ESTIMATIVA DA DEMANDA – QUANTIDADE DE BENS E SERVIÇOS

- 3.1. A demanda de volume da Solução completo foi estudada nos subitens 2.3.5 e 2.3.8, o licenciamento da solução estimado para os próximos 03 anos é de 70 TB.
- 3.2. Deverá haver garantia de 36 meses para os equipamentos, conforme o ciclo de vida do hardware, definido por meio do Documento de Boas práticas, Orientações e Vedações, vinculado à Portaria MP/STI nº 20, de 14 de junho de 2016, da Secretário de Tecnologia da Informação do Ministério do Planejamento, Desenvolvimento e Gestão.

4. ANÁLISE DE SOLUÇÕES E CENÁRIOS

- 4.1. Disponibilidade de solução similar em outro órgão ou entidade da Administração Pública

ÓRGÃO	Nº PREGÃO ELETRÔNICO	OBJETO DA CONTRATAÇÃO
TRIBUNAL DE JUSTIÇA DE RONDÔNIA	PE Nº 75/2021	Registro de preços, pelo prazo de 12 (doze) meses, para eventual fornecimento de Solução <i>Netbackup</i> (solução integrada de <i>backup</i>), visando atender as necessidades do Poder Judiciário do Estado de Rondônia - PJRO.
MINISTÉRIO DO DESENVOLVIMENTO REGIONAL	PE Nº 20/2020	Contratação de empresas especializada para Aquisição de hardware, software licenciamento, configuração e garantia por 60 meses, incluindo suporte e manutenção com substituição de peças em regime 24x7 para ampliação e modernização tecnológica da infraestrutura de backup, objetivando o aumento da capacidade e velocidade das cópias de segurança e recuperação dos dados computacionais e corporativos, aliado a uma necessidade de ampliação e atualização da infraestrutura tecnológica de backup do MDR
TRIBUNAL DE CONTAS DA UNIÃO - TCU	PE Nº 56/2020	Contratação de serviços gerenciados de proteção de dados compostos por software e repositório de backup, instalação, configuração, administração, suporte, monitoramento e operação da solução, pelo período de 60 (sessenta) meses, em regime de empreitada por preço unitário, conforme

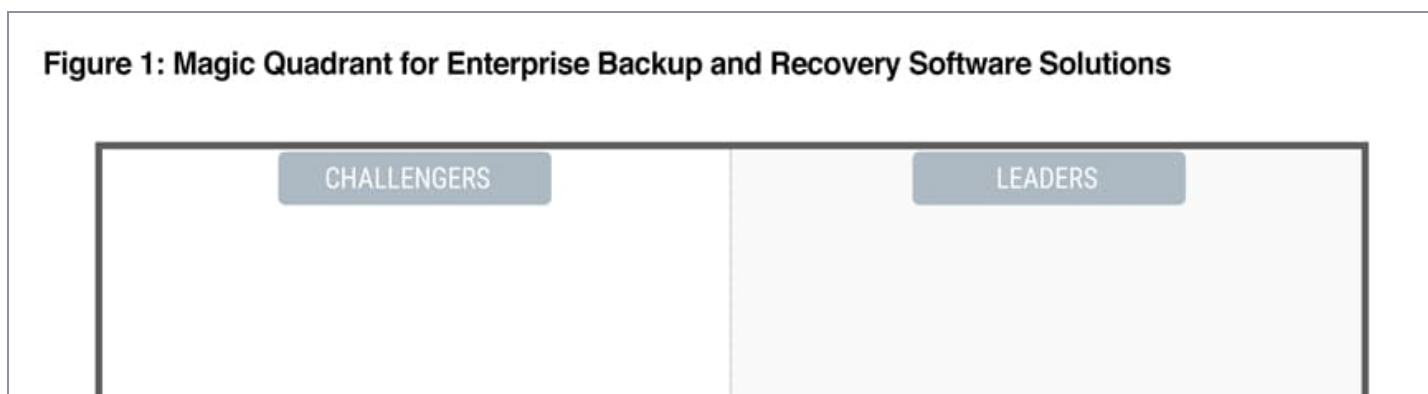
		condições e especificações dispostas no Edital do Pregão Eletrônico n.º 56/2020 e em seus Anexos.
SERVIÇO SOCIAL DO COMÉRCIO - SESC GO	PE Nº 21/01.00009	Registro de preços, por um período de 12 (doze) meses, para Aquisição de Solução Integrada para Proteção dos dados contemplando hardware e software, e informações do ambiente produtivo do Sesc/GO. Incluindo sua implantação, configuração, garantia e suporte para atendimento das necessidades do Sesc/GO.
FUNDO NACIONAL DE DESENVOLVIMENTO DA EDUCAÇÃO - FNDE	PE Nº 07/2020	Contratação de serviços de tecnologia da informação e comunicação aquisição de solução para backup, incluindo o fornecimento de dispositivo dedicado para cópias em disco com deduplicação de dados (Appliance de Backup), aquisição de softwares gerenciadores de backup, serviços de garantia e suporte técnico do fabricante, transferência de conhecimento e horas de operação assistida.

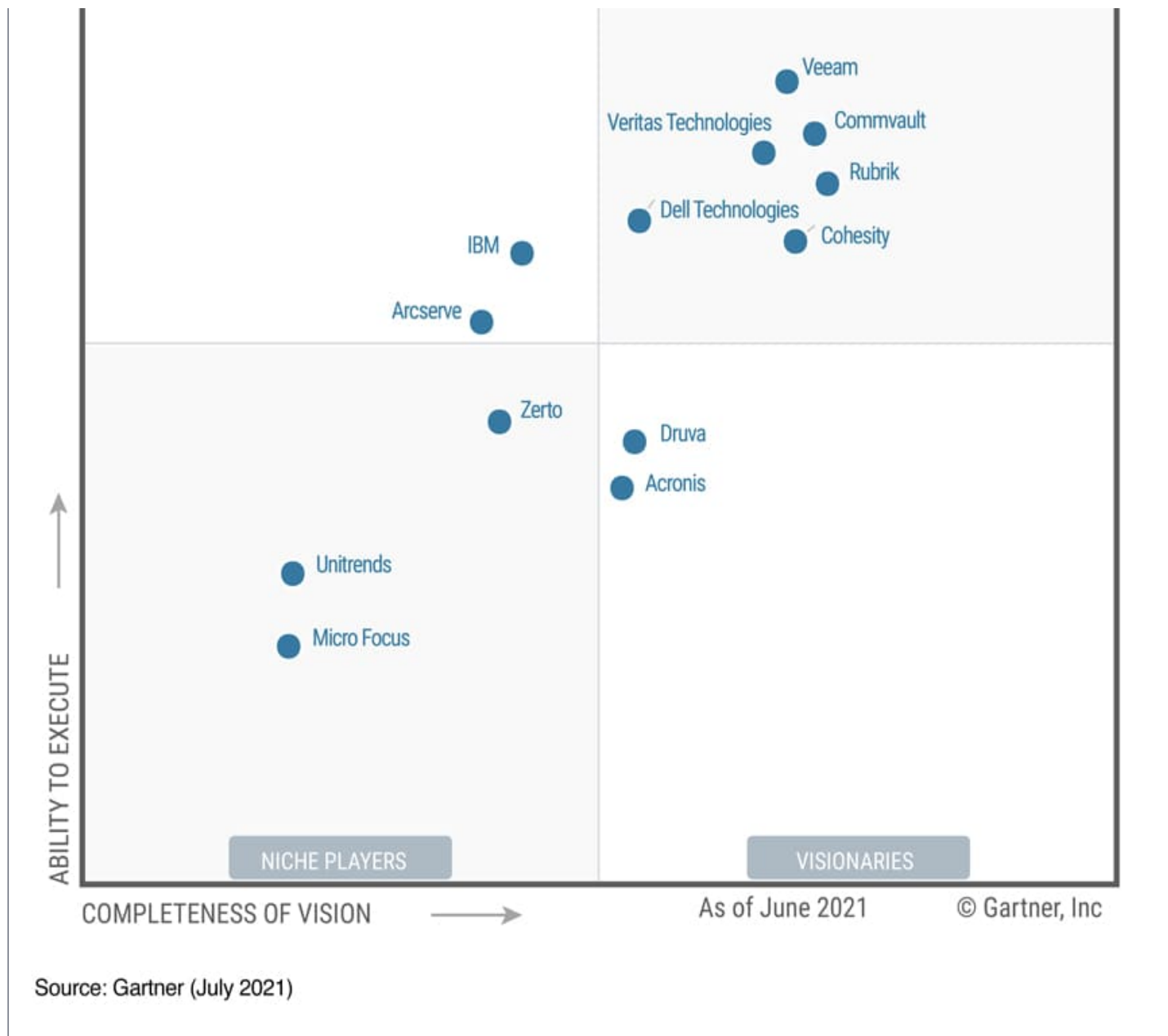
Tabela 04 - Soluções similares de outros órgãos.

4.2. Consoante análise de mercado realizada pelo Gartner (empresa com atuação no ramo de pesquisas, consultorias, eventos e prospecções acerca do mercado de TI), há no mercado diversas soluções de guarda, tratamento, proteção e recuperação de dados de missão crítica. Verificou-se após pesquisa de mercado, tanto nos sites dos fabricantes quanto em processos já realizados pela administração pública, que dentre os diversos fabricantes, as especificações técnicas das soluções são, em sua maioria, comuns entre si, o que permite especificar a solução desejada para posterior aquisição através de processo licitatório.

4.3. Um referencial de mercado mundialmente utilizado, não apenas pela Administração Pública Federal, mas também por empresas privadas, é a análise independente realizada por empresas de pesquisa, como por exemplo o Gartner. Anualmente são publicados relatórios comparando as principais soluções do mercado em determinados nichos da tecnologia da informação. Em cada um desses relatórios, fabricantes são avaliados e posicionados em um gráfico (chamado de quadrante mágico) em que são pesados “habilidade de execução” e “completude de visão”. Isso representa uma visão do nível de maturidade e posicionamento no mercado das soluções disponíveis.

4.4. No quadrante de solução de Backup, há alguns fabricantes que poderiam atender à demanda da Funasa e que são líderes de mercado, conforme o quadrante mágico do Gartner são: Commvault, Veeam, Veritas, entre outros.





4.4.1. O licenciamento de software pode ser realizado de diversas formas, como por exemplo: Do tipo perpétuo ou por subscrição e Por Terabytes (TB) ou Socket (processador ou pastilha).

4.4.2. Em pesquisa de mercado nos sites dos principais fabricantes de solução de backup/restore, conforme quadrante mágico do Gartner, verificou-se a seguinte matriz de possibilidades de licenciamento:

FABRICANTE	SOCKET		TERABYTE (TB)	
	Perpétua	Subscrição	Perpétua	Subscrição
Veeam	Sim	Não	Não	Não
Veritas	Sim	Não	Sim	Sim
Acronis	Sim	Sim	Não	Não
Commvault	Sim	Sim	Sim	Sim

Tabela 05 - Comparativo de licenciamento de solução.

4.5. Desta forma, para análise da solução, esta foi particionada em 5 Itens distintos, quais sejam: Software de Backup, Hardware de Backup, Backup para Office365, Serviço Especializado e Repasse de Conhecimento, com análise dos cenários de Manter e Expandir a atual solução, Contratação de nova solução de mercado, Adoção de Software Livre.

ITEM	DESCRIÇÃO	CENÁRIOS
1	Aquisição / Renovação de software de Backup	Cenário 1 - Manter e Expandir a atual solução
		Cenário 2 - Contratação de nova solução de mercado
		Cenário 3 - Adoção de Software Livre
2	Aquisição / Renovação de Hardware de Backup	Cenário 1 - Manter e Expandir a atual solução
		Cenário 2 - Contratação de nova solução de mercado
		Cenário 3 - Adoção de Software Livre
3	Aquisição de Solução para Backup de Office365	Cenário 1 - Manter e Expandir a atual solução
		Cenário 2 - Contratação de nova solução de mercado
		Cenário 3 - Adoção de Software Livre
4	Serviço de suporte técnico	Cenário 1 - Suporte técnico na solução já existente.
		Cenário 2 - Suporte técnico em uma nova solução
5	Repasse de conhecimento	Cenário 1 - Repasse de conhecimento na solução já existente

Cenário 2 - Repasse de conhecimento em uma nova solução

Tabela 06 - Composição dos itens da solução de backup.

5. ANÁLISE COMPARATIVA DE CENÁRIOS PARA CADA UM DOS ITENS**5.1. ITEM 1 - AQUISIÇÃO / RENOVAÇÃO DE SOFTWARE DE BACKUP****5.1.1. Cenário 1 - Item 1 - Manter e Expandir a atual solução.**

5.1.1.1. Em se tratando de aspectos técnicos, observa-se que a solução está operando em produção há anos, atendendo plenamente às expectativas e necessidades do órgão. A equipe técnica da instituição está capacitada na sua operação, reduzindo a necessidade de investir em treinamentos adicionais.

5.1.1.2. O ambiente de produção é complexo, e para atender à demanda a solução atual possui centenas de regras e customizações, configuradas no decorrer dos anos de operação. A migração para uma plataforma diferente implicaria tanto em grande esforço técnico, custo e risco inerente a alterações em um ambiente de alta complexidade. Como a solução em questão representa o ponto central de salvaguarda de dados do órgão, qualquer falha em sua operação pode causar indisponibilidade no ambiente. Trata-se, portanto de um ativo de alta criticidade, o que eleva drasticamente o impacto de eventuais falhas no seu uso.

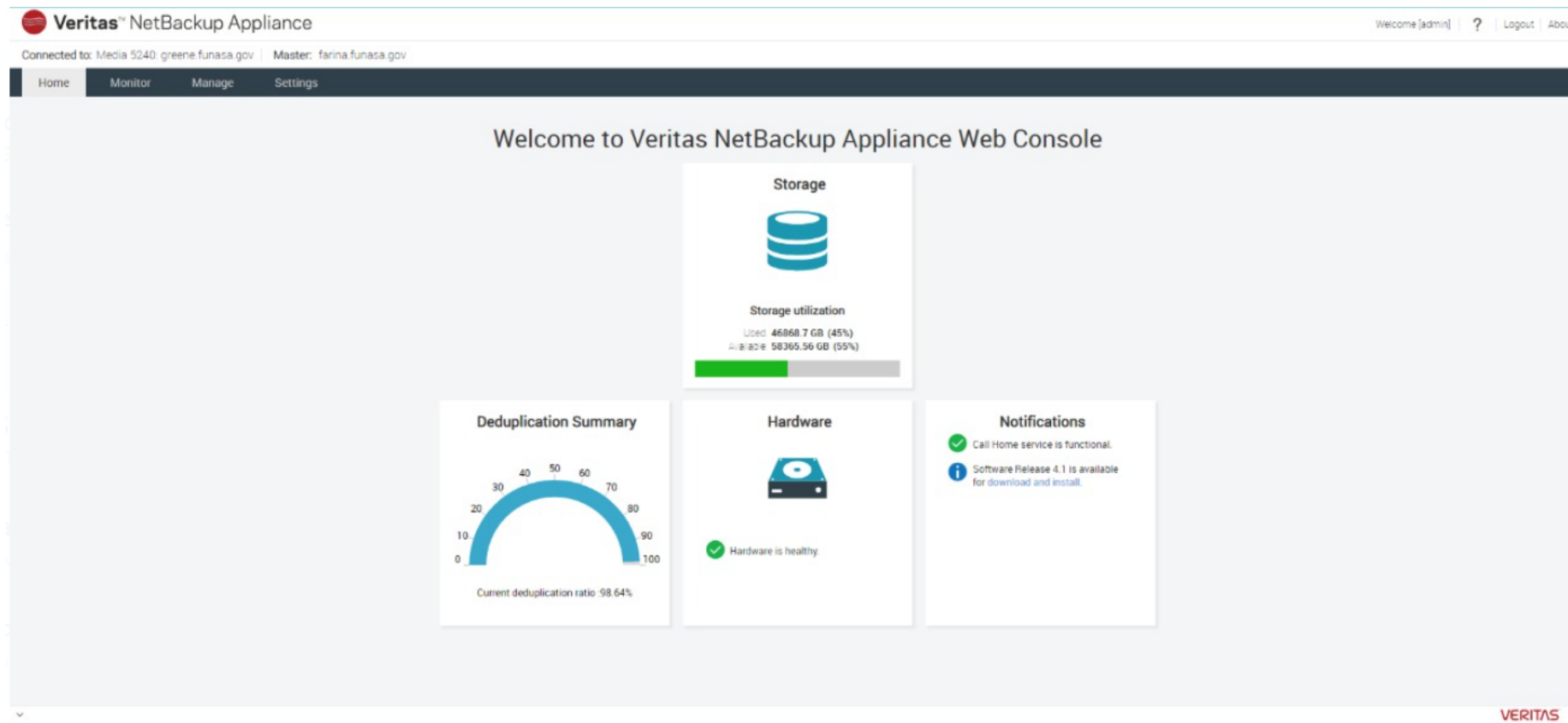
5.1.1.3. Deve ser levado em consideração, também, que a solução atual é avaliada (inclusive pelo Instituto Gartner) como uma das melhores do mundo, e possui funcionalidades que não são encontradas em vários outros produtos no mercado. Uma eventual troca de plataforma deve considerar esse aspecto, para evitar o risco de substituição por uma solução de qualidade inferior, que eventualmente possa não possuir os requisitos técnicos necessários para atender às necessidades de ambiente de produção da Funasa.

5.1.2. Cenário 2 - Item 1 - Contratação de nova solução de mercado

5.1.2.1. Tecnicamente, pensando no cenário 2, seria necessário substituir todos os equipamentos existentes, bem como configurar todos os agentes na Presidência e em todas as Suest's. Seria necessário, também, realizar o treinamento de toda a equipe técnica e realizar diversas paradas no ambiente de produção para realizar o ajuste da nova solução. Além disso o ambiente na Funasa, de backup tem a utilização 46TB de dados no appliance físico, como apresentado na figura do relatório retirado do próprio appliance, abaixo. No caso de se migrar para uma outra solução de backup será necessários um storage, para armazenamento de transição, com uma volumetria em volume de peta bytes, para armazenamento total dos dados, pois todos esses dados são desduplicados dentro da solução.

5.1.2.2. A deduplicação reduz o volume de dados armazenados com a remoção de cópias redundantes. Ela substitui os dados originais por um indicador, agora armazenado uma vez, que fica em seu lugar.

5.1.2.3. A deduplicação tem o potencial para diminuir os requisitos de capacidade em disco e largura de banda em até 98%.



5.1.2.4. A necessidade de um Storage, com cerca de 3.2PiB, como pode ser comprovado na próxima figura abaixo da console do appliance, se faz necessária, pois não existe migração de backup entre fabricantes diferentes, consequentemente, a Funasa teria que restaurar todos os backups existentes para uma área de armazenamento de transição, um Storage ou mesmo espaço em nuvem e em seguida refazer todos os backups, o que além do impacto financeiro de se ter essa área de armazenamento de transição, gera vários riscos nesse processo, por exemplo:

1. Não basta ter volume de Storage disponível para restauração dos dados, a Funasa terá que disponibilizar uma infraestrutura de hardware e software de todos os ambientes protegidos, para que seja possível restaurar com garantia de consistência dos dados e em seguida que seja possível ser feito o novo backup para a nova solução.
2. Após restaurar as imagens de backup, perderíamos o histórico de retenção e começaríamos a contar do zero os prazos de retenções, ou seja, um backup que possuía expiração para 5 anos, e se passaram 2 anos, ele passaria a ter novamente mais 5 anos, consumindo mais área de armazenamento.

```
Support      NetBackup Support.

greene.Main_Menu> Reports
Entering NetBackup reporting view...

Deduplication  Show deduplication statistics.
Exit           Log out and exit from the current shell.
Process        Show current process status.
Return         Return to the previous menu.
Shell          Shell operations.

greene.Reports> Deduplication
Deduplication statistics
Deduplication technology  MSDP
Deduplication rate        98.637%
Data Protected            3244090333 MB
Space Used For Protection 44205374 MB
Physical free space       44060838 MB
Logical free space        0 MB
Total free space          44060838 MB
Maximum Disk Space        88322008 MB
Used Disk Space           44261169 MB

greene.Reports> █
```

5.1.2.5. A deduplicação do Appliance atual está chegando em 98% conforme apresentado acima, também pode ser verificado o valor de “Data Protected”, que é referente a quantidade de dados hidratados que está protegido no Appliance, ou seja, a quantidade de Storage (3.2PiB) que a Funasa precisaria disponibilizar para restaurar todos os dados que estão armazenados no Appliance.

5.1.2.6. Abaixo, observamos mais uma evidência sobre a taxa de deduplicação (Deduplication Ratio) que está em 73.5, ou seja, se dividirmos o valor do “Data Protected” pelo valor do “Used Disk Space”, chegaríamos na taxa de deduplicação. A taxa de deduplicação é referente a quantidade de dados versus a quantidade de dados efetivamente armazenado no Appliance. Em seguida com as informações apresentadas, extraídas do próprio appliance, confirmamos que seriam necessários 3.2 petabytes de Storage ou armazenamento na nuvem para efetuarmos a restaurações de todas as imagens do backup.

Change Storage Server- greene.funasa.gov		
Server name:greene.funasa.gov		Server type:PureDisk
Media Servers	Properties	Replication
Property	Value	Description
storagepath	/msdp/data/dp1/pdvol	Storage Path
spalogpath	/msdp/data/dp1/pdvol/log	Storage Pool Log Path
dbpath	/msdp/cat	Database Path
required_interface	greene.funasa.gov	Required Interface
spalogretention	7	Storage Pool Log Retention
verboselevel	3	Storage Pool Verbose Lev...
servertype	MSDP	Deduplication Server Type
replication_target(s)	none	Replication Target(s)
encryption	0	Encryption Enabled
kmsenabled	0	KMS Enabled
kmsservertime	0	KMS Type (Range 0 - 1)
fipsenabled	0	FIPS Enabled
Storage Pool Raw Size	89.6TB	Storage Pool Raw Size
Storage Pool Reserved S...	5.4TB	Storage Pool Reserved S...
Storage Pool Size	84.2TB	Storage Pool Size
Storage Pool Used Space	42.2TB	Storage Pool Used Space
Storage Pool Available Sp...	42.0TB	Storage Pool Available Sp...
Catalog Logical Size	3098.1TB	Catalog Logical Size
Catalog files Count	912069	Catalog files Count
Deduplication Ratio	73.5	Deduplication Ratio

USED DISK SPACE

Digital Storage

44261169

=

44.261169

Megabyte

Terabyte

DATA PROTECTED

Digital Storage

3244090333

=

3.244090333

Megabyte

Petabyte

5.1.3. **Cenário 3 - Item 1 - Adoção de Software Livre.**

5.1.4. Por “software livre” devemos entender aquele software que respeita a liberdade e senso de comunidade dos usuários. Grosso modo, isso significa que os usuários possuem a liberdade de executar, copiar, distribuir, estudar, mudar e melhorar o software.

5.1.5. Ao mesmo tempo que tal fato pode ser encarado de forma positiva, há que se levar em consideração que traz 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.

5.1.6. 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.

5.2. **ITEM 2 - AQUISIÇÃO / RENOVAÇÃO DE HARDWARE DE BACKUP.**

5.2.1. **Cenário 1 - Item 2 - Manter e Expandir a atual solução.**

5.2.1.1. As explicações fornecidas para o cenário 1 (Manter e Expandir a atual solução) do Item 1 (Aquisição / Renovação de software de Backup) se repetem neste item pela dependência do software atrelado ao Hardware.

5.2.2. **Cenário 2 Item 2 - Contratação de nova solução de mercado.**

5.2.2.1. As explicações fornecidas para o cenário 2 (Manter e Expandir a atual solução) do item 1 (Aquisição / Renovação de software de Backup), se repetem neste item pela dependência do software atrelado ao Hardware.

5.2.2.2. Adicionalmente há que se dizer, que, como a FUNASA já possui um appliance de Backup, levando em consideração que não é possível coexistirem equipamentos de fabricantes distintos em uma arquitetura de site principal/DR, caso esta opção seja levada em consideração, deverá ser descartado o equipamento já existente e em pleno funcionamento na FUNASA, com fornecimento de outro.

5.2.2.3. Em suma, caso esta opção seja considerada, ao invés do licitante fornecer um equipamento, deverão ser fornecidos 2 equipamentos (um para o site principal e outro para o DR). Nesse sentido, foi anexado nos autos a especificação técnica destes equipamentos, conforme documento (SEI nº 3365255), o qual também foi anexado aos pedidos de cotações enviados aos fornecedores do cenário 2 (SEI nº 3324812), visto que os equipamentos deverão possuir características condizentes com a infraestrutura e atender a necessidade de segurança e performance do ambiente da Funasa.

5.2.3. **Cenário 3 - Item 2 - Adoção de Software Livre.**

5.2.3.1. Este cenário não se aplica a este Item.

5.3. **ITEM 3 - AQUISIÇÃO DE SOLUÇÃO PARA BACKUP DE OFFICE365**

5.3.1. **Cenário 1 - Item 3 - Manter e Expandir a atual solução.**

5.3.1.1. Para este item, não há como se levar em consideração a manutenção ou expansão da solução atual pois ela não existe.

5.3.2. Cenário 2 - Item 3 - Contratação de nova solução de mercado.

5.3.2.1. Assim como citado no item 4 que versa sobre a ANÁLISE DE SOLUÇÕES E CENÁRIOS, alguns fabricantes de mercado possuem solução para atender tal necessidade.

5.3.2.2. Contudo, há que se levar em consideração, por se tratar de solução de seguranças, que as premissas e boas práticas fundamentais neste sentido não podem ser deixadas de lado.

5.3.2.3. Ainda nesse sentido, também se torna fundamental enfatizar a necessidade de uma infraestrutura de nuvem atrelada ao objeto da contratação de forma segura e padronizada.

5.3.3. Cenário 3 - Item 3 - Adoção de Software Livre

5.3.3.1. Este cenário não se aplica a este Item.

5.4. ITEM 4 – SERVIÇO TÉCNICO ESPECIALIZADO.**5.4.1. Cenário 1 - Serviço técnico especializado na solução adquirida**

5.4.1.1. A CONTRATADA deve realizar o backup dos arquivos de configurações e logs da solução de proteção de dados (Backup) licitado pela CONTRATANTE através de ferramenta dedicada para esta finalidade, não sendo permitida a utilização de soluções em software livre;

5.4.1.2. A CONTRATADA deve garantir que os dados de configurações e logs da solução VERITAS NETBACKUP sejam inalteráveis e íntegros por meio de rotinas de teste de integridade;

5.4.1.3. Deve possuir uma área segregada do acesso externo para armazenar os dados “backupeados”;

5.4.1.4. A CONTRATADA deve garantir a integridade dos arquivos de backup das configurações e logs da solução VERITAS NETBACKUP através de hash MD5 ou SHA256;

5.4.1.5. Deve definir horário de execução dos backups dos arquivos de configuração e logs da solução de proteção de dados (Veritas NetBackup);

5.4.1.6. Deve ser capaz de receber syslog e SNMP traps da solução VERITAS NETBACKUP;

5.4.1.7. Permitir a visualização dos trabalhos de backup das configurações em andamento e permitir a interrupção dos mesmos se necessário;

5.4.1.8. A operação assistida deverá ser prestada para toda a solução adquirida e deverá ser acionado em caso de qualquer indisponibilidade da solução, podendo ser entregue de forma remota ou presencial, conforme os índices de severidade abaixo:

5.4.1.8.1 **Severidade 1 (Alta):** Sistema parado ou produto inoperante com impacto nas operações críticas de negócio. Exemplos: Servidor de produção ou outro sistema inicial está inativo. Parte substancial dos dados essenciais corre risco de perda ou corrupção. Operações relacionadas ao negócio foram afetadas, falha que compromete a integridade geral do sistema ou dos dados.

5.4.1.8.1.1 Prazo Máximo de Atendimento: Em até 2 horas um Engenheiro de Suporte do fabricante deve iniciar o atendimento no mínimo por telefone. O representante técnico especialista do suporte deve estar disponível 24x7 e ser automaticamente no ficado na abertura do caso.

5.4.1.8.2 **Severidade 2 (Média/Alta):** Alto impacto no ambiente de produção ou grande restrição de funcionalidade. Exemplo: Ocorreu um problema no qual um recurso importante foi gravemente danificado. As operações podem continuar de forma limitada, embora a produtividade em longo prazo possa ser afetada negativamente.

5.4.1.8.2.1 Prazo Máximo de Atendimento: Em até 4 horas um Engenheiro de Suporte do fabricante deve iniciar o atendimento no mínimo por telefone ou retorno de chamada. O Representante técnico especialista do suporte deve estar disponível 24x7 e ser automaticamente no ficado na abertura do caso.

5.4.1.8.3 **Severidade 3** (Média/Baixa): O defeito não gera impacto ao negócio. Exemplo: Ocorreu um erro que causou impacto negativo limitado nas operações.

5.4.1.8.3.1 Prazo Máximo de Atendimento: Em até 6 horas um Engenheiro de Suporte do fabricante deve iniciar o atendimento no mínimo por telefone ou retorno de chamada. O Representante técnico especialista do suporte deve estar disponível 24x7 e ser automaticamente notificado na abertura do caso.

5.4.1.9. **Severidade 4** (Baixa): O problema é pequeno, ou de documentação. Exemplos: O problema não afetou as operações da contratante; Encaminhamento de solicitações e ou sugestões para novos recursos ou aprimoramento do software licenciado.

5.4.1.9.0.2 Prazo Máximo de Atendimento: Em até 24 horas um Engenheiro de Suporte do fabricante deve iniciar o atendimento no mínimo por telefone ou retorno de chamada. O Representante técnico especialista do suporte deve estar disponível 24x7 e ser automaticamente notificado na abertura do caso.

5.4.1.10. O atendimento pelo fabricante deve estar disponível para todos os componentes da solução ofertada;

5.4.1.11. O fabricante deverá disponibilizar um recurso humano, que atuará como ponto único de contato, para fornecer assistência avançada em horário comercial através de telefone fixo, telefone móvel e e-mail. Caso este recurso humano esteja temporariamente indisponível, deve ser dada a opção de deixar uma mensagem ou ser redirecionado para um engenheiro de suporte de nível avançado;

5.4.1.12. A cada chamado de suporte categorizado como grau de severidade 1, o recurso previsto no item anterior, deverá ser notificado e iniciará o auxílio na condução do processo internamente junto ao fabricante;

5.4.1.13. O recurso humano designado pelo fabricante deverá manter o cliente informado sobre melhores práticas e roadmap das soluções ofertadas;

5.4.1.14. Estes serviços poderão ser prestados na modalidade remota, utilizando-se de ferramentas de acesso remoto através da Internet e permitida pelo Órgão (tal como Microsoft Teams), com total segurança e criptografia de dados, de forma que os recursos técnicos consigam acessar remotamente os servidores e dispositivos de rede para rápida resolução de problemas;

5.4.1.15. Possuir atendimento com consultores na língua portuguesa;

5.4.1.16. Assessorar e contribuir em projetos técnicos;

5.4.1.17. Participar do planejamento e execução de todas as atualizações, implantações, patches ou testes de recuperação de desastre;

5.4.1.18. Realizar revisões da configuração e do ambiente;

5.4.1.19. Auxiliar no planejamento de produção para minimizar os riscos no ambiente operacional e nos produtos escopo deste fornecimento;

5.4.1.20. Auxiliar no planejamento e gestão técnica das iniciativas proativas;

5.4.1.21. Auxiliar no planejamento e suporte de avaliações das novas características e funcionalidades dos produtos escopo deste fornecimento;

5.4.1.22. Fornecer detalhes técnicos e participar ativamente do processo de planejamento das contas e nas revisões de negócios para avaliar o estado do programa e na orientação estratégica em relação aos objetivos de negócio do Cliente;

5.4.1.23. Diagnosticar problemas técnicos encontrados nos produtos escopo deste fornecimento;

5.4.1.24. Monitorar e gerenciar questões de escalada e servir como ponto único de contato técnico;

5.4.1.25. Fornecer monitoramento e resposta a incidentes durante as atividades não rotineiras;

5.4.1.26. Auxiliar na identificação de processos para ajudar o cliente a assegurar que o produto(s) escopo deste fornecimento instalado(s), ou a ser instalado(s), está instalado de uma maneira compatível com os requerimentos dos ambientes/configurações do produto(s);

- 5.4.1.27. Prestar assessoria proativa e reativa nas questões relativas às atualizações, patches e alertas de impacto;
- 5.4.1.28. Dar resposta ou esclarecimento de dúvidas relacionadas com os produtos escopo deste fornecimento relevante no decorrer das operações diárias;
- 5.4.1.29. Coordenar com o suporte técnico do fornecedor para a resolução de escalões de problema do produto para auxiliar na resolução mais rápida e reduzir o tempo de inatividade não planejado;
- 5.4.1.30. Auxiliar na solução de problemas fornecendo detalhes técnicos para a análise de causa provável de problemas encontrados;
- 5.4.1.31. Acionar equipe de especialistas técnicos remotos da fabricante para o atendimento dependendo da necessidade específica do cliente;
- 5.4.1.32. Apresentar um relatório demonstrando a saúde do ambiente dos produtos escopo deste fornecimento;
- 5.4.1.33. Propor melhorias no ambiente;
- 5.4.1.34. Atuar junto ao Suporte do fabricante na escalada de problemas críticos e acompanhamento do problema até a resolução
- 5.4.1.35. Entregar relatórios mensais com status e descritivo detalhado das atividades realizadas no cliente, evidenciando a efetividade dos serviços prestados pelo fornecedor.
- 5.4.1.36. Deve possibilitar a abertura de chamados de suporte, para no mínimo, os seguintes métodos via telefone, e-mail, "website" do fabricante;
- 5.4.1.37. Todos os prazos para atendimento da garantia começarão a ser contados a partir da abertura do chamado independentemente deste ter sido feito via telefone, e-mail, Website do fabricante;
- 5.4.1.38. O período de suporte deve estar diretamente atrelado ao período de garantia da solução;
- 5.4.1.39. Dentro do prazo máximo de solução está compreendido o prazo de atendimento;
- 5.4.1.40. Dentro do prazo máximo de atendimento, cabe ao fornecedor dar início, junto ao CONTRATANTE, às providências que serão adotadas para a solução do chamado;
- 5.4.1.41. Considera-se plenamente solucionado o problema quando estabelecidos os sistemas/serviços sem restrições, ou seja, quando não se tratar de uma solução paliativa;
- 5.4.1.42. Os serviços de atendimento de garantia para chamados de severidades 1 e 2 não podem ser interrompidos até o completo restabelecimento de todas as funções do sistema paralisado (indisponível), mesmo que para isso tenham que se estender por períodos noturnos e dias não úteis (sábados, domingos e feriados);
- 5.4.1.43. O fabricante emitirá relatório sempre que solicitado pelo CONTRATANTE, em papel e em arquivo eletrônico, preferencialmente em arquivo texto, com informações analíticas e sintéticas dos chamados da garantia abertos e fechados no período, incluindo:
 - 5.4.1.43.1 Quantidade de ocorrências (chamados) registradas no período;
 - 5.4.1.43.2 Número do chamado registrado e nível de severidade, inclusive aqueles com reabertura;
 - 5.4.1.43.3 Data e hora de abertura;
 - 5.4.1.43.4 Data e hora de início e conclusão do atendimento;
 - 5.4.1.43.5 Identificação do técnico do CONTRATANTE que registrou o chamado;
 - 5.4.1.43.6 Identificação do técnico do CONTRATANTE que atendeu ao chamado da garantia;
 - 5.4.1.43.7 Descrição do problema;
 - 5.4.1.43.8 Descrição da solução;
 - 5.4.1.43.9 Informações sobre eventuais escalões;
 - 5.4.1.43.10 Resumo com a lista de chamados concluídos fora do prazo de solução estabelecido;

5.4.1.43.11 Total de chamados no mês e o total acumulado até a apresentação do relatório.

5.4.1.44. Não se encaixam nos prazos descritos nos itens referentes aos problemas cuja solução dependa de correção de falhas (bugs) ou da liberação de novas versões e patches de correção, desde que comprovados pelo fabricante da solução;

5.4.1.45. Para esses problemas, o fornecedor deverá nos prazos estabelecidos nos níveis de criticidade, restabelecer o ambiente, através de uma solução paliativa e informar ao CONTRATANTE;

5.4.1.46. Nos casos em que as manutenções necessitem de paradas da solução, o CONTRATANTE deverá ser imediatamente notificado para que se proceda a aprovação da manutenção, ou para que seja agendada nova data, a ser definida pelo CONTRATANTE, para execução das atividades de manutenção;

5.4.1.47. O proponente deve emitir relatórios de todas as intervenções realizadas, preventivas e corretivas, programadas ou de emergência, ressaltando os fatos importantes e detalhando os pormenores das intervenções, de forma a manter registros completos das ocorrências e subsidiar as decisões da administração do Complexo Central de Tecnologia do CONTRATANTE, caso requeiram;

5.4.1.48. O relatório deve ser assinado por representante do CONTRATANTE, responsável pelo acompanhamento do serviço, que se obriga a acompanhar a execução das manutenções;

5.4.1.49. Durante o período de garantia, o fornecedor executará, sem ônus adicionais, correções de falhas (bugs) de software;

5.4.1.50. Durante o período de garantia o CONTRATANTE terá direito, sem ônus adicional, a todas as atualizações de versão e releases dos softwares e firmwares que fazem parte da solução ofertada.

5.4.1.51. Deverá ser disponibilizado canal de atendimento e chamado técnico 24 (vinte e quatro) horas por dia, 7 (sete) dias por semana através de site na Internet e/ou canal telefônico gratuito 0800;

5.4.1.52. Em caso de indisponibilidade do canal de atendimento disponibilizado, os chamados técnicos poderão ser abertos via e-mail, "website" do fabricante, telefone, etc.;

5.4.1.53. O fornecedor deve informar página da Internet onde estejam disponíveis drivers atualizados, últimas versões do firmware e demais informações sobre detalhes técnicos dos equipamentos, sem restrições de acesso público ou via cadastramento de pessoas autorizadas pelo CONTRATANTE para o acesso.

5.5. **Cenário 2 - serviço técnico especializado em uma nova solução.**

5.5.1. O suporte técnico em uma nova solução de mercado deve seguir os mesmos requisitos citados no Suporte técnico na solução adquirida, levando em consideração uma similaridade do serviço com o fabricante em questão.

5.6. **ITEM 5 - REPASSE DE CONHECIMENTO**

5.7. **Cenário 1 - Repasse de conhecimento na solução já existente.**

5.7.1. Por se tratar de uma solução já existente no ambiente da FUNASA, não há que se falar sobre repasse de conhecimento por esta casa já possuir domínio na solução.

5.8. **Cenário 2 - Repasse de conhecimento em uma nova solução**

5.8.1. O treinamento será composto pelos módulos distintos que compõem o item, que deve consistir na oferta de cursos presenciais ou remotos, e com abordagem prática voltada a todos os requisitos funcionais da solução.

5.8.2. Caso a FUNASA opte por treinamento presencial, ele deverá ser ministrado em Brasília/DF.

5.8.3. O treinamento deverá abordar de forma teórica e prática todas as funcionalidades solicitadas para cada um dos itens, com o objetivo de formar multiplicadores e profissionais capacitados na utilização das funcionalidades.

- 5.8.4. O treinamento deverá ser realizado utilizando-se solução idêntica à adquirida pela FUNASA, inclusive quanto à versão dos sistemas;
- 5.8.5. A empresa vencedora será responsável pelos custos de elaboração, produção, impressão, fornecimento de ambiente virtual, e fornecimento de todo o material e logística necessários, bem como pela infraestrutura e pelo transporte, acomodação, hospedagem, impostos, taxas, tributos, alimentação, diárias e passagens de seus colaboradores/instrutores para cumprimento das atividades necessárias à execução do treinamento e capacitação.
- 5.8.6. A carga horária mínima exigida para este treinamento é de 32 horas para cada Item.
- 5.8.7. A atividade de treinamento e capacitação deverá ser realizada em dias úteis, com duração máxima de até 6 (seis) horas de instrução diária.
- 5.8.8. Deverá ser ministrada uma turma de treinamento que terá até 08 participantes.
- 5.8.9. Deverá ser fornecido material em formato digital ou impresso do conteúdo do treinamento.
- 5.8.10. Concluídas as atividades de treinamento, a empresa contratada fornecerá a cada participante que obteve, no mínimo, 80% de presença, um certificado de conclusão que contenha, expressamente, o nome da instituição organizadora, a carga horária do treinamento, o local, o período de realização e o nome completo do participante.
- 5.8.11. O(s) instrutor(es) deverá(ão) ser comprovadamente certificado(s) nos sistemas e/ou ferramentas fornecidos no escopo da solução.
- 5.8.12. As datas para a realização das atividades de treinamento e capacitação serão definidas previamente pela FUNASA, respeitados os prazos de vigência do Contrato.
- 5.8.13. O público alvo deste treinamento são os analistas responsáveis pela execução de atividades de administração e auditoria dos ambientes monitorados pela solução. Os participantes serão indicados pelo MEC.

6. ANÁLISE COMPARATIVA DE CUSTOS (TCO)

6.1. Premissas utilizadas:

- 6.1.1. A pesquisa de mercado foi realizada 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.
- 6.1.2. Todos os procedimentos adotados na pesquisa mercadológica para contratação de solução de proteção de dados (Backup) composto por hardware, licenciamento de software, configuração e garantia da solução por 36 meses, incluindo suporte e manutenção com substituição de peças em regime 24x7, considerando os cenários 01 e 02 analisados neste Estudo Técnico Preliminar, estão detalhados na Nota Técnica (SEI 3335507).

6.2. FORMA DE CONSTRUÇÃO DO TCO PARA CADA UM DOS ITENS.

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

SOLUÇÃO	DESCRIÇÃO	CENÁRIOS
Item 1	Aquisição / Renovação de software de Backup	Cenário 1 - Renovação das licenças perpetuas já existentes
		Cenário 2 - Expansão das licenças do mesmo fabricante
		Cenário 3 - Contratação de um novo do software de backup levando em consideração o ambiente da FUNASA, com suporte técnico por 36 meses e transferência de conhecimento.
Item 2	Aquisição / Renovação de Hardware de Backup	Cenário 1 - Renovação do suporte e garantia do appliance já existentes do fabricante atual para o site principal
		Cenário 2 - Aquisição de appliance, suporte e garantia do fabricante atual para o site DR
		Cenário 3 - Aquisição de 2 novos Hardwares (site principal e DR) de outros fabricantes, com

		suporte técnico por 36 meses e transferência de conhecimento.
Item 3	Aquisição de Solução para Backup de Office365	Cenário 1 - Aquisição de software de Backup Office365 do mesmo fabricante do Backup OnPremisse, com serviço especializado por 12 meses e repasse de conhecimento.
		Cenário 2 - Contratação de software de backup para o Office 365 de outro fabricante
Item 4	Serviço Especializado	Cenário 1 – Serviço Especializado para a solução já existente - Item 1
		Cenário 2 - Serviço Especializado para a solução já existente - Item 2
		Cenário 3 - Serviço Especializado para uma nova solução - Item 1
		Cenário 4 - Serviço Especializado para uma nova solução - Item 2
Item 5	Repasse de conhecimento	Cenário 1 - Repasse de conhecimento na solução Backup Office365 do mesmo fabricante do Backup OnPremisse - Item 3

Tabela 07 - Forma de construção do TCO para cada um dos itens.

6.3. CÁLCULO DOS CUSTOS TOTAIS DE PROPRIEDADE – MEMÓRIA DE CÁLCULO

6.3.1. Para realização deste TCO, realizou-se pesquisa de preço de aquisições e contratações similares de outros entes públicos e pesquisa direta com fornecedores. O detalhamento destes procedimentos constam na Nota Técnica (SEI 3327283).

6.3.2. Para a definição do resultado da pesquisa dos preços coletados, **considerou-se tão somente os valores aceitáveis**, utilizando-se das metodologias previstas na IN SEGES/ME nº 65/2021.

6.3.3. TCO ITEM 01 – Aquisição / Renovação de software de Backup

6.3.4. Todos os procedimentos adotados na pesquisa mercadológica para contratação de solução de proteção de dados (Backup), considerando os cenários analisados neste Estudo Técnico Preliminar, estão detalhados na Nota Técnica (SEI 3335507).

6.3.4.1. CENÁRIO 01 Item 1 – Renovação das licenças perpétuas já existentes

Descrição	Parâmetro	Fonte de consulta	Valor Unitário	Média
Renovação de software de Backup	II	MDR PE 20/2020	R\$ 25.305,00	R\$ 26.375,74
	IV	FORNECEDOR 03	R\$ 26.762,15	
	IV	FORNECEDOR 04	R\$ 25.435,80	
	IV	FORNECEDOR 05	R\$ 28.000,00	

Tabela 08 - Média dos preços aceitáveis para o item "Renovação de software de Backup".

6.3.4.2. Os valores acima já contemplam suporte técnico por 36 meses.

6.3.4.3. CENÁRIO 02 Item 1 - Expansão das licenças do mesmo fabricante

Descrição	Parâmetro	Fonte de consulta	Valor Unitário	Média
-----------	-----------	-------------------	----------------	-------

Expansão de software de Backup	II	MDR PE 20/2020	R\$ 53.905,00	R\$ 53.084,29
	II	TJRO PE 75/2021	R\$ 56.600,00	
	IV	FORNECEDOR 03	R\$ 50.002,16	
	IV	FORNECEDOR 05	R\$ 51.830,00	

Tabela 09 - Média dos preços aceitáveis para o item "Expansão de software de Backup".

6.3.4.4. Os valores acima já contemplam suporte técnico por 36 meses.

6.3.4.5. **CENÁRIO 03 Item 1 – Contratação de um novo do software de backup levando em consideração o ambiente da FUNASA.**

Descrição	Parâmetro	Fonte de consulta	Valor Unitário	Média
Aquisição de software de Backup (<i>Licenciamento por TB</i>)	IV	FORNECEDOR 01	R\$ 44.137,76	R\$ 44.137,76
Aquisição de software de Backup (<i>Licenciamento por VM</i>)	IV	FORNECEDOR 06	R\$ 8.000,00	R\$ 8.000,00

Tabela 10 - Média dos preços aceitáveis para o item "Aquisição de software de Backup".

6.3.4.6. Os valores acima não contemplam suporte técnico por 36 meses, além de não contemplar os serviços de "Transferência de Conhecimento" na nova solução, desse modo foi realizada cotação junto aos fornecedores para obtenção da estimativa destes custos, portanto para efeitos de comparação é necessário realizar a soma do item "Aquisição de software de Backup" com o serviço "Suporte Técnico" e "Transferência de Conhecimento" discriminados nas tabelas abaixo.

Descrição	Parâmetro	Fonte de consulta	Valor Unitário	Média
Suporte Técnico (36 meses)	IV	FORNECEDOR 02	R\$ 34.000,00	R\$ 33.666,67
	IV	FORNECEDOR 06	R\$ 31.000,00	
	IV	FORNECEDOR 07	R\$ 36.000,00	

Tabela 11 - Média dos preços aceitáveis para o serviço "Suporte Técnico" para o item 1.

Descrição	Parâmetro	Fonte de consulta	Valor Unitário	Média
Transferência de conhecimento	IV	FORNECEDOR 02	R\$ 16.000,00	R\$ 16.100,00
	IV	FORNECEDOR 07	R\$ 16.200,00	

Tabela 12 - Média dos preços aceitáveis para o serviço "Transferência de conhecimento" para o item 1.

6.3.5. **Mapa comparativo dos cálculos totais de propriedade (TCO) entre os cenários do item 1**

Descrição	Cenários	Média de valores
-----------	----------	------------------

Aquisição / Renovação de software de Backup	Cenário 1 - Renovação das licenças perpetuas já existentes	R\$ 26.375,74
	Cenário 2 - Expansão das licenças do mesmo fabricante	R\$ 53.084,29
	Cenário 3 - Contratação de um novo do software de backup levando em consideração o ambiente da FUNASA.	R\$ 93.904,43 *
		R\$ 57.766,67 *

Tabela 13 - Comparativo dos cálculos totais de propriedade (TCO) entre os cenários do item 1.

* A métrica para o item 1 da solução 2 pode ser Terabyte (TB) ou Máquina Virtual, a depender do fabricante, como foram obtidas cotações para ambos os licenciamentos, foi calculada a média do item 1 tanto para a métrica Terabyte, como para Máquina Virtual.

6.3.5.1. Para uma comparação eficiente, se faz necessário realizar a soma do cenário 1 com o cenário 2 a fim de se obter a quantidade de 70TB pleiteado nesta contratação, obtendo-se os seguintes valores:

Descrição	Cenários	Média de valores
Aquisição / Renovação de software de Backup	Cenário 1 + Cenário 2	R\$ 79.460,03
	Cenário 3 - Contratação de um novo do software de backup levando em consideração o ambiente da FUNASA.	R\$ 93.904,43 (TB)
		R\$ 57.766,67 VM)

Tabela 14 - Comparativo do TCO entre os cenários do item 1 - Consolidado.

6.3.5.2. Analisando-se os custos entre os cenários acima, apresentou-se como a solução mais econômica a Solução do cenário 3, com licenciamento do item 1 por máquina virtual.

6.3.6. TCO ITEM 02 – Aquisição / Renovação de hardware de Backup

6.3.7. Para a definição dos custos, **considerou-se tão somente os valores aceitáveis**, utilizando-se das metodologias previstas na IN SEGES/ME nº 65/2021, conforme detalhado na Nota Técnica (SEI 3335507).

6.3.7.1. CENÁRIO 01 Item 2 - Renovação do suporte e garantia do appliance já existente do fabricante atual para o site principal

Descrição	Parâmetro	Fonte de consulta	Valor Unitário	Média
Renovação de Garantia de Hardware de Backup	II	TJRO PE 75/2021	R\$ 252.000,00	R\$ 256.360,04
	IV	FORNECEDOR 03	R\$ 267.481,23	
	IV	FORNECEDOR 04	R\$ 249.598,89	

Tabela 15 - Média dos preços aceitáveis para o item "Renovação de Garantia de Hardware de Backup".

6.3.7.2. Os valores acima já contemplam suporte técnico por 36 meses.

6.3.7.3. **CENÁRIO 2 Item 2 - Aquisição de appliance, suporte e garantia do fabricante atual para o site DR.**

Descrição	Parâmetro	Fonte de consulta	Valor Unitário	Média
Expansão de Hardware de Backup	II	TJRO PE 75/2021	R\$ 967.400,00	R\$ 1.191.067,33
	IV	FORNECEDOR 03	R\$ 1.302.571,00	
	IV	FORNECEDOR 04	R\$ 1.297.458,33	
	IV	FORNECEDOR 05	R\$ 1.196.840,00	

Tabela 16 - Média dos preços aceitáveis para o item "Expansão de Hardware de Backup".

6.3.7.4. Os valores acima já contemplam suporte técnico por 36 meses.

6.3.7.5. **CENÁRIO 3 Item 2 - Aquisição de 2 novos Hardwares (site principal e DR) de outros fabricantes**

Descrição	Parâmetro	Fonte de consulta	Valor Unitário	Média
Aquisição de Hardware de Backup	IV	FORNECEDOR 01	R\$ 1.896.653,23	R\$ 1.798.326,62
	IV	FORNECEDOR 06	R\$ 1.700.000,00	

Tabela 17 - Média dos preços aceitáveis para o item "Aquisição de Hardware de Backup".

6.3.7.6. Os valores acima não contemplam suporte técnico por 36 meses, além de não contemplar os serviços de "Transferência de Conhecimento" na nova solução, desse modo foi solicitado orçamento junto aos fornecedores para obtenção da estimativa destes custos, portanto para efeitos de comparação é necessário realizar a soma do item "Aquisição de Hardware de Backup" com o serviço "Suporte Técnico" e "Transferência de Conhecimento" discriminados nas tabelas abaixo.

Descrição	Parâmetro	Fonte de consulta	Valor Unitário	Média
Suporte Técnico (36 meses)	IV	FORNECEDOR 02	R\$ 26.800,00	R\$ 25.900,00
	IV	FORNECEDOR 06	R\$ 25.000,00	

Tabela 18 - Média dos preços aceitáveis para o serviço "Suporte Técnico" para o item 2.

Descrição	Parâmetro	Fonte de consulta	Valor Unitário	Média
Transferência de conhecimento	IV	FORNECEDOR 01	R\$ 15.000,00	R\$ 14.000,00
	IV	FORNECEDOR 02	R\$ 13.000,00	

Tabela 19 - Média dos preços aceitáveis para o serviço "Transferência de conhecimento" para o item 2.

6.3.7.7. É importante salientar que se faz necessário a aquisição de hardware de Storage para servir de repositório de Backup, visto que, atualmente, a Funasa não possui Storage ou servidor de rede para servir de armazenamento.

6.3.7.8. É importante pontuar que as soluções de repositório de backup são ambientes mais seguros que servidores de redes ou Storage tradicionais. Visto que estes hardwares específicos - que servem para guardar dados, possuem diversas funcionalidades de segurança, por exemplo: sistema de firewall interno para controle de acesso, proteção contra ataques de ransowares, criptografia de disco, tanto para o dado em repouso quanto para o dado em trânsito, entre outros.

6.3.8. Mapa comparativo dos cálculos totais de propriedade (TCO) entre os cenários do item 2

Descrição	Cenários	Média de valores
Aquisição / Renovação de Hardware de Backup	Cenário 1 - Renovação do suporte e garantia do appliance já existentes do fabricante atual para o site principal	R\$ 256.360,04
	Cenário 2 - Aquisição de appliance, suporte e garantia do fabricante atual para o site DR	R\$ 1.191.067,33
	Cenário 3 - Aquisição de 2 novos Hardwares (site principal e DR) de outros fabricantes	R\$ 1.838.226,62

Tabela 20 - Comparativo dos cálculos totais de propriedade (TCO) entre os cenários do item 2.

6.3.8.1. Para uma comparação eficiente, se faz necessário realizar a soma do cenário 1 com o cenário 2 a fim de se obter a quantidade de 2 appliances (site principal e DR) pleiteado nesta contratação, obtendo-se os seguintes valores:

Descrição	Cenários	Média de valores
Aquisição / Renovação de Hardware de Backup	Cenário 1 + Cenário 2	R\$ 1.447.427,37
	Cenário 3 - Aquisição de 2 novos Hardwares (site principal e DR) de outros fabricantes	R\$ 1.838.226,62

Tabela 21 - Comparativo do TCO entre os cenários do item 2 - Consolidado.

6.3.8.2. Analisando-se os custos entre os cenários acima, apresentou-se como a solução mais econômica a Solução dos cenários 1 + 2.

6.3.9. TCO ITEM 03 – Aquisição de Solução para Backup de Office365

6.3.9.1. Para a definição dos custos, **considerou-se tão somente os valores aceitáveis**, utilizando-se das metodologias previstas na IN SEGES/ME nº 65/2021, conforme detalhado na Nota Técnica (SEI 3335507).

6.3.9.2. CENÁRIO 1 Item 3 - Aquisição de software de Backup Office365 do mesmo fabricante do Backup OnPremisse

Descrição	Parâmetro	Fonte de consulta	Valor Unitário	Média
Aquisição de Solução para Backup de Office365	II	TCU PE 56/2020	R\$ 371,11	R\$ 462,09
	IV	FORNECEDOR 03	R\$ 492,13	
	IV	FORNECEDOR 04	R\$ 481,11	
	IV	FORNECEDOR 05	R\$ 504,00	

Tabela 22 - Média dos preços aceitáveis para o item "Aquisição de Solução para Backup de Office365".

6.3.9.3. Para efeitos de comparação é necessário realizar a soma do item "Aquisição de Solução para Backup de Office365" com o item "Serviço Especializado" e "Transferência de Conhecimento" discriminados nas tabelas abaixo.

Descrição	Parâmetro	Fonte de consulta	Valor Unitário	Média
Serviço Especializado (12 meses)	IV	FORNECEDOR 05	R\$ 10.700,00	R\$ 10.700,00

Tabela 23 - Média dos preços aceitáveis para o item "Serviço Especializado" para o item 3.

Descrição	Parâmetro	Fonte de consulta	Valor Unitário	Média
Repasse de conhecimento	IV	FORNECEDOR 04	R\$ 80.699,98	R\$ 80.699,98

Tabela 24 - Média dos preços aceitáveis para o serviço "Repasse de conhecimento" para o item 3.

6.3.9.4. CENÁRIO 02 Item 3 - Contratação de software de backup para o Office 365 de outro fabricante

Descrição	Parâmetro	Fonte de consulta	Valor Unitário	Média
Aquisição de Solução para Backup de Office365	IV	FORNECEDOR 06	R\$ 600,00	R\$ 627,50
	IV	FORNECEDOR 07	R\$ 655,00	

Tabela 25 - Média dos preços aceitáveis para o item "Aquisição de Solução para Backup de Office365".

6.3.10. Mapa comparativo dos cálculos totais de propriedade (TCO) entre os cenários do item 3

Descrição	Cenários	Média de valores
Aquisição de Solução para Backup de Office365	Cenário 1 - Aquisição de software de Backup Office365 do mesmo fabricante do Backup OnPremisse	R\$ 91.862,07
	Cenário 2 - Contratação de software de backup para o Office 365 de outro fabricante	R\$ 627,50

Tabela 26 - Comparativo dos cálculos totais de propriedade (TCO) entre os cenários do item 3.

6.3.10.1. Analisando-se os custos entre os cenários acima, apresentou-se como a solução mais econômica a Solução do cenário 2,

6.3.10.2. No entanto, é importante ressaltar que a média de valores do cenário 2 contempla apenas o fornecimento de licenças. O custo da infraestrutura necessária para execução do backup na nuvem será de responsabilidade da Funasa. Desconhecemos a infraestrutura necessária na nuvem e não temos como qualificar e dimensionar os custos da infraestrutura na nuvem.

6.3.11. **TCO ITEM 04 – Serviço Especializado**

6.3.11.1. Para a definição dos custos, **considerou-se tão somente os valores aceitáveis**, utilizando-se das metodologias previstas na IN SEGES/ME nº 65/2021, conforme detalhado na Nota Técnica (SEI 3335507).

6.3.11.2. **Cenário 1 - ITEM 04 – Serviço técnico especializado na solução já existente Item 1**

Descrição	Parâmetro	Fonte de consulta	Valor Unitário	Média
Serviço Especializado (12 meses) para o item 1	IV	FORNECEDOR 04	R\$ 8.978,00	R\$ 8.978,00

Tabela 27 - Média dos preços aceitáveis para o item "Serviço Especializado" na solução já existente - Item 1.

6.3.11.3. **Cenário 2 - ITEM 04 – Serviço Especializado na solução já existente - Item 2**

Descrição	Parâmetro	Fonte de consulta	Valor Unitário	Média
Serviço Especializado (12 meses) para o item 2	IV	FORNECEDOR 03	R\$ 11.790,00	R\$ 11.245,00
	IV	FORNECEDOR 05	R\$ 10.700,00	

Tabela 28 - Média dos preços aceitáveis para o item "Serviço Especializado" na solução já existente - Item 2.

6.3.11.4. **Cenário 3 - ITEM 04 – Serviço Especializado em uma nova solução - Item 1**

Descrição	Parâmetro	Fonte de consulta	Valor Unitário	Média
Serviço Especializado (12 meses) para o item 1	IV	FORNECEDOR 02	R\$ 14.000,00	R\$ 12.000,00
	IV	FORNECEDOR 06	R\$ 10.000,00	

Tabela 29 - Média dos preços aceitáveis para o item "Serviço Especializado" em uma nova solução - Item 1.

6.3.11.5. **Cenário 4 - ITEM 04 – Serviço Especializado em uma nova solução - Item 2**

Descrição	Parâmetro	Fonte de consulta	Valor Unitário	Média
Serviço Especializado (12 meses) para o item 2	IV	FORNECEDOR 06	R\$ 10.000,00	R\$ 9.750,00
	IV	FORNECEDOR 07	R\$ 9.500,00	

Tabela 30 - Média dos preços aceitáveis para o item "Serviço Especializado" em uma nova solução - Item 2.

6.3.12. **Mapa comparativo dos cálculos totais de propriedade (TCO) entre os cenários do item 4**

Descrição	Cenários	Média de valores
Serviço de Suporte Técnico Especializado	Cenários 1 e 2 – Serviço técnico especializado na solução já existente - Itens 1 e 2	R\$ 20.223,00
	Cenários 3 e 4 – Serviço técnico especializado em uma nova solução - Itens 1 e 2	R\$ 21.750,00

Tabela 31 - Comparativo dos cálculos totais de propriedade (TCO) entre os cenários do item 4.

6.3.12.1. Analisando-se os custos entre os cenários acima, apresentou-se como a solução mais econômica a Solução dos cenários 1 e 2.

6.3.13. TCO ITEM 05 – Repasse de conhecimento

6.3.13.1. Para a definição dos custos, **considerou-se tão somente os valores aceitáveis**, utilizando-se das metodologias previstas na IN SEGES/ME nº 65/2021, conforme detalhado na Nota Técnica (SEI 3335507).

6.3.13.2. Por se tratar de uma solução já existente no ambiente da FUNASA, não há que se falar sobre repasse de conhecimento por esta casa já possuir domínio na solução (Item 1 -Aquisição / Renovação de software de Backup; e item 2 - Aquisição / Renovação de Hardware de Backup). Desta forma, para o cenário 1 (Manter e Expandir a Atual Solução) foi realizada pesquisa de preço para o serviço "Repasse de Conhecimento" apenas para o item 3 (Solução Backup Office365).

6.3.13.3. Cenário 1 - Repasse de conhecimento na solução Backup Office365 do mesmo fabricante do Backup OnPremise - Item3

6.3.13.4. Este custo refere-se ao item "Aquisição de Solução para Backup de Office365" portanto o mesmo já foi mensurado para efeitos de comparação no item 6.3.9 "TCO ITEM 3", subitem 6.3.9.3 deste ETPC.

6.3.14. Ressalte-se que os custos referentes a transferência de conhecimento em uma nova solução (itens 1 e 2) já foram mensurados para efeitos de comparação nos subitens 6.3.4.6 e 6.3.7.6 deste ETPC.

6.3.15. MAPA COMPARATIVO DOS CÁLCULOS TOTAIS DE PROPRIEDADE (TCO)

6.3.15.1. Para a definição do resultado da pesquisa dos preços coletados, considerou-se tão somente os valores aceitáveis e, utilizando-se das metodologias previstas na IN SEGES/ME nº 65/2021, estimou-se os custos dos itens com base na média dos preços considerados aceitáveis, na forma como segue:

CUSTO ESTIMADO - CENÁRIO 1				
ITEM	DESCRIÇÃO	QUANTIDADE	VALOR UNITÁRIO	VALOR TOTAL
1	Renovação de software de Backup	30	R\$ 26.375,74	R\$ 791.272,20
2	Expansão de software de Backup	40	R\$ 53.084,29	R\$ 2.123.371,60
3	Serviço Especializado	12	R\$ 8.978,00	R\$ 107.736,00
4	Renovação de Garantia de Hardware de Backup	1	R\$ 256.360,04	R\$ 256.360,04
5	Expansão de Hardware de Backup	1	R\$ 1.191.067,33	R\$ 1.191.067,33
6	Serviço Especializado	12	R\$ 11.245,00	R\$ 134.940,00

7	Aquisição de Solução para Backup de Office365	3190	R\$ 462,09	R\$ 1.474.067,10
8	Serviço Especializado	12	R\$ 10.700,00	R\$ 128.400,00
9	Repasse de conhecimento	1	R\$ 80.699,98	R\$ 80.699,98
Custo Estimado Total				R\$ 6.287.914,25

Tabela 32 - Custo Estimado Total - Cenário 1.

CUSTO ESTIMADO - CENÁRIO 2				
ITEM	DESCRIÇÃO	QUANTIDADE	VALOR UNITÁRIO	VALOR TOTAL
1	Aquisição de software de Backup (TB)	70	R\$ 44.137,76	R\$ 3.089.643,20
	Aquisição de software de Backup (VM)	214	R\$ 8.000,00	R\$ 1.712.000,00
2	Suporte Técnico	36	R\$ 33.666,67	R\$ 1.212.000,12
3	Suporte Especializado	12	R\$ 12.000,00	R\$ 144.000,00
4	Transferência de conhecimento	5	R\$ 16.100,00	R\$ 80.500,00
5	Aquisição de Hardware de Backup	2	R\$ 1.798.326,62	R\$ 3.596.653,24
6	Suporte Técnico	36	R\$ 25.900,00	R\$ 932.400,00
7	Serviço Especializado	12	R\$ 9.750,00	R\$ 117.000,00
8	Transferência de Conhecimento	5	R\$ 14.000,00	R\$ 70.000,00
9	Aquisição de Solução para Backup de Office365	3190	R\$ 627,50	R\$ 2.001.725,00
Custo Estimado Total (Com licenciamento do Item 1 por Terabyte)				R\$ 11.243.921,56
Custo Estimado Total (Com licenciamento do Item 1 por VM)				R\$ 9.866.278,36

Tabela 33 - Custo Estimado Total - Cenário 2.

COMPARATIVO	
Solução	Custo Estimativo Total da Solução
Cenário 1 (Manter e Expandir a Atual Solução).	R\$ 6.287.914,25
Cenário 2 (Contratação de Nova Solução de Mercado).	R\$ 11.243.921,56 <i>(com o licenciamento do Item 1 por Terabyte)</i>

R\$ 9.866.278,36*(com o licenciamento do Item 1 por Máquina Virtual)*

Tabela 34 - Comparativo entre as soluções dos Cenários 1 e 2.

6.3.15.2. Analisando-se os custos entre os cenários acima, **apresentou-se como a solução mais econômica a Solução do cenário 1 (Manter e Expandir a Atual Solução).**

6.3.15.3. Conforme evidenciado na tabela acima o custo estimativo total da solução do cenário 1 apresentou uma diferença de R\$ 4.956.007,31 (quatro milhões, novecentos e cinquenta e seis mil sete reais e trinta e um centavos) a menos em relação ao cenário 2 *(com o licenciamento do Item 1 por Terabyte)* e R\$ 3.578.364,11 (três milhões, quinhentos e setenta e oito mil trezentos e sessenta e quatro reais e onze centavos) a menos em relação ao cenário 2 *(com o licenciamento do Item 1 por Máquina Virtual)*.

7. DESCRIÇÃO DA SOLUÇÃO ESCOLHIDA

7.1. Justificativa do ponto de vista econômico

7.1.1. A solução 1 apresentou-se como a solução mais econômica para um horizonte de 03 (três) anos, conforme demonstrado no mapa comparativo dos Cálculos Totais de Propriedade – TCO (Item 6.3.14), contudo este não é o único prisma desta análise, razão pela qual passaremos a análise do ponto de vista técnico, conforme a seguir:

7.2. Justificativa do ponto de vista técnico

7.2.1. Inicialmente, é importante ressaltar que a solução atual utilizada na Funasa está em uso na Fundação há mais de 4 anos, em pleno funcionamento, e é componente essencial da estratégia de backup. A sua eficácia e funcionalidade estão largamente comprovadas. Há uma grande vantagem na manutenção da solução de Backup atual, seja do ponto de vista da retenção do conhecimento da solução, curva de aprendizagem ou da deduplicação dos dados com consumo excessivo de espaço em disco.

7.2.2. Considerando que no caso de uma mudança de software, se faz necessário todo o serviço de migração de dados, e que este procedimento traz grande risco a esta fundação, é importante pontuar que a equipe técnica realizou reuniões com outros fabricantes de solução de Backup líderes de mercado, conforme quadrante mágico do Gartner, durante estas reuniões restou evidenciado que a migração de base de backup é a parte mais onerosa, tecnicamente, em uma mudança de solução, e que deve ser levado em consideração o impacto do risco de continuidade do negócio, conforme Atas de Reunião em anexo (SEI 3333735 e 3333735).

7.2.3. Importante destacar que o Hardware utilizado para o armazenamento de backup possui uma capacidade ociosa que necessariamente, a bem da economicidade, merece ser utilizada e neste caso deve-se somente contratar a garantia adicional para o hardware existente, uma vez que ele satisfaz a todos os requisitos de segurança preconizados pelo Acórdão TCU 1109/2021.

7.2.4. A opção pela adoção de outra plataforma de backup implicaria a substituição integral do hardware atualmente em uso, ainda que com capacidade ociosa, visto que ele somente funciona com o software de backup atualmente instalado na Fundação, Veritas Netbackup. Além disso, para a montagem do ambiente de redundância e *disaster recover*, em consonância com o estabelecido no Acórdão do TCU seria necessário contratar 2 (dois) novos equipamentos ao invés de apenas 1 (um) na manutenção da atual estrutura, o que além de trazer riscos de continuidade, demandaria um custo mais alto para a administração, conforme evidenciado no item 6.3.8, subitens 6.3.8.1 e 6.3.8.2 deste ETPC.

7.2.5. Políticas de Retenção para backups

7.2.5.1. No último relatório de consumo de backup (SEI nº 2760757) verificou-se que a FUNASA possui 52,75 TB de massa de dados de backup, incluindo Presidência-Brasília e todas as unidades das Superintendências Estaduais - Suest's.

7.2.5.2. Sabemos que a funcionalidade de deduplicação está em uso e a taxa de deduplicação (Deduplication Ratio) está em 98.6% conforme imagem abaixo; A contratação de uma nova solução teria que contemplar uma infraestrutura de armazenamento de transição contendo hardware e software em um ambiente controlado e seguro que suporte a volumetria de aproximadamente 3.2PiB conforme imagem abaixo.

```
Support      NetBackup Support.

greene.Main_Menu> Reports
Entering NetBackup reporting view...

Deduplication  Show deduplication statistics.
Exit           Log out and exit from the current shell.
Process        Show current process status.
Return         Return to the previous menu.
Shell          Shell operations.

greene.Reports> Deduplication
Deduplication statistics
Deduplication technology  MSDP
Deduplication rate        98.637%
Data Protected            3244090333 MB
Space Used For Protection 44205374 MB
Physical free space       44060838 MB
Logical free space        0 MB
Total free space          44060838 MB
Maximum Disk Space        88322008 MB
Used Disk Space           44261169 MB
```

7.2.5.3. Ressalte-se ainda que para iniciar todo o processo backup para a nova solução todas as customizações existentes para atender o ambiente de alta complexidade da Funasa teriam que ser refeitas por não existir a possibilidade de migração de backup e respectivas configurações de fabricantes distintos.

7.2.5.4. Todo o processo de migração afetaria a rastreabilidade temporal dos dados e consequentemente todo o histórico de retenção.

7.2.5.5. A invasão ao sistema do Superior Tribunal de Justiça (STJ), ocorrida no início de novembro do ano passado, que comprometeu a integridade dos arquivos da corte, ao que tudo indica visava servidores ou máquinas de backup. O Superior Tribunal de Justiça (STJ) considerou ter sofrido “**o pior ataque cibernético já empreendido contra uma instituição pública brasileira**, em termos de dimensão e complexidade”. As atividades criminosas também causaram indisponibilidade de serviços de tecnologia da informação (TI) no Conselho Nacional de Justiça (CNJ), Controladoria-Geral da União (CGU), Ministério da Saúde (MS), Governo do Distrito Federal (GDF), entre outros.

7.2.5.6. De acordo com informações do portal do governo digital brasileiro, o Gov.br, o número de serviços digitais oferecidos pelo governo saltou de 737 em 2017 para 2.424 serviços em 2020, sendo que 62% dessa quantia eram considerados pelo governo como totalmente digitais. Desde então o número não parou de crescer. Atualmente, o portal do governo divulga que estão disponíveis **on-line 3.909 serviços de 190 órgãos da administração pública**. Diante desse cenário fica evidente que uma solução de backup e suas respectivas rotinas e retenções é de suma importância para a FUNASA.

7.2.5.7. Com o advento da LGPD e tomando como base a norma ABNT NBR ISO/IEC 27002:2013 que versa sobre as diretrizes para gestão de segurança da informação e levando em consideração os ambientes de risco das organizações.

7.2.5.8. De acordo com o item 12.3.1 da norma, cópias de segurança (backups) de dados e de sistemas devem ser efetuadas e testadas regularmente conforme uma política previamente definida.

7.2.5.9. Ainda sobre a ABNT NBR ISO/IEC 27002:2013, quando da elaboração de um plano de backup, ressaltamos o ITEM “b” que deve ser levado em consideração e diz:

*b) convém que a abrangência (por exemplo, completa ou diferencial) e a **frequência da geração das cópias de segurança reflitam os requisitos de negócio da organização**, além dos requisitos de segurança da informação envolvidos e a criticidade da informação para a operação da organização;*

7.2.5.10. Nesse sentido, Deve-se também levar em consideração o recente Acórdão Nº 1109/2021 – TCU Plenário, abaixo colacionado:

*"orientar os gestores e regulamentar a obrigatoriedade de que as entidades e órgãos públicos aprovelem formalmente e **mantenham atualizadas políticas gerais e planos específicos de backup (para suas bases de dados e sistemas críticos, por exemplo)**, contemplando requisitos mínimos para endereçar os cinco subcontroles do controle 10 (Data Recovery Capabilities) do framework preconizado pelo Center for Internet Security (CIS), em especial quanto à definição do escopo dos dados a serem copiados, suas respectivas periodicidades, tipos, quantidades de cópias, locais de armazenamento, tempos de retenção e outros requisitos de segurança" (grifo nosso)*

7.2.5.11. Em pesquisas livres foram encontradas políticas de backup com o objetivo de estabelecer diretrizes para o processo de cópia e armazenamento de dados, vejamos:

7.2.5.12. **CNJ PORTARIA Nº CJF-POR-2018/00085 de 15 de março de 2018**

[...]

c) mensal: deverá ser programado para execução no primeiro fim de semana de cada mês entre 21h de sexta-feira e 8h da segunda-feira seguinte.

II – quanto à aplicação e retenção e replicação do backup:

a) ambiente de produção do CJF:

a1) proveniente de sistema de arquivos: diário, com retenção de 90 dias; semanal, com retenção de 26 semanas; e mensal, com retenção de 48 meses;

a2) proveniente de sistema operacional: diário, com retenção de 90 dias; semanal, com retenção de 26 semanas; e mensal, com retenção de 48 meses;

a3) proveniente de aplicação: diário, com retenção de 90 dias; semanal, com retenção de 26 semanas; e mensal, com retenção de 48 meses;

a4) proveniente de banco de dados: diário, com retenção de 90 dias; semanal, com retenção de 26 semanas; e mensal, com retenção de 48 meses.

7.2.5.13. **Política de Backup e Recuperação de Dados Digitais da Justiça Federal da 1ª Região PORTARIA PRESI 10264108**

Seção III

Da frequência e retenção dos dados

Art. 13. Os backups dos serviços de TI críticos da Justiça Federal da 1ª Região devem ser realizados utilizando-se as seguintes frequências temporais:

I – diária;

II – semanal;

III – mensal;

IV – anual.

Art. 14. Os serviços de TI críticos da Justiça Federal da 1ª Região devem ser resguardados sob um padrão mínimo, o qual deve observar a correlação frequência/retenção de dados estabelecida a seguir:

I – diária: 2 meses;

II – semanal:

4 meses;

III – mensal: 1 ano;

IV – anual: 5 anos

7.2.5.14. A Justiça Federal também possui um padrão mínimo de 5 anos para backups anuais.

7.2.5.15. **PODER JUDICIÁRIO JUSTIÇA DO TRABALHO TRIBUNAL REGIONAL DO TRABALHO DA 11ª REGIÃO**



PODER JUDICIÁRIO
JUSTIÇA DO TRABALHO
TRIBUNAL REGIONAL DO TRABALHO DA 11ª REGIÃO
Gabinete da Presidência

Backup diário	Dias e horários	Incremental, de segunda a sexta-feira, com início às 21h.	Incremental, de segunda a sexta-feira, com início às 21h.	Completo, todos os dias.
	Retenção	A versão objeto do backup será retida pelo período de trinta (30) dias.	A versão objeto do backup será retida pelo período de trinta (30) dias.	A versão objeto do backup será retida pelo período de quinze (15) dias.
Backup mensal (tipo archive)	Dia	Segundo domingo do mês	Segundo domingo do mês	Segundo domingo do mês
	Retenção	A versão objeto do backup será retida pelo período de um (1) ano	A versão objeto do backup será retida pelo período de um (1) ano	A versão objeto do backup será retida pelo período de um (1) ano
Backup anual (tipo archive)	Dia	Em janeiro do ano seguinte, entre os dias 1º e 28, preferencialmente no primeiro domingo.	Em janeiro do ano seguinte, entre os dias 1º e 28, preferencialmente no primeiro domingo.	Em janeiro do ano seguinte, entre os dias 1º e 28, preferencialmente no primeiro domingo.
	Retenção	A versão objeto do backup será retida pelo período de cinco (5) anos.	A versão objeto do backup será retida pelo período de cinco (5) anos.	A versão objeto do backup será retida pelo período de cinco (5) anos.

7.2.5.16. Conforme imagem acima, o TRT da 11ª Região também possui políticas de backup com retenções previstas para 5 anos.

7.2.5.17. Conselho Federal de Contabilidade PORTARIA CFC N.º 275, DE 5 DE OUTUBRO DE 2020

§ 2º Todos os backups criados deverão ser testados antes de aplicar a programação solicitada. Esses testes deverão incluir uma restauração para comprovar a eficácia do backup, que deverá inserir um atestado de aprovação do administrador de backup.

Art. 8º Os backups realizados em mídias magnéticas e que necessitem de armazenamento para disaster recovery serão guardados em ambientes seguros no Conselho Federal de Contabilidade, observando a sua capacidade, de forma que seja priorizado o armazenamento dos cinco últimos backups diários; dos quatro últimos backups semanais; dos doze últimos backups mensais; e dos cinco últimos backups anuais.

Art. 9º A retenção dos backups deve observar os seguintes prazos:

I. – diário: cinco últimos dias;

II. – semanal: quatro últimas semanas;

III. – mensal: doze últimos meses;

IV. – anual: cinco últimos anos.

7.2.5.18. O Conselho Federal de Contabilidade também possui prazos de retenções definidos alcançando o mínimo de 5 anos de retenção para backups anuais.

7.2.5.19. Como podemos observar vários órgãos possuem políticas de retenções bem definidas. Para manter a continuidade do negócio da Funasa, em sua missão como instituição de promover a saúde pública e a inclusão social por meio de ações de saneamento e saúde ambiental, é fundamental estabelecer mecanismos que permitam a guarda dos dados e sua eventual restauração em casos de perdas por erro humano, ataques externos, catástrofes naturais ou outras ameaças. No sentido de assegurar a proteção dos dados eletrônicos desta Fundação, entendemos que a capacidade de armazenamento, gravação, recuperação dos dados por um período **mínimo de 12 meses**, segurança e disponibilidade das informações para atender às demandas atuais e futuras da Funasa é um período razoável e amplamente praticado dentro da Administração Pública e Federal.

7.2.6. **COMPLIANCE - REGULARIZAÇÃO DAS LICENÇAS VERITAS NETBACKUP**

7.2.6.1. Outro fator que deve ser levado em consideração é o fato de que a capacidade atualmente licenciada no ambiente da FUNASA é de 30 TB (Licenças perpétuas), e conforme discriminado no subitem 2.3.6 deste ETPC a capacidade atualmente em uso é de 52,75 TB.

7.2.6.2. De plano, verifica-se que há uma lacuna de compliance no licenciamento atual, visto que durante os últimos 2 anos a Fundação vem utilizando uma capacidade além da contratada (sobreutilização), sendo necessária a regularização do uso excedente das licenças Veritas Netbackup.

7.2.6.3. Para efeitos de verificação do impacto financeiro para regularização das licenças em sobreutilização, segue demonstrativo de valores para regularização nos termos do EULA (Compliance) e também em valores de mercado:

7.2.6.4. **Licenciamento Atual vs Consumo**

Licenças Adquiridas

Contract Number	Customer Name	Contract Line Status	MSKU	MSKU Description	Quantity	Contract Start Date	Contract End Date
US000000152249	FUNDACAO NACIONAL DE SAUDE FUNASA	EXPIRED	10915-M0374-23	ESSENTIAL 12 MONTHS RENEWAL FOR NETBACKUP PLATFORM BASE COMPLETE ED XPLAT 1 FRONT END TB ONPREMISE STANDARD PERPETUAL LICENSE QTY 0 to 10 GOV	10	14-Jun-18	13-Jun-19
515009002	FUNDACAO NACIONAL DE SAUDE	EXPIRED	10915-M0399-23	ESSENTIAL 12 MONTHS RENEWAL FOR NETBACKUP PLATFORM BASE COMPLETE ED XPLAT 1 FRONT END TB ONPREMISE STANDARD PERPETUAL LICENSE QTY 11 to 50 GOV	20	01-Jun-18	31-May-19

7.2.6.5. Análise de Utilização

Total adquirido: 30 TB

Total utilizado: 52,75 TB (4/Março/2021)

Gap: **23TB**

7.2.6.6. Proposta de Regularização e Renovação (Valores de lista - Compliance)

7.2.6.7. Aquisição COMPLIANCE – REGRA CONTRATO EULA END USER LICENSE AGREEMENT

COMPLIANCE	SKU	SKU DESCRIPTION	SKU SHORT DESCRIPTION	PRICE LIST(MSRP)	QTD	PRICE LIST MSRP (TOTAL)
Renovação Garantia 30 TB	10915-M3-25	ESSENTIAL 60 MONTHS RENEWAL FOR NETBACKUP PLATFORM BASE COMPLETE ED XPLAT 1 FRONT END TB ONPREMISE STANDARD PERPETUAL LICENSE GOV	ESS 60MO RNW FOR NBU PLAT BASE COMPLETE ED XPLAT 1 FRONT END TB ONPREM STD PERPETUAL LIC GOV	R\$ 60.693,96	30	R\$ 1.820.818,80
Compliance 23 TB sem o licenciamento	10915-M3-23	ESSENTIAL 12 MONTHS RENEWAL FOR NETBACKUP PLATFORM BASE COMPLETE ED XPLAT 1 FRONT END TB ONPREMISE STANDARD PERPETUAL LICENSE GOV (BACK MANTAINANCE 12 MONTHS)	ESS 12MO RNW FOR NBU PLAT BASE COMPLETE ED XPLAT 1 FRONT END TB ONPREM STD PERPETUAL LIC GOV (BACK MANTAINANCE 12 MONTHS)	R\$ 10.231,32	23	R\$ 235.320,36
	23369-M3	NETBACKUP PLATFORM BASE COMPLETE ED WITH FLEXIBLE LICENSING XPLAT 1 FRONT END TB PLUS ONPREMISE STANDARD PERPETUAL LICENSE GOV (36 MONTHS)	NBU PLAT BASE COMPLETE ED WITH FLEXIBLE LIC XPLAT 1 FRONT END TB PLUS ONPREM STD PERPETUAL LIC GOV (36MONTHS)	R\$ 75.177,96	23	R\$ 1.729.093,08
TOTAL						R\$ 3.785.232,24

Informações adicionais

- Adequação de 23TB de licenciamento VERITAS NetBackup em uso excedente
- Renovação de Suporte de licenciamento VERITAS NetBackup 30TB
- Período de suporte 36 meses
- Pagamento Unico

Renovação Garantia	BRL	1.820.818,80
TOTAL Compliance	BRL	1.964.413,44
PREÇO TOTAL	BRL	3.785.232,24

7.2.6.8. **Proposta Regularização, Renovação e Expansão (aquisição part-numbers)**

7.2.6.9. Valores Compliance x Regularização processo licitatório Veritas

Valores Compliance

COMPLIAN CE	SKU	SKU DESCRIPTION	SKU SHORT DESCRIPTION	PRICE LIST(MSRP)	QTD	PRICE LIST MSRP (TOTAL)
Renovação Garantia 30 TB	10915- M3-25	ESSENTIAL 60 MONTHS RENEWAL FOR NETBACKUP PLATFORM BASE COMPLETE ED XPLAT 1 FRONT END TB ONPREMISE STANDARD PERPETUAL LICENSE GOV	ESS 60MO RNW FOR NBU PLAT BASE COMPLETE ED XPLAT 1 FRONT END TB ONPREM STD PERPETUAL LIC GOV	R\$ 60.693,96	30	R\$ 1.820.818,80
Compliance 23 TB sem o licenciamento	10915- M3-23	ESSENTIAL 12 MONTHS RENEWAL FOR NETBACKUP PLATFORM BASE COMPLETE ED XPLAT 1 FRONT END TB ONPREMISE STANDARD PERPETUAL LICENSE GOV (BACK MANTAINANCE 12 MONTHS)	ESS 12MO RNW FOR NBU PLAT BASE COMPLETE ED XPLAT 1 FRONT END TB ONPREM STD PERPETUAL LIC GOV (BACK MANTAINANCE 12 MONTHS)	R\$ 10.231,32	23	R\$ 235.320,36
	23369- M3	NETBACKUP PLATFORM BASE COMPLETE ED WITH FLEXIBLE LICENSING XPLAT 1 FRONT END TB PLUS ONPREMISE STANDARD PERPETUAL LICENSE GOV (36 MONTHS)	NBU PLAT BASE COMPLETE ED WITH FLEXIBLE LIC XPLAT 1 FRONT END TB PLUS ONPREM STD PERPETUAL LIC GOV (36MONTHS)	R\$ 75.177,96	23	R\$ 1.729.093,08
TOTAL						R\$ 3.785.232,24

**TOTAL Regularização
compliance** **BRL** **3.785.232,24**

TOTAL Processo licitatório **BRL** **1.974.629,39**

CONDIÇÃO ESPECIAL **BRL** **(1.810.602,85)**

7.2.6.10. **Regularização processo licitatório – Part Number Veritas – Cotação de mercado**

Regularização Processo licitatório	Tipo de licença	Quantidade	Valor Unitário Mercado	Valor total Estimado Mercado
Renovação Suporte Software de Backup	TB	30	R\$ 27.246,66	R\$ 817.399,80
Expansão do Licenciamento Software para backup	TB	23	R\$ 50.314,33	R\$ 1.157.229,59
			TOTAL	R\$ 1.974.629,39

7.2.6.11. Conforme demonstrado acima, verifica-se que há um impacto financeiro considerável no processo de regularização das licenças em sobreutilização no ambiente da Funasa durante os últimos 2 anos.

7.2.6.12. É importante ressaltar que este estudo demonstrando os valores da regularização das licenças, nos termos do EULA (Compliance), à preço de catálogo, foi realizado no primeiro trimestre deste ano (2021) considerando a cotação do dólar daquele período.

7.2.6.13. Tendo em vista que a cotação comercial do dólar reflete no custo dos serviços para regularização das licenças, os valores acima definidos para conformidade de uso (compliance) podem sofrer alterações, em razão da variação da cotação da moeda.

7.2.7. **Em face do exposto, considerando:**

I. O legado existente: (licenças perpétuas) e Hardware com capacidade ociosa;

II. A possibilidade de aproveitamento integral do legado, e seu atendimento aos requisitos preconizados pelo Acórdão TCU 1109/2021;

III. A dificuldade operacional para migração da solução e os riscos que este processo apresenta;

IV. A economicidade comprovada, mediante pesquisa de preços, em manter e expandir a atual solução em uso na FUNASA.

7.2.8. A equipe de planejamento da contratação decidiu optar pela solução do cenário 1 - Manter e Expandir a Atual Solução, com 36 meses de garantia.

Observação:

I. O valor demonstrado para regularização das licenças em sobreutilização no ambiente da Funasa não foi levado em consideração para a decisão de escolha do melhor cenário.

II. O estudo foi apresentado por se tratar de um risco relativo à uma eventual mudança de solução, visto que há uma lacuna de compliance no licenciamento atual e este custo deverá ser levado em consideração em caso de adoção de outra plataforma.

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

8.1. O custo total da contratação foi estimado em R\$ 6.287.914,25 (seis milhões, duzentos e oitenta e sete mil novecentos e quatorze reais e vinte e cinco centavos) e encontra-se detalhado na Nota Técnica de Elaboração de Pesquisa de Preços (3335507), item 6.1.

9. **CONSOLIDAÇÃO DA SOLUÇÃO ESCOLHIDA**

9.1. Conforme sintetizado nos itens anteriores, a consolidação da solução escolhida foi realizada considerando os aspectos do ponto de vista técnico e econômico.

ITEM	DESCRIÇÃO	QUANTIDADE
1	Renovação de software de Backup	30
2	Expansão de software de Backup	40
3	Serviço Especializado para os itens 1 e 2	12
4	Renovação de Garantia de Hardware de Backup	1
5	Expansão de Hardware de Backup	1
6	Serviço Especializado para os itens 4 e 5	12
7	Aquisição de Solução para Backup de Office365	3190
8	Serviço Especializado para o item7	12
9	Repasse de conhecimento para o item 7	1

Tabela 35 - Consolidação da solução escolhida.

10. DECLARAÇÃO DE VIABILIDADE DA CONTRATAÇÃO

10.1. 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.

10.2. 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.

11. ASSINATURAS

11.1. Em conformidade com a Instrução Normativa nº 01/2019 SGD/ME, assinam este documento Integrantes Técnico e Requisitante da Equipe de Planejamento da Contratação e pela autoridade máxima da Área de TIC.

EQUIPE DE PLANEJAMENTO DA CONTRATAÇÃO		SIAPÉ	E-MAIL	TELEFONE
Integrante Requisitante:	Telvio Martins de Mello	1.425.456	telvio.mello@funasa.gov.br	(61) 3314-6575
Integrante Técnico:	André Wilson Pimenta Santana	1.347.001	andre.pimenta@funasa.gov.br	(61) 3314-6417

Integrante Administrativo	Márcio Biage da Silveira	1.749.292	marcio.silveira@funasa.gov.br	(61) 3314-6365
----------------------------------	--------------------------	-----------	-------------------------------	----------------

Tabela 36 - Equipe de Planejamento da Contratação.

Autoridade máxima da área de TIC
<p>Telvio Martins de Mello</p> <p>Coordenador-Geral de Modernização e de Tecnologia da Informação</p> <p>SIAPE 1.425.456</p>

Tabela 37 - Autoridade máxima da área de TIC.

11.2. Nos termos da Instrução Normativa nº 01/2019 SGD/ME, aprovo este Estudo Técnico Preliminar da Contratação.

Autoridade Competente
<p>Vinicius Pinto Correa</p> <p>Diretor do Departamento de Administração</p> <p>SIAPE 6.002.124-1</p>

Tabela 38 - Autoridade Competente.



Documento assinado eletronicamente por **Andre Wilson Pimenta Santana, Coordenador de Inovação e Infraestrutura Tecnológica**, em 19/11/2021, às 15:34, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do [Decreto nº 8.539, de 8 de outubro de 2015](#).



Documento assinado eletronicamente por **Telvio Martins de Mello, Coordenador-Geral de Modernização e de Tecnologia da Informação**, em 19/11/2021, às 15:40, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do [Decreto nº 8.539, de 8 de outubro de 2015](#).



Documento assinado eletronicamente por **Vinicius Pinto Correa, Diretor do Departamento de Administração**, em 19/11/2021, às 16:08, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do [Decreto nº 8.539, de 8 de outubro de 2015](#).

A autenticidade deste documento pode ser conferida no site <https://sei.funasa.gov.br/consulta>, informando o código verificador **3370878** e o código CRC **8211488B**.



Referência: Processo nº 25100.000386/2021-95

SEI nº 3370878